

BAN CƠ YẾU CHÍNH PHỦ
HỌC VIỆN KỸ THUẬT MẬT MÃ
KHOA CÔNG NGHỆ THÔNG TIN



THỰC TẬP CƠ SỞ CHUYÊN NGÀNH
CÁC KỸ THUẬT ĐẢM BẢO AN TOÀN MẠNG

Ngành: An toàn thông tin

Sinh viên thực hiện:

Đào Hữu Quý – AT160439

Trần Huy Hoàng – AT160423

Nguyễn Bắc Hoàng – AT160422

Người hướng dẫn :

ThS. Cao Thanh Vinh

Hà Nội, 2022

MỤC LỤC

MỤC LỤC	I
DANH MỤC VIẾT TẮT	IV
DANH MỤC HÌNH ẢNH.....	V
LỜI MỞ ĐẦU	1
CHƯƠNG I : TỔNG QUAN VỀ AN NINH MẠNG	2
1.1 SỰ CẦN THIẾT PHẢI CÓ AN NINH MẠNG VÀ CÁC YẾU TỐ BẢO VỆ.....	2
1.2 CÁC TIÊU CHÍ ĐÁNH GIÁ MỨC ĐỘ AN NINH AN TOÀN MẠNG.....	2
1.2.1 Đánh giá trên phương diện vật lý.....	2
1.2.2 Đánh giá trên phương diện logic.....	3
1.3 XÁC ĐỊNH CÁC MỐI ĐE DỌA ĐẾN AN NINH MẠNG.....	5
1.3.1 Mối đe dọa không có cấu trúc (Unstructured threat).....	5
1.3.2 Mối đe dọa có cấu trúc (Structured threat)	5
1.3.3 Mối đe dọa từ bên ngoài (External threat)	6
1.3.4 Mối đe dọa từ bên trong (Internal threat).....	6
1.3.5 Xác định lỗ hổng hệ thống và các nguy cơ.....	6
1.3.5.1 Lỗ hổng hệ thống.....	6
1.3.5.2 Nguy cơ hệ thống.....	7
1.3.5.3 Xác định các lỗ hổng hệ thống	7
1.3.5.4 Xác định các mối đe dọa.....	7
1.3.5.5 Kiểm tra các biện pháp an ninh mạng hiện có.....	7
1.3.6 Nhận dạng các hiểm họa	8
1.3.6.1 Virus.....	8
1.3.6.2 Con ngựa thành Troy(Trojan Horse)	8
1.3.6.3 Sâu mạng-Worm	8
1.3.6.4 Bom logic – Logic Bombs.....	9
1.3.6.5 Adware - advertising-supported software	9
1.3.6.6 Spyware.....	9

1.3.6.7 Backdoor.....	9
CHƯƠNG II : CÁC HIỂM HỌA ĐỐI VỚI AN NINH MẠNG VÀ CÁC KỸ THUẬT ĐẢM BẢO AN TOÀN MẠNG	10
2.1 MỘT SỐ PHƯƠNG PHÁP TẤN CÔNG MẠNG VÀ CÁCH PHÒNG CHỐNG.....	10
2.1.1.1 Phương thức ăn cắp thông tin bằng Packet Sniffers.....	10
2.1.1.2 Phương thức tấn công mật khẩu Password attack.....	11
2.1.1.3 Phương thức tấn công bằng Mail Relay.....	12
2.1.1.4 Phương thức tấn công hệ thống DNS.....	12
2.1.1.5. Phương thức tấn công Man-in-the-middle attack	12
2.1.1.6 Phương thức tấn công để thăm dò mạng.....	13
2.1.1.7 Phương thức tấn công Trust exploitation.....	13
2.1.1.8 Phương thức tấn công Port redirection	13
2.1.1.9 Phương thức tấn công lớp ứng dụng.....	14
2.1.1.10 Phương thức tấn Virus và Trojan Horse	14
2.2 CÁC KỸ THUẬT ĐẢM BẢO AN TOÀN MẠNG	15
2.2.1 Tổng quan về tường lửa	15
2.2.1.1 Ưu điểm của tường lửa.....	16
2.2.1.2 Nhược điểm của tường lửa	16
2.2.2 Hệ thống phát hiện và ngăn chặn xâm nhập	17
2.2.2.1 Tổng quan	17
2.2.2.2 Ưu và nhược điểm của hệ thống phát hiện và ngăn chặn xâm nhập	19
2.2.3 Tổng quan về Honeypot.....	20
2.2.3.1 Tổng quan về honeypot.....	20
2.2.3.2 Ưu và nhược điểm của honeypot	21
CHƯƠNG III : THỰC NGHIỆM	23
3.1 FIRE WALL	23
3.1.1 Mô tả	23
3.1.2 Chuẩn bị	23

3.1.3 Mô hình cài đặt.....	24
3.1.4 Các kịch bản thực hiện.....	24
3.2 HỆ THỐNG PHÁT HIỆN XÂM NHẬP IDS/IPS	27
3.2.1 Mô tả	27
3.2.2 Chuẩn bị	27
3.2.3 Mô hình cài đặt.....	28
3.2.4 Kịch bản thực hiện tấn công và phát hiện	28
3.3 HONEYPOT.....	31
3.3.1 Mô tả	31
3.3.2 Chuẩn bị	32
3.3.3 Mô hình cài đặt.....	32
3.3.4 Các bước cài đặt	32
3.3.5 Thực hiện.....	32
3.4 TRIỂN KHAI HONEYNET SỬ DỤNG HONEYWALL.....	38
3.4.1. Mô tả	38
3.4.2. Chuẩn bị	39
3.4.3 Kịch bản thực hiện	40

DANH MỤC VIẾT TẮT

STT	Ký hiệu chữ viết tắt	Chữ viết đầy đủ
1	ACL	Access Control Lists
2	OTPs	One-Type Password
3	PIN	Personal Identification Number
4	IDS	Intrusion Detection Systems
5	IPS	Intrusion Prevention Systems
6	NIPS	Network-based Intrusion Prevention
7	HIPS	Host-based Intrusion Prevention
8	CDN	Content Delivery Network
9	LAN	Local Area Network
10	DMZ	Demilitarized Zone
11	PING	Packet Internet Groper
12	IP	Internet Protocol
13	DDoS	Distributed Denial of Service
14	NAT	Network Address Translation

DANH MỤC HÌNH ẢNH

Hình 3. 1 Mô hình cài đặt	24
Hình 3. 2 Kiểm tra Ping	25
Hình 3. 3 Kiểm tra tên của các giao diện mạng.....	25
Hình 3. 4 Kiểm tra Ping	26
Hình 3. 5 Dùng lệnh nslookup để truy vấn.....	26
Hình 3. 6 Kiểm tra kết quả.....	27
Hình 3. 7 Mô hình cài đặt	28
Hình 3. 8 Kiểm tra sự hoạt động của snort	28
Hình 3. 9 Hiển thị kết quả.....	29
Hình 3. 10 Hiển thị Ping	30
Hình 3. 11 Kết quả thu được.....	31
Hình 3. 12 Mô hình cài đặt	32
Hình 3. 13 Giao diện máy ảo	33
Hình 3. 14 Dùng lệnh ifconfig	33
Hình 3. 15 Chạy chương trình	33
Hình 3. 16 Giao diện quản lý.....	34
Hình 3. 17 Thử tấn công thăm dò nội bộ	34
Hình 3. 18 Thực hiện dò quét	34
Hình 3. 19 Tấn công từ điển	35
Hình 3. 20 Thực hiện lệnh kết nối tới máy chủ	35
Hình 3. 21 Thực hiện một số lệnh.....	36
Hình 3. 22 Giao diện cho biết mật khẩu và số lượng tin tặc đã sử dụng ..	36
Hình 3. 23 Giao diện này cho biết tài khoản và số lần đăng nhập.....	37

Hình 3. 24 Giao diện này cho biết tài khoản được đăng nhập bởi mật khẩu tương ứng	37
Hình 3. 25 Giao diện này cho biết số lần đăng nhập đúng và sai.....	37
Hình 3. 26 Giao diện này cho biết IP của tin tặc đã sử dụng để xâm nhập vào máy chủ Honeypot.....	38
Hình 3. 27 Phân tích một số lệnh tin tặc đã sử dụng	38
Hình 3. 28 Mô hình chuẩn bị	39
Hình 3. 29 Giao diện đăng nhập quản trị Honeywall	39
Hình 3. 30 Giao diện quản trị Honeywall sau khi đăng nhập.....	40
Hình 3. 31 Sử dụng Nmap để tấn công quét cổng vào máy	40
Hình 3. 32 Giao diện quản trị của Honeywall đã thấy thông tin thu thập được	41
Hình 3. 33 Hình ảnh các kết nối nhận được	42
Hình 3. 34 Kết quả thu được.....	42
Hình 3. 35 Các sự kiện mà IDS cảnh báo	42
Hình 3. 36 Phân tích sâu hơn	43
Hình 3. 37 Tiến trình kết nối.....	43
Hình 3. 38 Các gói tin chứa thông tin tên và phiên bản hệ điều hành của máy	43
Hình 3. 39 Trường hợp 1	44
Hình 3. 40 Trường hợp 3	44
Hình 3. 41 Trường hợp 2	44
Hình 3. 42 Hiển thị thông tin thu thập được	44
Hình 3. 43 Phân tích chi tiết.....	44

Hình 3. 44 Các gói tin chứa thông tin của cách tấn công SQL Injection .	44
Hình 3. 45 Giao diện của hydra attack password	44
Hình 3. 46 Các thông tin hệ thống thu thập được	44
Hình 3. 47 Thông tin chi tiết.....	44
Hình 3. 48 Các gói tin có chứa mật khẩu mà chúng ta dùng hydra tấn công Brute Force máy DVWA	44

LỜI MỞ ĐẦU

Với nhu cầu trao đổi thông tin ngày nay bắt buộc các cá nhân cũng như các cơ quan, tổ chức phải hoà mình vào mạng toàn cầu Internet. An toàn và bảo mật thông tin là một trong những vấn đề quan trọng hàng đầu khi thực hiện kết nối Internet. Ngày nay, các biện pháp an toàn thông tin cho máy tính cá nhân cũng như các mạng nội bộ đã được nghiên cứu và triển khai. Tuy nhiên, vẫn thường xuyên có các mạng bị tấn công, có các tổ chức bị đánh cắp thông tin,...gây nên những hậu quả vô cùng nghiêm trọng. Những vụ tấn công này nhằm vào tất cả các máy tính có mặt trên mạng Internet, đa phần vì mục đích xấu và các cuộc tấn công không được báo trước, số lượng các vụ tấn công tăng lên nhanh chóng và các phương pháp tấn công cũng liên tục được hoàn thiện. Vì vậy việc kết nối một máy tính vào mạng nội bộ cũng như vào mạng Internet cần phải có các biện pháp đảm bảo an ninh. Trong bài báo cáo này, nhóm chúng em tìm hiểu các kiến thức cơ bản về an toàn mạng máy tính, các kỹ thuật đảm bảo an toàn như firewall, hệ thống phát hiện và ngăn chặn xâm nhập, hệ thống honeynet, đồng thời cũng triển khai một số thực nghiệm về các kỹ thuật đảm bảo an toàn mạng.

Trong suốt quá trình nghiên cứu và thực hiện báo cáo, nhóm em đã nhận được sự động viên, giúp đỡ tận tâm của Ths. Cao Thanh Vinh. Nhóm em xin chân thành cảm ơn cô và bày tỏ lòng biết ơn sâu sắc đến cô.

Tuy nhiên, trong quá trình làm báo cáo do còn thiếu nhiều kinh nghiệm nên khi trình bày không tránh những sai sót. Kính mong thầy cô thông cảm và đóng góp ý kiến để báo cáo của nhóm em được hoàn thiện hơn.

Nhóm em xin chân thành cảm ơn!

CHƯƠNG I : TỔNG QUAN VỀ AN NINH MẠNG

1.1 Sự cần thiết phải có an ninh mạng và các yếu tố bảo vệ

Trong hệ thống mạng, vấn đề an toàn và bảo mật một hệ thống thông tin đóng một vai trò hết sức quan trọng. Thông tin chỉ có giá trị khi nó giữ được tính chính xác, thông tin chỉ có tính bảo mật khi chỉ có những người được phép nắm giữ thông tin biết được nó. Khi ta chưa có thông tin, hoặc việc sử dụng hệ thống thông tin chưa phải là phương tiện duy nhất trong quản lý, điều hành thì vấn đề an toàn, bảo mật đôi khi bị xem thường. Nhưng một khi nhìn nhận tới mức độ quan trọng của tính bền hệ thống và giá trị đích thực của thông tin đang có thì chúng ta sẽ có mức độ đánh giá về an toàn và bảo mật hệ thống thông tin. Để đảm bảo được tính an toàn và bảo mật cho một hệ thống cần phải có sự phối hợp giữa các yếu tố phần cứng, phần mềm và con người.

Để thấy được tầm quan trọng của việc đảm bảo an ninh mạng ta tìm hiểu các tác động của việc mất an ninh mạng và từ đó đưa ra các yếu tố cần bảo vệ:

Tác hại của việc không đảm bảo an ninh mạng :

- Làm tổn kém chi phí
- Tổn kém thời gian
- Ảnh hưởng đến tài nguyên hệ thống
- Ảnh hưởng danh dự, uy tín
- Mất cơ hội kinh doanh

Các yếu tố cần bảo vệ :

- Dữ liệu
- Tài nguyên: con người, hệ thống, đường truyền
- Danh tiếng của công ty

1.2 Các tiêu chí đánh giá mức độ an ninh an toàn mạng

Để đảm bảo an ninh an toàn cho mạng, cần phải xây dựng một số tiêu chuẩn đánh giá mức độ an ninh an toàn mạng. Một số tiêu chuẩn đã được thừa nhận là thước đo mức độ an ninh mạng.

1.2.1 Đánh giá trên phương diện vật lý

An toàn thiết bị :

- + Có thiết bị dự phòng nóng cho các tình huống hỏng đột ngột. Có khả năng thay thế nóng từng phần hoặc toàn phần.

- + Khả năng cập nhật, nâng cấp, bổ xung phần cứng và phần mềm.

- + Yêu cầu nguồn điện, có dự phòng trong tình huống mất điện đột ngột

- + Các yêu cầu phù hợp với môi trường xung quanh: độ ẩm, nhiệt độ, chống sét, phòng chống cháy nổ, vv...

An toàn dữ liệu

- + Có các biện pháp sao lưu dữ liệu một cách định kỳ và không định kỳ trong các tình huống phát sinh.

- + Có biện pháp lưu trữ dữ liệu tập trung và phân tán nhằm chia bớt rủi ro trong các trường hợp đặc biệt như cháy nổ, thiên tai, chiến tranh, vv..

1.2.2 Đánh giá trên phương diện logic

Đánh giá theo phương diện này có thể chia thành các yếu tố cơ bản sau:

- + Tính bí mật, tin cậy (Confidentiality)

Là sự bảo vệ dữ liệu truyền đi khỏi những cuộc tấn công bị động. Có thể dùng vài mức bảo vệ để chống lại kiểu tấn công này. Dịch vụ rộng nhất là bảo vệ mọi dữ liệu của người sử dụng truyền giữa hai người dùng trong một khoảng thời gian. Nếu một kênh ảo được thiết lập giữa hai hệ thống, mức bảo vệ rộng sẽ ngăn chặn sự rò rỉ của bất kỳ dữ liệu nào truyền trên kênh đó.

Cấu trúc hẹp hơn của dịch vụ này bao gồm việc bảo vệ một bản tin riêng lẻ hay những trường hợp cụ thể bên trong một bản tin. Khía cạnh khác của tin bí mật là việc bảo vệ lưu lượng khỏi việc phân tích.

Điều này làm cho những kẻ tấn công không thể quan sát được tần suất, độ dài của nguồn và đích hoặc những đặc điểm khác của lưu lượng trên một phương tiện giao tiếp.

- + Tính xác thực (Authentication)

Liên quan tới việc đảm bảo rằng một cuộc trao đổi thông tin là đáng tin cậy. Trong trường hợp một bản tin đơn lẻ, ví dụ như một tín hiệu báo động hay cảnh báo, chức năng của dịch vụ ủy quyền là đảm bảo bên nhận rằng bản tin là từ nguồn mà nó xác nhận là đúng.

Trong trường hợp một tương tác đang xảy ra, ví dụ kết nối của một đầu cuối đến máy chủ, có hai vấn đề sau: thứ nhất tại thời điểm khởi tạo kết nối, dịch vụ

đảm bảo rằng hai thực thể là đáng tin. Mỗi chúng là một thực thể được xác nhận. Thứ hai, dịch vụ cần phải đảm bảo rằng kết nối là không bị gây nhiễu do một thực thể thứ ba có thể giả mạo là một trong hai thực thể hợp pháp để truyền tin hoặc nhận tin không được cho phép.

+ Tính toàn vẹn (Integrity)

Cùng với tính bí mật, toàn vẹn có thể áp dụng cho một luồng các bản tin, một bản tin riêng biệt hoặc những trường lựa chọn trong bản tin. Một lần nữa, phương thức có ích nhất và dễ dàng nhất là bảo vệ toàn bộ luồng dữ liệu.

Một dịch vụ toàn vẹn hướng kết nối, liên quan tới luồng dữ liệu, đảm bảo rằng các bản tin nhận được cũng như gửi không có sự trùng lặp, chèn, sửa, hoán vị hoặc tái sử dụng. Việc hủy dữ liệu này cũng được bao gồm trong dịch vụ này. Vì vậy, dịch vụ toàn vẹn hướng kết nối phá hủy được cả sự thay đổi luồng dữ liệu và cả từ chối dữ liệu. Mặt khác, một dịch vụ toàn vẹn không kết nối, liên quan tới từng bản tin riêng lẻ, không quan tâm tới bất kỳ một hoàn cảnh rộng nào, chỉ cung cấp sự bảo vệ chống lại sửa đổi bản tin.

Chúng ta có thể phân biệt giữa dịch vụ có và không có phục hồi. Bởi vì dịch vụ toàn vẹn liên quan tới tấn công chủ động, chúng ta quan tâm tới phát hiện hơn là ngăn chặn. Nếu một sự vi phạm toàn vẹn được phát hiện, thì phần dịch vụ đơn giản là báo cáo sự vi phạm này và một vài những phần của phần mềm hoặc sự ngăn chặn của con người sẽ được yêu cầu để khôi phục từ những vi phạm đó. Có những cơ chế giành sẵn để khôi phục lại những mất mát của việc toàn vẹn dữ liệu.

