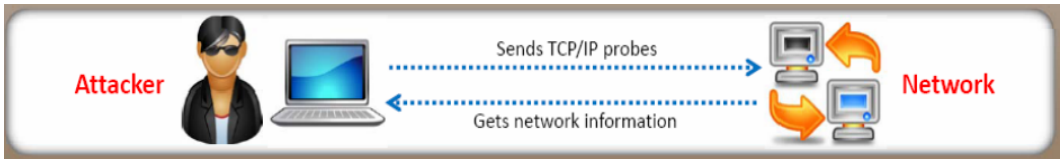
Module 3
Scanning Network

Các Chủ Đề Chính Trong Chương Này

Định Nghĩa Các Kiểu Scanning.
Quy Trình Scanning Của CEH.
Kiểm Tra Các Hệ Thống Đang Hoạt Động Và Những Cổng Mở.
Nắm Vững Các Kỹ Thuật Quét Mạng.
Các Công Cụ Thường Dùng Trong Quá Trình Quét Mạng.
Banner Grabbing Và OS Fingerpringting
Lập Sơ Đồ Mạng Của Các Host Nhạy Cảm.
Chuẩn Bị Proxy.
Anonymize Là Gì ?
Phòng Chống Kiểu Tấn Công Quét Mạng.

Trong bước đầu tiên của tiến trình tấn công các hacker thường tiến hành quét mạng mà chúng ta sẽ gọi bằng thuật ngữ *scanning* để kiểm tra các cổng đang mở hay những dịch vụ mà mục tiêu đang sử dụng. Bên cạnh đó *scanning* còn cho biết các thông tin quan trọng như hệ điều hành đang sử dụng hay hệ thống máy chủ mà trang web đang dùng là IIS, Apache …

Scanning bao gồm các thao tác để xác định các host (máy trạm) và những port (cổng) đang hoạt động hay những dịch vụ đang chạy trên hệ thống của mục tiêu cần tấn công và khai thác. Đây là một trong những bước quan trọng của tiến trình thu thập thông tin thông minh (*intelligence gathering*) mà các hacker sử dụng để lập sơ đồ của các tổ chức hay mạng mục tiêu. Trong tiến trình scanning những kẻ tấn công sẽ gởi các gói tin TCP/IP đến mục tiêu như Hình 3.1 và phân tích các kết quả trả về nhằm xác định các thông tin giá trị mà họ quan tâm.



Hình 3.1 – Attacker gởi các gói tin thăm dò mạng

Các Kiểu Scanning

Có ba dạng *scanning* khác nhau đó là *Port Scanning, Vulnerability Scanning* và *Network Scanning*.

Hình 3.2 – Các Kiểu Scanning

Port Scanning : Kẻ tấn công sẽ gởi một loạt các thông điệp đến mục tiêu nhằm xác định các cổng đang mở, và thông qua các cổng này họ sẽ biết được có những dịch vụ nào đang chạy trên máy tính mục tiêu. Một trong các ứng dụng *port scanning* phổ biên là **Nmap**.

Vulnerability Scanning : Là quá trình quét lỗi nhằm xác định ra các lỗ hổng bảo mật hay những điểm yếu mà thường gọi là các điểm "nhạy cảm" của các ứng dụng hay máy chủ, máy trạm đê từ đó đưa ra các phương án tấn công thích hợp. Tiến trình quét lỗi có thể xác định được các bản cập nhật hệ thống bị thiếu, hay những lỗi hệ thống chưa được vá các chuyên gia bảo mật cũng thường tiến hành *vulnerability scanning* trong công tác bảo vệ hệ thống mạng của mình.

Network Scanning : Quá trình này dùng để xác định các máy đang hoạt động trên hệ thống mạng thường được các hacker, chuyên gia bảo mật hay những quản trị hệ thống thực hiện.

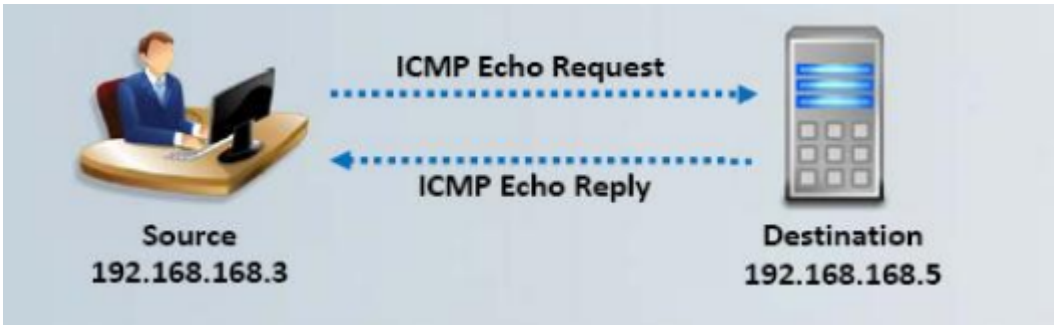
Quy Trình Scanning Của CEH

Kiểm Tra Các Hệ Thống Đang Hoạt Động

Để kiểm tra tình trạng hoạt động của hệ thống các hacker có thể sử dụng nhiều công cụ và những hình thức khác nhau để thu được kết qua mong muốn như *ICMP Scanning* hay *Ping Sweep*.

ICMP Scanning

Hacker sẽ gởi các tín hiệu *ICMP ECHO Request* đến mục tiêu (host) và nếu một host đang tồn tại nghĩa là đang hoạt động thì sẽ phản hồi lại thông qua *ICMP ECHO Reply* như Hình 3.3. Tuy nhiên, quá trình này có thể thất bại nếu như giao thức ICMP bị chặn bởi firewall.



Hình 3.3 – ICMP Scanning

Kết quả của *ICMP Scanning* thực hiện bằng công cụ Nmap

```
#nmap -sP -v 192.168.168.5
Starting nmap 5.21 (http://nmap.org) at 2010-07-11 16:30 EDT
Host 192.168.168.5 appears to be up.
MAC Address: 00:E8:48:12:CD:8A (Hewlett Packard)
Nmap finished: 1 IP address (1 host up) scanned in 0.889 seconds
Raw packets sent: 5 (30B) | Rcvd: 2 (25B)
```

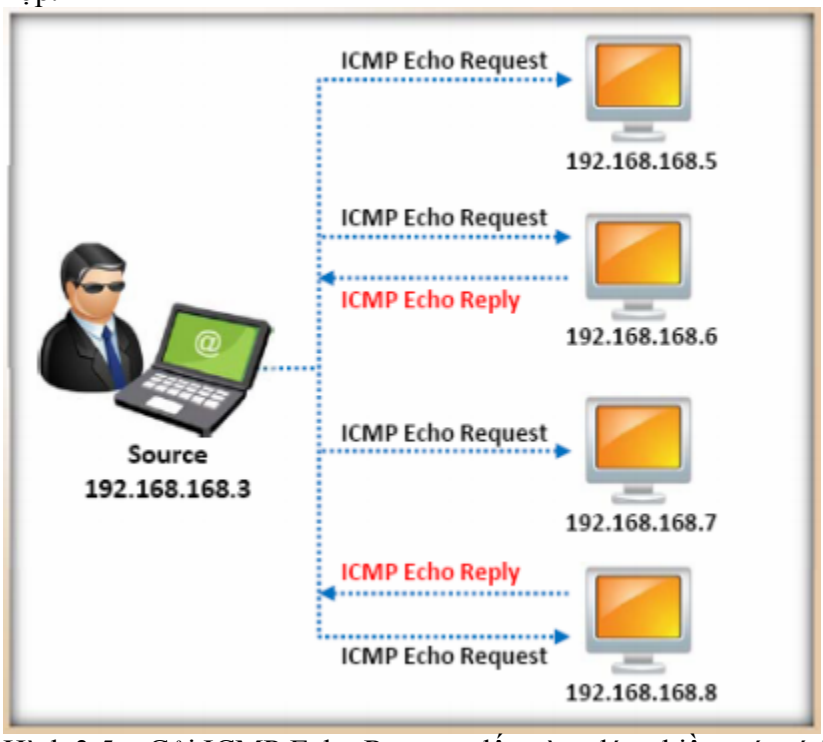
Hình 3.4 – Scanning với Nmap

Trong hình minh họa trên hacker từ máy **192.168.168.3** sẽ tiến hành *ICMP Scanning* bằng công cụ Nmap để gởi các tín hiệu *ICMP ECHO Request* thông qua tùy chọn **–sP** đến mục tiêu có địa chỉ **192.168.168.5** và các bạn có thể thất kết quả trả về cho biết

mục tiêu có địa chỉ **192.168.168.**5 đang hoạt động với các thông số phần cứng như địa chỉ *MAC*, nhà sản xuất.

