



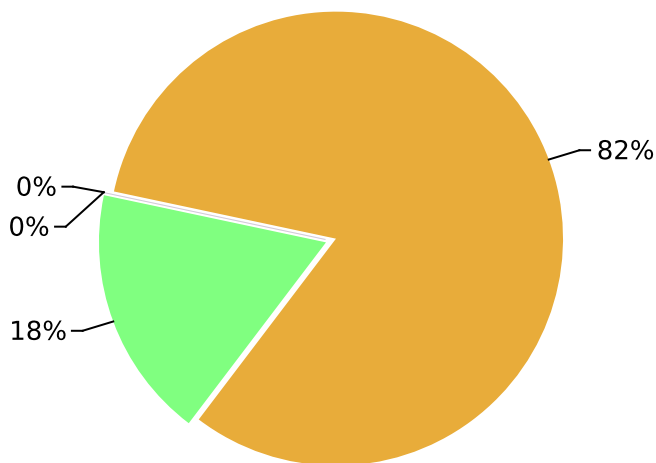
Hệ thống hỗ trợ nâng cao chất lượng tài liệu

KẾT QUẢ KIỂM TRA TRÙNG LẬP TÀI LIỆU

THÔNG TIN TÀI LIỆU

Tác giả	Lê Mạnh Cường
Tên tài liệu	Luận Văn ThsKT - NGHIÊN CỨU GIẢI PHÁP PHÁT HIỆN XÂM NHẬP TÍCH HỢP CHO MẠNG LAN -Le Manh Cuong v2.3
Thời gian kiểm tra	09-05-2021, 15:41:21
Thời gian tạo báo cáo	09-05-2021, 15:43:52

KẾT QUẢ KIỂM TRA TRÙNG LẬP



- Câu (đoạn) người dùng phản hồi
- Phần trăm câu (đoạn) hệ thống không kiểm tra
- Phần trăm câu (đoạn) không trùng lặp
- Phần trăm câu (đoạn) trùng lặp

Điểm	18
Nguồn trùng lặp tiêu biểu	[text.123doc.org, 123doc.org, viblo.asia]

(*) Kết quả trùng lặp phụ thuộc vào dữ liệu hệ thống tại thời điểm kiểm tra

DANH SÁCH CÂU TRÙNG LẬP

Trang	Câu trùng lập	Nguồn	Điểm
1	HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG	Học viện Công nghệ Bưu chính Viễn thông Hà Nội 17	100
		https://text.123doc.org/document/4781200-hoan-thien-cong-tac-quan-ly-du-an-dau-tu-xay-dung-tai-ban-quan-ly-du-an-quan-bac-tu-liem-thanh-pho-ha-noi-tt.htm	
1	NGHIÊN CỨU GIẢI PHÁP PHÁT HIỆN XÂM	Do yêu cầu thực tế trên tôi lựa chọn đề tài nghiên cứu khoa học là N ghi ên cứu giải pháp phát hiện xâm nhập trái phép cho máy tính tham gia mạng	100
		https://text.123doc.org/document/3520589-nghien-cuu-giai-phap-phat-hien-xam-nhap-trai-phep-cho-may-tinh-tham-gia-mang.htm	
2	HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG	Học viện Công nghệ Bưu chính Viễn thông Hà Nội 17	100
		https://text.123doc.org/document/4781200-hoan-thien-cong-tac-quan-ly-du-an-dau-tu-xay-dung-tai-ban-quan-ly-du-an-quan-bac-tu-liem-thanh-pho-ha-noi-tt.htm	
2	NGHIÊN CỨU GIẢI PHÁP PHÁT HIỆN XÂM	Do yêu cầu thực tế trên tôi lựa chọn đề tài nghiên cứu khoa học là N ghi ên cứu giải pháp phát hiện xâm nhập trái phép cho máy tính tham gia mạng	100
		https://text.123doc.org/document/3520589-nghien-cuu-giai-phap-phat-hien-xam-nhap-trai-phep-cho-may-tinh-tham-gia-mang.htm	

Trang	Câu trùng lặp	Nguồn	Điểm
2	CHUYÊN NGÀNH : HỆ THỐNG THÔNG TIN	nbsp Báo Cáo Thực Tập Kiểm Soát Nội Bộ Hệ Thống ERP TRƯỜNG ĐẠI HỌC MỞ THÀNH PHỐ HỒ CHÍ MINH KHOA CÔNG NGHỆ THÔNG TIN HỌ VÀ TÊN TÁC GIẢ LÊ THỊ TÚ HOAN KIỂM SOÁT NỘI BỘ HỆ THỐNG ERP TẠI CÔNG TY TNHH PHẦN MỀM 3S BÁO CÁO THỰC TẬP TỐT NGHIỆP Ngành Công Nghệ Thông Tin Hướng chuyên ngành Hệ Thống Thông Tin Quản Lý Lớp DH 13 TK 02 GIÁO VIÊN HƯỚNG DẪN Nguyễn Thị Mai Trang Thành phố Hồ Chí Minh Năm 2016 LỜI CẢM ƠN Đầu tiên em xin gửi lời cảm ơn chân thành đến Quý thầy cô trường Đại học Mở đã tận tình trong quá trình giảng dạy và truyền đạt kiến thức cho em trong suốt thời gian học tập tại trường	100
		https://text.123doc.org/document/4781624-bao-caoc-thuc-tap-kiem-soat-noi-bo-he-thong-erp.htm	
4	Tôi cam đoan đây là sản phẩm nghiên cứu của riêng tôi.	NGUYỄN THỊ HỒNG HƯƠNG HÀ NỘI 2017 LỜI CAM ĐOAN Tôi xin cam đoan đây là sản phẩm nghiên cứu độc lập của riêng tôi	76
		https://text.123doc.org/document/4744988-xay-dung-ung-dung-tin-tuc-video-tren-nen-tang-android-tt.htm	
4	Các số liệu, kết quả nêu trong luận văn là trung thực và chưa từng được ai công bố trong bất kỳ công trình nào khác.	Các số liệu kết quả nêu trong luận văn là trung thực và chưa từng được ai công bố trong bất kỳ công trình nào khác Đà Nẵng ngày tháng năm Người cam đoan Đặng Trương Hạnh Nguyễn MỤC LỤC MỞ ĐẦU 1 CHƯƠNG 1	100
		https://text.123doc.org/document/4620331-phat-trien-thuong-hieu-vinafor-da-nang.htm	
4	Tôi xin chịu trách nhiệm về luận văn của mình.	Tôi xin chịu trách nhiệm về luận văn của mình	100
		https://text.123doc.org/document/3310446-cai-toi-tru-tinh-trong-tho-nguyen-quang-thieu.htm	

Trang	Câu trùng lặp	Nguồn	Điểm
5	MỤC LỤC LỜI CẢM ƠN LỜI CAM ĐOAN	Hà Nội ngày 06 tháng 06 năm 2016 TÁC GIẢ LUẬN VĂN N gu yễn Thị Bích Ngọc 2 MỤC LỤC LỜI CẢM ƠN i LỜI CAM ĐOAN ii DANH MỤC CHỮ VIẾT TẮT vi DANH MỤC CÁC BẢNG vii DANH MỤC HÌNH VẼ viii MỞ ĐẦU 6 CHƯƠNG I https://text.123doc.org/document/4729627-dspace-at-vnu-nghien-cuu-de-xuat-giai-phap-quan-ly-tong-hop-chat-thai-ran-sinh-haotj-tai-huyen-thanh-oai-thanh-pho-ha-noi.htm	100
5	ii MỤC LỤC.....	Hà nội tháng 9 năm 2011 Tác giả Hoàng Ngọc Thành ii MỤC LỤC TRANG PHỤ BÌA LỜI CẢM ƠN i MỤC LỤC ii DANH MỤC CÁC KÝ HIỆU VÀ TỪ VIẾT TẮT ii DANH MỤC CÁC BẢNG vii DANH MỤC CÁC HÌNH viii ĐẶT VẤN ĐỀ 1 C hự ơ n g 1 TỔNG QUAN VỀ VẤN ĐỀ NGHIÊN CỨU 3 1 1 https://text.123doc.org/document/4422445-nghien-cuu-sinh-truong-dac-diem-lam-hoc-va-kha-nang-tich-luy-cacbon-cua-rung-keo-lai-acacia-hybrid-trong-thuan-loai-tai-cong-ty-lam-nghiep-ben-hai-tin.htm	100
5	iii DANH MỤC VIẾT TẮT DANH MỤC HÌNH ẢNH.....	Kết quả của nghiên cứu là xây dựng thành công mạng lưới điện đối với các lớp đối tượng trạm điện cột điện đường dây dẫn điện cũng như thể hiện được các điểm phân bố trung tâm giúp người sử dụng dễ dàng trong việc quản lý hiện trạng các cơ sở vật chất và phân bố nhân lực theo mạng lưới điện giảm thiểu chi phí tiết kiệm thời gian ii MỤC LỤC LỜI CẢM ƠN i TÓM TẮT ii MỤC LỤC iii DANH MỤC VIẾT TẮT v DANH MỤC BẢNG BIỂU vi DANH MỤC HÌNH ẢNH vii CHƯƠNG 1 https://text.123doc.org/document/3754835-ung-dung-gis-phan-bo-mang-luoi-dien-theo-nhan-luc-tinh-binh-duong.htm	100
5	vii MỞ ĐẦU 1 CHƯƠNG I.	VII MỞ ĐẦU 1 CHƯƠNG I TỔNG QUAN CÁC VẤN ĐỀ CẦN NGHIÊN CỨU 4 1 1	100

Trang	Câu trùng lặp	Nguồn	Điểm
		https://text.123doc.org/document/4555568-ta-thi-xuan-pdf.htm	
5	TỔNG QUAN VỀ XÂM NHẬP VÀ PHÁT HIỆN XÂM NHẬP...2	C hư ơ n g này trình bày tổng quan về xâm nhập và phát hiện xâm phạm 1 1	84
		https://text.123doc.org/document/4490861-danh-gia-hieu-nang-mot-so-thuat-toan-phan-lop-cho-phat-hien-xam-nhap-tt.htm	
5	CÁC HỆ THỐNG PHÁT HIỆN XÂM NHẬP.....17	Các hệ thống có nhiệm vụ nhậ vậ đợc gọi là hệ thống phát hiện xâm nhập 1 3 1	85
		https://text.123doc.org/document/4729605-dspace-at-vnu-danh-gia-hieu-qua-mot-so-thuat-toan-trong-phat-hien-xam-nhap-mang.htm	

Trang	Câu trùng lặp	Nguồn	Điểm
62	3.4. Kết luận Chương III..... 62	Nội dung của luận văn 3 CHƯƠNG 1 TỔNG QUAN VỀ THI CÔNG XÂY DỰNG CÔNG TRÌNH VÀ QUẢN LÝ CHI PHÍ THI CÔNG XÂY DỰNG CÔNG TRÌNH 4 1 1 Tổng quan về thi công xây dựng công trình và quản lý thi công xây dựng công trình 4 1 1 1 Tổng quan về thi công xây dựng công trình 4 1 1 2 Tổng quan về quản lý thi công xây dựng công trình 5 1 2 Chi phí và quản lý chi phí thi công xây dựng công trình 8 1 2 1 Chi phí thi công xây dựng công trình 8 1 2 2 Quản lý chi phí thi công xây dựng công trình 15 1 3 Những nhân tố ảnh hưởng đến công tác quản lý chi phí thi công xây dựng công trình 20 1 3 1 Các nhân tố bên trong doanh nghiệp 20 1 3 2 Các nhân tố bên ngoài doanh nghiệp 22 1 4 Kết luận chương I 22 CHƯƠNG 2 NGHIÊN CỨU THỰC TRẠNG QUẢN LÝ CHI PHÍ TRONG QUÁ TRÌNH THI CÔNG XÂY DỰNG CÔNG TRÌNH TẠI TỔNG CÔNG TY XÂY DỰNG CÔNG TRÌNH GIAO THÔNG 4 24 2 1 Giới thiệu chung về Tổng công ty Xây dựng công trình giao thông 4 24 2 1 1 Giới thiệu chung 24 2 1 2 Chức năng nhiệm vụ ngành nghề kinh doanh của Tổng công ty 26 2 2 Thực trạng công tác quản lý chi phí trong quá trình thi công xây dựng công trình tại Tổng công ty Xây dựng công trình giao thông 4 trong những năm qua 27 2 2 1 Mô hình quản lý và chức năng nhiệm vụ bộ máy của Tổng công ty 27 2 2 2 Tình hình thực hiện dự án của Tổng công ty từ năm 2009 2012 34 2 2 3 Thực trạng công tác quản lý chi phí trong quá trình thi công xây dựng 39 2 3 Đánh giá công tác quản lý chi phí thi công xây dựng công trình trong thời gian qua 44 2 3 1 Những kết quả đạt được 44 2 3 2 Những tồn tại trong công tác quản lý chi phí thi công xây dựng công trình và nguyên nhân 45 2 4 Kết luận chương II 51 CHƯƠNG 3 ĐỀ XUẤT GIẢI PHÁP QUẢN LÝ CHI PHÍ TRONG QUÁ TRÌNH THI CÔNG TẠI TỔNG CÔNG TY XÂY DỰNG CÔNG TRÌNH GIAO THÔNG 452 3 1 Định hướng thi công xây dựng các công trình tại Tổng công ty xây dựng công trình giao thông 4 trong thời gian tới	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>52 3 1 1 Chiến lược phát triển của Tổng công ty đến năm 2015 và 2020 52 3 1 2 Nội dung chiến lược phát triển tổng công ty 55 3 2 Những thuận lợi khó khăn trong và những cơ hội thách thức trong hoạt động thi công xây dựng các công trình tại Tổng công ty Xây dựng công trình giao thông 4 59 3 2 1 Thuận lợi 59 3 2 2 Khó khăn 60 3 2 3 Những cơ hội thách thức 61 3 3 Đề xuất một số giải pháp tăng cường công tác quản lý chi phí trong quá trình thi công xây dựng công trình tại tổng công ty xây dựng công trình giao thông 4 62 3 3 1 Cơ sở đề xuất các giải pháp quản lý chi phí trong quá trình thi công xây dựng công trình 62 3 3 2 Các giải pháp tăng cường công tác quản lý chi phí trong quá trình thi công xây dựng công trình tại Tổng công ty xây dựng công trình giao thông 4 62 3 3 3 Ứng dụng bài toán tối ưu tìm phương án vận chuyển trên công trường 85 3 4 Kết luận chương III 94 KẾT LUẬN V KIẾN NGHỊ 96 DANH MỤC BẢNG Bảng 2 1 Năng lực kinh nghiệm của Tổng công ty 35 Bảng 2 2 Thông tin tài chính Tổng công ty trong 3 năm 36 Bảng 2 3 Các dự án điển hình của Tổng công ty 37 Bảng 2 4 Vật tư thi công của Tổng công ty 43 Bảng 2 5 Một số Định mức không phù hợp AF 33320 AF 33330 47 Bảng 2 6 Một số Định mức không phù hợp AF 33410 48 Bảng 3 1 Nội dung của chiến lược phát triển Tổng công ty 54 Bảng 3 2 Bảng tính đơn giá xây dựng chi tiết tổng quát 72 Bảng 3 4 Bảng năng suất thực nghiệm 83 Bảng 3 5 Khối lượng đất đắp từ các điểm cấp 89 Bảng 3 6 Khối lượng đất đắp đến các điểm nhận 89 Bảng 3 7 Tổng hợp khối lượng đất của các điểm cấp và nhận 89 Bảng 3 8 Đường vận chuyển của các điểm cấp và nhận 90 Bảng 3 9 Đơn giá cước vận chuyển cho công tác vận chuyển đất 91 DANH MỤC HÌNH Hình 2 1 Sơ đồ tổ chức Tổng công ty 28 Hình 2 2 Giá trị sản lượng của Tổng công ty qua các năm 35 Hình 3 1 Sơ đồ vận chuyển từ 1 điểm cấp đến nhiều điểm nhận 86 Hình 3 2 Sơ đồ vận chuyển từ một số điểm cấp đến một điểm nhận 86 Hình 3 3 Sơ đồ vận</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		chuyển từ một số điểm cấp đến một số điểm nhận 87 Hình 3 4 Sơ đồ vận chuyển đất từ điểm cấp đến điểm nhận 88 1 MỞ ĐẦU 1	
		https://text.123doc.org/document/2291609-de-xuat-mot-so-giai-phap-quan-ly-chi-phi-trong-qua-trinh-thi-cong-nham-giam-gia-thanh-cong-trinh-tai-tong-cong-ty-xay-dung-cong-trinh-giao-thong-4.htm	
6	KẾT LUẬN 63 DANH MỤC CÁC TÀI LIỆU THAM KHẢO 64 v	CÁC ĐỀ XUẤT VÀ KIẾN NGHỊ CỦA EM VỀ CÔNG TY NHẪM NÂNG CAO HIỆU QUẢ TRONG CÔNG TÁC QUẢN TRỊ LỰC LƯỢNG BÁN HÀNG 62 KẾT LUẬN 63 Danh mục các tài liệu tham khảo 64 SVTH Đỗ Nhật Tân Khóa luận tốt nghiệp GVHD ThS Hồ Nguyễn Khoa LỜI MỞ ĐẦU 1	90
		https://text.123doc.org/document/4826566-giai-phap-nang-cao-cong-tac-quan-tri-luc-luong-ban-hang-tai-cong-ty-tnhh-trung-tam-dich-vu-total-viet-nam.htm	
7	Ký hiệu Tên Tiếng Anh Ý nghĩa Tiếng Việt	2 M B 4 X Y amp Y SVTH Lê Thị Hồng Thanh Lớp K45E6 Khóa luận tốt nghiệp GVHD ThS Nguyễn Ngọc Yến Nguyễn Ngọc Nga DANH MỤC TỪ VIẾT TẮT Ký hiệu Tên tiếng anh Ý nghĩa 9 lt EE 9	73
		https://text.123doc.org/document/2574911-giai-phap-vuot-rao-can-moi-truong-nham-day-manh-xuat-khau-hang-may-tre-dan-sang-thi-truong-nhat-ban-cua-cong-ty-tnhh-hong-tien.htm	
7	ARP Address Resolution Protocol Giao thức phân giải địa chỉ	ARP Address Resolution Protocol Giao thức phân giải địa chỉ ATM Asynchronous Transfer Model Chế độ Truyền tải Bất đồng bộ BGP Border Gateway Protocol Giao thức cổng nối biên	100
		https://text.123doc.org/document/4327182-tim-hieu-ve-giam-sat-va-danh-gia-mang.htm	
7	Công nghệ mô phỏng hình ảnh bằng máy tính	Tôi muốn mang hơi ấm và trực giác của những bức vẽ tay tới công nghệ mô phỏng hình ảnh bằng máy tính	100

Trang	Câu trùng lặp	Nguồn	Điểm
		https://vi.wikipedia.org/wiki/Người đẹp tóc mây	

Trang	Câu trùng lặp	Nguồn	Điểm
7	CPU Central Processing Unit Bộ xử lý trung tâm	<p>10 1 5 1 C om mu ni ty s tri ng 19 1 5 2 View 20 1 5 3 SNMP Access Con tro l List 21 CHƯƠNG II PHẦN MỀM QUẢN LÝ HỆ THỐNG MẠNG ZABBIX 23 CHƯƠNG III TRIỂN KHAI PHẦN MỀM QUẢN LÝ HỆ THỐNG MẠNG ZABBIX 25 KẾT LUẬN 44 TÀI LIỆU THAM KHẢO 45 Khoa Khoa học máy tính Lớp CCMM 07 A N gu yễn Thanh Hưng Quản lý hệ thống mạng cho doanh nghiệp bằng phần mềm Zab bi x 5 DANH MỤC HÌNH ẢNH Hình 1 Các phương thức của SNMP 17 Hình 2 Cấu trúc bảng tin SNMP 21 Hình 3 P h u ơ n g th u c gi á m s á t Poll 22 Hình 4 P h u ơ n g th u c gi á m s á t Alert 22 Hình 5 Cài đặt hệ điều hành CentOS 6 5 trên máy ảo 25 Hình 6 Khai báo các thông số cần thiết khi cài CentOS 25 Hình 7 Cài Repo trên CentOS 26 Hình 8 Cài đặt A pa che cho máy chủ 26 Hình 9 Cài hệ cơ sở dữ liệu MySQL 27 Hình 10 Cài đặt PHP 27 Hình 11 Cài đặt Repo cho Zab bi x 2 4 27 Hình 12 Chọn phiên bản phù hợp nếu cài từ Source trên website của Zab bi x 28 Hình 13 Cài Zab bi x từ Packages 28 Hình 14 Cài đặt Zab bi x Agent để quản lý thông tin của máy chủ 28 Hình 15 Cấu hình địa chỉ máy chủ cho Agent 29 Hình 16 Cấu hình lại thời gian cho Zab bi x 29 Hình 17 Import các Da ta ba se mặc định của Zab bi x 30 Hình 18 Cấu hình các thông số cho Zab bi x Ser ve r 30 Hình 19 Giao diện cài đặt của Zab bi x 2 4 31 Hình 20 Giao diện kiểm tra các cấu hình của Zab bi x 32 Hình 21 Giao diện khai báo cơ sở dữ liệu và tài khoản mật khẩu 32 Hình 22 Giao diện khai báo ip cổng và tên máy chủ 33 Hình 23 Giao diện kiểm tra lại thông tin trước khi cài đặt 33 Hình 24 Giao diện sau khi cài đặt thành công 34 Hình 25 Giao diện đăng nhập của Zab bi x 2 4 34 Hình 26 Giao diện sau khi đăng nhập thành công 35 Hình 27 Khởi động Zab bi x Ser ve r để tiếp nhận các thông tin từ Agent 35 Hình 28 Giao diện thông tin CPU của máy chủ 35 Hình 29 Giao diện thông tin RAM của máy chủ 36 Khoa Khoa học máy tính Lớp CCMM 07 A N gu yễn Thanh Hưng Quản lý hệ thống mạng cho doanh nghiệp bằng</p>	100

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>phần mềm Zab bi x 6 Hình 30 Giao diện thông tin hiệu năng của máy chủ 36 Hình 31 Cài đặt SSMTP 36 Hình 32 Gửi mail bằng sc ri pt 37 Khoa Khoa học máy tính Lớp CCMM 07 A N gu yễn Thanh Hưng Quản lý hệ thống mạng cho doanh nghiệp bằng phần mềm Zab bi x 7 DANH MỤC CÁC TỪ VIẾT TẮT Từ viết tắt Giải thích SNMP S im p le Network M an ag em ent P ro to co l giao thức quản lý mạng đơn giản HĐH Hệ điều hành SNMPv 2 Phiên bản thứ 2 SNMPv 3 Phiên bản thứ 3 CPU CPU Cen tra l P ro ces sin g Unit Bộ xử lý trung tâm RAM R an dom Access M em ory bộ nhớ truy xuất ngẫu nhiên IETF In te r ne t En gi ne e ri ng Task Force tạm dịch là Lực Lượng Quản Lý Kỹ Thuật</p> <p>https://text.123doc.org/document/4309760-quan-ly-he-thong-mang-cho-doanh-nghiep-bang-phan-mem-zabbix.htm</p>	
7	DDOS Distributed Denial of Service	<p>Lưu Nội dung Text Tấn công DDOS và Phân tích các kỹ thuật Anti DDoS DISTRIBUTED DENIAL OF SERVICE DDOS GIỚI THIỆU Dis tri bu te d De nia l Of Ser vi ce DDoS là kỹ thuật tấn công làm các ISP lo âu giới hacker chính thống thì không công nhận DdoS là kỹ thuật tấn công chính thống</p> <p>http://tailieu.vn/doc/tan-cong-ddos-va-ph-an-ti-ch-c-a-c-k-y-t-h-u-a-t-a-n-t-i-ddos-639101.html</p>	100

Trang	Câu trùng lặp	Nguồn	Điểm
7	Tấn công từ chối dịch vụ phân tán	<p>Do đó hệ thống sẽ không còn tài nguyên để phục vụ các yêu cầu sau Hình thức chủ yếu của kiểu này tấn công từ chối dịch vụ phân tán Loại 2 Làm cho hệ thống bị treo tê liệt do tấn công vào đặc điểm của hệ thống hoặc lỗi về an toàn thông tin Tin tặc lợi dụng kẽ hở an toàn thông tin của hệ thống để gửi các yêu cầu hoặc các gói tin không hợp lệ không đúng theo tiêu chuẩn một cách cố ý khiến cho hệ thống bị tấn công khi nhận được yêu cầu hay gói tin C hu yền đề an toàn mạng www A the na Edu Vn Trang 2 này xử lý không đúng hoặc không theo trình tự đã được thiết kế dẫn đến sự sụp đổ của chính hệ thống đó Diễn hình là kiểu tấn công Ping of Death hoặc SYN Flood 2 Các cách thức tấn công 2 1 Tấn công thông qua kết nối SYN Flood At ta ck Được xem là một trong những kiểu tấn công DoS kinh điển nhất</p> <p>https://text.123doc.org/document/4756887-de-tai-phong-chong-dos-ddos.htm</p>	100
7	DNS Domain Name Servers Hệ thống phân giải tên miền	<p>DSL Di gi ta l Subsc ri be r Line Đường dây thuê bao số là công nghệ phục vụ mạng truy nhập truyền dẫn giữa khách hàng và nhà cung cấp dịch vụ truyền tải trên đường dây điện thoại DNS D om ai n Name Sys tem Hệ thống phân giải tên miền DHCP DiffServ Dy na mi c Host Confi gu ra ti on P ro to co l giao thức cấu hình động máy chủ Diffe ren tia te d se r vi ces Các dịch vụ khác biệt Ex ten de d B in ary Coded Dec im al In te r chang e Code mã EBCDIC trao đổi mở rộng của số thập phân đợc mã hóa bằng nhị phân 5 Tìm hiểu về giám sát và đánh giá mạng Lê Gia Vĩnh EIGRP E nhan ced IGRP FDDI Fiber Dis tri bu te d Data In te rface giao diện số liệu phân bố theo cáp quang FTP File T ran sfer P ro to co l Giao thức truyền tập tin GTP GTP là một nhóm giao thức truyền thông dựa trên nền công nghệ IP</p> <p>https://text.123doc.org/document/4327182-tim-hieu-ve-giam-sat-va-danh-gia-mang.htm</p>	71

Trang	Câu trùng lặp	Nguồn	Điểm
7	DOS Denial of Service Tấn công từ chối dịch vụ	Kiểu tấn công sẽ khiến cho hệ thống không thể sử dụng được vì tài nguyên đã bị sử dụng hết không còn tiến trình để thực thi nữa 2 3 KHÁI NIỆM DDOS DISTRIBUTED DENIAL OF SERVICE Tấn công từ chối dịch vụ DoS nhằm mục đích ngăn cản người dùng truy cập hợp pháp vào hệ thống máy tính hay hệ thống mạng của vi c tim	88
		https://text.123doc.org/document/2448535-tim-hieu-tan-cong-ddos-va-cach-phong-chong.htm	

Trang	Câu trùng lặp	Nguồn	Điểm
7	FTP File Transfer Protocol Giao thức truyền tải tập tin	<p>CÁC TỪ VIẾT TẮT Từ viết tắt Từ đầy đủ</p> <p>Giải nghĩa AAL2 ATM a da p ta ti on layer type 2 Lớp thích ứng ATM kiểu 2</p> <p>Abis in te rface be tween BSC and BTS in GSM ne tworks Giao diện giữa BSC và BTS trong mạng GSM ALCAP access link con tro l app li ca ti on part Phần ứng dụng điều khiển liên kết truy nhập AM</p> <p>ack no w le dge mode in RLC Chế độ báo nhận trong RLC AMR a da p ti ve multi rate Đa tốc độ thích ứng BCH b roa d ca st chan ne l Kênh quảng bá BLER Block Error Rate Tỷ lệ lỗi khối BSC base s ta ti on con tro l le r Khối điều khiển trạm gốc BSS base s ta ti on su bsys tem Phân hệ trạm gốc BSSMAP base s ta ti on su bsys tem ma na g em ent app li ca ti on part Phần ứng dụng quản lý phân hệ trạm gốc CCPCH co m mon con tro l p hy si ca l chan ne l Kênh vật lý điều khiển chung CPICH co m mon pilot chan ne l Kênh hoa tiêu chung CRC cyc li c re du n dan cy check Kiểm dư vòng CS cir cui t swit che d C huy ển mạch kênh DCCH de di ca te d con tro l chan ne l Kênh điều khiển chuyên dụng DCH de di ca te d chan ne l Kênh dành riêng DPCH de di ca te d p hy si ca l chan ne l Kênh vật lý dành riêng DRNC drift radio ne twork con tro l le r Drift RNC DSCH do wn lin k s ha re d chan ne l Kênh chia sẻ đường xuống DTAP di re ct tra nsfer app li ca ti on part Phần ứng dụng truyền tải trực tiếp DTCH de di ca te d tra ffic chan ne l Kênh lưu lượng dành riêng EDGE e nhan ced data rates for GSM e vo lu ti on EDGE là công nghệ được sử dụng làm tiền đề để tiến lên công nghệ 3G FACH forward access chan ne l Kênh truy nhập đường xuống FDD f re quen cy di vi si on du p le x Song công chia theo tần số FP frame pro to co l Giao thức khung FTP file tra nsfer pro to co l Giao thức truyền tải tập tin Gb GPRS in te rface be tween SGSN and GSM BSS Giao diện giữa SGSN và hệ thống trạm gốc GSM GERAN GSM EDGE radio access ne twork Mạng truy nhập vô tuyến GSM EDGE GGSN ga te way GPRS su pport node Nút định tuyến GPRS GMSC ga te way MSC Tổng đài vô tuyến cổng GSM</p>	100

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>G lo ba l Sys tem for Mo bi le C om mu ni ca ti on Hệ thống thông tin di động toàn cầu HLR home lo ca ti on re gi s te r Bộ ghi định vị thường trú HO hạn do ve r C huy ển giao HSDPA high speed do wn lin k pa c ke t access Truy cập gói đường xuống tốc độ cao HS DSCH high speed do wn lin k s ha re d chan ne l Kênh chia sẻ đường xuống tốc độ cao IFHO inter f re quen cy hard hạn do ve r C huy ển giao cứng giữa các tần số InFHHO intra f re quen cy hard hạn do ve r C huy ển giao cứng trong tần số IP In te r ne t pro to co l Giao thức in te r ne t ITU In te r na ti o na l Te le co m mu ni ca ti on Union Liên minh viễn thông quốc tế KPI key pe rfor man ce in di ca to r Bộ tham số chất lượng mạng cơ bản MAC me di um access con tro l me s sa ge au then ti ca ti on code Điều khiển truy nhập môi trường MMS mu l ti me di a me s sa gin g se r vi ce Dịch vụ nhắn tin đa phương tiện MOC mobile o ri gi na te d call Cuộc gọi đi MSC mobile swit chi ng cen tre Trung tâm chuyển mạch di động MTC mobile te r mi na te d call Cuộc gọi đến NAS non access s tra tum Tập hợp các giao thức không liên quan trực tiếp đến phần truy nhập mạng NBAP Node B app li ca ti on part Phần ứng dụng node B Node B UMTS base s ta ti on Trạm gốc của UMTS OMC o pe ra ti on and ma in ten an ce cen tre Trung tâm khai thác và bảo dưỡng P CCPCH p ri ma ry co m mon con tro l p hy si ca l chan ne l Kênh vật lý điều khiển chung sơ cấp PCH pa gin g chan ne l Kênh tìm gọi PDP pa c ke t data pro to co l e g</p> <p>https://text.123doc.org/document/4325020-nghien-cuu-xay-dung-cac-chi-tieu-va-bai-do-danh-gia-chat-luong-mang-truy-nhap-wcdma-cua-he-thong-3g.htm</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
7	GNU/GPL GNU General Public License Giấy phép phần mềm tự do	nhỏ phải Logo GPLv 3 nhỏ phải 200px Biểu trưng Hec ke rt của GNU Giấy phép Công cộng GNU tiếng Anh GNU Ge ne ra l Pub li c Licen se viết tắt GNU GPL hay chỉ GPL là giấy phép phần mềm tự do được sử dụng rộng rãi đảm bảo cho người dùng cuối tự do chạy nghiên cứu sửa đổi và chia sẻ phần mềm	71
		https://vi.wikipedia.org/wiki/Giấy phép Công cộng GNU	
7	Hệ thống phát hiện xâm nhập host	Và các Cấu port của các dịch vụ thừa này trở thành điểm yếu cho các tấn công DoS tràn hình bộ đệm hoặc tránh sự xác thực Mức Các công nghệ mới còn non yếu có thể bị tấn công bẻ gãy hoặc mất điều ứng khiển đối với các dịch vụ dụng Một số vấn đề bảo mật cho mạng VoIP như sử dụng IP Sec chữ ký số fi re wall hệ thống phát hiện xâm nhập mạng NIDS Network In tru si on De te c ti on Sys tem hệ Học viên Đặng Tuấn Hùng 11 Luận văn thạc sĩ C hự ợ n g 1 Tổng quan về công nghệ VoIP thống phát hiện xâm nhập Host Host based In tru si on De te c ti on Sys tem được xây dựng và phần nào hạn chế được sự phá hoại từ bên ngoài 1 7 2	100
		https://text.123doc.org/document/ 4327046-nghien-cuu-cong-nghe-voip-va- ung-dung-vao-trien-khai-tong-dai-cho- doanh.htm	

Trang	Câu trùng lặp	Nguồn	Điểm
7	HTTP Hypertext Transfer Protocol	<p>Giao thức HTTP HYPERTEXT TRANSFER PROTOCOL Giao thức của tầng ứng dụng cho Web Giao thức truyền thông giữa Ser ve r và C li ent Phục vụ cho dịch vụ WWW World Wide Web Phía C li ent Phía Ser ve r Tiếp nhận các yêu cầu và đáp ứng chúng Gửi kết quả cho C li ent Gửi các yêu cầu Tiếp nhận kết quả Biểu diễn các đối tượng 8 Slide 8 of 21 Cơ sở lý thuyết 2 6 Quá trình trao đổi thông điệp C li ent b ro w se r thiết lập liên kết tới web se r ve r TCP con ne c ti on qua cổng 80 mặc định Ser ve r đồng ý kết nối accept Các thông điệp HTTP me s sa ges được trao đổi giữa b ro w se r và se r ve r Ngắt kết nối 9 Slide 9 of 21 Cơ sở lý thuyết 3 6 Ví dụ Giả sử người dùng truy cập URL www hau1 edu cs index htm trang web có text và 10 hình ảnh jpeg 1a http c li ent thiết lập liên kết TCP với http se r ve r pro cess tại địa chỉ www hau1 edu vn cổng 80 ngầm định với http se r ve r 1b http se r ve r tại máy phục vụ www hau1 edu vn chờ yêu cầu kết nối TCP tại cổng 80 chấp nhận kết nối rồi thông báo với c li ent 2 http c li ent gửi http re que st me s sa ge bao gồm cả URL tới TCP con ne c ti on so c ke t 3 http se r ve r nhận re que st me s sa ge tạo ra http re spon se me s sa ge có chứa các đối tượng được yêu cầu rồi gửi vào so c ke t 10 Slide 10 of 21 Cơ sở lý thuyết 4 6 4 http se r ve r ngắt liên kết 5 http c li ent nhận re spon se me s sa ge có chứa html file hiển thị html</p> <p>https://text.123doc.org/document/1475844-bao-cao-tot-nghiep-xay-dung-bo-cong-cu-giam-sat-hinh-anh-qua-camera.htm</p>	100

Trang	Câu trùng lặp	Nguồn	Điểm
7	ICMP Internet Control Message Protocol	<p>ARP được dùng trong tất cả những trường hợp một nút trên một mạng TCP/IP cần biết địa chỉ MAC của một nút khác trên cùng mạng vật lý b DỊCH VỤ ICMP INTERNET CONTROL MESSAGE PROTOCOL Dịch vụ ICMP là dịch vụ thông báo điều khiển mạng nó hỗ trợ cho IP vì IP không có cơ chế kiểm soát lỗi và kiểm soát luồng dữ liệu nên luôn đi kèm với ICMP nó định nghĩa một tập các thông điệp lỗi sẽ gửi về các host khi một router hay một host không thể xử lý một IP đa tạ g ram thành công sử dụng lệnh kiểm tra mạng ping c DỊCH VỤ DHCP DYNAMIC HOST CONFIGURATION PROTOCOL Dy na mi c Host Confi gu ra ti on P ro to co l DHCP giao thức cấu hình động máy chủ là một giao thức cấu hình tự động địa chỉ IP</p> <p>https://text.123doc.org/document/3184456-thiet-ke-he-thong-thuc-hanh-mang-peer-to-peer.htm</p>	100

Trang	Câu trùng lặp	Nguồn	Điểm
7	Giao thức Thông điệp Điều khiển Internet IDS Intrusion Detection System Hệ thống phát hiện xâm nhập	Kết chương 59 KẾT LUẬN 60 TÀI LIỆU THAM KHẢO 61 iv DANH MỤC TỪ VIẾT TẮT Viết tắt Tiếng Anh Tiếng Việt IDS In tru si on De te c ti on Sys tem Hệ thống phát hiện xâm nhập NIDS Network In tru si on De te c ti on Sys tem Hệ thống phát hiện xâm nhập cho mạng HIDS Host In tru si on De te c ti on Sys tem Hệ thống phát hiện xâm nhập cho máy trạm SMTP S im p le Network M an ag em ent P ro to co l Giao thức quản lý mạng đơn giản DNS D om ai n Name Sys tem Hệ thống tên miền FPT File T ran sfer P ro to co l Giao thức truyền tải file IP In te r ne t P ro to co l Giao thức mạng In te r ne t TCP IP T ran s miss ion Con tro l P ro to co l In te r ne t P ro to co l Bộ giao thức In te r ne t TCP IP ICMP In te r ne t Con tro l Mes sa ge P ro to co l Giao thức thông điệp điều khiển In te r ne t UDP User Da ta g ram P ro to co l Giao thức gói dữ liệu người dùng MIB M an ag em ent Infor ma ti on Base Thông tin quản lý cơ sở MIDAS Mul ti cs In tru si on De te c ti on and A le r tin g Sys tem Hệ thống đa phát hiện xâm nhập và c ảnh báo IDES In tru si on De te c ti on Ex pe rt Sys tem Hệ chuyên gia phát hiện xâm nhập AAFID Au to no mo us A gen ts For In tru si on De te c ti on Tác nhân tự trị phát hiện xâm nhập NIDES Next Ge ne ra ti on In tru si on De te c ti on Ex pe rt Sys tem Hệ chuyên gia phát hi ện xâm nhập thể hệ tiếp theo FDDI Fiber Dis tri bu te d Data In te rface Giao diện phân tán dữ liệu quang v HDLC High Level Data Link Con tro l Giao thức điều khiển liên kết dữ liệu SLIP Se ria l Line In te r ne t P ro to co l Giao thức In te r ne t qua đường mo de m PPP Point to Point P ro to co l Giao thức điểm điểm PF Pac ke t Fil te r Lọc gói tin RB Re se r ve d Bit Bít dự phòng DF Don t F ra g men t Bit Bít không bị phân mảnh MF More F ra g men ts Bit Bít bị phân mảnh MTU Ma xi mu m T ran s miss ion Unit Đơn vị truyền tối đa TTL Time To Live Thời gian sống vi DANH SÁCH HÌNH VẼ Hình 1 1 Mô hình chức năng IDS 9 Hình 1 2 Các HIDS trong hệ thống mạng 12 Hình 1 3 Các NIDS trong hệ thống mạng 13 Hình 1 5 Các bước xử	90

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>lý của Cisco IDS 14 Hình 2 1 Kiến trúc IDS 17 Hình 2 2 Một mô hình phát hiện lạm dụng điển hình 24 Hình 2 3 Mô hình phát hiện bất thường 27 Hình 3 1 Kiến trúc của Snort 33 Hình 3 2 Giải mã gói tin Ethernet 34 Hình 3 3 Cấu trúc luật của Snort 38 Hình 3 4 Hea de r luật của Snort 38 Hình 3 5 Mô hình hệ thống phát hiện xâm nhập Snort công ty PAMA 49 Hình 3 6 Khởi động Snort làm việc với MySQL 53 Hình 3 7 Mô hình thử nghiệm 54 Hình 3 8 Cảnh báo S can Port trên Base 55 Hình 3 9 Chi tiết các cảnh báo S can Port 56 Hình 3 10 Mail gửi về cảnh báo S can Port 56 Hình 3 11 Cảnh báo Alert từ Snort thông qua BASE 57 Hình 3 12 Cảnh báo có tấn công UDP FLOOD 57 Hình 3 13 Chi tiết cảnh báo UDP FLOOD 58 Hình 3 14 Các cảnh báo được gửi về email 58 Hình 3 15 Cảnh báo về UDP FLOOD được gửi về email 59 DANH SÁCH CÁC BẢNG Bảng 3 2 Các cờ sử dụng với từ khoá Flags 46 1 MỞ ĐẦU Hiện nay cùng với sự phát triển mạnh mẽ của mạng in te r ne t đảm bảo an toàn thông tin đang trở thành một yêu cầu quan trọng thiết yếu đối với lĩnh vực phát triển công nghệ thông tin cũng như trong mọi hoạt động kinh tế xã hội</p> <p>https://text.123doc.org/document/1393684-luan-van-thac-si-ky-thuat-nghien-cuu-cac-ky-thuat-phat-hien-dot-nhap-mang-va-xay-dung-mo-hinh-ung-dung-dua-tren-snort.htm</p>	
7	IRC Internet Relay Chat Giao thức IRC	<p>Down loa d Pal ta lkSce ne Giá cả Miễn phí IceC ha t Giao thức IRC In te r ne t Relay Chat vẫn còn tồn tại và vẫn còn có rất nhiều người sử dụng nó để chat và trao đổi các file hàng ngày</p> <p>https://text.123doc.org/document/1972454-giao-trinh-tin-hoc-16-cong-cu-tro-giup-cho-e-mail-va-im-doc.htm</p>	91

Trang	Câu trùng lặp	Nguồn	Điểm
7	LAN Local Area Network Mạng cục bộ	<p>Tài liệu tham khảo 9 Danh mục các từ viết tắt Từ viết tắt Từ gốc Nghĩa tiếng Việt</p> <p>AG Access Ga te way Cổng truy nhập AS App li ca ti on Ser ve r Máy chủ ứng dụng AS F AS Func ti on Chức năng máy chủ ứng dụng ATM Asynch ro no us T ran sfer Mode Chế độ chuyển giao không đồng bộ CA Call Agent Tác nhân cuộc gọi FS Fea tu re Ser ve r Máy chủ chức năng IN In te l li gen t Network Mạng thông minh INAP IN App li ca ti on P ro to co l Giao thức ứng dụng mạng IN IP In te r ne t P ro to co l Giao thức In te r ne t ISDN In te g ra te d Ser vi ce Di gi ta l Network Mạng số liên kết đa dịch vụ ISP In te r ne t Ser vi ce P ro vi de r Nhà cung cấp dịch vụ In te r ne t ITU ITU T In te r na ti o na l Te le co m mu ni ca ti on Union ITU Te le co m Sec to r Liên minh Viễn thông Quốc tế bộ phận tiêu chuẩn hóa viễn thông của ITU IW F In te r wor ki ng Func ti on Chức năng liên kết mạng LAN Local Area Network Mạng cục bộ M2UA MTP level 2 User A đa p tai on T ơ ng thích với ng ời dùng mức 2 MEGACO ME dia GA te way CO n tro l le r Giao thức điều khiển cổng ph ơng tiện MG Media Ga te way Cổng ph ơng tiện MGC Media Ga te way Con tro l e r Bộ điều khiển cổng ph ơng tiện MGC F MGC Func ti on Chức năng MGC MGCP Media Ga te way Con tro l P ro to co l Giao thức điều khiển cổng l u l ợng MG F MG Func ti on Chức năng cổng MG Từ viết tắt Từ gốc Nghĩa tiếng Việt MPLS Mul ti P ro to co l Label Swit chi ng C huy ển mạch nhãn đa giao thức NGN Next Ge ne ra ti on Network Mạng thế hệ sau PBX P ri va te B ran ch eX chang e Tổng đài nhánh PRI P ri ma ry Rate In te rface Giao diện tốc độ sơ cấp PSDN Pub li c Swit che d Data Network Mạng dữ liệu chuyển mạch công cộng PSTN Pub li c Swit che d Te le pho ne Network Mạng điện thoại chuyển mạch công cộng R F Rou tin g Func ti on Chức năng định tuyến RTCP Real Time T ran sport Con tro l P ro to co l Giao thức điều khiển truyền tải thời gian thực RTP Real Time T ran sport P ro to co l Giao thức truyền tải thời gian thực SPC S to re d P ro g</p>	100

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>ram me Con tro l Điều khiển theo ch ơng trình l u trữ SG Sig na l lin g Ga te way Cổng báo hiệu SIP Ses si on In tia ti on P ro to co l Giao thức khởi đầu phiên SIP T Ses si on In tia ti on P ro to co l for Te le pho ny Phần mở rộng giao thức SIP dành cho thoại SNMP S im p le Network M an ag em ent P ro to co l Giao thức quản lý mạng đơn giản SS7 Sig na lin g Sys tem No7 Hệ thống báo hiệu số 7 SUA SCCP User A đa ta ti on Thích ứng ng ời dùng SCCP TCP T ran s miss ion Con tro l P ro to co l Giao thức điều khiển truyền tải TDM Time Di vi si on Mu ti p le xin g Ghép kênh theo thời gian TGW Trunk Ga te Way Cổng trung kế UDP User Đa ta g ram P ro to co l Giao thức gói tin ng ời dùng VoIP Voice over IP Thoại qua mạng IP WAN Wide Area Network Mạng diện rộng Tổ viỐt t t WDM Tổ gèc Wa ve leng ht Di vi si on Mul ti p le xin g NghŨa tiỔng ViỐt GhĐp k^nh ph n chia theo b íc sãng Danh mục các hình vẽ Hình 1 Các thành phần chính của mạng viễn thông Er ro r</p> <p>https://text.123doc.org/document/4734199-dspace-at-vnu-nghien-cuu-ung-dung-cong-nghe-chuyen-mach-mem-softswitch-tren-mang-ngn-viet-nam.htm</p>	
7	Địa chỉ điều khiển truy nhập môi trường	<p>Hai phương tiện để truy nhập tại phần MAC điều khiển truy nhập môi trường truyền dẫn của tầng liên kết dữ liệu và một định dạng chung cho việc định địa chỉ</p> <p>https://text.123doc.org/document/4550536-tim-hieu-ve-mang-internet.htm</p>	77

