

Đánh giá & Kiểm định an toàn hệ thống thông tin

Module 5. Network Pentesting
Methodology - Internal

1

Tổng quan

2

Quy trình thực hiện

1

Tổng quan

2

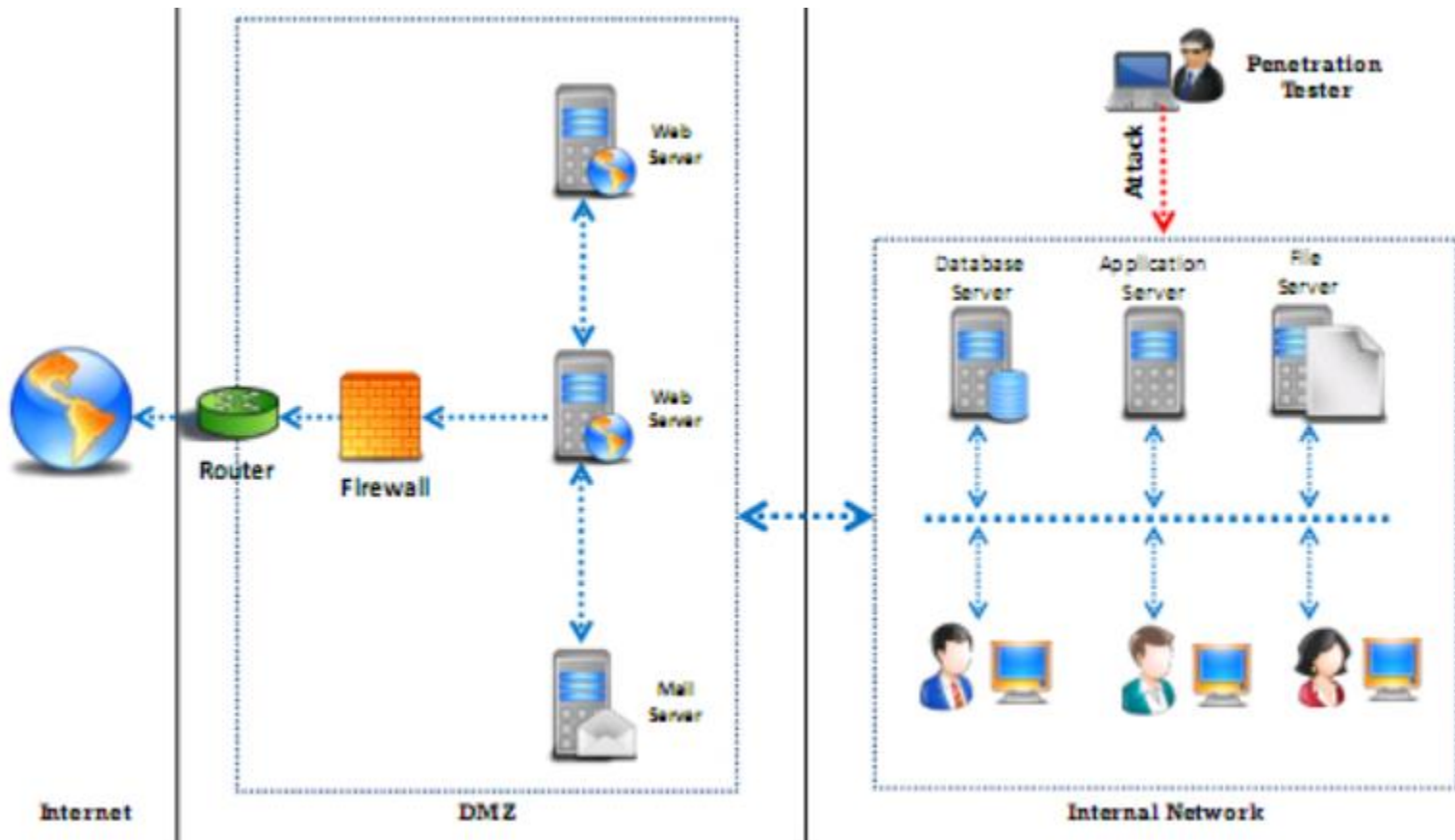
Quy trình thực hiện

Internal Network Pentesting

- ❑ Thực hiện kiểm tra, đánh giá tất cả mạng nội bộ, thiết bị hạ tầng mạng, ứng dụng, servers và endpoints từ bên trong nhằm:
 - Kiểm tra mức độ đảm bảo an toàn hiện có
 - Xác định các thông tin có thể thu thập
 - Tìm kiếm các lỗ hổng
 - Đánh giá mức độ rủi ro cho tổ chức từ các mối đe dọa nội bộ
 - Xây dựng các phương án cập nhật hệ thống và giảm thiểu rủi ro
 - Thường mô phỏng tấn công do người trong nội bộ tiến hành

Internal Network Pentesting

- Truy cập từ mạng nội bộ
- Không cần vượt qua các giải pháp phòng thủ (FW/IDPS) của tổ chức



1

Tổng quan

2

Quy trình thực hiện

Internal Network Pentesting Steps

- Step 1. Footprinting
- Step 2. Network Scanning
- Step 3. OS & Service Fingerprinting
- Step 4. Enumeration
- Step 5. Vulnerability Assessment
- Step 6. Exploitation
- Step 7. Post Exploitation
- Step 8. Document the report

Step 1. Footprinting

- Xác định Internal Domains/Host
 - Sử dụng *net view /domain*
- Xác định Internal IP Range
 - Sử dụng *arp -a*, *ipconfig/ifconfig*,...
- Xác định tất cả các Subnets

C:\WINDOWS\system32\cmd.exe

```
C:\Users\Karaoke>net view /domain
Domain
```

WORKGROUP

The command completed successfully.

```
C:\Users\Karaoke>net view /domain:WORKGROUP
Server Name          Remark
```

\\KARAOKE

Karaoke

The command completed successfully.

C:\WINDOWS\system32\cmd.exe

```
Interface: 169.254.186.247 --- 0x4
Internet Address      Physical Address      Type
169.254.255.255       ff-ff-ff-ff-ff-ff     static
224.0.0.2             01-00-5e-00-00-02     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.251           01-00-5e-00-00-fb     static
224.0.0.252           01-00-5e-00-00-fc     static
239.255.255.250       01-00-5e-7f-ff-fa     static
255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