Ping Sweep

Trong ví dụ trên chúng ta sử dụng *ICMP Scanning* để xác định tình trạng hoạt động của một máy trạm, nếu như các bạn muốn kiểm tra trên một dãy các địa chỉ IP thì *Ping Sweep* là giải pháp thích hợp thông qua hình thức gởi các tín hiệu *ICMP ECHO Request* đến nhiều máy tính cùng lúc như Hình 3.5 để nhận các kết quả trả về thích hợp.



Hình 3.5 – Gởi ICMP Echo Request đến cùng lúc nhiều máy tính.

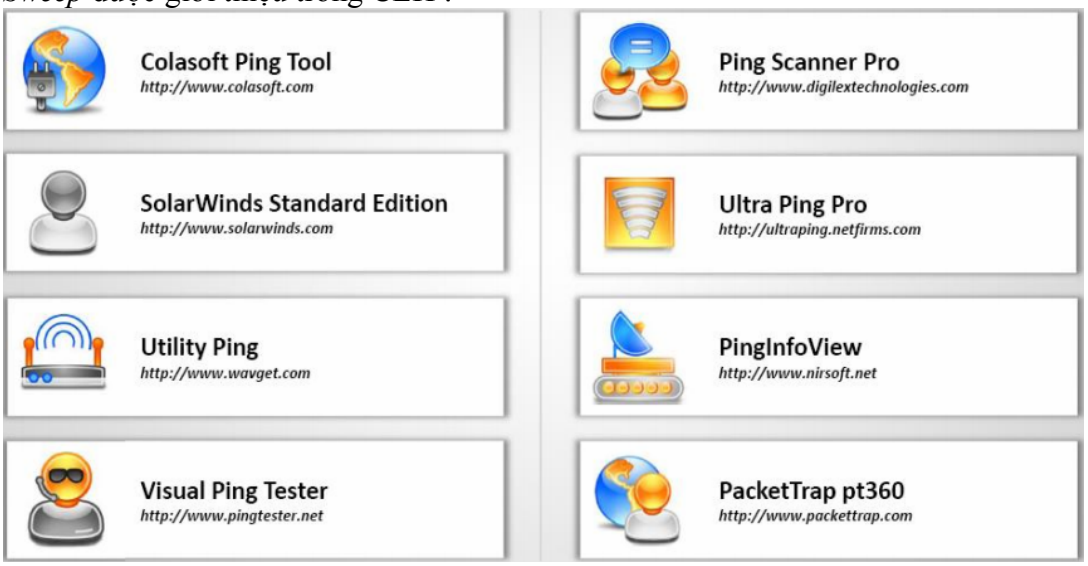
Sau đây là kết quả của *Ping Sweep* với Nmap :

```
nmap -sP -PE -PA21,23,80,3389 192.168.168.
50

Starting Nmap 5.21 ( http://nmap.org ) at
2010-07-13 14:16 EDT
Nmap scan report for 192.168.168.1
Host is up (0.00s latency).
MAC Address: 00:A8:5A:E0:83:05 (Hewlett
Packard)
Nmap scan report for 192.168.168.2
Host is up (0.016s latency).
MAC Address: 00:01:6B:0A:8E:15 (Foxconn)
Nmap scan report for 192.168.168.4
Host is up (0.00s latency).
MAC Address: 00:2A:B9:03:DD:80 (Dell)
Nmap scan report for 192.168.168.6
Host is up (0.00s latency).
```

Hình 3.6 – Ping Sweep với Nmap

Theo Hình 3.6 thì chúng ta thấy kết quả trả về khá chi tiết với các máy tính có địa chỉ IP *192.168.168.1, 192.168.168.2, 192.168.168.4* và *192.168.168.6* đang hoạt động.
Các công cụ *Ping Sweep* khác thường được sử dụng là **Angry IP Scanner** và **Solarwinds Engineer's Toolset**. Trong Hình 3.7 là danh sách các công cụ *Ping Sweep* được giới thiệu trong CEH :



Hình 3.7 – Các công cụ Ping Sweep

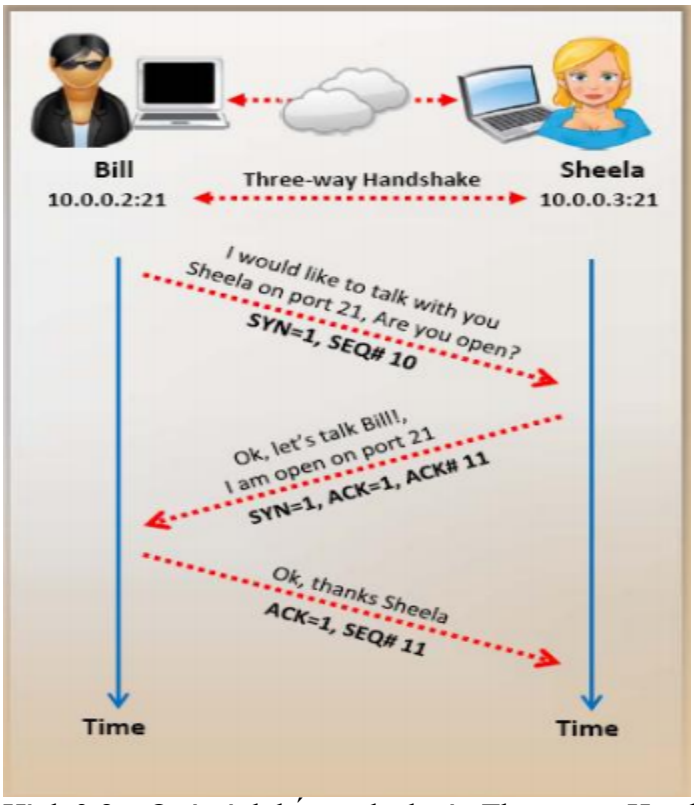
Phòng Chống Ping Sweep

Hầu hết các hệ thống *IDS – Instruction Detect System* (hệ thống phát hiện xâm nhập trái phép) đều có thể nhận biết được dạng tấn công *Ping Sweep* và gởi cảnh báo về cho quản trị hệ thống mạng. *IDS* có thể là những thiết bị phần cứng của **Cisco 4250/4235 Appliance Sensor**, **Juniper Networks Intrusion Detection** với các dòng

IDP75, IDP250 hay các ứng dụng *IDS* phần mềm nguồn mở như **SNORT** hoạt động dưới cả hai dạng *Network-base IDS* và *Host-based IDS*. Ngoài ra, phần lớn các firewalll và proxy server được cấu hình để chặn ICMP mặc định, giúp phòng chống Ping Sweep hiệu quả.

Xác Định Những Cổng Mở Và Dịch Vụ Đang Hoạt Động

Các cổng (hay port) đang mở có nghĩa là các dịch vụ liên quan đến những cổng này đang hoạt động và thông qua kết quả đó hacker sẽ xác định phương án tấn công thích hợp với những dịch vụ. Để có thể nắm vững kỹ thuật này các bạn cần hiểu rõ quá trình bắt tay 3 bước hay thường được gọi là Three-Way Handshake khi các máy tính sử dụng giao thức truyền thông TCP tại tầng vận chuyển như Hình 3.8 :



Hình 3.8 – Quá trình bắt tay ba bước Three-way Handshake

Trong hình trên, máy tính của *Bill* có địa chỉ 10.0.0.2 cần khởi tạo một phiên làm việc truyền file qua giao thức FTP (số hiệu port là 21) đến máy tính của *Sheela* có địa chỉ là 10.0.0.3. Vì vậy Bill Computer sẽ gởi các tín hiệu SYN=1 và SEQ# 10 đến Sheela Computer, sau đó ta thấy máy tính 10.0.0.3 trả về thông báo chấp nhận kết nối với tín hiệu SYN=1 và ACK=1 (thông báo chấp nhận kết nối), cùng với ACK# 11. Khi tiếp nhận những tín hiệu này, máy tính của Bill (10.0.0.2) đáp ứng lại thông báo báo nhận bằng cách gởi những tín hiệu ACK=1 với số hiệu SEQ# 11 (tăng 1 giá trị). Lúc này phiên làm việc sẽ được kết nối giữa 2 máy tính 10.0.0.2 và 10.0.0.3 trên port 21.