Trang	Câu trùng lặp	Nguồn	Điểm
	NIC Network Interface Card Card giao tiếp mạng	<p>Người thực hiện VÕ DŨNG MỤC LỤC LỜI CẢM ƠN B LỜI CAM ĐOAN C MỤC LỤC D BẢNG TỪ VIẾT TẮT G LỜI MỞ ĐẦU I CHƯƠNG 1 1 HIỆN TRẠNG MẠNG VIỄN THÔNG VIỆT NAM VÀ XU HƯỚNG PHÁT TRIỂN MẠNG TRUY NHẬP CỦA THẾ GIỚI 1 1 1 Giới thiệu chương 1 1 2 Hiện trạng mạng truyền thông của Việt Nam 1 1 2 1 T ru yền dẫn Quốc Tế 1 1 2 2 T ru yền dẫn Quốc Gia 1 1 2 3 T ru yền dẫn nội tỉnh 2 1 3 Sự phát triển của lưu lượng 2 1 4 Xu hướng phát triển hiện nay 3 1 5 Mạng truy nhập thế hệ sau 4 1 6 So sánh giữa các giải pháp truy nhập và thị trường mạng quang thụ động toàn cầu 5 Bảng 1 1 Thị trường mạng quang thụ động toàn cầu 2003 2008 5 1 7 Kết luận chương 7 CHƯƠNG 2 8 MẠNG TRUY NHẬP QUANG THỤ ĐỘNG PON 8 2 1 Giới thiệu chương 8 2 2 Tổng quang về công nghệ PON 8 2 2 1 Bộ tách ghép quang 9 2 2 2 Các đầu cuối mạng PON 11 2 2 3 Mô hình PON 11 2 2 4 WDM và TDM PON 13 2 3 Kết luận chương 15 CHƯƠNG 3 16 CÔNG NGHỆ ETHERNET 16 3 1 Giới thiệu chương 16 3 2 Tổng quan về E the r ne t 17 3 3 Các phần tử của mạng E the r ne t 17 3 4 Kiến trúc mô hình mạng E the r ne t 18 3 5 Quan hệ vật lý giữa IEEE 802 3 và mô hình tham chiếu ISO 19 3 6 Lớp con MAC E the r ne t 21 3 6 1 Dạng khung cơ bản của E the r ne t 21 3 6 2 Sự truyền khung dữ liệu 22 3 6 2 1 T ru yền đơn công phương thức truy nhập CSMA CD 23 3 6 2 2 T ru yền song công một cách tiếp cận để hiệu quả mạng cao hơn 24 3 7 Lớp vật lý E the r ne t 24 3 8 Quan hệ giữa lớp vật lý E the r ne t và mô hình tham chiếu ISO 25 3 9 Kết luận chương 26 CHƯƠNG 4 27 MẠNG TRUY CẬP QUANG THỤ ĐỘNG ETHERNET EPON 27 4 1 Giới thiệu chương 27 4 2 Lợi ích của mạng truy cập quang thụ động E the r ne t PON 27 4 3 Mạng truy cập quang thụ động EPON 28 4 3 1 N gu yên lý hoạt động 28 4 3 2 Giao thức điều khiển đa điểm MPCP Multi Point Con tro l P ro to co l 30 4 3 3 EPON với kiến trúc 802 34 4 3 3 1 Point to Point E mu la ti</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>on 35 4 3 3 2 Share Me di um E mu la ti on 36 4 4 Kết luận chương 37 CHƯƠNG 5 39 KHẢO SÁT TRỄ VÀ CÁC PHƯƠNG PHÁP PHÂN PHỐI BĂNG THÔNG TRONG EPON 39 5 1 Giới thiệu chương 39 5 2 Mô hình của EPON 39 5 3 Thuật toán In te r le a ve d Pol lin g 41 5 4 Kế hoạch phân bổ băng thông của sổ truyền cực đại 44 5 5 Các thành phần của trễ gói 46 5 6 Cấp phát băng thông cố định 47 5 7 Cấp phát băng thông cân đối 48 5 8 Sự cấp phát băng thông theo quyền ưu tiên 49 5 9 SLA aware p DBA 50 5 10 SLA aware A đa p ti ve DBA 52 5 11 Kết luận chương 53 CHƯƠNG 6 54 GIAO DIỆN CHƯƠNG TRÌNH MÔ PHỎNG VÀ KẾT QUẢ TÍNH TOÁN 54 6 1 Giới thiệu chương 54 6 2 Giao diện chính của chương trình mô phỏng 54 6 3 Giao diện thể hiện mô phỏng quá trình truyền dữ liệu từ OLT đến các ONU hướng xuống 55 6 4 Giao diện mô phỏng quá trình truyền dữ liệu từ các ONU đến OLT hướng lên 56 6 5 Cấp phát băng thông truyền tải theo tỷ lệ lượng bytes có trong hàng đợi cho từng ONU 56 6 6 Tỷ lệ cấp phát băng thông cho các ONU 58 6 7 Thuật toán phân bổ băng thông theo tỷ lệ bytes có trong hàng đợi dựa trên tính ưu tiên của dịch vụ 58 6 8 Thuật toán tính toán trễ trong mạng truy nhập quang EPON 63 6 9 Kết luận chương 65 KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN ĐỀ TÀI II TÀI LIỆU THAM KHẢO III PHỤ LỤC V BẢNG TỪ VIẾT TẮT TỪ VIẾT TẮT TÊN TIẾNG ANH TÊN TIẾNG VIỆT A DBA A đa p ti ve Dy na mi c B an dwidth Al lo ca ti on Cấp phát băng thông thích ứng dữ liệu ATM Asynch ro no us T ran sfer Mode Chế độ truyền dị bội CSMA CD Car ri er Sense Mul ti p le Access with Col li si on De te ct Đa truy nhập cảm nhận sóng mang có phát hiện xung đột DA Des ti na ti on Add re ss Địa chỉ đích DCE Data C om mu ni ca ti on E qui p men t Thiết bị giao dịch dữ liệu DTE Data Ter mi na l E qui p men t Thiết bị dữ liệu đầu cuối DSL Di gi ta l Subsc ri be r Line Đường dây thuê bao số EMS E le men t M an ag em ent Sys tem Hệ thống quản lý EPON E the r ne t Pas si</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>ve Op ti ca l Network Mạng quang thụ động E the r ne t FCS Frame Check Sequence Kiểm tra khung tuần tự FR Frame Relay Công nghệ Frame Relay FSAN Full Ser vi ce Access Network Mạng truy cập dịch vụ đầy đủ FTTB Fiber To The B u i l d i n g Sợi quang đến tòa nhà FTTC Fiber To The Curb Sợi quang đến cụm thuê bao FTTH Fiber To The Home Sợi quang đến tận nhà thuê bao IEEE Ins ti tu te of E le c tri ca l and E le c tro ni cs En gi ne ers Hiệp hội các kỹ sư điện và điện tử thế giới ID In de n ti fy Des ti na ti on Chỉ định địa chỉ đích IP In te r ne t P ro to co l Giao thức In te r ne t ISDN In te g ra te d Ser vi ces Di gi ta l Network Mạng tích hợp dịch vụ số ITU In te r na ti o na l Te le co m mu ni ca ti on Union Liên hiệp viễn thông quốc tế LAN Local Area Network Mạng cục bộ LLC Lo gi ca l Link Con tro l Điều khiển kết nối logic MAN Me tro po li tan Area Network Mạng khu vực thủ đô MAC Media Access Con tro l Lớp điều khiển truy nhập phương tiện MDI Me di um De pe nt de nt In te rface Giao diện phụ thuộc phương tiện MII Me di um In de pe nt de nt In te rface Giao diện độc lập phương tiện MPCP Mul ti P oi nt Con tro l P ro to co l Giao thức điều khiển đa điểm MPtP Mul ti P oi nt to Point Mô hình điểm đa điểm NGN Next Ge ne ra ti on Network Mạng thế hệ sau NIC Network In te rface Card Card giao tiếp mạng OLT Op ti ca l Line Ter mi na l Kết cuối đường truyền quang ONU Op ti ca l Network Unit Đơn vị mạng quang PC Per so na l C om pu te r Máy vi tính PCS P hy si ca l Co di ng Sub lay er Lớp con mã hóa vật lý PDH P le si o cho ro no us Di gi ta l Hie ra rc hy Phân cấp số cận đồng bộ PMA P hy si ca l Me di um At ta ch men t Lớp con thuộc lớp vật lý PON Pas si ve Op ti ca l Network Mạng quang thụ động POTS Plain Old Te le pho ny Sys tem Hệ thống điện thoại kiểu cũ PRE P re am b le Mào đầu PtP Point to Point Mô hình điểm điểm PtPE Point to Point E mu la ti on PtMP Point to Multi Point Mô hình điểm đa điểm QoS Qua li ty of Ser vi ce Chất lượng dịch vụ SA Source Add</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>re ss Địa chỉ nguồn SDH Syn cho ro no us Di gi ta l Hie ra rc hy Phân cấp số đồng bộ SDM Space Di vi si on Mul ti p le xin g Ghép kênh phân chia theo không gian SFD Start of Frame De li mi te r Byte xác định sự bắt đầu khung SLA DBA Ser vi ce Level Ag re em ent Dy na mi c B an dwidth Al lo ca ti on Cấp phát băng thông động theo mức dịch vụ cam kết SBA S ta ti c B an dwidth Al lo ca ti on cấp phát băng thông cố định SP DBA S tri ct P ri o ri ty Dy na mi c B an dwidth Al lo ca ti on Cấp phát băng thông động theo chế độ ưu tiên SLA Ser vi ce Level Ag re em ent Cam kết mức độ dịch vụ SME S ha re d Me di um E mu la ti on SONET Syn cho ro no us Op ti ca l Network Mạng quang đồng bộ TDM Time Di vi si on Mul ti p le xin g Ghép kênh phân chia theo thời gian WAN Wide Area Network Mạng truy nhập diện rộng LỖI MỞ ĐẦU Mạng đường trục Bắc Nam nước ta sử dụng mạng Ring cáp quang SDH 20 Gbps</p>	
		<p>https://text.123doc.org/document/1213866-do-an-mang-truy-nhap-quang-thu-dong-ethernet-pon-potx.htm</p>	
7	Hệ thống phát hiện xâm nhập mạng	<p>nbsp N ghi ên cứu triển khai hệ thống phát hiện xâm nhập mạng với phần mềm mã nguồn mở Snort In li ne 1 LỖI CẢM ƠN Trước tiên tôi xin gửi lời cảm ơn chân thành đến thầy giáo đã hướng dẫn tôi hoàn thành đồ án này</p>	100
		<p>https://text.123doc.org/document/4573914-nghien-cuu-trien-khai-he-thong-phat-hien-xam-nhap-mang-voi-phan-mem-ma-nguon-mo-snort-inline.htm</p>	
8	Ký hiệu Tên Tiếng Anh Ý nghĩa Tiếng Việt	<p>2 M B 4 X Y amp Y SVTH Lê Thị Hồng Thanh Lớp K45E6 Khóa luận tốt nghiệp GVHD ThS N gu yễn N gu yệt Nga DANH MỤC TỪ VIẾT TẮT Ký hiệu Tên tiếng anh Ý nghĩa 9 lt EE 9</p>	73

Trang	Câu trùng lặp	Nguồn	Điểm
		https://text.123doc.org/document/2574911-giai-phap-vuot-rao-can-moi-truong-nham-day-manh-xuat-khau-hang-may-tre-dan-sang-thi-truong-nhat-ban-cua-cong-ty-tnhh-hong-tien.htm	

Trang	Câu trùng lặp	Nguồn	Điểm
8	Bộ tiêu chuẩn bảo mật dữ liệu thẻ thanh toán	Thuật ngữ và các từ viết tắt Viết tắt Ý Nghĩa AI Trí tuệ nhân tạo Ar ti ficial In te l li gen ce API Giao diện lập trình ứng dụng App li ca ti on P ro g ram min g In te rface BI Báo cáo quản trị thông minh Bu si ne ss In te l li gen ce BPMN Mô hình và ký hiệu quy trình nghiệp vụ Bu si ne ss P ro cess Model and No ta ti on CMND Chứng minh nhân dân CSDL Cơ sở dữ liệu CSF Khung an toàn thông tin không gian mạng Cy be r se cu ri ty F ra me work DC DR Trung tâm dữ liệu phòng ngừa thảm hoạ Data Cen te r Di sa s te r Re co ve ry DIP Hệ thống tích hợp dữ liệu Data In te rg ra ti on P la tform DSP Nền tảng dịch vụ dữ liệu Data Ser vi ce P la tform ESB Trục liên thông En te rp ri se Ser vi ce Bus GIS Hệ thống thông tin địa lý bản đồ số G eo g ra phi c Infor ma ti on Sys tem GPS Hệ thống định vị toàn cầu G lo ba l Po si ti o ni ng Sys tem GUI Giao diện người dùng đồ hoạ G ra phi ca l User In te rface IaaS Điện toán đám mây ở mức hạ tầng Inf ra s tru c tu re as a se r vi ce ICT Công nghệ thông tin và truyền thông Infor ma ti on and C om mu ni ca ti on Tech no lo gie s IoT Vạn vật kết nối In te r ne t of T hin gs ISO Hệ thống quản lý chất lượng In te r na ti o na l Or ga ni za ti on for S tan da r di za ti on LGSP Nền tảng tích hợp chia sẻ cấp tỉnh Local Go ve rn men t Ser vi ce P la tform MIS Kho dữ liệu thông tin quản lý tổng hợp M an ag em ent Infor ma ti on Sys tem NGSP Cổng kết nối quốc gia Na ti o na l Go ve rn men t Ser vi ce P la tform NIST Viện Tiêu chuẩn và Kỹ thuật Quốc gia Na ti o na l Ins ti tu te of S tan da rds and Tech no lo gy NOC Trung tâm điều hành hệ thống mạng Network O pe ra ti ons Cen te r PaaS Điện toán đám mây ở mức nền tảng P la tform as a se r vi ce PCCC Phòng cháy chữa cháy PCI DSS Tiêu chuẩn bảo mật dữ liệu thẻ thanh toán Pay men t Card In du stry Data Se cu ri ty S tan da rd PPP Đầu tư theo hình thức đối tác công tư Pub li c P ri va te P art ne rs hi p SMS Dịch vụ tin nhắn ngắn Short Mes sa ge Ser vi ces SOA Kiến trúc hướng dịch vụ Ser vi ce O ri en te d Ar	88

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>chi tiết về SOC Trung tâm An toàn thông tin Security Operations Center SSO Hệ thống định danh và xác thực người dùng tập trung Single Sign On II</p> <p>https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Quyết-dinh-4250-QĐ-UBND-2018-Kien-truc-Chinh-quyen-dien-tu-Ho-Chi-Minh-402815.aspx</p>	
8	POC Proof of Concept Chứng minh khái niệm	<p>Hiện FPT đã bắt đầu thiết lập quan hệ cấp cao với các đối tác quốc tế cùng tích cực tham gia phát triển sản xuất và thương mại hóa PoC proof of concept chứng minh khái niệm và dịch vụ chuyển đổi số</p> <p>https://techinsight.com.vn/thoai-von-da-nganh-fpt-tap-trung-toan-luc-vao-cong-nghe/</p>	100

Trang	Câu trùng lặp	Nguồn	Điểm
	PPP Point-to-point Protocol Giao thức mạng ngang hàng	<p>Điểm bằng chữ Ngày tháng 11 năm 2008</p> <p>Giáo viên phản biện Mục lục Đồ án tốt nghiệp Mục lục Mục lục 1 Mục lục Đồ án tốt nghiệp 1 Danh mục hình vẽ 2 Danh mục hình vẽ Đồ án tốt nghiệp 2 Thuật ngữ viết tắt 4 Thuật ngữ viết tắt Đồ án tốt nghiệp 4 Lời nói đầu 5 Lời nói đầu Đồ án tốt nghiệp 5 C h ư ơ n g 1 Lý thuyết chung về mạng ngang hàng 6 C h ư ơ n g 1 Lý thuyết chung về mạng ngang hàng Đồ án tốt nghiệp 8 C h ư ơ n g 2 Lý thuyết về Bảng băm phân tán DHT 24 C h ư ơ n g 2 Lý thuyết chung về bảng băm phân tán DHT Đồ án tốt nghiệp 24 C h ư ơ n g 3 P h ư ơ n g pháp nghiên cứu mạng ngang hàng 44 C h ư ơ n g 3 P h ư ơ n g pháp nghiên cứu mạng ngang hàng Đồ án tốt nghiệp 44 C h ư ơ n g 4 Đánh giá hiệu năng một số DHT 56 C h ư ơ n g 4 Đánh giá hiệu năng một số DHT Đồ án tốt nghiệp 56 Kết luận 75 Kết luận Đồ án tốt nghiệp 75 Tài liệu tham khảo 76 Tài liệu tham khảo Đồ án tốt nghiệp 76 N g u y ề n</p> <p>Thế Tùng Đ 04 VT 1 1 Danh mục hình vẽ Đồ án tốt nghiệp Danh mục hình vẽ Hình 1 1 Hệ thống mạng 6 Hình 1 2 Hệ thống mạng chủ khách 7 Hình 1 3 Mạng ngang hàng 8 Hình 1 4 Mạng ngang hàng hoàn toàn 11 Hình 1 5 Mạng lai ghép 12 Hình 1 6 Mạng lai ghép với chỉ số hoá tập trung 13 Hình 1 7 Mạng lai ghép với chỉ số hoá phân tán 13 Hình 1 8 Cơ chế danh mục tập trung 14 Hình 1 9 Cơ chế yêu cầu liên tục 15 Hình 1 10 Cơ chế bảng băm phân tán 15 Hình 1 11 Mạng E don ke y 20 Hình 1 12 Mạng G n u t e l a 21 Hình 1 13 Mạng Naps te r 22 Hình 1 14 Tìm kiếm trên mạng Naps te r 23 Hình 2 1 Chức năng chính của DHT 25 Hình 2 2 Không gian ID của mạng Chord N 64 27 Hình 2 3 Các item lưu trên mạng Chord 27 Hình 2 4 Quá trình node tham gia vào mạng Chord 33 Hình 2 5 Quá trình node rời khỏi mạng Chord 34 Hình 2 6 Không gian ID của mạng Ka de m lia N 16 35 Hình 2 7 Các k bu c ke t của một node 35 Hình 2 8 Bảng định tuyến của node 110 37 Hình 2 9 Quá trình node tham gia vào mạng Ke li ps 39 Hình 2 10 Bảng định tuyến của một node trong mạng Ta pe stry 40 Hình 2 11 Các mức</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>liên kết của node 4227 41 Hình 2 12</p> <p>Đường đi của một me s sa ge từ node 5230 tới node 42AD 41 Hình 2 13 Các bản sao được định tuyến tới root node 4377 42 Hình 2 14 Các node truy vấn đến node lưu item gần nhất 42 Hình 3 1 Minh họa NS 2 47 Hình 3 2 Minh họa PeerS im 48 Hình 3 3 Minh họa P la ne tS im 49 Hình 3 4 Minh họa OMNet 51 Hình 3 5 Minh họa O ve rS im 52 Hình 3 6 Minh họa GPS 53 N gu yễn Thế Tùng Đ 04 VT 1 2 Danh mục hình vẽ Đồ án tốt nghiệp Hình 3 7 Minh họa P 2 PS im 55 Hình 4 1 Minh họa mô hình thực tế 57 Hình 4 2 Hoạt động của P 2 PS im 58 Hình 4 3 Lưu đồ xác định ngưỡng churn rate 62 Hình 4 4 Ngưỡng churn rate Chord hoạt động tốt 62 Hình 4 5 Ngưỡng churn rate Ka de m lia hoạt động tốt 63 Hình 4 6 Ngưỡng churn rate Ke li ps hoạt động tốt 63 Hình 4 7 Ngưỡng churn rate Ta pe stry hoạt động tốt 64 Hình 4 8 Hiệu năng Chord với churn rate rất cao 65 Hình 4 9 Hiệu năng Ka de m lia với churn rate rất cao 65 Hình 4 10 Hiệu năng Ke li ps với churn rate rất cao 66 Hình 4 11 Hiệu năng Ta pe stry với churn rate rất cao 66 Hình 4 12 So sánh các DHT với churn rate 60s 67 Hình 4 13 So sánh các DHT với churn rate 300s 67 Hình 4 14 Ảnh hưởng của base đối với Chord 68 Hình 4 15 Ảnh hưởng của pns ti me r đối với Chord 68 Hình 4 16 Ảnh hưởng của alpha đối với Ka de m lia 69 Hình 4 17 Ảnh hưởng của s ta bi li ze timer đối với Ka de m lia 69 Hình 4 18 Ảnh hưởng của round in te r va l đối với Ke li ps 70 Hình 4 19 Ảnh hưởng của n con ta cts đối với Ke li ps 70 Hình 4 20 Ảnh hưởng của s ta b ti me r đối với Ta pe stry 71 Hình 4 21 Ảnh hưởng của base đối với Ta pe stry 71 Hình 4 22 Tính khả mở của Chord 72 Hình 4 23 Tính khả mở của Ka de m lia 72 Hình 4 24 Tính khả mở của Ke li ps 73 Hình 4 25 Tính khả mở của Ta pe stry 73 N gu yễn Thế Tùng Đ 04 VT 1 3 Thuật ngữ viết tắt Đồ án tốt nghiệp Thuật ngữ viết tắt Từ viết tắt Tiếng Anh Tiếng Việt CLI C om man d Line In te rface Giao diện dòng lệnh DHT Dis tri bu te d Hash Table</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>Bảng băm phân tán FAQ Frequent ly Asked Questions Các câu hỏi thường gặp FTP File Transfer Protocol Giao thức truyền file GUI Graphical User Interface Giao diện đồ họa ICQ I seek you C hứ ợ n g trình máy tính nhắn tin tức thời trên In te r ne t ID I de n ti fier Số nhận dạng IP In te r ne t P ro to co l Giao thức mạng In te r ne t IPv6 In te r ne t P ro to co l ve r si on 6 Giao thức IP phiên bản 6 JXTA Jux ta po se Giao thức mạng ngang hàng mã nguồn mở của Sun Micro sys tem s MAC Media Access Con tro l Điều khiển Truy nhập Vật lý MIT Mas sa chu se tts Ins ti tu te of Tech no lo gy Học viện kĩ thuật Ma sa chu se t Mĩ OSPF Open S ho r te st Path First Đường đi ngắn nhất mở đầu tiên P2P Peer to Peer Mạng ngang hàng PDA Per so na l Di gi ta l As si s tan t Máy trợ lý cá nhân kỹ thuật số PPP Point to Point P ro to co l Giao thức điểm nối điểm PVC Perfor man ce ve r su s Cost Hiệu năng đối với chi phí RIP Rou tin g Infor ma ti on P ro to co l Giao thức định tuyến thông tin RTT Round Trip Time Thời gian đi hết một vòng SHA Se cu re Hash Al go ri thm Thuật toán băm an toàn SETI Search for Ex tra te r re s tri al In te l li gen ce Dự án tìm kiếm nền văn minh ngoài trái đất TCL Tool C om man d L an gu age Bộ công cụ lập trình dòng lệnh TCP T ran s miss ion Con tro l P ro to co l Giao thức điều khiển truyền dẫn UDP User Da ta g ram P ro to co l Giao thức gói dữ liệu người dùng VoD Video on D em an d Video theo yêu cầu N gu yễn Thế Tùng Đ 04 VT 1 4 Lời nói đầu Đồ án tốt nghiệp Lời nói đầu K hoảng mười năm trở lại đây thế giới đã chứng kiến sự bùng nổ của In te r ne t bằng thông rộng cùng với nó là sự phát triển mạnh mẽ của các ứng dụng peer to peer</p> <p>https://text.123doc.org/document/1339403-do-an-danh-gia-hieu-nang-mot-so-giao-thuc-dht-trong-mang-ngang-hang.htm</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
8	RAM Random Access Memory Bộ nhớ truy xuất ngẫu nhiên	<p>IV DANH MỤC THUẬT NGỮ CHỮ VIẾT TẮT Viết tắt Tiếng Anh Tiếng Việt ACK Acknowledgement Báo nhận ADV Advertisement based MAC MAC quảng cáo AP Access Point Điểm truy nhập BSS Basic Service Set Điểm dịch vụ cơ bản BTS Base Transceiver Station Trạm thu phát sóng di động Code Division Multiple Access Đa truy nhập đa người dùng phân chia theo mã GPRS General Packet Radio System Hệ thống định vị toàn cầu Low Energy Adaptive Clustering Hierarchy Phân bậc tương thích năng lượng thấp Level Multiple Access Đa truy nhập đa người dùng phân chia theo mã MAC Media Access Control Điều khiển truy nhập môi trường Node Activation Multiple Access Nút kích hoạt nhiều truy cập Network Allocation Vector Vector thời gian chiếm giữ mạng Power aware medium access with Năng lượng báo hiệu trong truy tín mạng nhập trung bình QoS Quality of Service Chất lượng dịch vụ RAM Random Access Memory Bộ nhớ truy xuất ngẫu nhiên ROM Read Only Memory Bộ nhớ chỉ đọc S-MAC Sensor MAC dựa trên sensor TDMA Time Division Multiple Access T-MAC Time Division Multiple Access CDMA GPS LEACH LMS MAC MAC NAMA NAV PAMAS Đa truy nhập phân chia theo thời gian MAC dựa trên khoảng thời gian timeout V MỤC LỤC LỜI CAM ĐOAN</p> <p>https://text.123doc.org/document/4490556-nghien-cuu-giao-thuc-dinh-tuyen-ho-tro-hieu-qua-nang-luong-trong-mang-wsn-lv-thac-si.htm</p>	100

Trang	Câu trùng lặp	Nguồn	Điểm
	SEM security event management quản lý sự kiện bảo mật	Hướng phát triển giải pháp mở rộng hoàn thiện hệ thống GSANM 64 TÀI LIỆU THAM KHẢO 66 5 DANH MỤC TỪ VIẾT TẮT STT Thuật Ngữ Từ Viết Tắt Giải thích từ ngữ 1 AD Ac ti ve Di re c to ry Mic ro so ft 2 APT Ad van ced Per si s ten t Th re at 3 ATANTT An toàn an ninh thông tin 4 ATTT An toàn thông tin 5 BGP Giao thức định tuyến Bor de r Ga te way P ro to co l 6 BTTTT Bộ Thông tin và T ru yền thông 7 CATP Công an thành phố 8 CGI Chuẩn kết nối chương trình ứng dụng với web se r ve r C om mon Ga te way In te rface 9 CIFS C om mon In te r ne t File Sys tem 10 CNTT Công nghệ Thông tin 11 CPU Bộ xử lý trung tâm Cen tra l P ro ces sin g Unit 12 CSDL Cơ sở dữ liệu 13 DDoS Tấn công từ chối dịch vụ phân tán Dis tri bu te d De nia l of Ser vi ce 14 DHCP Giao thức cấu hình động máy chủ Dy na mi c Host 15 DNS Hệ thống tên miền D om ai n Name Sys tem 16 DoS Tấn công từ chối dịch vụ De nia l of Ser vi ce 17 ESM En te rp ri se Se cu ri ty M an ag em ent 18 FTP Giao thức truyền tập tin File T ran sfer P ro to co l 19 GSANM Giám sát an ninh mạng 20 GSM Hệ thống thông tin di động toàn cầu G lo ba l Sys tem for Mo bi le C om mu ni ca ti ons 21 GUI Giao diện người dùng đồ họa G ra phi ca l User In te rface 22 HOST Máy chủ 23 HTML Ngôn ngữ đánh dấu siêu văn bản Hy pe rText Markup L an gu age 24 HTTP Giao thức truyền siêu văn bản Hy pe r te xt T ran sfer P ro to co l 6 25 ICMP Giao thức bản tin điều khiển In te r ne t In te r ne t Con tro l Mes sa ge P ro to co l 26 ID Định danh I de n ti fier 27 IDS Hệ thống phát hiện xâm nhập In tru si on De te c ti on Sys tem 28 IM Tin nhắn nhanh Ins tan t Mes sa gin g 29 IMAP Giao thức truy cập thông điệp In te r ne t In te r ne t 30 ISO In te r na ti o na l Or ga ni za ti on for S tan da r di za ti on 31 LAN Local Area Network mạng cục bộ 32 LDAP Lightweight Di re c to ry Access P ro to co l 33 NAS Network At ta che d S to ra ge 34 NFS Network File Sys tem 35 NIST Na ti o na l Ins ti tu te of S tan da rds and Tech no lo gy Viện Tiêu	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>chuẩn và Kỹ thuật Quốc gia Hoa Kỳ 36 NIST SP NIST Special Publication 37 POP3 Post Office Protocol 3 giao thức nhận thư điện tử 38 RAID Redundant Array of Independent Disks 39 SAN S to ra ge Area Network 40 SCAP Se cu ri ty Con ten t Au to ma ti on P ro to co l Giao thức tự động bảo mật nội dung 41 SEM Se cu ri ty Event M an ag em ent Quản lý Sự kiện Bảo mật 42 SIEM Se cu ri ty Infor ma ti on and Event M an ag em ent Quản lý Thông tin và Sự kiện Bảo mật 43 SIM Se cu ri ty Infor ma ti on M an ag em ent Quản lý Thông tin Bảo mật 44 SMTP S im p le Mail T ran sfer P ro to co l giao thức chuẩn gửi thư điện tử 45 TTĐT Thông tin Điện tử 46 TTTDDL Trung Tâm Tích hợp Dữ liệu 50 VPN Vir tua l P ri va te Network mạng riêng ảo 51 WAN Wide area ne twork mạng diện rộng 7 DANH MỤC HÌNH VẼ Hình 1 1 Thành phần và chức năng của hệ thống GSANM 18 Hình 2 1 Mô hình hoạt động hệ thống GSANM tại phòng quản lý xuất nhập cảnh 25 Hình 2 2 Sơ đồ logic mạng tổng thể tại Phòng Quản lý xuất nhập cảnh CATP 31 Hình 3 1 ArcSight SIEM 4 bước để đảm bảo an toàn 47 Hình 3 2 Mẫu dữ liệu nhật ký dạng nguyên thủy 49 Hình 3 3 Mẫu dữ liệu nhật ký sau khi được ArcSight chuẩn hóa 49 Hình 3 4 ArcSight chuẩn hóa nhật ký thành 1 định dạng chung CEF 49 Hình 3 5 Các kỹ thuật ArcSight sử dụng để phân tích tương quan Cor re la ti on 50 Hình 3 6 ArcSight I de n ti ty View 51 Hình 3 7 ArcSight phân tích và phát hiện T ro j an and Bot ne t de te c ti on 1 52 Hình 3 8 ArcSight phân tích và phát hiện T ro j an and Bot ne t de te c ti on 2 52 Hình 3 9 ArcSight Use cases 53 Hình 3 10 Giao diện theo dõi ArcSight Dash boar d 54 Hình 3 11 Giám sát bùng nổ WORM trong mạng 54 Hình 3 12 Giám sát việc phát tán Mã độc trong hệ thống 55 Hình 3 13 Giao diện quản lý thông báo cảnh báo an ninh 56 Hình 3 14 Mô hình triển khai logic của giải pháp 57 Hình 3 15 Mẫu cảnh báo tình trạng mất kết nối cổng mạng tại màn hình giám sát 59 Hình 3 16 Mẫu thư điện tử cảnh báo tình</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>trạng mất kết nối cổng mạng 59 Hình 3 17 Mẫu báo cáo các cảnh báo của Fi re wall 60 Hình 3 18 Mẫu báo cáo Vmwa re E ven ts 61 Hình 3 19 Mẫu cảnh báo Brute Force Login 62 Hình 3 20 Mẫu báo cáo Trend Micro spam rules 63 8 DANH MỤC BẢNG BIỂU Bảng 2 1 Thông tin cần nắm bắt khi giám sát một TTTDHL 9 CHƯƠNG MỞ ĐẦU 1</p> <p>https://text.123doc.org/document/4745146-nghien-cuu-thiet-ke-va-trien-khai-giai-phap-giam-sat-cho-he-thong-an-ninh-thong-tin-cua-phong-quan-ly-xuat-nhap-can-h-cong-an-thanh-pho-ha-noi.htm</p>	
8	Security Information and Event	<p>ĐẠI HỌC QUỐC GIA HÀ NỘI TRƯỜNG ĐẠI HỌC CÔNG NGHỆ Bùi Ánh Quyết TÌM HIỂU VÀ TRIỂN KHAI CÔNG NGHỆ QUẢN LÝ THÔNG TIN VÀ SỰ KIỆN AN NINH KHÓA LUẬN TỐT NGHIỆP ĐẠI HỌC HỆ CHÍNH QUY Ngành Công Nghệ Thông Tin HÀ NỘI 2014 ĐẠI HỌC QUỐC GIA HÀ NỘI TRƯỜNG ĐẠI HỌC CÔNG NGHỆ Bùi Ánh Quyết TÌM HIỂU VÀ TRIỂN KHAI CÔNG NGHỆ QUẢN LÝ THÔNG TIN VÀ SỰ KIỆN AN NINH KHÓA LUẬN TỐT NGHIỆP ĐẠI HỌC HỆ CHÍNH QUY Ngành Công Nghệ Thông Tin Cán bộ hướng dẫn Thạc sĩ Đoàn Minh P h u ơ n g HÀ NỘI 2014 VIETNAM NATIONAL UNIVERSITY HANOI UNIVERSITY OF ENGINEERING AND TECHNOLOGY Bui Anh Quyet STUDY AND IMPLEMENT SECURITY INFORMATION AND EVENT MANAGEMENT Major FACULTY OF INFORMATION TECHNOLOGY Su p e r vi so r DOAN MINH PHUONG HA NOI 2014 i TÓM TẮT Tóm tắt Cùng với sự phát triển của xã hội việc ứng dụng Công nghệ thông tin vào đời sống và làm việc ngày càng được phát triển và nâng cao hiệu quả</p> <p>KHOA_LUAN-tonghop.pdf</p>	100

Trang	Câu trùng lặp	Nguồn	Điểm
	Quản lý thông tin và sự kiện bảo mật	<p>Hướng phát triển giải pháp mở rộng hoàn thiện hệ thống GSANM 64 TÀI LIỆU THAM KHẢO 66 5 DANH MỤC TỪ VIẾT TẮT STT Thuật Ngữ Từ Viết Tắt</p> <p>Giải thích từ ngữ 1 AD Ac ti ve Di re c to ry Mic ro so ft 2 APT Ad van ced Per si s ten t Th re at 3 ATANTT An toàn an ninh thông tin 4 ATTT An toàn thông tin 5 BGP Giao thức định tuyến Bor de r Ga te way P ro to co l 6 BTTTT Bộ Thông tin và T ru yền thông 7 CATP Công an thành phố 8 CGI Chuẩn kết nối chương trình ứng dụng với web se r ve r C om mon Ga te way In te rface 9 CIFS C om mon In te r ne t File Sys tem 10 CNTT Công nghệ Thông tin 11 CPU Bộ xử lý trung tâm Cen tra l P ro ces sin g Unit 12 CSDL Cơ sở dữ liệu 13 DDoS Tấn công từ chối dịch vụ phân tán Dis tri bu te d De nia l of Ser vi ce 14 DHCP Giao thức cấu hình động máy chủ Dy na mi c Host 15 DNS Hệ thống tên miền D om ai n Name Sys tem 16 DoS Tấn công từ chối dịch vụ De nia l of Ser vi ce 17 ESM En te rp ri se Se cu ri ty M an ag em ent 18 FTP Giao thức truyền tập tin File T ran sfer P ro to co l 19 GSANM Giám sát an ninh mạng 20 GSM Hệ thống thông tin di động toàn cầu G lo ba l Sys tem for Mo bi le C om mu ni ca ti ons 21 GUI Giao diện người dùng đồ họa G ra phi ca l User In te rface 22 HOST Máy chủ 23 HTML Ngôn ngữ đánh dấu siêu văn bản Hy pe rText Markup L an gu age 24 HTTP Giao thức truyền siêu văn bản Hy pe r te xt T ran sfer P ro to co l 25 ICMP Giao thức bản tin điều khiển In te r ne t In te r ne t Con tro l Mes sa ge P ro to co l 26 ID Định danh I de n ti fier 27 IDS Hệ thống phát hiện xâm nhập In tru si on De te c ti on Sys tem 28 IM Tin nhắn nhanh Ins tan t Mes sa gin g 29 IMAP Giao thức truy cập thông điệp In te r ne t In te r ne t 30 ISO In te r na ti o na l Or ga ni za ti on for S tan da r di za ti on 31 LAN Local Area Network mạng cục bộ 32 LDAP Lightweight Di re c to ry Access P ro to co l 33 NAS Network At ta che d S to ra ge 34 NFS Network File Sys tem 35 NIST Na ti o na l Ins ti tu te of S tan da rds and Tech no lo gy Viện Tiêu</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>chuẩn và Kỹ thuật Quốc gia Hoa Kỳ 36 NIST SP NIST Special Publication 37 POP3 Post Office Protocol 3 giao thức nhận thư điện tử 38 RAID Redundant Array of Independent Disks 39 SAN S to ra ge Area Network 40 SCAP Se curi ty Con tent Au to ma ti on P ro to co l Giao thức tự động bảo mật nội dung 41 SEM Se curi ty Event M an ag em ent Quản lý Sự kiện Bảo mật 42 SIEM Se cu ri ty Infor ma ti on and Event M an ag em ent Quản lý Thông tin và Sự kiện Bảo mật 43 SIM Se curi ty Infor ma ti on M an ag em ent Quản lý Thông tin Bảo mật 44 SMTP S im p le Mail T ran sfer P ro to co l giao thức chuẩn gửi thư điện tử 45 TTĐT Thông tin Điện tử 46 TTTDDL Trung Tâm Tích hợp Dữ liệu 50 VPN Vir tua l P ri va te Network mạng riêng ảo 51 WAN Wide area ne twork mạng diện rộng 7 DANH MỤC HÌNH VẼ Hình 1 1 Thành phần và chức năng của hệ thống GSANM 18 Hình 2 1 Mô hình hoạt động hệ thống GSANM tại phòng quản lý xuất nhập cảnh 25 Hình 2 2 Sơ đồ logic mạng tổng thể tại Phòng Quản lý xuất nhập cảnh CATP 31 Hình 3 1 ArcSight SIEM 4 bước để đảm bảo an toàn 47 Hình 3 2 Mẫu dữ liệu nhật ký dạng nguyên thủy 49 Hình 3 3 Mẫu dữ liệu nhật ký sau khi được ArcSight chuẩn hóa 49 Hình 3 4 ArcSight chuẩn hóa nhật ký thành 1 định dạng chung CEF 49 Hình 3 5 Các kỹ thuật ArcSight sử dụng để phân tích tương quan Cor re la ti on 50 Hình 3 6 ArcSight I de n ti ty View 51 Hình 3 7 ArcSight phân tích và phát hiện T ro j an and Bot ne t de te c ti on 1 52 Hình 3 8 ArcSight phân tích và phát hiện T ro j an and Bot ne t de te c ti on 2 52 Hình 3 9 ArcSight Use cases 53 Hình 3 10 Giao diện theo dõi ArcSight Dash boar d 54 Hình 3 11 Giám sát bùng nổ WORM trong mạng 54 Hình 3 12 Giám sát việc phát tán Mã độc trong hệ thống 55 Hình 3 13 Giao diện quản lý thông báo cảnh báo an ninh 56 Hình 3 14 Mô hình triển khai logic của giải pháp 57 Hình 3 15 Mẫu cảnh báo tình trạng mất kết nối cổng mạng tại màn hình giám sát 59 Hình 3 16 Mẫu thư điện tử cảnh báo tình</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>trạng mất kết nối cổng mạng 59 Hình 3 17 Mẫu báo cáo các cảnh báo của Fi re wall 60 Hình 3 18 Mẫu báo cáo Vmwa re E ven ts 61 Hình 3 19 Mẫu cảnh báo Brute Force Login 62 Hình 3 20 Mẫu báo cáo Trend Micro spam rules 63 8 DANH MỤC BẢNG BIỂU Bảng 2 1 Thông tin cần nắm bắt khi giám sát một TTTHDL 9 CHƯƠNG MỞ ĐẦU 1</p> <p>https://text.123doc.org/document/4745146-nghien-cuu-thiet-ke-va-trien-khai-giai-phap-giam-sat-cho-he-thong-an-ninh-thong-tin-cua-phong-quan-ly-xuat-nhap-canh-cong-an-thanh-pho-ha-noi.htm</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
	Giao thức giám sát mạng đơn giản	<p>Nghệ An tháng 12 năm 2011 Nhóm sinh viên Đường Minh Danh Ngu yễn Hữu Anh SVTH êng Minh Danh Ngu yễn H u Anh GVHD Ngu yễn C ng NhỀt 2 ả n</p> <p>Tết nghỉ Ôp Qu n lý hỒ thềng m ng MỤC LỤC LỜI NÓI ĐẦU 1 CHƯƠNG I TỔNG QUAN VỀ GIAO THỨC SNMP 5 1 1 Hai phương thức giám sát Poll và Alert 6 1 1 1 P hư ợn g thức Poll 6 1 1 2 P hư ợn g thức Alert 6 1 2 Giới thiệu giao thức SNMP 7 1 2 1 Ưu điểm trong thiết kế của SNMP 8 1 2 2 Nhược điểm của SNMP 8 1 2 3 Các phiên bản của SNMP 8 1 3 Điều hành SNMP 9 1 3 1 Các thành phần trong SNMP 9 1 3 2 Bộ phận quản lý ma na ger 9 1 3 3 Agent 10 1 3 4 Cơ sở thông tin quản lý MIB 10 1 3 5 Các lệnh cơ bản trong SNMP 11 1 4 Quản lí liên lạc giữa ma na g em ent với các agent 13 1 5 Cơ chế vận chuyển thông tin giữa ma na g em ent và agent 13 1 6 Bảo vệ truyền thông liên lạc giữa ma na g em ent và các agent khỏi sự cố 13 1 7 Các phương thức của SNMP 15 1 7 1 GetRe que st 15 1 7 2 GetNextRe que st 15 1 7 3 SetRe que st 16 1 7 4 GetRespon se 16 1 7 5 Trap 16 1 8 Các cơ chế bảo mật cho SNMP 18 1 8 1 C om mu ni ty s tri ng 18 1 8 2 View 19 1 8 3 SNMP access con tro l list 20 1 9 Cấu trúc bản tin SNMP 20 CHƯƠNG II TỔNG QUAN VỀ PHẦN MỀM GIÁM SÁT VÀ QUẢN TRỊ MẠNG SOLARWINDS 21 2 1 Giới thiệu về so la r win ds 21 2 2 Các chức năng quản trị của So la r win ds 21 2 3 Cài đặt và cấu hình So la r win ds Orion NetWork Perfor man ce Mo ni to r 22 2 3 1 Giới thiệu về Orion Network Porfor man ce Mo ni to r NPM 22 2 4 Cài đặt và cấu hình 23 2 4 1 Yêu cầu cần thiết trước khi cài đặt 23 2 4 2 Cài đặt 24 2 4 3 Cấu hình 28</p> <p>CHƯƠNG III HƯỚNG DẪN SỬ DỤNG CÁC TÍNH NĂNG CHÍNH TRONG SOLARWINDS ORION NETWORK PERFORMANCE MONITOR NPM 32 3 1 Đăng Nhập Lần Đầu Tiên 32 3 2 Giao Diện Chính Của C hư ợn g Trình 32 3 3 Giới Thiệu Giao Diện Home 33 3 3 1 S um ma ry 33 3 3 2 Group 35 SVTH êng Minh Danh Ngu yễn H u Anh GVHD N</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>gu yỔn C ng NhỄt 3 ả n Tèt nghi Ổp Qu n lý hỔ thềng m ng 3 3 3 Top 10 35 3 3 4 Event sự kiện 36 3 3 5 A le rts cảnh báo 36 3 3 6 Sys lo g 36 3 3 7 Trap bẫy lỗi 37 3 4 Giới thiệu giao diện Network 37 3 4 1 Wi re le ss 37 3 4 2 VSAN Vir tua l S to ra ge Area Network 37 3 4 3 O ve r vi ew 37 3 5 Thực hành giám sát mạng với So la r win ds NPM 43 3 5 1 Mô hình giả lập 43 3 5 2 Thực hiện tìm kiếm phát hiện thiết bị mạng sử dụng Network Sonar W in zad 43 3 5 3 Thiết lập một cảnh báo A le rts 49 SVTH êng Minh Danh N gu yỔn H u Anh GVHD N gu yỔn C ng NhỄt 4 ả n Tèt nghi Ổp Qu n lý hỔ thềng m ng</p> <p>MỤC LỤC HÌNH ẢNH Hình 1 1 Minh họa cơ chế Poll 6 Hình 1 2 Minh họa cơ chế Alert 7 Hình 1 3 Mô hình giao thức hoạt động SNMP 12 Hình 1 4 Hoạt động của giao thức SNMP 12 Hình 1 5 Hình minh họa các phương thức SNMPv 1 18 Hình 1 6 Cấu trúc bản tin SNMP 20 Hình 2 7 Giao diện bắt đầu cài đặt NPM 25 Hình 2 8 Điền Email để đăng ký trước khi bắt đầu cài đặt 25 Hình 2 9 Bắt đầu cài đặt 25 Hình 2 10 Chọn đường dẫn để lưu thư mục cài đặt 26 Hình 2 11 Lựa chọn cài đặt 26 Hình 2 12 Quá trình cài đặt các gói cấu hình 27 Hình 2 13 Cài đặt thành công 27 Hình 2 14 Giao diện đăng nhập quản lý So la r win ds 28 Hình 2 15 Đường dẫn đến tiện ích cấu hình 28 Hình 2 16 Lựa chọn các thành phần được cấu hình 29 Hình 2 17 Lựa chọn kiểu chứng thực 29 Hình 2 18 Sử dụng CSDL hiện hành 30 Hình 2 19 Lựa chọn tùy chọn kích hoạt hay không kích hoạt chứng thực 30 Hình 2 20 Lựa chọn dịch vụ muốn cài đặt 31 Hình 2 21 Quá trình cấu hình 31 Hình 3 22 Giao diện đăng nhập 32</p> <p>CHƯƠNG I TỔNG QUAN VỀ GIAO THỨC SNMP Mục đích của chương này là cung cấp cho chúng ta những khái niệm cơ bản nhất về giao thức quản lý mạng đơn giản SNMP các thành phần chức năng và phương thức hoạt động của giao thức</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		http://123doc.org/document/870206-tim-hieu-giao-thuc-snmp-va-trien-khai-he-thong-giam-sat-va-quan-tri-he-thong-mang-solarwinds-orion-network-performance-monitor.htm?page=4	

Trang	Câu trùng lặp	Nguồn	Điểm
8	SSH Secure Shell Giao thức SSH	<p>NGÔ BÁ HÙNG Email nb.hung.cit@ctu.edu.vn Quản trị Linux từ xa Quản trị từ xa Cần một tài khoản trên máy tính Server Đăng nhập từ xa Đăng nhập vào Server với tài khoản đã có bằng một phần mềm thực thi trên một máy tính trạm Thực hiện các thao tác quản trị tương tự như đăng nhập trực tiếp tại server Copy dữ liệu giữa các máy tính Thực thi chương trình trên một máy tính khác 07/08/12 Ngô Bá Hùng Khoa CNTT và TT ĐH Cần Thơ 2 Quản trị Linux từ xa Một số phần mềm quản trị từ xa Chưa không bảo mật mã hóa không mã hóa remote login Đăng nhập từ xa rcp/ftp Copy dữ liệu rexec Thực thi chương trình từ xa An toàn mã hóa dữ liệu chứng thực 07/08/12 Giao thức SSH Secure Shell OpenSSH Bộ phần mềm cài đặt SSH Ngô Bá Hùng Khoa CNTT và TT ĐH Cần Thơ 3 Quản trị Linux từ xa SSH Secure Shell Giao thức truy cập máy tính từ xa an toàn Mô hình Client-Server trên nền TCP Cổng 22 SSH 1 Tatu Ylönen Univer-sity of Helsinki 1995 Một giao thức cho truyền tải chứng thực an toàn SSH 2 RFC 4251 07/08/12 Gồm các giao thức cho truyền tải chứng thực nối kết Sử dụng mã hóa công khai cho chứng thực người dùng và máy tính Ngô Bá Hùng Khoa CNTT và TT ĐH Cần Thơ 4 Quản trị Linux từ xa http://suport.suso.com/supki/SSH/Tutorial/forLinux 07/08/12 Ngô Bá Hùng Khoa CNTT và TT ĐH Cần Thơ 5 Quản trị Linux từ xa http://suport.suso.com/supki/SSH/Tutorial/forLinux 07/08/12 Ngô Bá Hùng Khoa CNTT và TT ĐH Cần Thơ 6 Quản trị Linux từ xa Lợi điểm của SSH Tăng cường bảo mật nhờ kênh truyền được mã hóa Chứng thực người dùng client-server Cung cấp kênh giao tiếp an toàn 07/08/12 Tạo kênh giao tiếp an toàn chia sẻ cho nhiều ứng dụng giữa 2 đầu cuối nhờ đó giảm số lượng cổng mở trên mỗi đầu cuối Bổ sung cơ chế an toàn cho các giao thức không an toàn Ngô Bá Hùng Khoa CNTT và TT ĐH Cần Thơ 7 Quản trị Linux từ xa Mã hóa công khai Được sử dụng trong SSH Cập nhật khóa công khai cá nhân Khóa công khai</p>	100