```
Interface: 10.0.60.228 --- 0xb
Internet Address      Physical Address      Type
10.0.60.1             c0-64-e4-12-c0-44     dynamic
10.0.60.64            ac-84-c6-43-c2-bf     dynamic
10.0.60.80            c0-c9-e3-b8-73-34     dynamic
10.0.60.105           b0-83-fe-6c-3e-3c     dynamic
10.0.60.151           74-da-88-c6-7b-1c     dynamic
10.0.60.153           f4-f2-6d-fd-06-2d     dynamic
10.0.60.169           f8-2f-a8-fd-ab-29     dynamic
10.0.60.200           c0-c9-e3-b8-6b-54     dynamic
10.0.60.255           ff-ff-ff-ff-ff-ff     static
224.0.0.2             01-00-5e-00-00-02     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.251           01-00-5e-00-00-fb     static
224.0.0.252           01-00-5e-00-00-fc     static
239.255.255.250       01-00-5e-7f-ff-fa     static
255.255.255.255       ff-ff-ff-ff-ff-ff     static
```


Step 2. Network Scanning

- ❑ Xác định hosts hoạt động, open port, services...
- ❑ Sử dụng các công cụ như nmap, Angry IP Scanner, SoftPerfect Network Scanner...
 - ❑ Scan single host: *\$nmap 10.10.10.10*
 - ❑ Scan multiple hosts: *\$nmap 10.10.10.10-15*
 - ❑ Scan a subnet: *\$nmap 10.10.10.0/24*
 - ❑ Port scan: *\$nmap -p- 10.10.10.10*

Step 3. OS&Service Fingerprinting

- ❑ Xác định thông tin về hệ điều hành
- ❑ Công cụ: nmap, ping, p0f, wireshark
- ❑ Danh sách TTL Values:

Device / OS	Version	Protocol	TTL
AIX		TCP	60
AIX		UDP	30
AIX	3.2, 4.1	ICMP	255
BSDI	BSD/OS 3.1 and 4.0	ICMP	255
Compaq	Tru64 v5.0	ICMP	64
Cisco		ICMP	254
DEC Pathworks	V5	TCP and UDP	30
Foundry		ICMP	64
FreeBSD	2.1R	TCP and UDP	64
FreeBSD	3.4, 4.0	ICMP	255
FreeBSD	5	ICMP	64
HP-UX	9.0x	TCP and UDP	30
HP-UX	10.01	TCP and UDP	64
HP-UX	10.2	ICMP	255
HP-UX	11	ICMP	255
HP-UX	11	TCP	64
Irix	5.3	TCP and UDP	60
Irix	6.x	TCP and UDP	60
Irix	6.5.3, 6.5.8	ICMP	255
Juniper		ICMP	64
MPE/iX (HP)		ICMP	200
Linux	2.0.x kernel	ICMP	64
Linux	2.2.14 kernel	ICMP	255
Linux	2.4 kernel	ICMP	255
Linux	Red Hat 9	ICMP and TCP	64

MacOS/MacTCP	X(10.5.6)	ICMP/TCP/UDP	64
NetBSD		ICMP	255
Netgear FVG318		ICMP and UDP	64
OpenBSD	2.6 & 2.7	ICMP	255
OpenVMS	07.01.2002	ICMP	255
OS/2	TCP/IP 3.0		64
OSF/1	V3.2A	TCP	60
MacOS/MacTCP	2.0.x	TCP and UDP	60
Windows	98, 98 SE	ICMP	128
Windows	98	TCP	128
Windows	NT 3.51	TCP and UDP	32
Windows	NT 4.0	TCP and UDP	128
Windows	NT 4.0 SP5-		32
Windows	NT 4.0 SP6+		128
Windows	NT 4 WRKS SP 3, SP 6a	ICMP	128
Windows	NT 4 Server SP4	ICMP	128
Windows	ME	ICMP	128
Windows	2000 pro	ICMP/TCP/UDP	128
Windows	2000 family	ICMP	128
Windows	Server 2003		128
Windows	XP	ICMP/TCP/UDP	128
Windows	Vista	ICMP/TCP/UDP	128
Windows	7	ICMP/TCP/UDP	128
Windows	Server 2008	ICMP/TCP/UDP	128
Windows	10	ICMP/TCP/UDP	128

OSF/1	V3.2A	UDP	30
Solaris	2.5.1, 2.6, 2.7, 2.8	ICMP	255
Solaris	2.8	TCP	64
Stratus	TCP_OS	ICMP	255
Stratus	TCP_OS (14.2-)	TCP and UDP	30
Stratus	TCP_OS (14.3+)	TCP and UDP	64
Stratus	STCP	ICMP/TCP/UDP	60
SunOS	4.1.3/4.1.4	TCP and UDP	60
SunOS	5.7	ICMP and TCP	255
Ultrix	V4.1/V4.2A	TCP	60
Ultrix	V4.1/V4.2A	UDP	30
Ultrix	V4.2 - 4.5	ICMP	255
VMS/Multinet		TCP and UDP	64
VMS/TCPware		TCP	60
VMS/TCPware		UDP	64
VMS/Wollongong	1.1.1.1	TCP	128
VMS/Wollongong	1.1.1.1	UDP	30
VMS/UCX		TCP and UDP	128
Windows	for Workgroups	TCP and UDP	32
Windows	95	TCP and UDP	32
Windows	98	ICMP	32

OS&Service Fingerprinting

❑ Sử dụng **ping** để xác định thông tin OS

```
C:\Users\Karaoke>ping actvn.edu.vn
```

```
Pinging actvn.edu.vn [103.21.148.154] with 32 bytes of data:
```

```
Reply from 103.21.148.154: bytes=32 time=25ms TTL=114
```

```
Reply from 103.21.148.154: bytes=32 time=24ms TTL=114
```

```
Reply from 103.21.148.154: bytes=32 time=43ms TTL=114
```

```
Reply from 103.21.148.154: bytes=32 time=26ms TTL=114
```

```
Ping statistics for 103.21.148.154:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 24ms, Maximum = 43ms, Average = 29ms
```

Netblock owner	IP address	OS	Web server	Last seen
► CMC Telecom Infrastruc...	103.21.148.154	Windows Server 2016	Microsoft-IIS/10.0	29-Mar-2021
► CMC Telecom Infrastruc...	115.146.127.72	Windows Server 2016	Microsoft-IIS/10.0	10-Feb-2020
► CMC Telecom Infrastruc...	115.146.127.72	unknown	Microsoft-IIS/10.0	30-Dec-2019
CMC Telecom Service Company 273 Doi Can, Ba Dinh, Ha Noi	115.146.127.72	Windows Server 2008	Microsoft-IIS/7.5	24-May-2019
CMC Telecom Service Company 273 Doi Can, Ba Dinh, Ha Noi	115.146.127.72	unknown	Microsoft-IIS/7.5	11-Dec-2018
CMC Telecom Service Company 273 Doi Can, Ba Dinh, Ha Noi	115.146.127.72	Windows Server 2008	Microsoft-IIS/7.5	10-Dec-2018

OS&Service Fingerprinting

❑ Sử dụng **ping** để xác định thông tin OS

▣ Hosting History

Netblock owner	IP address	OS	Web server	Last seen
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	104.21.34.223	Linux	cloudflare	28-Mar-2021
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	172.67.165.236	Linux	cloudflare	26-Mar-2021
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	104.21.34.223	Linux	cloudflare	24-Mar-2021
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	172.67.165.236	Linux	cloudflare	23-Mar-2021
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	104.21.34.223	Linux	cloudflare	11-Mar-2021
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	172.67.165.236	Linux	cloudflare	8-Mar-2021

```
C:\WINDOWS\system32\cmd.exe
```

```
C:\Users\Karaoke>ping gbhackers.com
```

```
Pinging gbhackers.com [104.21.34.223] with 32 bytes of data:
```

```
Reply from 104.21.34.223: bytes=32 time=37ms TTL=48
```

```
Reply from 104.21.34.223: bytes=32 time=36ms TTL=48
```

```
Reply from 104.21.34.223: bytes=32 time=36ms TTL=48
```

```
Reply from 104.21.34.223: bytes=32 time=45ms TTL=48
```

```
Ping statistics for 104.21.34.223:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 36ms, Maximum = 45ms, Average = 38ms
```

Identify the Services

- ❑ Xác định các dịch vụ đang hoạt động trên các port
- ❑ Ví dụ: Xác định Ipsec được sử dụng trên các thiết bị và hosts
 - Xác định Ipsec dựa trên VPNs
 - Sử dụng Nmap để xác định dịch vụ isakmp trên UDP 500

```
Parrot Terminal
[r7909@parrot]~$ nmap -sV certifiedhacker.com
Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-22 22:59 EDT
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.22s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com
Not shown: 981 filtered ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Pure-FTPd
22/tcp    open  ssh          OpenSSH 5.3 (protocol 2.0)
25/tcp    open  smtp         Exim smtpd 4.93
26/tcp    open  smtp         Exim smtpd 4.93
53/tcp    open  domain       ISC BIND 9.8.2rc1 (RedHat Enterprise Linux 6)
80/tcp    open  http         Apache httpd
110/tcp   open  pop3         Dovecot pop3d
143/tcp   open  imap         Dovecot imapd
443/tcp   open  ssl/http     Apache httpd
465/tcp   open  ssl/smtp     Exim smtpd 4.93
587/tcp   open  smtp         Exim smtpd 4.93
993/tcp   open  imaps?
995/tcp   open  pop3s?
2000/tcp  open  tcpwrapped
2222/tcp  open  ssh          OpenSSH 5.3 (protocol 2.0)
3306/tcp  open  mysql        MySQL 5.6.41-84.1
```

```
root@kali: ~
File Edit View Search Terminal Help

root@kali:~# nmap -sU -p 500 10.10.10.10

Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-22 04:59 EST
Nmap scan report for 10.10.10.10
Host is up (-0.20s latency).

