

## Chương 2 | Các kỹ thuật và các bước tấn công của hacker (Phần 1)

- Tổng quan các bước tấn công của hacker
- Thu thập thông tin chủ động/thụ động (Active/Passive information gathering)
- Rà quét phát hiện cổng (Port scanning)
- Rà quét các lỗ hổng
- Tấn công lỗ hổng Network
- Tấn công lỗ hổng OS
- Tấn công ứng dụng web
- Tấn công sử dụng mã độc và cách thức xử lý, ngăn chặn bóc gỡ mã độc

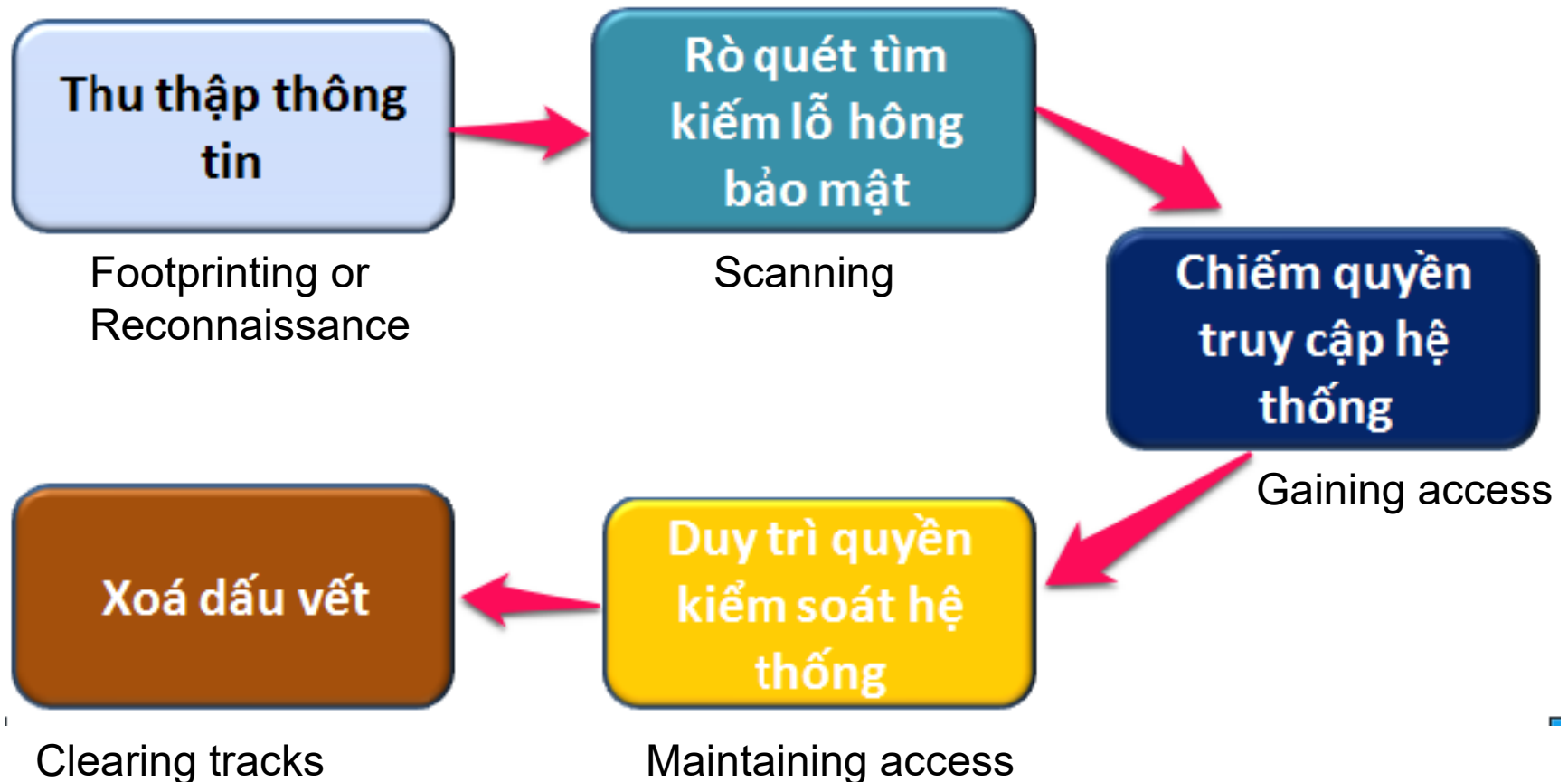
# Các giai đoạn tấn công mạng (1)

