

**ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG**

ĐINH THỊ THÚY HƯỜNG

**NGHIÊN CỨU KỸ THUẬT ĐIỀU TRA SỐ
TRONG GIÁM SÁT AN TOÀN MẠNG MÁY TÍNH
VÀ ỨNG DỤNG**

Chuyên ngành: Khoa học máy tính

Mã số: 8 48 01 01

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

Giáo viên hướng dẫn: TS. Hồ Văn Hương

THÁI NGUYÊN - 2021

LỜI CẢM ƠN

Trong suốt quá trình học tập vừa qua, em đã được quý thầy cô cung cấp và truyền đạt tất cả kiến thức chuyên môn cần thiết và quý giá nhất. Ngoài ra, em còn được rèn luyện một tinh thần học tập và làm việc độc lập và sáng tạo. Đây là tính cách hết sức cần thiết để có thể thành công khi bắt tay vào nghề nghiệp trong tương lai.

Đề tài luận văn thạc sĩ là cơ hội để em có thể áp dụng, tổng kết lại những kiến thức mà mình đã học. Đồng thời, rút ra được những kinh nghiệm thực tế và quý giá trong suốt quá trình thực hiện đề tài. Sau một thời gian em tập trung công sức cho đề tài và làm việc tích cực, đặc biệt là nhờ sự chỉ đạo và hướng dẫn tận tình của **TS Hồ Văn Hương** cùng với các thầy cô trong trường Đại học Công nghệ thông tin & Truyền thông - Đại học Thái Nguyên, đã giúp cho em hoàn thành đề tài một cách thuận lợi và gặt hái được những kết quả mong muốn. Bên cạnh những kết quả khiêm tốn mà em đạt được, chắc chắn không tránh khỏi những thiếu sót khi thực hiện luận văn của mình, kính mong thầy cô thông cảm. Sự phê bình, góp ý của quý thầy cô sẽ là những bài học kinh nghiệm rất quý báu cho công việc thực tế của em sau này.

Em xin chân thành cảm ơn **TS Hồ Văn Hương** đã tận tình giúp đỡ em hoàn thành đề tài này.

Em xin chân thành cảm ơn!

Thái Nguyên, tháng 01 năm 2021

Học viên

Đinh Thị Thúy Hương

LỜI CAM ĐOAN

Em xin cam đoan nội dung luận văn này là do chính em thực hiện, các số liệu thu thập và kết quả phân tích trong báo cáo là trung thực, không sao chép từ bất cứ đề tài nghiên cứu khoa học nào. Nếu sai, em xin hoàn toàn chịu trách nhiệm trước Nhà trường.

Thái Nguyên, tháng 01 năm 2021

Học viên

Đinh Thị Thúy Hương

MỤC LỤC

LỜI CẢM ƠN	i
LỜI CAM ĐOAN	ii
MỤC LỤC.....	iii
DANH MỤC CÁC TỪ VIẾT TẮT	vi
DANH MỤC BẢNG.....	vii
DANH MỤC HÌNH ẢNH	viii
LỜI MỞ ĐẦU	1
1. Tính cấp thiết của đề tài	1
2. Đối tượng và phạm vi nghiên cứu.....	1
3. Hướng nghiên cứu của đề tài	2
4. Những nội dung và bố cục của luận văn	2
5. Phương pháp nghiên cứu.....	3
6. Ý nghĩa khoa học của đề tài	3
CHƯƠNG 1: TỔNG QUAN VỀ ĐIỀU TRA SỐ	4
1.1. Khái niệm về điều tra số.....	4
<i>1.1.1. Khái niệm</i>	<i>4</i>
<i>1.1.2. Mục đích của điều tra số.....</i>	<i>4</i>
<i>1.1.3. Các bước thực hiện điều tra.....</i>	<i>5</i>
<i>1.1.4. Một số loại hình điều tra phổ biến.....</i>	<i>6</i>
1.2. Đặc điểm của điều tra số	10
<i>1.2.1. Tội phạm máy tính.....</i>	<i>10</i>
<i>1.2.2. Bằng chứng số.....</i>	<i>13</i>
<i>1.2.3. Vấn đề pháp lý.....</i>	<i>14</i>
<i>1.2.4 Các loại bằng chứng số.....</i>	<i>15</i>
1.3. Kết luận chương 1	17
CHƯƠNG 2: KỸ THUẬT ĐIỀU TRA SỐ	18
2.1. Chuẩn bị	19

2.2. Bảo vệ và giám định hiện trường.....	22
2.3. Lập tài liệu hiện trường.....	24
2.4 Thu thập bằng chứng.....	24
2.4.1 Thu thập dữ liệu	24
2.4.2 Xác nhận tính toàn vẹn của dữ liệu.....	27
2.4.3 Nhân bản dữ liệu	28
2.4.4 Công cụ sử dụng để thu thập.....	30
2.5. Đánh dấu, vận chuyển và lưu trữ	34
2.6. Kiểm tra.....	34
2.7. Phân tích.....	35
2.8. Thuật toán lọc gói tin	36
2.9. Kết luận chương 2	39
CHƯƠNG 3. ÁP DỤNG KỸ THUẬT ĐIỀU TRA SỐ ĐỂ GIÁM SÁT	
AN TOÀN MẠNG MÁY TÍNH UBND TỈNH QUẢNG NINH.....	40
3.1. Thực trạng và nhu cầu giám sát an toàn mạng máy tính tại UBND tỉnh Quảng Ninh.	40
3.2. Mô tả hệ thống	41
3.2.1. Kiến trúc và thành phần hệ thống.....	43
3.3. Mô hình triển khai	44
3.3.1. Triển khai chủ động	45
3.3.2. Triển khai thụ động	45
3.4. Thực hiện điều tra số dựa trên hệ thống đã mô tả.....	46
3.4.1. Thu thập và tập hợp dữ liệu	47
3.4.2. Sàng lọc, chuẩn hóa và tương quan dữ liệu	47
3.4.3. Phân tích dữ liệu	48
3.4.4. Công cụ phân tích gói tin Wireshark	50
3.5. Thực nghiệm	55
3.5.1. Xác định địa chỉ IP của kẻ tấn công và của nạn nhân.....	56