PORT      STATE      SERVICE
500/udp    open|filtered isakmp
MAC Address: 00:0C:29:E6:67:AD (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.50 seconds
root@kali:~#
```

Map the Internal Network

- ❑ Lập bản đồ mạng nội bộ để xác định
 - Số lượng subnets
 - Số lượng host
 - OS & Port/Service đang hoạt động trên mỗi host



Step 4. Enumeration

- ❑ Liệt kê (Enumeration) được thực hiện nhằm:
 - Tạo các kết nối chủ động với mục tiêu nhằm thu thập nhiều hơn nữa thông tin có thể
 - Trích xuất những thông tin thu được trước đó thành một hệ thống có trật tự bao gồm những thứ có liên quan đến mục tiêu cần tấn công (username, password, host name, share file, routing tables, banners...)
 - Công cụ: **SuperScan**, **Hyena**, **Winfingerprint**...

Enumeration Techniques & Tools

❑ NetBIOS Enumeration

- Danh sách các máy tính trong domain
- Danh sách tài nguyên được chia sẻ trong mạng
- Chính sách & mật khẩu
- Công cụ: Nbtstat, SuperScan, Hyena, Winfingerprint

❑ SNMP Enumeration

- Thông tin về các tài nguyên mạng như hosts, routers, devices, tài nguyên chia sẻ
- Công cụ: OpUtlis, SNMP Scanner

❑ LDAP Enumeration

- Tên người dùng hợp lệ, địa chỉ
- Công cụ: LDAP Admin Tools

Enumeration Techniques & Tools

- ❑ NTP Enumeration
- ❑ RPC Enumeration
- ❑ NFS Enumeration
- ❑ SMTP Enumeration
- ❑ SMB Enumeration
- ❑ VoIP Enumeration
- ❑ IPSEC Enumeration
- ❑ NULL Enumeration

Enumeration Techniques & Tools

❑ Example:

- Sử dụng telnet để tương tác với SMTP server và thu thập thông tin về người dùng hợp lệ
- Sử dụng VRFY, EXPN, RCPT TO để kiểm tra thông tin
 - VRFY: kiểm tra users
 - EXPN: kiểm tra sự tồn tại của hộp thư trên local host
 - RCPT TO: chỉ định người nhận thư

Use the SMTPVRFY Command

```
$ telnet 192.168.168.1 25
Trying 192.168.168.1...
Connected to 192.168.168.1.
Escape character is '^]'.
220 NYmailserver ESMTSP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 NYmailserver Hello [10.0.0.86],
pleased to meet you
VRFY Jonathan
250 Super-User <Jonathan@NYmailserver>
VRFY Smith
550 Smith... User unknown
```

Use the SMTP EXPN Command

```
$ telnet 192.168.168.1 25
Trying 192.168.168.1...
Connected to 192.168.168.1.
Escape character is '^]'.
220 NYmailserver ESMTSP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 NYmailserver Hello [10.0.0.86],
pleased to meet you
EXPN Jonathan
250 Super-User <Jonathan@NYmailserver>
EXPN Smith
550 Smith... User unknown
```

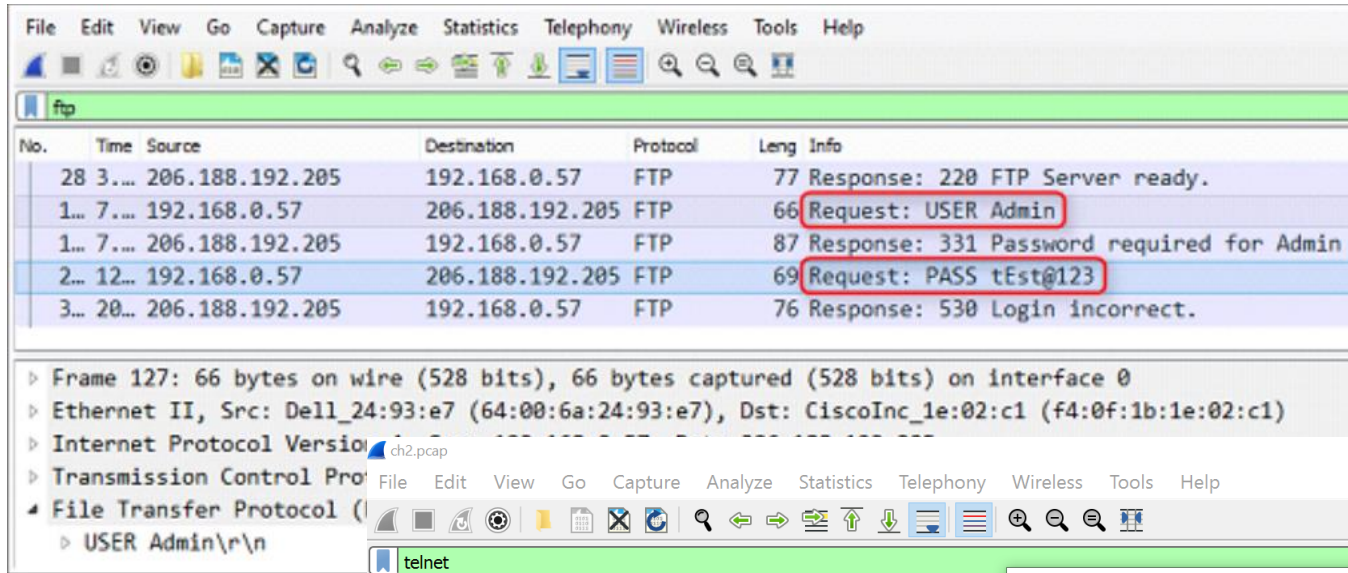
Use the SMTP RCPT TO Command