Sau đây là một số tín hiệu (còn gọi là các cờ) được dùng trong các quá trình khởi tạo phiên làm việc này :

SYN (Synchronize) : Dùng khi khởi tạo kết nối giữa hai máy.

ACK (Acknowledgement) : Dùng để gởi thông báo chấp nhận khi nhận được tín hiệu từ máy gởi.

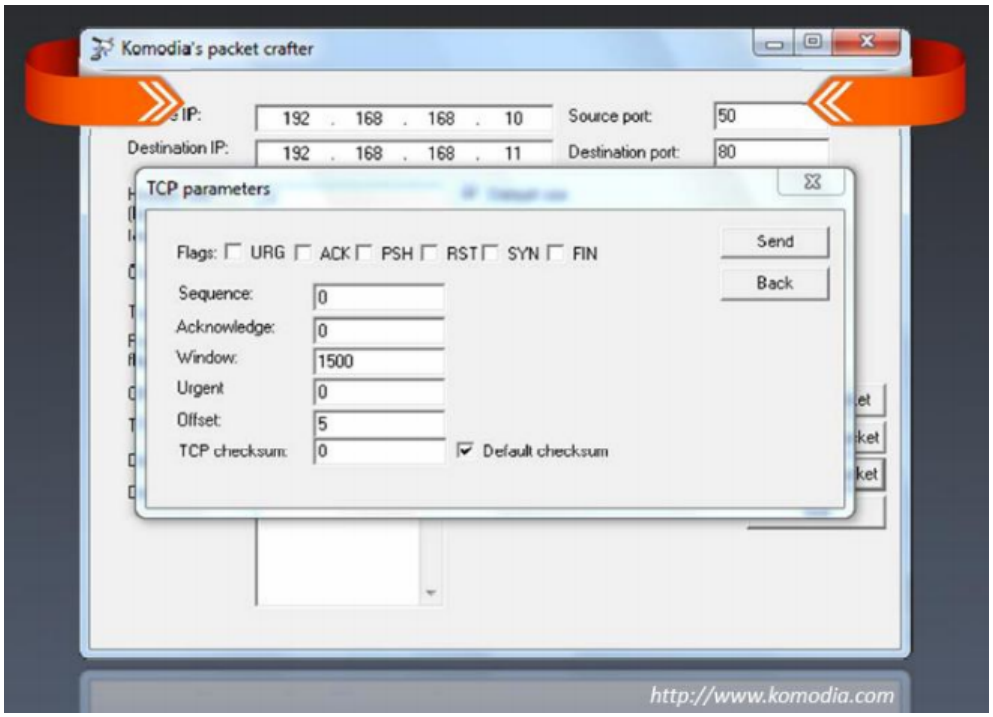
PSH (Push) : Yêu cầu xử lý các dữ liệu trong bộ nhớ đệm ngay lập tức.

RST (Reset) : Yêu cầu reset lại kết nối, các bạn lưu ý là khi nhận được tín hiệu này cũng có nghĩa là mục tiêu hay máy tính đang không hoạt động (Offline)

FIN (Finish) : Yêu cầu kết thúc liên kết

URG (Urgent) : Tín hiệu khẩn, có mức ưu tiên cao nhất. Khi nhận được dữ liệu cùng cờ này thì phải xử lý ngay.

Khi nắm vững ý nghĩa và mục đích của các cờ các bạn có thể tạo ra các gói tin với những giá trị được tùy biến cho phù hợp với yêu cầu của mình. Như Hình 3.9 minh họa ứng dụng *Komodia packet crafter* cho phép thiết lập các giá trị *flag* thích hợp của gói tin cũng như số hiệu port muốn kiểm tra khi gởi từ máy tính có IP 192.168.168.10 đến máy tính 192.168.168.11



Hình 3.9 - Komodia packet crafter

Phòng Chống Port-Scan

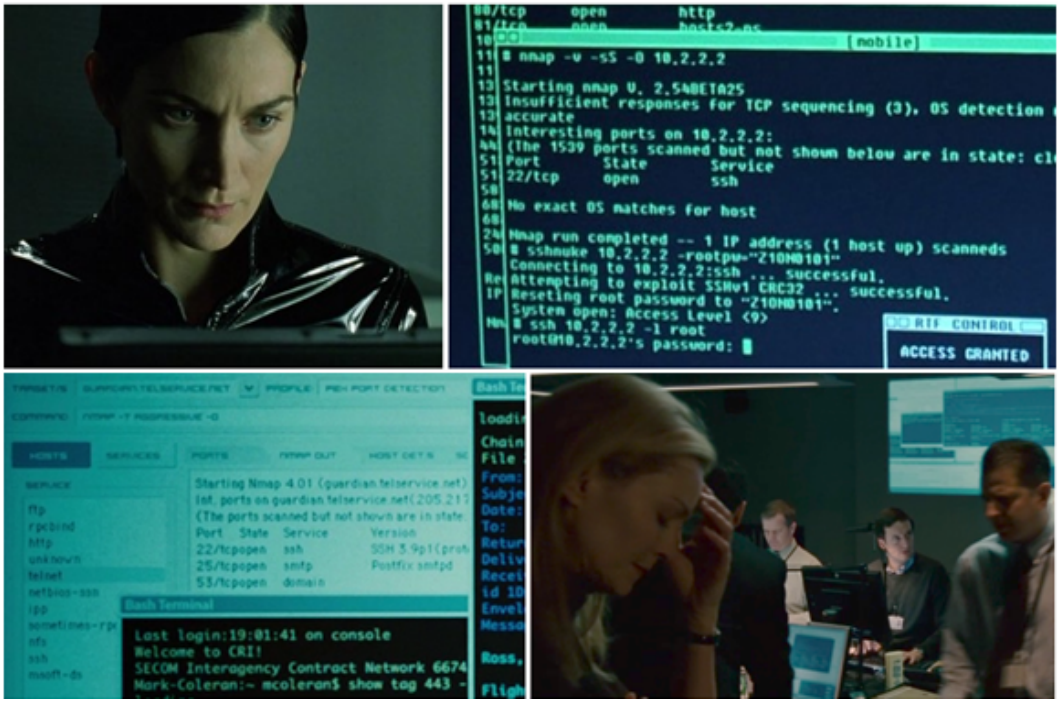
Để phòng chống tấn công quét cổng các hệ thống cần triển khai firewall và thiết lập các chính sách ngăn chặn những tín hiệu dò tìm hay khởi tạo kết nối không hợp lệ. Che dấu các cổng mở như hệ thống tường lữa ISA Server Firewall có chức năng hidden port. Đặc biệt chỉ mở các cổng cần thiết cho quá trình vận hành, đối với các dịch vụ không hoạt động hãy đóng những cổng liên quan.

Ngoài ra, hệ thống mạng cần được thiết kế khoa học theo các nguyên tắc phòng thủ theo chiều sâu với thiết bị *firewall* bảo vệ lớp ngoài và có *IDS* để phát hiện khi bị quét cổng.

Nmap

Chương trình quét cổng được đề cập nhiều nhất trong CEH là Nmap, đây là ứng dụng miễn phí có khả năng mạnh mẽ trong việc quét cổng, ping sweep, xác định dịch vụ, hệ điều hành. Nmap chạy được trên nền Windows hay Linux, Unix và có thể tiến hành quét cùng lúc nhiều máy tính. Nmap có thể tìm kiếm các cổng mở và những cổng được che dấu với các chức năng lọc. Ví dụ khi firewall chặn các ứng dụng quét cổng thông thường bằng cách ngắt những tín hiệu hồi đáp trong quá trình three-way handshake, hay ngăn ngừa việc tiếp nhận tín hiệu trên nhiều cổng trong thời gian ngắn thì nmap vẫn có thể vượt qua bằng phương pháp half-path scan hay tiến hành quét các cổng với thời gian cách xa nhau.

Chính vì những khả năng mạnh mẽ trên mà Nmap từng được các hacker và chuyên gia bầu chọn là ứng dụng tấn công số 1 thế giới nhiều năm liền. Và những bộ phim có cảnh tấn công của hacker như *Matrix Reloaded* sử dụng Nmap để tìm ra máy chủ SSH bị lỗi hoặc *The Bourne Ultimatum* cũng sử dụng Nmap phiên bản GUI là Zenmap để minh họa tiến trình kiểm tra dịch vụ đang chạy SSH 3.9p1, Posfix smtpd, và một name server như Hình 3.10.