## Khái niệm tấn công mạng

- Là hành vi truy nhập, sử dụng, tiết lộ, làm gián đoạn, sửa đổi, phá hoại trái phép thông tin, hệ thống thông tin. *(tham khảo Luật ATTT mạng).*
- ⇒
- Kẻ tấn công (Attacker) khai thác lỗ hổng hệ thống, thoả hiệp (vượt qua) các cơ chế kiểm soát an ninh, chiếm quyền truy cập bất hợp pháp tài nguyên hệ thống
  - Làm thay đổi trái phép hệ thống hoặc các tính năng của ứng dụng
  - Đánh cắp dữ liệu các loại dữ liệu nhạy cảm

# Các giai đoạn tấn công mạng (2)

## ❖ Các giai đoạn tấn công



# Kỹ thuật Footprinting & Reconnaissance (2)

- **Khái niệm:**

- Là bước đầu tiên của quá trình tấn công nhằm thu thập (càng nhiều càng tốt) thông tin (nhạy cảm) về hệ thống mục tiêu => bước này còn gọi là tiền tấn công (Pre-attack) hoặc là bước trinh sát (reconnaissance)

- ❖ **Tại sao cần?**

- Nhằm đưa ra được phương án tấn công hiệu quả và khó bị phát hiện (lựa chọn thông tin và thu hẹp phạm vi cần tập trung)

- ❖ **Phân loại thông tin**

- Thông tin về mạng
- Thông tin về hệ thống
- Thông tin về tổ chức

- Hệ thống mạng (sơ đồ vật lý, các loại thiết bị mạng ...)
  - Hệ điều hành
  - Ứng dụng
  - Hệ thống bảo vệ: FW, IDS, IPS
  - Có áp dụng các cơ chế mã hoá (dữ liệu, trên đường truyền)?
  - Kinh nghiệm/ trình độ chuyên gia bảo mật ntn?
  - Chính sách => đã được xây dựng hay chưa. Tuân thủ thể nào?
  - Nhân viên => được đào tạo hay chưa; email, sđt, thói quen...
- => Chính là xác định hiện trạng attt sau đó thu hẹp phạm vi trọng tâm cho việc tấn công

## Information Available on Social Networking Sites

What Attacker Gets	What Users Do	What Organizations Do	What Attacker Gets
Contact info, location, etc.	Maintain profile	User surveys	Business strategies
Friends list, friends info, etc.	Connect to friends, chatting	Promote products	Product profile
Identify of a family members	Share photos and videos	User support	Social engineering
Interests	Play games, join groups	Recruitment	Platform/technology information
Activities	Creates events	Background check to hire employees	Type of business

# Một số kỹ thuật thu thập thông tin

- Các kỹ thuật tìm kiếm: Google Search (thông tin tuyển dụng), Google Hacking, Bing...
- Các trang mạng xã hội



Twitter



Youtube



Facebook



LinkedIn

- WHOIS: thông tin về chủ sở hữu tên miền
- Hoạt động tình báo
- Các trang web (trang tuyển dụng)
- Social Engineering

– <https://www.shodan.io>

- [Thu thập TT thiết bị kết nối mạng \(camera\)](#)

The screenshot displays the Shodan search engine interface. At the top, there is a search bar with the query 'camera' and buttons for 'Explore', 'Developer Pricing', and 'Enterprise Access'. Below the search bar, there are tabs for 'Exploits', 'Maps', and 'Images'. The main content area shows search results for 'camera'. On the left, there is a section titled 'TOTAL RESULTS' with the value '231,341'. Below this is a 'TOP COUNTRIES' section with a world map and a table of countries and their result counts. On the right, there is a list of search results. The first result is for the IP address '181.43.87.144', which is linked to 'Entel Chile S.A.'. A red arrow points from this IP address to a login dialog box that appears in the foreground. The dialog box has the title 'Đăng nhập' and contains the URL 'http://181.43.87.144:3954'. It also displays a message in Vietnamese: 'Kết nối của bạn tới trang web này không ở chế độ riêng tư'. Below the message are input fields for 'Tên người dùng' (Username) and 'Mật khẩu' (Password), and buttons for 'Đăng nhập' (Login) and 'Hủy' (Cancel).

SHODAN camera Explore Developer Pricing Enterprise Access

Exploits Maps Images

TOTAL RESULTS  
231,341

TOP COUNTRIES

Germany 53,877  
United States 34,273  
France 15,304  
Japan 10,655  
Italy 10,239

TOP SERVICES

181.43.87.144  
client-181-43-87-144.imovil.entelpcs.cl  
Entel Chile S.A.  
Added on 2019-03-26 03:49:55 GMT

HTTP/1.1 200 OK  
Server: Netwave IP Camera  
Date: Tue, 26 Mar 2019 03:49:55 GMT

181.43.87.144:3954

Đăng nhập  
http://181.43.87.144:3954  
Kết nối của bạn tới trang web này không ở chế độ riêng tư