```
$ telnet1 192.168.168.1 25
Trying 192.168.168.1 ...
Connected to 192.168.168.1.
Escape character is '^]'.
220 NYmailserver ESMTSP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 NYmailserver Hello [10.0.0.86], pleased
to meet you
MAIL FROM:Jonathan
250 Jonathan... Sender ok
RCPT TO:Ryder
250 Ryder... Recipient ok
RCPT TO: Smith
550 Smith... User unknown
```

Sniff the Network

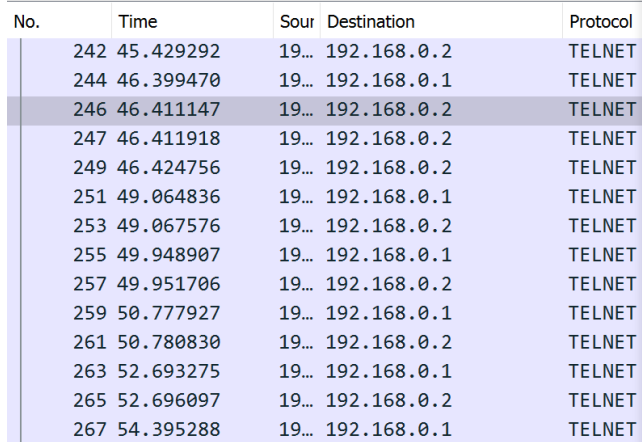
- ❑ Sniffing (nghe lén) là quá trình theo dõi và thu thập toàn bộ các gói tin được truyền đi trong mạng
- ❑ Các thông tin thu được:
 - ❑ DNS, Email, Web, Syslog traffic
 - ❑ POP3/FTP/Telnet password
 - ❑ Router configuration
 - ❑ Chat sessions
- ❑ Công cụ: Wireshark, tcpdump...

Sniff the Network - Example

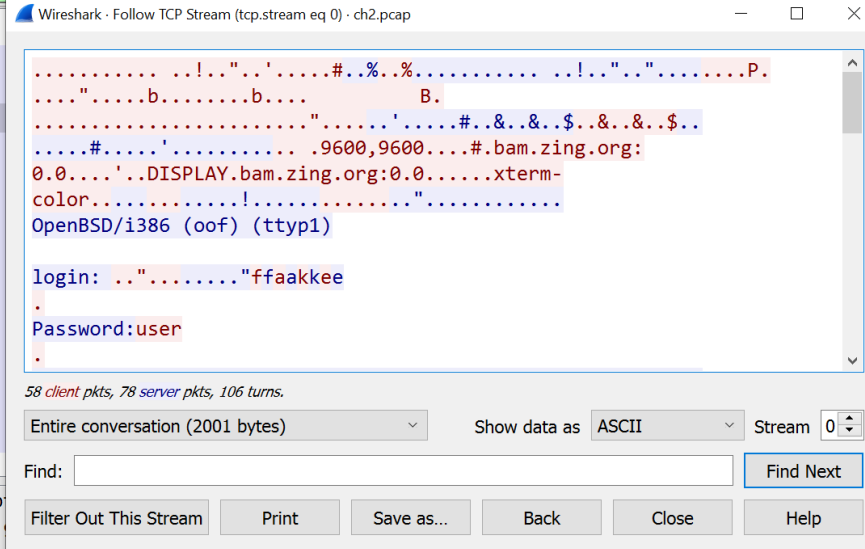


No.	Time	Source	Destination	Protocol	Leng	Info
28	3...	206.188.192.205	192.168.0.57	FTP	77	Response: 220 FTP Server ready.
1...	7...	192.168.0.57	206.188.192.205	FTP	66	Request: USER Admin
1...	7...	206.188.192.205	192.168.0.57	FTP	87	Response: 331 Password required for Admin
2...	12...	192.168.0.57	206.188.192.205	FTP	69	Request: PASS tEst@123
3...	20...	206.188.192.205	192.168.0.57	FTP	76	Response: 530 Login incorrect.

Frame 127: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: Dell_24:93:e7 (64:00:6a:24:93:e7), Dst: CiscoInc_1e:02:c1 (f4:0f:1b:1e:02:c1)
Internet Protocol Version 4, Src: 192.168.0.57, Dst: 206.188.192.205
Transmission Control Protocol, Src Port: 21, Dst Port: 21, Seq: 1580, Len: 66
File Transfer Protocol (FTP), Src: 192.168.0.57, Dst: 206.188.192.205
USER Admin\r\n



No.	Time	Sour	Destination	Protocol
242	45.429292	19...	192.168.0.2	TELNET
244	46.399470	19...	192.168.0.1	TELNET
246	46.411147	19...	192.168.0.2	TELNET
247	46.411918	19...	192.168.0.2	TELNET
249	46.424756	19...	192.168.0.2	TELNET
251	49.064836	19...	192.168.0.1	TELNET
253	49.067576	19...	192.168.0.2	TELNET
255	49.948907	19...	192.168.0.1	TELNET
257	49.951706	19...	192.168.0.2	TELNET
259	50.777927	19...	192.168.0.1	TELNET
261	50.780830	19...	192.168.0.2	TELNET
263	52.693275	19...	192.168.0.1	TELNET
265	52.696097	19...	192.168.0.2	TELNET
267	54.395288	19...	192.168.0.1	TELNET



Wireshark · Follow TCP Stream (tcp.stream eq 0) · ch2.pcap

.....!..".'.#..%..%.....!..".#.....P.
.....".b.....b.....B.
.....".#.....'.....#..&..&..\$..&..\$..
.....#.....'.9600,9600....#.bam.zing.org:
0.0.....'.DISPLAY.bam.zing.org:0.0.....xterm-
color.....!....."
OpenBSD/i386 (oof) (ttyp1)

login: .."....."ffaakkee
.
Password:user
.

58 client pkts, 78 server pkts, 106 turns.

Entire conversation (2001 bytes) Show data as ASCII Stream 0

Find: Find Next

Filter Out This Stream Print Save as... Back Close Help

Frame 246: 67 bytes on wire (536 bits), 67 bytes captured on interface 0
Ethernet II, Src: WesternD_9f:a0:97 (00:00:c0:9f:a0:97), Dst: 192.168.0.2
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.2
Transmission Control Protocol, Src Port: 23, Dst Port: 1254, Seq: 1580, Ack: 254, Len: 1
Telnet

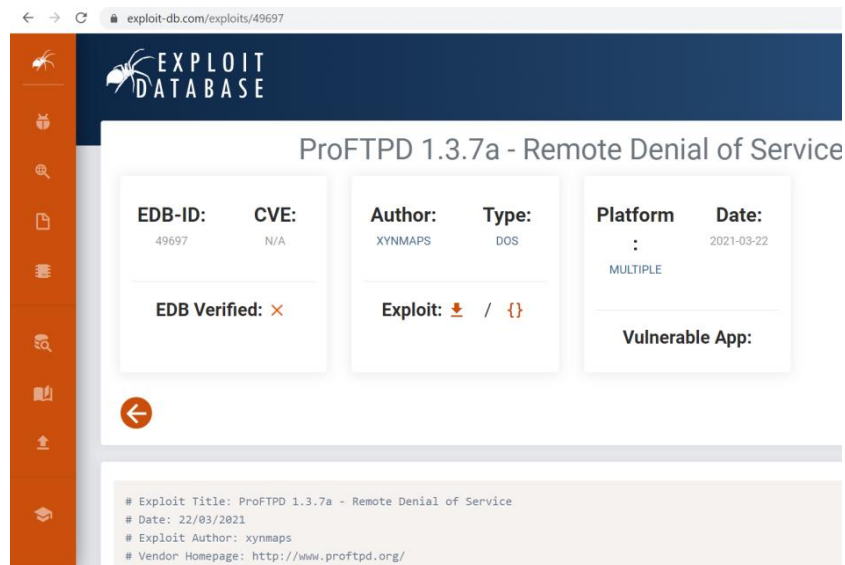
Step 5. Vulnerability Assessment

❑ Internal vulnerability assessment

- Xác định lỗ hổng của OS, thiết bị, ứng dụng
- Công cụ: Nessus, Acunetix, nmap

❑ Tìm kiếm các thông tin có liên quan về lỗ hổng

- Sử dụng Google
- Sử dụng Exploit Database



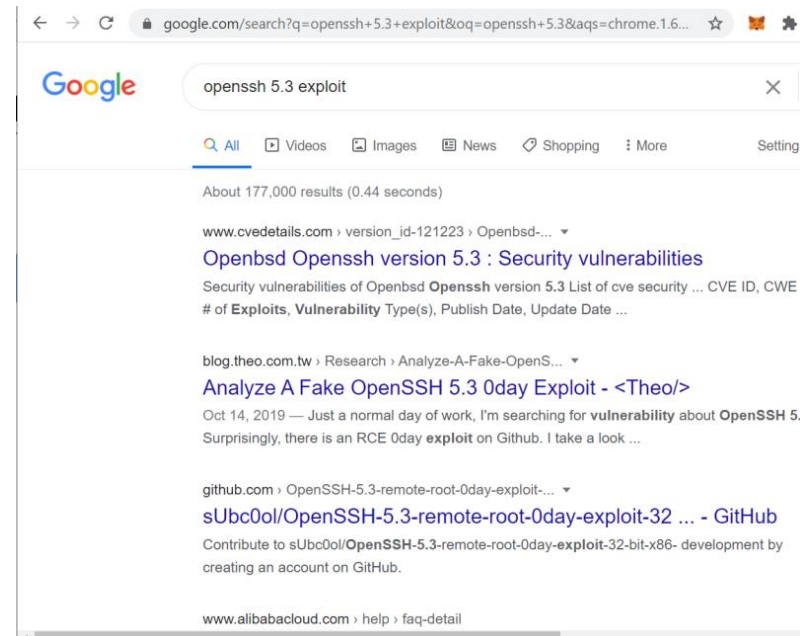
The screenshot shows the Exploit Database website. The main heading is "ProFTPD 1.3.7a - Remote Denial of Service". Below this, there is a table with the following information:

EDB-ID:	CVE:	Author:	Type:	Platform	Date:
49697	N/A	XYNMAPS	DOS	MULTIPLE	2021-03-22

Below the table, there are two sections: "EDB Verified: ✗" and "Exploit: 📄 / 📄". At the bottom, there is a section titled "Vulnerable App:".

At the bottom of the page, there is a footer with the following information:

```
# Exploit Title: ProFTPD 1.3.7a - Remote Denial of Service
# Date: 22/03/2021
# Exploit Author: xynmaps
# Vendor Homepage: http://www.proftpd.org/
```



The screenshot shows a Google search results page for the query "openssh 5.3 exploit". The search bar shows the query and the Google logo. Below the search bar, there are tabs for "All", "Videos", "Images", "News", "Shopping", and "More". The search results show "About 177,000 results (0.44 seconds)".

The first result is from "www.cvedetails.com" and is titled "Openbsd Openssh version 5.3 : Security vulnerabilities". The snippet below the title reads: "Security vulnerabilities of Openbsd Openssh version 5.3 List of cve security ... CVE ID, CWE # of Exploits, Vulnerability Type(s), Publish Date, Update Date ...".

The second result is from "blog.theo.com.tw" and is titled "Analyze A Fake OpenSSH 5.3 0day Exploit - <Theo/>". The snippet below the title reads: "Oct 14, 2019 — Just a normal day of work, I'm searching for vulnerability about OpenSSH 5. Surprisingly, there is an RCE 0day exploit on Github. I take a look ...".

The third result is from "github.com" and is titled "sUbc00l/OpenSSH-5.3-remote-root-0day-exploit-32 ... - GitHub". The snippet below the title reads: "Contribute to sUbc00l/OpenSSH-5.3-remote-root-0day-exploit-32-bit-x86- development by creating an account on GitHub."

The fourth result is from "www.alibabacloud.com" and is titled "help > faq-detail".

Internal Vulnerability Assessment

- ❑ Sử dụng NSE script `/usr/share/nmap/scripts` để dò quét lỗ hổng chỉ định

```
root@kali:~# nmap -O -p 445 --script=smb-vuln-ms17-010.nse 192.168.40.134
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-28 16:31 CST
Nmap scan report for 192.168.40.134
Host is up (0.00100s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds
MAC Address: 00:0C:29:0E:6A:3E (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized|phone
Running: Microsoft Windows 2008|8.1|7|Phone|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008::
:microsoft:windows_7 cpe:/o:microsoft:windows_
OS details: Microsoft Windows Server 2008 or 2008 R2
Embedded Standard 7, Microsoft Windows 8.1 R1
ows Server 2008 SP1, or Windows 7, Microsoft W
Network Distance: 1 hop

Host script results:
smb-vuln-ms17-010:
VULNERABLE:
Remote Code Execution vulnerability in Mic
State: VULNERABLE
IDs: CVE:CVE-2017-0143
Risk factor: HIGH
A critical remote code execution vulne
servers (ms17-010).

Disclosure date: 2017-03-14
References:
https://cve.mitre.org/cgi-bin/cvename.
https://blogs.technet.microsoft.com/ms
https://technet.microsoft.com/en-us/li
OS detection performed. Please report any incor
Nmap done: 1 IP address (1 host up) scanned in
```

```
root@Jir0w:~# nmap --script=smb-vuln* -p 445 10.0.1.134
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-03 00:43 EDT
Nmap scan report for 10.0.1.134
Host is up (0.00050s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds
MAC Address: 00:0C:29:38:58:55 (VMware)

Host script results:
_smb-vuln-ms10-054: false
_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
smb-vuln-ms17-010:
VULNERABLE:
Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
State: VULNERABLE
IDs: CVE:CVE-2017-0143
Risk factor: HIGH
A critical remote code execution vulnerability exists in Microsoft SMBv1
servers (ms17-010).

Disclosure date: 2017-03-14
References:
https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

Nmap done: 1 IP address (1 host up) scanned in 9.75 seconds
```

Step 6. Exploitation

❑ Windows exploitation:

- Tìm kiếm, xác định Local/Remote Exploit để chiếm quyền truy cập vào hệ thống

The screenshot shows the Exploit Database website. The main heading is "Microsoft Windows - 'NetAPI32.dll' Code Execution (Python) (MS08-067)". Below this, there is a table with details about the exploit, including EDB-ID, Author, Published date, CVE, Type, Platform, Aliases, Advisory/Source, Tags, E-DB Verified status, Exploit status, and Vulnerable App.

EDB-ID	Author	Published
40279	ohnozy	2016-02-26

Below the table, there is a code snippet for the exploit:

```
1 import struct
2 import time
3 import sys
4
5 from threading import Thread #Thread is imported incase you would
```

On the right, there is a search bar with the text "buffer overflow" and a "Search" button. Below the search bar, there is a table of search results. The table has columns: Date, D, A, V, Title, Platform, and Author. The results are sorted by date, with the most recent results at the top.

Date	D	A	V	Title	Platform	Author
2013-10-28	📄	-	✓	BlazeDVD 6.2 - '.pif' Local Buffer Overflow (SEH)	Windows	Mike Czumak
2013-10-27	📄	📄	✓	VideoCharge Studio 2.12.3.685 - Local Buffer Overflow (SEH)	Windows	metacom
2013-10-26	📄	📄	✓	Photodex ProShow Producer 5.0.3310 - Local Buffer Overflow (SEH)	Windows	Mike Czumak
2013-10-22	📄	-	🕒	D-Link DIR-605L - Captcha Handling Buffer Overflow (Metasploit)	Hardware	Metasploit

Exploit Verification

❑ Linux/Unix exploitation:

- Tìm kiếm, xác định Local/Remote Exploit để chiếm quyền truy cập/ quyền root

The image shows two screenshots of the Exploit-DB website. The top screenshot displays the entry for 'sudo 1.8.27 - Security Bypass' (EDB-ID: 47502, CVE: 2019-14287, Author: MOHIN PARAMASIVAM, Type: LOCAL). The bottom screenshot displays the entry for 'Libc locale - Local Privilege Escalation (1)' (EDB-ID: 20189, CVE: 2000-0844, Author: SYNNERGY.NET, Type: LOCAL, Date: 2000-09-04). Both entries show the 'Exploit' download icon and the 'Vulnerable App' section.

sudo 1.8.27 - Security Bypass

EDB-ID:	CVE:	Author:	Type:
47502	2019-14287	MOHIN PARAMASIVAM	LOCAL

EDB Verified: ✗

Exploit: /

Libc locale - Local Privilege Escalation (1)

EDB-ID:	CVE:	Author:	Type:	Platform	Date:
20189	2000-0844	SYNNERGY.NET	LOCAL	:	2000-09-04

EDB Verified: ✓

Exploit: /

Vulnerable App:

```
# Exploit Title : sudo 1.8.27 - Security Bypass
# Date : 2019-10-15
# Original Author: Joe Vennix
# Exploit Author : Mohin Paramasivam (Shad0wQu35t)
```

```
/*
source: https://www.securityfocus.com/bid/1634/info

ectiva 4.x/5.x, Debian 2.x, IBM AIX 3.x/4.x, Mandrake 7, RedHat 5.x/6.x, IRIX 6.x, Solaris 2.x/7/8, Turbolinux 6.x,
```


Exploit Verification

❑ Linux/Unix exploitation:

- Trích xuất User Accounts
- Trích xuất Password Hash/ Bẻ khóa mật khẩu