Hình 3.10 – Sử dụng Nmap trong Matrix Reloades và The Bourne Ultimatum

Sau đây là một phương pháp quét mạng với Nmap mà các bạn cần ghi nhớ :

TCP connect : Hacker khởi tạo kết nối TCP đầy đủ với mục tiêu.

XMAS tree scan : Kiểm tra các dịch vụ TCP bằng cách gởi các gói tin XMAS-tree (các gói tin được đặc cờ FIN, URG và PSH.

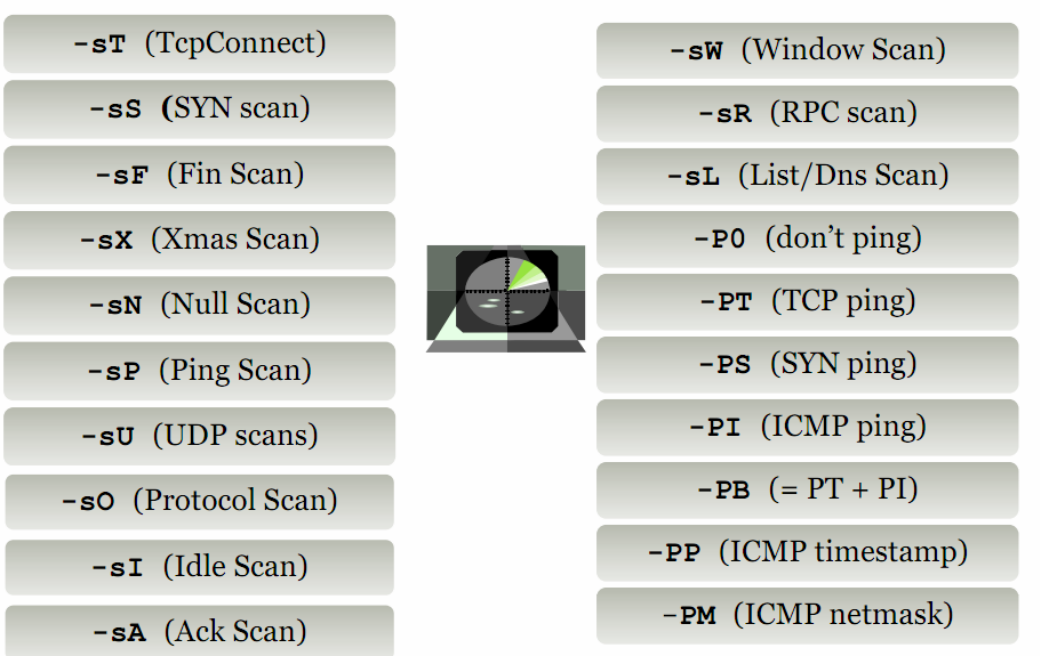
SYN stealth scan : Còn được gọi là *half-open scanning*. Hacker hỏi các gói tin SYN và nhận gói tin đáp ứng SYN-ACK từ server. Trong trường hợp này máy tính của hacker và server không thiết lập kết nối TCP đầy đủ nên được gọi là stealth.

Null scan : Đây là phương pháp quét mạng nâng cao và có thể vượt qua cờ chế dò tìm của firewall. Null scan chỉ hoạt động trên các hệ thống Unix với tất cả các cờ được tắt.

Windows scan : Tương tự như ACK scan và có thể phát hiển các cổng mở.

ACK scan : Được dùng để dò tìm các quy tắt của firewall, dạng này chỉ hoạt động trên hệ thống UNIX.

Ngoài ra, Nmap còn có nhiều tùy chọn thích hợp với những nhu cầu quét cổng hay dò tìm dịch vụ khác nhau như trong danh sách sau :



Ví dụ dùng Nmap để scan một máy có địa chỉ IP là 192.168.0.1 sủng dụng TCP connect scan ta thực hiện lệnh sau :

C:\nmap 192.168.0.1 –sT

SYN, STEALTH,XMAS, NULL, ADLE, và FIN Scan

SYN : SYN hoặc stealth scan cũng được gọi là haft-open scan vì nó không thực hiện đầy đủ quy trình bắt tay ba bước của TCP (three-way hanshake Hacker gửi gói tin SYN đến đích, nếu nhận lại một SYN/ACK, sau đó nó giả định các mục tiêu sẽ hoàn thành việc kết nối và các cổng đang lắng nghe. Nếu nó nhận một 1 RST từ mục tiêu, nó giả định cổng không hoạt động hay bị đóng. SYN stealth scan là ít bị phát hiện hơn bởi các hệ thống IDS.

XMAS: XMAS scan gửi một gói với cờ FIN,URG, và PSH được thiết lập. Nếu cổng mở, không đáp lại; nếu đóng mục tiêu gửi lại gói RST/ACK. XMAS scan chỉ làm việc trên hệ thống máy đích theo RFC 793 của TCP/IP.

FIN: FIN scan tương tự XMAS scan nhưng gửi gói dữ liệu chỉ với cờ FIN được thiết lập.

NULL: NULL scan cũng tương tự như XMAS và FIN trong giới hạn và trả lời, nhưng nó chỉ gửi một packet mà không có thiết lập cờ.

IDLE: IDLE scan sử dụng địa chỉ IP giả mạo để gửi một gói SYN đến mục tiêu. Phụ thuộc vào trả lời, cổng có thể được xác định là mở hoặc đóng. IDLE scan xác định phản ứng quét cổng bằng cách theo dõi số thứ tự IP header.

Công Cụ

Sau đây là một số công cụ có thể dùng để tiến hành quét cổng, xác định dịch vụ hay các máy đang hoạt động trên mạng :

IPEye là máy quét cổng TCP có thể làm SYN, FIN,Null, và XMAS scans. Nó là công cụ command-line(dòng lệnh). IPEye thăm dò cổng trên máy đích và phản hồi lại các trạng thái closed, reject, drop, or open. Closed có nghĩa là có một máy ở đầu bên kia nhưng nó không lắng nghe tại cổng. Reject là tường lửa từ chối kết nối tại cổng. Drop có nghĩa là tường lửa hủy bỏ mọi thứ vào cổng hoặc không có máy tính ở đầu bên kia. Open có nghĩa một số loại dịch vụ đang lắng nghe tại cổng. Những phản hồi này giúp hacker xác định loại của hệ thống đang trả lời.

IPSecScan là công cụ có thể quét một địa IP duy nhất hoặc một dãy địa chỉ IP tìm kiếm thông tin hệ thống.

Netscan Tools Pro 2000, Hping2, KingPingicmpenum, và SNMP Scanner là tất cả các công cụ quét và cũng có thể sử dụng để lấy dấu hệ điều hành.

Icmpenum không chỉ dùng gói ICMP Echo để thăm dò mạng, mà còn dùng gói ICMP Timestamp và ICMP Information. Hơn nữa, nó hỗ trợ gói trả lời giả mạo hoặc đánh hơi. Icmpenum rất hữu ích khi quét mạng mà tường lửa khóa ICMP.

Hping2 đáng chú ý vì nó bao gồm một loạt các tính năng khác ngoài OS fingerprinting như TCP, User Datagram Protocol (UDP),ICMP, và giao thức ping raw-IP, hping2 có thể tiến hàng gởi tín hiệu ICMP đến nhiều máy cùng lúc.