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>Pub li c key Dùng để mã dữ liệu gửi Có thể truyền trên kênh truyền công cộng mà không ảnh hưởng đến tính bảo mật của dữ liệu đã mã hóa Khóa cá nhân P ri va te key 07 08 12 Dùng để giải mã dữ liệu Phải giữ bí mật Ngô Bá Hùng Khoa CNTT amp TT ĐH Cần Thơ 8 Quản trị Linux từ xa O pe nSSH http www o pe nssh org Bộ công cụ cài đặt SSH li cen se BSD Ser ve r sshd C li ent ssh r lo gin te l ne t scp rcp sftp ftp ssh add ssh agent ssh ke y si gn ssh ke ys can ssh ke y gen và sftp se r ve r Hỗ trợ nhiều hệ điều hành khác nhau 07 08 12 Linux So la ri s F re eBSD AIX HP UX</p>	
		<p>https://text.123doc.org/document/4649801-www-tinhgiac-com-ssh.htm</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
	TCP Transmission Control Protocol Giao thức TCP	<p>Hải Phòng ngày tháng Sinh viên năm 2015 MỤC LỤC DANH MỤC CÁC CHỮ VIẾT TẮT VÀ KÝ HIỆU iii DANH MỤC CÁC BẢNG v DANH MỤC CÁC HÌNH vi</p> <p>MỞ ĐẦU 1 CHƯƠNG 1 TỔNG QUAN VỀ CÔNG NGHỆ MOBILE IP 3 1 1 GIỚI THIỆU VỀ ĐỊA CHỈ IP 3 1 2 BỘ GIAO THỨC TCP IP 3 1 3 GIAO THỨC IPV6 5 1 4 TRIỂN KHAI IPV6 VÀO THỰC TẾ 8 1 4 1 Hiện trạng IPv6 trên thế giới 8 1 4 2 Thúc đẩy và phát triển IPv6 tại Việt Nam 11 1 5 CÔNG NGHỆ MOBILE IP 12 1 5 1 Giới thiệu về Mo bi le IP 12 1 5 2 Các thành phần của Mo bi le IPv6 13 1 5 3 Các đặc tính nổi bật của Mo bi le IPv6 so với Mo bi le IPv4 14</p> <p>CHƯƠNG 2 GIAO THỨC MOBILE IPV6 16 2 1 CẤU TRÚC ĐỊA CHỈ IPV6 16 2 1 1 Không gian địa chỉ 16 2 1 2 Biểu diễn địa chỉ IPv6 16 2 1 3 Phân loại địa chỉ IPv6 17 2 2 CẤU TRÚC DỮ LIỆU MOBILE IPV6 19 2 2 1 B in di ng Cache 19 2 2 2 B in di ng Up da te List 21 2 2 3 Home Agent List 21 2 3 CÁC BẢN TIN VÀ CÁC TÙY CHỌN TRONG MOBILE IPV6 22 i 2 3 1 Định dạng gói tin Mo bi le IPv6 23 2 3 2 Tùy chọn Home Add re ss cho Des ti na ti on Op ti ons Hea de r 25 2 3 3 Type 2 Rou tin g Hea de r 26 2 3 4 Các bản tin ICMPv 6 cho Mo bi le IPv6 27</p> <p>CHƯƠNG 3 PHÂN TÍCH HOẠT ĐỘNG CỦA MOBILE IPV6 31 3 1 SỰ TRAO ĐỔI BẢN TIN MOBILE IPV6 31 3 1 1 Trao đổi dữ liệu giữa một nút di động và một nút đối tác 31 3 1 2 Duy trì ràng buộc 33 3 1 3 Phát hiện đại diện thường trú 37 3 1 4 Phát hiện tiền tố di động 39 3 2 HOẠT ĐỘNG CỦA MOBILE IPV6 41 3 2 1 Khi gắn với liên kết thường trú 41 3 2 2 Di chuyển từ liên kết thường trú đến liên kết ngoài 42 3 2 3 Nút di động thay đổi địa chỉ thường trú của nó 44 3 2 4 Di chuyển từ liên kết ngoài đến một liên kết ngoài khác 45 3 2 5 Nút di động trở lại mạng thường trú 48 KẾT LUẬN 50 TÀI LIỆU THAM KHẢO 51 ii DANH MỤC CÁC CHỮ VIẾT TẮT VÀ KÝ HIỆU APNIC Asia Pacific Network Infor ma ti on Cen te r Trung tâm thông tin mạng châu Á Thái Bình Dạng ARIN A me ri can Re gi stry for In te r ne t N um be rs Cơ quan</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p> đăng ký số hiệu In te r ne t khu vực Bắc Mỹ ARP Add re ss Re so lu ti on P ro to co l Giao thức phân giải địa chỉ ATM Asynch ro no us T ran sfer Mode Chế độ truyền không đồng bộ Cor re spon de nt Node Nút đối tác CNA Cor re spon de nt Node Add re ss Địa chỉ của nút đối tác CoA Care of Add re ss Địa chỉ tạm trú Dy na mi c Host Confi gu ra ti on P ro to co l Giao thức cấu hình động máy chủ D om ai n Name Sys tem Hệ thống tên miền En ca p su la tin g Se cu ri ty Pay loa d Cung cấp khả năng bảo mật và bảo vệ tính toàn vẹn của dữ liệu Fast H an do ve rs Mo bi le IPv6 Cơ chế chuyển giao nhanh IPv6 FTP File T ran sfer P ro to co l Giao thức truyền dữ liệu tệp tin HA Home Agent Đại diện thường trú Home Agent Add re ss Địa chỉ đại diện thường trú Hie ra r chi ca l Mo bi le IPv6 Cơ chế chuyển giao phân cấp IPv6 HoA Home Add re ss Địa chỉ thường trú IANA In te r ne t As si g ne d N um be rs Au tho ri ty Tổ chức cấp phát số hiệu In te r ne t toàn cầu ICMP In te r ne t Con tro l Mes sa ge P ro to co l Giao thức thông báo điều khiển của tầng liên mạng In te r ne t En gi ne e ri ng Task Force Lực lượng chuyên trách quản lý kỹ thuật In te r ne t CN DHCP DNS ESP FMIPv 6 HAA HMIPv 6 IETF iii In te r ne t Group M an ag em ent P ro to co l Giao thức quản lý nhóm In te r ne t Key Ex chang e Cơ chế trao đổi khóa In te r ne t In te r ne t P ro to co l Giao thức In te r ne t IPsec In te r ne t P ro to co l Se cu ri ty Bảo mật trong giao thức mạng IPv4 In te r ne t P ro to co l ve r si on 4 Giao thức In te r ne t phiên bản 4 IPv6 In te r ne t P ro to co l ve r si on 6 Giao thức In te r ne t phiên bản 6 ISOC In te r ne t Socie ty Hiệp hội In te r ne t quốc tế Latin A me ri can and Ca ri b be an In te r ne t Add re s se s Re gi stry Cơ quan đăng ký địa chỉ In te r ne t khu vực Nam Mỹ Media Access Con tro l Điều khiển truy nhập truyền thông Mo bi le Node Nút di động Per so na l Di gi ta l As si s tan t Thiết bị hỗ trợ kỹ thuật số cá nhân Qua li ty of Ser vi ce Chất lượng dịch vụ Re que st For C om men ts Chuỗi các bản ghi nhớ đợc đề xuất và cho ý </p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p> kiến Rou tin g Infor ma ti on P ro to co l Giao thức định tuyến thông tin theo vector khoảng cách RIPE NCC Re se au x IP Eu ro pe ens Network Coor di na ti on Cen tre Trung tâm điều phối mạng lqới In te r ne t châu Âu và Trung Đông SMTP S im p le Mail T ran sfer P ro to co l Giao thức truyền thq đơn giản SNMP S im p le Network M an ag em ent P ro to co l Giao thức quản lý mạng đơn giản TCP T ran s miss ion Con tro l P ro to co l Giao thức điều khiển giao vận T ri vi al File T ran sfer P ro to co l Giao thức truyền tệp tin thông thường User Da ta g ram P ro to co l Giao thức gói dữ liệu nggời dùng Viet nam In te r ne t Network Infor ma ti on Cen te r Trung tâm In te r ne t Việt Nam IGMP IKE IP LACNIC MAC MN PDAs QoS RFC RIP TFTP UDP VNNIC iv DANH MỤC CÁC BẢNG Số bảng Tên bảng Trang 1 1 Sự khác biệt giữa địa chỉ IPv6 và IPv4 7 1 2 Đánh giá quá trình triển khai IPv6 của một số quốc gia hàng đầu và các quốc gia trong khu vực Đông Nam Á tính đến tháng 11 2015 9 1 3 Đánh giá tình hình triển khai IPv6 của một số quốc gia tại thời điểm tháng 3 2014 10 1 4 So sánh tỉ lệ triển khai IPv6 trong năm 2014 và 2015 của một số quốc gia 10 2 1 Phạm vi của địa chỉ IPv6 mu ti ca st 18 2 2 Bộ nhớ B in di ng Cache Mo bi le IPv6 20 v DANH MỤC CÁC HÌNH Số hình Tên hình Trang 1 1 Mô hình phân tầng TCP IP 4 1 2 Tình hình triển khai IPv6 trên thế giới 8 1 3 Các thành phần của mạng Mo bi le IPv6 13 2 1 Cấu trúc chung của địa chỉ IPv6 16 2 2 Cấu trúc địa chỉ IPv6 mu ti ca st 18 2 3 Mô tả đqờng đi của gói tin đến địa chỉ an y ca st 19 2 4 Cấu trúc tiêu đề mở rộng Mo bi li ty 23 2 5 Quá trình định tuyến phản hồi Re tu rn Rou ta bi li ty P ro ce du re 24 2 6 Cấu trúc của Des ti na ti on Op ti ons Hea de r 26 2 7 Cấu trúc của tiêu đề Type 2 Rou tin g 27 2 8 Cấu trúc bản tin Home Agent Add re ss Dis co ve ry Re que st 28 2 9 Cấu trúc bản tin Home Agent Add re ss Dis co ve ry Reply 28 2 10 Cấu trúc bản tin Mo bi le P re fix So li ci ta ti on 29 2 11 Cấu trúc bản tin Mo bi le P re fix Ad ve r ti se men t 30 </p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>3 1 3 2 Cập nhật ràng buộc gửi từ nút di động đến đại diện thường trú Bản tin duy trì ràng buộc gửi từ đại diện thường trú đến nút di động 34 35 3 3 Cập nhật ràng buộc được gửi từ nút di động đến nút đối tác 35 3 4 Duy trì ràng buộc gửi từ nút đối tác đến nút di động 36 3 5 ICMPv 6 Home Agent Add re ss Dis co ve ry Re que st được gửi từ nút di động 37 3 6 ICMPv 6 Home Agent Add re ss Dis co ve ry Reply được gửi từ đại diện thường trú 38 vi 3 7 ICMPv 6 Mo bi le P re fix So li ci ta ti on được gửi từ nút di động 39 3 8 ICMPv 6 Mo bi le P re fix Ad ve r ti s men t được gửi từ đại diện thường trú 40 3 9 Đăng ký CoA với đại diện thường trú 43 3 10 Nút di động chuyển đến liên kết ngoài mới 47 vii MỞ ĐẦU Ngày nay với sự phát triển nhanh chóng của công nghệ và truyền thông chúng ta có thể dễ dàng trao đổi thông tin xử lý công việc thông qua các thiết bị nhạ điện thoại di động máy tính bảng máy tính xách tay Mỗi một thiết bị điện tử khi hoạt động trên hệ thống mạng In te r ne t cần sử dụng một địa chỉ IP để định danh và liên lạc với nhau</p> <p>https://text.123doc.org/document/4483717-nghien-cuu-cong-nghe-mobile-ipv6-di-sau-phan-tich-hoat-dong-cua-giao-thuc.htm</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
	UDP User Datagram Protocol Giao thức UCP	<p>N gu yễn Văn Tuân Số hóa bởi Trung tâm Học liệu Đại học Thái N gu yễn http://www.lrc.tnu.edu.vn iv MỤC LỤC LỜI CAM ĐOAN i LỜI CẢM ƠN iii MỤC LỤC iv DANH MỤC CÁC KÝ HIỆU CHỮ VIẾT TẮT vi DANH MỤC CÁC BẢNG ix DANH MỤC HÌNH VẼ x MỞ ĐẦU 1 CHƯƠNG I TỔNG QUAN VỀ CHẤT LƯỢNG DỊCH VỤ CỦA LUỒNG ÂM THANH TRỰC TUYẾN 3 1 1 Chất lượng dịch vụ Qua li ty of Ser vi ce trên In te r ne t 3 1 1 1 Khái niệm về chất lượng dịch vụ QoS 3 1 1 2 Các tham số QoS 4 1 1 3 Các nguyên nhân ảnh hưởng đến chất lượng dịch vụ 5 1 1 3 1 N gu yễn nhân trễ Delay 5 1 1 3 2 N gu yễn nhân của biến thiên trễ Jit te r 6 1 1 3 3 N gu yễn nhân của mất gói pa c ke t loss 8 1 1 4 Những điều kiện QoS cho luồng âm thanh thời gian thực 9 1 1 4 1 Thông lượng Th ro ughput 9 1 1 4 2 Trễ Delay 10 1 1 4 3 Biến thiên trễ Delay Jit te r 11 1 1 4 4 Độ tin cậy Re lia bi li ty 11 1 2 Giao thức đa phq ợn g tiện trên In te r ne t 11 1 2 1 Giao thức TCP T ran s mi si on Con tro l P ro to co l 13 1 2 2 Giao thức UDP USER DATAGRAM PROTOCOL 16 1 2 3 Giao thức truyền thông thời gian thực RTP Real Time T ran sport P ro to co l 17 1 3 4 Giao thức thời gian thực RTSP Real Time S tre am P ro to co l 20 1 3 5 Giao thức điều khiển truyền thông thời gian thực RTCP Real Time T ran sport Con tro l P ro to co l 23 CHƯƠNG II CHẤT LƯỢNG DỊCH VỤ LUỒNG ÂM THANH TRÊN INTERNET 25 2 1 QoS lớp ứng dụng 25 2 1 1 T ru yễn gói 25 2 1 2 Điều chỉnh lỗi Forward Error Cor re c ti on 27 2 1 3 Sự thích ứng A da p ta ti on 28 2 1 4 Bộ đệm nhận Recei ve r bu ffe ri ng 29 2 2 QoS lớp mạng 30 Số hóa bởi Trung tâm Học liệu Đại học Thái N gu yễn http://www.lrc.tnu.edu.vn v 2 2 1 Đánh dấu quyền qu tiên tợng đối 30 2 2 2 Dịch vụ đánh dấu 31 2 2 3 Dịch vụ tích hợp IntServ 31 2 2 3 1 Khái quát về IntServ 31 2 2 3 2 Thành phần và nguyên tắc hoạt động của IntServ 33 2 2 3 3 Điều khiển dịch vụ QoS 35 2 2 3 5 Giao thức giữ trợc tài nguyên RSVP 35 2 2 3 6 RSVP và IntServ 41 2 2 3 7 Qju</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>điểm và Nhợc điểm của IntServ RSVP 42 2 2 4 Dịch vụ phân biệt 42 2 2 4 1 N gu yên tắc cơ bản của DiffServ 42 2 2 4 2 Các mức chất lượng dịch vụ cung cấp bởi DiffServ 44 2 2 4 3 Khả năng linh hoạt của DiffServ 46 2 2 4 4 Mô hình của DiffServ 46 2 2 4 5 Tác động từng chặng 47 2 2 4 6 Vùng mạng dịch vụ phân biệt 50 2 2 4 7 Phân bổ băng thông 51 2 2 4 8 Qu điểm amp Nhợc điểm của DiffServ 51 2 2 5 C huy ền mạch nhãn IP 52 CHƯƠNG III THỬ NGHIỆM ỨNG DỤNG WEBAUDIO VỚI GIAO THỨC RTSP 53 3 1 Mô hình ứng dụng Web Audio 53 3 2 Cấu hình hệ thống Web Audio 56 3 3 Đánh giá chất lượng hệ thống 60 3 4 Đánh giá kết quả thực nghiệm 68 KẾT LUẬN 69 TÀI LIỆU THAM KHẢO 70 Số hóa bởi Trung tâm Học liệu Đại học Thái N gu yên http www lrc tnu edu vn vi DANH MỤC CÁC KÝ HIỆU CHỮ VIẾT TẮT ACK ANSI ADPCM API ACK no w le dg men t A me ri can Na ti o na l S tan da rds Ins ti tu te A da p ti ve Diffe ren tia l Pulse Code Mo du la ti on App li ca ti on P ro g ram mìn g In te rface Xác nhận đáp ứng Viện tiêu chuẩn quốc gia Mỹ điều xung mã PCM vi sai thích ứng Giao diện lập trình ứng dụng ARJ Ad miss ion ReJect Từ chối yêu cầu đăng nhập ARQ Ad miss ion ReQuest Yêu cầu đăng nhập ATM Asynch ro no us T ran sfer Mode BRQ B an dwith ReQuest Yêu cầu băng tần CCS C om mon C han ne l Sig na lin g Báo hiệu kênh chung Code Exci te d L in ear Dự báo tuyến tính được thực hiện P re di c ti on bằng mã CODEC Code and DECo de c Mã hoá và giải mã CQ Cus tom Que ui ng Xếp hàng tùy biến CRC Cyc li c Re du n dan cy Check Kiểm tra độ dư thừa có chu kỳ DCF Di se nga ge ConFirm Xác nhận huỷ bỏ liên kết CELP DPCM DNS Diffe ren tia l Pulse Code Mo du la ti on D om ai n Name Ser ve r P hư ơn g thức truyền tải không đồng bộ điều xung mã vi sai Máy chủ dịch vụ tên miền Số hóa bởi Trung tâm Học liệu Đại học Thái N gu yên http www lrc tnu edu vn vii DTX ETSI Dis con ti nu ous T ran s miss ion Eu ro pe an te le co m mu ni ca ti ons</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p> S tan da rds lns ti tu te Kỹ thuật truyền gián đoạn Viện tiêu chuẩn viễn thông châu Âu Forward Error Cor re c ti on Hiệu chỉnh lỗi trước First In First Out Que ui ng Xếp hàng vào trước ra trước FIN FINaI Bít đánh dấu se g men t cuối cùng FTP File T ran sfer P ro to co l Giao thức truyền file GQOS Gua ran te ed Qua li ty of Ser vi ce Bảo đảm chất lượng dịch vụ HTTP Hyper Text T ran sfer P ro to co l Giao thức truyền tải siêu văn bản FEC FIFO Que ui ng ICMP In te r ne t Con tro l Mes sa ge P ro to co l Giao thức bản tin điều khiển In te r ne t IP In te r ne t P ro to co l Giao thức In te r ne t IRQ Infor ma ti on ReQuest Yêu cầu thông tin ISDN in te g ra te d Ser vi ce Di gi ta l Network Mạng số đa dịch vụ ISP In te r ne t Ser vi ce P ro vi de r Nhà cung cấp dịch vụ In te r ne t Kbps Ki lo bi t per se con d Kilo bít trên giây LAN Local Area Network Mạng nội hạt LPC Line P re di ct Coder Bộ mã hoá dự báo tuyến tính LRQ Lo ca ti on ReQuest Yêu cầu định vị Mbps Me ga bi t per se con d Mêga bít trên 1 giây MOS Mean O pi ni on Score Điểm đánh giá trung bình MPE Mul ti Pul se Exci te Bộ kích thích đa xung MTU Ma xi mu m T ran sfer Unit NGN Next Ge ne ra ti on Network Mạng thể hệ sau OSI Open Sys tem In te r con ne c ti on Mô hình kết nối các hệ thống mở Kích thước tối đa của một đơn vị truyền tải Số hóa bởi Trung tâm Học liệu Đại học Thái N gu yê n http www lrc thu edu vn viii OSPF Open S ho r te st Path First Mở đường ngắn nhất đầu tiên PC Per so na l C om pu te r Máy tính cá nhân PCM Pulse Code Mo du la ti on Điều chế xung mã PPP Point to Point P ro to co l Giao thức điểm tới điểm PQ P ri o ri ty Que ui ng Xếp hàng theo mức ưu tiên PSH PuSH Bít PUSH QoS Qua li ty of Ser vi ce Chất lượng dịch vụ RTCP Real Time Con tro l P ro to co l Giao thức điều khiển thời gian thực RTP Real Time P ro to co l Giao thức thời gian thực RTSP Real Time S tre am P ro to co l Giao thức luồng thời gian thực RTSP RED R an dom Early De te c ti on phát hiện sớm ngẫu nhiên SDP Ses si on Desc ri p ti on P ro to co l Giao thức miêu </p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>tả phiên SIP Ses si on I ni tia ti on P ro to co l Giao thức khởi đầu phiên SMTP S im p le Mail T ran sfer P ro to co l Giao thức truyền tải mail STM Synch ro nu os T ran fer Mode Chế độ truyền tải đồng bộ SYN SYNch ro nu os bit Bít đồng bộ TCP T ran s miss ion Con tro l P ro to co l Giao thức điều khiển truyền tải TELNET TELNET Giao thức truy nhập từ xa VoIP Voice over In te r ne t P ro to co l Thoại truyền qua giao thức In te r ne t WFQ Weigh te d Fair Que ui ng Xếp hàng theo công bằng trọng số Số hóa bởi Trung tâm Học liệu Đại học Thái N gu yên http://www.lrc.tnu.edu.vn/ix DANH MỤC CÁC BẢNG Bảng 1 1 4 1a Chất lượng Voice mã hóa và thông lượng 10 Bảng 1 1 4 1b Chất lượng CD mã hóa và thông lượng 10 Bảng 1 3 5 Mô hình phương thức RTSP hướng đi và yêu cầu 23 Bảng 2 1 1 Gói tin O ve r he ad của Mã hóa Audio khác nhau và cơ chế truyền 27 Bảng 2 2 3 5a Các kiểu và thuộc tính bảo lưu 39 Bảng 2 2 3 6a Các tham số của các đối tượng CL khác nhau 42 Bảng 2 2 3 6b Các tham số của dịch vụ được cam kết Rspec 42 Bảng 2 2 4 5a Các loại AF 49 Bảng 3 3a Chất lượng truyền gói tin D em an d 60 Bảng 3 3b Chất lượng âm thanh truyền nhận gói tin B roa d ca s tin g 60 Số hóa bởi Trung tâm Học liệu Đại học Thái N gu yên http://www.lrc.tnu.edu.vn/x DANH MỤC HÌNH VẼ Hình 1 1 3 2 Phân cụm gói tin 6 Hình 2 1 Các giao thức và dịch vụ đa phương tiện 13 Hình 1 2 1a Hoạt động của giao thức TCP trong việc cung cấp kết nối 13 Hình 1 2 1b Khuôn dạng TCP Seg men t 14 Hình 1 2 2 Khuôn dạng UDP Da ta g ram 16 Hình 1 2 3a Khuôn dạng phần cố định gói tin RTP 18 Hình 1 2 3b Khuôn dạng phần mở rộng RTP 19 Hình 2 1 4 ước tính phát lại gói tin 30 Hình 2 2 3 2a Mô hình dịch vụ IntServ 33 Hình 2 2 3 2b Kiến trúc IntServ 34 Hình 2 2 3 2c Ví dụ về hoạt động của mạng IntServ 34 Hình 2 2 3 5a Các chức năng RSVP tại Host và Rou te r 36 Hình 2 2 3 5b Hoạt động của RSVP 37 Hình 2 2 3 5c Hoạt động của thuật toán gầu thẻ IP 40 Hình 2 2 3 5d Hoạt động của gầu thẻ kết hợp với</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>chỉnh sửa tốc độ đỉnh 41 Hình 2 2 3 5e Phân loại bản tin cho luồng lưu lượng tuân thủ và các gói tin BE 41 Hình 2 2 4 1a Mô hình tổng quát của DiffServ 44 Hình 2 2 4 4a T rường dịch vụ phân biệt DS 47 Hình 2 2 4 4b Mô hình DiffServ tại biên và lõi mạng 47 Hình 2 2 4 5a C huy ển tiếp nhanh mã hóa một lựa chọn hàng đợi đơn 48 Hình 2 2 4 5b C huy ển tiếp được đảm bảo mã hóa lớp dịch vụ và mức ưu tiên loại bỏ gói 49 Hình 2 2 4 6a Mạng dịch vụ phân biệt 50 Hình 2 2 4 6b Phân loại gói tin và kiểm tra lưu lượng 50 Hình 3 1a Mô hình tổng quan mô phỏng WebAudio 54 Hình 3 1b Các giao thức hỗ trợ quá trình truyền nhận Audio 55 Số hóa bởi Trung tâm Học liệu Đại học Thái Nguyên http://www.lrc.tnu.edu.vn/data/error</p>	
		<p>https://text.123doc.org/document/4203709-dam-bao-chat-luong-cho-luong-am-thanh-truc-tuyen.htm</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
8	VPN Virtual Private Network Mạng riêng ảo	<p>DES Data Encryp ti on S tan da rd</p> <p>Chuẩn mã hoá dữ liệu ESP En ca p su la ti on Se cu ri ty Pay loa d Đóng gói tải tin an toàn GRE Ge ne ri c Rou tin g En ca p su la ti on Giao thức đóng gói định tuyến chung ID I de n ti ty Nhận dạng IKE In te r ne t Key Ex chang e Giao thức trao đổi khóa In te r ne t IP In te r ne t P ro to co l Giao thức In te r ne t IPX In te r ne t Pac ke t Ex chang e Giao thức trao đổi gói In te r ne t L2F Layer 2 Forwar di ng Giao thức chuyển tiếp lớp 2 L2TP Layer 2 Tun ne lin g P ro to co l Giao thức định đường hầm lớp 2 LAC L2TP Access Concen tra to r Bộ tập trung truy nhập giao thức L2TP LAN Local Area Network Mạng cục bộ LNS L2TP Network Ser ve r Máy chủ phục vụ L2TP NAS Network Access Ser ve r Máy chủ truy cập mạng NetBEUI NetBIOS E nhan ced User In te rface Giao thức người dùng mở rộng trong NetBIOS OSI Open Sys tem s In te r con ne c ti on Mô hình liên kết các hệ thống mở PPP Point to Point P ro to co l Giao thức điểm nối điểm PPTP Point to Point Tun ne l P ro to co l Giao thức đường hầm điểm nối điểm PSTN Pub li c Swit che d Te le pho ne Network Mạng điện thoại chuyển mạch công cộng QoS Qua li ty of Ser vi ce Chất lượng dịch vụ RADIUS R em o te Au then ti ca ti on DialIn User Ser vi ce Dịch vụ người sử dụng quay số xác thực từ xa SVTH Mai Quốc Hùng VT06A 2 Tìm hiểu kỹ thuật lưu lượng trong mạng không dây RSA Chữ cái đầu của 3 tác giả là Ri ve st S ha mi r Ad lem an Thuật toán mã hóa công khai SA Se cu ri ty As so cia ti on Liên kết an ninh SHA Se cu re Hash Al go ri thm Thuật toán phân tách bảo mật SPI Se cu ri ty Pa ra me te rs Index Chỉ số thông số an ninh TACACS Ter mi na l Access Con tro l le r Access Con tro l Sys tem Hệ thống điều khiển truy nhập của bộ điều khiển truy nhập đầu cuối TCP T ran s miss ion Con tro l P ro to co l Giao thức điều khiển truyền thông UDP User Da ta g ram P ro to co l Giao thức dữ liệu đồ người sử dụng VPN Vir tua l P ri va te Network Mạng riêng ảo WAN Wide Area Network Mạng diện rộng</p>	100

Trang	Câu trùng lặp	Nguồn	Điểm
		SVTH Mai Quốc Hùng VT06A 3 Tìm hiểu kỹ thuật lưu lượng trong mạng không dây DANH MỤC HÌNH ẢNH Hình 1 Một số chuẩn thông dụng 14 Hình 2	
		https://text.123doc.org/document/4303649-tim-hieu-ky-thuat-luu-luong-trong-mang-khong-day-wlan.htm	

Trang	Câu trùng lặp	Nguồn	Điểm
	<p>.....9 Hình 2.1:Mô tả sơ đồ của Snort</p> <p>18 Hình 2.2:Mô tả sơ đồ Suricata.</p>	<p>Chế độ bảo vệ chương trình 198 2012 ICDREC SG8V1 Hướng dẫn sử dụng 5</p> <p>Nội dung Mục lục hình Hình 1 1 Sơ đồ chân 14 Hình 1 2 Sơ đồ khối của SG8V1 16 Hình 2 1 Các bước thực hiện lệnh 17 Hình 2 2 Hoạt động thực hiện lệnh với kiến trúc không có pi pe li ne 18 Hình 2 3 Thực hiện lệnh với kiến trúc có pi pe li ne 18 Hình 2 4 Thực hiện lệnh thường với kiến trúc đường ống 18 Hình 2 5 Thực hiện lệnh by pa ss với kiến trúc đường ống 19 Hình 2 6 Thực hiện lệnh rẽ nhánh đơn chu kỳ với kiến trúc đường ống 19 Hình 2 7 Thực hiện lệnh rẽ nhánh 2 chu kỳ với kiến trúc đường ống 20 Hình 3 1 Mô tả clock trong chế độ nghỉ 21 Hình 3 2 Mô tả trường hợp CPU wake up và thực hiện tiếp tục quá trình trước đó 22 Hình 3 3 Mô tả trường hợp CPU wake up và vào chương trình ngắt 22 Hình 3 4 Stack và các thanh ghi liên quan 24 Hình 4 1 Mạch kết nối đến chân RST 27 Hình 4 2 Mạch reset ngoài 29 Hình 5 1 Bản đồ địa chỉ của bộ nhớ dữ liệu 30 Hình 5 2 Stack và các thanh ghi liên quan 32 Hình 6 1 Cấu trúc bộ nhớ dữ liệu 33 Hình 6 2 Sử dụng thanh ghi BS để chọn băng 34 Hình 9 1 Cell chuẩn của IO PAD 57 Hình 9 2 Mô tả một kết nối Port cơ bản 59 Hình9 3 IO PortA 60 Hình9 4 IO PortB 0 1 và PortB 4 dùng chung với T im er 0 61 Hình9 5 IO PortB 2 3 dùng chung với UART 61 Hình9 6 IO PortB 5 7 dùng chung với bộ lập trình FLASH 62 Hình9 7 IO PortC 0 1 dùng chung với UART1 64 Hình9 8 IO PortC 2 3 dùng chung với PWM 64 Hình9 9 IO PortC 4 5 dùng chung với SPI 64 Hình9 10 IO PortC 6 7 dùng chung với SPI 65 Hình 9 11 IO PortD 0 3 dùng chung với ngắt ngoài 67 Hình 9 12 IO PortD 4 5 dùng chung với I2C 67 Hình 9 13 IO PortD 6 dùng chung với Cap tu re C om pa re 68 Hình 9 14 IO PortD 7 dùng chung với T im er 1 68 Hình 10 1 Mô tả khối Watch do g Timer 70 Hình 11 1 Mô tả sơ đồ khối T im er 0 73 Hình 12 1 Mô tả sơ đồ khối Timer 1 77 Hình 12 2 Sơ đồ của khối bắt sự kiện 80 Hình 12 3 Sơ đồ của khối so sánh sự kiện 80 Hình 13 1 Sơ đồ khối Timer x Timer 2 hoặc Timer 3 83 Hình 14 1 Sơ</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p> đồ của khối PWM x 87 Hình 14 2 Dạng sóng PWM 89 H ình 15 1 Sơ đồ khối SPI 91 H ình 15 2 Sơ đồ kết nối của SPI 95 Hình 15 3 các chế độ truyền dữ liệu của SPI 95 Hình 15 4 dạng sóng của SPI slave CKP 0 CKE 1 98 Hình 15 5 đồng bộ tín hiệu SPI SSx 98 Hình 16 1 Kết nối các thiết bị đến bus I2C 108 2012 ICDREC SG8V1 Hướng dẫn sử dụng 6 Nội dung Hình 16 2 Khung truyền với địa chỉ 7 bit ở chế độ Master truyền 109 Hình 16 3 Khung truyền với địa chỉ 10 bit ở chế độ Master truyền 110 Hình 16 4 Khung truyền với địa chỉ 7 bit ở chế độ Master nhận 111 Hình 16 5 Khung truyền với địa chỉ 10 bit ở chế độ Master nhận 113 Hình 16 6 Đồng bộ clock 114 Hình 16 7 Phân xử 115 Hình 16 8 Định thời của quá trình tạo sự kiện Start 116 Hình 16 9 Định thời của quá trình tạo sự kiện Re pe at Start 117 Hình 16 10 Định thời của quá trình tạo sự kiện Stop 117 Hình 16 11 Xung độ bus khi tạo Start 1 118 Hình 16 12 Xung độ bus khi tạo Start 2 118 Hình 16 13 Xung độ bus khi tạo Re pe at Start 1 119 Hình 16 14 Xung độ bus khi tạo Re pe at Start 2 119 Hình 16 15 Xung độ bus khi tạo Re pe at Start 3 119 Hình 16 16 Xung độ bus khi tạo Stop 119 Hình 16 17 Xung đột bus trong quá trình truyền nhận dữ liệu 120 Hình 16 18 Địa chỉ 7 bit 122 Hình 16 19 Định địa chỉ chế độ 10 bit 124 Hình 16 20 Dạng sóng I2C Master phát 127 Hình 16 21 Dạng sóng I2C Master nhận 128 Hình 16 22 Dạng sóng I2C Slave nhận chế độ 7 bit địa chỉ 129 Hình 16 23 Dạng sóng I2C Slave phát chế độ 7 bit địa chỉ 130 Hình 16 24 Dạng sóng I2C Slave nhận chế độ 10 bit địa chỉ 131 Hình 16 25 Dạng sóng I2C Slave phát chế độ 10 bit địa chỉ 132 Hình 17 1 Các thành phần chính của ngoại vi UART 133 Hình 17 2 Xung lấy mẫu dữ liệu và xung dịch dữ liệu tính theo hệ số N 144 Hình 17 3 Xung lấy mẫu dữ liệu và xung dịch dữ liệu với N 0 144 Hình 17 4 Xung lấy mẫu dữ liệu và xung dịch dữ liệu với N 1 145 Hình 17 5 Lấy mẫu dữ liệu với N 0 145 Hình 17 6 Lấy mẫu dữ liệu với N 0 145 Hình 17 7 Dịch dữ liệu 146 Hình 17 8 Minh họa cầu </p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>trúc cơ bản của bộ truyền UART 147</p> <p>Hình 17 9 T ru yền một khung dữ liệu 148</p> <p>Hình 17 10 T ru yền liên tục 149</p> <p>Hình 17 11 Cấu trúc của UART nhận 150</p> <p>Hình 17 12 UART tiếp nhận 152</p> <p>Hình 18 1 Sơ đồ khối ngoại vi ADC 153</p> <p>Hình 18 2 Giải đồ thời gian cho hoạt động của ADC 158</p> <p>Hình 18 3 Lần chuyển đổi đầu tiên sau khi bit ADON ADON 1 7 được tích cực 158</p> <p>Hình 18 4 Mô hình ngõ vào của ADC 160</p> <p>Hình 20 1 Sơ đồ kết nối bộ nạp 197</p> <p>2012 ICDREC SG8V1</p> <p>Hướng dẫn sử dụng 7</p> <p>Nội dung Mục lục</p> <p>Bảng 1 1 Mô tả chân 15</p> <p>Bảng 4 1 Điều kiện reset cho các thanh ghi đặc biệt 28</p> <p>Bảng 6 1 Các thanh ghi chức năng đặc biệt 36</p> <p>Bảng 9 1 Mô tả chân của một IO PAD 57</p> <p>Bảng 9 2 Mô tả chiều 58</p> <p>Bảng 9 3 Mô tả bảng nhận dữ liệu 58</p> <p>Bảng 9 4 Thanh ghi DIRA 60</p> <p>Bảng 9 5 Mô tả thanh ghi PORTA 60</p> <p>Bảng 9 6 Chức năng của PortB 62</p> <p>Bảng 9 7 Thanh ghi DIRB 62</p> <p>Bảng 9 8 Mô tả thanh ghi PORTB 63</p> <p>Bảng 9 9 Chức năng của PortC 65</p> <p>Bảng 9 10 Thanh ghi DIRC 65</p> <p>Bảng 9 11 Chức năng PORTC 66</p> <p>Bảng 9 12 Chức năng của PortD 68</p> <p>Bảng 9 13 Thanh ghi DIRD 69</p> <p>Bảng 9 14 Mô tả chức năng PORTD 69</p> <p>Bảng 10 1 Mô tả thanh ghi WT 0 CON 70</p> <p>Bảng 11 1 Mô tả thanh ghi WT 0 CON 74</p> <p>Bảng 11 2 Mô tả thanh ghi T0REG 75</p> <p>Bảng 12 1 Mô tả thanh ghi T1CON 81</p> <p>Bảng 12 2 Mô tả thanh ghi T1RH 82</p> <p>Bảng 12 3 Mô tả thanh ghi T1RL 82</p> <p>Bảng 12 4 Mô tả thanh ghi CCRH 82</p> <p>Bảng 12 5 Mô tả thanh ghi CCRL 82</p> <p>Bảng 13 1 Mô tả thanh ghi TxCON 85</p> <p>Bảng 13 2 Mô tả thanh ghi TxRH 85</p> <p>Bảng 13 3 Mô tả thanh ghi TxRL 86</p> <p>Bảng 13 4 Mô tả thanh ghi TxPRH 86</p> <p>Bảng 13 5 Mô tả thanh ghi TxPRL 86</p> <p>Bảng 14 1 Mô tả thanh ghi PWMxCON 90</p> <p>Bảng 14 2 Mô tả thanh ghi PWMxRL 90</p> <p>Bảng 15 1 Thanh ghi SPI 92</p> <p>Bảng 15 2 Thanh ghi điều khiển SPI SPICON 92</p> <p>Bảng 15 3 Thanh ghi trạng thái SPI SPISTA 93</p> <p>Bảng 16 1 Mô tả thanh ghi I 2 CCON 1 ở chế độ Master 99</p> <p>Bảng 16 2 Mô tả thanh ghi I 2 CCON 1 ở chế độ Slave 100</p> <p>Bảng 18 1</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		https://text.123doc.org/document/4333249-ebook-huong-dan-su-dung-vi-dieu-khien-8-bit-sg8v1-phan-1.htm	
9 23 Hình 2.3:Minh họa sơ đồ OSSEC.	Trên hình 2 3 minh họa sơ đồ hệ điều khiển PCS 7 với Bộ điều khiển là PLC S7 400 của Si em ens	73
		https://text.123doc.org/document/4323153-thiet-ke-he-thong-dieu-khien-trung-tam-phan-phoi-khi-gdc-phu-my.htm	

Trang	Câu trùng lặp	Nguồn	Điểm
	<p>.....</p> <p>31 Hình 2.6: Minh họa sơ đồ Security Onion.</p>	<p>Tác giả Phạm Văn Danh IV DANH MỤC CÁC HÌNH VỀ Hình 1 1 Kiến trúc hệ thống GNSS 3 Hình 1 2 Sơ đồ khối bộ thu RF 4 Hình 1 3 Cấu trúc của một thiết bị MOS 5 Hình 1 4 Sự kết nối chất nền 6 Hình 1 5 a thiết bị PMOS đơn giản b PMOS bên trong n well 7 Hình 1 6 Đặc tuyến V A của MOSFET 8 Hình 2 1 Hoạt động của bộ ADC 2 10 Hình 2 2 Đáp ứng của bộ ADC lý tưởng 2 11 Hình 2 3 Sai số độ lệch dương 3 13 Hình 2 4 Sai số khuếch đại dương 3 14 Hình 2 5 Minh họa sai số kích thước bão hòa 3 14 Hình 2 6 Minh họa về độ phi tuyến vi phân 3 15 Hình 2 7 Sai từ mã ở ADC 3 bit do DNL quá lớn 3 16 Hình 2 8 INL của một bộ ADC 3 bit 3 17 Hình 2 9 Spurious Free Dynamic Range 5 19 Hình 2 10 Kiến trúc bộ ADC truyền thống 6 20 Hình 2 11 Lưu đồ thuật toán bộ kiến trúc ADC đề nghị 22 Hình 2 12 Kiến trúc bộ ADC 4 bit đề nghị 7 23 Hình 2 13 Kiến trúc SAR ADCs đơn giản 9 24 Hình 2 14 Minh họa nhược điểm của SAR ADC so với Flash ADC 26 Hình 2 15 Kiến trúc SAR có khả năng đồng bộ CLK 28 Hình 3 1 Mô hình cơ bản của bộ so sánh 29 Hình 3 2 Sơ đồ khối bộ so sánh 30 Hình 3 3 Đặc tuyến truyền đạt của bộ so sánh 31 Hình 3 4 Các tham số của Comparator lý tưởng 32 Hình 3 5 Input Common Mode Voltage 33 Hình 3 6 Tham số Gain Bandwidth Op amp 34 V Hình 3 7 Tham số slew rate 34 Hình 3 8 Tham số voltage swing 35 Hình 3 9 Cấu trúc bộ so sánh CMOS SR Latch 37 Hình 3 10 Cơ chế phóng xả của tụ ở M6 9 38 Hình 3 11 Hình minh họa tín hiệu INV1 INV2 của khối CMOS latch 39 Hình 3 12 Kiến trúc comparator đồng bộ xung CLK 39 Hình 3 13 Hình minh họa quá trình tạo xung CLK1 từ xung CLK0 40 Hình 4 1 Cấu trúc bộ comparator CMOS SR latch 42 Hình 4 2 Quy trình thiết kế cho mạch 4 bit flash ADC dạng nối tiếp 43 Hình 4 3 Cách tính thời gian trễ của mạch 44 Hình 4 4 Ảnh hưởng của V_{g1} tới trễ của mạch 45 Hình 4 5 Ảnh hưởng của kích thước số finger của M1 tới trễ của mạch 45 Hình 4 6 Xác định số finger N2 và N3 của M2 và M3 46 Hình 4 7</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>Minh họa M4 M5 trên CMOS SR latch 47 Hình 4 8 Xác định N4 N5 của M4 M5 47 Hình 4 9 Xác định kích thước của từng f in ger N6 N7 48 Hình 4 10 Xác định kích thước của N8 N9 49 Hình 4 11 Khối NOR2 a và Khối in ve r te r b 50 Hình 4 12 Mạch nguyên lý MUX 21 a và kết quả mô phỏng MUX 2 1 b 51 Hình 4 13 Sơ đồ bộ MUX 41 a và Kết quả mô phỏng MUX 4 1 b 52 Hình 4 14 Sơ đồ bộ MUX 81 a kết quả mô phỏng MUX 81 b 53 Hình 4 15 Mạch nguyên lý của 4 bit flash ADC 54 Hình 4 16 Sử dụng xung ramp tại đầu vào ADC 55 Hình 4 17 Tham số DNL và INL của 4 bit flash ADC dạng nối tiếp 56 Hình 4 18 Kết quả dạng sóng sau khi qua bộ DAC lý tưởng 57 Hình 4 19 Kết quả đạt được sau khi biến đổi Fou ri er 58 Hình 4 20 Hình minh họa thứ tự trên dưới các layer 61 Hình 4 21 Sơ đồ stich di ag ram của khối NAND3 62 Hình 4 22 Mạch nguyên lý cổng login AND ba đầu vào 62 VI Hình 4 23 Hình minh họa sơ đồ share gate khi thiết kế AND3 63 Hình 4 24 Sơ đồ thiết kế AND3 mới mỗi tra n si s to r gồm hai f in ger 63 Hình 4 25 Minh họa các linh kiện CMOS cơ bản 64 Hình 4 26 Thiết kế la you t của khối co m pa ra to r 65 Hình 4 27 Sơ đồ la you t khối mux21 65 Hình 4 28 Sơ đồ la you t khối ADC 66 VII DANH SÁCH BẢNG BIỂU Bảng 2 1 Bảng tổng kết so sánh ưu và nhược điểm giữa các kiến trúc ADC 25 Bảng 3 1 Bảng so sánh tham số của co m pa ra to r lý tưởng và thực tế 32 Bảng 3 2 Bảng trạng thái của SR latch 38 Bảng 4 1 Bảng yêu cầu thiết kế cho cấu trúc 4 bit flash ADC dạng nối tiếp 41 Bảng 4 2 Bảng trạng thái cho bộ MUX 2 1 51 Bảng 4 3 Bảng trạng thái cho bộ MUX 4 1 52 Bảng 4 4 Bảng trạng thái cho bộ MUX 81 53 Bảng 4 5 Bảng các giá trị DNL và INL 55 Bảng 4 6 Bảng kết quả đạt được của mạch 4 bit flash ADC dạng nối tiếp 58 Bảng 4 7 Bảng so sánh các kết quả với các bài báo công bố IEEE 59 Bảng 4 8 so sánh hai cấu trúc 4 bit flash ADC dạng nối tiếp Se ri es Flash ADC và 4 bit flash ADC truyền thống Co ven ti o na l Flash ADC 69 VIII DANH SÁCH CÁC TỪ VIẾT TẮT ADC</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>GNSS GPS RF LNA CMOS MOSFET NMOS A na lo g to Di gi ta I Con ve r te r G lo ba I Na vi ga ti on Sa te I li te Sys tem G lo ba I Po si ti o ni ng Sys tem Radio F re quen cy Low Noise Amp li fier C om p le men ta ry Metal Oxide S em i con du c to r Metal oxide se mi con du c to r Bộ chuyển đổi tương tự số Hệ thống vệ tinh dẫn đường toàn cầu Hệ thống định vị toàn cầu Tần số vô tuyến K hu ếch đại tạp âm thấp Công nghệ sử dụng trong thiết kế IC field effect T ran si s to r cảm ứng</p>	
		<p>https://text.123doc.org/document/4002952-nghien-cuu-va-thiet-ke-ic-chuyen-mach-adc.htm</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
	<p>.....46</p> <p>Hình 3.6:Kiểm tra thành phần NIDS.</p>	<p>1 1 2 Phân loại 2 1 3 hội Ưu nhược điểm và tầm quan trọng của gạch không nung đối với vấn đề kinh tế xã 3 1 4 Tình hình sản xuất và sử dụng gạch không nung ở Việt Nam 12 4 1 5 Tình hình sản xuất gạch không nung trên thế giới 12 6 1 6 Mục tiêu của đề tài 7 C h ư ơ n g II CƠ SỞ LÝ THUYẾT 10 2 1 Cơ sở hóa lý 10 2 1 1 Bản chất của chất kết dính xi măng Port lan d XMP 1 10 2 1 1 1 Quá trình đông rắn của XMP 1 10 2 1 2 Bản chất của cốt liệu 13 2 1 3 P h ư ơ n g pháp tạo hình 14 2 1 4 Quy trình bảo dưỡng gạch sau khi tạo hình 2 15 2 2 Cơ sở các phương pháp nghiên cứu 16 2 2 1 Xác định thành phần hóa bằng huỳnh quang tia X XRF 16 2 2 2 Độ hút vôi 16 2 2 3 Xác định thành phần hạt 16 2 2 4 Xác định thành phần hóa bằng phương pháp phổ hồng ngoại IR 17 2 2 5 Xác định thành phần khoáng bằng phương pháp nhiễu xạ tia X XRD 4 17 2 2 6 Phân tích nhiệt vi sai DTA 4 18 2 2 7 Quan sát bề mặt kính hiển vi điện tử quét SEM 4 18 2 2 8 Xác định tính chất cơ lý của sản phẩm 3 18 C h ư ơ n g III NGUYÊN LIỆU 19 3 1 Cốt liệu 19 3 1 1 Bùn đỏ 19 3 1 2 Đá mi 26 iv 3 2 Chất kết dính 26 3 3 Phụ gia 26 C h ư ơ n g IV THỰC NGHIỆM VÀ KẾT QUẢ 31 4 1 Quy trình tiến hành thí nghiệm 31 4 1 1 Sơ đồ chung 31 4 1 2 T h ư y ết minh sơ đồ chung 32 4 2 Thí nghiệm 32 4 2 1 Khảo sát lượng chất kết dính xi măng Hạ Long PCB 40 cần sử dụng 32 4 2 2 Khảo sát độ ẩm tạo hình 34 4 2 3 Khảo sát áp lực ép 35 4 2 3 Xác định pH của bùn đỏ và xỉ than 36 4 2 4 Tính thành phần phối liệu 38 4 2 5 Đo độ bền sản phẩm 39 4 2 5 1 Độ bền uốn 3 39 4 2 5 2 Độ bền nén 3 48 4 2 6 Kiểm tra thành phần khoáng của mẫu có cường độ nén cao 50 4 2 7 Kiểm tra pH của sản sau cùng 51 4 2 7 1 Kiểm tra độ giảm pH của bùn đỏ khi cho xỉ than vào 51 4 2 7 2 So sánh pH của phối liệu ban đầu và pH của sản phẩm 52 C h ư ơ n g V KẾT LUẬN VÀ KIẾN NGHỊ 55 5 1 Kết luận 55 5 2 Kiến nghị 55 TÀI LIỆU THAM KHẢO 57 Phụ lục A Kết quả đo độ hút vôi của xỉ than 58 Phụ lục B Kết quả đo độ bền uốn của các mẫu gạch 59 Phụ</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>lục C Phổ nhiễu xạ tia X 62 v DANH SÁCH HÌNH VẼ Hình 1 1 Một số loại gạch không nung trên thị trường hiện nay 1 Hình 1 2 Một số chủng loại gạch không nung hiện nay 8 Hình 2 1 Cơ chế po ly me r hóa của đất 8 14 Hình 3 1 Các dạng tồn tại của B au xi t trong tự nhiên 20 Hình 3 2 Quy trình luyện nhôm bằng công nghệ Bayer 20 Hình 3 3 Phổ hồng ngoại của bùn đỏ 21 Hình 3 4 Phổ nhiễu xạ tia X của bùn đỏ 22 Hình 3 5 Biểu đồ biểu thị pH của bùn đỏ ứng với từng lượng nước cụ thể 24 Hình 3 6 Kết quả phân tích cỡ hạt của bùn đỏ bằng phương pháp Lazer 25 Hình 3 7 Phổ nhiễu xạ tia X XRD của mẫu xỉ than 28 Hình 4 1 Sơ đồ chung của quá trình tiến hành thí nghiệm 31 Hình 4 2 Biểu đồ biểu thị cường độ uốn của mẫu ứng với từng hàm lượng xi măng 33 Hình 4 3 Biểu đồ biểu thị độ bền uốn của mẫu ứng với từng độ ẩm tạo hình 34 Hình 4 4 Biểu đồ biểu thị độ bền uốn của mẫu ứng với từng áp lực tạo hình mẫu 35 Hình 4 5 Biểu đồ biểu thị pH của bùn đỏ ứng với từng lượng nước cụ thể 36 Hình 4 6 Biểu đồ biểu thị pH của xỉ than ứng với từng lượng nước cụ thể 37 Hình 4 7 Biểu đồ biểu thị độ bền uốn của các mẫu không chứa đá mi ở 8 ngày tuổi 41 Hình 4 8 Biểu đồ biểu thị độ bền uốn của các mẫu có chứa đá mi ở 8 ngày tuổi 42 Hình 4 9 Biểu đồ biểu thị độ bền uốn của mẫu chỉ chứa xi măng và bùn đỏ ở 28 ngày tuổi 43 Hình 4 10 Biểu đồ biểu thị độ bền uốn của các mẫu không chứa đá mi ở 8 ngày tuổi 45 Hình 4 11 Biểu đồ biểu thị độ bền uốn của các mẫu có chứa 1 đá mi ở 28 ngày tuổi 46 Hình 4 12 Biểu đồ biểu thị độ bền uốn của các mẫu có chứa 2 đá mi ở 28 ngày tuổi 47 Hình 4 13 Biểu đồ biểu thị cường độ nén của các tổ mẫu 20 5 1 28 và 20 5 2 28 49 Hình 4 14 Phổ nhiễu xạ tia X của tổ mẫu 20 5 1 28 50 Hình 4 15 Biểu đồ biểu thị pH của 40g bùn đỏ khi tăng lượng xỉ than cho vào 52 v DANH SÁCH BẢNG BIỂU Bảng 3 1 Các khoáng tồn tại trong quặng B au xi t 19 Bảng 3 2 Thành phần hóa của bùn đỏ 21 Bảng 3 3 pH của bùn đỏ ứng với 100ml nước 23 Bảng 3 4 pH của bùn đỏ</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p> ứng với 200ml nước 23 Bảng 3 5 pH của bùn đỏ ứng với 300ml nước 23 Bảng 3 6 Các thông số kỹ thuật của xi măng Hạ Long PCB 40 26 Bảng 3 7 Thành phần hóa của xỉ 27 Bảng 3 8 Độ hút vôi của xỉ than 29 Bảng 4 1 Cường độ uốn ở 28 ngày tuổi của các mẫu ứng với từng lượng xi măng trong thành phần phối liệu 33 Bảng 4 2 Độ bền uốn của mẫu ứng với từng độ ẩm tạo hình khác nhau 34 Bảng 4 3 Độ bền uốn của mẫu ứng với từng áp lực ép tạo hình 35 Bảng 4 4 pH của bùn đỏ ứng với 100ml nước 36 Bảng 4 5 pH của bùn đỏ ứng với 200ml nước 36 Bảng 4 6 pH của bùn đỏ ứng với 300ml nước 36 Bảng 4 7 pH của xỉ than ứng với 100ml H₂O 37 Bảng 4 8 pH của xỉ than ứng với 200ml H₂O 37 Bảng 4 9 pH của xỉ than ứng với 300ml H₂O 37 Bảng 4 10 Thành phần phối liệu 38 Bảng 4 11 Độ bền uốn trung bình của các mẫu không chứa đá mi ở 8 ngày tuổi 40 Bảng 4 12 Độ bền uốn trung bình của các mẫu có chứa đá mi ở 8 ngày tuổi 41 Bảng 4 13 Độ bền uốn trung bình của các mẫu chỉ chứa xi măng và bùn đỏ ở 28 ngày tuổi 43 Bảng 4 14 Độ bền uốn trung bình của các mẫu không chứa đá mi ở 28 ngày tuổi 44 Bảng 4 15 Độ bền uốn trung bình của các mẫu có chứa 1 đá mi ở 28 ngày tuổi 45 Bảng 4 16 Độ bền uốn trung bình của các mẫu có chứa 2 đá mi ở 28 ngày tuổi 47 Bảng 4 17 Độ bền nén của tổ mẫu 20 5 1 28 49 vii Bảng 4 18 Độ bền nén của tổ mẫu 20 5 2 28 49 Bảng 4 19 pH của 40g bùn đỏ khi tăng lượng xỉ than cho vào 51 Bảng 4 20 pH của phối liệu ban đầu và của sản phẩm có thành phần phối liệu 20 xỉ than 5 xi măng 1 đá mi 42 ngày tuổi 53 Bảng 4 21 pH của phối liệu ban đầu và của sản phẩm có thành phần phối liệu 20 xỉ than 5 xi măng 2 đá mi 42 ngày tuổi 53 viii C hư ơ n g I TỔNG QUAN 1 1 Gạch không nung là gì </p> <p> https://text.123doc.org/document/3924389-nghien-cuu-gach-khong-nung-tu-bun-do-thuyet-minh.htm </p>	

Trang	Câu trùng lặp	Nguồn	Điểm
12	Các cuộc tấn công có thể đến từ nhiều hướng theo các cách khác nhau, do đó cần phải đưa ra các chính sách và biện pháp đề phòng cần thiết.	<p>Các cuộc tấn công có thể đến từ nhiều hướng theo các cách khác nhau do đó cần phải đưa ra các chính sách và biện pháp đề phòng cần thiết</p> <p>http://123doc.org/document/1080878-tai-lieu-luan-van-xay-dung-he-thong-phat-hien-xam-nhap-bang-phan-mem-snort-pot.htm?pageh=1</p>	100
12	Mục đích cuối cùng của an toàn bảo mật hệ thống thông tin và tài nguyên theo các yêu cầu sau: - Đảm bảo tính bí mật (Confidentiality): Thông tin không thể bị truy nhập trái phép bởi những người không có thẩm quyền.	<p>Mục đích cuối cùng của an toàn bảo mật hệ thống thông tin và tài nguyên theo các yêu cầu sau Đảm bảo tính tin cậy Confi de n tia li ty Thông tin không thể bị truy nhập trái phép bởi những người không có thẩm quyền Đảm bảo tính nguyên vẹn In te g ri ty Thông tin không thể bị sửa đổi bị làm giả bởi những người không có thẩm quyền Đảm bảo tính sẵn sàng A vai la bi li ty Thông tin luôn sẵn sàng để đáp ứng sử dụng cho người có thẩm quyền Đảm bảo tính không thể từ chối Non re pu di a ti on Thông tin được cam kết về mặt pháp luật của người cung cấp</p> <p>https://text.123doc.org/document/2311662-xay-dung-he-thong-phat-hien-xam-nhap-bat-thuong-voi-phan-mem-snort.htm</p>	92
12	- Đảm bảo tính nguyên vẹn (Intergrity): Thông tin không thể bị sửa đổi, bị làm giả bởi những người không có thẩm quyền.	<p>Nói chung đảm bảo an toàn thông tin trong mọi lĩnh vực là phải đảm bảo được các yêu cầu sau Đảm bảo tính bí mật Confi de n tia li ty Thông tin không thể bị truy nhập trái phép bởi những người không có thẩm quyền Đảm bảo tính nguyên vẹn In te g ri ty Thông tin không thể bị sửa đổi bị làm giả bởi những người không có thẩm quyền Đảm bảo tính sẵn sàng A vai la bi li ty Thông tin luôn sẵn sàng để đáp ứng nhu cầu sử dụng cho người có thẩm quyền Đảm bảo tính không thể từ chối Non re pu di a ti on Thông tin được cam kết về mặt pháp luật của người cung cấp</p> <p>https://text.123doc.org/document/2976100-mat-ma-va-an-toan-thong-tin-tren-mang-may-tinh.htm</p>	88