3.5.2. Xác định số phiên TCP trong file dump.....	57
3.5.3. Xác định thời gian của cuộc tấn công.....	58
3.5.4. Xác định dịch vụ bị tấn công và lỗ hổng trên dịch vụ bị tấn công	58
3.6. Giải mã thông tin trong các gói tin bị mã hóa.....	60
3.7. Mô phỏng lại cuộc tấn công của Hacker	63
3.7.1. Quét cổng 445 để xem cổng này có mở không, điều này thể hiện qua các gói tin SYN, SYN/ACK, ACK, FIN liên tục.....	63
3.7.2. Thiết lập kết nối IPC và request đến SMB.....	64
3.8. Đề xuất xử lý tự động quá trình chặn bắt và phân tích gói tin.....	64
3.9. Kết luận chương 3	67
KẾT LUẬN VÀ ĐỀ NGHỊ	68
TÀI LIỆU THAM KHẢO	70

DANH MỤC CÁC TỪ VIẾT TẮT

Viết tắt	Từ tiếng Anh	Từ tiếng Việt
SHA	Secure Hash Algorithm	Giải thuật băm an toàn
MD5	Message – Digest algorithm 5	Thuật toán hàm băm
PDA	Personal digital assistant	Thiết bị trợ giúp cá nhân
MDS	Maintenance Data System	Hệ thống dữ liệu bảo trì
FAT	File Allocation Table	Bảng định vị tập tin
NTFS	New Technology File System	Hệ thống tập tin công nghệ mới
DNS	Doman Name System	Hệ thống tên miền
NIDS	Network Intrusion Detection System	Hệ thống phát hiện xâm nhập mạng
RAM	Random Access Memory	Bộ nhớ truy cập ngẫu nhiên
NFAT	Network Forensics Analysis Tool	Công cụ phân tích mạng
ARP	Address Resolution Protocol	Giao thức phân giải địa chỉ

DANH MỤC BẢNG

Bảng 2.1: Thiết bị chống ghi phân cứng, phần mềm	21
Bảng 2-2: Công cụ phần mềm giúp thu thập	30
Bảng 2-3: Công cụ phân cứng giúp thu thập	32

DANH MỤC HÌNH ẢNH

Hình 1. Các bước thực hiện điều tra số.....	6
Hình 2. Sử dụng Regshot quan sát sự thay đổi trong Registry.	7
Hình 3.Passware Encryption Analyzer xác định những file được bảo vệ bởi mật khẩu.....	7
Hình 4. Sử dụng Volatility liệt kê các tiến trình đang chạy trên hệ thống	8
Hình 5. Sử dụng Wireshark phân tích tấn công Teadrop.....	9
Hình 6. Sử dụng skypelogview xem dữ liệu được trao đổi qua đường truyền. .9	9
Hình 7. Sử dụng WPDeviceManager để trích xuất SMS.....	10
Hình 8. Quy trình điều tra số.....	19
Hình 9: Mô hình thu thập thông tin.....	27
Hình 10: Lưu đồ thuật toán lọc gói tin.....	37
Hình 11: Hệ thống thu thập thông tin	41
Hình 12: Triển khai chủ động.	45
Hình 13: Quy trình phân tích gói tin.	49
Hình 14: Công cụ Filter.....	52
Hình 15: CTRL+F.....	53
Hình 16. Mô hình thực nghiệm.....	55
Hình 17. Quy trình xác định nguồn gốc và nguyên nhân vụ tấn công	56
Hình 18. Danh sách các gói tin truy cập đến máy nạn nhân.....	57
Hình 19. Danh sách các IP bắt được.	57
Hình 20. Xem số phiên TCP hiện có.	57
Hình 21. Lọc packet theo info.....	58
Hình 22. Một tập luật để phát hiện lỗi MS08-067 trong hệ thống của Suricata	59
Hình 23. Xuất hiện chuỗi dữ liệu “C8 4F 32 4B 70 16 D3 01 12 78 5A 47 BF 6E E1 88”	59
Hình 24. Xuất hiện chuỗi dữ liệu “00 2E 00 2E 00 5C 00 2E 00 2E 00 5C”.	60
Hình 25. Tìm các gói tin bị mã hóa bằng RSA.....	60

Hình 26. Xuất thông tin trong file .der sử dụng rsatool.....	61
Hình 27. Xuất ra modulus n.	61
Hình 28. Chuyển n về hệ thập phân.	62
Hình 29. Phân tích n thành tích của p và q.	62
Hình 30. Tạo ra khóa riêng private key.	62
Hình 31. Nhập thông tin địa chỉ IP của các gói tin cần giải mã và chọn khóa riêng.	63
Hình 32. Thông tin được giải mã thành công.	63
Hình 33. Quá trình quét cổng 445.....	63
Hình 34. Thiết lập kết nối IPC và request.....	64
Hình 35. Sử dụng Tshark bắt gói tin.....	65
Hình 36. Mã nguồn Lua.	66
Hình 37. Mô hình hoạt động của hệ thống phân tích tự động.	67