```
File Edit View Search Terminal Help
cat /etc/shadow
root:!:16592:0:99999:7:::
daemon:!:16105:0:99999:7:::
bin:!:16105:0:99999:7:::
sys:!:16105:0:99999:7:::
sync:!:16105:0:99999:7:::
games:!:16105:0:99999:7:::
man:!:16105:0:99999:7:::
lp:!:16105:0:99999:7:::
mail:!:16105:0:99999:7:::
news:!:16105:0:99999:7:::
uucp:!:16105:0:99999:7:::
proxy:!:16105:0:99999:7:::
www-data:!:16105:0:99999:7:::
backup:!:16105:0:99999:7:::
list:!:16105:0:99999:7:::
irc:!:16105:0:99999:7:::
gnats:!:16105:0:99999:7:::
nobody:!:16105:0:99999:7:::
libuid:!:16105:0:99999:7:::
syslog:!:16105:0:99999:7:::
messagebus:!:16105:0:99999:7:::
colord:!:16105:0:99999:7:::
lightdm:!:16105:0:99999:7:::
whoopsie:!:16105:0:99999:7:::

File Edit View Search Terminal Help
channel 1 created.
ls
cinema
shellshock-
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/s
games:x:5:60:games:/usr/games:/
man:x:6:12:man:/var/cache/man:/
lp:x:7:7:lp:/var/spool/lpd:/bin
mail:x:8:8:mail:/var/mail:/bin
news:x:9:9:news:/var/spool/new
uucp:x:10:10:uucp:/var/spool/u
proxy:x:13:13:proxy:/bin:/bin/s
www-data:x:33:33:www-data:/var/
backup:x:34:34:backup:/var/back
list:x:38:38:Mailing List Manag
irc:x:39:39:ircd:/var/run/ircd:
gnats:x:41:41:Gnats Bug-Reporti
nobody:x:65534:65534:nobody:/no
libuid:x:100:101::/var/lib/lib
syslog:x:101:103::/home/syslog:

File Edit View Search Terminal Help
root@kali:~# unshadow passwords.txt shadow.txt > cracked.txt
root@kali:~#