+ Không thể phủ nhận (Non repudiation)

Tính không thể phủ nhận bảo đảm rằng người gửi và người nhận không thể chối bỏ 1 bản tin đã được truyền. Vì vậy, khi một bản tin được gửi đi, bên nhận có thể chứng minh được rằng bản tin đó thật sự được gửi từ người gửi hợp pháp. Hoàn toàn tương tự, khi một bản tin được nhận, bên gửi có thể chứng minh được bản tin đó đúng thật được nhận bởi người nhận hợp lệ.

+ Khả năng điều khiển truy nhập (Access Control)

Trong hoàn cảnh của an ninh mạng, điều khiển truy cập là khả năng hạn chế các truy nhập tới máy chủ thông qua đường truyền thông. Để đạt được việc điều khiển này, mỗi một thực thể cố gắng đạt được quyền truy nhập cần phải được nhận diện, hoặc được xác nhận sao cho quyền truy nhập có thể được đáp ứng nhu cầu đối với từng người.

+ Tính khả dụng, sẵn sàng (Availability)

Một hệ thống đảm bảo tính sẵn sàng có nghĩa là có thể truy nhập dữ liệu bất cứ lúc nào mong muốn trong vòng một khoảng thời gian cho phép. Các cuộc tấn công khác nhau có thể tạo ra sự mất mát hoặc thiếu về sự sẵn sàng của dịch vụ. Tính khả dụng của dịch vụ thể hiện khả năng ngăn chặn và khôi phục những tổn thất của hệ thống do các cuộc tấn công gây ra.

1.3 Xác định các mối đe dọa đến an ninh mạng

1.3.1 Mối đe dọa không có cấu trúc (Unstructured threat)

Công cụ hack và script có rất nhiều trên Internet, vì thế bất cứ ai tò mò có thể tải chúng về và sử dụng thử trên mạng nội bộ và các mạng ở xa. Cũng có những người thích thú với việc xâm nhập vào máy tính và các hành động vượt khỏi tầm bảo vệ. Hầu hết tấn công không có cấu trúc đều được gây ra bởi Script Kiddies (những kẻ tấn công chỉ sử dụng các công cụ được cung cấp, không có hoặc có ít khả năng lập trình) hay những người có trình độ vừa phải. Hầu hết các cuộc tấn công đó vì sở thích cá nhân, nhưng cũng có nhiều cuộc tấn công có ý đồ xấu. Những trường hợp đó có ảnh hưởng xấu đến hệ thống và hình ảnh của công ty.

Mặc dù tính chuyên môn của các cuộc tấn công dạng này không cao nhưng nó vẫn có thể phá hoại hoạt động của công ty và là một mối nguy hại lớn. Đôi khi chỉ cần chạy một đoạn mã là có thể phá hủy chức năng mạng của công ty. Một Script Kiddies có thể không nhận ra và sử dụng đoạn mã tấn công.

1.3.2 Mối đe dọa có cấu trúc (Structured threat)

Structured threat là các hành động cố ý, có động cơ và kỹ thuật cao. Không như Script Kiddies, những kẻ tấn công này có đủ kỹ năng để hiểu các công cụ, có thể chỉnh sửa các công cụ hiện tại cũng như tạo ra các công cụ mới. Những kẻ tấn công này hoạt động độc lập hoặc theo nhóm, họ hiểu, phát triển và sử dụng các kỹ thuật hack phức tạp nhằm xâm nhập vào mục tiêu.

Động cơ của các cuộc tấn công này thì có rất nhiều. Một số yếu tố thường thấy có thể vì tiền, hoạt động chính trị, tức giận hay báo thù. Các tổ chức tội phạm, các đối thủ cạnh tranh hay các tổ chức sắc tộc có thể thuê các chuyên gia để thực hiện các cuộc tấn công dạng structured threat. Các cuộc tấn công này thường có mục đích từ trước, như để lấy được mã nguồn của đối thủ cạnh tranh. Cho dù động cơ là gì, thì các cuộc tấn công như vậy có thể gây hậu quả nghiêm trọng cho hệ thống. Một cuộc tấn công structured thành công có thể gây nên sự phá hủy cho toàn hệ thống.

1.3.3 Mối đe dọa từ bên ngoài (External threat)

External threat là các cuộc tấn công được tạo ra khi không có một quyền nào trong hệ thống. Người dùng trên toàn thế giới thông qua Internet đều có thể thực hiện các cuộc tấn công như vậy.

Các hệ thống bảo vệ vành đai là tuyến bảo vệ đầu tiên chống lại external threat. Bằng cách gia tăng hệ thống bảo vệ vành đai, ta có thể giảm tác động của kiểu tấn công này xuống tối thiểu. Mối đe dọa từ bên ngoài là mối đe dọa mà các công ty thường phải bỏ nhiều tiền và thời gian để ngăn ngừa.

1.3.4 Mối đe dọa từ bên trong (Internal threat)

Thuật ngữ “Mối đe dọa từ bên trong” được sử dụng để mô tả một kiểu tấn công được thực hiện từ một người hoặc một tổ chức có một vài quyền truy cập mạng của chúng ta. Các cách tấn công từ bên trong được thực hiện từ một khu vực được tin cậy trong mạng. Mối đe dọa này có thể khó phòng chống hơn vì các nhân viên có thể truy cập mạng và dữ liệu bí mật của công ty. Hầu hết các công ty chỉ có các tường lửa ở đường biên của mạng, và họ tin tưởng hoàn toàn vào các ACL (Access Control Lists) và quyền truy cập server để quy định cho sự bảo mật bên trong. Quyền truy cập server thường bảo vệ tài nguyên trên server nhưng không cung cấp bất kỳ sự bảo vệ nào cho mạng. Mối đe dọa ở bên trong thường được thực hiện bởi các nhân viên bất bình, muốn “quay mặt” lại với công ty. Nhiều phương pháp bảo mật liên quan đến vành đai của mạng, bảo vệ mạng bên trong khỏi các kết nối bên ngoài, như là Internet. Khi vành đai của mạng được bảo mật, các phần tin cậy bên trong có khuynh hướng bị bớt nghiêm ngặt hơn. Khi một kẻ xâm nhập vượt qua vỏ bọc bảo mật cứng cáp đó của mạng, mọi chuyện còn lại thường là rất đơn giản. Đôi khi các cuộc tấn công dạng structured vào hệ thống được thực hiện với sự giúp đỡ của người bên trong hệ thống. Trong trường hợp đó, kẻ tấn công trở thành structured internal threat, kẻ tấn công có thể gây hại nghiêm trọng cho hệ thống và ăn trộm tài nguyên quan trọng của công ty. Structured internal threat là kiểu tấn công nguy hiểm nhất cho mọi hệ thống.

1.3.5 Xác định lỗ hổng hệ thống và các nguy cơ

1.3.5.1 Lỗ hổng hệ thống

Lỗ hổng hệ thống là nơi mà đối tượng tấn công có thể khai thác để thực hiện các hành vi tấn công hệ thống. Lỗ hổng hệ thống có thể tồn tại trong hệ thống mạng hoặc trong thủ tục quản trị mạng. Ví dụ :

- Lỗ hổng lập trình (back-door)

- Lỗ hổng Hệ điều hành
- Lỗ hổng ứng dụng
- Lỗ hổng vật lý
- Lỗ hổng trong thủ tục quản lý (mật khẩu, chia sẻ,...)

1.3.5.2 Nguy cơ hệ thống

Nguy cơ hệ thống được hình thành bởi sự kết hợp giữa lỗ hổng hệ thống, các mối đe dọa đến hệ thống và các biện pháp an toàn hệ thống hiện có

Nguy cơ = Mối đe dọa + Lỗ hổng hệ thống + Các biện pháp an toàn hiện có

1.3.5.3 Xác định các lỗ hổng hệ thống

Việc xác định các lỗ hổng hệ thống được bắt đầu từ các điểm truy cập vào hệ thống như:

- Kết nối mạng Internet
- Các điểm kết nối từ xa
- Kết nối đến các tổ chức khác
- Các môi trường truy cập vật lý đến hệ thống
- Các điểm truy cập người dùng
- Các điểm truy cập không dây

1.3.5.4 Xác định các mối đe dọa

Việc xác định các mối đe dọa là rất khó khăn vì các lý do:

- Các mối đe dọa thường không xuất hiện rõ ràng
- Các hình thức và kỹ thuật tấn công đa dạng:
- DoS/DDoS, BackDoor, Tràn bộ đệm,... Virus, Trojan Horse, Worm Social Engineering
- Thời điểm tấn công không biết trước
- Qui mô tấn công không biết trước

1.3.5.5 Kiểm tra các biện pháp an ninh mạng hiện có

Các biện pháp an ninh gồm các loại sau:

- Bức tường lửa - Firewall
- Phần mềm diệt virus

- Điều khiển truy nhập
- Hệ thống chứng thực (mật khẩu, sinh trắc học, thẻ nhận dạng,...)
- Mã hóa dữ liệu
- Hệ thống dò xâm nhập IDS
- Các kỹ thuật khác: AD, VPN, NAT
- Ý thức người sử dụng
- Hệ thống chính sách bảo mật và tự động vá lỗi hệ thống

1.3.6 Nhận dạng các hiểm họa

1.3.6.1 Virus

Virus máy tính là một chương trình có thể tự động nhân bản. Chương trình nguồn Virus và các bản copy của nó có thể tự biến thể. Virus chỉ có thể lây nhiễm từ máy này sang máy khác khi máy tính có giao tiếp với nguồn gây bệnh thông qua các phương thức trao đổi dữ liệu như qua đĩa mềm, CD hoặc USB, đặc biệt trong trường hợp trao đổi qua hệ thống mạng.

1.3.6.2 Con ngựa thành Troy (Trojan Horse)

Trojan là một file xuất hiện một cách vô hại trước khi thi hành. Trái ngược với Virus Trojan không chèn các đoạn mã lệnh vào các file khác. Trojan thường được gắn vào các chương trình trò chơi hoặc phần mềm miễn phí, vô thưởng vô phạt. Khi một ứng dụng được thực thi thì Trojan cũng đồng thời thực hiện nhiệm vụ của nó. Nhiều máy tính cá nhân khi kết nối Internet là điều kiện thuận lợi để bị lây nhiễm Trojan. Ngày nay Trojan được cài đặt như là một bộ phận của phần mềm thâm nhập vào cửa sau của hệ thống và từ đó phát hiện các lỗ hổng bảo mật.

1.3.6.3 Sâu mạng-Worm

Sâu mạng Worm có thể lây nhiễm tự động từ máy này sang máy khác không nhất thiết phải dịch chuyển như là một bộ phận của host. Worm là chương trình có thể tự tái tạo thông qua giao dịch tìm kiếm các file đã bị lây nhiễm của hệ điều hành. Hiện nay Worm thường lây nhiễm qua đường thư điện tử, Worm tự động nhân bản và gửi đến các địa chỉ trong danh mục địa chỉ thư của người dùng. Worm cũng có thể lây nhiễm thông qua việc download file, sự nguy hiểm của Worm là nó có thể làm vô hiệu hoá các chương trình diệt virus và các biện pháp an ninh như là việc ăn cắp mật khẩu,...

1.3.6.4 Bom logic – Logic Bombs

Bom Logic là một đoạn mã lệnh ngoại lai được chèn vào hệ thống phần mềm có mục đích phá hoại được cài đặt ở chế độ tắt, khi gặp điều kiện thuận lợi sẽ được kích hoạt để phá hoại. Ví dụ người lập trình sẽ cài ẩn vào phần mềm của mình đoạn mã lệnh xóa file nếu trong quá trình sử dụng khách hàng không trả phí. Thông thường logic Bombs được kích hoạt theo chế độ giới hạn thời gian. Các kỹ thuật này cũng được sử dụng trong các chương trình Virus và Worm hoặc các Trojan được kích hoạt đồng loạt tại một thời điểm nào đó gọi là “Time bombs”.

1.3.6.5 Adware - advertising-supported software

Adware hay còn gọi là phần mềm hỗ trợ quảng cáo là một gói phần mềm tự động thực hiện, trình diễn hoặc tải về các chương trình quảng cáo sau khi được kích hoạt.

1.3.6.6 Spyware

Spyware là phần mềm máy tính dùng để thu thập các thông tin của cá nhân không được sự chấp thuận của họ. Thuật ngữ Spyware xuất hiện năm 1995 và được phổ biến rộng rãi sau đó 5 năm. Thông tin cá nhân bao gồm hệ thống khoá truy cập (username, password, ...), địa chỉ các trang Web thường xuyên truy cập, các thông tin được lưu trữ trên đĩa cứng của máy tính cá nhân... Spyware thường dùng phương thức đánh lừa khi khai báo để truy cập vào trang Web nào đó, đặc biệt là các thông tin mật, số PIN của thẻ tín dụng, số điện thoại,...

1.3.6.7 Backdoor

Backdoor là một giải pháp tìm đường vòng để truy cập từ xa vào hệ thống được đảm bảo an ninh một cách vô hình từ sự cầu thả quá trình kiểm duyệt. Backdoor có thể được đặt kèm theo chương trình hoặc biến đổi từ một chương trình hợp pháp.

CHƯƠNG II : CÁC HIỂM HỌA ĐỐI VỚI AN NINH MẠNG VÀ CÁC KỸ THUẬT ĐẢM BẢO AN TOÀN MẠNG

2.1 Một số phương pháp tấn công mạng và cách phòng chống

2.1.1.1 Phương thức ăn cắp thông tin bằng Packet Sniffers

Đây là một chương trình ứng dụng bắt giữ được tất cả các gói lưu chuyển trên mạng (trên một collision domain). Sniffer thường được dùng cho troubleshooting network hoặc để phân tích traffic. Tuy nhiên, do một số ứng dụng gửi dữ liệu qua mạng dưới dạng clear text (telnet, FTP, SMTP, POP3,...) nên sniffer cũng là một công cụ cho hacker để bắt các thông tin nhạy cảm như là username, password, và từ đó có thể truy xuất vào các thành phần khác của mạng.

Khả năng thực hiện Packet Sniffers có thể xảy ra từ trong các Segment của mạng nội bộ, các kết nối RAS hoặc phát sinh trong WAN.

Ta có thể cấm packet sniffer bằng một số cách như sau:

- Authentication

Kỹ thuật xác thực này được thực hiện phổ biến như one-type password (OTPs). Kỹ thuật này được thực hiện bao gồm hai yếu tố: personal identification number (PIN) và token card (token card là thiết bị phần cứng hoặc phần mềm sản sinh ra thông tin một cách ngẫu nhiên (password) tại một thời điểm, thường là 60 giây.) để xác thực một thiết bị hoặc một phần mềm ứng dụng.

Khách hàng sẽ kết nối password đó với một PIN để tạo ra một password duy nhất. Giả sử một hacker học được password đó bằng kỹ thuật packet sniffers, thông tin đó cũng không có giá trị vì nó đã hết hạn.

- Dùng switch thay vì Bridge hay hub: hạn chế được các gói broadcast trong mạng.

Kỹ thuật này có thể dùng để ngăn chặn packet sniffers trong môi trường mạng. Vd: nếu toàn bộ hệ thống sử dụng switch ethernet, hacker chỉ có thể xâm nhập vào luồng traffic đang lưu thông tại 1 host mà hacker kết nối đến. Kỹ thuật này không làm ngăn chặn hoàn toàn packet sniffer nhưng nó có thể giảm được tầm ảnh hưởng của nó.

Các công cụ Anti-sniffer: công cụ này phát hiện sự có mặt của packet siffer trên mạng.

Mã hóa: Tất cả các thông tin lưu chuyển trên mạng đều được mã hóa. Khi đó, nếu hacker dùng packet sniffer thì chỉ bắt được các gói dữ liệu đã được mã hóa. Cisco dùng giao thức IPSec để mã hóa

2.1.1.2 Phương thức tấn công mật khẩu Password attack

Các hacker tấn công password bằng một số phương pháp như: brute- force attack, chương trình Trojan Horse, IP spoofing, và packet sniffer. Mặc dù dùng packet sniffer và IP spoofing có thể lấy được user account và password, nhưng hacker lại thường sử dụng brute-force để lấy user account hơn.

Tấn công brute-force được thực hiện bằng cách dùng một chương trình chạy trên mạng, cố gắng login vào các phần share trên server bằng phương pháp “thử và sai” password.

- Khả năng thực hiện Packet Sniffers có thể xảy ra từ trong các Segment của mạng nội bộ, các kết nối RAS hoặc phát sinh trong WAN.

Ta có thể cấm packet sniffer bằng một số cách như sau: Authentication

Kỹ thuật xác thực này được thực hiện phổ biến như one-type password (OTPs). Kỹ thuật này được thực hiện bao gồm hai yếu tố: personal identification number (PIN) và token card để xác thực một thiết bị hoặc một phần mềm ứng dụng.

Token card là thiết bị phần cứng hoặc phần mềm sản sinh ra thông tin một cách ngẫu nhiên (password) tại một thời điểm, thường là 60 giây.

Khách hàng sẽ kết nối password đó với một PIN để tạo ra một password duy nhất. Giả sử một hacker học được password đó bằng kỹ thuật packet sniffers, thông tin đó cũng không có giá trị vì nó đã hết hạn.

Dùng switch thay vì Bridge hay hub: hạn chế được các gói broadcast trong mạng.

Kỹ thuật này có thể dùng để ngăn chặn packet sniffers trong môi trường mạng. Vd: nếu toàn bộ hệ thống sử dụng switch ethernet, hacker chỉ có thể xâm nhập vào luồng traffic đang lưu thông tại 1 host mà hacker kết nối đến. Kỹ thuật này không làm ngăn chặn hoàn toàn packet sniffer nhưng nó có thể giảm được tầm ảnh hưởng của nó.

Các công cụ Anti-sniffer: công cụ này phát hiện sự có mặt của packet siffer trên mạng.

Mã hóa: Tất cả các thông tin lưu chuyển trên mạng đều được mã hóa. Khi đó, nếu hacker dùng packet sniffer thì chỉ bắt được các gói dữ liệu đã được mã hóa. Cisco dùng giao thức IPSec để mã hoá dữ liệu.