Trang	Câu trùng lặp	Nguồn	Điểm
12	- Đảm bảo tính sẵn sàng (Availability): Thông tin luôn sẵn sàng để đáp ứng sử dụng cho người có thẩm quyền.	Đảm bảo tính sẵn sàng A vai la bi li ty Thông tin luôn sẵn sàng để đáp ứng sử dụng cho người có thẩm quyền 5 1 2	100
		https://text.123doc.org/document/103518-nghien-cuu-van-de-xac-thuc-trong-he-thong-thanh-toan-dien-tu.htm	
12	- Đảm bảo tính không thể từ chối (Non-repudiation): Thông tin được cam kết về mặt pháp luật của người cung cấp.	Nói chung đảm bảo an toàn thông tin trong mọi lĩnh vực là phải đảm bảo được các yêu cầu sau Đảm bảo tính bí mật Confi de n tia li ty Thông tin không thể bị truy nhập trái phép bởi những người không có thẩm quyền Đảm bảo tính nguyên vẹn In te g ri ty Thông tin không thể bị sửa đổi bị làm giả bởi những người không có thẩm quyền Đảm bảo tính sẵn sàng A vai la bi li ty Thông tin luôn sẵn sàng để đáp ứng nhu cầu sử dụng cho người có thẩm quyền Đảm bảo tính không thể từ chối Non re pu di a ti on Thông tin được cam kết về mặt pháp luật của người cung cấp	100
		https://text.123doc.org/document/2976100-mat-ma-va-an-toan-thong-tin-tren-mang-may-tinh.htm	
12	Chương II: Các hệ thống phát hiện xâm nhập.	Các hệ thống có nhiệm vụ nhq vậy đợc gọi là hệ thống phát hiện xâm nhập 1 3 1	73
		https://text.123doc.org/document/4729605-dspace-at-vnu-danh-gia-hieu-qua-mot-so-thuat-toan-trong-phat-hien-xam-nhap-mang.htm	
13	TỔNG QUAN VỀ XÂM NHẬP VÀ PHÁT HIỆN	C hư ợ n g này trình bày tổng quan về xâm nhập và phát hiện xâm phạm 1 1	100
		https://text.123doc.org/document/4490861-danh-gia-hieu-nang-mot-so-thuat-toan-phan-lop-cho-phat-hien-xam-nhap-tt.htm	
14	3 cho tội phạm mạng hoạt động.	Trào lưu mạng xã hội và phạm vi rộng mở của nó đang trở thành mảnh đất màu mỡ cho tội phạm mạng hoạt động	82
		https://quantrimang.com/panda-labs-du-doan-nguy-co-bao-mat-nam-2011-73974	

Trang	Câu trùng lặp	Nguồn	Điểm
14	1.1.1. Khái quát về tấn công, xâm nhập	TỔNG QUAN VỀ TẤN CÔNG CHÈN MÃ SQL VÀ CÁC BIỆN PHÁP PHÒNG CHỐNG 1 1 1 1 1 Khái quát về tấn công chèn mã SQL Giới thiệu tấn công chèn mã SQL 1 1 1 1 SQL Injection là gì Trong những năm gần đây các ứng dụng web có xu hướng trở thành phổ biến	76
		https://text.123doc.org/document/4020970-nghien-cuu-ve-phat-hien-tan-cong-chen-ma-sql-dua-tren-phan-tich-cu-phap-cau-lenh.htm	
14	Tấn công mạng là hành vi sử dụng không gian mạng, công nghệ thông tin hoặc phương tiện điện tử để phá hoại, gây gián đoạn hoạt động của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử.	Tấn công mạng là hành vi sử dụng không gian mạng công nghệ thông tin hoặc phương tiện điện tử để phá hoại gây gián đoạn hoạt động của mạng viễn thông mạng Internet mạng máy tính hệ thống thông tin hệ thống xử lý và điều khiển thông tin cơ sở dữ liệu phương tiện điện tử 9	100
		https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Law-24-2018-QH14-Cybersecurity-388829.aspx	
15	1.1.2. Các dạng tấn công, xâm nhập mạng	LỢI ÍCH CỦA IDS 10 1 7 CÁC DẠNG TẤN CÔNG XÂM NHẬP MẠNG 11 1 7 1	71
		https://text.123doc.org/document/4327155-phat-hien-xam-nhap-cac-dang-tan-cong-ma-doc-su-dung-ky-thuat-khai-pha-du-lieu.htm	

Trang	Câu trùng lặp	Nguồn	Điểm
	1.1.2.1. Tấn công từ chối dịch vụ - DOS	<p> nghiên cứu vấn đề tấn công DDoS trong IoT Đề án tốt nghiệp Đại học MỤC LỤC LỜI CẢM ƠN i MỤC LỤC ii THUẬT NGỮ VIẾT TẮT iv DANH MỤC HÌNH VẼ vii MỞ ĐẦU 1 CHƯƠNG I TỔNG QUAN INTERNET OF THINGS 2 1.1 KHÁI NIỆM INTERNET OF THINGS 2.1.1.1 Lịch sử hình thành 2.1.1.2 Định nghĩa Internet of Things 3.1.2 KIẾN TRÚC INTERNET OF THINGS 5.1.3 CÁC ĐẶC TÍNH CƠ BẢN CỦA INTERNET OF THINGS 6.1.4 YÊU CẦU Ở MỨC CAO ĐỐI VỚI MỘT HỆ THỐNG IOT 7.1.5 ỨNG DỤNG CỦA INTERNET OF THINGS 8.1.6 XU HƯỚNG PHÁT TRIỂN CỦA IOT 26.1.7 KẾT LUẬN CHƯƠNG 28 CHƯƠNG 2 TRÌNH BÀY CÁC KỸ THUẬT TẤN CÔNG DDOS 30.2 1 TẤN CÔNG TỪ CHỐI DỊCH VỤ DOS 30.2.1.1 Giới thiệu về DoS 30.2.1.2 Lịch sử các cuộc tấn công và phát triển của DoS 30.2.1.3 Động cơ của tấn công DoS 31.2.1.4 Mục đích của tấn công DoS và hiểm họa 32.2.1.5 Các hình thức tấn công DoS cơ bản 33.2.2 TẤN CÔNG TỪ CHỐI DỊCH VỤ PHÂN TÁN DDOS 35.2 2.1 Giới thiệu DDoS 35.2.2.2 Đặc tính của tấn công DDoS 36.2.2.3 Kiến trúc tấn công DDoS 37 Hoàng Mạnh Tuấn D 13 VT 7 ii Đề án tốt nghiệp Đại học 2.3 TẤN CÔNG DDOS PHẢN CHIẾU DRDOS 39.2.4 BOTNET 40.2.4.1 Giới thiệu về bot và botnet 40.2.4.2 Vai trò của bot và botnet trong tấn công DDoS 42.2.5 KẾT LUẬN CHƯƠNG 43 CHƯƠNG 3 NGUY CƠ TẤN CÔNG DDOS TRONG IOT 44.3.1 ĐẶC TÍNH CỦA IOT LIÊN QUAN ĐẾN NGUY CƠ TẤN CÔNG DDOS 44.3.1.1 Đặc tính bảo mật kém của thiết bị IoT 46.3.1.2 Đặc tính không đồng nhất của IoT 48.3.2 CÁC GIẢI PHÁP PHÒNG NGỪA 50.3.2 1 Tăng cường bảo mật thiết bị IoT 50.3.2 2 Bảo mật định tuyến lớp mạng IoT 51.3 2.3 Bảo mật tầng ứng dụng 52.3.3 BẢO VỆ HIỆT IOT TRƯỚC DDOS VỚI MECSHIELD FRAMEWORK 54.3.3.1 Giới thiệu MECs framework 54.3 3.2 Mạng HIOT hỗ trợ MEC 55.3.3.3 Các vấn đề an ninh liên quan 57.3.3.4 MECs framework 59.3.3.5 Đánh giá </p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>hiệu suất 63 3 4 KẾT LUẬN CHƯƠNG 68 KẾT LUẬN 69 TÀI LIỆU THAM KHẢO 70 Hoàng Mạnh Tuấn D 13 VT 7 iii Đồ án tốt nghiệp Đại học THUẬT NGỮ VIẾT TẮT AAL Am bi ent As si s te d Li vin g Ci phe rB lo ck C ha in in g Môi trường hỗ trợ cuộc sống AES Ad van ced Encryp ti on S tan da rd Tiêu chuẩn mã hóa tiên tiến AOSP And roi d Open Source P ro ject Dự án mã nguồn mở And roi d API App li ca ti on P ro gm ra min g In te rface Giao diện chq ợn g trình ứng dụng CNTT Công nghệ thông tin CPU Cen tra l P ro ces sin g Unit Khối xử lý trung tâm DDoS Dis tri bu te d De nia l of Ser vi ce Từ chối dịch vụ phân tán DoS De nia l of Ser vi ce Từ chối dịch vụ DNS D om ai n Name Sys tem Hệ thống tên miền DRDoS Dis tri bu te d Ref le c ti on De nia l of Ser vi ce Từ chối dịch vụ phản chiếu phân tán ECCDH El li p ti ca l Cur ve d Cryp to g rap hy Diffie Hell man Mật mã đqờng cong El li p ti c theo cơ chế Diffie Hell man H IoT He te ro gen eo us IoT IoT không đồng bộ IACAC I de n ti ty Au then ti ca ti on and Con tro l Access Ca pa ci ty IEEE Ins ti tu te of E le c tri ca l and E le c tro ni cs En gi ne ers Hoàng Mạnh Tuấn D 13 VT 7 Viện kỹ nghệ Điện và Điện tử iv Đồ án tốt nghiệp Đại học IIC In du s tri al In te r ne t Con so r ti um Hiệp hội In te r ne t Công nghiệp IoT In te r ne t of E ne rgys Mạng lưới năng lượng kết nối In te r ne t IoT In te r ne t of T hin gs Mạng lưới vạn vật kết nối In te r ne t IPv6 In te r ne t P ro to co l ve r si on 6 Giao thức liên mạng thế hệ 6 IRC In te r ne t Relay Chat Giáo thức chat chuyển tiếp In te r ne t OIC Open In te r ne t Con so r ti um Hiệp hội In te r ne t mở M2M Ma chi ne to Ma chi ne Máy đến máy MAC Mes sa ge Au then ti ca ti on Code Mã xác thực bản tin MEC Mo bi le Edge C om pu tin g Tính toán cạnh di động PC Per so na l C om pu te r Máy tính cá nhân RPL Rou tin g for Low power and Lossy Networks Định tuyến cho mạng năng lượng thấp và mất mát RSA Thuật toán mã hóa công khai RSA SDNFV Softwa re Def in ed Network Func ti on Vir tua li za ti on Ảo hóa chức năng mạng</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>đọc định nghĩa bởi phần mềm SOM Self Organizing Map Bản đồ tự tổ chức SHA Secure Hash Algorithm Giải thuật bảo mật SSL Secure Soc kets Layer Giao thức bảo mật mạng SSL VLAN Virtual Local Access Network Mạng truy nhập cục bộ ảo Hoàng Mạnh Tuấn D 13 VT 7 v Đề án tốt nghệ nghiệp Đại học WSN Wireless sen so r network Hoàng Mạnh Tuấn D 13 VT 7 Mạng cảm biến không dây vi Đề án tốt nghệ nghiệp Đại học DANH MỤC HÌNH VẼ Hình 1 1 Hình minh họa tiêu chí của In t ernet of Things 4 Hình 1 2 Thông kê của IoT Analysis các dự án IoT được chia sẻ toàn cầu 100 Hình 2 1 Kiến trúc tấn công DDoS trực tiếp 37 Hình 2 2 Kiến trúc tấn công DDoS gián tiếp hay phản chiếu 38 Hình 2 3 Mô hình t ấn công DDoS phản chiếu DNS 40 Hình 3 1 Xác thực và mã hóa dữ liệu 51 Hình 3 2 Cấu trúc trợ giúp bảo mật trong RPL 52 Hình 3 3 Truy vấn thông lớp ứng dụng IoT với bảo mật CoAP 53 Hình 3 4 Các kịch bản tấn công DDoS trong mạng H IoT hỗ trợ MEC 55 Hình 3 5 MECs hi eld framework cho H IoT 60 Hình 3 6 Thời gian phản ứng đến các mức tấn công khác nhau 66 Hình 3 7 Tỷ lệ phát hiện và Độ chính xác trong phân loại lợu lượng bất thường với bản đồ SOM 66 Hình 3 8 Tiêu tổn CPU trong bộ điều khiển dợi các cuộc tấn công DDoS 67 Hoàng Mạnh Tuấn D 13 VT 7 vi Đề án tốt nghệ nghiệp Đại học MỞ ĐẦU Cuộc cách mạng công nghiệp lần thứ tậ đã và đang đến</p> <p>https://text.123doc.org/document/4818472-nghien-cuu-van-de-tan-cong-ddos-trong-iot.htm</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
15	Mặc dù phương tiện để tiến hành, động cơ, mục tiêu của tấn công từ chối dịch vụ có thể khác nhau, nhưng nói chung nó gồm có sự phối hợp, sự cố ý của một người hay nhiều người để một trang, hay hệ thống mạng không thể sử dụng, làm gián đoạn, hoặc làm cho hệ thống đó chậm đi một cách đáng kể với người dùng bình thường, bằng cách làm quá tải tài nguyên của hệ thống.	Mặc dù phương tiện để tiến hành động cơ mục tiêu của tấn công từ chối dịch vụ có thể khác nhau nhưng nói chung nó gồm có sự phối hợp sự cố gắng ác ý của một người hay nhiều người để một trang hay hệ thống mạng không thể sử dụng làm gián đoạn hoặc làm cho hệ thống đó chậm đi một cách đáng kể với người dùng bình thường bằng cách làm quá tải tài nguyên của hệ thống	98
		https://text.123doc.org/document/4571460-bai-bao-cai-on-tap-tin-hoc-dai-cuong-chuong-9-10-11.htm	
15	Thủ đoạn phổ biến nhất là từ máy của hacker gửi đồng loạt một lượng lớn request hay yêu cầu truy cập tới máy chủ, làm5 cho máy chủ của bị quá tải, không thể hiển thị kết quả hoặc tốn rất nhiều thời gian để gửi lại response.	Thủ đoạn phổ biến nhất là từ máy của hacker gửi đồng loạt một lượng lớn re que st hay yêu cầu truy cập tới máy chủ làm cho máy chủ của Web si te bị quá tải không thể hiển thị kết quả hoặc tốn rất nhiều thời gian để gửi lại re spon se như hiện tượng của	100
		https://viblo.asia/p/dos-vs-ddos-tan-cong-va-phong-thu-PwRkgmQAGEd	
16	1.1.2.2. Từ chối dịch vụ phân tán – DDOS	Thủ phạm có thể gây ra nhiều ảnh hưởng bởi tấn công từ chối dịch vụ phân tán DDoS 1 1 2 2 Mô hình và các bước tấn công 1 1 2 2 1 Các bước tấn công Gồm 3 giai đoạn tấn công bằng DDoS Giai đoạn chuẩn bị Chuẩn bị công cụ quan trọng của cuộc tấn công công cụ này thông thường hoạt động theo mô hình c li ent se r ve r	84
		https://text.123doc.org/document/3816852-giai-phap-phong-chong-tan-cong-ddos-tren-snort.htm	
16	Điểm khác biệt lớn nhất giữa DOS và DDOS là thay vì gửi request trực tiếp từ máy mình, hacker sẽ sử dụng các máy đã bị hack từ trước để đồng loạt gửi lượng lớn request và yêu cầu truy cập tới máy chủ.	là thay vì gửi re que st trực tiếp từ máy mình hacker sẽ sử dụng các máy đã bị hack từ trước để đồng loạt gửi lượng lớn re que st và yêu cầu truy cập tới máy chủ	79
		https://viblo.asia/p/dos-vs-ddos-tan-cong-va-phong-thu-PwRkgmQAGEd	

Trang	Câu trùng lặp	Nguồn	Điểm
16	Hình 1.1: Minh họa tấn công Dos/DDos.	<p>Kết luận chương 3 37 KẾT LUẬN 38 DANH MỤC TÀI LIỆU THAM KHẢO 39 v DANH MỤC CÁC THUẬT NGỮ CÁC CHỮ VIẾT TẮT CPU Cen tra I P ro ces sin g Unit Bộ xử lý trung tâm DDoS Dis tri bu te d De nia I of Ser vi ce Tấn công từ chối dịch vụ phân tán DNS D om ai n Name Sys tem Hệ thống phân giải tên miền DoS De nia I of Ser vi ce Tấn công từ chối dịch vụ HTTP Hy pe r te xt T ran sfer P ro to co I Giao thức truyền tải siêu văn bản Hy pe r te xt T ran sfer P ro to co I Giao thức truyền tải siêu văn bản an Se cu re to àn In te r ne t Con tro I Mes sa ge Giao thức thông báo điều khiển mạng P ro to co I in te r ne t IDS In tru si on De te c ti on Sys tem Hệ thống phát hiện xâm nhập IP In te r ne t P ro to co I Giao thức kết nối In te r ne t IPS In tru si on P re ven ti on Sys tem Hệ thống phòng chống xâm nhập P2P Peer to peer Mạng ngang hàng SIP Ses si on I ni tia ti on P ro to co I Giao thức khởi tạo phiên SMTP S im p le Mail T ran sfer P ro to co I SYN Synch ro ni za ti on Đồng bộ hóa TCP T ran sport Con tro I P ro to co I Giao thứ điều khiển truyền vận UDP User Da ta g ram P ro to co I Giao thức gói dữ liệu người dùng HTTPS ICMP Giao thức truyền tải thực diện tử đơn giản vi DANH MỤC CÁC HÌNH VẼ ĐỒ THỊ Hình 1 1 Minh họa kỹ thuật tấn công Buffer O ve r flo w 5 Hình 1 2 Minh họa tấn công kiểu Smurf 6 Hình 1 3 Minh họa tấn công SYN f lo ods 8 Hình 1 4 Kiến trúc tấn công DDoS trực tiếp 10 Hình 1 5 Kiến trúc tấn công DDoS gián tiếp hay phản chiếu 11 Hình 2 1 Mô hình phát hiện tấn công DDoS dựa trên en tro py của IP nguồn 27 Hình 3 1 En tro py của các gói tin hợp pháp theo cửa sổ thời gian 31 Hình 3 2 En tro py của lưu lượng hỗn hợp với cửa sổ 2 giây 32 Hình 3 3 En tro py của lưu lượng hỗn hợp với cửa sổ 5 giây 33 Hình 3 4 En tro py của lưu lượng mạng bình thường với cửa sổ 100 gói tin 34 Hình 3 5 En tro py của lưu lượng mạng hỗn hợp với cửa sổ 1000 gói tin 35 Hình 3 6 En tro py của lưu lượng mạng hỗn hợp với cửa sổ 10000 gói tin 35 Hình 3 7 Mô hình hệ thống phát hiện tấn công DDoS online</p>	73

Trang	Câu trùng lặp	Nguồn	Điểm
		dựa trên entropy 37 1 LỜI MỞ ĐẦU 1	
		https://text.123doc.org/document/4020966-nghien-cuu-phat-hien-tan-cong-ddos-dua-tren-ip-entropy.htm	
18	Khi một máy tính ở bên ngoài hệ thống mạng giả mạo là một máy tính đáng tin cậy trong hệ thống, hành động này của kẻ tấn công được gọi là giả mạo IP (IP Spoofing)	Khi một máy tính ở bên ngoài hệ thống mạng của bạn giả vờ là một máy tính đáng tin cậy trong hệ thống hành động này của kẻ tấn công được gọi là IP Spoofing	78
		https://quantrimang.com/ip-spoofing-la-gi-va-tan-cong-tu-choi-dich-vu-dos-la-gi-124029	
18	Để truy cập vào hệ thống mạng, máy tính bên ngoài phải “giành” được một địa chỉ IP tin cậy trên hệ thống mạng.	Để truy cập vào hệ thống mạng của bạn máy tính bên ngoài phải giành được một địa chỉ IP tin cậy trên hệ thống mạng	93
		https://quantrimang.com/s?q=thietbiso+mo+hop+lg+isai+phien+ban+chong+nuoc+cua+g2+108480&p=54	
19	Trong mạng máy tính, giả mạo giao thức ARP (ARP cache poisoning, hay ARP poisoning), là một kỹ thuật qua đó kẻ tấn công giả thông điệp ARP trong mạng cục bộ. Mục tiêu là kết hợp địa chỉ MAC của kẻ tấn công với địa chỉ IP của máy chủ làm cho bất kỳ lưu lượng truy cập nào dành cho địa chỉ IP đó được gửi đến kẻ tấn công. Giả mạo giao thức ARP có thể cho phép kẻ tấn công chặn các khung dữ liệu trên mạng, sửa đổi lưu lượng, hoặc dừng tất cả lưu lượng.	Trong mạng máy tính ARP spoofing hay ARP cache poisoning là một kỹ thuật qua đó kẻ tấn công giả thông điệp ARP trong mạng cục bộ. Nói chung mục tiêu là kết hợp địa chỉ MAC của kẻ tấn công với địa chỉ IP của máy chủ khác chẳng hạn như cổng mặc định default gateway làm cho bất kỳ lưu lượng truy cập nào dành cho địa chỉ IP đó được gửi đến kẻ tấn công. ARP spoofing có thể cho phép kẻ tấn công chặn các khung dữ liệu trên mạng sửa đổi lưu lượng hoặc dừng tất cả lưu lượng	100
		https://vi.wikipedia.org/wiki/ARP_spoofing	
20	- Chiếm phiên thông qua kịch bản - Cross-site scripting (XSS) là một kỹ thuật tấn công bằng cách chèn vào những website động (ASP, PHP, CGI, ...) những thẻ HTML hay những đoạn mã script nguy hiểm có thể gây hại cho những người sử dụng.	Khái niệm Hình 2.1 Minh họa XSS Cross Site Scripting hay còn được viết tắt là XSS là một kỹ thuật tấn công bằng cách chèn vào những website động ASP PHP CGI những thẻ HTML hay những đoạn mã script nguy hiểm có thể gây hại cho những người sử dụng khác	83
		https://text.123doc.org/document/3574922-tim-hieu-ve-tan-cong-xss-va-cach-phong-thu.htm	

Trang	Câu trùng lặp	Nguồn	Điểm
20	XSS là loại tấn công phổ biến nhất và đang thực sự đe dọa tới rất nhiều người dùng web hiện nay.	XSS là loại tấn công phổ biến nhất và đang thực sự đe dọa tới rất nhiều người dùng web hiện nay do đó mình viết bài này để giúp mọi người có cái nhìn về loại hình tấn công này	100
		https://viblo.asia:443/p/tan-cong-xss-va-cach-phong-chong-L4x5x09O5BM	
21	Tràn bộ nhớ đệm xảy ra trên nhiều hệ điều hành, đặc biệt là trên UNIX và Windows, và trên nhiều ứng dụng khác nhau như web, mail, ftp, dns, telnet, ssh, database, ...	Tràn bộ đệm xảy ra trên nhiều hệ điều hành đặc biệt là trên UNIX và Windows và trên nhiều ứng dụng khác nhau như web mail ftp dns telnet ssh database Tháng 8 2001 sâu máy tính Code Red đã khiến thế giới thiệt hại hàng tỉ USD cũng bắt nguồn từ một lỗ hổng tràn bộ đệm trong phần mềm máy chủ Microsoft Internet Information Services	92
		https://text.123doc.org/document/2603752-nghien-cuu-va-xay-dung-phuong-phap-chong-tan-cong-tran-stack.htm	
21	1.1.3. Các dạng tấn công, xâm nhập host	Có thể chia các dạng tấn công xâm nhập thành 4 loại chính như sau Giả mạo Fabrications Giả mạo thông tin thường để đánh lừa người dùng thông thường Chặn bắt Interceptations Liên quan đến việc nghe trộm trên đường truyền và chuyển hướng thông tin để sử dụng trái phép Gây ngất quaggle Interruptions Gây ngất kênh truyền thông ngăn cản việc truyền dữ liệu Spoofs Modifications Liên quan đến việc sửa đổi thông tin trên đường truyền hoặc sửa đổi dữ liệu file	71
		https://text.123doc.org/document/4583906-phat-hien-xam-nhap-mang-dua-tren-phan-tich-sau-goi-tin.htm	
23	1.2. Tổng quan về phát hiện xâm nhập	Một số mối đe dọa là cố ý nhưng một số khác có thể chỉ là ngẫu nhiên hoặc vô tình 7 Đồ án tốt nghiệp Đại học mạng Công nghệ 1 Tổng quan về phát hiện xâm nhập	80
		https://text.123doc.org/document/4583906-phat-hien-xam-nhap-mang-dua-tren-phan-tich-sau-goi-tin.htm	

Trang	Câu trùng lặp	Nguồn	Điểm
	1.2.1. Khái quát về phát hiện xâm nhập	<p>Hà Nội ngày 28 tháng 5 năm 2017 Tác giả luận văn Đặng Ngọc Danh iii MỤC LỤC LỜI CẢM ƠN i LỜI CAM ĐOAN ii DANH MỤC CÁC KÝ HIỆU VÀ CHỮ VIẾT TẮT v DANH MỤC CÁC HÌNH VẼ SƠ ĐỒ vi LỜI MỞ ĐẦU 1 CHƯƠNG 1 TỔNG QUAN VỀ SÂU MẠNG VÀ PHÒNG CHỐNG 2 1 1 Khái quát về các phần mềm độc hại 2 1 1 1 Định nghĩa 2 1 1 2 Phân loại 2 1 1 3 Tác hại của các phần mềm độc hại 13 1 2 Khái quát về sâu mạng và cơ chế lây nhiễm 15 1 2 1 Khái niệm 15 1 2 2 Lịch sử 15 1 2 3 Phân loại 16 1 2 4 Cách thức làm việc của sâu 17 1 2 5 Một số loại sâu điển hình 18 1 3 Phòng chống sâu mạng và các phần mềm độc hại khác 21 1 3 1 P h u r o n g p h á p p h o n g c h o n g v i r u s 21 1 3 2 P h u r o n g p h á p p h o n g c h o n g W o r m 21 1 4 Kết chương 22 CHƯƠNG 2 CÁC KỸ THUẬT QUÉT CỦA SÂU MẠNG VÀ CÁC PHƯƠNG PHÁP PHÁT HIỆN 23 2 1 Các kỹ thuật quét của sâu mạng 23 2 1 1 Quét ngẫu nhiên có chọn lọc 23 2 1 2 Quét định tuyến 25 2 1 3 Quét kiểu chia để trị 27 2 1 4 Quét kiểu kết hợp 29 2 1 5 Quét toàn bộ 29 iv 2 1 6 So sánh các phương pháp quét của sâu mạng 30 2 2 Các phương pháp phát hiện sâu mạng 31 2 2 1 Khái quát về các phương pháp phát hiện sâu mạng 31 2 2 2 Các phương pháp phát hiện sâu mạng 33 2 2 3 So sánh các phương pháp phát hiện sâu mạng 38 2 3 Kết chương 38 CHƯƠNG 3 THỬ NGHIỆM PHÁT HIỆN SÂU MẠNG 39 3 1 Giới thiệu mô hình phát hiện sâu mạng dựa trên tương quan nguồn đích 39 3 2 Cài đặt thử nghiệm 41 3 2 1 Tập dữ liệu và tiền xử lý dữ liệu 41 3 2 2 Kết quả phát hiện 42 3 3 Kết chương 43 KẾT LUẬN 44 DANH MỤC CÁC TÀI LIỆU THAM KHẢO 45 v DANH MỤC CÁC KÝ HIỆU VÀ CHỮ VIẾT TẮT Chữ viết tắt AAWP ACK API BGP BIOS A n a l y t i c a l A c t i v e W o r m P r o p a g a t i o n A c k n o w l e d g e m e n t A p p l i c a t i o n P r o g r a m m i n g I n t e r f a c e B o r d e r G a t e w a y P r o t o c o l B a s i c I n p u t O u t p u t S y s t e m C E R T C o m p u t e r E m e r g e n c y R e s p o n s e T e a m C P U D D O S D N S D O S H D D I A N A I D S I R C C e n t r a l P r o</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>ces sin g Unit Dis tri bu te d De nia I of Ser vi ce D om ai n Name Sys tem De nia I of Ser vi ce NIST P2P RAM SYN</p> <p>Nghĩa tiếng anh Hard Disk Drive In te r ne t As si g ne dN um be rsAu tho ri ty In tru si on De te c ti on Sys tem In te r ne t Relay Chat Na ti o na l Ins ti tu te of S tan da rds and Tech no lo gy Peer to Peer R an dom Access M em ory The Synch ro no us Idle C ha ra c te rld le ra c te r</p> <p>Nghĩa tiếng việt Phân tích sâu hoạt động lan truyền Trả lời trong quá trình bắt tay 3 bước Giao tiếp lập trình ứng dụng Giao thức định tuyến lưu lượng Hệ thống Đầu vào Đầu ra Cơ bản Trung tâm ứng cứu khẩn cấp máy tính Đơn vị xử lý trung tâm Tấn công từ chối dịch vụ phân tán Hệ thống phân giải tên Tấn công từ chối dịch vụ Ổ đĩa cứng truyền thống Tổ chức cấp phát số hiệu In te r ne t Hệ thống phát hiện xâm nhập Chat chuyển tiếp In te r ne t Viện tiêu chuẩn và công nghệ quốc gia Hoa Kỳ Mạng ngang hàng Bộ nhớ truy cập ngẫu nhiên Ký tự đồng bộ hóa vi DANH MỤC CÁC HÌNH VẼ SỐ ĐỒ SỐ HIỆU Bảng 1 1 Hình 1 1 Hình 2 1 Hình 2 2 Bảng 2 2 Hình 2 3 Hình 2 4 Hình 2 5 Hình 2 6 Hình 2 7 TÊN HÌNH VẼ Phân loại phần mềm độc hại của NIST Phân loại phần mềm độc hại của Peter Szor So sánh mô hình AAWP và Wea ve r So sánh tốc độ lan truyền của quét ngẫu nhiên và quét ngẫu nhiên có lựa chọn So sánh các phương pháp phát hiện sâu mạng So sánh tốc độ lan truyền của kỹ thuật quét ngẫu nhiên và quét định tuyến So sánh tốc độ lan truyền của kỹ thuật quét ngẫu nhiên và quét chia để trị So sánh tốc độ lan truyền của kỹ thuật quét ngẫu nhiên và hoàn toàn TRANG 3 7 27 28 41 30 32 33 35 Hình 3 2 So sánh các phương pháp quét của sâu mạng Sơ đồ mô tả hệ thống phát hiện worm Sự biến đổi của số nạn nhân trong trường hợp quét ngẫu nhiên và quét định tuyến Mô hình quét tìm đích lây nhiễm của sâu mạng Lưu đồ cài đặt thuật toán phát hiện sâu mạng dựa trên tương quan nguồn đích Hình 3 3 Một bản ghi logs thu thập được từ tường lửa 41 Hình 3 4 Trích một số bản ghi trích xuất từ logs tường lửa</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		41 Hình 3 5 Kết quả phát hiện các cặp tương quan nguồn đích 42 Hình 2 8 Hình 3 1 36 38 39 40 1 LỜI MỞ ĐẦU Sâu mạng Network worms là một trong các loại phần mềm độc hại Malware có tốc độ lây lan rất nhanh và khả năng tàn phá lớn	
		https://text.123doc.org/document/4490641-nghien-cuu-cac-ky-thuat-quet-cua-sau-mang-va-cac-phuong-phap-phat-hien-lv-thac-si.htm	
23	Phát hiện xâm nhập còn là khả năng nhận dạng xâm nhập do các cá nhân gây ra, bao gồm: những người sử dụng hệ thống bất hợp pháp (“tội phạm máy tính” - hacker) và những người sử dụng hợp pháp nhưng lại lạm dụng các đặc quyền của mình “đẻ	Phát hiện xâm nhập là khả năng nhận dạng xâm nhập do các cá nhân gây ra bao gồm những người sử dụng hệ thống bất hợp pháp tội phạm máy tính hacker và những người sử dụng hợp pháp nhưng lại lạm dụng các đặc quyền của mình để doạ bên trong	95
		https://text.123doc.org/document/3759558-bai-giang-mon-an-toan-co-so-du-lieu-phat-hien-xam-nhap-co-so-du-lieu-trai-phep-nguyen-phuong-tam.htm	

Trang	Câu trùng lặp	Nguồn	Điểm
	1.2.2.1. Phát hiện xâm nhập mạng (NIDS - Network -based IDS)	<p>Sổ hóa Trung tâm Học liệu ĐHTN http://www.lrc.tnu.edu.vn i MỤC LỤC MỞ ĐẦU</p> <p>4 Chương 1 KHÁI QUÁT BÀI TOÁN PHÁT HIỆN XÂM NHẬP 1 1 Định nghĩa phát xâm nhập 1 1 1 Định nghĩa 1 1 2 Sự khác IDS IPS 1 2 Các thành phần chức hệ thống phát thâm nhập 5 1 2 1 Thành phần thu thập gói tin 6 1 2 2 Thành phần phát gói tin 6 1 2 3 Thành phần phản hồi 1 3 Phân loại phát xâm nhập 1 3 1 Network based IDS NIDS 7 1 3 2 Host based IDS HIDS 9 11 1 4 1 Mô hình phát lạm dụng 11 1 4 2 Mô hình phát bất thường 12 1 4 3 So sánh hai mô hình 15</p> <p>Chương 2 PHÁT HIỆN XÂM NHẬP DỰA TRÊN THUẬT TOÁN K MEANS 17</p> <p>2 1 Thuật toán K means 17 2 1 1 Các khái niệm 17 2 1 2 Thuật toán 20 2 1 3 Nhược điểm K Means cách khắc phục 35 2 2 Thuật toán K means với phát xâm nhập 35 2 2 1 Phân tích tập liệu kiểm thử 35 2 2 2 Mô hình phát bất thường dựa thuật toán K means 39</p> <p>Chương 3 XÂY DỰNG CHƯƠNG TRÌNH PHÁT HIỆN XÂM NHẬP DỰA TRÊN THUẬT TOÁN K MEANS 47 3 1 Mô tả toán 47 3 2 Mô tả liệu đầu vào 47 3 2 1 Mô tả thuộc tính file liệu đầu vào 48 3 2 2 Giảm số lượng ghi liệu đầu vào 50 3 3 Cài đặt thuật toán K Means thử nghiệm phân cụm phần tử dị biệt 53 3 3 1 Giới thiệu môi trường cài đặt 53 3 3 2 Các chức chương trình 53 3 4 Nhận xét đánh giá chương trình thử nghiệm 59</p> <p>KẾT LUẬN VÀ HƯỚNG NGHIÊN CỨU 60</p> <p>TÀI LIỆU THAM KHẢO 61</p> <p>PHẦN PHỤ LỤC 62</p> <p>Sổ hóa Trung tâm Học liệu ĐHTN http://www.lrc.tnu.edu.vn ii DANH MỤC HÌNH ẢNH</p> <p>Hình 1 1 Các vị trí đặt IDS mạng 4</p> <p>Hình 1 2 Mô hình kiến trúc hệ thống phát xâm nhập IDS</p> <p>Hình 1 3 Mô hình NIDS</p> <p>Hình 2 1 Ví dụ phân nhóm đối tượng 17</p> <p>Hình 2 2 Các thiết lập để xác định ranh giới cụm ban đầu 18</p> <p>Hình 2 3 Mô tả độ đo khoảng cách đối tượng 19</p> <p>Hình 2 4 Sơ đồ thuật toán phân nhóm K Means 21</p> <p>Hình 2 5 Mô tả trực quan trình phân cụm liệu 22</p> <p>Hình 2 6 Biểu diễn đối tượng mặt phẳng tọa độ x y 25</p> <p>Hình 2 7 Biểu diễn đối tượng phần tử trung tâm mặt phẳng tọa độ x y 26</p> <p>Hình 2 8 Biểu diễn đối tượng</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>phần tử trung tâm mặt phẳng tọa độ x y Vòng lặp 1 29 Hình 2 9 Biểu diễn đối tượng phần tử trung tâm mặt phẳng tọa độ x y 31 Vòng lặp 2 31 Hình 2 10 Biểu diễn đối tượng phần tử trung tâm mặt phẳng tọa độ x y Vòng lặp 3 33 Hình 2 11 Mô hình hệ thống phát bất thường sử dụng thuật toán K means 40 Hình 2 12 Bốn quan hệ công 42 Hình 2 13 Mô tả hoạt động mô đun tổng hợp 44 Hình 3 1 Giảm số ghi cho file đầu vào chương trình 51 Hình 3 2 Xem chỉnh sửa cho file đầu vào chương trình cần 52 Hình 3 3 Dữ liệu chương trình mở No te pa d 52 Hình 3 5 Giao diện chọn liệu 54 Hình 3 6 Hiện thị chi tiết liệu đầu vào 55 Hình 3 7 Form thực thuật toán K Means 56 Hình 3 8 Kết thực thuật toán K Means 57 Hình 3 9 Số ghi kết nối thuộc cụm 58 Hình 3 10 Kết thực thuật toán K Means với liệu có 494020 ghi kết nối 58 Số hóa Trung tâm Học liệu ĐHTN http://www.lrc.tnu.edu.vn iii</p> <p>DANH MỤC BẢNG Bảng 2 1 Danh mục đối tượng 24 Bảng 2 2 Bảng biểu diễn thuộc tính mặt phẳng x y 24 Bảng 2 3 Khởi tạo phần tử trọng tâm 25 Bảng 2 4 Bảng khoảng cách Euc li de an vòng lặp 1 28 Bảng 2 5 Tìm khoảng cách khoảng cách Vòng lặp 1 28 Bảng 2 6 Kết phân nhóm đối tượng vòng lặp 1 28 Bảng 2 7 Phần tử trọng tâm vòng lặp 1 29 Bảng 2 8 Bảng khoảng cách Euc li de an Vòng lặp 2 30 Bảng 2 9 Tìm khoảng cách khoảng cách Vòng lặp 2 30 Bảng 2 10 Kết phân nhóm đối tượng vòng lặp 2 31 Bảng 2 11 Phần tử trọng tâm vòng lặp 2 31 Bảng 2 12 Bảng khoảng cách Euc li de an vòng lặp 3 32 Bảng 2 13 Tìm khoảng cách khoảng cách vòng lặp 3 32 Bảng 2 14 Kết phân nhóm đối tượng vòng lặp 3 33 Bảng 2 15 Phần tử trọng tâm vòng lặp 3 33 Bảng 2 16 Kết phân nhóm đối tượng vòng lặp 4 34 Bảng 2 17 Bảng kết phân nhóm thuộc 34 Bảng 2 18 danh sách cảnh báo chưa rút gọn 45 Bảng 2 19 Danh sách cảnh báo sau rút gọn 46 Bảng 3 1 Các thuộc tính nhóm chứa tất thuộc tính có từ kết nối TCP IP 48 Bảng 3 2 Các thuộc tính lưu thông nhóm bao gồm thuộc tính mà tính toán với khoảng thời gian cửa sổ 49 Bảng 3 2</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>Các thuộc tính nội dung 49 Số hóa Trung tâm Học liệu ĐHTN http://www.lrc.tnu.edu.vn/iv BẢNG TỪ VIẾT TẮT IDS IPS In tru si on De te c ti on Sys tem In tru si on P re ven ti on Sys tem s HIDS Host based IDS NIDS Network based IDS Số hóa Trung tâm Học liệu ĐHTN http://www.lrc.tnu.edu.vn MỞ ĐẦU Ngày nay hệ thống mạng máy tính trở nên phổ biến ứng dụng hầu hết hoạt động kinh tế xã hội nước ta Tuy nhiên mạng máy tính phải đương đầu với nhiều thách thức đặc biệt vấn đề an toàn bảo mật liệu mạng Trong mối đe dọa an ninh mạng việc xâm nhập mạng để thay đổi thông tin lấy cắp liệu phá hoại hạ tầng mạng nghiêm trọng Chính vậy việc phát ngăn chặn xâm nhập mạng máy tính chủ đề quan tâm nghiên cứu phát triển ứng dụng mạnh mẽ Phát ngăn chặn hiểu xác định xâm nhập ngăn chặn cách nhanh xảy Hiện phương pháp phát truy nhập trái phép hoàn hảo kĩ thuật xâm nhập ngày tinh vi luôn đổi Khi phương pháp phát xâm nhập biết đến kẻ xâm nhập sửa chiến lược thử kiểu xâm nhập Chính lựa chọn chủ đề means đề tài nghiên cứu cho luận văn Cấu trúc luận văn bao gồm chương sau Chọ ơ n g 1 C h ư ơ n g trình bày kiến thức phát xâm nhập như định nghĩa thành phần chức hệ thống phân loại phương pháp phát xâm nhập Chọ ơ n g 2 C h ư ơ n g trình bày việc phát xâm nhập dựa thuật toán K means Nội dung thuật toán ví dụ minh họa thuật toán tập liệu kiểm thử mô hình phát xâm nhập dựa thuật toán K means Chọ ơ n g 3 C h ư ơ n g kết cài đặt toán phát xâm nhập dựa thuật toán k means Số hóa Trung tâm Học liệu ĐHTN http://www.lrc.tnu.edu.vn Chọ ơ n g KHÁI QUÁT BÀI TOÁN PHÁT HIỆN XÂM NHẬP 1 1 Định nghĩa phát xâm nhập 1 1 1 Định nghĩa Hệ thống phát xâm nhập IDS hệ thống có nhiệm vụ theo dõi phát có thể ngăn cản xâm nhập hành vi khai thác trái phép tài nguyên hệ thống bảo vệ mà dẫn đến việc làm tổn hại đến tính bảo mật tính toàn vẹn tính sẵn sàng hệ thống 6 Hệ thống IDS thu thập thông tin từ nhiều nguồn hệ thống bảo vệ sau tiến hành phân tích</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>thông tin theo cách khác để phát xâm nhập trái phép Khi hệ thống IDS có khả năng ngăn chặn nguy xâm nhập mà phát gọi hệ thống phòng chống xâm nhập hay IPS Hình sau minh họa vị trí thường cài đặt IDS mạng Hình 1 1 Các vị trí đặt IDS mạng 1 1 2 Sự khác IDS IPS Có thể nhận thấy khác biệt hai khái niệm tên gọi phát hiện ngăn chặn Các hệ thống IDS thiết kế với mục đích chủ yếu phát cảnh báo nguy xâm nhập mạng máy tính bảo vệ đó hệ thống IPS khả phát tự hành động chống lại Số hóa Trung tâm Học liệu ĐHTN http://www.lrc.tnu.edu.vn 53</p> <p>Mỗi dòng tương ứng với giá trị đối tượng luận văn dòng thể liệu ghi kết nối Các giá trị thuộc tính cách dấu 3 3 Cài đặt thuật toán K Means thử nghiệm phân cụm phần tử dị biệt 3 3 1 Giới thiệu môi trường cài đặt Chương trình viết ngôn ngữ C Net Visual Studio 2010 sử dụng phiên Net Framework 4 0 Các thuộc tính liệu đầu vào lưu thành trường liệu chương trình lưu trữ hệ quản trị sở liệu Sql Server 2008 R2 Thuật toán K mean thuật toán kinh điển cài đặt sử dụng rộng rãi Trong ta sử dụng thư viện thuật toán K Means ứng dụng cho toán phát cụm dị biệt thư viện sử dụng có tên IKVM OpenJDK Core.dll IKVM OpenJDK Util.dll IKVM OpenJDK Text.dll IKVM Runtime.dll JNI.dll WekaSharp.dll 3 3 2 Các chức năng chương trình Lưu đồ thực hiện chương trình Số hóa Trung tâm Học liệu ĐHTN http://www.lrc.tnu.edu.vn 54 a</p> <p>Đọc file liệu đầu vào Cho phép nhập liệu từ tệp có cấu trúc mô tả mục 3 2 Trước nhập liệu cho chương trình người dùng chỉnh sửa giao diện phần mềm Weka Để nhập liệu người dùng nhấn vào nút Chọn sau tìm đến tệp liệu có cấu trúc lưu trữ máy tính có đuôi dạng arff Sau chọn tệp liệu lấy thông tin cần thiết thuộc tính thực đưa vào sở liệu hiển thị lên nhóm Chi tiết liệu để phục vụ cho việc thực thuật toán dễ dàng Hình 3 5 Giao diện chọn liệu b</p> <p>Chi tiết liệu Nhóm chi tiết liệu hiển thị thông tin ghi kết nối file liệu đầu vào số dòng thứ tự ghi cột thuộc tính chi tiết nội dung liệu ghi Do số lượng ghi liệu đầu thường lớn nên việc hiển thị chi tiết liệu</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>thực với số lượng nhỏ để tránh ảnh hưởng tới tốc độ thực thi Mặc định liệu hiển thị đặt từ tới 100 Nếu muốn xem chi tiết ghi ta đánh số vào te xt bo x liệu từ đến nhấn hiển thị để xem Số hóa Trung tâm Học liệu ĐHTN http://www.lrc.tnu.edu.vn 55 Hình 3 6 Hiển thị chi tiết liệu đầu vào Sau chọn file liệu đầu vào ta click vào bu t ton Thực KMeans để chuyển sang form thực thuật toán phân cụm ghi thông thường dị biệt c Tham số phân cụm K Means Cho phép người dùng nhập tham số điều khiển cho thuật toán K Means bao gồm số cụm cần phân Theo phân tích chương việc phân cụm phát phần tử dị biệt ta chọn số cụm cần phân C hữ ợn g trình cho phép thực hàm khoảng cách theo Euc li d Sau lựa chọn đầy đủ tham số người dùng nhấn nút Thực K Means để chương trình xử lý tính toán Số hóa Trung tâm Học liệu ĐHTN http://www.lrc.tnu.edu.vn 56 Hình 3 7 Form thực thuật toán K Means Do số lượng ghi lớn nên việc thực hết khoảng phút máy tính có cấu hình CPU Ce le ro n D 1 6GHZ nhớ Ram 1GB cho liệu có 49402 ghi kết nối Và khoảng 20 phút cho liệu có 49402 ghi 1 10 liệu KDD đầy đủ Sau thực xong thuật toán thông tin chi tiết phân cụm ghi hiển thị bảng bên trái Ta chọn chi tiết phân cụm từ ghi x đến y chọn hiển thị để xem chi tiết khoảng Thông tin số lần lặp tổng bình phương lỗi khai tính khoảng cách Euc li d cụm hiển thị Kết phân cụm K Means phía bên phải form Các giá trị bị thay giá trị trung bình tính lại trọng tâm cho cụm Số hóa Trung tâm Học liệu ĐHTN http://www.lrc.tnu.edu.vn 57 Hình 3 8 Kết thực thuật toán K Means Bảng phân cụm cho ta thông tin chi tiết trọng tâm thuộc tính cụm số ghi cụm Từ ta nhận thấy thông tin cụm thể nhiều biểu cụm ghi dị biệt lấy ví dụ như đăng nhập không thành công login giá trị 0 Số giây kết nối du ra ti on ngắn số kết nối tới host thời điểm khoản thời gian s trước với số kết nối tới có loại dịch vụ thời điểm khoản thời gian s trước lớn biểu cho công v v Còn phần tử đánh dấu là ghi kết nối bình thường Việc nhận biết cụm bình thường dị biệt phụ thuộc vào</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>giá trị thuộc tính vào số hay thuật toán K Means khả năng nhận biết cụm có giá trị thuộc tính thuộc dạng Ở cuối bảng phân cụm thông số tỉ lệ ghi thuộc cụm bình thường hay dị biệt cụ thể số ghi cụm Số hóa Trung tâm Học liệu ĐHTN http://www.lrc.tnu.edu.vn 58 Hình 3.9 Số ghi kết nối thuộc cụm Ảnh cho ta thấy kết thực thuật toán K Means liệu lớn 49402 ghi 1.10 liệu KDD cup Kết cho thấy cụm liệu đánh số cụm chứa ghi kết nối thông thường cụm liệu đánh cụm ghi kết nối dị biệt Hình 3.10 Kết thực thuật toán K Means với liệu có 494020 ghi kết nối Số hóa Trung tâm Học liệu ĐHTN http://www.lrc.tnu.edu.vn 59 Ngoài chương trình cho phép lưu kết định dạng file text ta nhấn vào Lưu kết file chọn đường dẫn tên file save 3.4 Nhận xét đánh giá chương trình thử nghiệm Chương trình cài đặt dựa thuật toán K Means sử dụng hai hàm khoảng cách phổ biến khoảng cách Euc li d Cho phép người dùng tùy chọn số cụm K khoảng cách tối đa seed thông số ảnh hưởng tới số lần lặp để kết cuối Kết thu phần tử phân theo cụm đánh số từ đến số cụm Nhược điểm chương trình kết hiển thị chưa trực quan Số hóa Trung tâm Học liệu ĐHTN http://www.lrc.tnu.edu.vn 60 KẾT LUẬN VÀ HƯỚNG NGHIÊN CỨU KẾT LUẬN Trong luận văn tìm hiểu nghiên cứu số vấn đề sau Luận văn trình bày lý thuyết công mạng kiểu công phân cụm liệu thuật toán K Means phân cụm liệu dựa vào cụm trung tâm để ứng dụng vào phân cụm phân tử dị biệt kết nối Giới thiệu cấu trúc thuộc tính liệu KDD Cup 1999 phương pháp giảm số ghi liệu đầu vào Luận văn cài đặt thuật toán phân cụm K means để minh họa cho việc phân loại kết nối thông thường dị biệt Tuy nhiên chương trình có nhiều hạn chế kết hiển thị chưa trực quan định dạng tệp hỗ trợ đầu vào tệp arff HƯỚNG NGHIÊN CỨU Trong tương lai đề tài phát triển theo hướng nghiên cứu phân thu thập trực tiếp ghi kết nối từ mạng thực phân loại có modul phát đầu kết nối thông thường đầu kết nối dị biệt từ cảnh báo kết nối không an toàn lượng ghi kết nối thuộc nhóm dị biệt xuất nhiều Số hóa</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>Trung tâm Học liệu ĐHTN http://www.lrc.tnu.edu.vn 61 TÀI LIỆU THAM KHẢO</p> <p>Tiếng Việt 1 Vũ Lan P. h.ư. ơ. n. g. N. ghi. ê. n. cứu. c. ài. đ.ặ. t. số. gi.ải. thu.ậ. t. phân. c.ụ. m. phân. lớp. 2006 Đại học Bách khoa Hà Nội 2</p> <p>Hoàng Thị Toàn 2012 N. ghi. ê. n. cứu. s.ở. li.ệ. u. KDD 99 ứng. d.ụ. n. g. cho. bảo. m.ậ. t. mạng. Đề. tài. nghiên. cứu. khoa. học. Tiếng. Anh. 3 Han J and K. am. be. r. M. Data. M. in. in. g. Concepts. and. Tech. ni. que. s. 3rd. E. di. ti. on. Mor. gan. K. au. f. man. A. ca. de. mi. c. Press. 2011 4 Tapas K. an. ung. o. An. Efficient. K. Means. C. lu. s. te. ri. ng. Al. go. ri. thm. A. na. ly. si. s. and. Imp. le. men. ta. ti. on. 2002 5 And. re. w. Moore. K. means. and. Hie. ra. r. chi. ca. l. C. lu. s. te. ri. ng. Tu. to. ria. IS. li. de. s. http://www2.cs.cmu.edu/awm/tu-to-ria/ls/km-e-an-s.html 6 IATAC In. tru. si. on. De. te. c. ti. on. Sys. tem. s. The. Infor. ma. ti. on. As. su. ran. ce. Tech. no. lo. gy. A. na. ly. si. s. Cen. te. r. Sixth. E. di. ti. on. Sep. tem. be. r. 25. 2009 7 Ger. ha. rd. M. un. z. Sa. Li. Georg. Carle. Wil. he. lm. S. chi. ck. ard. T. ra. ffic. A. no. ma. ly. De. te. c. ti. on. Using. K. Means. C. lu. s. te. ri. ng. U. ni. ve. r. si. ty. of. Tue. bin. gen. Ger. man. y. 2008 Số. hóa. Trung. tâm. Học. li.ệ. u. ĐHTN http://www.lrc.tnu.edu.vn 62 PHẦN PHỤ LỤC</p> <p>Xử. lý. giao. di.ệ. n. người. dùng. phần. thu.ậ. t. toán. K. Means. using. using. using. using. using. using. using. using. using. using. Sys. tem. Confi. gu. ra. ti. on. Sys. tem. weka. WekaS. ha. rp. weka. core. weka. c. lu. s. te. re. rs. weka. core. ma. tri. x. Sys. tem. Col. le. c. ti. ons. Ge. ne. ri. c. Sys. tem. C. om. po. nen. t. Mo. de. l. Sys. tem. Data. Sys. tem. D. ra. win. g. Sys. tem. Linq. Sys. tem. Text. Sys. tem. W. in. do. ws. Forms. Sys. tem. IO. na. me. s. pa. ce. GSSL. pub. li. c. pa. r. tia. l. class. frm. M. ai. n. Form. pub. li. c. s. tri. ng. s. Fi. le. Path. pub. li. c. int. as. si. gn. men. ts. pub. li. c. frm. M. ai. n. l. ni. tia. li. ze. C. om. po. nen. t. p. ri. va. te. void. btn. T. hu. ch. ien. Click. object. sen. de. r. E. ven. t. Args. e. int. number. Of. C. lu. s. te. rs. Con. ve. rt. To. Int. 16. txt. N. um. C. lu. s. te. r. Text. Sc. ri. p. tin. g. Fi. le. Sys. tem. Object. My. Fi. le. new. Sc. ri. p. tin. g. Fi. le. Sys. tem. Object. s. tri. ng. s. Fi. le. N. am. e. Sc. ri. p. tin. g. Text. S. tre. am. s. tri. ng. s. Con. ten. ts. s. tri. ng. str. R. Số. hóa. Trung. tâm. Học. li.ệ. u. ĐHTN. msg. S. tre. am. http://www.lrc.tnu.edu.vn 63 Ins. tan. ces. insts.</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>new Ins tan ces new java io Buffe re dRea de r new java io Fi le Rea de r sFi le Path weka fil te rs un su pe r vi se d at tri bu te S tri ngToN om in al fil te r new weka fil te rs un su pe r vi se d at tri bu te S tri ngToN om in al fil te r se tAt tri bu te R ang e first fil te r se tInputFor ma t insts weka fil te rs Fil te r u se Fil te r insts fil te r S im p le KMe an s km e an s new S im p le KMe an s km e an s se tSeed Con ve rt ToInt 16 txtSeed Text This is the im por tan t pa ra me te r to set km e an s se tP re se r ve Ins tan cesOr de r true km e an s se tN um C lu s te rs number OfC lu s te rs km e an s bu ildC lu s te re r insts C lu s te rE va lua ti on eval new C lu s te rE va lua ti on eval se tC lu s te re r km e an s eval e va lua te C lu s te re r new Ins tan ces insts km e an s getC lu s te rCen tro ids sCon ten ts eval c lu s te rRe su ltsToS tri ng sFi le N am e D DE TAI THAC SI BoCai M an gu on IDS KDDCupOutPut txt msgS tre am MyFi le C re a te TextFi le sFi le N am e true true msgS tre am Write sCon ten ts msgS tre am Close sCon ten ts msgS tre am MyFi le O pe nTextFi le sFi le N am e Sc ri p tin g IOMo de ForRea di ng fal se Sc ri p tin g T ri s ta te T ri s ta te T ru e int i 0 s tri ng words words File ReadAll in es sFi le N am e En co di ng Def au lt for i 0 i words L eng th i i 1 s tri ng t words i Trim t Rep la ce t Rep la ce t Rep la ce t Rep la ce t Rep la ce t Rep la ce s tri ng strlv t Split Số hóa Trung tâm Học liệu ĐHTN http www lrc tnu edu vn 64 t t Rep la ce At tri bu te Thuộc tính t t Rep la ce N um be r of i te ra ti on Số lần lặp t t Rep la ce Mis sin g va lu es g lo ba l ly re p la ced with mean mode Toàn giá trị bị thay trung bình mode t t Rep la ce Full Data Dữ liệu đầy đủ t t Rep la ce C lu s te r cen tro ids Trọng tâm cụm t t Rep la ce C lu s te r Cụm t t Rep la ce Wi thin c lu s te r sum of s qua re d er ro rs Tổng bình phương lỗi cụm t t Rep la ce C lu s te re d Ins tan ces Các cụm phân if i 11 ListViewI tem lvt new ListViewI tem Số ghi for int j 0 j strlv L eng th j if strlv E le men tAt j ToS tri ng</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		http://123doc.org/document/3339212-phat-hien-xam-nhap-dua-tren-thuat-toan-kmeans.htm	
24	NIDS cung cấp dữ liệu về hiệu suất mạng nội bộ, tổng hợp lại các gói tin và phân tích chúng.	<p>NIDS cung cấp dữ liệu về hiệu suất mạng nội bộ tập hợp lại các gói tin và phân tích chúng</p> <p>https://text.123doc.org/document/1797837-chuong-1-tong-quan-ve-he-thong-phat-hien-xam-nhap.htm</p>	87
24	Điểm yếu của NIDS là gây ảnh hưởng đến băng thông mạng do trực tiếp truy cập vào lưu thông mạng. NIDS không được định lượng đúng về khả năng xử lý sẽ trở thành một nút cổ chai gây ách tắc trong mạng.	<p>Trong hệ thống NIDS các Sensor được đặt ở các điểm cần kiểm tra trong mạng thường là trước miền DMZ hoặc ở vùng biên của mạng các Sensor bắt tất cả các gói tin lưu thông trên mạng và phân tích nội dung bên trong của từng gói để phát hiện các dấu hiệu tấn công trong mạng</p> <p>21 Hình 1.6 Hoạt động của HIDS</p> <p>XÂY DỰNG HỆ THỐNG PHÁT HIỆN XÂM NHẬP BẤT THƯỜNG VỚI PHẦN MỀM SNORT</p> <p>Điểm yếu của NIDS là gây ảnh hưởng đến băng thông mạng do trực tiếp truy cập vào lưu thông mạng NIDS không được định lượng đúng về khả năng xử lý sẽ trở thành một nút cổ chai gây ách tắc trong mạng</p> <p>https://text.123doc.org/document/2311662-xay-dung-he-thong-phat-hien-xam-nhap-bat-thuong-voi-phan-mem-snort.htm</p>	100
24	Ngoài ra NIDS còn gặp khó khăn với các vấn đề giao thức truyền như việc phân tách gói tin (IP fragmentation), hay việc điều chỉnh thông số TTL trong gói tin IP.	<p>Ngoài ra NIDS còn gặp khó khăn với các vấn đề giao thức truyền như việc phân tách gói tin IP fragmentation hay việc điều chỉnh thông số TTL trong gói tin IP</p> <p>14 Hình 1.6 Hoạt động của HIDS</p> <p>17 Hoạt động của NIDS</p> <p>HIDS NIDS Tính quản trị thấp</p> <p>https://text.123doc.org/document/1080878-tai-lieu-luan-van-xay-dung-he-thong-phat-hien-xam-nhap-bang-phan-mem-snort-pot.htm</p>	100