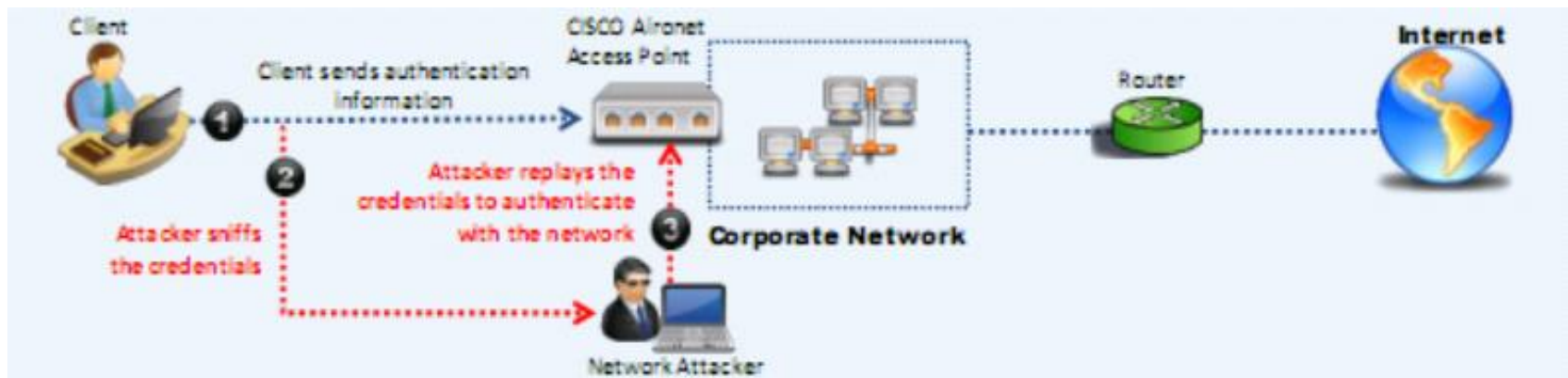
File Edit View Search Terminal Help
root@kali:~# john cracked.txt
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (sha512crypt, crypt(3) $6$ [SHA5
12 128/128 SSE4.1 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
password (bill)
orange (john)
green (fred)
pineapple (mercy)
4g 0:00:02:54 28.07% 2/3 (ETA: 04:18:38) 0.02292g/s 298.6p/s 597.9c/s 597.9C/s g
atito5..notused5
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
```

Other Internal Network Exploitation Techniques

❑ **Tấn công phát lại (Replay Attacks):** là một hình thức tấn công mạng trong đó dữ liệu hợp lệ được truyền lặp đi lặp lại hoặc bị bẻ khóa

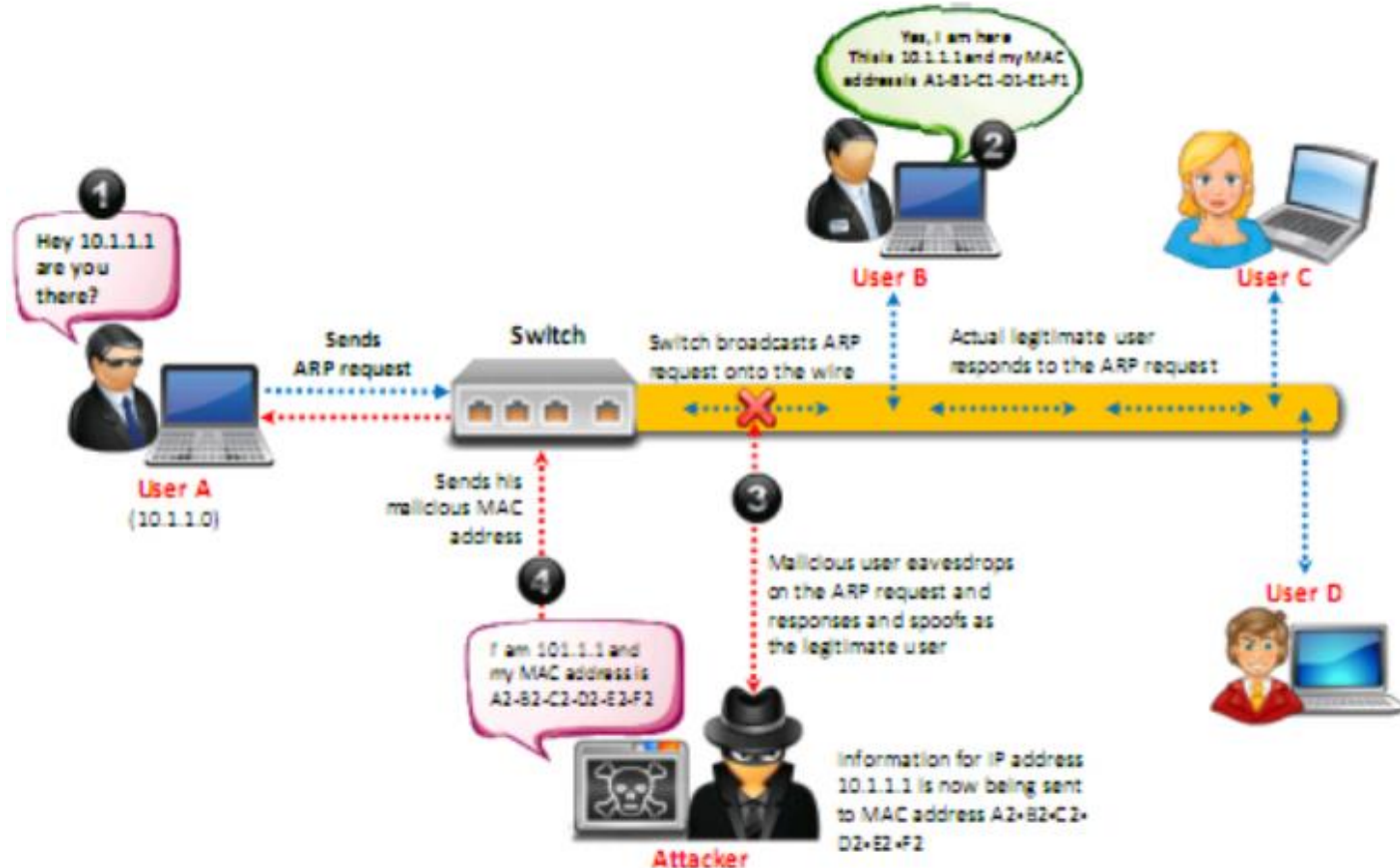
Ví dụ:

- Kẻ tấn công lấy được thông tin hàm băm của mật khẩu và sử dụng để đăng nhập lại vào hệ thống
- Sử dụng lại phiên làm việc



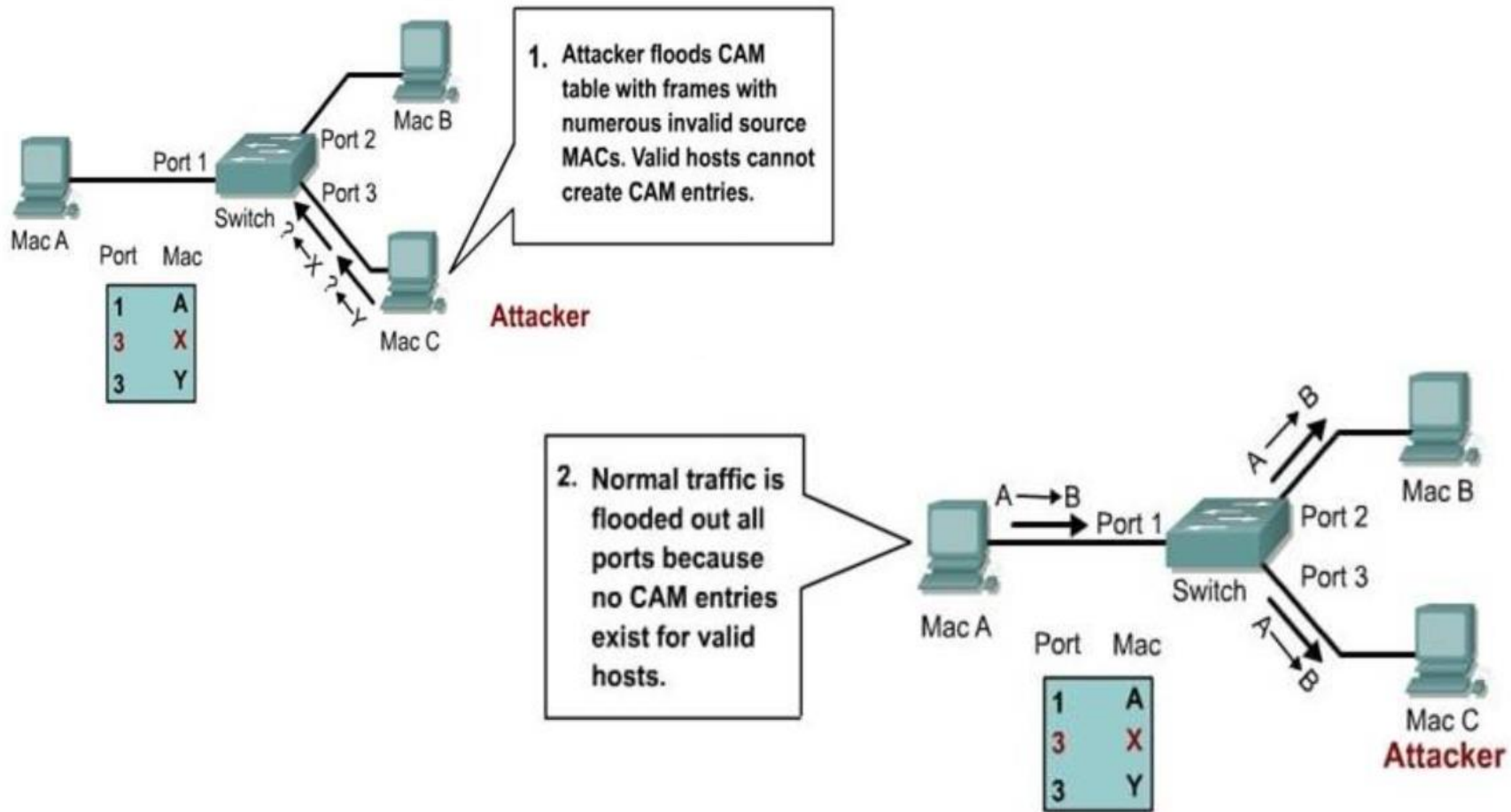
Other Internal Network Exploitation Techniques

- ❑ **ARP Poisoning/Spoofing:** cho phép bất kỳ lưu lượng truy cập đều được gửi tới kẻ tấn công
 - Thường dùng để tấn công DoS, MiTM



Other Internal Network Exploitation Techniques

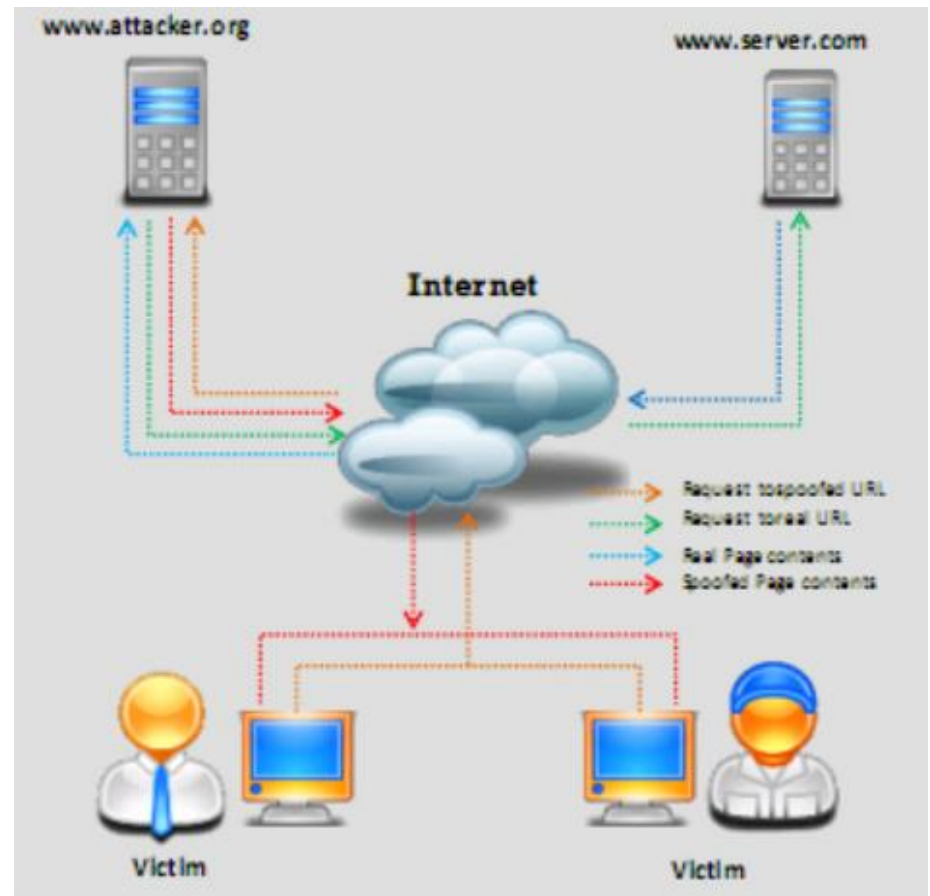
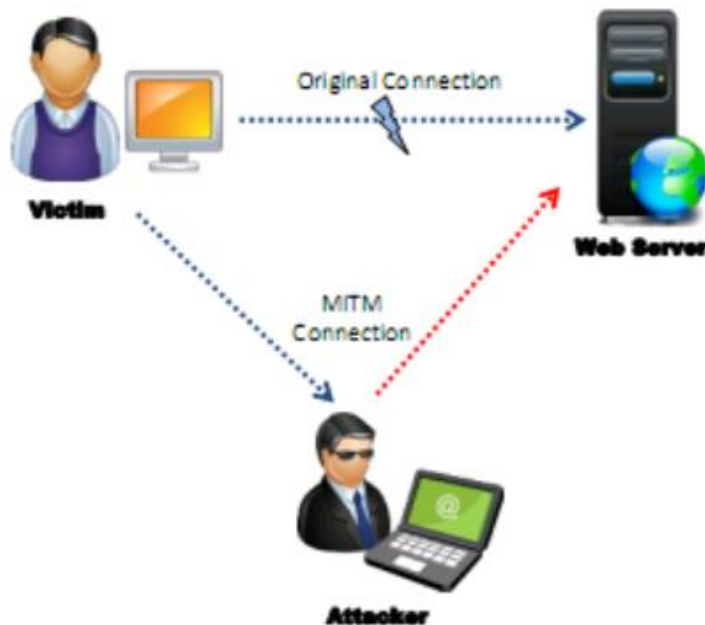
❑ **Mac Flooding:** kẻ tấn công làm tràn bảng CAM trên switch với fake MAC & IP -> khiến cho switch reset về "learning mode"



Other Internal Network Exploitation Techniques

❑ **MiTM Attack** có thể dễ dàng thực hiện sử dụng:

- DNS cache poisoning
- ARP spoofing



Other Internal Network Exploitation Techniques

❑ Escalate User Privileges:

- ❑ Thực hiện chiếm quyền cao hơn trong hệ thống (system/root)
- ❑ Thử thực hiện reset local administrator/nomal user account
- ❑ Thử cài đặt keylogger/spyware/trojan để lấy trộm thông tin mật khẩu
- ❑ Thử cài đặt backdoor trên hệ thống
- ❑ Thử bypass Antivirus Software
- ❑ Thử phát tán mã độc trong mạng máy tính
- ❑ Thử kiểm tra các mật khẩu, cài đặt mặc định
- ❑ Thử ẩn, giấu các dữ liệu nhạy cảm

Other Internal Network Exploitation Techniques

☐ **Kiểm tra một số lỗi hỏng phổ biến thường gặp trên Web servers, ứng dụng web...**

- ☐ Buffer Overflow
- ☐ Format String
- ☐ Manipulating input parameter

Automated Internal Network Pentesting Tool

- ☐ Metasploit
- ☐ Nexpose
- ☐ Kali Linux/Parrot Sec
- ☐ CANVAS
- ☐



nexpose[®]



Step 7. Post Exploitation

- ❑ Kiểm tra sự tồn tại của các bản vá
- ❑ Sau khi khai thác thành công, pentester cần khôi phục hệ thống lại trạng thái trước khi khai thác
 - Loại bỏ các tài khoản mới được tạo ra, xóa các file thực thi, scripts... được sử dụng trong quá trình khai thác lỗ hổng

Step 8. Reports

- ❑ Báo cáo chỉ ra các thông tin:
 - Lỗ hổng bảo mật mới tìm được
 - Cổng và dịch vụ đang mở
 - Các đề xuất khắc phục lỗ hổng

Sample Network Assessment Reports

Table of Contents

1. Executive Summary.....

2. Scan Results

3. Our Findings

4. Risk Assessment...

Critical Severity Vulnerabilities

High Severity Vulnerabilities

Medium Severity Vulnerabilities

Low Severity Vulnerabilities

5. Recommendations

Remediation.....

1. Executive Summary

The purpose of this vulnerability scan is to gather data on Windows hosts in the SAMPLE-INC domain in the 00.00.00.0/01 subnet. 100 systems were found to be active and were scanned.

2. Scan Results

The raw scan results will be provided upon delivery.

3. Our Findings

The results from the credentialed patch audit are listed below. Of the 100 identified hosts that were able to be scanned during this assessment, only 100 were successfully scanned. The 100 systems that were not successfully scanned were not included in the host list provided.

4. Risk Assessment

This report identifies security risks that could have significant impact on day-to-day business operations.