2.1.1.3 Phương thức tấn công bằng Mail Relay

Đây là phương pháp phổ biến hiện nay. Email server nếu cấu hình không chuẩn hoặc Username/ password của user sử dụng mail bị lộ. Hacker có thể lợi dụng email server để gửi mail gây ngập mạng, phá hoại hệ thống email khác. Ngoài ra với hình thức gắn thêm các đoạn script trong mail hacker có thể gây ra các cuộc tấn công Spam cùng lúc với khả năng tấn công gián tiếp đến các máy chủ Database nội bộ hoặc các cuộc tấn công D.o.S vào một mục tiêu nào đó.

Phương pháp giảm thiểu :

- Giới hạn dung lượng Mail box.
- Sử dụng các phương thức chống Relay Spam bằng các công cụ bảo mật cho SMTP server, đặt password cho SMTP.
- Sử dụng gateway SMTP riêng.

2.1.1.4 Phương thức tấn công hệ thống DNS

DNS Server là điểm yếu nhất trong toàn bộ các loại máy chủ ứng dụng và cũng là hệ thống quan trọng nhất trong hệ thống máy chủ

- Việc tấn công và chiếm quyền điều khiển máy chủ phục vụ DNS là một sự phá hoại nguy hiểm liên quan đến toàn bộ hoạt động của hệ thống truyền thông trên mạng.
- Hạn chế tối đa các dịch vụ khác trên hệ thống máy chủ DNS Cài đặt hệ thống IDS Host cho hệ thống DNS
- Luôn cập nhật phiên bản mới có sửa lỗi của hệ thống phần mềm DNS.
- Phương pháp hạn chế:
- Hạn chế tối đa các dịch vụ khác trên hệ thống máy chủ DNS. Cài đặt hệ thống IDS Host cho hệ thống DNS.
- Luôn cập nhật phiên bản mới có sửa lỗi của hệ thống phần mềm DNS

2.1.1.5. Phương thức tấn công Man-in-the-middle attack

Dạng tấn công này đòi hỏi hacker phải truy nhập được các gói mạng của mạng. Một ví dụ về tấn công này là một người làm việc tại ISP, có thể bắt được

tất cả các gói mạng của công ty khách hàng cũng như tất cả các gói mạng của các công ty khác thuê Leased line đến ISP đó để ăn cắp thông tin hoặc tiếp tục session truy nhập vào mạng riêng của công ty khách hàng. Tấn công dạng này được thực hiện nhờ một packet sniffer.

Tấn công dạng này có thể hạn chế bằng cách mã hoá dữ liệu được gửi đi ra. Nếu các hacker có bắt được các gói dữ liệu thì là các dữ liệu đã được mã hóa.

2.1.1.6 Phương thức tấn công để thăm dò mạng

Thăm dò mạng là tất cả các hoạt động nhằm mục đích lấy các thông tin về mạng. Khi một hacker cố gắng chọc thủng một mạng, thường thì họ phải thu thập được thông tin về mạng càng nhiều càng tốt trước khi tấn công. Điều này có thể thực hiện bởi các công cụ như DNS queries, ping sweep, hay port scan.

Ta không thể ngăn chặn được hoàn toàn các hoạt động thăm dò kiểu như vậy. Ví dụ ta có thể tắt đi ICMP echo và echo-reply, khi đó có thể chặn được ping sweep, nhưng lại khó cho ta khi mạng có sự cố, cần phải chẩn đoán lỗi do đâu.

NIDS và HIDS giúp nhắc nhở (notify) khi có các hoạt động thăm dò xảy ra trong mạng.

2.1.1.7 Phương thức tấn công Trust exploitation

Loại tấn công kiểu này được thực hiện bằng cách tận dụng mối quan hệ tin cậy đối với mạng. Một ví dụ cho tấn công kiểu này là bên ngoài firewall có một quan hệ tin cậy với hệ thống bên trong firewall. Khi bên ngoài hệ thống bị xâm hại, các hacker có thể lần theo quan hệ đó để tấn công vào bên trong firewall.

Có thể giới hạn các tấn công kiểu này bằng cách tạo ra các mức truy xuất khác nhau vào mạng và quy định chặt chẽ mức truy xuất nào sẽ được truy xuất vào các tài nguyên nào của mạng.

2.1.1.8 Phương thức tấn công Port redirection

Tấn công này là một loại của tấn công trust exploitation, lợi dụng một host đã bị đột nhập đi qua firewall. Ví dụ, một firewall có 3 interface, một host ở outside có thể truy nhập được một host trên DMZ, nhưng không thể vào được host ở inside. Host ở DMZ có thể vào được host ở inside, cũng như outside. Nếu hacker chọc thủng được host trên DMZ, họ có thể cài phần mềm trên host của DMZ để bẻ hướng traffic từ host outside đến host inside.

Ta ngăn chặn tấn công loại này bằng cách sử dụng HIDS cài trên mỗi server. HIDS có thể giúp phát hiện được các chương trình lạ hoạt động trên server đó.

2.1.1.9 Phương thức tấn công lớp ứng dụng

Tấn công lớp ứng dụng được thực hiện bằng nhiều cách khác nhau. Một trong những cách thông dụng nhất là tấn công vào các điểm yếu của phần mềm như sendmail, HTTP, hay FTP.

Nguyên nhân chủ yếu của các tấn công lớp ứng dụng này là chúng sử dụng những port cho qua bởi firewall. Ví dụ các hacker tấn công Web server bằng cách sử dụng TCP port 80, mail server bằng TCP port 25.

Một số phương cách để hạn chế tấn công lớp ứng dụng: Lưu lại log file, và thường xuyên phân tích log file.

Luôn cập nhật các patch cho OS và các ứng dụng. Dùng IDS, có 2 loại IDS:

- + HIDS: cài đặt trên mỗi server một agent của HIDS để phát hiện các tấn công lên server đó.
- + NIDS: xem xét tất cả các packet trên mạng (collision domain). Khi nó thấy có một packet hay một chuỗi packet giống như bị tấn công, nó có thể phát cảnh báo, hay cắt session đó.

Các IDS phát hiện các tấn công bằng cách dùng các signature. Signature của một tấn công là một profile về loại tấn công đó. Khi IDS phát hiện thấy traffic giống như một signature nào đó, nó sẽ phát cảnh báo.

2.1.1.10 Phương thức tấn công Virus và Trojan Horse

Các nguy hiểm chính cho các workstation và end user là các tấn công virus và ngựa thành Trojan (Trojan horse). Virus là một phần mềm có hại, được đính kèm vào một chương trình thực thi khác để thực hiện một chức năng phá hại nào đó. Trojan horse thì hoạt động khác hơn. Một ví dụ về Trojan horse là một phần mềm ứng dụng để chạy một game đơn giản ở máy workstation. Trong khi người dùng đang mãi mê chơi game, Trojan horse sẽ gửi một bản copy đến tất cả các user trong address book. Khi user khác nhận và chơi trò chơi, thì nó lại tiếp tục làm như vậy, gửi đến tất cả các địa chỉ mail có trong address book của user đó.

Có thể dùng các phần mềm chống virus để diệt các virus và Trojan horse và luôn luôn cập nhật chương trình chống virus mới.

2.2 Các kỹ thuật đảm bảo an toàn mạng

2.2.1 Tổng quan về tường lửa

Firewall là hàng phòng vệ chống lại những kẻ hay đi xâm nhập trộm giúp ngăn chặn ý đồ xâm nhập xấu vào máy tính và hạn chế những gì đi ra khỏi máy nếu chưa được cho phép.

Tường lửa được định nghĩa một cách đúng nhất là một hệ thống an ninh mạng. Chúng hoạt động như một rào chắn giữa mạng an toàn và mạng không an toàn. Tức là chúng sẽ kiểm soát các thông tin các truy cập đến nguồn lực của mạng, lúc này chỉ có những traffic phù hợp với chính sách được định nghĩa trong tường lửa thì mới được truy cập vào mạng, còn lại sẽ bị từ chối.

Tường lửa (Firewall) sẽ đảm bảo rằng máy tính được bảo vệ từ hầu hết các mối tấn công nguy hại phổ biến. Và máy tính nào khi kết nối tới Internet cũng cần có firewall, điều này giúp quản lý những gì được phép vào mạng và những gì được phép ra khỏi mạng

Chức năng của tường lửa trong phòng chống các hình thức tấn công mạng

- + Tường lửa ngăn chặn các truy cập trái phép vào mạng riêng. Nó hoạt động như người gác cửa, kiểm tra tất cả dữ liệu đi vào hoặc đi ra từ mạng riêng. Khi phát hiện có bất kỳ sự truy cập trái phép nào thì nó sẽ ngăn chặn, không cho traffic đó tiếp cận đến mạng riêng.
- + Tường lửa giúp chặn được các cuộc tấn công mạng.
- + Firewall hoạt động như chốt chặn kiểm tra an ninh. Bằng cách lọc thông tin kết nối qua internet vào mạng hay máy tính cá nhân.
- + Dễ dàng kiểm soát các kết nối vào website hoặc hạn chế một số kết nối từ người dùng mà doanh nghiệp không mong muốn.
- + Bạn có thể tùy chỉnh tường lửa theo nhu cầu sử dụng. Bằng cách thiết lập các chính sách bảo mật phù hợp.

Ví dụ:

Cách phòng tránh tấn công DDoS:

Nếu bạn tìm ra được địa chỉ của máy tính thực hiện tấn công DDoS, bạn có thể tạo một danh sách quản lý các truy cập (ACL) trong tường lửa để chặn các địa chỉ này.

2.2.1.1 Ưu điểm của tường lửa

Tường lửa mạng:

- + Bảo mật nhất quán: Tường lửa phần cứng cung cấp khả năng bảo mật nhất quán cho tất cả các thiết bị mà nó bảo vệ.
- + Bảo vệ độc lập: Tường lửa phần cứng chạy trên phần cứng của nó. Do vậy việc tăng lưu lượng truy cập hoặc các yêu cầu bảo mật không ảnh hưởng đến hiệu suất của máy được bảo vệ.
- + Quản lý đơn giản: Tường lửa phần cứng là một thiết bị duy nhất bảo vệ toàn bộ mạng. Bất kỳ bản cập nhật hoặc thay đổi cấu hình nào được yêu cầu đều có thể được áp dụng một lần và sẽ ngay lập tức áp dụng cho tất cả các thiết bị được bảo vệ bởi tường lửa.
- + Cải thiện khả năng bảo mật: Như đã nói tường lửa phần cứng chạy trên phần cứng chuyên dụng của nó thay vì dựa vào tài nguyên của máy tính mà nó được cài đặt. Điều này có thể giúp bảo vệ tường lửa khỏi các cuộc tấn công được thiết kế để khai thác hệ điều hành cơ sở (Underlying Operating System) hoặc các chương trình chạy cùng với nó.
- + Khả năng hiển thị tập trung: Tường lửa phần cứng tập trung giám sát mạng và đăng nhập vào một thiết bị duy nhất.

Tường lửa ứng dụng:

- + Linh hoạt, dễ cấu hình: Người dùng có thể dễ dàng thiết lập mức độ bảo vệ mong muốn, cung cấp các mức độ bảo mật khác nhau tùy theo máy hoặc người dùng.
- + Bảo vệ mọi lúc, mọi nơi: Tường lửa phần mềm bảo vệ máy tính được cài đặt bất kể máy tính đó được kết nối ở đâu.
- + Chi phí triển khai thấp

2.2.1.2 Nhược điểm của tường lửa

Tường lửa mạng:

Bên cạnh những ưu điểm, loại tường lửa này cũng có những nhược điểm xuất phát từ hạn chế của phần cứng (số lượng Card giao diện mạng (NIC), giới hạn băng thông,...). Ngoài ra chi phí đầu tư khá cao. Tường lửa khó cấu hình, cần đến sự giúp đỡ của các chuyên gia.

Tường lửa ứng dụng:

- + Sử dụng nhiều tài nguyên hệ thống hơn, chẳng hạn như bộ nhớ và dung lượng đĩa
- + Để sử dụng tường lửa phần mềm, mỗi máy tính cần được cấu hình, quản lý và cập nhật riêng
- + Triển khai tường lửa phần mềm độc lập trên mỗi thiết bị trong mạng của tổ chức đồng nghĩa với việc thiếu khả năng hiển thị toàn bộ mạng hoặc nhân viên IT phải nỗ lực nhiều hơn để tổng hợp và đồng bộ thông tin từ tất cả các thiết bị khác nhau.

2.2.2 Hệ thống phát hiện và ngăn chặn xâm nhập

2.2.2.1 Tổng quan

Hiện nay có nhiều công cụ nhằm gia tăng tính bảo mật cho hệ thống. Các công cụ đó vẫn đang hoạt động có hiệu quả, tuy nhiên chúng đều có những hạn chế riêng làm hệ thống vẫn có nguy cơ bị tấn công cao vì thế cần thiết phải có một thiết bị phát hiện và ngăn chặn các cố gắng xâm nhập vào hệ thống. Và trong đó nổi trội là

Hệ thống phát hiện xâm nhập IDS và hệ thống ngăn ngừa xâm nhập IPS

Hệ thống IDS

IDS là viết tắt của Intrusion Detection System - Hệ thống Phát hiện Xâm nhập. Đây là các phần mềm hoặc công cụ giúp bạn bảo mật hệ thống và cảnh báo mỗi khi có xâm nhập. IDS thường là một phần của các hệ thống bảo mật hoặc phần mềm khác, đi kèm với nhiệm vụ bảo vệ hệ thống thông tin.

Các tính năng quan trọng nhất của IDS bao gồm: giám sát traffic mạng và các hoạt động khả nghi; đưa ra các cảnh báo về những điểm bất thường cho hệ thống và đơn vị quản trị mạng; kết hợp với tường lửa, phần mềm diệt virus tạo nên một hệ thống bảo mật hoàn chỉnh

Phân loại IDS:

- + NIDS: Network Intrusion Detection Systems được đặt tại một điểm chiến lược hoặc những điểm giám sát traffic đến và đi từ tất cả các thiết bị trên mạng. Lý tưởng nhất là bạn có thể quét tất cả traffic inbound và outbound, nhưng việc này có thể tạo ra nút thắt cổ chai làm giảm tốc độ chung của mạng.
- + HIDS: Host Intrusion Detection Systems, hệ thống phát hiện xâm nhập này chạy trên máy chủ riêng hoặc một thiết bị đặc biệt trên mạng. HIDS chỉ

giám sát các gói dữ liệu inbound và outbound từ thiết bị và cảnh báo người dùng hoặc quản trị viên về những hoạt động đáng ngờ được phát hiện.

- + **Signature-Based:** Là các IDS hoạt động dựa trên chữ ký, giám sát các gói tin trên mạng và so sánh chúng với cơ sở dữ liệu chữ ký, thuộc tính từ những mối đe dọa đã biết, tương tự như cách phần mềm diệt virus hoạt động. Vấn đề đối với hệ thống IDS này là có thể không phát hiện ra mối đe dọa mới, khi chữ ký để nhận biết nó chưa được IDS kịp cập nhật.
- + **Anomaly-Based:** IDS này sẽ phát hiện mối đe dọa dựa trên sự bất thường. Nó giám sát traffic mạng và so sánh với baseline đã được thiết lập. Baseline sẽ xác định đâu là mức bình thường của mạng: loại băng thông thường được dùng, giao thức thường dùng, cổng và thiết bị thường kết nối với nhau, cảnh báo cho quản trị viên mạng hoặc người dùng khi phát hiện traffic truy cập bất thường hoặc những khác biệt đáng kể so với baseline.
- + **Passive:** IDS thụ động sẽ chỉ phát hiện và cảnh báo. Khi phát hiện traffic đáng ngờ hoặc độc hại, nó sẽ tạo cảnh báo và gửi đến quản trị viên hoặc người dùng. Việc hành động như nào sau đó tùy thuộc vào người dùng và quản trị viên.
- + **Reactive:** Loại IDS này bên cạnh nhiệm vụ như IDS Passive, nó còn thực hiện những hành động được thiết lập sẵn để ngay lập tức phản ứng lại các mối đe dọa, ví như: chặn truy cập, khóa IP

Hệ thống IPS

IPS là hệ thống theo dõi, ngăn ngừa kịp thời các hoạt động xâm nhập không mong muốn. Chức năng chính của IPS là xác định các hoạt động nguy hại, lưu giữ các thông tin này. Sau đó kết hợp với firewall để dừng ngay các hoạt động này, và cuối cùng đưa ra các báo cáo chi tiết về các hoạt động xâm nhập trái phép trên. Hệ thống IPS được xem là trường hợp mở rộng của hệ thống IDS, cách thức hoạt động cũng như đặc điểm của 2 hệ thống này tương tự nhau. Điểm khác nhau duy nhất là hệ thống IPS ngoài khả năng theo dõi, giám sát thì còn có chức năng ngăn chặn kịp thời các hoạt động nguy hại đối với hệ thống. Hệ thống IPS sử dụng tập luật tương tự như hệ thống IDS

Phân loại IPS

- + **Hệ thống ngăn ngừa xâm nhập mạng (NIPS – Network-based Intrusion Prevention)** thường được triển khai trước hoặc sau firewall. Khi triển khai IPS trước firewall là có thể bảo vệ được toàn bộ hệ thống bên trong kể cả

firewall, vùng DMZ. Có thể giảm thiểu nguy cơ bị tấn công từ chối dịch vụ đối với firewall. Khi triển khai IPS sau firewall có thể phòng tránh được một số kiểu tấn công thông qua khai thác điểm yếu trên các thiết bị di động sử dụng VPN để kết nối vào bên trong.

- + Hệ thống ngăn ngừa xâm nhập host (HIPS – Host-based Intrusion Prevention) thường được triển khai với mục đích phát hiện và ngăn chặn kịp thời các hoạt động thâm nhập trên các host. Để có thể ngăn chặn ngay các tấn công, HIPS sử dụng công nghệ tương tự như các giải pháp antivirus. Ngoài khả năng phát hiện ngăn ngừa các hoạt động thâm nhập, HIPS còn có khả năng phát hiện sự thay đổi các tập tin cấu hình.

2.2.2.2 Ưu và nhược điểm của hệ thống phát hiện và ngăn chặn xâm nhập

- IDS

- **Ưu điểm :**

- + Thích hợp sử dụng để thu thập số liệu, bằng chứng phục vụ công tác điều tra và ứng cứu sự cố
- + Đem đến cái nhìn bao quát, toàn diện về toàn bộ hệ thống mạng
- + Là công cụ thích hợp phục vụ việc kiểm tra các sự cố trong hệ thống mạng.

- **Nhược điểm:**

- + Thích hợp sử dụng để thu thập số liệu, bằng chứng phục vụ công tác điều tra và ứng cứu sự cố
- + Đem đến cái nhìn bao quát, toàn diện về toàn bộ hệ thống mạng
- + Là công cụ thích hợp phục vụ việc kiểm tra các sự cố trong hệ thống mạng.