Trang	Câu trùng lặp	Nguồn	Điểm
	1.2.2.2. Phát hiện xâm nhập host (HIDS – Host -based IDS)	<p>Số hóa Trung tâm Học liệu ĐHTN http://www.lrc.tnu.edu.vn i MỤC LỤC MỞ ĐẦU</p> <p>4 Chương 1 KHÁI QUÁT BÀI TOÁN PHÁT HIỆN XÂM NHẬP 1 1 Định nghĩa phát xâm nhập 1 1 1 Định nghĩa 1 1 2 Sự khác IDS IPS 1 2 Các thành phần chức hệ thống phát thâm nhập 5 1 2 1 Thành phần thu thập gói tin 6 1 2 2 Thành phần phát gói tin 6 1 2 3 Thành phần phản hồi 1 3 Phân loại phát xâm nhập 1 3 1 Network based IDS NIDS 7 1 3 2 Host based IDS HIDS 9 11 1 4 1 Mô hình phát lạm dụng 11 1 4 2 Mô hình phát bất thường 12 1 4 3 So sánh hai mô hình 15</p> <p>Chương 2 PHÁT HIỆN XÂM NHẬP DỰA TRÊN THUẬT TOÁN K MEANS 17</p> <p>2 1 Thuật toán K means 17 2 1 1 Các khái niệm 17 2 1 2 Thuật toán 20 2 1 3 Nhược điểm K Means cách khắc phục 35 2 2 Thuật toán K means với phát xâm nhập 35 2 2 1 Phân tích tập liệu kiểm thử 35 2 2 2 Mô hình phát bất thường dựa thuật toán K means 39</p> <p>Chương 3 XÂY DỰNG CHƯƠNG TRÌNH PHÁT HIỆN XÂM NHẬP DỰA TRÊN THUẬT TOÁN K MEANS 47 3 1 Mô tả toán 47 3 2 Mô tả liệu đầu vào 47 3 2 1 Mô tả thuộc tính file liệu đầu vào 48 3 2 2 Giảm số lượng ghi liệu đầu vào 50 3 3 Cài đặt thuật toán K Means thử nghiệm phân cụm phần tử dị biệt 53 3 3 1 Giới thiệu môi trường cài đặt 53 3 3 2 Các chức chương trình 53 3 4 Nhận xét đánh giá chương trình thử nghiệm 59</p> <p>KẾT LUẬN VÀ HƯỚNG NGHIÊN CỨU 60</p> <p>TÀI LIỆU THAM KHẢO 61</p> <p>PHẦN PHỤ LỤC 62</p> <p>Số hóa Trung tâm Học liệu ĐHTN http://www.lrc.tnu.edu.vn ii DANH MỤC HÌNH ẢNH</p> <p>Hình 1 1 Các vị trí đặt IDS mạng 4</p> <p>Hình 1 2 Mô hình kiến trúc hệ thống phát xâm nhập IDS</p> <p>Hình 1 3 Mô hình NIDS</p> <p>Hình 2 1 Ví dụ phân nhóm đối tượng 17</p> <p>Hình 2 2 Các thiết lập để xác định ranh giới cụm ban đầu 18</p> <p>Hình 2 3 Mô tả độ đo khoảng cách đối tượng 19</p> <p>Hình 2 4 Sơ đồ thuật toán phân nhóm K Means 21</p> <p>Hình 2 5 Mô tả trực quan trình phân cụm liệu 22</p> <p>Hình 2 6 Biểu diễn đối tượng mặt phẳng tọa độ x y 25</p> <p>Hình 2 7 Biểu diễn đối tượng phần tử trung tâm mặt phẳng tọa độ x y 26</p> <p>Hình 2 8 Biểu diễn đối tượng</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>phần tử trung tâm mặt phẳng tọa độ x y Vòng lặp 1 29 Hình 2 9 Biểu diễn đối tượng phần tử trung tâm mặt phẳng tọa độ x y 31 Vòng lặp 2 31 Hình 2 10 Biểu diễn đối tượng phần tử trung tâm mặt phẳng tọa độ x y Vòng lặp 3 33 Hình 2 11 Mô hình hệ thống phát bất thường sử dụng thuật toán K means 40 Hình 2 12 Bốn quan hệ công 42 Hình 2 13 Mô tả hoạt động mô đun tổng hợp 44 Hình 3 1 Giảm số ghi cho file đầu vào chương trình 51 Hình 3 2 Xem chỉnh sửa cho file đầu vào chương trình cần 52 Hình 3 3 Dữ liệu chương trình mở No te pa d 52 Hình 3 5 Giao diện chọn liệu 54 Hình 3 6 Hiện thị chi tiết liệu đầu vào 55 Hình 3 7 Form thực thuật toán K Means 56 Hình 3 8 Kết thực thuật toán K Means 57 Hình 3 9 Số ghi kết nối thuộc cụm 58 Hình 3 10 Kết thực thuật toán K Means với liệu có 494020 ghi kết nối 58 Số hóa Trung tâm Học liệu ĐHTN http://www.lrc.tnu.edu.vn iii</p> <p>DANH MỤC BẢNG Bảng 2 1 Danh mục đối tượng 24 Bảng 2 2 Bảng biểu diễn thuộc tính mặt phẳng x y 24 Bảng 2 3 Khởi tạo phần tử trọng tâm 25 Bảng 2 4 Bảng khoảng cách Euc li de an vòng lặp 1 28 Bảng 2 5 Tìm khoảng cách khoảng cách Vòng lặp 1 28 Bảng 2 6 Kết phân nhóm đối tượng vòng lặp 1 28 Bảng 2 7 Phần tử trọng tâm vòng lặp 1 29 Bảng 2 8 Bảng khoảng cách Euc li de an Vòng lặp 2 30 Bảng 2 9 Tìm khoảng cách khoảng cách Vòng lặp 2 30 Bảng 2 10 Kết phân nhóm đối tượng vòng lặp 2 31 Bảng 2 11 Phần tử trọng tâm vòng lặp 2 31 Bảng 2 12 Bảng khoảng cách Euc li de an vòng lặp 3 32 Bảng 2 13 Tìm khoảng cách khoảng cách vòng lặp 3 32 Bảng 2 14 Kết phân nhóm đối tượng vòng lặp 3 33 Bảng 2 15 Phần tử trọng tâm vòng lặp 3 33 Bảng 2 16 Kết phân nhóm đối tượng vòng lặp 4 34 Bảng 2 17 Bảng kết phân nhóm thuộc 34 Bảng 2 18 danh sách cảnh báo chưa rút gọn 45 Bảng 2 19 Danh sách cảnh báo sau rút gọn 46 Bảng 3 1 Các thuộc tính nhóm chứa tất thuộc tính có từ kết nối TCP IP 48 Bảng 3 2 Các thuộc tính lưu thông nhóm bao gồm thuộc tính mà tính toán với khoảng thời gian cửa sổ 49 Bảng 3 2</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>Các thuộc tính nội dung 49 Số hóa Trung tâm Học liệu ĐHTN http://www.lrc.tnu.edu.vn/iv BẢNG TỪ VIẾT TẮT IDS IPS In trư si on De te c ti on Sys tem In trư si on P re ven ti on Sys tem s HIDS Host based IDS NIDS Network based IDS Số hóa Trung tâm Học liệu ĐHTN http://www.lrc.tnu.edu.vn MỞ ĐẦU Ngày nay hệ thống mạng máy tính trở nên phổ biến ứng dụng hầu hết hoạt động kinh tế xã hội nước ta Tuy nhiên mạng máy tính phải đương đầu với nhiều thách thức đặc biệt vấn đề an toàn bảo mật liệu mạng Trong mối đe dọa an ninh mạng việc xâm nhập mạng để thay đổi thông tin lấy cắp liệu phá hoại hạ tầng mạng nghiêm trọng Chính vậy việc phát ngăn chặn xâm nhập mạng máy tính chủ đề quan tâm nghiên cứu phát triển ứng dụng mạnh mẽ Phát ngăn chặn hiểu xác định xâm nhập ngăn chặn cách nhanh xảy Hiện phương pháp phát truy nhập trái phép hoàn hảo kĩ thuật xâm nhập ngày tinh vi luôn đổi Khi phương pháp phát xâm nhập biết đến kẻ xâm nhập sửa chiến lược thử kiểu xâm nhập Chính lựa chọn chủ đề means đề tài nghiên cứu cho luận văn Cấu trúc luận văn bao gồm chương sau Chọ ơ n g 1 C h ư ơ n g trình bày kiến thức phát xâm nhập như định nghĩa thành phần chức hệ thống phân loại phương pháp phát xâm nhập Chọ ơ n g 2 C h ư ơ n g trình bày việc phát xâm nhập dựa thuật toán K means Nội dung thuật toán ví dụ minh họa thuật toán tập liệu kiểm thử mô hình phát xâm nhập dựa thuật toán K means Chọ ơ n g 3 C h ư ơ n g kết cái đặt toán phát xâm nhập dựa thuật toán k means Số hóa Trung tâm Học liệu ĐHTN http://www.lrc.tnu.edu.vn Chọ ơ n g KHÁI QUÁT BÀI TOÁN PHÁT HIỆN XÂM NHẬP 1 1 Định nghĩa phát xâm nhập 1 1 1 Định nghĩa Hệ thống phát xâm nhập IDS hệ thống có nhiệm vụ theo dõi phát có thể ngăn cản xâm nhập hành vi khai thác trái phép tài nguyên hệ thống bảo vệ mà dẫn đến việc làm tổn hại đến tính bảo mật tính toàn vẹn tính sẵn sàng hệ thống 6 Hệ thống IDS thu thập thông tin từ nhiều nguồn hệ thống bảo vệ sau tiến hành phân tích</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>thông tin theo cách khác để phát xâm nhập trái phép Khi hệ thống IDS có khả năng ngăn chặn nguy xâm nhập mà phát gọi hệ thống phòng chống xâm nhập hay IPS Hình sau minh họa vị trí thường cài đặt IDS mạng Hình 1 1 Các vị trí đặt IDS mạng 1 1 2 Sự khác IDS IPS Có thể nhận thấy khác biệt hai khái niệm tên gọi phát hiện ngăn chặn Các hệ thống IDS thiết kế với mục đích chủ yếu phát cảnh báo nguy xâm nhập mạng máy tính bảo vệ đó hệ thống IPS khả phát tự hành động chống lại Số hóa Trung tâm Học liệu ĐHTN http://www.lrc.tnu.edu.vn 53</p> <p>Mỗi dòng tương ứng với giá trị đối tượng luận văn dòng thể liệu ghi kết nối Các giá trị thuộc tính cách dấu 3 3 Cài đặt thuật toán K Means thử nghiệm phân cụm phần tử dị biệt 3 3 1 Giới thiệu môi trường cài đặt Chương trình viết ngôn ngữ C Net Visual Studio 2010 sử dụng phiên Net Framework 4 0 Các thuộc tính liệu đầu vào lưu thành trường liệu chương trình lưu trữ hệ quản trị sở liệu Sql Server 2008 R2 Thuật toán K mean thuật toán kinh điển cài đặt sử dụng rộng rãi Trong ta sử dụng thư viện thuật toán K Means ứng dụng cho toán phát cụm dị biệt thư viện sử dụng có tên IKVM OpenJDK Core.dll IKVM OpenJDK Util.dll IKVM OpenJDK Text.dll IKVM Runtime.dll JNI.dll WekaSharp.dll 3 3 2 Các chức năng chương trình Lưu đồ thực hiện chương trình Số hóa Trung tâm Học liệu ĐHTN http://www.lrc.tnu.edu.vn 54 a</p> <p>Đọc file liệu đầu vào Cho phép nhập liệu từ tệp có cấu trúc mô tả mục 3 2 Trước nhập liệu cho chương trình người dùng chỉnh sửa giao diện phần mềm Weka Để nhập liệu người dùng nhấn vào nút Chọn sau tìm đến tệp liệu có cấu trúc lưu trữ máy tính có đuôi dạng arff Sau chọn tệp liệu lấy thông tin cần thiết thuộc tính thực đưa vào sở liệu hiển thị lên nhóm Chi tiết liệu để phục vụ cho việc thực thuật toán dễ dàng Hình 3 5 Giao diện chọn liệu b</p> <p>Chi tiết liệu Nhóm chi tiết liệu hiển thị thông tin ghi kết nối file liệu đầu vào số dòng thứ tự ghi cột thuộc tính chi tiết nội dung liệu ghi Do số lượng ghi liệu đầu thường lớn nên việc hiển thị chi tiết liệu</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>thực với số lượng nhỏ để tránh ảnh hưởng tới tốc độ thực thi Mặc định liệu hiển thị đặt từ tới 100 Nếu muốn xem chi tiết ghi ta đánh số vào te xt bo x liệu từ đến nhấn hiển thị để xem Số hóa Trung tâm Học liệu ĐHTN http://www.lrc.tnu.edu.vn 55 Hình 3 6 Hiển thị chi tiết liệu đầu vào Sau chọn file liệu đầu vào ta click vào bu t ton Thực KMeans để chuyển sang form thực thuật toán phân cụm ghi thông thường dị biệt c Tham số phân cụm K Means Cho phép người dùng nhập tham số điều khiển cho thuật toán K Means bao gồm số cụm cần phân Theo phân tích chương việc phân cụm phát phần tử dị biệt ta chọn số cụm cần phân C hữ ợn g trình cho phép thực hàm khoảng cách theo Euc li d Sau lựa chọn đầy đủ tham số người dùng nhấn nút Thực K Means để chương trình xử lý tính toán Số hóa Trung tâm Học liệu ĐHTN http://www.lrc.tnu.edu.vn 56 Hình 3 7 Form thực thuật toán K Means Do số lượng ghi lớn nên việc thực hết khoảng phút máy tính có cấu hình CPU Ce le ro n D 1 6GHZ nhớ Ram 1GB cho liệu có 49402 ghi kết nối Và khoảng 20 phút cho liệu có 49402 ghi 1 10 liệu KDD đầy đủ Sau thực xong thuật toán thông tin chi tiết phân cụm ghi hiển thị bảng bên trái Ta chọn chi tiết phân cụm từ ghi x đến y chọn hiển thị để xem chi tiết khoảng Thông tin số lần lặp tổng bình phương lỗi khai tính khoảng cách Euc li d cụm hiển thị Kết phân cụm K Means phía bên phải form Các giá trị bị thay giá trị trung bình tính lại trọng tâm cho cụm Số hóa Trung tâm Học liệu ĐHTN http://www.lrc.tnu.edu.vn 57 Hình 3 8 Kết thực thuật toán K Means Bảng phân cụm cho ta thông tin chi tiết trọng tâm thuộc tính cụm số ghi cụm Từ ta nhận thấy thông tin cụm thể nhiều biểu cụm ghi dị biệt lấy ví dụ như đăng nhập không thành công login giá trị 0 Số giây kết nối du ra ti on ngắn số kết nối tới host thời điểm khoản thời gian s trước với số kết nối tới có loại dịch vụ thời điểm khoản thời gian s trước lớn biểu cho công v v Còn phần tử đánh dấu là ghi kết nối bình thường Việc nhận biết cụm bình thường dị biệt phụ thuộc vào</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>giá trị thuộc tính vào số hay thuật toán K Means khả nhận biết cụm có giá trị thuộc tính thuộc dạng Ở cuối bảng phân cụm thông số tỉ lệ ghi thuộc cụm bình thường hay dị biệt cụ thể số ghi cụm Số hóa Trung tâm Học liệu ĐHTN http://www.lrc.tnu.edu.vn 58 Hình 3.9 Số ghi kết nối thuộc cụm Ảnh cho ta thấy kết thực thuật toán K Means liệu lớn 49402 ghi 1.10 liệu KDD cup Kết cho thấy cụm liệu đánh số cụm chứa ghi kết nối thông thường cụm liệu đánh cụm ghi kết nối dị biệt Hình 3.10 Kết thực thuật toán K Means với liệu có 494020 ghi kết nối Số hóa Trung tâm Học liệu ĐHTN http://www.lrc.tnu.edu.vn 59 Ngoài chương trình cho phép lưu kết định dạng file text ta nhấn vào Lưu kết file chọn đường dẫn tên file save 3.4 Nhận xét đánh giá chơ ơng trình thử nghiệm C hơ ơng trình cài đặt dựa thuật toán K Meana sử dụng hai hàm khoảng cách phổ biến khoảng cách Euc li d Cho phép người dùng tùy chọn số cụm K hoảng cách tối đa seed thông số ảnh hưởng tới số lần lặp để kết cuối Kết thu phần tử phân theo cụm đánh số từ đến số cụm Nhược điểm chương trình kết hiển thị chưa trực quan Số hóa Trung tâm Học liệu ĐHTN http://www.lrc.tnu.edu.vn 60 KẾT LUẬN VÀ HỢI CƯƠNG NGHIÊN CỨU KẾT LUẬN Trong luận văn tìm hiểu nghiên cứu số vấn đề sau Luận văn trình bày lý thuyết công mạng kiểu công phân cụm liệu thuật toán K Means phân cụm liệu dựa vào cụm trung tâm để ứng dụng vào phân cụm phân tự dị biệt kết nối Giới thiệu cấu trúc thuộc tính liệu KDD Cup 1999 phương pháp giảm số ghi liệu đầu vào Luận văn cài đặt thuật toán phân cụm K means để minh họa cho việc phân loại kết nối thông thường dị biệt Tuy nhiên chương trình có nhiều hạn chế kết hiển thị chưa trực quan định dạng tệp hỗ trợ đầu vào tệp arff HỢI CƯƠNG NGHIÊN CỨU Trong tương lai đề tài phát triển theo hướng nghiên cứu phân thu thập trực tiếp ghi kết nối từ mạng thực phân loại có modul phát đầu kết nối thông thường đầu kết nối dị biệt từ cảnh báo kết nối không an toàn lượng ghi kết nối thuộc nhóm dị biệt xuất nhiều Số hóa</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>Trung tâm Học liệu ĐHTN http://www.lrc.tnu.edu.vn 61 TÀI LIỆU THAM KHẢO</p> <p>Tiếng Việt 1 Vũ Lan P. h.ư. ơ. n. g. N. ghi. ê. n. cứu. c. ài. đ.ặ. t. số. gi.ải. thu.ậ. t. phân. c.ụ. m. phân. lớp. 2006 Đại học Bách khoa Hà Nội 2</p> <p>Hoàng Thị Toàn 2012 N. ghi. ê. n. cứu. s.ở. li.ệ. u. KDD 99 ứng. d.ụ. n. g. cho. bảo. m.ậ. t. mạng. Đề. tài. nghiên. cứu. khoa. học. Tiếng. Anh. 3 Han J and K. am. b. e. r. M. Data. M. in. in. g. Concepts. and. Tech. ni. que. s. 3rd. E. di. ti. on. Mor. gan. K. au. f. man. A. ca. de. mi. c. Press. 2011 4 Tapas K. an. ung. o. An. Efficient. K. Means. C. lu. s. te. ri. ng. Al. go. ri. thm. A. na. ly. si. s. and. Imp. le. men. ta. ti. on. 2002 5 And. re. w. Moore. K. means. and. Hie. ra. r. chi. ca. l. C. lu. s. te. ri. ng. Tu. to. ria. IS. li. de. s. http://www2.cs.cmu.edu/awm/tu-to-ria/ls/km/ean/s.html 6 IATAC In. tru. si. on. De. te. c. ti. on. Sys. tem. s. The. Infor. ma. ti. on. As. su. ran. ce. Tech. no. lo. gy. A. na. ly. si. s. Cen. te. r. Sixth. E. di. ti. on. Sep. tem. b. e. r. 25. 2009 7 Ger. ha. rd. M. un. z. Sa. Li. Georg. Carle. Wil. he. lm. S. chi. ckard. T. ra. ffic. A. no. ma. ly. De. te. c. ti. on. Using. K. Means. C. lu. s. te. ri. ng. U. ni. ve. r. si. ty. of. Tue. bin. gen. Ger. man. y. 2008 Số. hóa. Trung. tâm. Học. li.ệ. u. ĐHTN http://www.lrc.tnu.edu.vn 62 PHẦN PHỤ LỤC</p> <p>Xử. lý. giao. di.ệ. n. người. dùng. phần. thu.ậ. t. toán. K. Means. using. using. using. using. using. using. using. using. using. using. Sys. tem. Confi. gu. ra. ti. on. Sys. tem. weka. WekaS. ha. rp. weka. core. weka. c. lu. s. te. re. rs. weka. core. ma. tri. x. Sys. tem. Col. le. c. ti. ons. Ge. ne. ri. c. Sys. tem. C. om. po. nen. t. Mo. de. l. Sys. tem. Data. Sys. tem. D. ra. win. g. Sys. tem. Linq. Sys. tem. Text. Sys. tem. W. in. do. ws. Forms. Sys. tem. IO. na. me. s. pa. ce. GSSL. pub. li. c. pa. r. tia. l. class. frm. M. ai. n. Form. pub. li. c. s. tri. ng. s. Fi. le. Path. pub. li. c. int. as. si. gn. men. ts. pub. li. c. frm. M. ai. n. l. ni. tia. li. ze. C. om. po. nen. t. p. ri. va. te. void. btn. T. hu. c. Hien. Click. object. sen. de. r. E. ven. t. Args. e. int. number. Of. C. lu. s. te. rs. Con. ve. rt. To. Int. 16. txt. N. um. C. lu. s. te. r. Text. Sc. ri. p. tin. g. Fi. le. Sys. tem. Object. My. Fi. le. new. Sc. ri. p. tin. g. Fi. le. Sys. tem. Object. s. tri. ng. s. Fi. le. N. am. e. Sc. ri. p. tin. g. Text. S. tre. am. s. tri. ng. s. Con. ten. ts. s. tri. ng. str. R. Số. hóa. Trung. tâm. Học. li.ệ. u. ĐHTN. msg. S. tre. am. http://www.lrc.tnu.edu.vn 63 Ins. tan. ces. insts.</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>new Ins tan ces new java io Buffe re dRea de r new java io Fi le Rea de r sFi le Path weka fil te rs un su pe r vi se d at tri bu te S tri ngToN om in al fil te r new weka fil te rs un su pe r vi se d at tri bu te S tri ngToN om in al fil te r se tAt tri bu te R ang e first fil te r se tInputFor ma t insts weka fil te rs Fil te r u se Fil te r insts fil te r S im p le KMe an s km e an s new S im p le KMe an s km e an s se tSeed Con ve rt ToInt 16 txtSeed Text This is the im por tan t pa ra me te r to set km e an s se tP re se r ve Ins tan cesOr de r true km e an s se tN um C lu s te rs number OfC lu s te rs km e an s bu ildC lu s te re r insts C lu s te rE va lua ti on eval new C lu s te rE va lua ti on eval se tC lu s te re r km e an s eval e va lua te C lu s te re r new Ins tan ces insts km e an s getC lu s te rCen tro ids sCon ten ts eval c lu s te rRe su ltsToS tri ng sFi le N am e D DE TAI THAC SI BoCai M an gu on IDS KDDCupOutPut txt msgS tre am MyFi le C re a te TextFi le sFi le N am e true true msgS tre am Write sCon ten ts msgS tre am Close sCon ten ts msgS tre am MyFi le O pe nTextFi le sFi le N am e Sc ri p tin g IOMo de ForRea di ng fal se Sc ri p tin g T ri s ta te T ri s ta te T ru e int i 0 s tri ng words words File ReadAll in es sFi le N am e En co di ng Def au lt for i 0 i words L eng th i i 1 s tri ng t words i Trim t Rep la ce t Rep la ce t Rep la ce t Rep la ce t Rep la ce t Rep la ce s tri ng strlv t Split Số hóa Trung tâm Học liệu ĐHTN http www lrc tnu edu vn 64 t t Rep la ce At tri bu te Thuộc tính t t Rep la ce N um be r of i te ra ti on Số lần lặp t t Rep la ce Mis sin g va lu es g lo ba l ly re p la ced with mean mode Toàn giá trị bị thay trung bình mode t t Rep la ce Full Data Dữ liệu đầy đủ t t Rep la ce C lu s te r cen tro ids Trọng tâm cụm t t Rep la ce C lu s te r Cụm t t Rep la ce Wi thin c lu s te r sum of s qua re d er ro rs Tổng bình phương lỗi cụm t t Rep la ce C lu s te re d Ins tan ces Các cụm phân if i 11 ListViewI tem lvt new ListViewI tem Số ghi for int j 0 j strlv L eng th j if strlv E le men tAt j ToS tri ng</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		http://123doc.org/document/3339212-phat-hien-xam-nhap-dua-tren-thuat-toan-kmeans.htm	
24	Những hệ thống Host-based là kiểu IDS được nghiên cứu và triển khai đầu tiên. Bằng cách cài đặt những phần mềm IDS trên các máy trạm (gọi là Agent), HIDS có	<p>Nói một cách ngắn gọn Host based IDS giám sát dữ liệu trên những máy tính riêng lẻ trong khi Network based IDS giám sát lưu thông của một hệ thống mạng</p> <p>1 2 2 1 Host based IDS HIDS Những hệ thống Host based là kiểu IDS được nghiên cứu và triển khai đầu tiên Bằng cách cài đặt những phần mềm IDS trên các máy trạm gọi là Agent HIDS có thể giám sát toàn bộ hoạt động của hệ thống các log file và lưu thông mạng đi tới từng máy trạm</p> <p>https://text.123doc.org/document/2311662-xay-dung-he-thong-phat-hien-xam-nhap-bat-thuong-voi-phan-mem-snort.htm</p>	100
25	14 thể giám sát toàn bộ hoạt động của hệ thống, các log file và lưu thông mạng đi tới từng máy trạm.	<p>Bằng cách cài đặt những phần mềm IDS trên các máy trạm gọi là agent Host based IDS có thể giám sát toàn bộ hoạt động của hệ thống các log file và lưu thông mạng đi tới từng máy trạm</p> <p>https://text.123doc.org/document/3746237-su-dung-ky-thuat-khai-pha-du-lieu-de-xay-dung-he-thong-phat-hien-xam-nhap-trai-phep.htm</p>	95
25	IDS kiểm tra lưu thông mạng đang được chuyển đến máy trạm, bảo vệ máy trạm thông qua việc ngăn chặn các gói tin nghi ngờ. HIDS có khả năng kiểm tra hoạt động đăng nhập vào máy trạm, tìm kiếm các hoạt động không bình thường như dò tìm mật khẩu, leo thang đặc quyền. Ngoài ra HIDS còn có thể giám sát sâu vào bên trong Hệ điều hành của máy trạm để kiểm tra tính toàn vẹn của nhân hệ điều hành, file lưu trữ trong hệ thống.	<p>HIDS kiểm tra lưu thông mạng đang được chuyển đến máy trạm bảo vệ máy trạm thông qua việc ngăn chặn các gói tin nghi ngờ HIDS có khả năng kiểm tra hoạt động đăng nhập vào máy trạm tìm kiếm các hoạt động không bình thường như dò tìm password leo thang đặc quyền Ngoài ra HIDS còn có thể giám sát sâu vào bên trong Hệ điều hành của máy trạm để kiểm tra tính toàn vẹn của Nhân hệ điều hành file lưu trữ trong hệ thống</p> <p>https://text.123doc.org/document/2311662-xay-dung-he-thong-phat-hien-xam-nhap-bat-thuong-voi-phan-mem-snort.htm</p>	100

Trang	Câu trùng lặp	Nguồn	Điểm
25	Hệ thống IDS có hiệu quả cao khi phát hiện việc người dùng sử dụng sai các tài nguyên trên mạng.	<p>Có khả năng kiểm tra hoạt động đăng nhập vào máy trạm tìm kiếm các hoạt động không bình thường như: người dùng password leo tường, người dùng password eo tag đặc quyền. Hệ thống IDS có hiệu quả cao khi phát hiện việc Hệ thống IDS có hiệu quả cao khi phát hiện việc người dùng sử dụng sai các tài nguyên trên mạng</p> <p>https://text.123doc.org/document/2044799-chuong-ix-he-thong-phat-hien-va-ngan-chan-xam-nhap-potx.htm</p>	100
25	Nếu người dùng cố gắng thực hiện các hành vi không hợp pháp thì những hệ thống HIDS thông thường phát hiện và tập hợp thông tin thích hợp nhất và nhanh nhất. Điểm yếu của HIDS là công kênh.	<p>Nếu người dùng cố gắng thực hiện các hành vi không hợp pháp thì những hệ thống HIDS thông thường phát hiện và tập hợp thông tin thích hợp nhất và nhanh nhất. 18 Hình 1.3 Mô hình HIDS. Lợi thế của HIDS. Có khả năng xác định user liên quan tới một event HIDS có khả năng phát hiện các cuộc tấn công diễn ra trên một máy NIDS không có khả năng này. Có thể phân tích các dữ liệu mã hoá. Cung cấp các thông tin về host trong lúc cuộc tấn công diễn ra trên host này. Hạn chế của HIDS. Điểm yếu của HIDS là công kênh.</p> <p>https://text.123doc.org/document/3746237-su-dung-ky-thuat-khai-pha-du-lieu-de-xay-dung-he-thong-phat-hien-xam-nhap-trai-phep.htm</p>	100
25	Với vài ngàn máy trạm trên một mạng lớn, việc thu thập và tập hợp các thông tin máy tính đặc biệt riêng biệt cho mỗi máy riêng lẻ là không có hiệu quả.	<p>Với vài ngàn máy trạm trên một mạng lớn, việc thu thập và tập hợp các thông tin máy tính đặc biệt riêng biệt cho mỗi máy riêng lẻ là không có hiệu quả.</p> <p>https://text.123doc.org/document/2311662-xay-dung-he-thong-phat-hien-xam-nhap-bat-thuong-voi-phan-mem-snort.htm</p>	100
25	Ngoài ra, nếu thủ phạm vô hiệu hóa việc thu thập dữ liệu trên máy tính thì HIDS trên máy đó sẽ không còn có ý nghĩa.	Ngoài ra, nếu thủ phạm vô hiệu hóa việc thu thập dữ liệu trên máy tính thì HIDS trên máy đó sẽ không còn có ý nghĩa.	100

Trang	Câu trùng lặp	Nguồn	Điểm
		https://text.123doc.org/document/4250633-luan-van-xay-dung-he-thong-phat-hien-xam-nhap-bang-phan-mem-snort.htm	
25	Phát hiện xâm nhập dựa trên dấu hiệu và dựa trên bất thường.	<p>Phát hiện xâm nhập trái phép tiếp cận bằng quyền g pháp học máy Ma chi ne Lear ni ng Ap pro ach Hệ thống phát hiện xâm nhập dựa trên bất thường có 2 ưu điểm chính so với hệ thống dựa trên dấu hiệu</p> <p>https://text.123doc.org/document/4020963-nghien-cuu-cac-phuong-phap-hoc-may-va-ung-dung-trong-phat-hien-xam-nhap-trai-phep.htm</p>	78
25	1.2.3.1. Phát hiện xâm nhập dựa trên dấu hiệu	<p>Tác giả N gu yễn Thị Thu Hiền 4 Danh mục các ký hiệu các chữ viết tắt 1 Từ Tiếng Anh viết tắt ID In tru si on De te c ti on Phát hiện xâm nhập 2 IDS In tru si on De te c ti on Sys tem Hệ thống phát hiện xâm nhập 3 NIDS Network based IDS Hệ thống phát hiện xâm nhập dựa STT Tiếng Việt trên mạng 4 HIDS Host based IDS Hệ thống phát hiện xâm nhập dựa trên host 5 DoS De nia I Of Ser vi ce Tấn công từ chối dịch vụ 6 DDoS Dis tri bu te d De nia I Of Ser vi ce Tấn công từ chối dịch vụ phân tán 7 SBIDS Sig na tu re Based IDS Hệ thống phát hiện xâm nhập dựa trên dấu hiệu 8 ABIDS A no ma ly Based IDS Hệ thống phát hiện xâm nhập dựa trên bất thường 9 CUSUM C um u la ti ve SUM 10 KPD L Thuật toán cộng tích lũy Data min in g Khai phá dữ liệu 11 ADAM Audit Data A na ly si s and M in in g Khai phá và phân tích dữ liệu kiểm toán 12 SOM Self Or ga ni z in g Maps 13 ICMP In te r ne t 14 TCP Con tro l Bản đồ tự tổ chức Mes sa ge Giao thức thông điệp điều khiển P ro to co l In te r ne t T ran s miss ion C om u ni ca ti on Giao thức điều khiển truyền vận P ro to co l 15 UDP User Da ta g ram P ro to co l Giao thức không liên kết 16 SFD SYN F lo o di ng de te c ti on Phát hiện tấn công SYN f lo o di ng 5 Danh mục các bảng Bảng 3 1</p>	71

Trang	Câu trùng lặp	Nguồn	Điểm
		https://text.123doc.org/document/4327911-nghien-cuu-thu-nghiem-cac-phuong-phap-phat-hien-xam-nhap-trai-phiep-dua-tren-phat-hien-bat-thuong.htm	
25	Phát hiện xâm nhập dựa trên dấu hiệu của hành vi xâm nhập (Signature-based	<p>Phân loại IDS theo phạm vi gia m sa t Networ based IDS NIDS Là những IDS giám sát trên toàn bộ mạng Host based IDS HIDS Là những IDS giám sát hoạt động của từng máy tính riêng biệt Phân loại IDS theo kỹ thuật thực hiện Sig na tu re based IDS phát hiện xâm nhập dựa trên dấu hiệu của hành vi xâm nhập A no ma ly based IDS phát hiện xâm nhập bằng cách so sánh các hành vi hiện 11 2 0</p> <p>Slide báo cáo.pdf</p>	89
25	Kỹ thuật này đòi hỏi phải duy trì một cơ sở dữ liệu về các dấu hiệu xâm nhập (signature database), và cơ sở dữ liệu này phải được cập nhật thường xuyên mỗi khi có một hình thức hoặc kỹ thuật xâm nhập mới.	<p>Kỹ thuật này đòi hỏi phải duy trì một cơ sở dữ liệu về các dấu hiệu xâm nhập si g na tu re đa ta ba se và cơ sở dữ liệu này phải được cập nhật thường xuyên mỗi khi có một hình thức hoặc kỹ thuật xâm nhập mới</p> <p>https://viblo.asia:443/p/tim-hieu-ve-he-thong-phat-hien-xam-nhap-ossec-phan-i-m68Z03JzKkG</p>	100
25	Signature-based IDS là hệ sử dụng định nghĩa trừu tượng để mô tả về tấn công gọi là dấu hiệu.	<p>Hình 1 8 K no w le dge based IDS 16 1 2 2 3 2 Sig na tu re based IDS Sig na tu re based IDS là hệ sử dụng định nghĩa trừu tượng để mô tả về tấn công gọi là dấu hiệu</p> <p>https://text.123doc.org/document/3969147-luan-van-xay-dung-he-thong-phat-hien-xam-nhap-bang-phan-mem-snort.htm</p>	100

Trang	Câu trùng lặp	Nguồn	Điểm
25	Dấu hiệu bao gồm một nhóm các thông tin cần thiết để mô tả kiểu tấn công. Ví dụ như hệ thống mạng IDS có thể lưu trữ trong cơ sở dữ liệu nội dung 15 các gói tin có liên quan đến kiểu tấn công đã biết. Thường thì dấu hiệu được lưu ở dạng cho phép so sánh trực tiếp với thông tin có trong chuỗi sự kiện.	Dấu hiệu bao gồm một nhóm các thông tin cần thiết để mô tả kiểu tấn công Ví dụ như hệ thống mạng IDS có thể lưu trữ trong cơ sở dữ liệu nội dung các gói tin có liên quan đến kiểu tấn công đã biết Ví dụ như hệ thống mạng IDS có thể lưu trữ trong cơ sở dữ liệu nội dung các gói tin có liên quan đến kiểu tấn công đã biết Thường thì dấu hiệu được lưu ở dạng cho phép so sánh trực tiếp với thông tin có trong chuỗi sự kiện	100
		https://text.123doc.org/document/4229276-thiet-bi-an-ninh-mang.htm	
26	Trong quá trình xử lý, sự kiện được so sánh với các mục trong file dấu hiệu, nếu thấy có sự giống nhau thì hệ tạo ra cảnh báo. Signature-based IDS hiện nay rất thông dụng vì chúng dễ phát triển, cho phản hồi chính xác về cảnh báo và thường yêu cầu ít tài nguyên tính toán.	Trong quá trình xử lý sự kiện được so sánh với các mục trong file dấu hiệu nếu thấy có sự giống nhau thì hệ tạo ra cảnh báo Signature-based IDS hiện nay rất thông dụng vì chúng dễ phát triển cho phản hồi chính xác về cảnh báo và thường yêu cầu ít tài nguyên tính toán	100
		https://text.123doc.org/document/2311662-xay-dung-he-thong-phat-hien-xam-nhap-bat-thuong-voi-phan-mem-snort.htm	
26	Tuy nhiên, chúng có những điểm yếu sau:- Mô tả về cuộc tấn công thường ở mức độ thấp, khó hiểu.	Tuy nhiên chúng có những điểm yếu sau Mô tả về cuộc tấn công thường ở mức độ thấp khó hiểu Mỗi cuộc tấn công hay biến thể của nó đều cần thêm dấu hiệu đưa vào cơ sở dữ liệu nên kích cỡ của nó sẽ trở nên rất lớn Dấu hiệu càng cụ thể thì càng tạo ra ít cảnh báo nhầm nhưng càng khó phát hiện những biến thể của nó	100
		https://text.123doc.org/document/4229276-thiet-bi-an-ninh-mang.htm	
26	- Mỗi cuộc tấn công hay biến thể của nó đều cần thêm dấu hiệu đưa vào cơ sở dữ liệu, nên kích cỡ của nó sẽ trở nên rất lớn.	Mỗi cuộc tấn công hay biến thể của nó đều cần thêm dấu hiệu đưa vào cơ sở dữ liệu nên kích cỡ của nó sẽ trở nên rất lớn	100
		https://text.123doc.org/document/2426413-ung-dung-ban-do-tu-to-chuc-som-self-organizing-map-phat-hien-phat-tan-virus-may-tinh-qua-hanh-vi.htm	

Trang	Câu trùng lặp	Nguồn	Điểm
26	- Dấu hiệu càng cụ thể, thì càng tạo ra ít cảnh báo nhầm, nhưng càng khó phát hiện những biến thể của nó.	Tuy nhiên chúng có những điểm yếu sau Mô tả về cuộc tấn công thường ở mức độ thấp khó hiểu Mỗi cuộc tấn công hay biến thể của nó đều cần thêm dấu hiệu đưa vào cơ sở dữ liệu nên kích cỡ của nó sẽ trở nên rất lớn Dấu hiệu càng cụ thể thì càng tạo ra ít cảnh báo nhầm nhưng càng khó phát hiện những biến thể của nó	100
		https://text.123doc.org/document/4229276-thiet-bi-an-ninh-mang.htm	