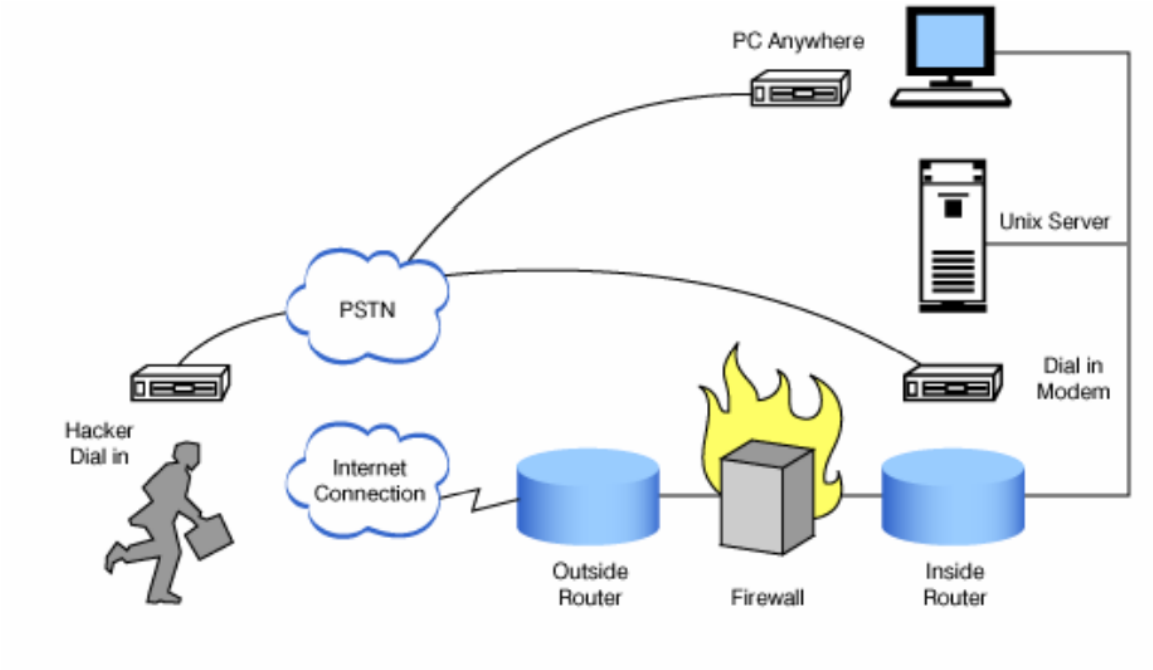
SNMP Scanner cho phép quét một dãy hoặc một danh sách các máy chủ thực hiện ping, DNS, và Simple Network Managerment Protocol (SNMP).

Tìm hiểu về kỹ thuật War-Dialing

War-Dialing là quá trình quay số modem để tìm một kết nối modem đang mở, kết nối này cung cấp truy cập từ xa vào mạng, để tấn công vào hệ thống đích. Thuật ngữ War dialing bắt nguồn từ những ngày đầu của Internet khi hầu hết các công ty đã được kết nối với Internet thông qua kết nối dial-up modem. War dialing được xem như là một phương pháp quét bởi vì nó tìm thấy một kết nối mạng mà có thể có bảo mật yếu hơn so với các kết nối Internet chính. Nhiều tổ chức thiết lập truy cập từ xa qua modem, mà bây giờ đã cổ, nhưng đã không thể loại bỏ các máy chủ truy cập từ xa này. Điều này cho phép tin tặc dễ dàng xâm nhập vào mạng với cơ chế bảo mật yếu hơn nhiều. Ví dụ, nhiều hệ thống truy cập từ xa sử dụng phương thức xác nhận PAP (Password Authentication Protocol), gửi mật khẩu ở dạng clear text,hay hơn nữa là dùng công nghệ VPN mới hơn với mật khẩu được.

War-dialing là công cụ làm việc trên tiền đề rằng: các công ty không kiểm soát quay số tại cổng chặt chẽ như tường lửa, và máy tính với modem gắn liền có mặt ở khắp mọi nơi, ngay cả khi những modem không còn sử dụng. Nhiều máy chủ vẫn còn có modem với đường dây điện thoại được kết nối như là một sao lưu dự phòng trong trường hợp kết nối Internet chính gặp xự cố. Những kết nối modem có thể được sử dụng bởi một chương war-dialing để truy cập từ xa vào hệ thống và mạng nội bộ.

Hình 3.11 là mô hình hoạt động cơ bản của War-dialing. Tại đây chúng ta thấy hacker có thể sử dụng modem của mình để giả một kết nối vào hệ thống mạng của công.



Hình 3.11: Mô hình hoạt động của War-dialing

Công Cụ

THC-Scan, Phonesweep, war dialer, và telesweep là tất cả công cụ được sử dụng để xác định các số điện thoại và có thể quay số đến mục tiêu để tạo kết nối tới modem máy tính. Những công cụ thường làm việc bằng cách sử dụng một danh sách người dùng và mật khẩu đã được xác định trước để cố gắng truy cập hệ thống. Hầu hết các truy cập từ xa bằng kết nối quay số không được bảo vệ bằng mật khẩu hoặc sử dụng bảo mật rất thô sơ.

Banner Grabing và Operating System Fingerprint

Banner Grabbing và OS Fingerprint – cũng có thể định nghĩa là Fingerprinting TCP/IP stack – là bước thứ 4 trong phương pháp quét của CEH. Quá trình fingerprinting cho phép hacker xác định vùng đặc biệt dế bị tổn thương của mục tiêu trên mạng. Banner

grabbing là quá trình tạo kết nối và đọc biểu ngữ được gửi trả lời bởi ứng dụng. Nhiều server (mail, web, ftp…) sẽ trả lời đến một kết nối telnet với tên và version của software. Hacker có thể tìm thấy nhiều mối liên hệ giữa hệ điều hành và phần mềm ứng dụng. Ví dụ, Microsoft Exchange e-mail server chỉ cài được trên HĐH Windows.

OS Fingerprint là kỹ thuật xác định thông tin hệ điều hành chạy trên host đích. Có hai phương thức để thực hiện OS Fingerprint như sau:

> Active stack fingerprinting là hình thức phổ biến nhất của fingerprinting. Nó bao gồm việc gửi dữ liệu đến hệ thống để xem cách hệ thống trả lời. Nó dựa trên thực tế là các nhà cung cấp hệ điều hành thực hiện các TCP stack khác nhau, và khác nhau dựa trên hệ điều hành. Các phản ứng này sau đó được so sánh với cơ sở dữ liệu để xác định hệ điều hành. Active stack fingerprinting bị phát hiện bởi vì nó cố gắng nhiều lần để kết nối với hệ thống mục tiêu.
>
> Passive stack fingerprinting thì "tàng hình" hơn và bao gồm sự kiểm tra lưu lượng trên mạng để xác định hệ điều hành. Nó sử dụng kỹ thuật Sniffing thay vì kỹ thuật Scanning. Passive stack fingerprinting thường không phát hiện ra bởi IDS hoặc hệ thống bảo mật khác nhưng ít chính xác hơn Active fingerprinting.

Công Cụ

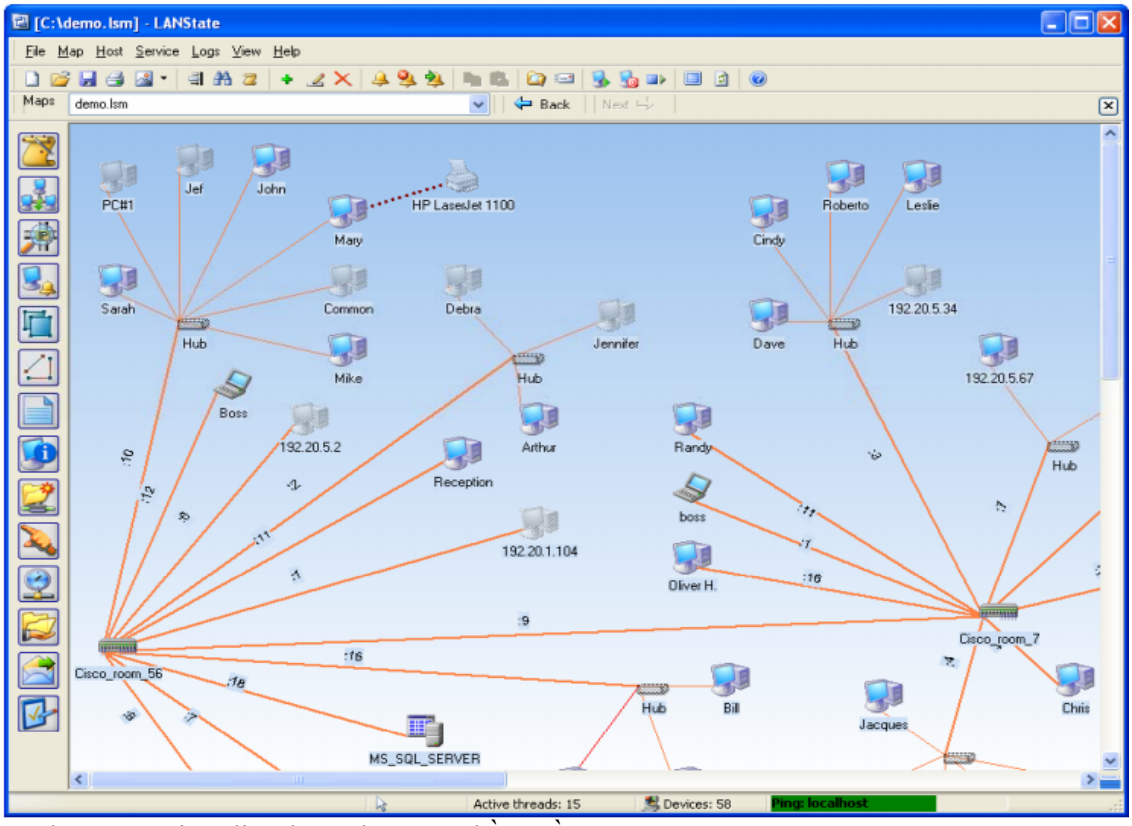
Sử dụng telnet cũng có thể thu thập thông tin hệ điều hành, khi bạn kết nối đến host.
POF, HTTPRINT, Mairn HTTP Header là những công cụ thực hiện thu thập thông tin hệ điều hành theo cơ chế Passive. Trong khi các công cụ như XPRobe2, Ring V2 Nercraft thì thu thập thông tin bằng cơ chế Active.