- IPS

- **Ưu điểm :**

- + Cung cấp giải pháp bảo vệ toàn diện hơn đối với tài nguyên hệ thống.
- + Ngăn chặn kịp thời các tấn công đã biết hoặc chưa được biết.

- **Nhược điểm :**

- + Có thể gây ra tình trạng phát hiện nhầm (faulse positives), có thể không cho phép các truy cập hợp lệ tới hệ thống

2.2.3 Tổng quan về Honeypot

2.2.3.1 Tổng quan về honeypot

Thuật ngữ “Honeypot” được nhắc đến lần đầu tiên vào ngày 4 tháng 8 năm 1999 trong bài báo “To Buil a Honeypot” của tác giả Lance Spitzner - một trong những người đứng ra thành lập dự án Honeynet, giới thiệu về ý tưởng xây dựng hệ thống Honeynet nhằm mục đích nghiên cứu các kỹ thuật tấn công của Hacker, từ đó có biện pháp ngăn chặn tấn công kịp thời. Và tháng 6 năm 2000, dự án Honeynet được thành lập bởi 30 chuyên gia an ninh mạng ở các công ty bảo mật như: Foundstone, Security Focus, Source Fire,..., tình nguyện tham gia nghiên cứu phi lợi nhuận.

Honeypot là một hệ thống tài nguyên thông tin được xây dựng với mục đích giả dạng đánh lừa những kẻ sử dụng và xâm nhập không hợp pháp, thu hút sự chú ý của chúng, ngăn không cho chúng tiếp xúc với hệ thống thật.

- Phân loại honeypot

+ Phân loại honeypot theo cấp độ

Low-interaction honeypot

Đây là kiểu honeypot đơn giản, sử dụng ít tài nguyên đồng thời thông tin thu thập được cũng ở mức cơ bản. Chúng có thể triển khai dễ dàng và nhanh chóng dưới dạng mô phỏng cơ bản các các dịch vụ mạng, giao thức TCP và IP.

High-interaction honeypots

Đây là kiểu honeypot phức tạp nhằm thu hút nhiều thời gian và thao tác của kẻ tấn công. Nhằm thu thập càng nhiều càng tốt về mục đích, quá trình, lỗ hổng mà kẻ tấn công muốn khai thác. Hệ thống dạng này sẽ tốn nhiều tài nguyên hơn nữa để triển khai cũng như giám sát cần người có kinh nghiệm vì nếu honeypot không bảo mật đúng cách sẽ bị tin tặc khai thác.

+ Phân loại honeypot theo mục đích sử dụng

Email trap

Đây là một địa chỉ email được tạo ra và đưa vào website để người dùng thông thường không tìm thấy nhưng để các công cụ thu thập tự động có thể tìm ra và để những kẻ spam gửi email. Địa chỉ email này thực tế là một cái bẫy chỉ để nhận email rác. Khi những email rác được gửi vào địa chỉ này dữ liệu sẽ được

phân tích và thu thập để đưa vào bộ lọc nhằm ngăn chặn người dùng nhận được những email tương tự

Decoy database / Database honeypot

Một cơ sở dữ liệu cũng có thể được lập ra để bẫy và theo dõi những cuộc tấn công SQL injection, khai thác dịch vụ của SQL... Với dạng honeypot này có thể triển khai bằng cách sử dụng tường lửa cơ sở dữ liệu (database firewall).

Malware honeypot

Đây là dạng honeypot thường được sử dụng bởi các công ty bảo mật, các chuyên gia nghiên cứu mã độc với mục đích phát hiện mã độc. Ví dụ sử dụng honeypot mô phỏng một thiết bị USB, nếu một máy bị nhiễm mã độc lây nhiễm qua USB, honeypot sẽ đánh lừa mã độc lây nhiễm sang thiết bị giả lập

Spider honeypot

Spider honeypot được dùng để bẫy các webcrawler/spider bằng cách tạo ra những trang web và những liên kết mà chỉ các crawler mới có thể truy cập. Sau đó dùng thông tin thu thập được để chặn các crawler độc hại.

Honeynet

Honeynet là một mạng bao gồm nhiều honeypot với nhiều loại khác nhau tạo thành có thể dùng để nghiên cứu các kiểu tấn công như DDos, tấn công vào CDN (content delivery network), tấn công của ransomware. Honeynet được sử dụng nhằm theo nghiên cứu quá trình cũng như phương pháp của kẻ tấn công đồng thời lưu lại traffic vào/ra hệ thống phục vụ mục đích theo dõi phân tích

2.2.3.2 Ưu và nhược điểm của honeypot

Ưu điểm

- + Có thể theo dõi được quá trình và kỹ thuật mà những kẻ tấn công sử dụng.
- + Giúp thu thập thông tin về những kẻ tấn công.
- + Xây dựng phương án phòng thủ dựa trên dữ liệu thu được.
- + Giúp tổ chức đánh lạc hướng, làm mất thời gian những kẻ tấn công từ bên ngoài.
- + Giúp phát hiện sớm những nguy cơ tiềm ẩn từ nội bộ doanh nghiệp.

Nhược điểm

- + Honeypot không được bảo mật tốt có thể bị lợi dụng để tấn công vào hệ thống thật của tổ chức, doanh nghiệp.
- + Một hệ thống honeypot vẫn có thể bị những kẻ tấn công có kinh nghiệm phát hiện và làm sai lệch dữ liệu honeypot cần thu thập nhằm đánh lạc hướng.

CHƯƠNG III : THỰC NGHIỆM

3.1 Fire Wall

3.1.1 Mô tả

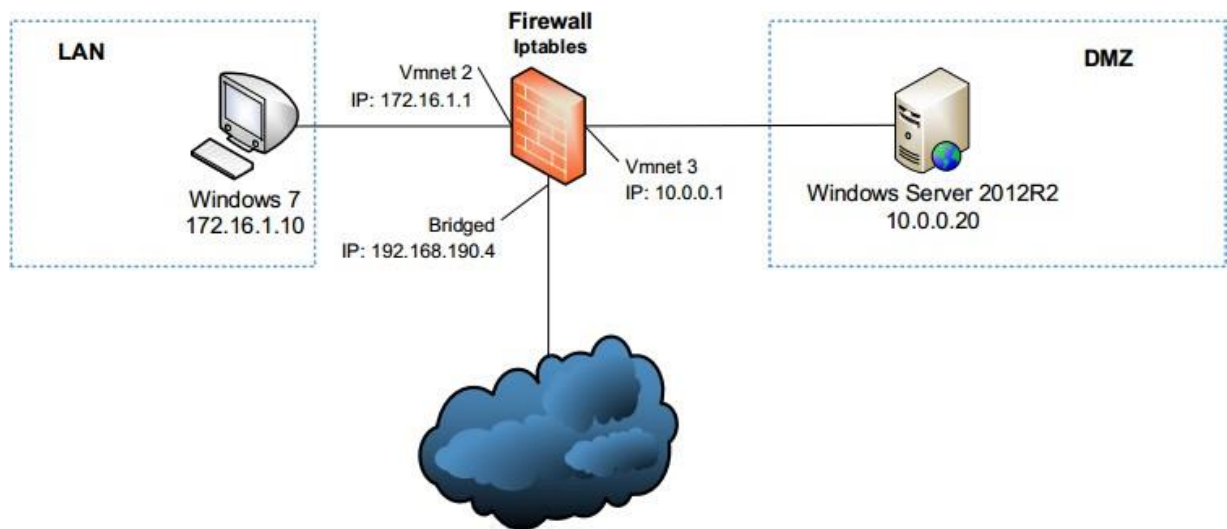
Tường lửa Iptables là loại tường lửa miễn phí được tích hợp sẵn trong các hệ điều hành Linux. Có thể ứng dụng để kiểm soát truy cập cho mạng máy tính nội bộ và phân vùng mạng máy chủ.

Thực nghiệm này thực hiện thiết lập tập luật cho tường lửa Iptables để kiểm soát các dịch vụ cho mạng nội bộ, mạng DMZ, mạng Internet. Cụ thể là cho phép người dùng trong mạng nội bộ LAN có thể truy cập được ra ngoài Internet với các giao thức ICMP, DNS.

3.1.2 Chuẩn bị

- + 01 máy ảo hệ điều hành Windows 7
- + 01 máy ảo hệ điều hành Windows Server 2012.
- + 01 máy ảo hệ điều hành CentOS 6.5 để làm tường lửa Iptables.

3.1.3 Mô hình cài đặt



Hình 3. 1 Mô hình cài đặt

Một số câu lệnh cơ bản sử dụng trong tường lửa Iptables

Lệnh khởi động tường lửa:

```
[root@server]# service iptables start [root@server]# service iptables stop  
[root@server]# service iptables restart
```

 Để khởi động Iptables mỗi khi khởi động máy:

```
[root@server]# chkconfig iptables on
```

Để xem tình trạng của Iptables:

```
[root@server]# service iptables status
```

Lưu thông tin cấu hình:

```
[root@server]# /etc/init.d/iptables save
```

Lệnh xóa toàn bộ luật có trong Iptables:

```
[root@server]# iptables -F [root@server]# iptables -t nat -F
```

3.1.4 Các kịch bản thực hiện

Kịch bản 1. Cho phép máy tính trong LAN Ping ra ngoài mạng Internet

+ Bước 1. Kiểm tra Ping

Tại máy trạm Windows 7 thực Ping đến địa chỉ IP bất kỳ.


```
C:\Users\admin>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Hình 3. 2 Kiểm tra Ping

Kết quả, không Ping được ra ngoài mạng.

- + **Bước 2.** Thiết lập luật trên tường lửa Iptables để cho phép máy trạm Ping ra bên ngoài.

```
[root@server]# ifconfig
eth1      Link encap:Ethernet  HWaddr 00:0C:29:56:E3:8A
          inet addr:192.168.190.4  Bcast:192.168.190.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe56:e38a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

eth2      Link encap:Ethernet  HWaddr 00:0C:29:56:E3:94
          inet addr:172.16.1.1   Bcast:172.16.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe56:e394/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

eth3      Link encap:Ethernet  HWaddr 00:0C:29:56:E3:9E
          inet addr:10.0.0.1     Bcast:10.0.0.255   Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe56:e39e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
```

Hình 3. 3 Kiểm tra tên của các giao diện mạng

Trước hết cần kiểm tra tên của các giao diện mạng trên máy tường lửa Iptables:

Trong hình trên giao diện eth1 kết nối mạng Internet. Giao diện eth2 kết nối mạng nội bộ, giao diện eth3 kết nối mạng máy chủ.

Tiếp theo đặt lệnh cho Iptables để cho phép máy trạm trong mạng nội bộ Ping ra mạng Internet.

```
[root@server]#iptables -A FORWARD -i eth2 -o eth1 -s 172.16.1.0/24 -p icmp -
-icmp-type any -j ACCEPT
```

```
[root@server]#iptables -A FORWARD -i eth1 -o eth2 -d 172.16.1.0/24 -p icmp -
-icmp-type any -j ACCEPT
```

```
[root@server]#iptables -t nat -A POSTROUTING -o eth1 -s 172.16.1.0/24 -j
SNAT --to-source 192.168.190.4
```

```
[root@server]#nano /proc/sys/net/ipv4/ip_forward 0 -> 1
```

Ghi chú: địa chỉ IP 192.168.190.4 là địa chỉ của giao diện mạng kết nối Internet (eth1), tùy thuộc vào trường hợp cụ thể của máy ảo mà sử dụng địa chỉ IP này.

+ **Bước 3.** Kiểm tra kết quả

Trở lại máy trạm Windows 7 kiểm tra Ping tới địa chỉ IP tại bước 1. Kết quả thành công.

```
C:\Users\admin>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=35ms TTL=127
Reply from 8.8.8.8: bytes=32 time=38ms TTL=127
Reply from 8.8.8.8: bytes=32 time=36ms TTL=127
Reply from 8.8.8.8: bytes=32 time=36ms TTL=127

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 35ms, Maximum = 38ms, Average = 36ms
```

Hình 3. 4 Kiểm tra Ping

Kịch bản 2. Cho phép máy tính trong LAN truy vấn DNS ra Internet

+ **Bước 1.** Kiểm tra truy vấn

Trước khi thiết lập luật cho tường lửa, tại máy trạm Windows 7 không truy vấn được DNS. Sử dụng lệnh **nslookup** để truy vấn.

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\admin>nslookup
DNS request timed out.
    timeout was 2 seconds.
Default Server: UnKnown
Address: 8.8.8.8

>
```

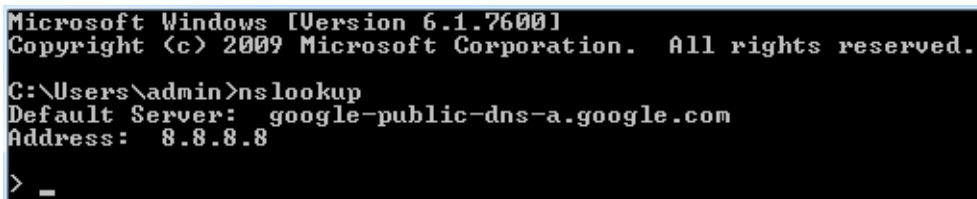
Hình 3. 5 Dùng lệnh nslookup để truy vấn

+ **Bước 2.** Cấu hình luật để cho phép truy vấn DNS tại tường lửa.

```
[root@server]#iptables -A FORWARD -i eth2 -o eth1 -s 172.16.1.0/24 -p udp --
dport 53 -j ACCEPT
```

```
[root@server]#iptables -A FORWARD -i eth1 -o eth2 -d 172.16.1.0/24 -p udp --
sport 53 -j ACCEPT
```

+ **Bước 3.** Kiểm tra kết quả



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\admin>nslookup
Default Server: google-public-dns-a.google.com
Address: 8.8.8.8

> _
```

Hình 3. 6 Kiểm tra kết quả

Kết quả, lúc này tại máy Windows 7 thực hiện truy vấn thành công

3.2 Hệ thống phát hiện xâm nhập IDS/IPS

3.2.1 Mô tả

Để đảm bảo an toàn cho mạng máy tính nhằm phát hiện các cuộc tấn công vào mạng nội bộ, cần triển khai hệ thống phát hiện xâm nhập. Hệ thống phát hiện xâm nhập có thể là thiết bị chuyên dụng hoặc dưới dạng phần mềm. Trong mô hình mạng thử nghiệm nghiên cứu và học tập thì phần mềm miễn phí Snort là phù hợp.

Yêu cầu của thực nghiệm này:

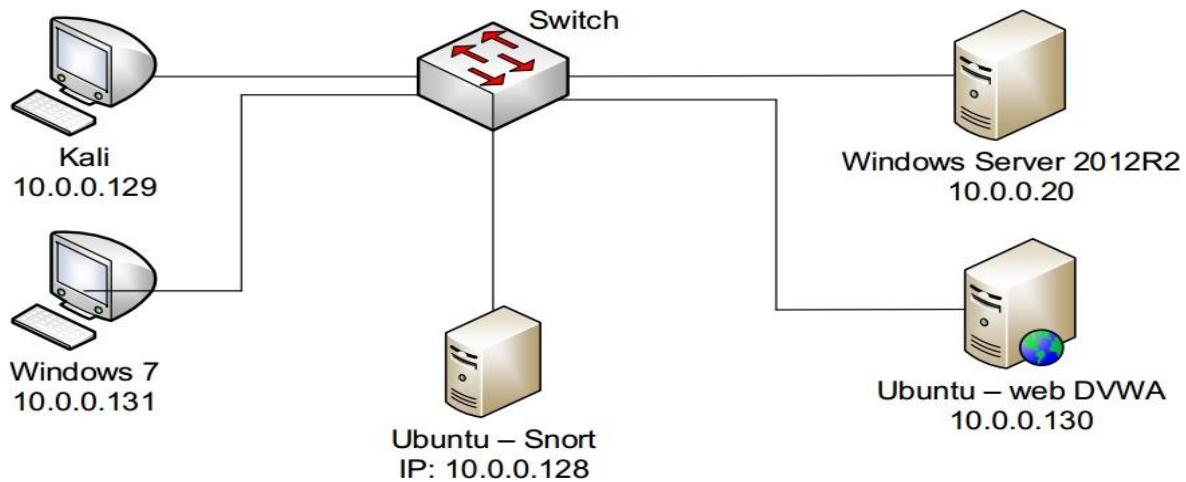
- Cài đặt phần mềm Snort
- Cấu hình các tham số cho Snort

Sử dụng Snort để phát hiện một số dạng tấn công phổ biến

3.2.2 Chuẩn bị

- 01 máy ảo chạy Ubuntu 14.04
- 01 máy ảo hệ điều hành Windows 7
- 01 máy ảo hệ điều hành Windows Server 2012.
- 01 máy ảo hệ điều hành Linux chạy website DVWA.
- 01 máy ảo hệ điều hành Kali linux.

3.2.3 Mô hình cài đặt



Hình 3. 7 Mô hình cài đặt

Kiểm tra sự hoạt động của Snort

Tại cửa sổ dòng lệnh chạy lệnh sau:

```
[attt@snort:~$] sudo snort -i eth0 -c /etc/snort/snort.conf -T
```

Kết quả như sau:

```
''_~ -*> Snort! <*-
o" )~ Version 2.9.12 GRE (Build 325)
  "" By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
  Copyright (C) 2014-2018 Cisco and/or its affiliates. All rights reserved.
  Copyright (C) 1998-2013 Sourcefire, Inc., et al.
  Using libpcap version 1.5.3
  Using PCRE version: 8.31 2012-07-06
  Using ZLIB version: 1.2.8

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.0 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>

Snort successfully validated the configuration!
Snort exiting
```

Hình 3. 8 Kiểm tra sự hoạt động của snort

Kết quả cài đặt và cấu hình Snort thành công.

3.2.4 Kịch bản thực hiện tấn công và phát hiện

Kịch bản 1. Phát hiện tấn công dò quét

Bước 1. Sử dụng phần mềm Nmap dò quét các máy tính đang chạy

```
root@kali:~# nmap -sP 10.0.0.0/24
```

Starting Nmap 7.70 (<https://nmap.org>) at 2019-01-07 03:05 EST
Nmap scan report for 10.0.0.1

Khi sử dụng phương pháp dò quét này, Nmap sẽ gửi các gói tin ARP tới địa chỉ broadcast để tìm địa chỉ IP các máy đang bật, sau đó nó gửi lại các gói ICMP để kiểm tra lại tình trạng hoạt động.

Do Snort chưa hỗ trợ phát hiện giao thức ARP nên chúng ta chỉ có thể phát hiện dò quét thông qua giao thức ICMP.

Bước 2. Phát hiện tấn công

Mã nguồn của luật phát hiện dò quét ICMP của Snort như sau:

```
alert icmp any any -> any any (msg:"Nmap ICMP scanning";sid:10000001; rev:1;)
```

Chạy chương trình Snort ở chế độ lắng nghe và phát hiện:

```
[attt@snort:~$] sudo snort -i eth0 -c /etc/snort/snort.conf
```

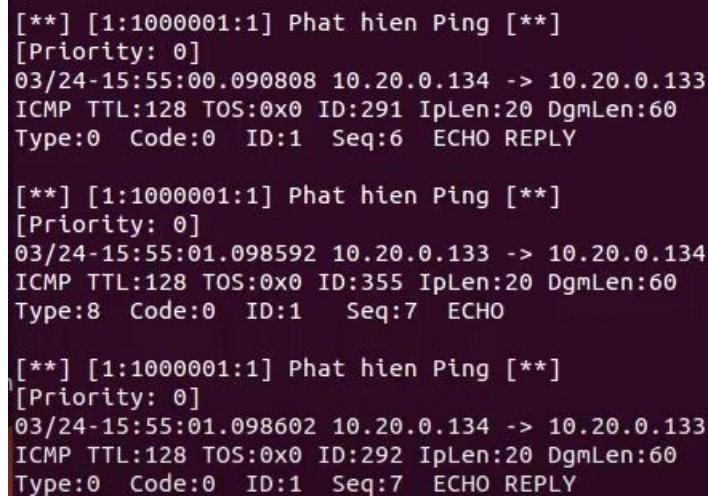
Trong quá trình Snort chặn bắt gói tin và so sánh với tập luật, những sự kiện nào trùng khớp sẽ được lưu trong tệp tin theo đường dẫn: /var/log/snort/alert

Chúng ta có thể xem trực tiếp theo thời gian thực sử dụng lệnh:

```
[attt@snort:~$] tail -f /var/log/snort/alert
```

Bước 3. Kết quả

Giao diện hiển thị của lệnh tail:



```
[**] [1:1000001:1] Phat hien Ping [**]
[Priority: 0]
03/24-15:55:00.090808 10.20.0.134 -> 10.20.0.133
ICMP TTL:128 TOS:0x0 ID:291 IpLen:20 DgmLen:60
Type:0 Code:0 ID:1 Seq:6 ECHO REPLY

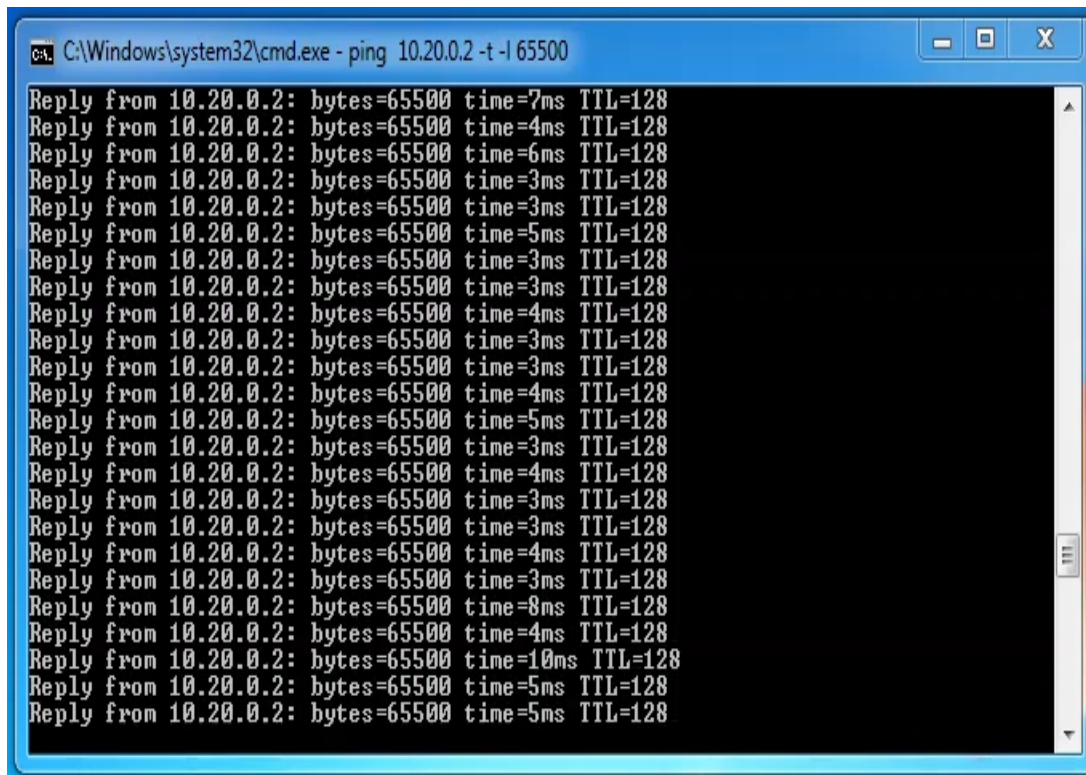
[**] [1:1000001:1] Phat hien Ping [**]
[Priority: 0]
03/24-15:55:01.098592 10.20.0.133 -> 10.20.0.134
ICMP TTL:128 TOS:0x0 ID:355 IpLen:20 DgmLen:60
Type:8 Code:0 ID:1 Seq:7 ECHO

[**] [1:1000001:1] Phat hien Ping [**]
[Priority: 0]
03/24-15:55:01.098602 10.20.0.134 -> 10.20.0.133
ICMP TTL:128 TOS:0x0 ID:292 IpLen:20 DgmLen:60
Type:0 Code:0 ID:1 Seq:7 ECHO REPLY
```

Hình 3. 9 Hiển thị kết quả

Kịch bản 2. Phát hiện tấn công từ chối dịch vụ

Bước 1. Tại máy tính Windows 7 sử dụng cửa sổ dòng lệnh CMD, Ping nhiều gói tin ICMP với kích thước lớn (2000byte) tới máy chủ Window Server 2012.



```
C:\Windows\system32\cmd.exe - ping 10.20.0.2 -t -l 65500
Reply from 10.20.0.2: bytes=65500 time=7ms TTL=128
Reply from 10.20.0.2: bytes=65500 time=4ms TTL=128
Reply from 10.20.0.2: bytes=65500 time=6ms TTL=128
Reply from 10.20.0.2: bytes=65500 time=3ms TTL=128
Reply from 10.20.0.2: bytes=65500 time=3ms TTL=128
Reply from 10.20.0.2: bytes=65500 time=5ms TTL=128
Reply from 10.20.0.2: bytes=65500 time=3ms TTL=128
Reply from 10.20.0.2: bytes=65500 time=3ms TTL=128
Reply from 10.20.0.2: bytes=65500 time=4ms TTL=128
Reply from 10.20.0.2: bytes=65500 time=3ms TTL=128
Reply from 10.20.0.2: bytes=65500 time=3ms TTL=128
Reply from 10.20.0.2: bytes=65500 time=4ms TTL=128
Reply from 10.20.0.2: bytes=65500 time=5ms TTL=128
Reply from 10.20.0.2: bytes=65500 time=3ms TTL=128
Reply from 10.20.0.2: bytes=65500 time=4ms TTL=128
Reply from 10.20.0.2: bytes=65500 time=3ms TTL=128
Reply from 10.20.0.2: bytes=65500 time=3ms TTL=128
Reply from 10.20.0.2: bytes=65500 time=3ms TTL=128
Reply from 10.20.0.2: bytes=65500 time=8ms TTL=128
Reply from 10.20.0.2: bytes=65500 time=4ms TTL=128
Reply from 10.20.0.2: bytes=65500 time=10ms TTL=128
Reply from 10.20.0.2: bytes=65500 time=5ms TTL=128
Reply from 10.20.0.2: bytes=65500 time=5ms TTL=128
```

Hình 3. 10 Hiển thị Ping

Bước 2. Thiết lập luật cho Snort phát hiện tấn công:

```
alert icmp any any -> $HOME_NET any (msg:"ICMP Ping Of Death attack";
itype:8; dsize:>1000; detection_filter:track by_src, count 10, seconds 5;
classtype:denialof-service; sid:1000003; rev:1;)
```

Bước 3. Kết quả

Giao diện hiển thị của lệnh tail:

```
[**] [1:1000003:1] ICMP Ping Of Death attack [**]  
[Classification: Detection of a Denial of Service Attack] [Priority: 2]  
03/30-09:45:55.605450 10.20.0.133 -> 10.20.0.2  
ICMP TTL:128 TOS:0x0 ID:942 IpLen:20 DgmLen:65028  
Type:8 Code:0 ID:1 Seq:339 ECHO  
  
[**] [1:1000003:1] ICMP Ping Of Death attack [**]  
[Classification: Detection of a Denial of Service Attack] [Priority: 2]  
03/30-09:45:55.700222 10.20.0.133 -> 10.20.0.2  
ICMP TTL:128 TOS:0x0 ID:943 IpLen:20 DgmLen:65028  
Type:8 Code:0 ID:1 Seq:340 ECHO  
  
[**] [1:1000003:1] ICMP Ping Of Death attack [**]  
[Classification: Detection of a Denial of Service Attack] [Priority: 2]  
03/30-09:45:55.775879 10.20.0.133 -> 10.20.0.2  
ICMP TTL:128 TOS:0x0 ID:944 IpLen:20 DgmLen:65028  
Type:8 Code:0 ID:1 Seq:341 ECHO
```

Hình 3. 11 Kết quả thu được

3.3 HONEYPOT

3.3.1 Mô tả

HoneyDrive là môi trường đã được cài đặt sẵn một số Honeypot để thu hút tấn công của tin tặc, giúp người quản trị xây dựng môi trường thử nghiệm. Bản thân HoneyDrive được tích hợp một số công cụ sau:

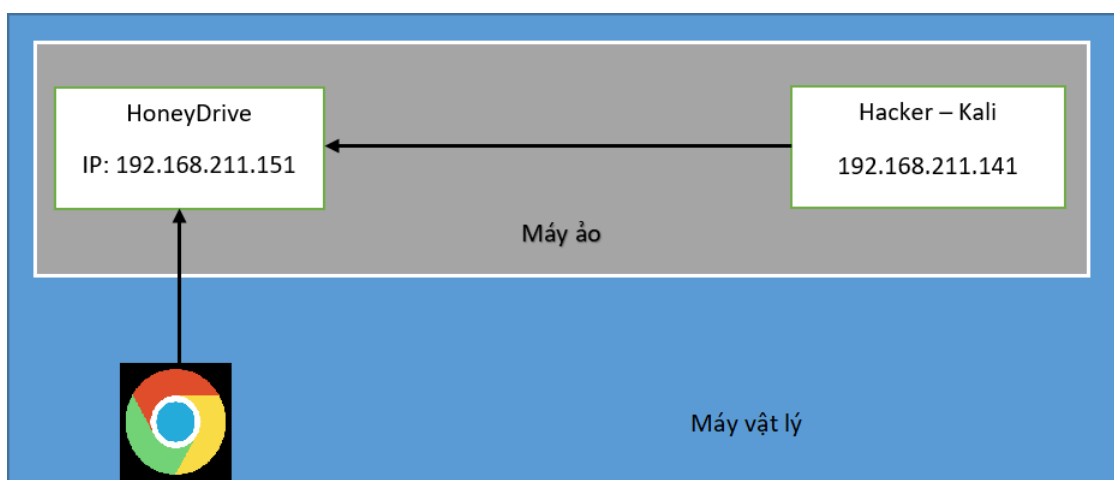
- Kippo SSH honeypot
- Dionaea and Amun malware honeypots
- Honeyd low-interaction honeypot
- Glastopf web honeypot and Wordpot
- Conpot SCADA/ICS honeypot
- Thug and PhoneyC honeyclients
- Kippo-Graph, Honeyd-Viz, DionaeaFR, an ELK stack

- Trong thực nghiệm này sử dụng Kippo SSH Honeypot.

3.3.2 Chuẩn bị

- 01 máy ảo hệ điều hành Kali linux
- 01 máy ảo hệ điều hành HoneyDrive.
- Trình duyệt trên máy vật lý

3.3.3 Mô hình cài đặt



Hình 3. 12 Mô hình cài đặt

3.3.4 Các bước cài đặt

- Download phần mềm: <https://sourceforge.net/projects/honeydrive/>
- Tải phần mềm dưới dạng máy ảo đã cài sẵn:
HoneyDrive_3_Royal_Jelly.ova
- Sử dụng phần mềm máy ảo để bung tệp tin ova này thành máy ảo HoneyDrive.
- Sử dụng máy Kali linux để thực hiện tấn công vào Honeypot SSH kippo
- Sử dụng trình duyệt trên máy vật lý truy cập vào Kippo-graph trên máy HoneyDrive để phân tích.

3.3.5 Thực hiện

Bước 1. Chạy máy ảo HoneyDrive

Sau khi bung nén máy ảo HoneyDrive, khởi chạy máy ảo thành công có giao diện như sau:



Hình 3. 13 Giao diện máy ảo

Tiếp theo cần xác định địa chỉ IP của máy:

Chạy terminal trên Desktop và sử dụng lệnh `ifconfig` để xem:

```
honeydrive@honeydrive:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:ea:45:d8
          inet addr:192.168.211.151  Bcast:192.168.211.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feea:45d8/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:73 errors:0 dropped:0 overruns:0 frame:0
          TX packets:65 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6269 (6.2 KB)  TX bytes:10587 (10.5 KB)
```

Hình 3. 14 Dùng lệnh ifconfig

Bước 2. Chạy chương trình Honeypot kippo

```
honeydrive@honeydrive:~$ /honeydrive/kippo/start.sh
Starting kippo in the background...

Loading dblog engine: mysql
honeydrive@honeydrive:~$
```

Hình 3. 15 Chạy chương trình

Bước 3. Quản lý Honeypot Kippo

Trên máy vật lý sử dụng trình duyệt web truy cập vào máy ảo HoneyDrivetho địa chỉ đã xem ở trên và theo đường dẫn sau:

<http://192.168.211.151/kippo-graph/>



Hình 3. 16 Giao diện quản lý

Bước 4: Kịch bản tấn công dò quét IP và dịch vụ

Sử dụng Nmap trên Kali tấn công thăm dò mạng nội bộ:

```
(kali@kali)-[~]
$ nmap -sP 192.168.211.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-01 03:41 EST
Nmap scan report for 192.168.211.2
Host is up (0.0019s latency).
Nmap scan report for 192.168.211.129
Host is up (0.00066s latency).
Nmap scan report for 192.168.211.141
Host is up (0.0040s latency).
Nmap scan report for 192.168.211.151
Host is up (0.0027s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.56 seconds
```

Hình 3. 17 Thử tấn công thăm dò nội bộ

Phát hiện một số máy tính đang chạy với IP.

```
(kali@kali)-[~]
$ sudo nmap -sV -O 192.168.211.151
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-01 03:44 EST
Nmap scan report for 192.168.211.151
Host is up (0.00067s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.1p1 Debian 5 (protocol 2.0)
80/tcp    open  http     Apache/2.2.22
MAC Address: 00:0C:29:EA:45:D8 (VMware)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 3.16
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.11 seconds
```

Hình 3. 18 Thực hiện dò quét

Thực hiện dò quét dịch vụ và hệ điều hành trên máy 192.168.211.151

Kết quả phát hiện dịch vụ SSH và web đang chạy trên cổng 22, 80. Hệ điều hành máy đích là Linux => khả năng đây là máy chủ web.

Kẻ tấn công thực hiện các bước mà không phát hiện ra họ đang tấn công vào dịch vụ của Honeypot.

Bước 5. Kịch bản tấn công mật khẩu dịch vụ SSH

Sử dụng Hydra trên Linux tấn công từ điển vào mật dịch vụ SSH

```
(kali@kali)-[~]
$ hydra -l root -P /usr/share/wordlists/rockyou.txt 192.168.211.151 -t 4 ssh
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or
n-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-02-01 03:48:08
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399),
[DATA] attacking ssh://192.168.211.151:22/
[22][ssh] host: 192.168.211.151 login: root password: 123456
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-02-01 03:48:12
```

Hình 3. 19 Tấn công từ điển

Kết quả thành công, thu được mật khẩu của tài khoản root.

Bước 6. Truy cập vào máy chủ thông qua dịch vụ SSH

Với tài khoản và mật khẩu đã có, kẻ tấn công thực hiện lệnh kết nối tới máy chủ:

```
(kali@kali)-[~]
$ ssh -o KexAlgorithms=+diffie-hellman-group1-sha1 root@192.168.211.151
Password:
root@svr03:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:4c:a8:ab:32:f4
          inet addr:10.98.55.4  Bcast:10.98.55.255  Mask:255.255.255.0
          inet6 addr: fe80::21f:c6ac:fd44:24d7/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:84045991 errors:0 dropped:0 overruns:0 frame:0
          TX packets:103776307 errors:0 dropped:0 overruns:0 carrier:2
          collisions:0 txqueuelen:1000
          RX bytes:50588302699 (47.1 GiB)  TX bytes:97318807157 (90.6 GiB)
```

Hình 3. 20 Thực hiện lệnh kết nối tới máy chủ

Truy cập thành công.

Bước 7. Thực hiện một số lệnh trên máy chủ