Trang	Câu trùng lặp	Nguồn	Điểm
	1.2.3.2. Phát hiện xâm nhập dựa trên bất thường	<p>Thuật toán One class SVM PHỤ LỤC 02 CÔNG TRÌNH KHOA HỌC ĐÃ CÔNG BỐ 75 75 78 82 83 vì DANH MỤC CÁC KÝ HIỆU CÁC CHỮ VIẾT TẮT Viết tắt Thuật ngữ Ý nghĩa Bộ dữ liệu nghiên cứu phát hiện xâm nhập trái phép DARPA Defense Advanced Research Projects Agency Mỹ Bộ dữ liệu nghiên cứu phát hiện xâm nhập trái phép của DARPA Hệ thống phát hiện xâm nhập trái phép trên HIDS Network Based IDS máy chủ IDS Intranet Detection System Hệ thống phát hiện xâm nhập trái phép ISCX Information Security Center Trung tâm nghiên cứu về an toàn thông tin của Center of Excellence trường đại học New Brunswick Bộ dữ liệu nghiên cứu phát hiện xâm nhập trái ISCX Data set phép của ISCX KNN K-Nearest Neighbor Thuật toán học máy K láng giềng gần nhất ML Machine Learning Học máy Định dạng dữ liệu được thu thập qua việc bắt Netflow giữ gói tin ở dạng Flow Hệ thống phát hiện xâm nhập trái phép trên NIDS Network Based IDS mạng SVM Support Vector Machine Thuật toán học máy Máy hỗ trợ Vector Định dạng dữ liệu được thu thập qua việc bắt Tcpdump giữ gói tin ở dạng Packet Phần mềm học máy của trường đại học Weka Waitakere Data set vì DANH SÁCH BẢNG Bảng 3 1 Các nhóm xâm nhập trái phép trong dữ liệu DARPA 46 Bảng 3 2 Bộ dữ liệu ISCX 47 Bảng 3 3 Các thông số cơ bản của bộ dữ liệu Netflow máy chủ Pasca 50 Bảng 3 4 Số lượng tấn công từ từng máy chủ tới máy chủ Pasca 51 Bảng 3 5 Số lượng tấn công theo các cổng đích tới máy chủ Pasca 51 Bảng 3 6 Các thông số cơ bản của bộ dữ liệu ISCX Netflow 52 Bảng 3 7 Số lượng tấn công theo các cổng đích với bộ dữ liệu ISCX 52 Bảng 3 8 Các đặc trưng lựa chọn trong phát hiện xâm nhập trái phép 53 Bảng 3 9 Thông tin bộ dữ liệu thử nghiệm DARPA Netflow máy chủ Pasca 53 Bảng 3 10 Thông tin bộ dữ liệu thử nghiệm ISCX Netflow ngày 14 6 53 Bảng 3 11 Confusion Matrix</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>55 Bảng 3 12 Đánh giá kết quả thử nghiệm với bộ dữ liệu DARPA Netf lo w</p> <p>57 Bảng 3 13 Đánh giá kết quả thử nghiệm với bộ dữ liệu ISCX Netf lo w 58</p> <p>viii DANH SÁCH HÌNH VẼ Hình 1 1 Dữ liệu cần phân lớp 8 Hình 1 2 Minh họa biên của một cách phân lớp 8 Hình 1 3 Minh họa biên cực đại của bài toán phân lớp 9 Hình 1 4 Mặt phẳng phân tách theo các giá trị ve c to r pháp tuyến và ngưỡng 10 Hình 1 5 Minh họa độ rộng của biên 11 Hình 1 6 Minh họa đường viền của biên 12 Hình 1 7 Ví dụ bài toán phân loại tuyến tính không tách biệt 16</p> <p>Hình 1 8 Các điểm lỗi của dữ liệu 17</p> <p>Hình 1 9 Ảnh hưởng của tham số C đến bài toán phân lớp 17 Hình 1 10 C huy ển đổi không gian biểu diễn 20 Hình 1 11 Không gian đầu vào 21 Hình 1 12 Không gian đặc trưng 21 Hình 1 13 Hình K láng giềng gần nhất 24 Hình 2 1 Các thành phần của hệ thống IPS 32 Hình 2 2 Hệ thống Network based IDS NIDS 34 Hình 2 3 Hệ thống Host based IDS HIDS 36</p> <p>Hình 2 4 Hệ thống Mi su se De te c ti on 37</p> <p>Hình 2 5 Hệ thống A no ma ly De te c ti on 38</p> <p>Hình 2 6 Kiến trúc của hệ thống phát hiện xâm nhập dựa trên bất thường 40</p> <p>Hình 3 1 Mô hình kiểm thử với thuật toán học máy có giám sát 44</p> <p>Hình 3 2 Mô hình kiểm thử với thuật toán học máy không có giám sát 45</p> <p>Hình 3 3 Sơ đồ chuyển đổi dữ liệu 48</p> <p>Hình 3 4 Ví dụ minh họa về đường ROC 56</p> <p>Hình 3 5 So sánh độ chính xác AC của các thuật toán học máy với bộ dữ liệu DARPA Netf lo w 57</p> <p>Hình 3 6 So sánh độ chính xác AC của các thuật toán học máy với bộ dữ liệu ISCX Netf lo w 58</p> <p>Hình 0 1 Chuẩn hóa dữ liệu P ro to co l DARPA Netf lo w với Disc re ti ze 63</p> <p>Hình 0 2 Chuẩn hóa dữ liệu Pac ke t DARPA Netf lo w với Disc re ti ze 63</p> <p>Hình 0 3 Chuẩn hóa dữ liệu Octet DARPA Netf lo w với Disc re ti ze 64</p> <p>Hình 0 4 Chuẩn hóa dữ liệu P ro to co l DARPA Netf lo w với Nor ma li ze 64</p> <p>Hình 0 5 Chuẩn hóa dữ liệu Pac ke ts DARPA Netf lo w với Nor ma li ze 65</p> <p>Hình 0 6 Chuẩn hóa dữ liệu Oc te ts DARPA Netf lo w với Nor ma li ze 65</p> <p>Hình 0 7 Chuẩn hóa dữ liệu P ro to co l</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>ISCX Netf lo w với Disc re ti ze 66 Hình 0 8 Chuẩn hóa dữ liệu Pac ke t ISCX Netf lo w với Disc re ti ze 66 Hình 0 9 Chuẩn hóa dữ liệu Octet ISCX Netf lo w với Disc re ti ze 67 Hình 0 10 Chuẩn hóa dữ liệu P ro to co l ISCX Netf lo w với Nor ma li ze 67 ix Hình 0 11 Chuẩn hóa dữ liệu Pac ke ts ISCX Netf lo w với Nor ma li ze 68 Hình 0 12 Chuẩn hóa dữ liệu Oc te ts ISCX Netf lo w với Nor ma li ze 68 Hình 0 13 ROC của thuật toán K NN với K 1 với bộ dữ liệu DARPA Netf lo w 69 Hình 0 14 ROC của thuật toán K NN với K 4 với bộ dữ liệu DARPA Netf lo w 70 Hình 0 15 ROC của thuật toán SVM L in ear với bộ dữ liệu DARPA Netf lo w 71 Hình 0 16 ROC của thuật toán SVM Po ly no mi na l với bộ dữ liệu DARPA Netf lo w 72 Hình 0 17 ROC của thuật toán SVM RBF với bộ dữ liệu DARPA Netf lo w 73 Hình 0 18 ROC của thuật toán SVM Sig moi d với bộ dữ liệu DARPA Netf lo w 74 Hình 0 19 Kết quả phân loại với thuật toán One class SVM với bộ dữ liệu DARPA Netf lo w 75 Hình 0 20 ROC của thuật toán K NN với K 1 với bộ dữ liệu ISCX Netf lo w 75 Hình 0 21 ROC của thuật toán K NN với K 4 với bộ dữ liệu ISCX Netf lo w 77 Hình 0 22 ROC của thuật toán SVM L in ear với bộ dữ liệu ISCX Netf lo w 78 Hình 0 23 ROC của thuật toán SVM Po ly no mi na l với bộ dữ liệu ISCX Netf lo w 79 Hình 0 24 ROC của thuật toán SVM RBF với bộ dữ liệu ISCX Netf lo w 80 Hình 0 25 ROC của thuật toán SVM Sig moi d với bộ dữ liệu ISCX Netf lo w 81 Hình 0 26 Kết quả phân loại với thuật toán One class SVM với bộ dữ liệu ISCX Netf lo w 82 MỞ ĐẦU 1</p> <p>https://text.123doc.org/document/4020962-nghien-cuu-cac-phuong-phap-hoc-may-va-ung-dung-trong-phat-hien-xam-nhap-trai-phep.htm</p>	
26	Thường là cách so sánh các hành vi hiện tại với hoạt động bình thường của hệ thống để phát hiện các bất thường (anomaly) có thể là dấu hiệu của xâm nhập.	phát hiện xâm nhập bằng cách so sánh mang tính thống kê các hành vi hiện tại với hoạt động bình thường của hệ thống để phát hiện các bất thường an om a ly có thể là dấu hiệu của xâm nhập	89

Trang	Câu trùng lặp	Nguồn	Điểm
		https://viblo.asia/p/tim-hieu-ve-he-thong-phat-hien-xam-nhap-ossec-phan-i-m68Z03JzKkG	

Trang	Câu trùng lặp	Nguồn	Điểm
27	Chương này cung cấp một cái nhìn tổng quan về xâm nhập và phát hiện xâm nhập.	<p>Các công cụ dò quét được 4 dạng 3</p> <p>Cách phát hiện Phát hiện bằng các pro fi le bất thường hoặc sự vi phạm chính sách an ninh Phát hiện bằng các pro fi le bất thường hoặc sự vi phạm các chính sách an ninh Thâm nhập vào hệ thống Phát hiện bằng cách giám sát một số hành vi điều khiển 4 Rò rỉ thông tin 5 Tấn công từ chối dịch vụ 6 Mã độc hại đặc biệt Phát hiện bằng cách giám sát việc sử dụng tài nguyên bất thường Phát hiện bằng cách giám sát khó khăn đối với một hệ thống mạng lớn nhiều dịch vụ trong khi các cuộc tấn công ngày càng đa dạng hơn Để khắc phục điểm yếu này người ta sử dụng một kỹ thuật phát hiện xâm nhập mới là Kỹ thuật dựa trên bất thường 21 CHƯƠNG 2 HỆ THỐNG IDS DỰA TRÊN PHÁT HIỆN BẤT THƯỜNG</p> <p>Hệ thống phát hiện bất thường giống các hệ thống IDS truyền thống ở chỗ nó cũng hướng đến việc kiểm soát và phát hiện sớm các dấu hiệu sự kiện được phát hiện bởi các Sen so r trong một cơ sở dữ liệu và sử dụng một hệ thống các luật để đưa ra các cảnh báo trên các sự kiện an ninh nhận được cho hệ thống hoặc cho người quản trị A le rts Con so le T ra ffic Network Sen so r En gi ne Hình 1 4</p> <p>Thành phần của một hệ thống IDS 10</p> <p>Như vậy hệ thống IDS hoạt động theo cơ chế phát hiện và cảnh báo Các Sen so r là bộ phận được bố trí trên hệ thống tại những cửa áp dụng vào Hệ thống phát hiện xâm nhập trái phép Ưu điểm vượt trội của phương pháp này là khả năng xử lý khối lượng dữ liệu lớn có thể phục vụ cho các hệ thống thời gian thực Hệ thống IDS sử dụng KPD L cũng được chia theo 2 hướng chính là phát hiện dựa trên hành vi lạm dụng và phát hiện bất thường Trong hướng phát hiện dựa trên hành vi lạm dụng các mẫu trong tập dữ liệu được gán nhãn là bình dụng tài nguyên bất thường Phát hiện các hành vi bất thường vi phạm chính sách an ninh sử dụng các đặc quyền bất thường 2 4</p> <p>Dữ liệu phát hiện bất thường Nguồn dữ liệu đóng vai trò quan trọng trong phương pháp phát hiện bất thường Số liệu chính xác về tình trạng hoạt động</p>	77

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>của mạng sẽ có tính chất quyết định đến việc các bất thường có được phát hiện hay không Do bản chất của phương pháp phát hiện bất này cung cấp một cái nhìn tổng quan về Hệ thống phát hiện xâm nhập trái phép IDS Trước tình hình mất an toàn an ninh mạng ngày càng gia tăng đòi hỏi các hệ thống máy tính phải có một chiến lược phòng thủ theo chiều sâu nhiều lớp Hệ thống IDS là một sự bổ sung cần thiết cho các thiết bị Firewall có chức năng phát hiện và cảnh báo trước các dấu hiệu tấn công lên hệ thống mạng giúp cho người quản trị chủ</p> <p>http://123doc.org/document/1080878-tai-lieu-luan-van-xay-dung-he-thong-phat-hien-xam-nhap-bang-phan-mem-snort-pot.htm?pageh=1</p>	
28	CÁC HỆ THỐNG PHÁT HIỆN XÂM NHẬP	<p>Các hệ thống có nhiệm vụ như vậy được gọi là hệ thống phát hiện xâm nhập 1 3 1</p> <p>https://text.123doc.org/document/4729605-dspace-at-vnu-danh-gia-hieu-qua-mot-so-thuat-toan-trong-phat-hien-xam-nhap-mang.htm</p>	100
28	Trong chương này sẽ cho chúng ta cái nhìn tổng quan về IDS bao gồm cả những điểm mạnh và điểm yếu của chúng.	<p>Trong chương này sẽ cho chúng ta cái nhìn tổng quan về IDS bao gồm cả những điểm mạnh và điểm yếu của chúng</p> <p>http://123doc.org/document/4960-he-thong-phat-hien-xam-nhap.htm</p>	100
28	Chúng ta sẽ đề cập đến cả Network IDS và cả Host IDS.	<p>Chúng ta sẽ đề cập đến cả network IDS nhiều khi được đề cập đến như sniffer và cả host IDS phân tích log kiểm tra tích hợp và nhiều thứ khác</p> <p>https://text.123doc.org/document/1024285-tai-lieu-he-thong-phat-hien-xam-nhap-idss-doc.htm</p>	87

Trang	Câu trùng lặp	Nguồn	Điểm
28	Sự khác nhau chủ yếu giữa NIDS và HIDS đó là dữ liệu mà nó tìm kiếm.	<p>NFR HID In truder Alert Sinh viên thực hiện Hoàng Thanh Tùng Lớp Tru yền thông và mạng máy tính 18 N ghi ên cứu và triển khai hệ thống phát hiện xâm nhập mạng Hình 1 8 Mô hình HIDS 3 Hybrid IDS Sự khác nhau chủ yếu giữa NIDS và HIDS đó là dữ liệu mà nó tìm kiếm NIDS nhìn vào toàn cảnh các chuyển dịch trên mạng trong khi host IDS thì quan sát các host hệ điều hành và các ứng dụng Vậy những thuận tiện đường truyền những mạng ảo và những sự rắc rối khác Thêm vào đó là sự mã hoá phân tích dữ liệu cũng làm cho quá trình hoạt động của IDS bị cản trở Bởi vậy như trên đã nói IDS hiện nay và trong tương lai thường được giám sát dựa trên một host cố định Sinh viên thực hiện Hoàng Thanh Tùng Lớp Tru yền thông và mạng máy tính 23 N ghi ên cứu và triển khai hệ thống phát hiện xâm nhập mạng 4 Hiện thị dữ Xem thêm Xem thêm NGHIÊN cứu và TRIỂN KHAI hệ THỐNG PHÁT HIỆN xâm NHẬP MẠNG NGHIÊN cứu và TRIỂN KHAI hệ THỐNG PHÁT HIỆN xâm NHẬP MẠNG NGHIÊN cứu và TRIỂN KHAI hệ THỐNG PHÁT HIỆN xâm NHẬP MẠNG</p> <p>Bình luận về tài liệu nghi en cuu va trien khai he thong phat hien xam nhap mang Tài liệu mới đăng Đề thi môn toán lớp 10 chuyên HẢI DƯƠNG năm 2012 1 41 0 Đề thi môn toán lớp 10 chuyên HÒA BÌNH năm 2012 1 17 0 Đề thi môn toán lớp 10 chuyên NGHỆ AN năm 2012 1 28 0 Đáp án đề thi môn toán lớp 10 chuyên TÂY NINH năm 2012 1 20 0 Đáp án đề thi môn toán lớp 10 chuyên VĨNH PHÚC năm 2012 1 21 0 Đề thi vào lớp 10 môn toán tỉnh Quảng Trị năm 2012 1 17 0 Đáp án đề thi môn toán lớp 10 chuyên phổ thông năng khiếu tp Hồ chí minh năm 2012 1 23 0 Đề thi vào lớp 10 môn toán tỉnh Cần Thơ năm 2012 1 27 0 Tài liệu mới bán Tập đề thi chọn học sinh giỏi lớp 9 môn lịch sử kèm đáp án chi tiết 95 0 0 Tập đề thi chọn học sinh giỏi lớp 9 môn tiếng anh kèm đáp án chi tiết 107 0 0 Tập đề thi chọn học sinh giỏi lớp 9 môn sinh kèm đáp án chi tiết 94 0 0 Tập đề thi chọn học sinh giỏi lớp 9 môn ngữ văn</p>	100

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>kèm đáp án chi tiết 77 0 0 Đề xuất các giải pháp để nâng cao chất lượng và thời hạn các công trình do Công ty 208 thực hiện 119 0 0 Tập đề thi chọn học sinh giỏi lớp 9 môn toán kèm đáp án chi tiết 70 0 0 NỘI DUNG ôn THI CUỐI kỳ môn học tư TƯỞNG hồ CHÍ MINH 32 0 0 ĐỀ CƯƠNG NGUYÊN lý 1 THẾ GIỚI QUAN và PHƯƠNG PHÁP LUẬN TRIẾT học của CHỦ NGHĨA mác LÊNIN 30 0 0 Mục lục 1</p> <p>http://123doc.org/document/976012-nghien-cuu-va-trien-khai-he-thong-phat-hien-xam-nhap-mang.htm?page=7</p>	
28	2.1. Các hệ thống phát hiện xâm nhập mạng	<p>Biên Hòa ngày 20 tháng 12 năm 2012 Học viên N gu yển Quốc Doanh MỤC LỤC LỜI CẢM ƠN LỜI CAM ĐOAN DANH MỤC CÁC TỪ VIẾT TẮT DANH MỤC CÁC HÌNH Trang CHƯƠNG 1 MỞ ĐẦU 1 1 1 Giới thiệu đề tài 1 1 1 1 Lý do chọn đề tài 1 1 1 2 Mục tiêu của đề tài 2 1 1 3 Các giai đoạn thực hiện đề tài 3 1 2 Đối tượng phạm vi nghiên cứu của đề tài 3 1 2 1 Các hệ học 3 1 2 2 Học giám sát 4 1 2 3 Học không giám sát 4 1 2 4 Bản đồ tự tổ chức SOM 5 1 2 3 Sâu máy tính và các hệ thống đích 5 1 3 Cấu trúc chung luận luận văn 6 1 4 Ý nghĩa thực tiễn của đề tài 7 CHƯƠNG 2 TÌM HIỂU HỆ THỐNG PHÁT HIỆN XÂM NHẬP 9 2 1 Khái niệm 9 2 2 Các thành phần và chức năng của IDS 9 2 2 1 Thành phần thu thập gói tin 11 2 2 2 Thành phần phát hiện gói tin 11 2 2 3 Thành phần phản hồi 11 2 3 Phân loại IDS 12 2 3 1 Network Base IDS NIDS 12 2 3 2 Host Based IDS HIDS 13 2 4 Hệ thống phát hiện xâm nhập theo dấu hiệu cho trước Misuse based IDS và hệ thống phát hiện xâm nhập bất thường Anomaly based IDS 14 2 4 1 Misuse based system 14 2 4 2 Anomaly based system 15 2 5 Phân loại các dấu hiệu 16 2 5 1 Phát hiện dấu hiệu bất thường 16 2 5 2 Các mẫu hành vi thông thường phát hiện bất thường 16 2 5 3 Các dấu hiệu có hành vi bất thường phát hiện dấu hiệu 17 CHƯƠNG 3 BẢN ĐỒ TỰ TỔ CHỨC 20 3 1</p>	88

Trang	Câu trùng lặp	Nguồn	Điểm
		https://text.123doc.org/document/2424986-luan-van-thac-si-cong-nghe-thong-tin-ung-dung-ban-do-tu-to-chuc-som-self-organizing-map-phat-hien-phat-tan-virus-may-tinh-qua-hanh-vi.htm	
28	Ngoài ra còn có nhiều chương trình thêm vào để cung cấp những cách khác nhau nhằm mục đích ghi dấu và quản lý logfile của Snort, thêm và bảo trì tập luật, thông báo cho người quản trị hệ thống khi có những traffic gây hại được nhận ra...Có nhiều cách để sử dụng Snort trong thiết kế bảo mật của công ty.	Ngoài ra còn có nhiều chương trình thêm vào để cung cấp những cách khác nhau nhằm mục đích ghi dấu và quản lý logfile của Snort thêm và bảo trì tập luật thông báo cho người quản trị hệ thống khi có những traffic gây hại được nhận ra Có nhiều cách để sử dụng Snort trong thiết kế bảo mật của công ty 44 Thông thường Snort chỉ sử dụng TCP IP nhưng những phần thêm vào có thể mở rộng khả năng cung cấp các loại ngôn ngữ khác như No ve II IPX	100
		Do Thanh Hung_K47CA_M.TTMT.pdf	
28	Thông thường Snort chỉ sử dụng TCP/IP nhưng những phần thêm vào có thể mở rộng khả năng cung cấp các loại ngôn ngữ khác .	Thông thường Snort chỉ sử dụng TCP IP nhưng những phần thêm vào có thể mở rộng khả năng cung cấp các loại ngôn ngữ khác như No ve II IPX	100
		Do Thanh Hung_K47CA_M.TTMT.pdf	

Trang	Câu trùng lặp	Nguồn	Điểm
29	2.1.1.2. Thành phần và chức năng	<p> nbsp N ghi ên cứu lựa chọn đơn pha chế hợp lý của hệ ul tra d ri l khi khoan qua tầng sét hoạt tính Báo cáo thực tập tốt nghiệp Trang 1 MỤC LỤC LỜI CẢM ƠN 3 MỞ ĐẦU 4 DANH MỤC CÁC HÌNH VẼ TRONG ĐỒ ÁN 5 DANH MỤC CÁC BẢNG BIỂU TRONG ĐỒ ÁN 6 BẢNG QUY ĐỔI ĐƠN VỊ SỬ DỤNG TRONG ĐỒ ÁN 6 CHƯƠNG 1 TỔNG QUAN VỀ DUNG DỊCH KHOAN 8 1 1 Khái niệm và chức năng của dung dịch khoan 8 1 1 1 Khái niệm 8 1 1 2 Chức năng 8 1 1 2 1 Làm sạch đáy và vận chuyển mùn khoan 8 1 1 2 2 Giữ mùn khoan lơ lửng khi ngừng tuần hoàn 9 1 1 2 3 Làm mát bôi trơn bộ dụng cụ khoan 10 1 1 2 4 Tạo phản áp giữ ổn định thành giếng khoan tránh hiện tượng dầu khí nước vào giếng khoan 11 1 1 2 5 Sét hóa thành giếng khoan 11 1 1 2 6 T ru yền năng lượng cho tua bin khoan 12 1 1 2 7 Các chức năng khác 13 1 2 Các tính chất của dung dịch khoan 13 1 2 1 Trọng lượng riêng γ 13 1 2 2 Độ thải nước B 14 1 2 3 Độ nhớt phổ T 14 1 2 4 Độ nhớt dẻo PV 14 1 2 5 Lực cắt động YP 14 1 2 6 Lực cắt tĩnh θ 15 1 2 7 Nồng độ pha rắn Π 15 1 2 8 Độ pH 15 1 3 Thành phần và phân loại 15 1 3 1 Thành phần 15 1 3 2 Phân loại 17 1 4 Các phương pháp tuần hoàn dung dịch 18 1 4 1 Tuần hoàn thuận 19 Báo cáo thực tập tốt nghiệp Trang 2 1 4 2 Tuần hoàn nghịch 19 1 4 3 Tuần hoàn cục bộ 20 1 5 Gia công hóa học dung dịch khoan 20 1 5 1 Mục đích của gia công hóa học 20 1 5 2 Một số hóa phẩm điển hình trong gia công hóa học dung dịch khoan 20 2 1 Đặc điểm địa chất Việt nam 22 2 1 1 Mối liên hệ chung nhất giữa điều kiện địa chất và thiết kế hệ dung dịch khoan 22 CHƯƠNG 3 ĐẶC ĐIỂM CÁC HỆ DUNG DỊCH SỬ DỤNG RỘNG RÃI HIỆN NAY 30 3 1 Các hệ dung dịch thường sử dụng 30 CHƯƠNG 4 NGHIÊN CỨU LỰA CHỌN ĐƠN PHA CHẾ HỢP LÝ CỦA HỆ ULTRADRIL 34 4 1 Giới thiệu chung về hệ ul tra d ri l 34 4 1 1 Mô tả chung 34 4 1 2 Thành phần hệ và chức năng của các chất trong hệ 38 4 2 N ghi ên cứu lựa chọn đơn pha chế hợp lý của hệ Ul tra d ri l 39 4 2 1 Nhiệm </p>	93

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>vụ và phương pháp nghiên cứu cách pha chế một mẫu dung dịch khoan 39 4 2 2 Cách xác định và tính toán các thông số 41 4 2 2 1 Các thông số lưu biến 41 4 2 2 2 Độ thải nước ở điều kiện thường 42 4 2 2 3 Độ thải nước ở điều kiện nhiệt độ cao áp suất cao 44 4 2 2 4 Độ PH 46 4 2 3 Kết quả thí nghiệm 47 4 2 3 1 Kết quả đo độ thải nước ở điều kiện thường 55 4 2 3 2 Đo độ thải nước ở điều kiện nhiệt độ cao áp suất cao 56 4 2 3 3 Đo tính chất lưu biến của các đơn pha chế 57 4 2 4 Lựa chọn đơn pha chế hợp lý 60 KẾT LUẬN 61 TÀI LIỆU THAM KHẢO 62 Báo cáo thực tập tốt nghiệp Trang 3 LỜI CẢM ƠN Em xin g i l i c n Bà R ban ch nhi m khoa Hóa và Công Ngh Th c Ph m o công ty TNHH Dung d ch khoan và d ch v gi ng khoan DMC WS u ki n t t nh t cho em c th c t p và án t t nghi p</p> <p>https://text.123doc.org/document/2980725-nghien-cuu-lua-chon-don-pha-che-hop-ly-cua-he-ultradril-khi-khoan-qua-tang-set-hoat-tinh.htm</p>	
29	Hình 2.1: Mô tả sơ đồ của Snort	<p>Hình 2 1 mô tả sơ đồ của một hệ thống máy đo thể 2 1 2</p> <p>https://text.123doc.org/document/4394195-phuong-phap-phan-tich-dien-hoa-va-ung-dung.htm</p>	87
29	Snort có 5 thành phần chính như sau:- Bộ giải mã gói tin - Packet Decoder	<p>Snort hỗ trợ khả năng hoạt động trên các giao thức sau E the r ne t 802 11 Token Ring FDDI Cisco HDLC SLIP PPP và PF của O pe nBSD 2 Kiến trúc của Snort Snort có 5 thành phần chính như sau Bộ giải mã gói tin Pac ke t De co de r Các bộ tiền xử lý P re P ro ces se rs Máy phát hiện De te c ti on En gi ne Hệ thống cảnh báo và ghi dấu Log gin g and A le r tin g Sys tem Mô đun xuất Output Mo du le s Sơ đồ sau biểu diễn quan hệ giữa các thành phần của Snort</p> <p>https://text.123doc.org/document/3374292-cac-he-thong-phat-hien-xam-nhap-dua-tren-dau-hieu.htm</p>	100

Trang	Câu trùng lặp	Nguồn	Điểm
29	Các gói dữ liệu đi vào qua các cổng giao tiếp mạng, các cổng giao tiếp này có thể là: Ethernet, SLIP, PPP...	Một Snort IDS cơ bản gồm các thành phần chính sau 2 AN TOÀN ỨNG DỤNG WEB VÀ CƠ SỞ DỮ LIỆU NHÓM 2 Các thành phần chính của Snort IDS Pac ke t De co de r bộ phận giải mã gói tin Các gói dữ liệu đi vào qua các cổng giao tiếp mạng các cổng giao tiếp này có thể là E the r ne t SLIP ppp	100
		https://text.123doc.org/document/4544345-bao-cau-tim-hieu-he-thong-phat-hien-xam-nhap-snort-ids.htm	
29	Và được giải mã bởi bộ giải mã gói tin (packet decoder), trong đó xác định giao thức được sử dụng cho gói tin và dữ liệu phù hợp với hành vi được cho phép của phần giao thức của chúng.	Và được giải mã bởi Pac ke t De co de r trong đó xác định giao thức được sử dụng cho gói tin và dữ liệu phù hợp với hành vi được cho phép của phần giao thức của chúng	86
		https://text.123doc.org/document/4517074-cai-dat-mot-he-thong-idsips-dua-tren-phan-mem.htm	
29	Packet Decoder có thể tạo ra các cảnh báo riêng của mình dựa trên phần header của giao thức, các gói tin quá dài, bất thường hoặc không chính xác các tùy chọn TCP được thiết lập trong phần header.	Pac ke t De co de r có thể tạo ra các cảnh báo riêng của mình dựa trên phần he a de r của giao thức các gói tin quá dài bất thường hoặc không chính xác các tùy chọn TCP được thiết lập trong phần he a de r	100
		https://text.123doc.org/document/4544345-bao-cau-tim-hieu-he-thong-phat-hien-xam-nhap-snort-ids.htm	
29	Sau khi dữ liệu được giải mã đúng, chúng sẽ được gửi đến bộ phận tiền xử lý (preprocessor).	Sau khi dữ liệu được giải mã đúng chúng sẽ được gửi đến bộ phận tiền xử lý P re pro ces so r	100
		https://text.123doc.org/document/4517074-cai-dat-mot-he-thong-idsips-dua-tren-phan-mem.htm	

Trang	Câu trùng lặp	Nguồn	Điểm
29	- Các bộ tiền xử lý – PreProcessers	Snort hỗ trợ khả năng hoạt động trên các giao thức sau Ethernet 802.11 Token Ring FDDI Cisco HDLC SLIP PPP và PF của OpenBSD 2 Kiến trúc của Snort Snort có 5 thành phần chính như sau Bộ giải mã gói tin Packet Decoder Các bộ tiền xử lý PreProcessors Máy phát hiện Detection Engine Hệ thống cảnh báo và ghi dấu Logging and Alerting System Môđun xuất Output Module Sơ đồ sau biểu diễn quan hệ giữa các thành phần của Snort	100
		https://text.123doc.org/document/3374292-cac-he-thong-phat-hien-xam-nhap-dua-tren-dau-hieu.htm	
29	Các bộ tiền xử lý (Preprocessor) là những thành phần hoặc plug-in có thể sử dụng cho Snort để sắp xếp, chỉnh sửa các gói dữ liệu trước khi bộ phận Detection Engine làm việc với chúng. Một số Preprocessor cũng thực hiện phát hiện dấu hiệu dị thường bằng cách tìm trong phần tiêu đề của gói tin và tạo ra các cảnh báo. Dùng để tái hợp gói tin cho các gói tin có kích thước lớn. Ngoài ra nó còn giải mã các gói tin đã được mã hóa trước khi chuyển đến bộ phận Detection Engine.	Sau khi dữ liệu được giải mã đúng chúng sẽ được gửi đến bộ phận tiền xử lý preprocessor Preprocessor bộ phận tiền xử lý Các Preprocessor là những thành phần hoặc plug-in có thể sử dụng cho Snort để sắp xếp chỉnh sửa các gói dữ liệu trước khi bộ phận Detection Engine làm việc với chúng Một số Preprocessor cũng thực hiện phát hiện dấu hiệu dị thường bằng cách tìm trong phần tiêu đề của gói tin và tạo ra các cảnh báo Preprocessor còn dùng để tái hợp gói tin cho các gói tin có kích thước lớn Ngoài ra nó còn giải mã các gói tin đã được mã hóa trước khi chuyển đến bộ phận Detection Engine Detection Engine bộ phận kiểm tra Detection Engine là bộ phận quan trọng nhất của Snort	100
		https://text.123doc.org/document/4544345-bao-cao-tim-hieu-he-thong-phat-hien-xam-nhap-snort-ids.htm	

Trang	Câu trùng lặp	Nguồn	Điểm
30	Detection Engine là bộ phận quan trọng nhất của Snort. Trách nhiệm của nó là phát hiện bất kỳ dấu hiệu tấn công nào tồn tại trong gói tin bằng cách sử dụng các rule để đối chiếu với thông tin trong gói tin. Detection Engine có thể phân chia gói tin và áp dụng rule cho các phần khác nhau của gói tin.	Ngoài ra nó còn giải mã các gói tin đã được mã hóa trước khi chuyển đến bộ phận De te c ti on En gi ne De te c ti on En gi ne bộ phận kiểm tra De te c ti on En gi ne là bộ phận quan trọng nhất của Snort Trách nhiệm của nó là phát hiện bất kỳ dấu hiệu tấn công nào tồn tại trong gói tin bằng cách sử dụng các rule để đối chiếu với thông tin trong gói tin Nếu gói tin là phù hợp với rule hành động thích hợp được thực hiện Hiệu suất hoạt động của bộ phận này phụ thuộc các yếu tố như số lượng rule cấu hình máy mà Snort đang chạy tốc độ bus sử dụng cho máy Snort lưu lượng mạng 3 AN TOÀN ỨNG DỤNG WEB VÀ CƠ SỞ DỮ LIỆU NHÓM 2 De te c ti on En gi ne có thể phân chia gói tin và áp dụng rule cho các phần khác nhau của gói tin Log gin g and A le r tin g Sys tem Bộ phận ghi nhận và thông báo Khi bộ phận de te c ti on eng in e phát hiện ra các dấu hiệu tấn công thì nó sẽ thông báo cho bộ phận Log gin g and A le r tin g Sys tem	100
		https://text.123doc.org/document/4544345-bao-cao-tim-hieu-he-thong-phat-hien-xam-nhap-snort-ids.htm	
30	Khi bộ phận detection engine phát hiện ra các dấu hiệu tấn công thì nó sẽ thông báo cho bộ phận cảnh báo và nhật ký(Logging and Alerting System).	Mo du le log và cảnh báo Log gin g and A le r tin g Sys tem Khi bộ phận de te c ti on eng in e phát hiện ra các dấu hiệu tấn công thì nó sẽ thông báo cho bộ phận Log gin g and A le r tin g Sys tem	79
		https://text.123doc.org/document/2630808-tieu-luan-mon-hoc-an-ninh-mang-cau-hinh-he-thong-ids.htm	
30	Các ghi nhận, thông báo có thể được lưu dưới dạng văn bản hoặc một số định dạng khác.	Các ghi nhận thông báo có thể được lưu dưới dạng văn bản hoặc một số định dạng khác Output Mo du le s bộ phận đầu ra Bộ phận đầu ra của Snort phụ thuộc vào việc ta ghi các ghi nhận thông báo theo cách thức nào	100
		https://text.123doc.org/document/4544345-bao-cao-tim-hieu-he-thong-phat-hien-xam-nhap-snort-ids.htm	

Trang	Câu trùng lặp	Nguồn	Điểm
30	Mặc định thì chúng được lưu tại thư mục /var/log/snort.	Mặc định thì chúng được lưu tại thư mục var log snort	100
		https://text.123doc.org/document/4517074-cai-dat-mot-he-thong-idsips-dua-tren-phan-mem.htm	
30	Bộ phận đầu ra của Snort phụ thuộc vào việc ta ghi các ghi nhận, thông báo theo cách thức nào. Có thể cấu hình bộ phận này để thực hiện các chức năng sau: - Lưu các ghi nhận và thông báo theo định dạng file văn bản hoặc cơ sở dữ liệu.	Các ghi nhận thông báo có thể được lưu dưới dạng văn bản hoặc một số định dạng khác Output Module s bộ phận đầu ra Bộ phận đầu ra của Snort phụ thuộc vào việc ta ghi các ghi nhận thông báo theo cách thức nào Có thể cấu hình bộ phận này để thực hiện các chức năng sau Lưu các ghi nhận và thông báo theo định dạng các file văn bản hoặc vào cơ sở dữ liệu Gửi thông tin SNMP Gửi các thông điệp đến hệ thống ghi log Lưu các ghi nhận và thông báo vào cơ sở dữ liệu MySQL O ra c le hình trên Rou te r Fi re wall 1 4 Chỉnh sửa cấu Rules Cũng giống như virus hầu hết các hoạt động tấn công hay xâm nhập đều có các dấu hiệu riêng	100
		https://text.123doc.org/document/4544345-bao-cao-tim-hieu-he-thong-phat-hien-xam-nhap-snort-ids.htm	
30	- Gửi các thông điệp đến hệ thống ghi log.	Có thể cấu hình bộ phận này để thực hiện các chức năng sau Gửi thông tin SNMP Gửi các thông điệp đến hệ thống ghi log Lưu các ghi nhận và thông báo vào cơ sở dữ liệu My SQL O ra c le Chỉnh sửa cấu hình trên Rou te r Fi re wall III 1 2 2	100
		https://text.123doc.org/document/4517074-cai-dat-mot-he-thong-idsips-dua-tren-phan-mem.htm	

Trang	Câu trùng lặp	Nguồn	Điểm
30	- Lưu các ghi nhận và thông báo vào cơ sở dữ liệu (MySQL, Oracle...).	Có thể cấu hình bộ phận này để thực hiện các chức năng sau Lưu các ghi nhận và thông báo theo định dạng các file văn bản hoặc vào cơ sở dữ liệu Gửi thông tin SNMP Gửi các thông điệp đến hệ thống ghi log Lưu các ghi nhận và thông báo vào cơ sở dữ liệu MySQL O ra c le hình trên Rou te r Fi re wall 1 4 Chỉnh sửa cấu Rules Cũng giống như virus hầu hết các hoạt động tấn công hay xâm nhập đều có các dấu hiệu riêng	100
		https://text.123doc.org/document/4544345-bao-cao-tim-hieu-he-thong-phat-hien-xam-nhap-snort-ids.htm	
30	- Chỉnh sửa cấu hình trên Router, Firewall.	Có thể cấu hình bộ phận này để thực hiện các chức năng sau Gửi thông tin SNMP Gửi các thông điệp đến hệ thống ghi log Lưu các ghi nhận và thông báo vào cơ sở dữ liệu My SQL O ra c le Chỉnh sửa cấu hình trên Rou te r Fi re wall III 1 2 2	100
		https://text.123doc.org/document/4517074-cai-dat-mot-he-thong-idsips-dua-tren-phan-mem.htm	
30	Snort có 4 chế độ hoạt động như sau:	Output modul sẽ loại bỏ các gói tin ghi log hay sinh ra cảnh báo Snort có 4 chế độ hoạt động như sau S ni ffer mode ở chế độ này snort sẽ lắng nghe và đọc các gói tin trên mạng sau đó sẽ trình bày kết quả trên giao diện hiển thị	100
		https://text.123doc.org/document/3374292-cac-he-thong-phat-hien-xam-nhap-dua-tren-dau-hieu.htm	

Trang	Câu trùng lặp	Nguồn	Điểm
30	- Chế độ đánh hơi - Sniffer mode: ở chế độ này Snort sẽ lắng nghe và đọc các gói tin trên mạng sau đó sẽ trình bày kết quả trên giao diện hiển thị.	<p>Snort có 4 chế độ hoạt động khác nhau đó là 21 Tìm hiểu về các phần mềm phát hiện và phòng chống xâm nhập trái phép Sniffer mode ở chế độ này snort sẽ lắng nghe và đọc các gói tin trên mạng sau đó sẽ trình bày kết quả trên giao diện hiển thị Pac ket Logger mode lưu trữ các gói tin trong các tập tin log Network in s tru c ti on de te ct sys tem NIDS đây là chế độ hoạt động mạnh mẽ và được áp dụng nhiều nhất khi hoạt động ở chế độ NIDS Snort sẽ phân tích các gói tin luân chuyển trên mạng và so sánh với các thông tin được định nghĩa của người dùng để từ đó có những hành động tương ứng như thông báo cho quản trị mạng khi xảy ra tình huống quét lỗi do các hacker at ta c ke r tiến hành hay cảnh báo virus</p> <p>https://text.123doc.org/document/2540750-tim-hieu-ve-cac-phan-mem-phat-hien-va-phong-chong-xam-nhap-trai-phiep.htm</p>	89
30	- Chế độ phát hiện xâm nhập mạng - Network instruction detect system (NIDS): đây là chế độ hoạt động mạnh mẽ và được áp dụng nhiều nhất, khi hoạt động ở chế độ NIDS Snort sẽ phân tích các gói tin luân chuyển trên mạng và so sánh với	<p>Snort có 4 chế độ hoạt động khác nhau đó là 21 Tìm hiểu về các phần mềm phát hiện và phòng chống xâm nhập trái phép Sniffer mode ở chế độ này snort sẽ lắng nghe và đọc các gói tin trên mạng sau đó sẽ trình bày kết quả trên giao diện hiển thị Pac ket Logger mode lưu trữ các gói tin trong các tập tin log Network in s tru c ti on de te ct sys tem NIDS đây là chế độ hoạt động mạnh mẽ và được áp dụng nhiều nhất khi hoạt động ở chế độ NIDS Snort sẽ phân tích các gói tin luân chuyển trên mạng và so sánh với các thông tin được định nghĩa của người dùng để từ đó có những hành động tương ứng như thông báo cho quản trị mạng khi xảy ra tình huống quét lỗi do các hacker at ta c ke r tiến hành hay cảnh báo virus</p> <p>https://text.123doc.org/document/2540750-tim-hieu-ve-cac-phan-mem-phat-hien-va-phong-chong-xam-nhap-trai-phiep.htm</p>	83

Trang	Câu trùng lặp	Nguồn	Điểm
31	20 các thông tin được định nghĩa của người dùng để từ đó có những hành động tương ứng.	Network in s tru c ti on de te ct sys tem NIDS đây là chế độ hoạt động mạnh mẽ và được áp dụng nhiều nhất khi hoạt động ở NIDS mode Snort sẽ phân tích các gói tin luân chuyển trên mạng và so sánh với các thông tin được định nghĩa của người dùng để từ đó có những hành động tương ứng như thông báo cho quản trị mạng khi xảy ra tình huống quét lỗi do các hacker at ta c ke r tiến hành hay cảnh báo virus	94
		https://text.123doc.org/document/3374292-cac-he-thong-phat-hien-xam-nhap-dua-tren-dau-hieu.htm	

Trang	Câu trùng lặp	Nguồn	Điểm
31	2.1.1.3. Ưu nhược điểm của Snort a.	<p>Bố cục của Khóa luận 3 PHẦN NỘI DUNG 5 CHƯƠNG 1 5 KHÁI QUÁT VỀ THƯ VIỆN QUỐC GIA VIỆT NAM 5 VÀ VAI TRÒ CỦA KHUNG PHÂN LOẠI 5 TRONG PHÂN LOẠI TÀI LIỆU 5 1 1 Khái quát về Thư viện Quốc gia Việt Nam 5 1 1 1 Quá trình hình thành và phát triển 5 1 1 2 Chức năng nhiệm vụ 11 1 1 3 Cơ cấu tổ chức đội ngũ cán bộ 14 1 1 3 1 Cơ cấu tổ chức 14 1 1 3 2 Đội ngũ cán bộ 16 1 1 4 Vốn tài liệu 16 1 2 Vai trò của khung phân loại trong phân loại tài liệu tại Thư viện Quốc gia Việt Nam 18</p> <p>CHƯƠNG 2 20 QUÁ TRÌNH NGHIÊN CỨU VÀ ỨNG DỤNG KHUNG PHÂN LOẠI TẠI THƯ VIỆN QUỐC GIA VIỆT NAM TỪ 1954 ĐẾN NAY 20 2 1 Tình hình sử dụng khung phân loại trước khi áp dụng DDC 1954 2002 20 2 1 1 Khung phân loại Trung tiểu hình 1954 1960 20 2 1 1 1 Hoàn cảnh xã hội 20 2 1 1 2 Quá trình nghiên cứu và ứng dụng Khung Trung tiểu hình 21 2 1 1 3 Ưu nhược điểm của Khung phân loại Trung tiểu hình 23 2 1 2 Khung phân loại 19 lớp 1960 1983 24 2 1 2 1 Hoàn cảnh xã hội 24 2 1 2 2 Quá trình nghiên cứu và sử dụng Bảng phân loại 19 lớp 25 2 1 2 3 Ưu nhược điểm của Bảng phân loại 19 lớp 32 2 1 3 Khung phân loại BBK 1983 2002 33 2 1 3 1 Hoàn cảnh xã hội 33 2 1 3 2 Quá trình nghiên cứu và ứng dụng Khung BBK tại Thư viện Quốc gia 33 2 1 3 3 Ưu nhược điểm của Khung phân loại BBK 37 2 2 Tình hình áp dụng khung phân loại DDC 2003 đến nay 38 2 2 1 Hoàn cảnh xã hội 38 2 2 2 Quá trình nghiên cứu và ứng dụng Khung phân loại DDC 39 2 2 2 1 Ấn bản DDC 14 rút gọn 45 2 2 2 2 Ấn bản DDC 23 50</p> <p>CHƯƠNG 3 54 MỘT SỐ NHẬN XÉT VÀ GIẢI PHÁP NÂNG CAO CHẤT LƯỢNG SỬ DỤNG KHUNG PHÂN LOẠI TẠI THƯ VIỆN QUỐC GIA VIỆT NAM 54 3 1 Nhận xét chung quá trình sử dụng Khung phân loại tại TVQGVN 54 3 2 Một số giải pháp nâng cao chất lượng trong quá trình sử dụng Khung phân loại 55 PHẦN KẾT LUẬN 60 PHẦN MỞ ĐẦU 1</p>	76

Trang	Câu trùng lặp	Nguồn	Điểm
		https://text.123doc.org/document/4171196-nghien-cuu-ung-dung-khung-phan-loai-tai-thu-vien-quoc-gia-viet-nam-tu-1954-den-nay.htm	
31	- Có một cộng đồng của người sử dụng và các nhà phát triển.	Hơn nữa các thông tin đăng nhập phải đáng tin cậy và bảo mật 1 4 2 Bảo mật trong học trực tuyến E le ar ni ng Có rất nhiều nguồn hệ thống mở e le ar ni ng có thể được cài đặt dễ dàng và có một cộng đồng lớn người sử dụng và các nhà phát triển	78
		https://text.123doc.org/document/3012256-nghien-cuu-va-trien-khai-bao-mat-he-thong-elearning-cho-truong-dai-hoc-dien-luc.htm	
31	- Có thể xảy ra trường hợp báo động giả, tức là không có dấu hiệu bất thường mà	Hạn chế của NIDS Có thể xảy ra trường hợp báo động giả tức là không có dấu hiệu bất thường mà IDS vẫn báo Không thể phân tích được các lưu lượng đã được mã hóa như SSH IPsec SSL Hệ Thống Phát Hiện Và Ngăn Chặn Xâm Nhập Với Snort và IPTab le s Văn Đình Quân 0021 Trang 6 NIDS đòi hỏi phải luôn được cập nhật các dấu hiệu tấn công mới nhất để thực sự hoạt động hiệu quả Không thể cho biết việc mạng bị tấn công có thành công hay không để người quản trị tiến hành bảo trì hệ thống Một trong những hạn chế là giới hạn băng thông	100
		http://123doc.org/document/1037857-he-thong-phat-hien-va-ngan-chan-xam-nhap-voi-snort-va-iptables.htm	

Trang	Câu trùng lặp	Nguồn	Điểm
31	<p>- Không phân tích được các lưu lượng được mã hóa như SSH, IPSec, SSL, v.v... - NIDS đòi hỏi phải luôn được cập nhật các dấu hiệu tấn công mới nhất để thực sự hoạt động hiệu quả.</p>	<p>Hạn chế của NIDS Có thể xảy ra trường hợp báo động giả tức là không có dấu hiệu bất thường mà IDS vẫn báo Không thể phân tích được các lưu lượng đã được mã hóa như SSH IPSec SSL Văn Đình Quân 0021 Trang 5 Hệ Thống Phát Hiện Và Ngăn Chặn Xâm Nhập Với Snort và IPTables NIDS đòi hỏi phải luôn được cập nhật các dấu hiệu tấn công mới nhất để thực sự hoạt động hiệu quả Không thể cho biết việc mạng bị tấn công có thành công hay không để người quản trị tiến hành bảo trì hệ thống Một trong những hạn chế là giới hạn băng thông</p>	86
		<p>https://text.123doc.org/document/2861261-he-thong-phat-hien-va-ngan-chan-xam-nhap-voi-snort-va-iptables.htm</p>	
31	<p>- Không thể cho biết việc mạng bị tấn công có thành công hay không.</p>	<p>Hạn chế của NIDS Có thể xảy ra trường hợp báo động giả tức là không có dấu hiệu bất thường mà IDS vẫn báo Không thể phân tích được các lưu lượng đã được mã hóa như SSH IPSec SSL Hệ Thống Phát Hiện Và Ngăn Chặn Xâm Nhập Với Snort và IPTables Văn Đình Quân 0021 Trang 6 NIDS đòi hỏi phải luôn được cập nhật các dấu hiệu tấn công mới nhất để thực sự hoạt động hiệu quả Không thể cho biết việc mạng bị tấn công có thành công hay không để người quản trị tiến hành bảo trì hệ thống Một trong những hạn chế là giới hạn băng thông</p>	100
		<p>http://123doc.org/document/1037857-he-thong-phat-hien-va-ngan-chan-xam-nhap-voi-snort-va-iptables.htm</p>	
31	<p>- Một trong những hạn chế là giới hạn băng thông.</p>	<p>Không cho biết việc attack có thành công hay không Một trong những hạn chế là giới hạn băng thông</p>	100
		<p>https://text.123doc.org/document/3581730-giam-sat-tap-trung-ma-nguon-mo-ossim.htm</p>	
31	<p>Những bộ thu thập dữ liệu phải thu thập tất cả lưu lượng mạng, sắp xếp lại và phân tích chúng.</p>	<p>Những bộ thu thập dữ liệu phải thu thập tất cả lưu lượng mạng sắp xếp lại và phân tích chúng</p>	100

Trang	Câu trùng lặp	Nguồn	Điểm
		https://text.123doc.org/document/2861261-he-thong-phat-hien-va-ngan-chan-xam-nhap-voi-snort-va-iptables.htm	
32	21 lên thì khả năng của bộ thu thập thông tin cũng vậy.	<p>Khi tốc độ mạng tăng lên thì khả năng của bộ thu thập thông tin cũng vậy</p> <p>http://123doc.org/document/1037857-he-thong-phat-hien-va-ngan-chan-xam-nhap-voi-snort-va-iptables.htm</p>	91
32	Một giải pháp là phải đảm bảo cho mạng được thiết kế chính xác.	<p>Một giải pháp là phải đảm bảo cho mạng được thiết kế chính xác</p> <p>https://text.123doc.org/document/2861261-he-thong-phat-hien-va-ngan-chan-xam-nhap-voi-snort-va-iptables.htm</p>	100
32	Suricata là một hệ thống phát hiện xâm nhập dựa trên mã nguồn mở.	<p>Giới thiệu về Su ri ca ta Su ri ca ta là một hệ thống phát hiện xâm nhập dựa trên mã nguồn mở</p> <p>https://text.123doc.org/document/4210277-nghien-cuu-cac-chuc-nang-cua-tuong-lua-the-he-moi-suricata-va-ung-dung-trong-mang-noi-bo-doanh-nghiep.htm</p>	100
32	Công cụ này được phát triển không nhằm cạnh tranh hay thay thế các công cụ hiện có, nhưng nó mang lại những ý tưởng và công nghệ mới trong lĩnh vực an ninh mạng. Suricata là công cụ IDS/IPS (Intrusion Detection System / Intrusion Prevention System) phát hiện và ngăn chặn xâm nhập dựa trên luật để theo dõi lưu lượng mạng và cung cấp cảnh báo đến người quản trị hệ thống khi có sự kiện đáng ngờ xảy ra.	<p>Công cụ này được phát triển không nhằm cạnh tranh hay thay thế các công cụ hiện có nhưng nó sẽ mang lại những ý tưởng và công nghệ mới trong lĩnh vực an ninh mạng Su ri ca ta là công cụ IDS IPS In tru si on De te c ti on Sys tem In tru si on P re ven ti on Sys tem phát hiện và ngăn chặn xâm nhập dựa trên luật để theo dõi lưu lượng mạng và cung cấp cảnh báo đến người quản trị hệ thống khi có sự kiện đáng ngờ xảy ra</p> <p>https://text.123doc.org/document/4724755-he-thong-phat-hien-xam-nhap-mang-suricata.htm</p>	100