Đối phó với thu thập thông tin hệ điều hành

Thay đổi thông tin hệ điều hành trong phần banner header của webserver.
Với Apache bạn có thể load module có tên là mod_headers lên, và chỉnh sửa cấu hình trong file httpd.conf
Header set Server "New Server Name"
Với IIS bạn có thể sử dụng các tool như IIS lockdown Tool, ServerMask. Cả hai công cụ này đều có chức năng thay đổi banner header của server hoặc khóa hẳn luôn, không hiển thị cho người dùng.

Lập Sơ Đồ Mạng

Lập sơ đồ mạng của máy chủ là cần thiết, đặc biệt chú ý đến những máy chủ dễ bị tổn thương. SolarWinds Toolset, Queso, Harris Stat, và Cheops là các công cụ quản lý mạng sử dụng nhận biết hệ điều hành, lập bảng đồ, sơ đồ mạng, danh sách các dịch vụ đang chạy trên mạng, quét cổng thông thường và hơn nữa. Những công cụ này vẽ toàn bộ mạng trong giao diện GUI gồm routers, servers, hosts và firewalls. Hầu hết các công cụ này để có thể tìm ra IP, host name, service, hệ điều hành, và thông tin version.



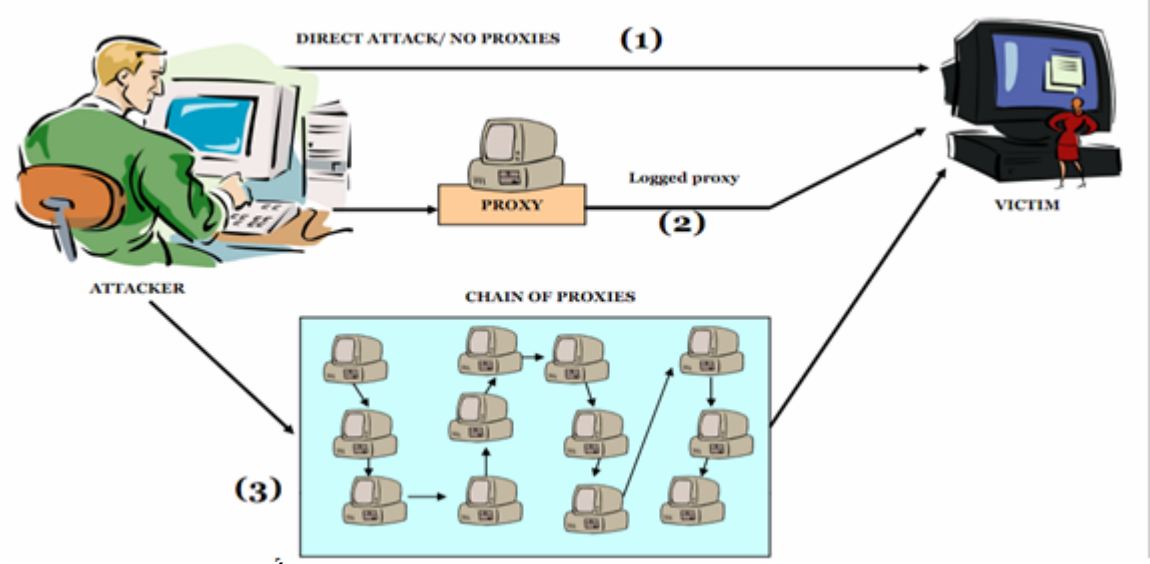
Hình 3.12 : Giao diện làm việc của phần mềm LanState

Netcraft và HTTrack là công cụ ghi dấu một hệ điều hành. Cả hai sử dụng để xác định hệ điều hành và số phiên bản phần mềm web-server.

HTTrack sắp xếp cấu trúc liên kết tương đối, ban đầu của các trang web. Bạn mở một trang của website được nhân đôi trong trình duyệt,và sau đó bạn có thể duyệt các trang web từ liên kết để liên kết như thể bạn đang xem nó trực tuyến. HTTrack cũng có thể cập nhật một trang web hiện có được nhân đôi và phục hồi download bị gián đoạn.

Triển Khai Proxy Server Để Tấn Công

Chuẩn bị máy chủ proxy là bước cuối cùng trong tiến trình quét mạng của CEH. Một proxy server là một máy tính hoạt động trung gian giữa hacker và máy tính đích. Sử dụng một proxy server có thể cho phép hacker trở thành vô danh trên mạng. Hacker trước tiên kết nối tới máy proxy server rồi yêu cầu kết nối tới máy đích thông qua kết nối có sẵn đến proxy. Cơ bản, proxy yêu cầu truy cập đến mục tiêu mà không phải là máy tính của hacker. Điều này làm hacker lướt web vô danh hoặc ẩn trong cuộc tấn công.



Hình 3.13: Mô hình tấn công của attacker

Trong hình 3.13 là mô hình tấn công được các attacker áp dụng. Trong đó, tấn công trực tiếp (1) ít được sử dụng nhất, vì nguy cơ bị phát hiện rất cao. Hai phương pháp còn lại lại thông qua một proxy (2) và qua hàng loạt các máy tính trung gian (3) được áp dụng nhiều hơn. Tuy nhiên cách thứ 3 thì khó triển khai hơn, và thường áp dụng cho một cuộc tấn công trên quy mô lớn.

Bạn có thể dễ dàng tìm thấy các proxy server miễn phí này trên mạng. Với từ khóa "free proxy server" trên google bạn có thể tìm thấy nhiều trang web cung cấp tính năng này. Ngoài ra OperaTOR là một dự án cho phép duyệt web quá các proxy một cách tự động.

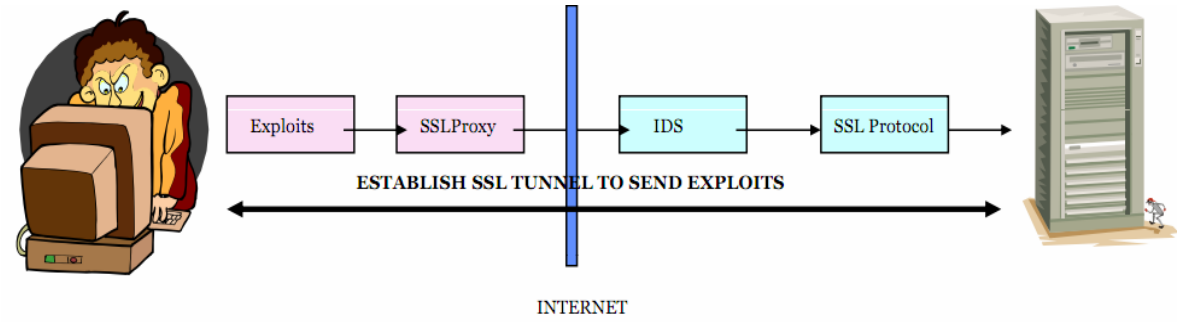
Công Cụ

SocksChain là công cụ cung cấp cho hacker khả năng tấn công thông qua một chuỗi proxy servers. Mục đích chính của việc này là ẩn IP thực và do đó sự phát hiện sẽ ở mức thấp nhất. Khi một hacker làm việc thông qua vài proxy servers trong series, thì khó khăn hơn nhiều để xác định vị trí hacker. Theo dõi địa chỉ IP của kẻ tấn công thông qua các bản ghi của máy chủ proxy là một số công việc phức tạp và tẻ nhạt. nếu một trong các tập tin đăng nhập của proxy server bị mất hoặc không đầy đủ, dây chuyền bị hỏng, và addess IP củahacker vẫn còn vô danh.