Critical Severity	High Severity	Medium Severity
286	171	

Critical Severity Vulnerability

286 were unique critical severity vulnerabilities. Critical vulnerabilities require immediate attention. They are relatively easy for attackers to exploit and may provide them with full control of the affected systems.

A table of the top critical severity vulnerabilities is provided below:

PLUGIN NAME	DESCRIPTION	SOLUTION	COUNT
Mozilla Firefox < 65.0	The version of Firefox installed on the remote Windows host is prior to 65.0. It is therefore affected by multiple vulnerabilities as referenced in the mfsa2019-01 advisory.	Upgrade to Mozilla Firefox version 65.0 or later.	22

High Severity Vulnerability

171 were unique high severity vulnerabilities. High severity vulnerabilities are often harder to exploit and may not provide the same access to affected systems.

A table of the top high severity vulnerabilities is provided below:

PLUGIN NAME	DESCRIPTION	SOLUTION	COUNT
MS15-124: Cumulative Security Update for Internet Explorer (3116180)	The version of Internet Explorer installed on the remote host is missing Cumulative Security Update 3116180. It is therefore affected by multiple vulnerabilities the majority of which are remote code execution vulnerabilities.	Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 8, RT 2012, 8.1, RT 8.1, 2012 R2, and 10.	24
Mozilla Firefox < 64.0 Multiple Vulnerabilities	The version of Mozilla Firefox installed on the remote Windows host is prior to 64.0. It is therefore affected by multiple vulnerabilities as noted in Mozilla Firefox stable channel update release notes for 2018/12/11.	Upgrade to Mozilla Firefox version 64.0 or later.	22

Medium Severity Vulnerability

116 were unique medium severity vulnerabilities. These vulnerabilities often provide information to attackers that may assist them in mounting subsequent attacks on your network. These should also be fixed in a timely manner but are not as urgent as the other vulnerabilities.

A table of the top high severity vulnerabilities is provided below:

PLUGIN NAME	DESCRIPTION	SOLUTION	COUNT
Mozilla Firefox < 62.0.2 Vulnerability	The version of Mozilla Firefox installed on the remote Windows host is prior to 62.0.2. It is therefore affected by a vulnerability as noted in Mozilla Firefox stable channel update release notes for 2018/09/21.	Upgrade to Mozilla Firefox version 62.0.2 or later.	17
Mozilla Firefox < 57.0.4 Speculative Execution Side-Channel Attack Vulnerability (Spectre)	The version of Mozilla Firefox installed on the remote Windows host is prior to 57.0.4. It is therefore vulnerable to a speculative execution side-channel attack. Code from a malicious web page could read data from memory.	Upgrade to Mozilla Firefox version 57.0.4 or later.	15

Countermeasures & Recommendations

- ❑ Phân chia nhiệm vụ chức năng của mỗi users
- ❑ Có cơ chế giám sát users
- ❑ Sao lưu dự phòng các dữ liệu quan trọng
- ❑ Thực hiện đào tạo nâng cao nhận thức
- ❑ Xây dựng chính sách an toàn
- ❑ Định kỳ đánh giá rủi ro và hiểm họa
- ❑ Đóng (xóa) các tài khoản không cần thiết, không còn được sử dụng

Countermeasures & Recommendations

- ☐ Scan toàn bộ lưu lượng đến để tìm kiếm, loại bỏ lưu lượng độc hại
- ☐ Đảm bảo rằng tất cả lưu lượng đi được kiểm soát thông qua proxy
- ☐ Sử dụng nguyên tắc đặc quyền tối thiểu
- ☐ Giới hạn quyền truy cập từ bên ngoài internet
- ☐ Đảm bảo rằng các bản vá được cập nhật liên tục
- ☐ Có các cơ chế và giải pháp phù hợp cho việc xác thực và phân quyền
- ☐ Có hệ thống ghi log & audit
- ☐ Đảm bảo an toàn về mặt vật lý cho các thiết bị, tài nguyên của tổ chức

Thank you & Any questions?