```

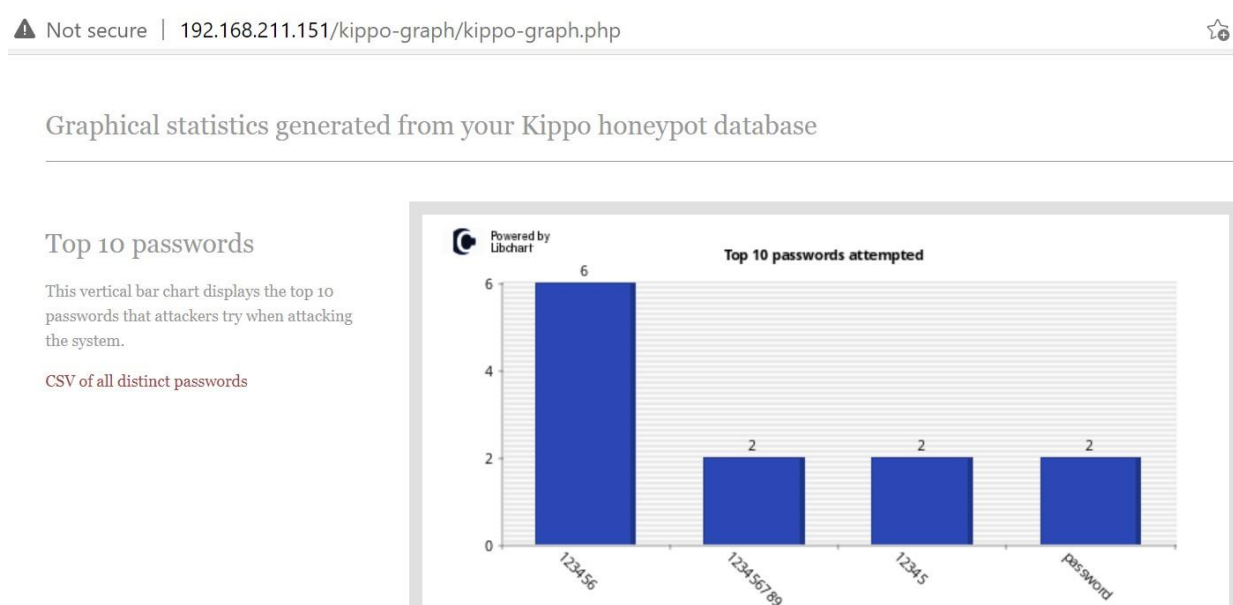
root@svr03:~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
sshd:x:101:65534::/var/run/sshd:/usr/sbin/nologin
richard:x:1000:1000:Richard Texas,,,:/home/richard:/bin/bash
root@svr03:~#

```

Bước 8. Phân tích hành vi

Hình 3. 21 Thực hiện một số lệnh

Tại trình duyệt Kippo đã bật trong bước 3. Refresh lại trình duyệt thì kết quả như sau:

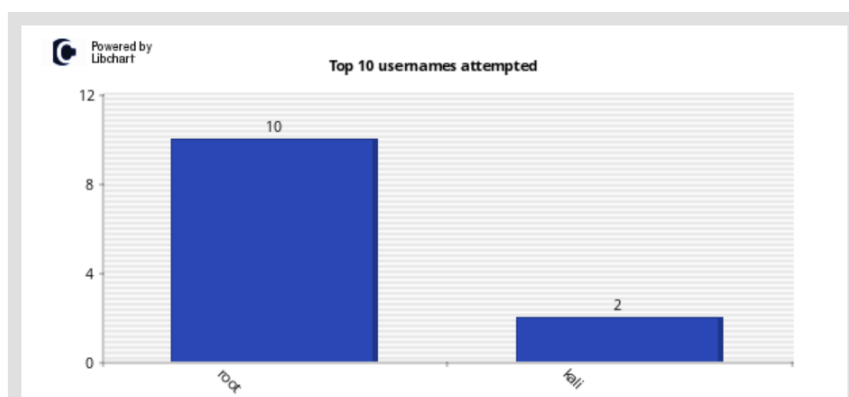


Hình 3. 22 Giao diện này cho biết mật khẩu và số lượng tin tặc đã sử dụng

Top 10 usernames

This vertical bar chart displays the top 10 usernames that attackers try when attacking the system.

CSV of all distinct Usernames

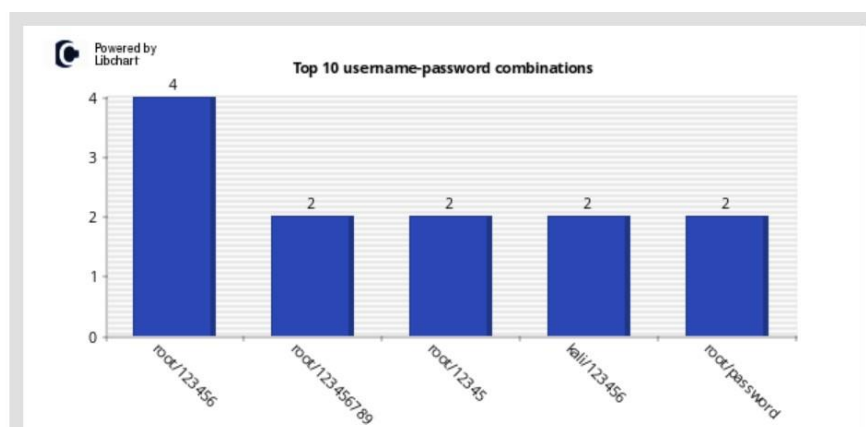


Hình 3. 23 Giao diện này cho biết tài khoản và số lần đăng nhập

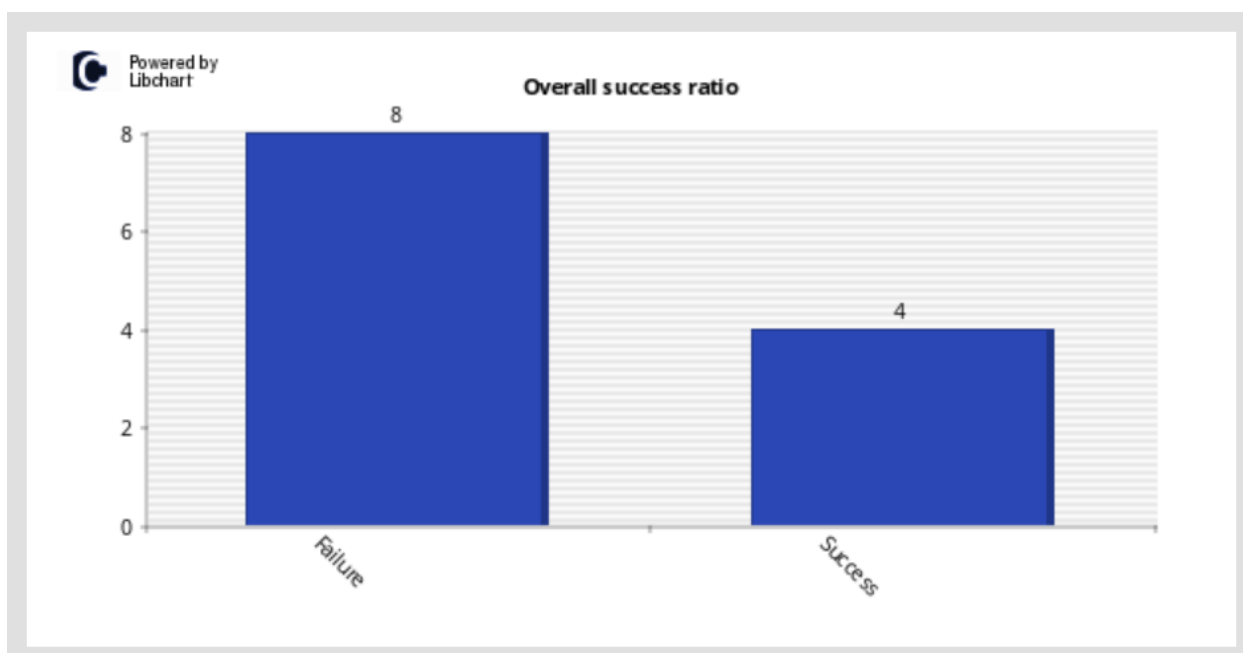
Top 10 user-pass combos

This vertical bar chart displays the top 10 username and password combinations that attackers try when attacking the system.

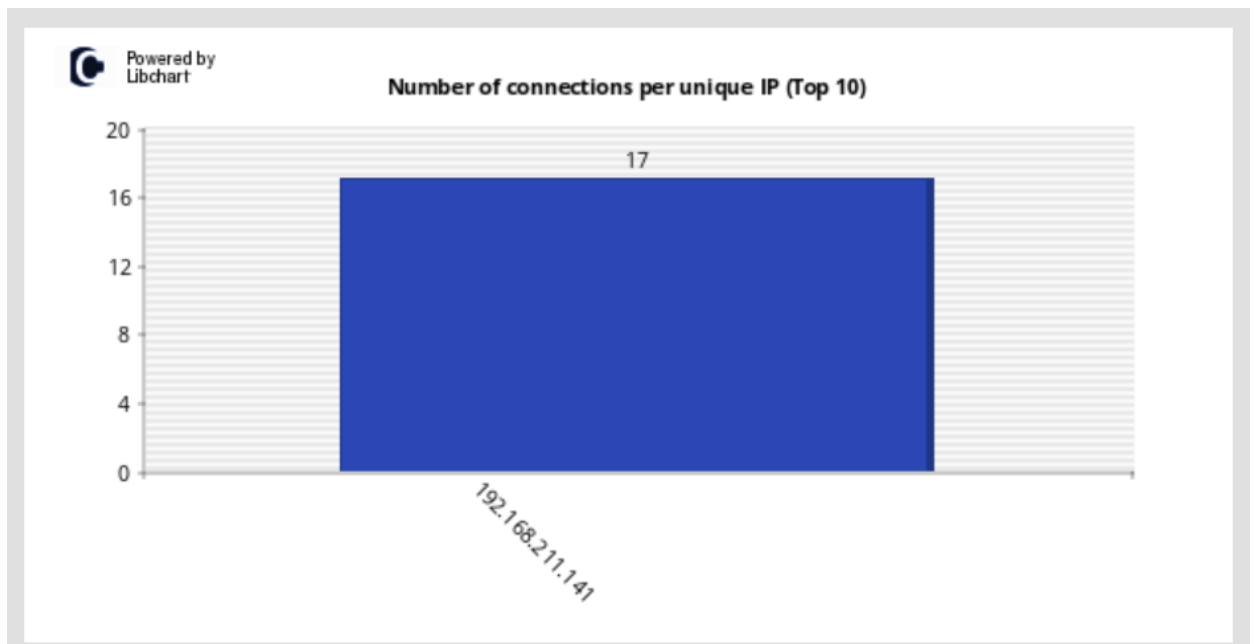
CSV of all distinct combinations



Hình 3. 24 Giao diện này cho biết tài khoản được đăng nhập bởi mật khẩu tương ứng



Hình 3. 23 Giao diện này cho biết số lần đăng nhập đúng và sai



Hình 3. 24 Giao diện này cho biết IP của tin tặc đã sử dụng để xâm nhập vào máy chủ Honeypot

Chuyển sang Tab Kippo-Input để phân tích một số lệnh tin tặc đã sử dụng

ID	Input (success)	Count
1	ls	2
2	cat /etc/passwd	2
3	exit	2
4	mkdir /adfj	1
5	mkdir /test	1
6	cd /var	1
7	cd /var/log/	1
8	cd	1
9	cat /etc/password	1
10	ifconfig	1

Hình 3. 25 Phân tích một số lệnh tin tặc đã sử dụng

3.4 TRIỂN KHAI HONEYNET SỬ DỤNG HONEYWALL

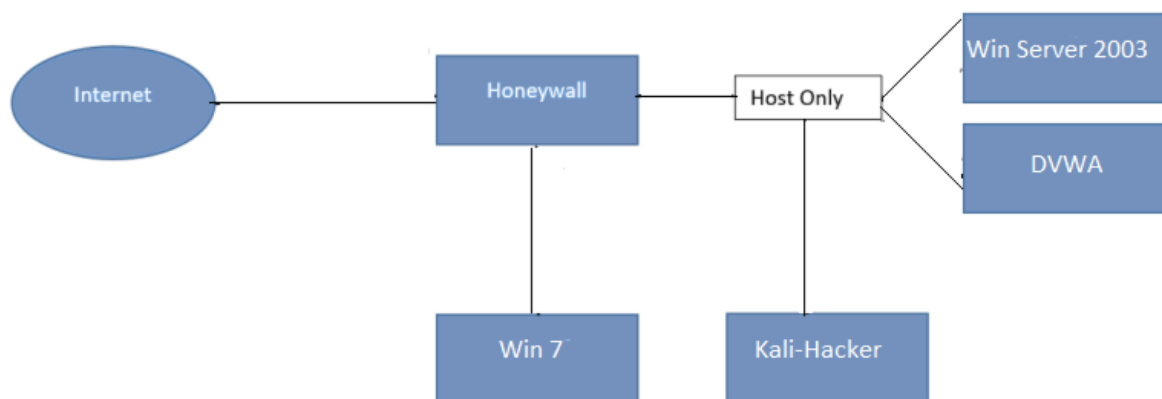
3.4.1. Mô tả

Honeynet là hệ thống có nhiều tài nguyên thực gồm phần mềm, hệ điều hành được kết nối thành mạng nhằm mục đích thu hút tấn công của tin tặc. Để làm được việc này dự án Honeynet phát triển bộ phần mềm Honeywall giúp các đối tượng làm về lĩnh vực an toàn thông tin cài đặt, thử nghiệm, phát triển hệ thống của mình hoàn chỉnh hơn.

Thực nghiệm này triển khai cách thức hoạt động của một hệ thống Honeynet thông qua Honeywall.

3.4.2. Chuẩn bị

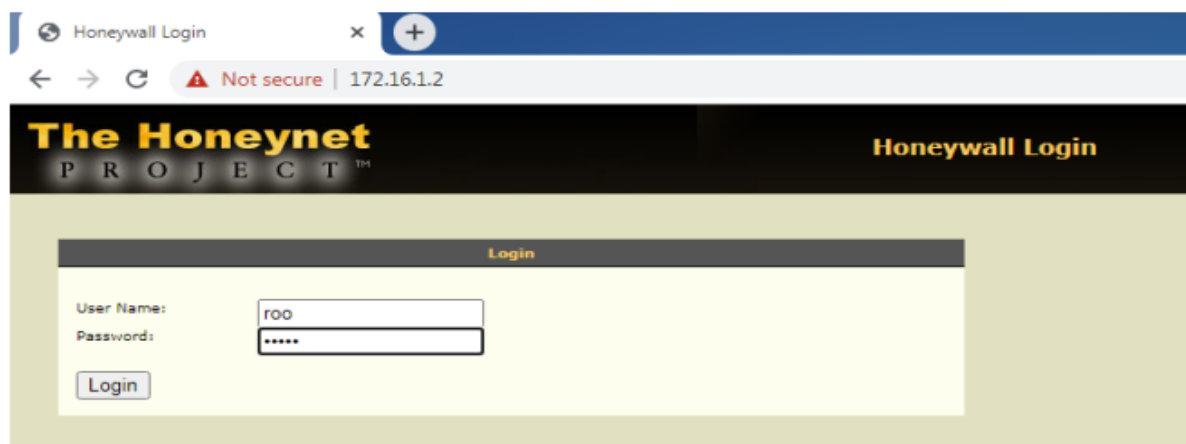
- 01 máy ảo hệ điều hành Server 2003
- 01 máy ảo chạy Honeywall
- 01 máy ảo hệ điều hành Windows 7
- 01 máy kali dung để tấn công
- 01 máy DVWA



Hình 3. 26 Mô hình chuẩn bị

Cài đặt: Quản trị Honeywall

Quản trị Honeywall từ máy Win 7



Hình 3. 27 Giao diện đăng nhập quản trị Honeywall

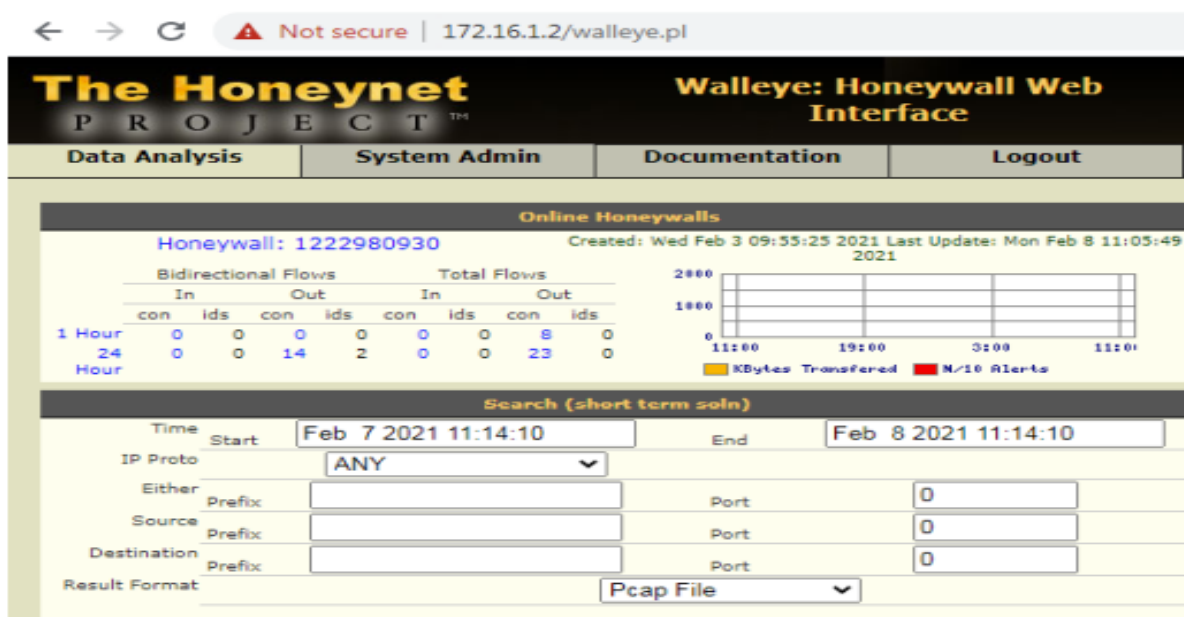
Lần đầu đăng nhập web quản trị với tài khoản:

User Name: roo

Password: honey

Sau khi đăng nhập thành công hệ thống yêu cầu thay đổi mật khẩu cho tài khoản này.

Giao diện sau khi đăng nhập thành công:



Hình 3. 28 Giao diện quản trị Honneywall sau khi đăng nhập

3.4.3 Kịch bản thực hiện

Kịch bản tấn công 1: Tấn công dò quét cổng vào máy Win Server 2003

Bước 1:

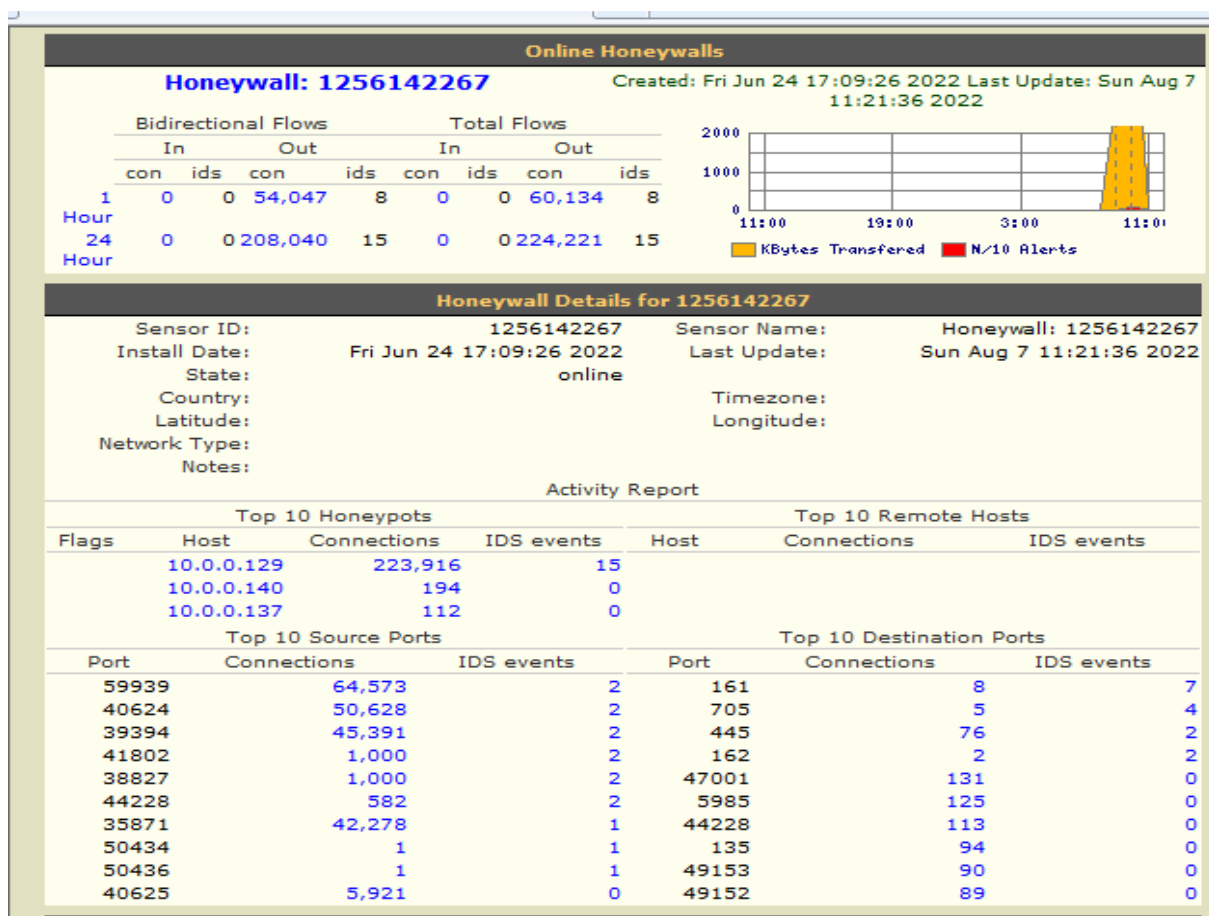
Tại máy Kali sử dụng Nmap tấn công quét cổng vào máy Win Server 2003