Trang	Câu trùng lặp	Nguồn	Điểm
32	Nó được thiết kế để tương thích với các thành phần an ninh mạng hiện có. Bản phát hành đầu tiên chạy trên nền tảng linux 2.6 có hỗ trợ nội tuyến (inline) và cấu hình giám sát lưu lượng thụ động có khả năng xử lý lưu lượng lên đến gigabit. Suricata là công cụ IDS/IPS miễn phí trong khi nó vẫn cung cấp những lựa chọn khả năng mở rộng cho các kiến trúc an ninh mạng phức tạp nhất.	Nó được thiết kế để tương thích với các thành phần an ninh mạng hiện có. Bản phát hành đầu tiên chạy trên nền tảng linux 2.6 có hỗ trợ nội tuyến inline và cấu hình giám sát lưu lượng thụ động có khả năng xử lý lưu lượng lên đến gigabit. Suricata là công cụ IDS/IPS miễn phí trong khi nó vẫn cung cấp những lựa chọn khả năng mở rộng cho các kiến trúc an ninh mạng phức tạp nhất	100
		https://text.123doc.org/document/4210277-nghien-cuu-cac-chuc-nang-cua-tuong-lua-the-he-moi-suricata-va-ung-dung-trong-mang-noi-bo-doanh-nghiep.htm	
32	Là một công cụ đa luồng, Suricata cung cấp tăng tốc độ và hiệu quả trong việc phân tích lưu lượng mạng.	Là một công cụ đa luồng Suricata cung cấp tăng tốc độ và hiệu quả trong việc phân tích lưu lượng mạng	100
		https://text.123doc.org/document/4724755-he-thong-phat-hien-xam-nhap-mang-suricata.htm	
32	Ngoài việc tăng hiệu quả phần cứng (với phần cứng và card mạng giới hạn), công cụ này được xây dựng để tận dụng khả năng xử lý cao được cung cấp bởi chip CPU đa lõi mới nhất.	Ngoài việc tăng hiệu quả phần cứng với phần cứng và card mạng giới hạn công cụ này được xây dựng để tận dụng khả năng xử lý cao được cung cấp bởi chip CPU đa lõi mới nhất	100
		https://text.123doc.org/document/4210277-nghien-cuu-cac-chuc-nang-cua-tuong-lua-the-he-moi-suricata-va-ung-dung-trong-mang-noi-bo-doanh-nghiep.htm	

Trang	Câu trùng lặp	Nguồn	Điểm
32	2.1.2.2. Thành phần và chức năng của Suricata	<p>Hồ Chí Minh ngày tháng 04 năm 2011</p> <p>NGUYỄN NGỌC HANH MỤC LỤC</p> <p>CHƯƠNG 1 CƠ SỞ LÝ LUẬN 1 1 Phân khúc thị trường 1 1 1 1 Khái niệm về thị trường 1 1 1 2 Các tiêu thức phân khúc thị trường 1 1 1 2 1 Phân khúc thị trường theo người tiêu dùng 2 1 1 2 2 Phân khúc thị trường doanh nghiệp 7 1 1 2 3 Phân khúc thị trường quốc tế 7 1 1 3 Các nguyên tắc khi phát triển phân khúc thị trường 9 1 1 4 Lợi ích của việc phân khúc 10 1 2 Tổ chức hoạt động Marketing tại doanh nghiệp 11 1 2 1 Khái niệm 11 1 2 2 Thành phần và chức năng của Marketing Mix 13 1 2 2 1 Sản phẩm 13 1 2 2 2 Giá 15 1 2 2 3 Phân Phối 18 1 2 2 4 Hình thức chiêu thị 19 1 3 Ma trận SWOT 21 1 3 1 Phân tích SWOT 21 1 3 2 Phân tích SWOT trong kinh doanh 22 1 3 3 Nội dung ma trận SWOT 22 1 3 3 1 Điểm mạnh 22 1 3 3 2 Điểm yếu 22 1 3 3 3 Cơ hội 23 1 3 3 4 Nguy Cơ 23</p> <p>CHƯƠNG 2 THỰC TRẠNG HOẠT ĐỘNG MARKETING TẠI CÔNG TY TNHH TM DV VIỄN THÔNG ÂN BẢO 2 1 Giới thiệu công ty 24 2 1 1 Quá trình phát triển của công ty 25 2 1 2 Cơ cấu tổ chức 26 2 1 3 Quy trình hoạt động kinh doanh 27 2 1 4 Kết quả hoạt động kinh doanh của Công ty TNHH TM DV Viễn Thông Ân Bảo 28 2 2 Thực trạng hoạt động marketing 33 2 2 1 Sản phẩm và khách hàng 34 2 2 2 Phân phối 35 2 2 3 Hệ thống phân phối 36 2 2 4 Phân phối pháp quảng cáo khuyến mãi và dịch vụ hậu mãi của công ty 37 2 3 Những thuận lợi và khó khăn của công ty 38 2 3 1 Phân tích SWOT tại công ty TNHH TM DV Viễn Thông Ân Bảo 38 2 3 2 Thuận lợi và khó khăn 41</p> <p>CHƯƠNG 3 GIẢI PHÁP HOÀN THIỆN HOẠT ĐỘNG MARKETING TẠI CÔNG TY TNHH TMDV VIỄN THÔNG ÂN BẢO 3 1 Cơ sở giải pháp 43 3 1 1 Thị trường hiện tại 43 3 1 2 Dự báo thị trường tương lai 45 3 1 3 Xác định sứ mệnh mục tiêu 46 3 2 Giải pháp 47 3 2 1 Giải pháp sản phẩm 47 3 2 2 Giải pháp giá 48 3 2 3 Giải pháp phân phối 50 3 2 4 Hoạt động khuyến mãi chiêu thị 51</p> <p>KẾT LUẬN 55 Tài liệu tham khảo 56</p>	89

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>Khóa luận tốt nghiệp GVHD ThS Ngô Ngọc Cường SVTH N gu yễn Ngọc Hạnh DANH MỤC CÁC TỪ VIẾT TẮT 1 www ta p chi cong san org vn asp</p> <p>https://text.123doc.org/document/2456903-giai-phap-hoan-thien-hoat-dong-marketing-tai-cong-ty-tnhh-tm-dv-vien-thong-an-bao.htm</p>	
32	Suricata được phát triển dựa trên Snort nên nó vẫn giữ nguyên kiến trúc bên trong của Snort.Kiến trúc của nó có nhiều thành phần, với mỗi thành phần có một chức năng riêng.	<p>Kiến trúc của Su ri ca ta Su ri ca ta được phát triển dựa trên snort nên nó vẫn giữ nguyên kiến trúc bên trong của snort Kiến trúc của nó có nhiều thành phần với mỗi thành phần có một chức năng riêng</p> <p>https://text.123doc.org/document/2244895-xay-dung-he-thong-suricata.htm</p>	100
32	Packet Sniffer là một thiết bị phần cứng hoặc phần mềm được đặt vào trong mạng.	<p>Hình 2 4 Quá trình xử lý gói 17 TRIỂN KHAI HỆ IDS SNORT TRÊN HỆ ĐIỀU HÀNH LINUX Bộ pa c ke t s ni ffer Bộ Pac ke t S ni ffer Bộ bắt gói là một thiết bị phần cứng hay phần mềm được đặt vào trong hệ thống làm nhiệm vụ bắt lưu lượng ra vào trong mạng</p> <p>https://text.123doc.org/document/4902856-trien-khai-he-thong-ids-snort-tren-he-dieu-hanh-linux.htm</p>	72
33	Packet Sniffer có thể được sử dụng với các mục đích như:	<p>Tuy nhiên không nên nhầm lẫn giữa các vấn đề định giá chuyển nhượng với các vấn đề trốn thuế hoặc tránh thuế thậm chí các chính sách định giá chuyển nhượng có thể được sử dụng với các mục đích như vậy OECD Report 1979 Điều rất quan trọng ở đây là cần phải phân biệt được thuật ngữ định giá chuyển nhượng và áp đặt giá chuyển nhượng</p> <p>https://text.123doc.org/document/3168216-kiem-toan-hoat-dong-chuyen-gia-cua-cac-cong-ty-da-quoc-gia-viet-nam.htm</p>	81

Trang	Câu trùng lặp	Nguồn	Điểm
33	- Phân tích mạng và troubleshooting.	Tương phản phân tích mạng và chọn tuyến được dùng phổ biến nhất trong quy hoạch giao thông và quy hoạch và quản lý môi trường sử dụng vùng đệm và xử lý chồng lớp	71
		https://text.123doc.org/document/2576367-tiep-can-gis-chuyen-doi-du-lieu-cad-phuc-vu-quy-hoach-va-quan-ly-do-thi.htm	
33	Phân tích dữ liệu - The Preprocessors	Trên thực tế công ty phân tích dữ liệu The Daily Viz thống kê ở Mỹ ngày đông người chào đời nhất là ngày 9 9 và 19 9 tương ứng với thời điểm thụ thai là 17 12 và 27 12	78
		http://baophapluat.vn/song-khoe/vi-sao-nhieu-em-be-duoc-thu-thai-vao-giang-sinh-371271.html	
33	Các luật có thể được chia thành 2 phần:	Thận của con người bao gồm một triệu đơn vị chức năng được gọi là các nephron có thể được chia thành 2 phần chức năng cầu thận đóng vai trò lọc từ sản phẩm huyết tương được gọi là nước tiểu loãng đầu và ống thận tái hấp thu hầu hết nước tiểu loãng đầu	73
		https://text.123doc.org/document/4314139-nghien-cuu-he-protein-nuoc-tieu-benh-nhan-ghep-than-co-bien-chung-thai-ghep-cap-tinh.htm	
33	ICMP...), địa chỉ IP nguồn, địa chỉ IP đích và port.	Phần header ảo chứa 3 trường trong IP header địa chỉ IP nguồn địa chỉ IP đích và trường chiều dài của UDP	79
		http://voer.edu.vn/c/tang-van-chuyen-trong-mang-internet/476ccb99/bd424f7f	

Trang	Câu trùng lặp	Nguồn	Điểm
34	Có thể gửi cảnh báo thông qua SMB (Server	Use case Danh sách yêu thích được chia thành các use case nhỏ hơn use case Xem danh sách yêu thích use case Thêm địa điểm có đặt FAirBox vào danh sách yêu thích và use case Xóa địa điểm có đặt FAirBox trong danh sách yêu thích 14 Mỗi quan hệ giữa use case Gửi cảnh báo thông qua no ti fi ca ti on và use case Đăng ký cảnh báo là mối quan hệ ex ten d do điều kiện để actor Ser vi ce có thể gửi cảnh báo đó là người dùng phải đăng ký cảnh báo 2 2 4	73
		CC_PhamManhCuong_CNTT4.pdf	
34	Hình 2.2:Mô tả sơ đồ Suricata.	Ngược lại MOSFET kênh N có hai miếng bán dẫn loại N đặt trên nền bán dẫn loại P 2 1 2 N gu yên lý hoạt động của MOSFET Hình 2 2 mô tả sơ đồ nguyên lý hoạt động của MOSFET	85
		https://text.123doc.org/document/3594607-ky-thuat-thiet-ke-mach-giam-cong-suat-ro-trong-vi-mach-so-dung-cong-nghe-45nm.htm	

Trang	Câu trùng lặp	Nguồn	Điểm
34	2.1.2.3. Ưu nhược điểm của Suricata a.	<p>Bố cục của Khóa luận 3 PHẦN NỘI DUNG 5 CHƯƠNG 1 5 KHÁI QUÁT VỀ THƯ VIỆN QUỐC GIA VIỆT NAM 5 VÀ VAI TRÒ CỦA KHUNG PHÂN LOẠI 5 TRONG PHÂN LOẠI TÀI LIỆU 5 1 1 Khái quát về Thư viện Quốc gia Việt Nam 5 1 1 1 Quá trình hình thành và phát triển 5 1 1 2 Chức năng nhiệm vụ 11 1 1 3 Cơ cấu tổ chức đội ngũ cán bộ 14 1 1 3 1 Cơ cấu tổ chức 14 1 1 3 2 Đội ngũ cán bộ 16 1 1 4 Vốn tài liệu 16 1 2 Vai trò của khung phân loại trong phân loại tài liệu tại Thư viện Quốc gia Việt Nam 18</p> <p>CHƯƠNG 2 20 QUÁ TRÌNH NGHIÊN CỨU VÀ ỨNG DỤNG KHUNG PHÂN LOẠI TẠI THƯ VIỆN QUỐC GIA VIỆT NAM TỪ 1954 ĐẾN NAY 20 2 1 Tình hình sử dụng khung phân loại trước khi áp dụng DDC 1954 2002 20 2 1 1 Khung phân loại Trung tiểu hình 1954 1960 20 2 1 1 1 Hoàn cảnh xã hội 20 2 1 1 2 Quá trình nghiên cứu và ứng dụng Khung Trung tiểu hình 21 2 1 1 3 Ưu nhược điểm của Khung phân loại Trung tiểu hình 23 2 1 2 Khung phân loại 19 lớp 1960 1983 24 2 1 2 1 Hoàn cảnh xã hội 24 2 1 2 2 Quá trình nghiên cứu và sử dụng Bảng phân loại 19 lớp 25 2 1 2 3 Ưu nhược điểm của Bảng phân loại 19 lớp 32 2 1 3 Khung phân loại BBK 1983 2002 33 2 1 3 1 Hoàn cảnh xã hội 33 2 1 3 2 Quá trình nghiên cứu và ứng dụng Khung BBK tại Thư viện Quốc gia 33 2 1 3 3 Ưu nhược điểm của Khung phân loại BBK 37 2 2 Tình hình áp dụng khung phân loại DDC 2003 đến nay 38 2 2 1 Hoàn cảnh xã hội 38 2 2 2 Quá trình nghiên cứu và ứng dụng Khung phân loại DDC 39 2 2 2 1 Ấn bản DDC 14 rút gọn 45 2 2 2 2 Ấn bản DDC 23 50</p> <p>CHƯƠNG 3 54 MỘT SỐ NHẬN XÉT VÀ GIẢI PHÁP NÂNG CAO CHẤT LƯỢNG SỬ DỤNG KHUNG PHÂN LOẠI TẠI THƯ VIỆN QUỐC GIA VIỆT NAM 54 3 1 Nhận xét chung quá trình sử dụng Khung phân loại tại TVQGVN 54 3 2 Một số giải pháp nâng cao chất lượng trong quá trình sử dụng Khung phân loại 55 PHẦN KẾT LUẬN 60 PHẦN MỞ ĐẦU 1</p>	76

Trang	Câu trùng lặp	Nguồn	Điểm
		https://text.123doc.org/document/4171196-nghien-cuu-ung-dung-khung-phan-loai-tai-thu-vien-quoc-gia-viet-nam-tu-1954-den-nay.htm	
35	24 - Dễ dàng cấu hình: Suricata làm việc như thế nào, tập tin cấu hình ở đâu, các luật như thế nào người quản trị đều có thể biết và cấu hình theo ý mình được.	<p>Khả năng tự động phát hiện các giao thức phổ biến như HTTP để phân tích và tìm ra các mối nguy hiểm như mã độc hay các kết nối tới máy chủ độc hại ngoài Dễ dàng cấu hình Su ri ca ta làm việc như thế nào tập tin cấu hình ở đâu các luật như thế nào người quản trị đều có thể biết và cấu hình theo ý mình được</p> <p>https://text.123doc.org/document/4724755-he-thong-phat-hien-xam-nhap-mang-suricata.htm</p>	97
35	- Suricata là phần mềm mã nguồn mở: Sricata được phát hành dưới giấy phép GNU/GPL điều này có nghĩa là bất cứ ai cũng có thể sử dụng Suricata một cách miễn phí dù đó là doanh nghiệp hay người dùng cá nhân.	<p>Kể cả việc tạo ra các luật mới Su ri ca ta là phần mềm mã nguồn mở S ri ca ta được phát hành dưới giấy phép GNU GPL điều này có nghĩa là bất cứ ai cũng có thể sử dụng Su ri ca ta một cách miễn phí dù đó là doanh nghiệp hay người dùng cá nhân</p> <p>https://text.123doc.org/document/4210277-nghien-cuu-cac-chuc-nang-cua-tuong-lua-the-he-moi-suricata-va-ung-dung-trong-mang-noi-bo-doanh-nghiep.htm</p>	100

Trang	Câu trùng lặp	Nguồn	Điểm
35	2.2. Các hệ thống phát hiện xâm nhập host	<p>Tác giả luận văn Ngu yễn P hư ợn g</p> <p>Thực MỤC LỤC MỞ ĐẦU 6 1 1 Hiện trạng về an ninh mạng 1 1 1 1 Hiện trạng về an ninh mạng trong nước 1 1 1 2 Số liệu khảo sát về an toàn thông tin tại Việt Nam 2 1 2 Sự cần thiết phải có an ninh mạng và các yếu tố cần bảo vệ 2 1 2 1 Sự cần thiết phải có an ninh mạng 2 1 2 2 Các yếu tố cần bảo vệ 2 1 2 3 Mô hình pho ng vệ theo chiều sâu 3 1 3 Chính sách an toàn an ninh mạng 3 1 3 1 Khái niệm chính sách an ninh mạng 3 1 3 2 Cấu trúc an toàn an ninh mạng 3 1 3 3 Chính sách an toàn an ninh mạng 3 1 4 P hư ợn g pháp phát hiện và pho ng chống xâm nhập 4 1 4 1 Xác định mối đe dọa 4 1 4 2 P hư ợn g pháp pho ng chống xâm nhập 4 C hư ợn g 2 HỆ THỐNG PHÁT HIỆN VÀ PHÒNG CHỐNG XÂM NHẬP IDS IPS 6 2 1 IDS 6 2 1 1 Khái niệm 6 2 1 3 Công nghệ 8 2 1 4 Phân loại 9 2 2 IPS 9 2 2 2 Ưu nhược điểm 9 2 2 3 Công nghệ 10 2 2 4 Phân loại 10 2 3 So sánh IDS và IPS 10 2 3 1 Sự giống nhau 10 2 3 2 Sự khác nhau 11 2 4 P hư ợn g pháp phát hiện xâm nhập 12 2 4 1 Phát hiện dấu hiệu không bình thường 12 2 4 2 Phát hiện dựa theo hành vi bất thường 12 2 4 3 Phát hiện dấu hiệu co hành vi xấu 13 2 4 4 Phát hiện dựa vào tương quan các mẫu tham số 13 2 5 Một số giải pháp IDS IPS thương mại 13 2 5 1 Giải pháp cu a Cisco 13 2 5 2 Giải pháp cu a ISS P ro ven tia 13 2 5 3 Giải pháp cu a NFR 14 C hư ợn g 3 TRIỂN KHAI VÀ ĐÁNH GIÁ THỬ NGHIỆM GIẢI PHÁP CISCO IPS 14 3 1 Giới thiệu kiến trúc hệ thống 14 3 1 1 Kiến trúc chung cu a các hệ thống IPS 14 3 2 Các yêu cầu triển khai 14 3 2 1 Các yêu cầu về bảo mật 14 3 2 2 Yêu cầu về phần cứng phần mềm 15 3 3 Xây dựng mô hình mạng thử nghiệm 16 3 3 1 Thiết kế mô hình mạng thử nghiệm 16 3 3 2 Triển khai cài đặt 16 3 3 3 Triển khai cấu hình 16 3 3 4 Sử dụng IPS ngăn chặn tấn công theo yêu cầu về bảo mật 17 3 4 Tùy chỉnh các tham số pho ng chống tấn công 20 3 4 1 Điều chỉnh tham số cảnh báo 20 3 4 2 Tùy chỉnh cu s tom a to mi c si g na tu re 20 3 4 3 Tùy chỉnh</p>	82

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>cu s tom s tre am si g na tu re 22 3 4 4 Tùy chỉnh cu s tom http si g na tu re 22 3 5 Đánh giá kết quả thử nghiệm 22 3 5 1 Kết quả đạt được 22 3 5 2 Nhận xét và đánh giá 23 3 5 3 Định hướng nghiên cứu 24 DANH MỤC TÀI LIỆU THAM KHẢO 25 DANH MỤC THUẬT NGỮ CHỮ VIẾT TẮT Chữ viết Nghĩa tiếng Anh Nghĩa tiếng Việt tắt In tru si on P re ven ti on Hệ thống ngăn chặn xâm IPS Sys tem nhập In tru si on De te c ti on Hệ thống phát hiện xâm IDS Sys tem nhập CNTT Công nghệ thông tin In te r ne t Se cu ri ty ISS Hệ thống bảo mật mạng Sys tem s DMZ D em i li ta ri zed Zone Vùng phì quân sự In te r ne t Ser vi ce Nhà cung cấp dịch vụ ISP P ro vi de r In te r ne t In te r na ti on S tan da rd ISO Tổ chức tiêu chuẩn quốc tế Or ga ni za ti on LAN Local Area Network Mạng cục bộ T ran s miss ion Con tro l Giao thức kiểm soát truyền TCP P ro to co l tin MỞ ĐẦU Ngày nay hệ thống mạng máy tính đã trở nên rất phổ biến trong hầu hết các hoạt động kinh tế xã hội</p> <p>http://tailieu.vn/doc/tom-tat-luan-van-thac-si-nghien-cuu-trien-khai-he-thong-phat-hien-va-phong-chong-xam-nhap-ids-ips-1624319.html</p>	
35	OSSEC dựa trên log mã nguồn mở, miễn phí, đa nền tảng có thể mở rộng và có nhiều cơ chế bảo mật khác nhau.OSSEC có thể phát hiện xâm nhập bằng cả chữ ký hoặc dấu hiệu bất thường.	<p>OSSEC là hệ thống phát hiện xâm nhập dựa trên host HIDS dựa trên log mã nguồn mở miễn phí đa nền tảng có thể mở rộng và có nhiều cơ chế bảo mật khác nhau OSSEC có thể phát hiện xâm nhập bằng cả chữ ký hoặc dấu hiệu bất thường</p> <p>https://viblo.asia/p/tim-hieu-ve-he-thong-phat-hien-xam-nhap-ossec-phan-i-m68Z03JzKkG</p>	100

Trang	Câu trùng lặp	Nguồn	Điểm
35	<p>Các dấu hiệu bình thường và bất thường được mô tả trong bộ luật của OSSEC.OSSEC có một công cụ phân tích và tương quan mạnh mẽ, tích hợp giám sát và phân tích log, kiểm tra tính toàn vẹn của file, kiểm tra registry của Windows, thực thi chính sách tập trung, giám sát chính sách, phát hiện rootkit, cảnh báo thời gian thực và phản ứng một cách chủ động cuộc tấn công đang diễn ra.25 hành động này cũng có thể được định nghĩa trước bằng luật trong OSSEC.Ngoài việc được triển khai như một HIDS, nó thường được sử dụng như một công cụ phân tích log, theo dõi và phân tích các bản ghi lại, IDS, các máy chủ Web và các bản ghi xác thực.</p>	<p>Các dấu hiệu bình thường và bất thường được mô tả trong bộ luật của OSSEC OSSEC có một công cụ phân tích và tương quan mạnh mẽ tích hợp giám sát và phân tích log kiểm tra tính toàn vẹn của file kiểm tra registry của Windows thực thi chính sách tập trung giám sát chính sách phát hiện rootkit cảnh báo thời gian thực và phản ứng một cách chủ động cuộc tấn công đang diễn ra Các hành động này cũng có thể được định nghĩa trước bằng luật trong OSSEC để OSSEC hoạt động theo ý muốn của người quản trị Ngoài việc được triển khai như một HIDS nó thường được sử dụng như một công cụ phân tích log theo dõi và phân tích các bản ghi lại IDS các máy chủ Web và các bản ghi xác thực</p>	100
		<p>https://viblo.asia:443/p/tim-hieu-ve-he-thong-phat-hien-xam-nhap-ossec-phan-i-m68Z03JzKkG</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
36	OSSEC chạy trên hầu hết các hệ điều hành, bao gồm Linux, OpenBSD,	<p>Tuy nhiên một điều tuyệt vời của nền tảng Ec li p se là nó chạy trên hầu hết các hệ điều hành bao gồm W in do ws 98 ME 2000 XP Linux So la ri s AIX HP UX và thậm chí cả Mac OS X 1 của 15 Trang sau Về đầu trang s ta ti c con ten t url <a "="" developerworks="" edu="" href="http://www.ibm.com/developerworks/js/art/ra/tin/g/SITE_ID_70_Zo_ne_Cong_ngh_e_Ja_va_Ar_ti_c_le_ID_423961_Tu_to_ria_ITit_le_Nhap_môn_lập_trình_Ja_va_pub_li_sh_date_03282013_au_tho_r_1_email_roy_ro_yw_mi_l_le_r_co_mau_tho_r_1_email_cc_Mục_lục_Gi_oi_thiệu_K_hởi_động_Các_khái_niệm_OOPN_gôn_ngữ_Java_đăng_sau_về_bềngoài_L_ập_trình_hướng_đối_tượng_với_công_nghệ_Ja_va_Đ_ối_tượng_Java_đầu_tiên_của_bạn_T_hê_m_hành_vì_T_hực_thi_điều_kiện_Các_bộ_sưu_tập_Col_le_c_ti_ons_Nâng_cấp_đối_tượng_của_bạn_Các_ứng_dụng_Ja_va_Viết_mã_lệnh_Java_tốt_Tóm_tắt_Tài_ngu_yên_Đ_ôi_nét_về_tác_giả1_của_15_Trang_sau_In_trang_này_Chia_sẻ_trang_này_Chia_sẻ_trang_này_Face_bo_ok_L_in_ke_dlnTwit_te_r_De_li_ciousDigg_Hướng_dẫn_Các_nguồn_RSST_hích_Phản_ánh_về_nội_dung_không_thích_hợp_tiếng_Anh_Điều_khoản_sử_dụng_T_hông_báo_của_bên_thứ_ba_Tính_riêng_tư_T ín_h_tiếp_cận_tiếng_Anh_Trang_hỗ_trợ_đại_học_A_ca_de_mi_c_l_ni_tia_ti_ve_tiếng_Anh_Cổng_dành_cho_sinh_viên_tiếng_Anh_Chọn_ngôn_ngữ_Eng_lì_sh中文日本語РусскийPor_tu_gu_ê_s_B_ra_sì_l_Es_pa_ñolViệt</p> <p>https://www.ibm.com/developerworks/vn/edu/j-introjava/</p>	74
36	FreeBSD, Mac OS X, Sun Solaris và Microsoft Windows.	<p>OSSEC chạy trên hầu hết các hệ điều hành Agent hành bao gồm cả Linux O pe nBSD F re eBSD Mac OS X Sun So la ri s và Mic ro so ft Vai trò của agent là tập hợp thông tin của host và gửi về ossec se r ve r</p> <p>https://text.123doc.org/document/3756146-nghien-cuu-va-xay-dung-he-quan-ly-luat-ho-tro-phat-hien-tan-cong-mang-cho-ma-nguon-mo-ossec.htm</p>	87

Trang	Câu trùng lặp	Nguồn	Điểm
36	2.2.1.2. Thành phần và chức năng	<p>Hồ Chí Minh ngày tháng 04 năm 2011</p> <p>NGUYỄN NGỌC HANH MỤC LỤC</p> <p>CHƯƠNG 1 CƠ SỞ LÝ LUẬN 1 1 Phân khúc thị trường 1 1 1 1 Khái niệm về thị trường 1 1 1 2 Các tiêu thức phân khúc thị trường 1 1 1 2 1 Phân khúc thị trường theo người tiêu dùng 2 1 1 2 2 Phân khúc thị trường doanh nghiệp 7 1 1 2 3 Phân khúc thị trường quốc tế 7 1 1 3 Các nguyên tắc khi phát triển phân khúc thị trường 9 1 1 4 Lợi ích của việc phân khúc 10 1 2 Tổ chức hoạt động Marketing tại doanh nghiệp 11 1 2 1 Khái niệm 11 1 2 2 Thành phần và chức năng của Marketing Mix 13 1 2 2 1 Sản phẩm 13 1 2 2 2 Giá 15 1 2 2 3 Phân Phối 18 1 2 2 4 Hình thức chiêu thị 19 1 3 Ma trận SWOT 21 1 3 1 Phân tích SWOT 21 1 3 2 Phân tích SWOT trong kinh doanh 22 1 3 3 Nội dung ma trận SWOT 22 1 3 3 1 Điểm mạnh 22 1 3 3 2 Điểm yếu 22 1 3 3 3 Cơ hội 23 1 3 3 4 Nguy Cơ 23</p> <p>CHƯƠNG 2 THỰC TRẠNG HOẠT ĐỘNG MARKETING TẠI CÔNG TY TNHH TM DV VIỄN THÔNG ÂN BẢO 2 1 Giới thiệu công ty 24 2 1 1 Quá trình phát triển của công ty 25 2 1 2 Cơ cấu tổ chức 26 2 1 3 Quy trình hoạt động kinh doanh 27 2 1 4 Kết quả hoạt động kinh doanh của Công ty TNHH TM DV Viễn Thông Ân Bảo 28 2 2 Thực trạng hoạt động marketing 33 2 2 1 Sản phẩm và khách hàng 34 2 2 2 Phân phối 35 2 2 3 Hệ thống phân phối 36 2 2 4 Phân phối quảng cáo khuyến mãi và dịch vụ hậu mãi của công ty 37 2 3 Những thuận lợi và khó khăn của công ty 38 2 3 1 Phân tích SWOT tại công ty TNHH TM DV Viễn Thông Ân Bảo 38 2 3 2 Thuận lợi và khó khăn 41</p> <p>CHƯƠNG 3 GIẢI PHÁP HOÀN THIỆN HOẠT ĐỘNG MARKETING TẠI CÔNG TY TNHH TMDV VIỄN THÔNG ÂN BẢO 3 1 Cơ sở giải pháp 43 3 1 1 Thị trường hiện tại 43 3 1 2 Dự báo thị trường tương lai 45 3 1 3 Xác định sứ mệnh mục tiêu 46 3 2 Giải pháp 47 3 2 1 Giải pháp sản phẩm 47 3 2 2 Giải pháp giá 48 3 2 3 Giải pháp phân phối 50 3 2 4 Hoạt động khuyến mãi chiêu thị 51</p> <p>KIẾN NGHỊ 54</p> <p>KẾT LUẬN 55 Tài liệu tham khảo 56</p>	93

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>Khóa luận tốt nghiệp GVHD ThS Ngô Ngọc Cường SVTH N gu yễn Ngọc Hạnh DANH MỤC CÁC TỪ VIẾT TẮT 1 www ta p chi cong san org vn asp</p> <p>https://text.123doc.org/document/2456903-giai-phap-hoan-thien-hoat-dong-marketing-tai-cong-ty-tnhh-tm-dv-vien-thong-an-bao.htm</p>	
36	Hình 2.3: Minh họa sơ đồ OSSEC.	<p>Trên hình 2 3 minh họa sơ đồ hệ điều khiển PCS 7 với Bộ điều khiển là PLC S7 400 của Si em ens</p> <p>https://text.123doc.org/document/4323153-thiet-ke-he-thong-dieu-khien-trung-tam-phan-phoi-khi-gdc-phu-my.htm</p>	85
37	Phát hiện các thay đổi đối với hệ thống.	<p>hành vi nhắc nhở của uac được điều chỉnh thông qua một s li de r bar với bốn vị trí có thể lựa chọn always no ti fy bạn sẽ nhận được các nhắc nhở của uac khi cài đặt phần mềm hoặc thực hiện các thay đổi đối với hệ thống no ti fy only when pro g ram s try to make chang es bạn sẽ nhận được các nhắc nhở nếu một chương trình nào đó yêu cầu các đặc quyền nâng cao tuy nhiên sẽ không khi bạn thực hiện các thay đổi đối với các thiết lập của windows mặc định no ti fy only when pro g ram s try to make chang es do not dim the de sk top giống như mặc định ngoại từ se cu re de sk top bị vô hiệu hóa trong khi nhắc nhở never no ti fy bạn không được nhắc nhở khi thay đổi các thiết lập windows hoặc khi cài đặt phần mềm mới không được tiến cử sử dụng hình 2 một s li de r bar cho phép bạn điều khiển uac nhắc nhở bạn như thế nào trong windows 7 sự nâng cao trong bi t lo c ke r bi t lo c ke r một sản phẩm có trong vista phiên bản en te r p ri se và ul ti ma te cho phép bạn mã hóa toàn bộ các phân vùng bằng aes sử dụng tru s te d p la tform mo du le tpm chip có trong một số máy tính hoặc usb key</p> <p>http://123doc.org/document/888352-tai-lieu-nhung-diem-moi-trong-bao-mat-cua-windows-7-pptx.htm</p>	87

Trang	Câu trùng lặp	Nguồn	Điểm
37	2.2.1.3. Ưu nhược điểm của Ossec a.	<p>Kiểm thử tĩnh S ta ti c te s tin g 8 1 3 2 Kiểm thử động Dy na mi c te s tin g 9 1 4 Kiểm thử phần mềm tự động 10 1 4 1 Ưu nhược điểm của kiểm thử tự động 10 1 4 2 Áp dụng kiểm thử tự động 11 vii 1 5 Các bước xây dựng kiểm thử tự động 11 CHƯƠNG 2 TỔNG QUAN VỀ CÔNG CỤ KIỂM THỬ SELENIUM IDE 13 2 1 Tổng quan về Se le ni um 13 2 1 1 Lịch sử hình thành 13 2 1 2 Đặc điểm của Se le ni um 14 2 1 3 Ưu nhược điểm của Se le ni um 15 2 2 Công cụ Se le ni um IDE 16 2 2 1 Giới thiệu 16 2 2 2 Đặc điểm của Se le ni um IDE 17 2 2 3 Cài đặt Se le ni um IDE 18 2 2 4 Tính năng của Se le ni um IDE 20 2 2 5 Cách xây dựng trường hợp kiểm thử 24 2 2 6 Các lệnh Se le ni um IDE cơ bản 27 CHƯƠNG 3 XÂY DỰNG ỨNG DỤNG NHẬP MÔN HỌC ĐĂNG KÝ CHO SINH VIÊN 29 3 1 Thiết kế cơ sở dữ liệu 29 3 2 Xây dựng ứng dụng 30 3 2 1</p> <p>https://text.123doc.org/document/4315047-trien-khai-kiem-thu-cac-ung-dung-cua-selenium-ide-tren-nhieu-trinh-duyet.htm</p>	76

Trang	Câu trùng lặp	Nguồn	Điểm
38	2.2.2.2. Thành phần và chức năng	<p>Hồ Chí Minh ngày tháng 04 năm 2011</p> <p>NGUYỄN NGỌC HANH MỤC LỤC</p> <p>CHƯƠNG 1 CƠ SỞ LÝ LUẬN 1 1 Phân khúc thị trường 1 1 1 1 Khái niệm về thị trường 1 1 1 2 Các tiêu thức phân khúc thị trường 1 1 1 2 1 Phân khúc thị trường theo người tiêu dùng 2 1 1 2 2 Phân khúc thị trường doanh nghiệp 7 1 1 2 3 Phân khúc thị trường quốc tế 7 1 1 3 Các nguyên tắc khi phát triển phân khúc thị trường 9 1 1 4 Lợi ích của việc phân khúc 10 1 2 Tổ chức hoạt động Marketing tại doanh nghiệp 11 1 2 1 Khái niệm 11 1 2 2 Thành phần và chức năng của Marketing Mix 13 1 2 2 1 Sản phẩm 13 1 2 2 2 Giá 15 1 2 2 3 Phân Phối 18 1 2 2 4 Hình thức chiêu thị 19 1 3 Ma trận SWOT 21 1 3 1 Phân tích SWOT 21 1 3 2 Phân tích SWOT trong kinh doanh 22 1 3 3 Nội dung ma trận SWOT 22 1 3 3 1 Điểm mạnh 22 1 3 3 2 Điểm yếu 22 1 3 3 3 Cơ hội 23 1 3 3 4 Nguy Cơ 23</p> <p>CHƯƠNG 2 THỰC TRẠNG HOẠT ĐỘNG MARKETING TẠI CÔNG TY TNHH TM DV VIỄN THÔNG ÂN BẢO 2 1 Giới thiệu công ty 24 2 1 1 Quá trình phát triển của công ty 25 2 1 2 Cơ cấu tổ chức 26 2 1 3 Quy trình hoạt động kinh doanh 27 2 1 4 Kết quả hoạt động kinh doanh của Công ty TNHH TM DV Viễn Thông Ân Bảo 28 2 2 Thực trạng hoạt động marketing 33 2 2 1 Sản phẩm và khách hàng 34 2 2 2 Phân phối 35 2 2 3 Hệ thống phân phối 36 2 2 4 Phân phối quảng cáo khuyến mãi và dịch vụ hậu mãi của công ty 37 2 3 Những thuận lợi và khó khăn của công ty 38 2 3 1 Phân tích SWOT tại công ty TNHH TM DV Viễn Thông Ân Bảo 38 2 3 2 Thuận lợi và khó khăn 41</p> <p>CHƯƠNG 3 GIẢI PHÁP HOÀN THIỆN HOẠT ĐỘNG MARKETING TẠI CÔNG TY TNHH TMDV VIỄN THÔNG ÂN BẢO 3 1 Cơ sở giải pháp 43 3 1 1 Thị trường hiện tại 43 3 1 2 Dự báo thị trường tương lai 45 3 1 3 Xác định sứ mệnh mục tiêu 46 3 2 Giải pháp 47 3 2 1 Giải pháp sản phẩm 47 3 2 2 Giải pháp giá 48 3 2 3 Giải pháp phân phối 50 3 2 4 Hoạt động khuyến mãi chiêu thị 51</p> <p>KIẾN NGHỊ 54</p> <p>KẾT LUẬN 55 Tài liệu tham khảo 56</p>	100

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>Khóa luận tốt nghiệp GVHD ThS Ngô Ngọc Cường SVTH N gu yễn Ngọc Hạnh DANH MỤC CÁC TỪ VIẾT TẮT 1 www ta p chi cong san org vn asp</p> <p>https://text.123doc.org/document/2456903-giai-phap-hoan-thien-hoat-dong-marketing-tai-cong-ty-tnhh-tm-dv-vien-thong-an-bao.htm</p>	
40	2.3. Các hệ thống phát hiện xâm nhập tích hợp	<p>Hình 2 2 Một ví dụ về hệ IDS 11 Học Viên Phạm Văn Dũng Lớp Mạng Và T ru yền Dữ Liệu M 12 CQCT 01 B N ghi ên cứ hệ thống phát hiện xâm nhập IDS Hình 2 3 Các thành phần chính của một hệ IDS Các hệ thống IDS có thể được triển khai theo 2 hướng là tập trung và phân tán</p> <p>https://text.123doc.org/document/2563757-nghien-cuu-he-thong-phat-hien-xam-nhap-ids.htm</p>	74

Trang	Câu trùng lặp	Nguồn	Điểm
41	2.3.1.2. Thành phần và chức năng	<p>Hồ Chí Minh ngày tháng 04 năm 2011</p> <p>NGUYỄN NGỌC HANH MỤC LỤC</p> <p>CHƯƠNG 1 CƠ SỞ LÝ LUẬN 1 1 Phân khúc thị trường 1 1 1 1 Khái niệm về thị trường 1 1 1 2 Các tiêu thức phân khúc thị trường 1 1 1 2 1 Phân khúc thị trường theo người tiêu dùng 2 1 1 2 2 Phân khúc thị trường doanh nghiệp 7 1 1 2 3 Phân khúc thị trường quốc tế 7 1 1 3 Các nguyên tắc khi phát triển phân khúc thị trường 9 1 1 4 Lợi ích của việc phân khúc 10 1 2 Tổ chức hoạt động Marketing tại doanh nghiệp 11 1 2 1 Khái niệm 11 1 2 2 Thành phần và chức năng của Marketing Mix 13 1 2 2 1 Sản phẩm 13 1 2 2 2 Giá 15 1 2 2 3 Phân Phối 18 1 2 2 4 Hình thức chiêu thị 19 1 3 Ma trận SWOT 21 1 3 1 Phân tích SWOT 21 1 3 2 Phân tích SWOT trong kinh doanh 22 1 3 3 Nội dung ma trận SWOT 22 1 3 3 1 Điểm mạnh 22 1 3 3 2 Điểm yếu 22 1 3 3 3 Cơ hội 23 1 3 3 4 Nguy Cơ 23</p> <p>CHƯƠNG 2 THỰC TRẠNG HOẠT ĐỘNG MARKETING TẠI CÔNG TY TNHH TM DV VIỄN THÔNG ÂN BẢO 2 1 Giới thiệu công ty 24 2 1 1 Quá trình phát triển của công ty 25 2 1 2 Cơ cấu tổ chức 26 2 1 3 Quy trình hoạt động kinh doanh 27 2 1 4 Kết quả hoạt động kinh doanh của Công ty TNHH TM DV Viễn Thông Ân Bảo 28 2 2 Thực trạng hoạt động marketing 33 2 2 1 Sản phẩm và khách hàng 34 2 2 2 Phân phối 35 2 2 3 Hệ thống phân phối 36 2 2 4 Phân phối quảng cáo khuyến mãi và dịch vụ hậu mãi của công ty 37 2 3 Những thuận lợi và khó khăn của công ty 38 2 3 1 Phân tích SWOT tại công ty TNHH TM DV Viễn Thông Ân Bảo 38 2 3 2 Thuận lợi và khó khăn 41</p> <p>CHƯƠNG 3 GIẢI PHÁP HOÀN THIỆN HOẠT ĐỘNG MARKETING TẠI CÔNG TY TNHH TMDV VIỄN THÔNG ÂN BẢO 3 1 Cơ sở giải pháp 43 3 1 1 Thị trường hiện tại 43 3 1 2 Dự báo thị trường tương lai 45 3 1 3 Xác định sứ mệnh mục tiêu 46 3 2 Giải pháp 47 3 2 1 Giải pháp sản phẩm 47 3 2 2 Giải pháp giá 48 3 2 3 Giải pháp phân phối 50 3 2 4 Hoạt động khuyến mãi chiêu thị 51</p> <p>KIẾN NGHỊ 54</p> <p>KẾT LUẬN 55 Tài liệu tham khảo 56</p>	93

Trang	Câu trùng lặp	Nguồn	Điểm
		Khóa luận tốt nghiệp GVHD ThS Ngô Ngọc Cương SVTH N gu yễn Ngọc Hạnh DANH MỤC CÁC TỪ VIẾT TẮT 1 www ta p chi cong san org vn asp	
		https://text.123doc.org/document/2456903-giai-phap-hoan-thien-hoat-dong-marketing-tai-cong-ty-tnhh-tm-dv-vien-thong-an-bao.htm	

Trang	Câu trùng lặp	Nguồn	Điểm
	Hình 2.5: Minh họa sơ đồ IBM Qradar.	<p>Tác giả Phạm Văn Danh IV DANH MỤC CÁC HÌNH VỀ</p> <p>Hình 1 1 Kiến trúc hệ thống GNSS 3 Hình 1 2 Sơ đồ khối bộ thu RF 4 Hình 1 3 Cấu trúc của một thiết bị MOS 5 Hình 1 4 Sự kết nối chất nền 6 Hình 1 5 a thiết bị PMOS đơn giản b PMOS bên trong n well 7 Hình 1 6 Đặc tuyến V A của MOSFET 8 Hình 2 1 Hoạt động của bộ ADC 2 10 Hình 2 2 Đáp ứng của bộ ADC lý tưởng 2 11 Hình 2 3 Sai số độ lệch dương 3 13 Hình 2 4 Sai số khuếch đại dương 3 14 Hình 2 5 Minh họa sai số kích thước bão hòa 3 14 Hình 2 6 Minh họa về độ phi tuyến vi phân 3 15 Hình 2 7 Sai từ mã ở ADC 3 bit do DNL quá lớn 3 16 Hình 2 8 INL của một bộ ADC 3 bit 3 17 Hình 2 9 Spur i ous Free Dy na mi c Range 5 19 Hình 2 10 Kiến trúc bộ ADC truyền thống 6 20 Hình 2 11 Lưu đồ thuật toán bộ kiến trúc ADC đề nghị 22 Hình 2 12 Kiến trúc bộ ADC 4 bit đề nghị 7 23 Hình 2 13 Kiến trúc SAR ADCs đơn giản 9 24 Hình 2 14 Minh họa nhược điểm của SAR ADC so với Flash ADC 26 Hình 2 15 Kiến trúc SAR có khả năng đồng bộ CLK 28 Hình 3 1 Mô hình cơ bản của bộ so sánh 29 Hình 3 2 Sơ đồ khối bộ so sánh 30 Hình 3 3 Đặc tuyến truyền đạt của bộ so sánh 31 Hình 3 4 Các tham số của C om pa ra to r lý tưởng 32 Hình 3 5 Input C om mon Mode Vol ta ge 33 Hình 3 6 Tham số Gain B an dwidth Op amp 34 V Hình 3 7 Tham số slew rate 34 Hình 3 8 Tham số vo l ta ge swing 35 Hình 3 9 Cấu trúc bộ so sánh CMOS SR Latch 37 Hình 3 10 Cơ chế phóng xả của tụ ở M6 9 38 Hình 3 11 Hình minh họa tín hiệu INV1 INV2 của khối CMOS latch 39 Hình 3 12 Kiến trúc co m pa ra to r đồng bộ xung CLK 39 Hình 3 13 Hình minh họa quá trình tạo xung CLK1 từ xung CLK0 40 Hình 4 1 Cấu trúc bộ co m pa ra to r CMOS SR latch 42 Hình 4 2 Quy trình thiết kế cho mạch 4 bit flash ADC dạng nối tiếp 43 Hình 4 3 Cách tính thời gian trễ của mạch 44 Hình 4 4 Ảnh hưởng của Vg1 tới trễ của mạch 45 Hình 4 5 Ảnh hưởng của kích thước số f in ger của M1 tới trễ của mạch 45 Hình 4 6 Xác định số f in ger N2 và N3 của M2 và M3 46 Hình 4 7</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p> Minh họa M4 M5 trên CMOS SR latch 47 Hình 4 8 Xác định N4 N5 của M4 M5 47 Hình 4 9 Xác định kích thước của từng f in ger N6 N7 48 Hình 4 10 Xác định kích thước của N8 N9 49 Hình 4 11 Khối NOR2 a và Khối in ve r te r b 50 Hình 4 12 Mạch nguyên lý MUX 21 a và kết quả mô phỏng MUX 2 1 b 51 Hình 4 13 Sơ đồ bộ MUX 41 a và Kết quả mô phỏng MUX 4 1 b 52 Hình 4 14 Sơ đồ bộ MUX 81 a kết quả mô phỏng MUX 81 b 53 Hình 4 15 Mạch nguyên lý của 4 bit flash ADC 54 Hình 4 16 Sử dụng xung ramp tại đầu vào ADC 55 Hình 4 17 Tham số DNL và INL của 4 bit flash ADC dạng nối tiếp 56 Hình 4 18 Kết quả dạng sóng sau khi qua bộ DAC lý tưởng 57 Hình 4 19 Kết quả đạt được sau khi biến đổi Fou ri er 58 Hình 4 20 Hình minh họa thứ tự trên dưới các layer 61 Hình 4 21 Sơ đồ stich di ag ram của khối NAND3 62 Hình 4 22 Mạch nguyên lý cổng login AND ba đầu vào 62 VI Hình 4 23 Hình minh họa sơ đồ share gate khi thiết kế AND3 63 Hình 4 24 Sơ đồ thiết kế AND3 mới mỗi tra n si s to r gồm hai f in ger 63 Hình 4 25 Minh họa các linh kiện CMOS cơ bản 64 Hình 4 26 Thiết kế la you t của khối co m pa ra to r 65 Hình 4 27 Sơ đồ la you t khối mux21 65 Hình 4 28 Sơ đồ la you t khối ADC 66 VII DANH SÁCH BẢNG BIỂU Bảng 2 1 Bảng tổng kết so sánh ưu và nhược điểm giữa các kiến trúc ADC 25 Bảng 3 1 Bảng so sánh tham số của co m pa ra to r lý tưởng và thực tế 32 Bảng 3 2 Bảng trạng thái của SR latch 38 Bảng 4 1 Bảng yêu cầu thiết kế cho cấu trúc 4 bit flash ADC dạng nối tiếp 41 Bảng 4 2 Bảng trạng thái cho bộ MUX 2 1 51 Bảng 4 3 Bảng trạng thái cho bộ MUX 4 1 52 Bảng 4 4 Bảng trạng thái cho bộ MUX 81 53 Bảng 4 5 Bảng các giá trị DNL và INL 55 Bảng 4 6 Bảng kết quả đạt được của mạch 4 bit flash ADC dạng nối tiếp 58 Bảng 4 7 Bảng so sánh các kết quả với các bài báo công bố IEEE 59 Bảng 4 8 so sánh hai cấu trúc 4 bit flash ADC dạng nối tiếp Se ri es Flash ADC và 4 bit flash ADC truyền thống Co ven ti o na l Flash ADC 69 VIII DANH SÁCH CÁC TỪ VIẾT TẮT ADC </p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>GNSS GPS RF LNA CMOS MOSFET NMOS A na lo g to Di gi ta I Con ve r te r G lo ba I Na vi ga ti on Sa te I li te Sys tem G lo ba I Po si ti o ni ng Sys tem Radio F re quen cy Low Noise Amp li fier C om p le men ta ry Metal Oxide S em i con du c to r Metal oxide se mi con du c to r Bộ chuyển đổi tương tự số Hệ thống vệ tinh dẫn đường toàn cầu Hệ thống định vị toàn cầu Tần số vô tuyến K hu ếch đại tạp âm thấp Công nghệ sử dụng trong thiết kế IC field effect T ran si s to r cảm ứng</p>	
		<p>https://text.123doc.org/document/4002952-nghien-cuu-va-thiet-ke-ic-chuyen-mach-adc.htm</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
45	2.3.2.2. Thành phần và chức năng	<p>Hồ Chí Minh ngày tháng 04 năm 2011</p> <p>NGUYỄN NGỌC HANH MỤC LỤC</p> <p>CHƯƠNG 1 CƠ SỞ LÝ LUẬN 1 1 Phân khúc thị trường 1 1 1 1 Khái niệm về thị trường 1 1 1 2 Các tiêu thức phân khúc thị trường 1 1 1 2 1 Phân khúc thị trường theo người tiêu dùng 2 1 1 2 2 Phân khúc thị trường doanh nghiệp 7 1 1 2 3 Phân khúc thị trường quốc tế 7 1 1 3 Các nguyên tắc khi phát triển phân khúc thị trường 9 1 1 4 Lợi ích của việc phân khúc 10 1 2 Tổ chức hoạt động Marketing tại doanh nghiệp 11 1 2 1 Khái niệm 11 1 2 2 Thành phần và chức năng của Marketing Mix 13 1 2 2 1 Sản phẩm 13 1 2 2 2 Giá 15 1 2 2 3 Phân Phối 18 1 2 2 4 Hình thức chiêu thị 19 1 3 Ma trận SWOT 21 1 3 1 Phân tích SWOT 21 1 3 2 Phân tích SWOT trong kinh doanh 22 1 3 3 Nội dung ma trận SWOT 22 1 3 3 1 Điểm mạnh 22 1 3 3 2 Điểm yếu 22 1 3 3 3 Cơ hội 23 1 3 3 4 Nguy Cơ 23</p> <p>CHƯƠNG 2 THỰC TRẠNG HOẠT ĐỘNG MARKETING TẠI CÔNG TY TNHH TM DV VIỄN THÔNG ÂN BẢO 2 1 Giới thiệu công ty 24 2 1 1 Quá trình phát triển của công ty 25 2 1 2 Cơ cấu tổ chức 26 2 1 3 Quy trình hoạt động kinh doanh 27 2 1 4 Kết quả hoạt động kinh doanh của Công ty TNHH TM DV Viễn Thông Ân Bảo 28 2 2 Thực trạng hoạt động marketing 33 2 2 1 Sản phẩm và khách hàng 34 2 2 2 Phân phối 35 2 2 3 Hệ thống phân phối 36 2 2 4 Phân phối pháp quảng cáo khuyến mãi và dịch vụ hậu mãi của công ty 37 2 3 Những thuận lợi và khó khăn của công ty 38 2 3 1 Phân tích SWOT tại công ty TNHH TM DV Viễn Thông Ân Bảo 38 2 3 2 Thuận lợi và khó khăn 41</p> <p>CHƯƠNG 3 GIẢI PHÁP HOÀN THIỆN HOẠT ĐỘNG MARKETING TẠI CÔNG TY TNHH TMDV VIỄN THÔNG ÂN BẢO 3 1 Cơ sở giải pháp 43 3 1 1 Thị trường hiện tại 43 3 1 2 Dự báo thị trường tương lai 45 3 1 3 Xác định sứ mệnh mục tiêu 46 3 2 Giải pháp 47 3 2 1 Giải pháp sản phẩm 47 3 2 2 Giải pháp giá 48 3 2 3 Giải pháp phân phối 50 3 2 4 Hoạt động khuyến mãi chiêu thị 51</p> <p>KIẾN NGHỊ 54</p> <p>KẾT LUẬN 55 Tài liệu tham khảo 56</p>	100