SSL Proxy là proxy trong suốt được sử dụng để chuyển đổi giữa hai hệ thống, một được mã hóa, và một không có mã hóa nào. Bạn sử dụng SSL Proxy trong các trường hợp sau: Tấn công vào một hệ thống có cài đặt dịch vụ SSL

Khai Thác Những Thông Tin Của Vượt Qua IDS.

Sử dụng SSL Proxy để tạo đường hầm (tunnel) kết nối đến hệ thống đích, chạy ngang qua một IDS, nơi mà có thể bị chặn đứng trong cuộc tấn công.



Hình 3.14: Mô hình sử dụng SSL Proxy để thực hiện tấn công

Công Cụ

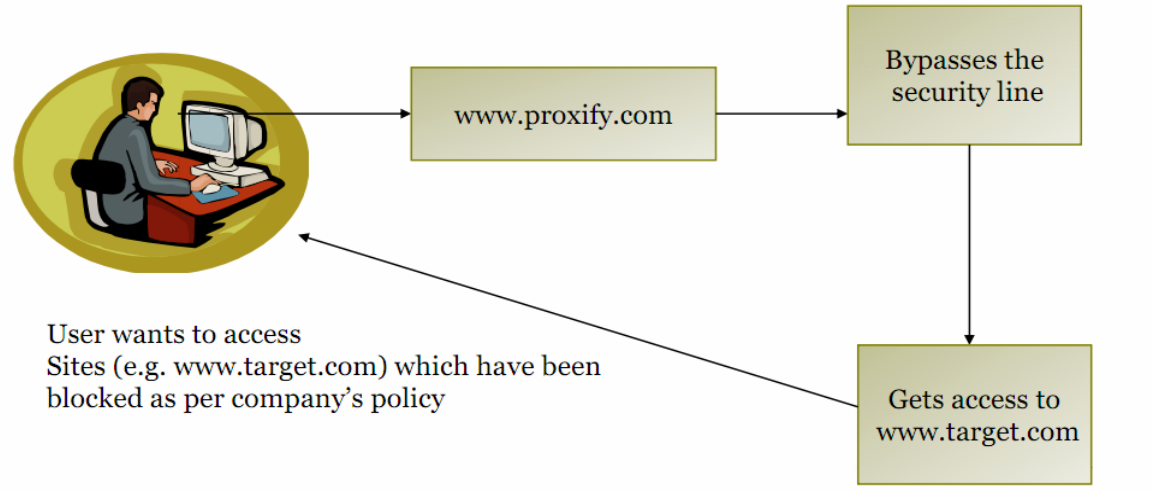
SSL Proxy cũng chính là tên công cụ dòng lệnh cho phép chúng ta tạo một SSL Proxy Tunnel, phục vụ cho cuộc tấn công sắp tới. Trong hình bên dưới là hướng dẫn cơ bản dòng lệnh chúng ta sử dụng khi đã cài SSL Proxy.

Ngoài ra, ta có thể tạo các kết nối tunnel với SSH. Trong các chương sau chúng tôi sẽ trình bày một bài thực hành về tình huống này.

Kỹ Thuật Anonymously

Anonymously (còn gọi là ân danh) là dịch vụ lướt web vô danh sử dụng một website mà hoạt động như một proxy server cho web client. Phần mềm ẩn danh đầu tiên phát triển bởi Anonymizer.com; nó được tạo ra năm 1997 bởi Lance Cottrell. Dịch vụ Anonymizers loại bỏ tất cả thông tin xác định từ máy tính người dùng trong khi họ lướt web trên Internet, theo cách đó đảm bảo sự riêng tư của người sử dụng. Để vào một website ẩn danh, hacker vào địa chỉ website qua phần mềm ẩn danh, và phần mềm ẩn danh tạo yêu cầu chọn trang web. Tất cả các trang web yêu cầu được chuyển tiếp qua các trang web ẩn danh, khó theo dõi các yêu cầu từ trang web.

Trong hình 3.15 là một vi dụ, khi bạn muốn truy cập vào website www.target.com nhưng lại bị cấm bởi các chính sách bảo mật của web server. Bạn thực hiện truy cập bằng cách thông qua một trang web giúp bạn ẩn danh là www.proxify.com



Hình 3.15: Ví dụ truy cập web thông qua Anonymizers

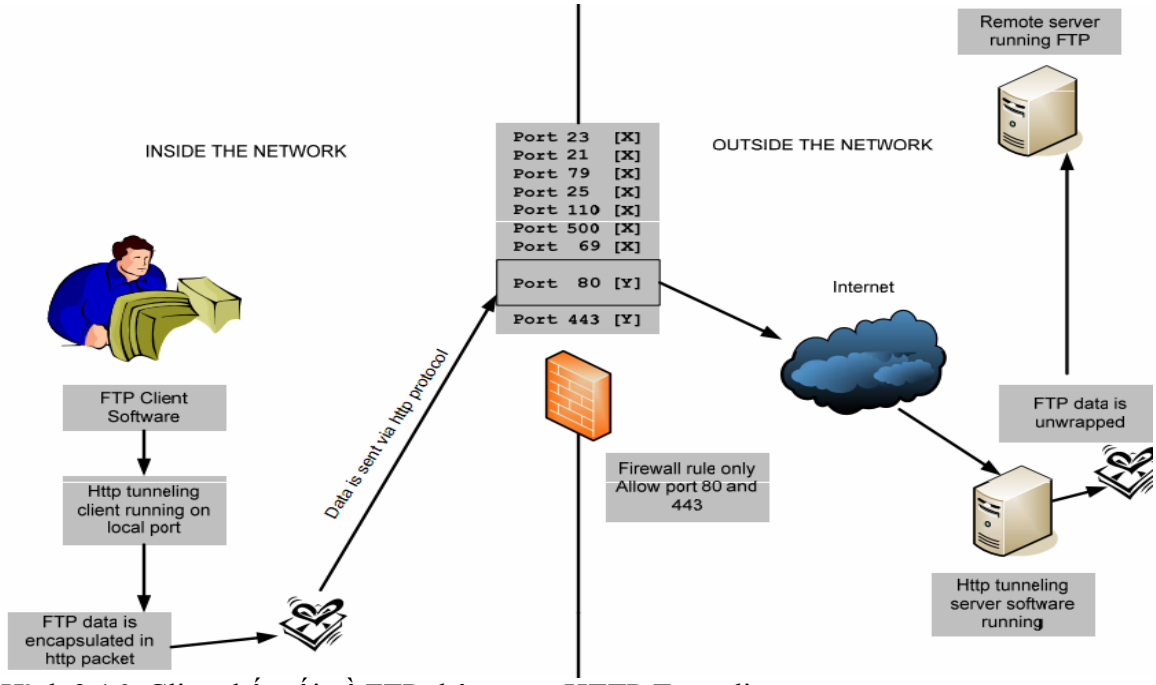
Công Cụ

Vài trang web sau đây sẽ giúp chúng ta giả danh trong việc truy cập web
http://www.primedius.com
http://www.browzar.com
http://www.rorrify.com

Kỹ Thuật HTTP TUNNELING

Một phương pháp phổ biến của vòng qua tường lửa hoặc IDS là một tạo một đường hầm (như SMTP) thông qua một giao thức cho phép (như HTTP). Hầu hết các IDS và tường lửa hoạt động như một proxy giữa máy tính của khách hàng và Internet, và chỉ cho phép truy cập với những host được định nghĩa là được phép. Hầu hết các công ty cho phép HTTP giao thông bởi vì nó thường truy cập web lành tính. Tuy nhiên, hacker có thể tạo ra một đường hầm bằng giao thức HTTP để truy cập vào mạng bên trong với giao thức không được phép.

HTTP Tunneling không hẳn là chỉ dành cho hacker. Bạn có thể áp dụng nó để tạo ra một hệ thống kết nối hai chi nhánh an toàn bằng giao thức HTTP. Trong hình 4.12 là một ví dụ về việc kết nối hai chi nhánh để trao đổi dữ liệu qua giao thức FTP, trong khi giao thức này bị chặn bởi tường lửa. Bằng cách này, client có thể kết nối về máy chủ FTP để lấy dữ liệu thông qua HTTP Tunneling.