```
(root@boyqb221201)~#
# nmap -A 10.0.0.137
Starting Nmap 7.91 ( https://nmap.org ) at 2022-08-07 11:14 +07
Nmap scan report for 10.0.0.137
Host is up (0.00033s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows Server 2003 3790 microsoft-ds
1025/tcp  open  msrpc        Microsoft Windows RPC
1026/tcp  open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:BD:B8:2F (VMware)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp cpe:/o:microsoft:windows_server_2003
OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_server_2003
```

Hình 3. 29 Sử dụng Nmap để tấn công quét cổng vào máy

Bước 2:

Chuyển sang Windows 7, website quản trị của Honeywall thấy xuất hiện các thông tin hệ thống thu thập được.



Hình 3. 30 Giao diện quản trị của Honeywall đã thấy thông tin thu thập được

Các thông tin thu thập được:

- Số lượng kết nối tăng đột biến trong 1 giờ.
- Trong biểu đồ cho biết thời gian và tần suất kết nối
- Các địa chỉ IP của Honeypot gửi thông tin về
- Các sự kiện IDS cảnh báo
- Các cổng nhận được kết nối với cảnh báo IDS

Kích chọn phần kết nối nhận được để xem chi tiết:

(Previous Page)	Start	24899	24900	24901	24902	24903
	August 7th 11:16:09	00:00:00				
	10.0.0.129	0	10.0.0.137			
TCP	57219 (57219)	0 kB 1 pkts --	135 (epmap)			
0	os unkn	<--0 kB 1 pkts	---			
	August 7th 11:16:09	00:00:00				
	10.0.0.129	0	10.0.0.137			
TCP	57220 (57220)	0 kB 2 pkts --	135 (epmap)			
47	os unkn	<--0 kB 1 pkts	---			
	August 7th 11:16:09	00:00:00				
	10.0.0.129	0	10.0.0.137			
TCP	57221 (57221)	0 kB 1 pkts --	135 (epmap)			
16	os unkn	<--0 kB 1 pkts	---			
	August 7th 11:16:09	00:00:00				
	10.0.0.129	0	10.0.0.137			
TCP	57222 (57222)	0 kB 1 pkts --	1 (tcpmux)			
2	UNKNOWN	<--0 kB 1 pkts	---			
	August 7th 11:16:09	00:00:00				
	10.0.0.129	0	10.0.0.137			
TCP	57223 (57223)	0 kB 1 pkts --	1 (tcpmux)			
16	os unkn	<--0 kB 1 pkts	---			
	August 7th 11:16:09	00:00:00				
	10.0.0.129	0	10.0.0.137			
TCP	57224 (57224)	0 kB 1 pkts --	1 (tcpmux)			
41	os unkn	<--0 kB 1 pkts	---			
	August 7th 11:16:09	00:00:00				
	10.0.0.129	0	10.0.0.137			
TCP	37584 (37584)	0 kB 1 pkts --	12576 (12576)			
2	UNKNOWN	<--0 kB 1 pkts	---			

Hình 3. 31 Hình ảnh các kết nối nhận được

Nhận thấy có 1 IP nguồn với cổng mặc định gửi rất nhiều các gói tin tới IP đích với các cổng khác nhau.

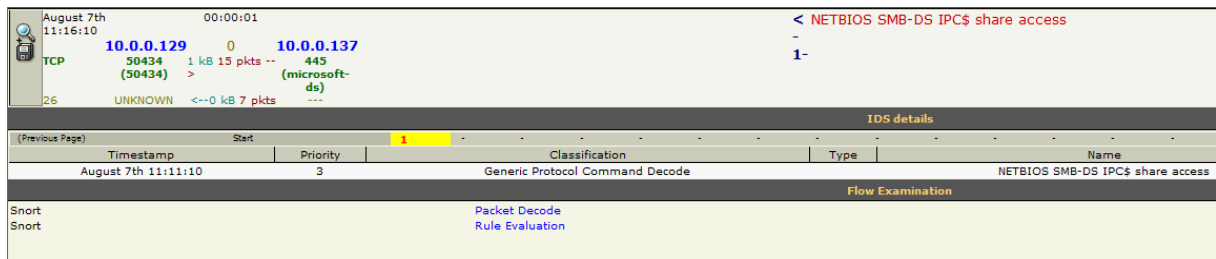
Kích chọn các sự kiện mà IDS cảnh báo:

Activity Report						
Top 10 Honeypots				Top 10 Remote Hosts		
Flags	Host	Connections	IDS events	Host	Connections	IDS events
	10.0.0.129	223,916	15			
	10.0.0.140	194	0			
	10.0.0.137	112	0			
Top 10 Source Ports				Top 10 Destination Ports		
Port	Connections	IDS events		Port	Connections	IDS events

Hình 3. 32 Kết quả thu được

	August 7th 11:15:14	00:00:00		< SNMP AgentX/tcp request
	10.0.0.129	0	10.0.0.137	-
TCP	44228 (44228)	0 kB 1 pkts --	705 (agentx)	1-
2	UNKNOWN	<--0 kB 1 pkts	---	
	August 7th 11:15:14	00:00:00		< SNMP request tcp
	10.0.0.129	0	10.0.0.137	-
TCP	44228 (44228)	0 kB 1 pkts --	161 (snmp)	1-
2	UNKNOWN	<--0 kB 1 pkts	---	
	August 7th 11:16:10	00:00:01		< NETBIOS SMB-DS IPC\$ share access
	10.0.0.129	0	10.0.0.137	-
TCP	50434 (50434)	1 kB 15 pkts --	445 (microsoft-ds)	1-
26	UNKNOWN	<--0 kB 7 pkts	---	
	August 7th 11:16:11	00:00:00		< NETBIOS SMB-DS IPC\$ share access
	10.0.0.129	0	10.0.0.137	-
TCP	50436 (50436)	0 kB 10 pkts --	445 (microsoft-ds)	1-
26	UNKNOWN	<--0 kB 5 pkts	---	

Hình 3. 33 Các sự kiện mà IDS cảnh báo



Kích chọn biểu tượng kính lúp và đĩa mềm để phân tích sâu hơn

Một máy nguồn gửi gói tin với cờ SYN tới máy đích có cổng 445, các gói tiếp theo giữa 2 máy có cờ SYN, ACK và kết thúc bằng cờ ACK => đây là quá trình bắt tay 3 bước TCP

Hình 3. 35 Tiến trình kết nối

```

08/07-11:16:10.413348 0:C:29:3:DD:A4 -> 0:C:29:BD:B8:2F type:0x800 len:0x4A
10.0.0.129:50434 -> 10.0.0.137:445 TCP TTL:64 TOS:0x0 ID:8095 IpLen:20 DgmLen:60 DF
*****S* Seq: 0x4A36A028 Ack: 0x0 Win: 0xFAF0 TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 3948862958 0 NOP WS: 7

=====

08/07-11:16:10.413348 0:C:29:3:DD:A4 -> 0:C:29:BD:B8:2F type:0x800 len:0x4A
10.0.0.129:50434 -> 10.0.0.137:445 TCP TTL:64 TOS:0x0 ID:8095 IpLen:20 DgmLen:60 DF
*****S* Seq: 0x4A36A028 Ack: 0x0 Win: 0xFAF0 TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 3948862958 0 NOP WS: 7

=====

08/07-11:16:10.413475 0:C:29:BD:B8:2F -> 0:C:29:3:DD:A4 type:0x800 len:0x4E
10.0.0.137:445 -> 10.0.0.129:50434 TCP TTL:128 TOS:0x0 ID:1208 IpLen:20 DgmLen:64 DF
***A**S* Seq: 0x89E4BB0D Ack: 0x4A36A029 Win: 0xFFFF TcpLen: 44
TCP Options (9) => MSS: 1460 NOP WS: 0 NOP NOP TS: 0 0 NOP NOP SackOK

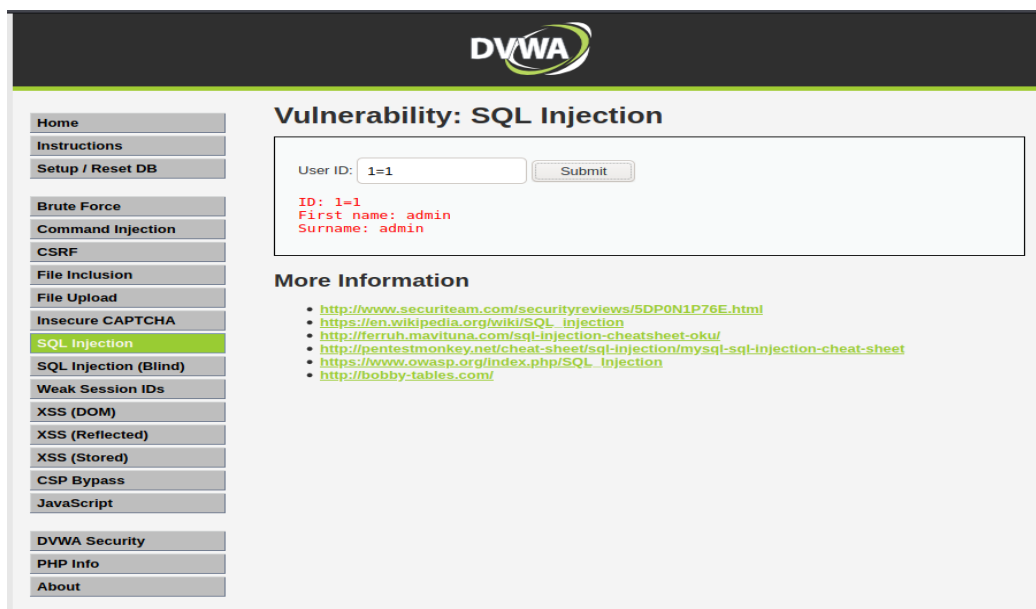
=====

```

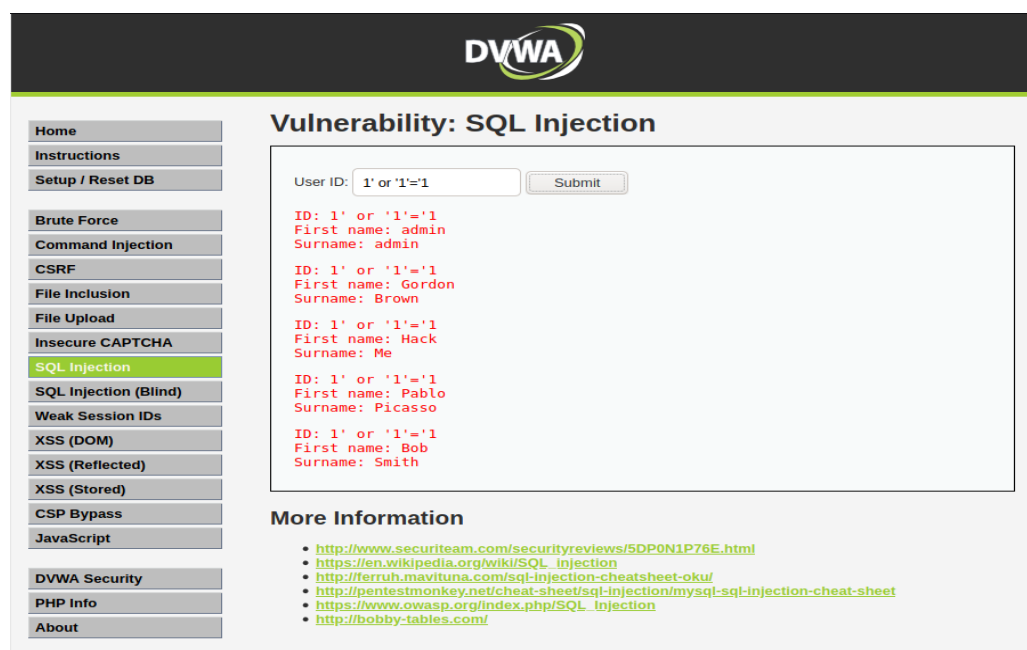
Kết luận: Từ thông tin thu thập được của Honeywall người quản trị biết được một máy tính nào đó có IP 10.0.0.129 đang tấn công dò quét cổng và hệ điều hành của máy Win Server 2003.

Kịch bản tấn công 2: Tấn công SQL Injection máy DVWA

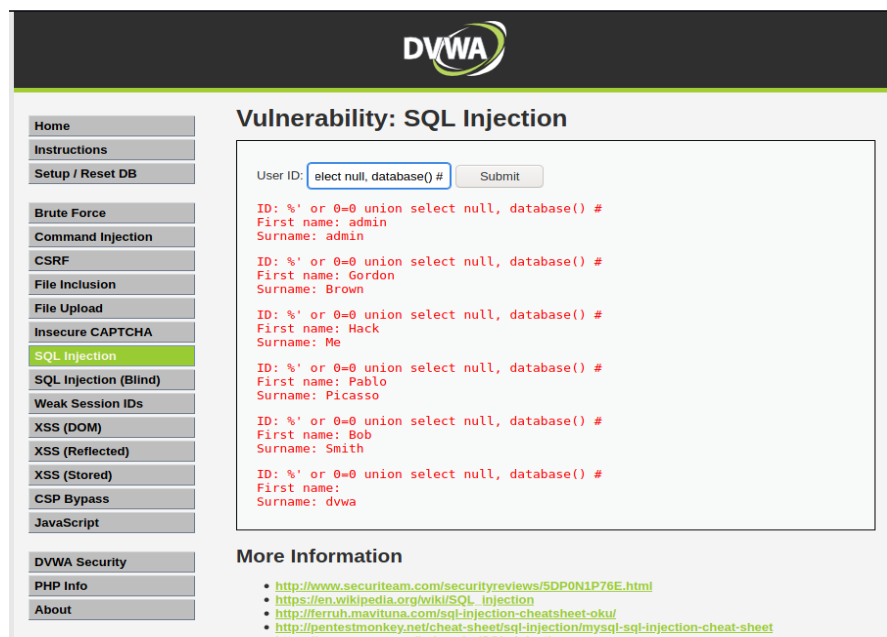
Bước 1: Tấn công



Hình 3. 39 Trường hợp 1



Hình 3. 38 Trường hợp 2



Hình 3. 41 Trường hợp 3

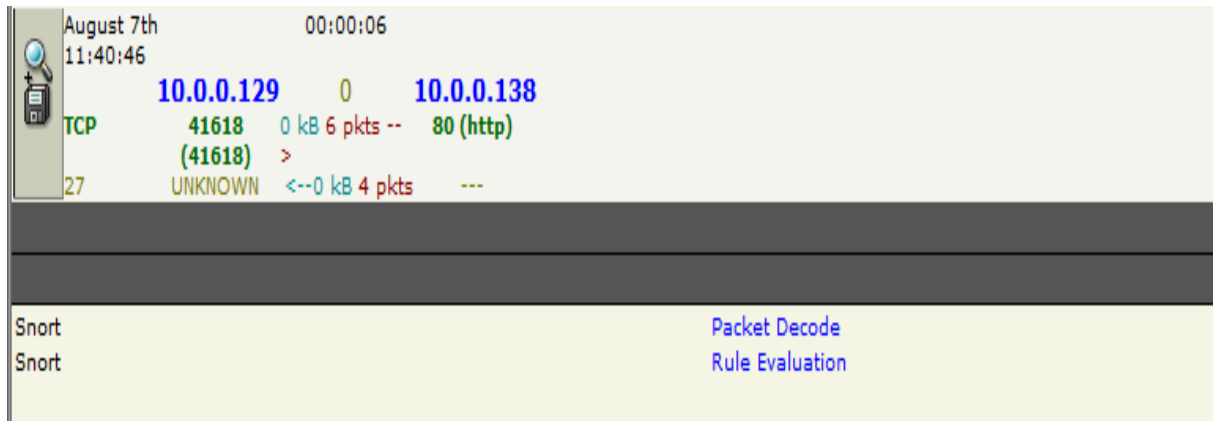
Bước 2:

Chuyển sang Windows 7, website quản trị của Honeywall thấy xuất hiện các thông tin hệ thống thu thập được:

August 7th 11:36:10	00:00:05	
TCP	10.0.0.129	0 10.0.0.138
	41606	1 kB 7 pkts -- 80 (http)
	(41606)	>
27	UNKNOWN	<--1 kB 6 pkts ---
August 7th 11:36:10	00:00:05	
TCP	10.0.0.129	0 10.0.0.138
	41608	0 kB 4 pkts -- 80 (http)
	(41608)	>
19	UNKNOWN	<--0 kB 2 pkts ---
August 7th 11:36:20	00:00:06	
TCP	10.0.0.129	0 10.0.0.138
	41610	1 kB 7 pkts -- 80 (http)
	(41610)	>
27	UNKNOWN	<--2 kB 7 pkts ---
August 7th 11:36:27	00:00:10	
TCP	10.0.0.129	0 10.0.0.138
	41612	2 kB 12 pkts -- 80 (http)
	(41612)	>
27	UNKNOWN	<--5 kB 9 pkts ---
August 7th 11:36:42	00:00:05	
TCP	10.0.0.129	0 10.0.0.138
	41614	0 kB 6 pkts -- 80 (http)
	(41614)	>
27	UNKNOWN	<--1 kB 5 pkts ---
August 7th 11:36:56	00:00:05	
TCP	10.0.0.129	0 10.0.0.138
	41616	0 kB 6 pkts -- 80 (http)
	(41616)	>
27	UNKNOWN	<--2 kB 5 pkts ---

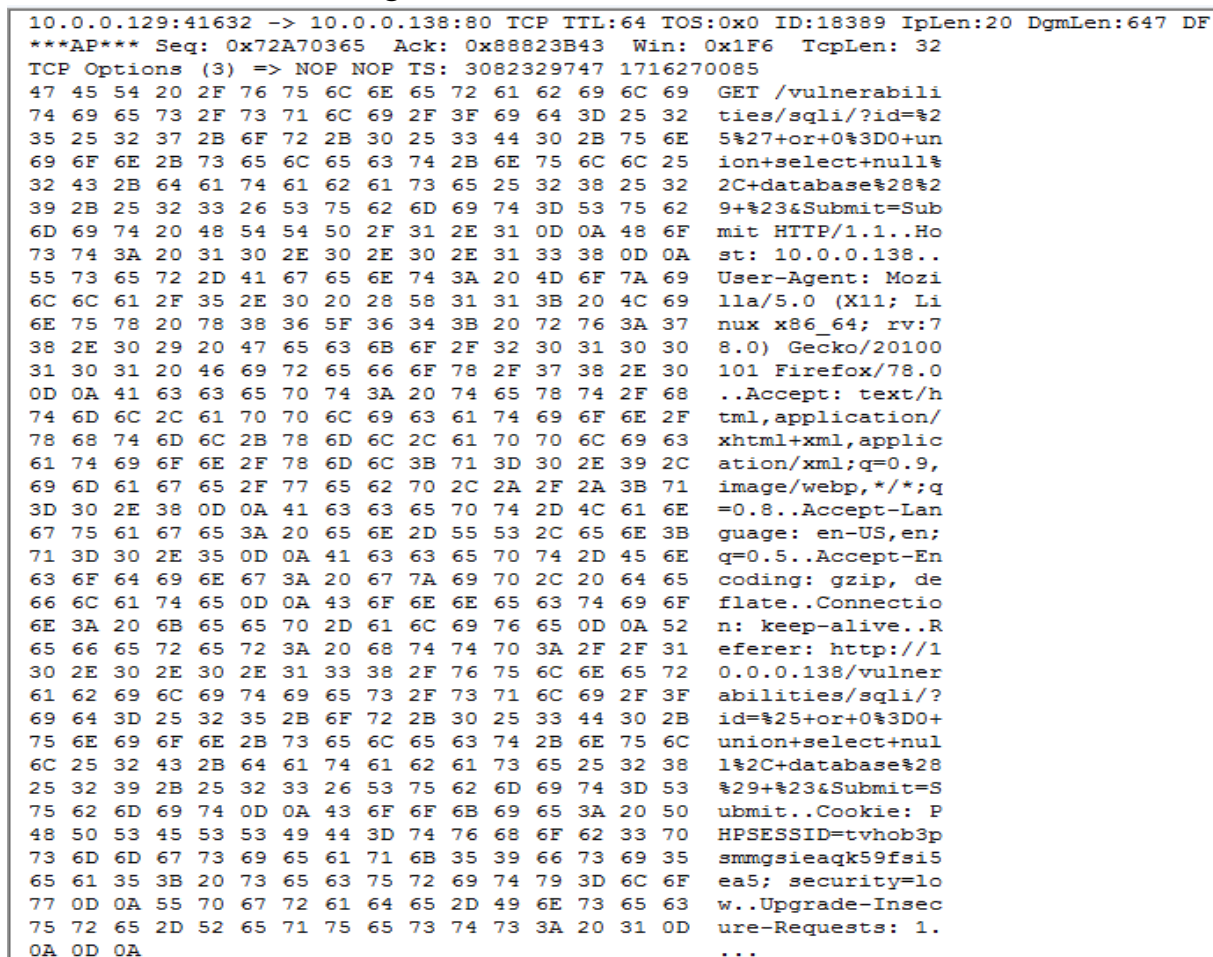
Hình 3. 39 Hiện thị thông tin thu thập được

Kích chọn biểu tượng kính lúp và đĩa mềm để phân tích sâu hơn



Hình 3. 40 Phân tích chi tiết

Kích vào chức năng Packet Decode để xem tiến trình kết nối:



Hình 3. 41 Các gói tin chứa thông tin của cách tấn công SQL Injection

Kết luận: Từ thông tin thu thập được của Honeywall người quản trị biết được một máy tính nào đó có IP 10.0.0.129 đang tấn công SQL Injection máy DVWA bằng những câu truy vấn nào

Kịch bản tấn công 3: Brute Force attack máy DVWA

Bước 1: Ở máy kali dùng hydra attack password