Trang	Câu trùng lặp	Nguồn	Điểm
		Khóa luận tốt nghiệp GVHD ThS Ngô Ngọc Cương SVTH N gu yễn Ngọc Hạnh DANH MỤC CÁC TỪ VIẾT TẮT 1 www ta p chi cong san org vn asp	
		https://text.123doc.org/document/2456903-giai-phap-hoan-thien-hoat-dong-marketing-tai-cong-ty-tnhh-tm-dv-vien-thong-an-bao.htm	

Trang	Câu trùng lặp	Nguồn	Điểm
	Hình 2.6: Minh họa sơ đồ Security Onion.	<p>Tác giả Phạm Văn Danh IV DANH MỤC CÁC HÌNH VỀ</p> <p>Hình 1 1 Kiến trúc hệ thống GNSS 3 Hình 1 2 Sơ đồ khối bộ thu RF 4 Hình 1 3 Cấu trúc của một thiết bị MOS 5 Hình 1 4 Sự kết nối chất nền 6 Hình 1 5 a thiết bị PMOS đơn giản b PMOS bên trong n well 7 Hình 1 6 Đặc tuyến V A của MOSFET 8 Hình 2 1 Hoạt động của bộ ADC 2 10 Hình 2 2 Đáp ứng của bộ ADC lý tưởng 2 11 Hình 2 3 Sai số độ lệch dương 3 13 Hình 2 4 Sai số khuếch đại dương 3 14 Hình 2 5 Minh họa sai số kích thước bão hòa 3 14 Hình 2 6 Minh họa về độ phi tuyến vi phân 3 15 Hình 2 7 Sai từ mã ở ADC 3 bit do DNL quá lớn 3 16 Hình 2 8 INL của một bộ ADC 3 bit 3 17 Hình 2 9 Spur i ous Free Dy na mi c Range 5 19 Hình 2 10 Kiến trúc bộ ADC truyền thống 6 20 Hình 2 11 Lưu đồ thuật toán bộ kiến trúc ADC đề nghị 22 Hình 2 12 Kiến trúc bộ ADC 4 bit đề nghị 7 23 Hình 2 13 Kiến trúc SAR ADCs đơn giản 9 24 Hình 2 14 Minh họa nhược điểm của SAR ADC so với Flash ADC 26 Hình 2 15 Kiến trúc SAR có khả năng đồng bộ CLK 28 Hình 3 1 Mô hình cơ bản của bộ so sánh 29 Hình 3 2 Sơ đồ khối bộ so sánh 30 Hình 3 3 Đặc tuyến truyền đạt của bộ so sánh 31 Hình 3 4 Các tham số của C om pa ra to r lý tưởng 32 Hình 3 5 Input C om mon Mode Vol ta ge 33 Hình 3 6 Tham số Gain B an dwidth Op amp 34 V Hình 3 7 Tham số slew rate 34 Hình 3 8 Tham số vo l ta ge swing 35 Hình 3 9 Cấu trúc bộ so sánh CMOS SR Latch 37 Hình 3 10 Cơ chế phóng xả của tụ ở M6 9 38 Hình 3 11 Hình minh họa tín hiệu INV1 INV2 của khối CMOS latch 39 Hình 3 12 Kiến trúc co m pa ra to r đồng bộ xung CLK 39 Hình 3 13 Hình minh họa quá trình tạo xung CLK1 từ xung CLK0 40 Hình 4 1 Cấu trúc bộ co m pa ra to r CMOS SR latch 42 Hình 4 2 Quy trình thiết kế cho mạch 4 bit flash ADC dạng nối tiếp 43 Hình 4 3 Cách tính thời gian trễ của mạch 44 Hình 4 4 Ảnh hưởng của Vg1 tới trễ của mạch 45 Hình 4 5 Ảnh hưởng của kích thước số f in ger của M1 tới trễ của mạch 45 Hình 4 6 Xác định số f in ger N2 và N3 của M2 và M3 46 Hình 4 7</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>Minh họa M4 M5 trên CMOS SR latch 47 Hình 4 8 Xác định N4 N5 của M4 M5 47 Hình 4 9 Xác định kích thước của từng f in ger N6 N7 48 Hình 4 10 Xác định kích thước của N8 N9 49 Hình 4 11 Khối NOR2 a và Khối in ve r te r b 50 Hình 4 12 Mạch nguyên lý MUX 21 a và kết quả mô phỏng MUX 2 1 b 51 Hình 4 13 Sơ đồ bộ MUX 41 a và Kết quả mô phỏng MUX 4 1 b 52 Hình 4 14 Sơ đồ bộ MUX 81 a kết quả mô phỏng MUX 81 b 53 Hình 4 15 Mạch nguyên lý của 4 bit flash ADC 54 Hình 4 16 Sử dụng xung ramp tại đầu vào ADC 55 Hình 4 17 Tham số DNL và INL của 4 bit flash ADC dạng nối tiếp 56 Hình 4 18 Kết quả dạng sóng sau khi qua bộ DAC lý tưởng 57 Hình 4 19 Kết quả đạt được sau khi biến đổi Fou ri er 58 Hình 4 20 Hình minh họa thứ tự trên dưới các layer 61 Hình 4 21 Sơ đồ stich di ag ram của khối NAND3 62 Hình 4 22 Mạch nguyên lý cổng login AND ba đầu vào 62 VI Hình 4 23 Hình minh họa sơ đồ share gate khi thiết kế AND3 63 Hình 4 24 Sơ đồ thiết kế AND3 mới mỗi tra n si s to r gồm hai f in ger 63 Hình 4 25 Minh họa các linh kiện CMOS cơ bản 64 Hình 4 26 Thiết kế la you t của khối co m pa ra to r 65 Hình 4 27 Sơ đồ la you t khối mux21 65 Hình 4 28 Sơ đồ la you t khối ADC 66 VII DANH SÁCH BẢNG BIỂU Bảng 2 1 Bảng tổng kết so sánh ưu và nhược điểm giữa các kiến trúc ADC 25 Bảng 3 1 Bảng so sánh tham số của co m pa ra to r lý tưởng và thực tế 32 Bảng 3 2 Bảng trạng thái của SR latch 38 Bảng 4 1 Bảng yêu cầu thiết kế cho cấu trúc 4 bit flash ADC dạng nối tiếp 41 Bảng 4 2 Bảng trạng thái cho bộ MUX 2 1 51 Bảng 4 3 Bảng trạng thái cho bộ MUX 4 1 52 Bảng 4 4 Bảng trạng thái cho bộ MUX 81 53 Bảng 4 5 Bảng các giá trị DNL và INL 55 Bảng 4 6 Bảng kết quả đạt được của mạch 4 bit flash ADC dạng nối tiếp 58 Bảng 4 7 Bảng so sánh các kết quả với các bài báo công bố IEEE 59 Bảng 4 8 so sánh hai cấu trúc 4 bit flash ADC dạng nối tiếp Se ri es Flash ADC và 4 bit flash ADC truyền thống Co ven ti o na l Flash ADC 69 VIII DANH SÁCH CÁC TỪ VIẾT TẮT ADC</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>GNSS GPS RF LNA CMOS MOSFET NMOS A na lo g to Di gi ta I Con ve r te r G lo ba I Na vi ga ti on Sa te I li te Sys tem G lo ba I Po si ti o ni ng Sys tem Radio F re quen cy Low Noise Amp li fier C om p le men ta ry Metal Oxide S em i con du c to r Metal oxide se mi con du c to r Bộ chuyển đổi tương tự số Hệ thống vệ tinh dẫn đường toàn cầu Hệ thống định vị toàn cầu Tần số vô tuyến K hu ếch đại tạp âm thấp Công nghệ sử dụng trong thiết kế IC field effect T ran si s to r cảm ứng</p>	
		<p>https://text.123doc.org/document/4002952-nghien-cuu-va-thiet-ke-ic-chuyen-mach-adc.htm</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
49	2.4. Phân tích so sánh các hệ thống phát hiện xâm nhập	<p>Mặc dù kinh tế c nhiều kh khăn do chịu ảnh hưởng c a cuộc kh ng hoảng kinh tế toàn hoạt động xâm nhập từ các máy chu nghỉ ngò Hệ thống phát hiện xâm nhập mềm Cũng tương tự như trong phần công nghệ cu a IDS Hệ thống phát hiện xâm nhập cứng cisco Cisco cung cấp nhiều loại thiết bị phát hiện xâm nhập co nhiều nền cảm biến cho phép quyết định vị trí tốt nhất để giám sát hoạt động xâm nhập cho hệ thống 2 2 4 Phân loại 2 2 4 1 IPS ngoài luồng P ro mi s cu ous Mode IPS 2 2 4 2 IPS trong luồng In line IPS 2 3 So sánh IDS và IPS 2 3 1 Sự giống nhau 11 Đều là hệ thống phát hiện xâm nhập dùng hệ thống phân cứng hoặc phần mềm co chức năng tự động theo dõi các sự kiện xảy ra trên hệ thống máy tính phân tích để phát hiện ra các vấn đề liên quan đến an ninh bảo mật Khi mà số vụ tấn công đột nhập vào các hệ thống máy tính mạng ngày càng tăng hệ thống phát hiện xâm nhập càng co ý nghĩa 2 2 2 1 Phát hiện sự bất thường 10 2 2 2 2 Kiểm tra lạm phát 2 2 2 3 Kiểm tra các chính sách 2 2 2 4 Phân tích giao thức 2 2 3 Công nghệ Chu động bảo vệ tài nguyên hệ thống mạng là xu hướng mới nhất trong bảo mật Hầu hết các hệ thống phát hiện xâm nhập IDS thụ động giám sát hệ thống cho các dấu hiệu cu a hoạt động xâm nhập Khi hoạt động xâm nhập được phát hiện IDS cung cấp khả năng cho việc pho ng chống kho khăn và hướng giải quyết khi triển khai hệ thống pho ng chống xâm nhập trên một hệ thống mạng thực tế 3 5 2 Nhận xét và đánh giá Ưu điểm Sau khi nghiên cứu tìm hiểu công nghệ pho ng chống xâm nhập IDS IPS qua một trong do ng thiết bị điển hình cu a Cisco IDS 4215 em nhận thấy thiết bị này co khả năng pho ng chống được hầu hết các tấn công trong tầm hiểu biết cu a các hacker bình thường hiện nay cu a các hệ thống IPS Một hệ thống IPS 12 co thể thực hiện nhanh chính xác đưa ra các thông báo hợp lý phân tích được toàn bộ thông lượng cảm biến tối đa ngăn chặn thành công và chính sách quản lý mềm dẻo 2 4 P hư ợn g pháp phát hiện xâm nhập 2 4</p>	74

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>1 Phát hiện dấu hiệu không bình thường Hệ thống phát hiện xâm nhập phải có khả năng phân biệt giữa các hoạt động thông thường của người dùng và hoạt động bất thường</p> <p>http://123doc.org/document/1040698-nghien-cuu-trien-khai-he-thong-phat-hien-va-phong-chong-xam-nhap-ids-ps.htm?page=4</p>	
49	Khả năng phân tích mạng mã hóa	<p>Chức năng phân tích mạng trong công cụ này cũng có khả năng phân tích các giao thức mã hóa như HTTP và SSH 1 và chứa các bộ lọc để nắm bắt thông tin từ một loạt các cơ chế xác thực 1 6</p> <p>https://text.123doc.org/document/4794717-nghien-cuu-mot-so-ky-thuat-be-khoa-mat-khau-va-thu-nghiem-tren-gpu.htm</p>	73
50	Nhận biết một cuộc tấn công có thành công hay không ?	<p>Khác với NIDS hoạt động cùng với các bộ cảm biến sensor có nhiệm vụ giám sát và ngăn chặn các cuộc tấn công trên một network segment hay trên toàn hệ thống mạng HIDS thường được cài đặt và giám sát các hoạt động trên mỗi máy tính độc lập nên nó có thể xác định xem một cuộc tấn công có thành công hay không dựa vào những ảnh hưởng trên hệ thống</p> <p>https://text.123doc.org/document/4079912-bao-cao-ve-snort-tren-window.htm</p>	79
50	Bảo vệ chống lại các cuộc tấn công có chủ đích	<p>Mục tiêu chung của Group IB tại Việt Nam là cung cấp cho các tổ chức chính phủ và doanh nghiệp sự bảo vệ chống lại các cuộc tấn công có chủ đích phần mềm độc hại lỗ hổng zero day và các mối đe dọa mạng khác</p> <p>https://vnreview.vn/headlines-detail/-/headline/co-quan-nha-nuoc-phai-hop-tac-de-phong-chong-nguy-co-bi-tan-cong-mang</p>	100

Trang	Câu trùng lặp	Nguồn	Điểm
50	Sử dụng tài nguyên máy tính của máy chủ	Ngoài ra theo tỷ lệ số lượng người dùng tăng nhiều tài nguyên máy tính của máy chủ là cần thiết gây ra sự khó khăn trong việc nhận ra các đối tượng trong một thời gian thực	73
		https://text.123doc.org/document/4205840-ap-dung-thuat-toan-surf-va-svm-trong-viec-xay-dung-ung-dung-quan-ly-dinh-duong-dua-tren-nen-tang-android.htm	
50	Bổ sung thành phần Không Không Không Không Có Có	Đối với cải tiến về phạm vi đối tượng bảng hỏi của cuộc Điều tra lao động việc làm do TCTK thực hiện năm 2007 đã được thiết kế nhằm Lần đầu tiên ở Việt Nam tính toán được lao động đang làm việc trong khu vực kinh tế phi chính thức và lao động phi chính thức ở qui mô rộng hơn bao gồm cả công việc chính và công việc làm thêm theo đúng định nghĩa do Tổ chức lao động thế giới đưa ra ILO 1993 và 2002 và các đặc tính của nó Xác định sản xuất kinh doanh của hộ và các đơn vị sản xuất phi chính thức để phỏng vấn ở giai đoạn 2 16 Biểu 2 2 Các đặc điểm chính của cuộc Điều tra lao động việc làm do TCTK tiến hành năm 2007 và điều tra biến động dân số nguồn lao động và kế hoạch hoá gia đình 2008 Năm Thời gian điều tra Đối tượng điều tra Thiết kế mẫu Tổng số tỉnh Tổng số đơn vị điều tra Số hộ lý thuyết Số hộ thực tế Số hộ được hỏi lại Nội dung Bảng hỏi Số lượng câu hỏi Thất nghiệp Thiểu việc làm Có việc làm ngành nghề tình trạng công việc Thành phần kinh tế Qui mô doanh nghiệp Thu nhập hàng tháng Công việc phụ Kết quả Xuất bản phẩm Báo cáo kết quả Tài liệu phân tích 2007 Tháng 8 Hộ cá nhân 2008 Tháng 4 Hộ cá nhân 64 5 768 173 040 170 090 Không 64 3 840 380 000 Chưa có Có 1 phần 60 Có Có Có 15 Thị trường lao động Có Có Có Có Có Có Có 1 phần Không Không Không Có Có Chưa có Chưa có Nguồn Điều tra lao động việc làm năm 2007 Điều tra biến động dân số nguồn lao động và kế hoạch hoá gia đình 2008 Tổng cục Thống kê Tính toán của tác giả	71

Trang	Câu trùng lặp	Nguồn	Điểm
		https://text.123doc.org/document/4926711-dieu-tra-lao-dong-viec-lam-o-viet-nam-danh-gia-nhung-cuoc-dieu-tra-da-thuc-hien-va-khuyen-nghi-cho-thiet-ke-cuoc-dieu-tra-moi.htm	

Trang	Câu trùng lặp	Nguồn	Điểm
51	Khả năng thích nghi trong các nền ứng dụng	<p>So sánh giữa NIDS và HIDS Chức năng HIDS NIDS Các đánh giá Cả hai đều bảo vệ khi user hoạt động khi trong mạng LAN Bảo vệ ngoài mạng LAN Dễ dàng cho việc quản trị Tính linh hoạt HIDS là hệ thống linh hoạt hơn Giá thành HIDS là hệ thống ưu tiết kiệm hơn nếu chọn đúng sản phẩm Dễ dàng trong việc bổ sung Đào tạo ngắn hạn cần thiết HIDS yêu cầu việc đào tạo ít hơn NIDS Tổng giá thành HIDS tiêu tốn ít hơn Bảng tần cần yêu cầu trong LAN 0 2 Network o ve r he ad 1 2 Bảng tần cần yêu cầu In te r ne t Các yêu cầu về cổng mở rộng Bảo vệ trong mạng LAN Chu kỳ nâng cấp cho các c li ent Khả năng thích nghi trong các nền ứng dụng Chế độ quét thanh ghi cục bộ Chỉ có HIDS Tương đương như nhau xét về bối cảnh quản trị chung Cả hai tương đương nhau NIDS sử dụng băng tần LAN rộng còn HIDS thì không NIDS cần 2 yêu cầu băng tần mạng đối với bất kỳ mạng LAN nào Cả hai đều cần băng tần In te r ne t để cập nhật kịp thời các file mẫu NIDS yêu cầu phải kích hoạt mở rộng cổng để đảm bảo lưu lượng LAN của bạn được quét HIDS nâng cấp tất cả các c li ent với một file mẫu trung tâm NIDS có khả năng thích nghi trong các nền ứng dụng hơn Chỉ HIDS mới có thể thực hiện các kiểu quét này Bản ghi Cả hai hệ thống đều có chức năng bản ghi Chức năng cảnh báo Cả hai hệ thống đều có chức năng cảnh báo cho từng cá nhân và quản trị viên Quét PAN Chỉ có HIDS quét các vùng mạng cá nhân của bạn Chỉ các tính năng NIDS mới có phương thức này Loại bỏ gói tin 14 Chức năng HIDS NIDS Các đánh giá Kiến thức chuyên môn Cần nhiều kiến thức chuyên môn khi cài đặt và sử dụng NIDS đối với toàn bộ vấn đề bảo mật mạng của bạn Quản lý tập trung NIDS có chiếm ưu thế hơn Khả năng vô hiệu hóa các hệ số rủi ro Khả năng cập nhật Các nút phát hiện nhiều đoạn mạng LAN NIDS có hệ số rủi ro nhiều hơn so với HIDS Rõ ràng khả năng nâng cấp phần mềm là dễ hơn phần cứng</p>	100

Trang	Câu trùng lặp	Nguồn	Điểm
		https://text.123doc.org/document/3816855-he-thong-phong-chong-xam-nhap-mang-snort.htm	
53	3.1.2. Các yêu cầu phần cứng và phần mềm	<p>Tùy từng loại ca me ra mà yêu cầu cấu hình phần cứng và phần mềm khác nhau</p> <p>Hình 2 1 C am e ra 3D Real sen se F200</p> <p>Yêu cầu phần cứng Bộ vi xử lý Intel Core thế hệ thứ 4 Haswell 8GB dung lượng ổ cứng Intel RealSen se C am e ra cổng kết nối USB 3 0 Yêu cần phần mềm Hệ điều hành 64 bit Mic ro so ft W in do ws 8 1 hoặc 10 Mic ro so ft Vi su al S tu di o 2010 2015 với gói cập nhật mới nhất F ra me work Mic ro so ft NET 4 0 dành cho C Unity PRO 4 1 0 Một trong số các phiên bản trình duyệt sau Mic ro so ft In te r ne t Exp lo re r 11 0 9600 12 Mic ro so ft Edge 20 10240 16384 0 Goog le Ch ro me 42 0 2311 Mozil la Fi re fox 37 0 Java JDK 1 7 0 11 O pe nCL 1 2 Các ngôn ngữ lập trình được Intel RealSen se SDK hỗ trợ C C Java Ja va Sc ri pt C UWP 2 2 Thư viện mã nguồn mở SDK Thư viện SDK của ca me ra 3D Intel Real sen se là một thư viện gồm các định nghĩa tiêu chuẩn và các thuật toán nhận diện đối tượng</p> <p>https://text.123doc.org/document/4339436-tim-hieu-camera-3d-ung-dung-lap-trinh-giao-tiep-giua-nguoi-va-may-bang-cac-cu-chi-cua-tay.htm</p>	79

Trang	Câu trùng lặp	Nguồn	Điểm
53	Security Onion chỉ hỗ trợ kiến trúc x86-64.	<p>Tháng tiếp theo trang mạng Ars Technica gửi một bài viết thông báo rằng đội ngũ phát triển KDE muốn chuyển từ KHTML sang WebKit 13 Phát triển sau này sửa sửa mã nguồn Vào tháng 11 năm 2007 dự án thông báo rằng đã hoàn thành hỗ trợ cho các phương tiện chức năng của HTML 5 cho phép các đoạn video nhúng được dựng hình và điều khiển trong WebKit 14 Vào ngày 2 tháng 6 2008 dự án WebKit thông báo rằng họ đã viết lại Ja va Sc ri ptCo re thành S qui r re IFish một trình thông dịch by te co de 15 16 Dự án tiếp tục phát triển nó thành S qui r re IFish Ex tre me viết tắt SFX ra mắt vào ngày 18 tháng 9 2008 hoạt động bằng cách biên dịch Ja va Sc ri pt thành mã máy việc từ bỏ thông dịch by te co de đã giúp tăng tốc các đoạn mã Ja va Sc ri pt 17 Trước đây SFX chỉ hỗ trợ kiến trúc x86 nhưng vào cuối tháng 1 năm 2009 SFX đã có thể chạy trong Mac OS X với kiến trúc x86 64 và nó đã vượt qua tất cả các bài kiểm tra trên nền tảng này 18 Sử dụng sửa sửa mã nguồn WebKit được sử dụng như là một cỗ máy dựng hình cho Safa ri chạy trên Mac OS X W in do ws và iP ho ne OS</p> <p>https://vi.wikipedia.org/wiki/WebKit</p>	73

Trang	Câu trùng lặp	Nguồn	Điểm
	Hình 3.6:Kiểm tra thành phần NIDS.	<p>1 1 2 Phân loại 2 1 3 hội Ưu nhược điểm và tầm quan trọng của gạch không nung đối với vấn đề kinh tế xã 3 1 4 Tình hình sản xuất và sử dụng gạch không nung ở Việt Nam 12 4 1 5 Tình hình sản xuất gạch không nung trên thế giới 12 6 1 6 Mục tiêu của đề tài 7 C h ư ơ n g II CƠ SỞ LÝ THUYẾT 10 2 1 Cơ sở hóa lý 10 2 1 1 Bản chất của chất kết dính xi măng Port lan d XMP 1 10 2 1 1 1 Quá trình đông rắn của XMP 1 10 2 1 2 Bản chất của cốt liệu 13 2 1 3 P h ư ơ n g pháp tạo hình 14 2 1 4 Quy trình bảo dưỡng gạch sau khi tạo hình 2 15 2 2 Cơ sở các phương pháp nghiên cứu 16 2 2 1 Xác định thành phần hóa bằng huỳnh quang tia X XRF 16 2 2 2 Độ hút vôi 16 2 2 3 Xác định thành phần hạt 16 2 2 4 Xác định thành phần hóa bằng phương pháp phổ hồng ngoại IR 17 2 2 5 Xác định thành phần khoáng bằng phương pháp nhiễu xạ tia X XRD 4 17 2 2 6 Phân tích nhiệt vi sai DTA 4 18 2 2 7 Quan sát bề mặt kính hiển vi điện tử quét SEM 4 18 2 2 8 Xác định tính chất cơ lý của sản phẩm 3 18 C h ư ơ n g III NGUYÊN LIỆU 19 3 1 Cốt liệu 19 3 1 1 Bùn đỏ 19 3 1 2 Đá mi 26 iv 3 2 Chất kết dính 26 3 3 Phụ gia 26 C h ư ơ n g IV THỰC NGHIỆM VÀ KẾT QUẢ 31 4 1 Quy trình tiến hành thí nghiệm 31 4 1 1 Sơ đồ chung 31 4 1 2 T h ư y ết minh sơ đồ chung 32 4 2 Thí nghiệm 32 4 2 1 Khảo sát lượng chất kết dính xi măng Hạ Long PCB 40 cần sử dụng 32 4 2 2 Khảo sát độ ẩm tạo hình 34 4 2 3 Khảo sát áp lực ép 35 4 2 3 Xác định pH của bùn đỏ và xỉ than 36 4 2 4 Tính thành phần phối liệu 38 4 2 5 Đo độ bền sản phẩm 39 4 2 5 1 Độ bền uốn 3 39 4 2 5 2 Độ bền nén 3 48 4 2 6 Kiểm tra thành phần khoáng của mẫu có cường độ nén cao 50 4 2 7 Kiểm tra pH của sản sau cùng 51 4 2 7 1 Kiểm tra độ giảm pH của bùn đỏ khi cho xỉ than vào 51 4 2 7 2 So sánh pH của phối liệu ban đầu và pH của sản phẩm 52 C h ư ơ n g V KẾT LUẬN VÀ KIẾN NGHỊ 55 5 1 Kết luận 55 5 2 Kiến nghị 55 TÀI LIỆU THAM KHẢO 57 Phụ lục A Kết quả đo độ hút vôi của xỉ than 58 Phụ lục B Kết quả đo độ bền uốn của các mẫu gạch 59 Phụ</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>lục C Phổ nhiễu xạ tia X 62 v DANH SÁCH HÌNH VẼ Hình 1 1 Một số loại gạch không nung trên thị trường hiện nay 1 Hình 1 2 Một số chủng loại gạch không nung hiện nay 8 Hình 2 1 Cơ chế po ly me r hóa của đất 8 14 Hình 3 1 Các dạng tồn tại của B au xi t trong tự nhiên 20 Hình 3 2 Quy trình luyện nhôm bằng công nghệ Bayer 20 Hình 3 3 Phổ hồng ngoại của bùn đỏ 21 Hình 3 4 Phổ nhiễu xạ tia X của bùn đỏ 22 Hình 3 5 Biểu đồ biểu thị pH của bùn đỏ ứng với từng lượng nước cụ thể 24 Hình 3 6 Kết quả phân tích cỡ hạt của bùn đỏ bằng phương pháp Lazer 25 Hình 3 7 Phổ nhiễu xạ tia X XRD của mẫu xỉ than 28 Hình 4 1 Sơ đồ chung của quá trình tiến hành thí nghiệm 31 Hình 4 2 Biểu đồ biểu thị cường độ uốn của mẫu ứng với từng hàm lượng xi măng 33 Hình 4 3 Biểu đồ biểu thị độ bền uốn của mẫu ứng với từng độ ẩm tạo hình 34 Hình 4 4 Biểu đồ biểu thị độ bền uốn của mẫu ứng với từng áp lực tạo hình mẫu 35 Hình 4 5 Biểu đồ biểu thị pH của bùn đỏ ứng với từng lượng nước cụ thể 36 Hình 4 6 Biểu đồ biểu thị pH của xỉ than ứng với từng lượng nước cụ thể 37 Hình 4 7 Biểu đồ biểu thị độ bền uốn của các mẫu không chứa đá mi ở 8 ngày tuổi 41 Hình 4 8 Biểu đồ biểu thị độ bền uốn của các mẫu có chứa đá mi ở 8 ngày tuổi 42 Hình 4 9 Biểu đồ biểu thị độ bền uốn của mẫu chỉ chứa xi măng và bùn đỏ ở 28 ngày tuổi 43 Hình 4 10 Biểu đồ biểu thị độ bền uốn của các mẫu không chứa đá mi ở 8 ngày tuổi 45 Hình 4 11 Biểu đồ biểu thị độ bền uốn của các mẫu có chứa 1 đá mi ở 28 ngày tuổi 46 Hình 4 12 Biểu đồ biểu thị độ bền uốn của các mẫu có chứa 2 đá mi ở 28 ngày tuổi 47 Hình 4 13 Biểu đồ biểu thị cường độ nén của các tổ mẫu 20 5 1 28 và 20 5 2 28 49 Hình 4 14 Phổ nhiễu xạ tia X của tổ mẫu 20 5 1 28 50 Hình 4 15 Biểu đồ biểu thị pH của 40g bùn đỏ khi tăng lượng xỉ than cho vào 52 vi DANH SÁCH BẢNG BIỂU Bảng 3 1 Các khoáng tồn tại trong quặng B au xi t 19 Bảng 3 2 Thành phần hóa của bùn đỏ 21 Bảng 3 3 pH của bùn đỏ ứng với 100ml nước 23 Bảng 3 4 pH của bùn đỏ</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p> ứng với 200ml nước 23 Bảng 3 5 pH của bùn đỏ ứng với 300ml nước 23 Bảng 3 6 Các thông số kỹ thuật của xi măng Hạ Long PCB 40 26 Bảng 3 7 Thành phần hóa của xỉ 27 Bảng 3 8 Độ hút vôi của xỉ than 29 Bảng 4 1 Cường độ uốn ở 28 ngày tuổi của các mẫu ứng với từng lượng xi măng trong thành phần phối liệu 33 Bảng 4 2 Độ bền uốn của mẫu ứng với từng độ ẩm tạo hình khác nhau 34 Bảng 4 3 Độ bền uốn của mẫu ứng với từng áp lực ép tạo hình 35 Bảng 4 4 pH của bùn đỏ ứng với 100ml nước 36 Bảng 4 5 pH của bùn đỏ ứng với 200ml nước 36 Bảng 4 6 pH của bùn đỏ ứng với 300ml nước 36 Bảng 4 7 pH của xỉ than ứng với 100ml H₂O 37 Bảng 4 8 pH của xỉ than ứng với 200ml H₂O 37 Bảng 4 9 pH của xỉ than ứng với 300ml H₂O 37 Bảng 4 10 Thành phần phối liệu 38 Bảng 4 11 Độ bền uốn trung bình của các mẫu không chứa đá mi ở 8 ngày tuổi 40 Bảng 4 12 Độ bền uốn trung bình của các mẫu có chứa đá mi ở 8 ngày tuổi 41 Bảng 4 13 Độ bền uốn trung bình của các mẫu chỉ chứa xi măng và bùn đỏ ở 28 ngày tuổi 43 Bảng 4 14 Độ bền uốn trung bình của các mẫu không chứa đá mi ở 28 ngày tuổi 44 Bảng 4 15 Độ bền uốn trung bình của các mẫu có chứa 1 đá mi ở 28 ngày tuổi 45 Bảng 4 16 Độ bền uốn trung bình của các mẫu có chứa 2 đá mi ở 28 ngày tuổi 47 Bảng 4 17 Độ bền nén của tổ mẫu 20 5 1 28 49 vii Bảng 4 18 Độ bền nén của tổ mẫu 20 5 2 28 49 Bảng 4 19 pH của 40g bùn đỏ khi tăng lượng xỉ than cho vào 51 Bảng 4 20 pH của phối liệu ban đầu và của sản phẩm có thành phần phối liệu 20 xỉ than 5 xi măng 1 đá mi 42 ngày tuổi 53 Bảng 4 21 pH của phối liệu ban đầu và của sản phẩm có thành phần phối liệu 20 xỉ than 5 xi măng 2 đá mi 42 ngày tuổi 53 viii C hư ơ n g I TỔNG QUAN 1 1 Gạch không nung là gì </p> <p> https://text.123doc.org/document/3924389-nghien-cuu-gach-khong-nung-tu-bun-do-thuyet-minh.htm </p>	

Trang	Câu trùng lặp	Nguồn	Điểm
60	Điều này có thể dẫn đến hậu quả không mong muốn.	<p>trong nghiệp vụ giao nhận và kiểm tra hàng hoá ngay trước khi hàng hoá nhập cảng công ty giao trách nhiệm chuẩn bị chứng từ cho cán bộ nghiệp vụ đối với hợp đồng nhập khẩu trực tiếp công ty thường thuê doanh nghiệp chuyên giao nhận đảm nhiệm cho nên hoàn toàn có thể yên tâm chất lượng đối với các đơn đặt hàng nhập khẩu uỷ thác công ty đã kết hợp được khâu tiếp nhận hàng nhập khẩu với nghiệp vụ giao hàng nâng cao đời sống công nhân viên cụ thể hơn trong quy trình nghiệp vụ nhập khẩu công ty đã có những ưu điểm trong nghiệp vụ mở thư tín dụng công ty thường nhập khẩu theo hình thức uỷ thác cho nên sau khi nhận được thông báo của công ty đơn vị đặt hàng trong nước có trách nhiệm chuyển tiền ký quỹ cho công ty đúng hạn để công ty tiến hành mở l c cho kịp tiến độ giao hàng cho nên công ty không phải quá nhận hàng của ngân hàng doanh nghiệp này sẽ tiến hành vận chuyển lô hàng này về kho của công ty ở xuân đình hoặc hưng yên công ty chỉ việc chuẩn bị kho để nhận hàng và làm thủ tục lưu kho lô hàng đó sau một ngày tiếp nhận và vận chuyển hàng hoá doanh nghiệp vận tải sẽ giao lại toàn bộ các chứng từ giao nhận cần thiết đảm bảo cho tân hồng hà có thể giải quy t nốt các thủ tục còn lại đối với lô hàng nhập tối đa 120 ngày kể từ ngày thh hoàn tất việc giao hàng 2 3 6 khiếu nại và xử lý vi phạm hợp đồng thường trong quá trình giao nhận hàng hoá nếu thấy hàng hoá có dấu hiệu bị tổn thất công ty hoặc các doanh nghiệp thay mặt công ty để nhận hàng sẽ mời công ty giám định để có thể khiếu nại người bán người chuyên chở hay người bảo hiểm khi phát hiện hàng bị đổ vỡ hoặc hư hỏng công ty lập biên bản hàng đồ phòng ở công ty tnhh tân hồng hà như vậy quy trình nghiệp vụ nhập khẩu hàng hoá phải trải qua các bước tuân theo một trình tự và có liên quan chặt chẽ với nhau dù một sai sót nhỏ cũng có thể dẫn đến hậu quả không mong muốn cho nên công ty hoàn thành tốt tất cả các khâu không để một lỗi làm nhỏ xảy ra bất</p>	84

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>đầu từ khâu tiếp nhận hàng hoá điều này giúp cho công tác giao nhận hàng hoá của công ty diễn ra hợp đồng nhập khẩu theo điều kiện c f cho nên bên bán không có nghĩa vụ mua bảo hiểm cho hàng hoá nhưng việc mua bảo hiểm cho hàng hoá là rất cần thiết đặc biệt là hàng hoá vận chuyển bằng đường biển do thiên tai cướp biển việc mua bảo hiểm hàng hoá nhập khẩu giúp công ty chuyển giao rủi ro của mình cho các công ty bảo hiểm mức phí bảo hiểm không cao mà công ty có thể được an tâm khi hàng hoá xảy hiểm khi có tổn thất xảy ra cho nên công ty tiến hành xem xét kỹ lưỡng đảm bảo tính chính xác 2 3 3 làm thủ tục hải quan việc làm thủ tục hải quan cho lô hàng nhập khẩu của công ty tân hồng hà khá đơn giản hàng hoá của công ty thường nhập khẩu theo điều kiện cfr cho nên người bán nước ngoài sẽ tiến hành thuê tàu tiếp theo bên bán sẽ fax chứng từ giao hàng cho công ty và gửi tiếp một bộ chứng từ gốc</p> <p>http://123doc.org/document/685401-chuong-2-phan-tich-quy-trinh-nghiep-vu-nhap-khau-hang-hoa-o-cong-ty-tnhh-tan-hong-ha.htm</p>	
63	Kết quả thu được như hình sau:	<p>Kết quả thu được như hình sau Tuổi Thu nhập Dưới 100 000 Từ 100 000 đến 399 599 Trên 400 000 Dưới 40 6 9 5 Từ 40 đến 54 18 19 8 Trên 54 11 12 17 Với mức ý nghĩa 1 kiểm định giả thiết cho rằng tuổi và mức thu nhập có quan hệ với nhau hay không</p> <p>https://text.123doc.org/document/3038740-bao-cao-bai-tap-lon-xac-suat-thong-ke.htm</p>	100

Trang	Câu trùng lặp	Nguồn	Điểm
	3.3.1.3. Tấn công giao thức FTP	<p> P h ư ơ n g p h á p w a t e r m a r k i n g d ù n g biến đổi Wa ve le ts 61 4 4 1 Lý do dùng phân tích wa ve le t 61 4 4 2 Wa t e r m a r k i n g d ù n g p h â n t í c h w a v e l e t 62 4 4 3 Wa t e r m a r k i n g ả n h s ố d ù n g b i ế n đ ổi Wa v e l e t s 65 4 4 3 1 Q u á t r ì n h n h ứ n g w a t e r m a r k 66 4 4 3 2 Q u á t r ì n h t r í c h w a t e r m a r k 66 4 4 3 3 K i ể m t r a t í n h b ề n v ữ n g 66 C h ư ơ n g V C á c d ạng t ấ n c ồ n g 69 5 1 K h á i q u á t v ề t ấ n c ồ n g 69 v 5 2 V ấ n đ ề b ả o m ậ t 71 5 3 P h ậ n l ọ a i t ấ n c ồ n g c ố ý 71 5 3 1 T ấ n c ồ n g l ọ a i b ỏ R e m o v a l a t a c k 72 5 3 2 T ấ n c ồ n g h ì n h h ọ c G e o m e t r i c a t a c k 73 5 3 3 T ấ n c ồ n g m ã h ố a C r y p t o g r a p h i c a t a c k 73 5 3 4 T ấ n c ồ n g g i ả o t h ứ c P r o t o c o l a t a c k 74 5 4 S ơ l ự c b i ệ n p h á p c h ố n g l ại n h ữ n g k ẻ t ấ n c ồ n g 74 5 5 G i ớ i t h i ệ u v ề c h u ẩ n n én J P E G 76 5 6 G i ớ i t h i ệ u v ề c h u ẩ n n én J P E G 2000 77 C h ư ơ n g 6 G i ả i t h u ậ t m ô p h ồ n g 78 6 1 L ư u đ ồ g i ả i t h u ậ t 78 6 2 C á c b ư ớ c t h ự c h i ệ n 83 C h ư ơ n g 7 K ết q u ả w a t e r m a r k i n g t r ồ n g m i ề n w a v e l e t s 84 7 1 G i ả o d i ệ n c h ư ơ n g t r ì n h 84 7 2 K h ả o s á t q u á t r ì n h w a t e r m a r k i n g t r ồ n g t r ườ n g h ọ p c h ư a b ị t ấ n c ồ n g 87 7 2 1 K h ả o s á t v i ệ c l ự c c h ọ n ả n h w a t e r m a r k 87 7 2 2 K h ả o s á t v i ệ c l ự a c h ọ n k í c h t h ướ c ả n h g ố c 89 7 2 3 K h ả o s á t v i ệ c l ự a c h ọ n b ằ n g t ầ n n h ứ n g 90 7 2 4 K h ả o s á t v i ệ c l ự a c h ọ n c á c h ọ w a v e l e t s 92 7 3 K h ả o s á t ả n h s ầ u w a t e r m a r k i n g b ị t ấ n c ồ n g 95 7 3 1 T ấ n c ồ n g b ằ n g n én J P E G 95 7 3 2 T ấ n c ồ n g b ằ n g n én J P E G 2000 95 7 3 3 T ấ n c ồ n g b ằ n g c á c t h ả o t á c x ử l ý ả n h 96 v i K ết l ư ậ n v à h ướ n g p h á t t r i ể n 99 T ả i l i ệ u t h ầ m k h ả o v i i D A N H M Ụ C C Á C K Ý H I Ệ U C Á C C H Ữ V I Ệ T T Á T C W T C ồ n t i n u ous W a v e l e t T r a n s f o r m B i ế n đ ổi W a v e l e t l i ề n t ự c D C T D i s c r e t e C o s i n e T r a n s f o r m B i ế n đ ổi C o s i n e r ờ i r ặ c D E S D a t a E n c r y p t i o n S t a n d a r d C h u ẩ n m ậ t m ã h ố a d ữ l i ệ u D F T D i s c r e t e F o u r i e r T r a n s f o r m B i ế n đ ổi F o u r i e r r ờ i r ặ c D V D D i g i t a l V e r s a t i l e D i s c Đ ĩa q u ả n g D W T D i s c r e t e W a v e l e t T r a n s f o r m B i ế n đ ổi W a v e l e t r ờ i r ặ c E Z W E m b e d d e d Z e r o t r e e W a v e l e t W a v e l e t c â y z e r o H V S H u m a n v i s u a l s y s t e m H ệ t h ố n g c ầ m n h ậ n n h ìn ở n g ườ i I D W T I n v e r t D i s c r e </p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>te Wa ve le t T ran sform Biến đổi Wa ve le t rời rạc ngược JPEG Joint P ho to g ra phi c Ex pe rts Group Chuẩn nén ảnh JPEG quốc tế JPEG 200 Joint P ho to g ra phi c Ex pe rts Group 2000 Chuẩn nén ảnh JPEG 2000 MRA Multi Re so lu ti on A na ly si s Phân tích đa phân giải MSE Mean S qua re Error Sai số bình phương trung bình PSNR Peak Sig na l to Noise Ratio Tỉ số đỉnh tín hiệu trên nhiễu QMF Quard ra tu re Mir ro r Fil te rs Bộ lọc gương cầu từ phương RSA Ri ve st S ha mi r và Ad lem an P hụ ợn g pháp bảo mật dữ liệu STFT Short Time Fou ri er T ran sform Biến đổi Fou ri er thời gian ngắn WDT Wa ve le t De co mpo si ti on Tree Cây phân giải Wa ve le t viii DANH MỤC CÁC BẢNG Bảng 7 1 Ảnh sau khi nhúng wa te r ma rk tương ứng với 6 ảnh gốc MSE PSNR và các giá trị tương quan với wa te r ma rk là co py ri ght 101 Bảng 7 2 Ảnh wa te r ma rk trích MSE PSNR và hệ số tương quan với wa te r ma rk là Copy ri ght 102 Bảng 7 3 Ảnh sau khi nhúng tương ứng 5 wa te r ma rk khác nhau vào ảnh gốc Lena MSE PSNR và các giá trị tương quan 103 Bảng 7 4 Ảnh sau khi nhúng tương ứng 4 ảnh gốc có kích thước khác nhau MSE PSNR và các giá trị tương quan với wa te r ma rk là S qua re 104 Bảng 7 5 Ảnh sau khi nhúng ảnh s qua re vào ảnh f lo wer MSE PSNR và các giá trị tương quan với các bảng tần nhúng khác nhau 107 Bảng 7 6 Ảnh sau khi nhúng ảnh s qua re vào ảnh f lo wer MSE PSNR và các giá trị tương quan với các hàm phân tích wa ve le t khác nhau 108 Bảng 7 7 Ảnh trích MSE PSNR và tương quan giữa wa te r ma rk trích và wa te r ma rk sau khi tấn công JPEG với các tỉ lệ nén khác nhau của ảnh gốc f lo wer wa te r ma rk là s qua re 110 Bảng 7 8 Ảnh trích MSE PSNR và tương quan giữa wa te r ma rk trích và wa te r ma rk sau khi tấn công JPEG 2000 với các tỉ lệ nén khác nhau của ảnh gốc f lo wer wa te r ma rk là s qua re 111 Bảng 7 9 Ảnh trích MSE PSNR và các hệ số tương quan sau khi tấn công JPEG 2000 sau một số tấn công xử lý ảnh 112 ix DANH MỤC CÁC</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>HÌNH VẼ ĐỒ THỊ Hình 1 1 Mô hình giấu thông tin trong ảnh trang 4 Hình 1 2 Phân loại wa te r ma r ki ng 9 Hình 1 3 Phân loại các thuật toán wa te r ma r ki ng dựa trên miền biến đổi dùng cho quá trình nhúng wa te r ma r ki ng 10 Hình 1 4 Phân loại thuật toán wa te r ma r ki ng dựa vào ứng dụng của wa te r ma r ki ng 11 Hình 2 1 Mô hình giấu dữ liệu dạng tổng quát 15 Hình 2 2 Mô hình tổng quát giai đoạn nhúng dữ liệu 17 Hình 2 3 Mô hình phân phối ảnh wa te r ma r ke d 18 Hình 2 4 Mô hình trích ảnh wa te r ma r ke d 19 Hình 2 5 Mô hình giai đoạn phát hiện wa te r ma rk 20 Hình 2 6 Mô tả độ nhạy tương phản 23 Hình 2 7 Mô tả hàm mật độ chói 24 Hình 2 8 Hiệu ứng Mach band 24 Hình 3 1 Biến đổi Fou ri er 33 Hình 3 2 Biến Đổi Fou ri er thời gian ngắn 35 Hình 3 3 Biến đổi Wa ve le t 38 Hình 3 4 Mô tả các miền biến đổi của tín hiệu 38 Hình 3 5 Sóng sin và wa ve le t 39 Hình 3 6 Các thành phần sóng sin với các tần số khác nhau 40 Hình 3 7 Các thành phần wa ve le t tương ứng với các tỉ lệ và vị trí khác nhau 41 Hình 3 8 Biến đổi wa ve le t rời rạc của tín hiệu 44 Hình 3 9 Quá trình phân tích tín hiệu dùng biến đổi DWT một chiều 44 x Hình 3 10 Minh hoạ DWT hai chiều cho ảnh 45 Hình 3 11 Phân tích tín hiệu đa mức 46 Hình 3 12 Minh hoạ DWT kiểu dya di c mức 3 46 Hình 3 13 Quá trình phân tích và tổng hợp đa mức dùng DWT 47 Hình 3 14 Bộ lọc hai kênh cho dãy mã hóa và giải mã một chiều 48 Hình 3 15 Hàm ψ t của biến đổi Haar 50 Hình 3 16 Hàm ψ t của họ biến đổi D au be chi es n với n 2 3 4 5 51 Hình 3 17 Một vài hàm ψ t của các cặp họ biến đổi Bior tho go na l 52 Hình 3 18 Hàm ψ t của họ biến đổi C oi f le ts 52 Hình 3 19 Một vào hàm ψ t của họ biến đổi Sym le ts 53 Hình 3 20 Hàm ψ t của biến đổi Mor le t 53 Hình 3 21 Hàm ψ t của biến đổi Me xi can Hat 54 Hình 3 22 Hàm ψ t của biến đổi Meyer 54 Hình 4 1 Khối 8x8 ảnh rừng cây 57 Hình 4 2 Sơ đồ khối quá trình tạo wa te r ma rk 59 Hình 4 3 Sơ đồ wa te r ma r ki ng tổng quát dùng Wa ve le t 61 Hình 4 4 Kết quả phân tích DWT ảnh 63 Hình 4 5</p>	

Trang	Câu trùng lặp	Nguồn	Điểm
		<p>Sơ đồ thực hiện nhúng wa te r ma rk 66 Hình 4 6 Sơ đồ thực hiện trích wa te r ma rk 67 Hình 4 7 Sơ đồ mô tả ảnh wa te r ma r ke d trong thực tế 68 Hình 5 1 Các tấn công lên ảnh wa te r ma r ke d 70 Hình 5 2 Phân loại tấn công vô ý 72 Hình 6 1 Lưu đồ giải thuật quá trình nhúng wa te r ma rk 76 xi Hình 6 2 Lưu đồ giải thuật quá trình trích wa te r ma rk 77 Hình 6 3 Lưu đồ giải thuật phân tích wa ve le t 1D đa mức 78 Hình 6 4 Lưu đồ giải thuật khôi phục wa ve le t 1D đa mức 78 Hình 6 5 Lưu đồ giải thuật phân tích wa ve le t 2D đa mức 79 Hình 6 6 Lưu đồ giải thuật khôi phục wa ve le t 2D đa mức 80 Hình 7 1 Giao diện mô phỏng wa te r ma r ki ng ảnh số dùng wa ve le ts 84 Hình 7 2 Quá trình nhúng ảnh co py ri ght vào trong ảnh gốc Lena 85 Hình 7 3 PSNR Cor re la ti on của ảnh nhúng với các băng tần khác nhau 92 Hình 7 4 PSNR Cor re la ti on ảnh nhúng tương ứng với các hàm wa ve le ts khác nhau Haar db1 db2 db3 sym2 bior1 1 bior1 3 94 xii MỞ ĐẦU Sự phát triển của kỹ thuật nén như là nén JPEG MPEG và JPEG 2000 27 31 cho phép sử dụng phổ biến các ứng dụng đa phương tiện</p> <p>https://text.123doc.org/document/2307993-watermarking-dung-wavelets-doi-voi-anh-so.htm</p>	
74	Hướng phát triển của luận văn:	<p>Công khai công tác thiết kế đô thị trên cơ sở lấy ý kiến của cộng đồng dân cư 95 Thành lập Ban quản lý các dự án về thiết kế đô thị cho tuyến và khu vực Khu phố cũ lân cận P hư ơ n g hướng phát triển của luận văn Phạm vi nghiên cứu mới đầu chỉ có tính chất đề xuất các giải pháp cần phải nghiên cứu sâu hơn một số vấn đề Khảo sát khoa học điều tra toàn diện thông qua phiếu ý kiến của người dân tư vấn của chuyên gia</p> <p>https://text.123doc.org/document/4337250-to-chuc-khong-gian-kien-truc-canh-quan-tuyen-duong-van-phuc-quan-ba-dinh-thanh-pho-ha-noi-tt.htm</p>	100

Trang	Câu trùng lặp	Nguồn	Điểm
75	DANH MỤC CÁC TÀI LIỆU THAM KHẢO	Tuy nhiên khó có thể nói rằng thích làm việc với người lãnh đạo uy tín hay làm việc với người lãnh đạo cải cách bởi vì còn tùy thuộc vào hoàn cảnh thực tế tại mỗi thời điểm khác nhau của sự phát triển tổ chức DANH MỤC CÁC TÀI LIỆU THAM KHẢO 1	100
		https://text.123doc.org/document/4392505-bai-tap-phat-trien-kha-nang-lanh-dao-47.htm	
75	Nhà xuất bản Thông tin và Truyền thông, 2020.	Cuốn sách Pháp luật đất đai trong hoạt động nghề luật sư tác giả N gu yễn Minh Hằng chủ biên Nhà xuất bản Thông tin và truyền thông 2013	87
		https://text.123doc.org/document/4306863-hop-dong-chuyen-nhuong-quyen-su-dung-dat-o-theo-phap-luat-hien-hanh-cua-viet-nam.htm	

Trang	Câu trùng lặp	Nguồn	Lý do
-------	---------------	-------	-------