Hình 3.16: Client kết nối về FTP thông qua HTTP Tunneling

Công Cụ

HTTPort, Tunneld, và BackStealth là tất cả công cụ để đi qua đường hầm thông qua HTTP. Chúng cho phép bỏ qua một proxy của HTTP, mà khóa những phương pháp truy cập Internet nhất định. Những công cụ này cho phép các ứng dụng như Email, IRC, ICQ, AIM, FTP… các phần mềm nguy hiểm được sử dụng từ phía sau một proxy HTTP.

Kỹ Thuật Giả Mạo IP (Spoofing IP)

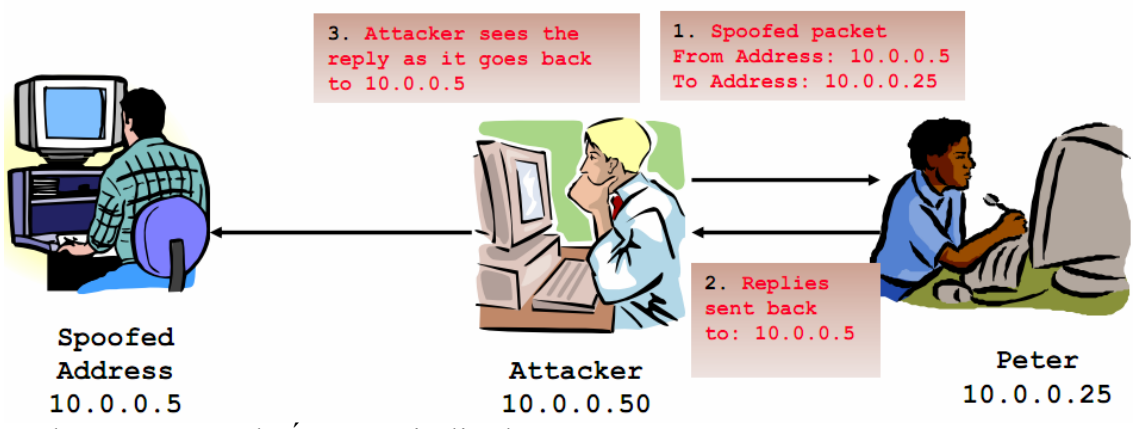
Một hacker có thể giả mạo địa chỉ IP khi quét máy hệ thống để hạn chế thấp nhất khả năng bị phát hiện. Khi nạn nhân (Victim) gửi trả lời về địa chỉ IP, nó sẽ không gửi đến địa chỉ giả mạo được. Một nhược điểm của giả mạo IP là một phiên TCP không thể hoàn thành được, do không thể gửi hồi đáp ACK.

Source routing cho phép kẻ tấn công chỉ định việc định tuyến một gói tin có thông qua Internet. Điều này cũng có thể giảm thiểu cơ hội phát hiện bằng cách bỏ qua IDS và tường lửa. Source routing được cài đặt trong giao thức TCP/IP với hai hình thức:

Loose Source routing (LSR): Routing không chính xác. Người gửi gửi một danh sách ip trong đó bao gồm ip của mình.

Strict Source routing (SSR): Routing chính xác. Người gửi chỉ ra một phần của đường dẫn để chuyển gói tin. Gói tin trả lời sẽ đi qua đường dẫn đó.

Source routing sử dụng trường địa chỉ của gói tin IP Header lên đến 39-byte tức là sẽ có tối đa 8 địa chỉ ip được thêm vào trường địa chỉ. Khi đó máy gửi sẽ gửi qua một loạt ip giả, trong số đó có ip thật của kẽ tấn công.

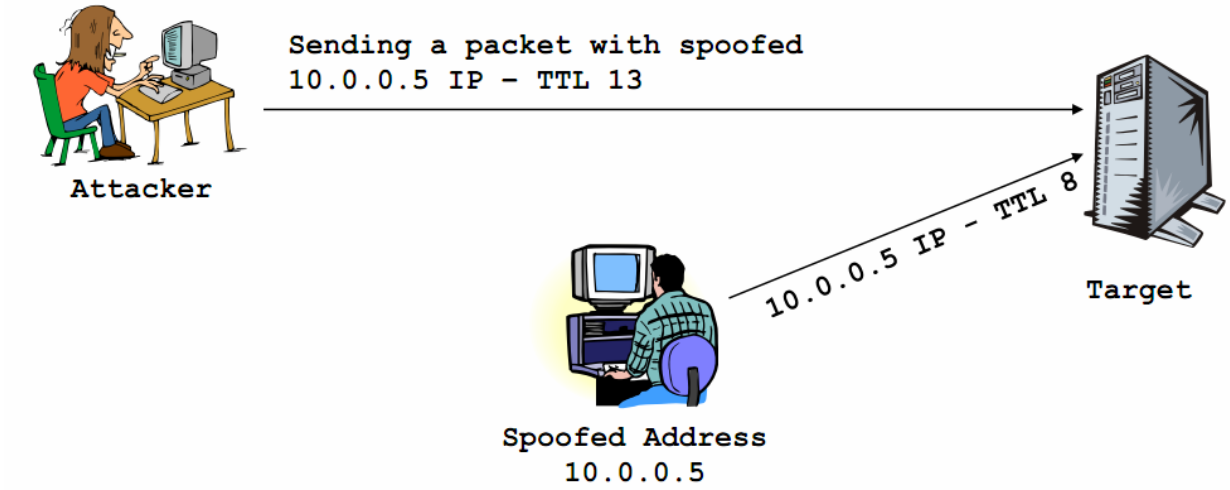


Hình 3.17: Quá trình tấn công giả địa chỉ IP.

Hình 3.17 là một ví dụ về quá trình giả IP. Bạn nhận thấy gói tin giả mạo có địa chỉ người gửi (from address) là 10.0.0.5 và gửi gói tin đến 10.0.0.25 Khi máy tính 10.0.0.25 gửi trả lời thì nó chuyển đến máy 10.0.0.5, mà đây không phải là máy tính của hacker.

Chống Lại Việc Giả IP

Để phát hiện giả mạo địa chỉ IP, bạn có thể so sánh thời gian sống (TTL) các giá trị:TTL của kẻ tấn công sẽ khác với TTL của địa chỉ giả mạo.



Hình 3.18: Phát hiện giả mạo ip

Các Biện Pháp Đối Phó Với Scanning

Trong phần trên, chúng ta cũng được giới thiệu vài phương pháp đối phó với các kỹ thuật của Scanning. Tuy nhiên, các bạn cần lưu ý một số điểm chính để đối phó với Scanning sau đây :

Firewall là một phần quan trọng của mạng. Như bạn thấy trong bài, các công cụ scan đều khó lòng vượt qua khỏi firewall.

Hệ thống phát hiện xâm nhập (IDS) cũng là một phần không thể thiếu khi triển khai mạng, muốn chống lại việc scanning. Hệ thống này chỉ có khả năng phát hiện quá trình scan mà không thể chặn quá trình scan được.

Chỉ nên mở những port cần thiết, và đóng những port không cần để tránh attacker lợi dụng.

Những thông tin nhạy cảm không nên đưa ra internet. Ví dụ như thông tin về hệ điều hành, phiên bản phần mềm đang dùng…

Tổng Kết

Trong chương này bạn cần nắm rõ các vấn đề như sau:

Có ba loại scanning chính là Port, network, and vulnerability scanning
Làm sao để biết được một hệ thống còn hoạt động hay không. Sử dụng ICMP để Ping Sweep như thế nào.
Tìm hiểu về công cụ scanning port nổi tiếng là NMAP.
Sự khác biệt của các loại scanning trong gia đình TCP như: TCP connect, SYN, NULL, IDLE, FIN, and XMAS và khi nào sử dụng loại nào.
Tìm hiểu về quy trình bắt tay ba bước TCP. Điều này giúp chúng ta tấn công giảm độ rũi ro bị phát hiện.
Hệ thống IDS, IPS được dùng để chống lại scanning.
War dialing là gì? Nó được sử dụng trong tấn công vào hệ thống dial-in.
Kỹ thuật fingerprinting có hai loại Active và Passive, Nó được dùng để thu thập thông tin hệ điều hành.
Kỹ thuật anonymously để lướt web vô danh và cơ chế HTTP Tunneling cùng kỹ thuật IP Spoofing là những kỹ thuật giúp chúng ta ân danh trong hoạt động tấn công. Sử dụng nó giúp tránh bị phát hiện.