```
(root@hoyqb221201)~# hydra -l admin 10.0.0.138 -P /home/hoyqb221201/Downloads/rockyou.txt http-form-post "/login.php:username='USER'&password='PASS'&login=Login:Login failed" -V -F
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-07 12:21:56
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking http-form-post://10.0.0.138:80/login.php:username='USER'&password='PASS'&login=Login:Login failed
[ATTEMPT] target 10.0.0.138 - login 'admin' - pass '12345' - 1 of 14344398 [child 0] (0/0)
[ATTEMPT] target 10.0.0.138 - login 'admin' - pass '123456789' - 2 of 14344398 [child 1] (0/0)
[ATTEMPT] target 10.0.0.138 - login 'admin' - pass 'password' - 3 of 14344398 [child 2] (0/0)
[ATTEMPT] target 10.0.0.138 - login 'admin' - pass 'iloveyou' - 4 of 14344398 [child 3] (0/0)
[ATTEMPT] target 10.0.0.138 - login 'admin' - pass 'princess' - 5 of 14344398 [child 4] (0/0)
[ATTEMPT] target 10.0.0.138 - login 'admin' - pass '1234567' - 6 of 14344398 [child 5] (0/0)
[ATTEMPT] target 10.0.0.138 - login 'admin' - pass 'rockyou' - 7 of 14344398 [child 6] (0/0)
[ATTEMPT] target 10.0.0.138 - login 'admin' - pass '12345678' - 8 of 14344398 [child 7] (0/0)
[ATTEMPT] target 10.0.0.138 - login 'admin' - pass 'abc123' - 9 of 14344398 [child 8] (0/0)
[ATTEMPT] target 10.0.0.138 - login 'admin' - pass 'nicole' - 10 of 14344398 [child 9] (0/0)
[ATTEMPT] target 10.0.0.138 - login 'admin' - pass 'daniel' - 11 of 14344398 [child 10] (0/0)
[ATTEMPT] target 10.0.0.138 - login 'admin' - pass 'babygirl' - 12 of 14344398 [child 11] (0/0)
[ATTEMPT] target 10.0.0.138 - login 'admin' - pass 'monkey' - 13 of 14344398 [child 12] (0/0)
[ATTEMPT] target 10.0.0.138 - login 'admin' - pass 'lovely' - 14 of 14344398 [child 13] (0/0)
[ATTEMPT] target 10.0.0.138 - login 'admin' - pass 'jessica' - 15 of 14344398 [child 14] (0/0)
[ATTEMPT] target 10.0.0.138 - login 'admin' - pass '554321' - 16 of 14344398 [child 15] (0/0)
[ATTEMPT] target 10.0.0.138 - login 'admin' - pass 'michael' - 17 of 14344398 [child 16] (0/0)
[ATTEMPT] target 10.0.0.138 - login 'admin' - pass 'ashley' - 18 of 14344398 [child 17] (0/0)
[ATTEMPT] target 10.0.0.138 - login 'admin' - pass 'qwerty' - 19 of 14344398 [child 18] (0/0)
[80][http-post-form] host: 10.0.0.138 login: admin password: password
[STATUS] attack finished for 10.0.0.138 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-08-07 12:21:58
```

Hình 3. 42 Giao diện của hydra attack password

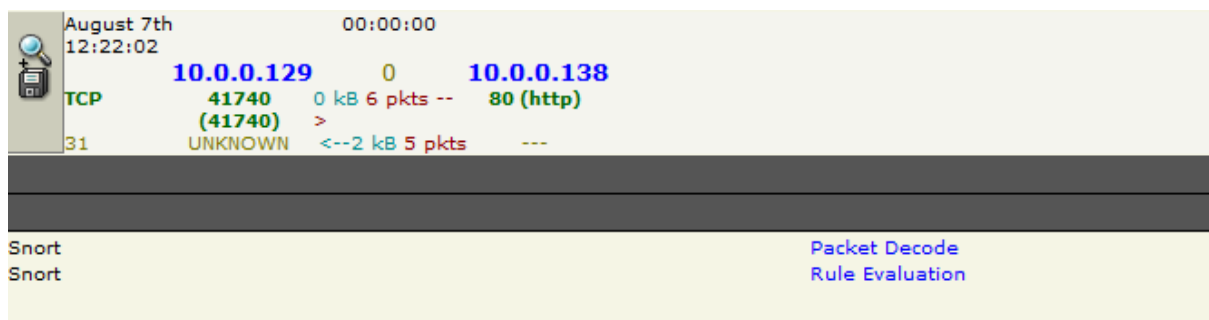
Bước 2:

Chuyển sang Windows 7, website quản trị của Honeywall thấy xuất hiện các thông tin hệ thống thu thập được:

August 7th 11:36:10	00:00:05	10.0.0.129	0	10.0.0.138
TCP	41606	1 kB 7 pkts --	80 (http)	
(41606)	>			
27	UNKNOWN	<--1 kB 6 pkts	---	
August 7th 11:36:10	00:00:05	10.0.0.129	0	10.0.0.138
TCP	41608	0 kB 4 pkts --	80 (http)	
(41608)	>			
19	UNKNOWN	<--0 kB 2 pkts	---	
August 7th 11:36:20	00:00:06	10.0.0.129	0	10.0.0.138
TCP	41610	1 kB 7 pkts --	80 (http)	
(41610)	>			
27	UNKNOWN	<--2 kB 7 pkts	---	
August 7th 11:36:27	00:00:10	10.0.0.129	0	10.0.0.138
TCP	41612	2 kB 12 pkts --	80 (http)	
(41612)	>			
27	UNKNOWN	<--5 kB 9 pkts	---	
August 7th 11:36:42	00:00:05	10.0.0.129	0	10.0.0.138
TCP	41614	0 kB 6 pkts --	80 (http)	
(41614)	>			
27	UNKNOWN	<--1 kB 5 pkts	---	
August 7th 11:36:56	00:00:05	10.0.0.129	0	10.0.0.138
TCP	41616	0 kB 6 pkts --	80 (http)	
(41616)	>			
27	UNKNOWN	<--2 kB 5 pkts	---	

Hình 3. 43 Các thông tin hệ thống thu thập được

Kích chọn biểu tượng kính lúp và đĩa mềm để phân tích sâu hơn



Hình 3. 44 Thông tin chi tiết

```

63 73 73 22 20 68 72 65 66 3D 22 64 76 77 61 2F  css" href="dvwa/
63 73 73 2F 6C 6F 67 69 6E 2E 63 73 73 22 20 2F  css/login.css" /
3E 0D 0A 0D 0A 09 3C 2F 68 65 61 64 3E 0D 0A 0D  >.....</head>...
0A 09 3C 62 6F 64 79 3E 0D 0A 0D 0A 09 3C 64 69  ..<body>.....<di
76 20 69 64 3D 22 77 72 61 70 70 65 72 22 3E 0D  v id="wrapper">.
0A 0D 0A 09 3C 64 69 76 20 69 64 3D 22 68 65 61  ....<div id="hea
64 65 72 22 3E 0D 0A 0D 0A 09 3C 62 72 20 2F 3E  der">.....<br />
0D 0A 0D 0A 09 3C 70 3E 3C 69 6D 67 20 73 72 63  ....<p><img src
3D 22 64 76 77 61 2F 69 6D 61 67 65 73 2F 6C 6F  ="dvwa/images/lo
67 69 6E 5F 6C 6F 67 6F 2E 70 6E 67 22 20 2F 3E  gin_logo.png" />
3C 2F 70 3E 0D 0A 0D 0A 09 3C 62 72 20 2F 3E 0D  </p>.....<br />.
0A 0D 0A 09 3C 2F 64 69 76 3E 20 3C 21 2D 2D 3C  ....</div> <!--<
64 69 76 20 69 64 3D 22 68 65 61 64 65 72 22 3E  div id="header">
2D 2D 3E 0D 0A 0D 0A 09 3C 64 69 76 20 69 64 3D  -->.....<div id=
22 63 6F 6E 74 65 6E 74 22 3E 0D 0A 0D 0A 09 3C  "content">.....<
66 6F 72 6D 20 61 63 74 69 6F 6E 3D 22 6C 6F 67  form action="log
69 6E 2E 70 68 70 22 20 6D 65 74 68 6F 64 3D 22  in.php" method="
70 6F 73 74 22 3E 0D 0A 0D 0A 09 3C 66 69 65 6C  post">.....<fiel
64 73 65 74 3E 0D 0A 0D 0A 09 09 09 3C 6C 61 62  dset>.....<lab
65 6C 20 66 6F 72 3D 22 75 73 65 72 22 3E 55 73  el for="user">Us
65 72 6E 61 6D 65 3C 2F 6C 61 62 65 6C 3E 20 3C  ername</label> <
69 6E 70 75 74 20 74 79 70 65 3D 22 74 65 78 74  input type="text
22 20 63 6C 61 73 73 3D 22 6C 6F 67 69 6E 49 6E  " class="loginIn
70 75 74 22 20 73 69 7A 65 3D 22 32 30 22 20 6E  put" size="20" n
61 6D 65 3D 22 75 73 65 72 6E 61 6D 65 22 3E 3C  ame="username"><
62 72 20 2F 3E 0D 0A 0D 0A 0D 0A 09 09 09 3C 6C  br />.....<l
61 62 65 6C 20 66 6F 72 3D 22 70 61 73 73 22 3E  abel for="pass">
50 61 73 73 77 6F 72 64 3C 2F 6C 61 62 65 6C 3E  Password</label>
20 3C 69 6E 70 75 74 20 74 79 70 65 3D 22 70 61  <input type="pa
73 73 77 6F 72 64 22 20 63 6C 61 73 73 3D 22 6C  ssword" class="l
6F 67 69 6E 49 6E 70 75 74 22 20 41 55 54 4F 43  oginInput" AUTOC
4F 4D 50 4C 45 54 45 3D 22 6F 66 66 22 20 73 69  OMPLETE="off" si
7A 65 3D 22 32 30 22 20 6E 61 6D 65 3D 22 70 61  ze="20" name="pa
73 73 77 6F 72 64 22 3E 3C 62 72 20 2F 3E 0D 0A  ssword"><br />..

```

Hình 3. 45 Các gói tin có chứa mật khẩu mà chúng ta dùng hydra tấn công Brute Force máy DVWA

Kết luận: Từ thông tin thu thập được của Honeywall người quản trị biết được một máy tính nào đó có IP 10.0.0.129 đang tấn công Brute Force máy DVWA bằng hydra và mật khẩu mà họ đã tìm được

Kết luận chung

Sau thời gian nghiên cứu và thực hiện đề tài “Các kỹ thuật đảm bảo an toàn mạng”, chúng em nhận ra được tầm vô cùng quan trọng của an ninh mạng, có được cái nhìn tổng quan, hiểu được an ninh mạng là gì, xác định được các mối đe dọa đến từ an ninh mạng. Cùng với đó là tìm hiểu và nắm bắt được một số phương pháp tấn công mạng và cách phòng chống nó, đồng thời tìm hiểu về các kỹ thuật đảm bảo an toàn mạng và thực hiện các thực nghiệm về các kỹ thuật đảm bảo an toàn mạng.

Tuy nhiên, nhóm vẫn còn những vấn đề tồn đọng đó là chưa tìm hiểu hết tất cả các kỹ thuật đảm bảo an toàn mạng hiện có, các thực nghiệm vẫn chưa thực hiện được các kịch bản khó và phức tạp.

Định hướng phát triển:

Tìm hiểu và thực hiện thực nghiệm hết những kỹ thuật đảm bảo an toàn mạng, chủ động đi sâu hơn thực hiện những kịch bản khó và phức tạp. Đồng thời tiếp tục tiếp thu những kiến thức an ninh mạng mới để luôn sẵn sàng phòng chống những cuộc tấn công trên Internet.

Tài liệu tham khảo

- [1] William Stallings, Network Security Essentials: Applications and Standards, PrenticeHall, New Jersey, 2010.
- [2] Andrew S.Tanenbaum, Computer Networks, Prentice Hall, New Jersey, Fourth Edition, 2010.
- [3] Man Young Rhee, Wilay, Internet Security -Cryptographic Principles, Algorithms and Protocols, 2010.