Tên người dùng  
Mật khẩu

Đăng nhập Hủy



# Một số kỹ thuật thu thập, khai thác -2

- <https://sitereport.netcraft.com/?url=https://vietcombank.com.vn> (<http://www.netcraft.com>)
  - Thông tin liên quan đến máy chủ, những loại máy chủ, ứng dụng nền tảng, phiên bản
- <https://centralops.net>; <http://Whois.com>;
  - Thông tin về cơ quan chủ quản Domain, người đăng ký
  - Thu thập thông tin về website mục tiêu, ví dụ: administrator's e-mail...
- <https://www.iplocation.net/>
- <http://whatismyipaddress.com/ip/54.230.159.234>
  - Kiểm tra nguồn gốc địa chỉ IP
- <http://www.zone-h.org/search>

# Các toán tử trong Google Advanced (google hacking)

Các toán tử tìm kiếm	Mô tả
Site:	Tìm kiếm theo tên miền
Related:	Tìm kiếm các trang web tương tự
Cache:	Hiển thị các trang web được lưu trữ trên Google cache
Link:	Liệt kê các website c
Allintext:	Tìm kiếm các trang web chứa từ khoá cụ thể
Intext:	Tìm kiếm tài liệu chứa từ khoá cụ thể
Allintitle:	Tìm kiếm website chứa những từ khoá cụ thể trong tiêu đề
Intitle:	Tìm những tài liệu chứa những tài liệu cụ thể trong tiêu đề
Allinurl:	Tìm kiếm các website chứa từ khoá cụ thể trong URL
Inurl	Tìm những tài liệu chứa từ khoá cụ thể trong URL

Vd: "Config" intitle:"Index of" & inurl:gov & inurl:gov

# Toán tử trong Google Advanced -2

- Tìm kiếm thông bằng công cụ google – google hacking
  - inurl(html|htm|php)intitle:"index of" + "parent directory"+  
"vietnamnet"
  - intext:SQL syntax & inurl:index.php?=id & inurl:gov & inurl:gov.vn
  - "Config" intitle:"Index of" intext:vpn
- Phân tích email header
  - <https://toolbox.googleapps.com>
  - <https://mxtoolbox.com/EmailHeaders.aspx>

## Kỹ thuật Footprinting (6)

- **Chú ý:** Đối với những hệ thống không được quan tâm, bảo vệ thì:
  - Đôi khi, hacker tiến hành tấn công mà không cần mất nhiều thời gian để thu thập thông tin về mục tiêu, nhưng vẫn có thể tấn công thành công
  - Việc tấn công cũng không nhất thiết phải triển khai đầy đủ các bước trên. Ví dụ hacker bỏ qua việc xoá dấu vết tấn công, vì hệ thống cũng chưa có hệ thống theo dõi hoặc chưa được cấu hình ghi vết, nhật ký (log)

# SCAN

## ❖ Scan:

Là việc thu thập các thông tin (bảo mật) liên quan đến hệ thống mạng, máy chủ, ứng dụng

## ❖ Thông tin cần quan tâm khi scan là gì?

- Máy tính đang tham gia kết nối mạng
- Địa chỉ IP của các máy tính kết nối
- Loại HĐH hành trên máy tính
- Dịch vụ được cài đặt trên máy tính
- Kiến trúc hệ thống mạng

# SCAN (cont)

---

- Quét mạng (Network Scanning):  
Nhằm xác định hệ thống (host) có còn tham gia vào hệ thống mạng hay không
- Quét cổng (Port Scanning):  
Nhằm xác định cổng dịch vụ đang lắng nghe(listening) hay đang mở
- Quét các lỗ hổng (Vulnerability Scanning)  
Xác định lỗ hổng/điểm yếu trên hệ thống và trên các ứng dụng

# SCAN PORT (cont)

TCP SYN – Open port



Computer A		Computer B	
192.168.1.2:2342	-----syn-----	>	192.168.1.3:80
192.168.1.2:2342	<-----syn/ack-----		192.168.1.3:80
192.168.1.2:2342	-----RST-----	>	192.168.1.3:80

Kỹ thuật TCP SYN (còn gọi là kt quét bán mở), vì không hoàn tất kết nối TCP đầy đủ. Đây là kỹ thuật có thể hạn chế được các hệ thống phát hiện xâm nhập cũng như ghi logfile

# SCAN PORT (cont)

## Xmas



**Computer A**

**Computer B**

**Xmas scan directed at open port:**

```
192.5.5.92:4031 -----FIN/URG/PSH----->192.5.5.110:23
192.5.5.92:4031 <-----NO RESPONSE-----192.5.5.110:23
```

**Xmas scan directed at closed port:**

```
192.5.5.92:4031 -----FIN/URG/PSH----->192.5.5.110:23
192.5.5.92:4031<-----RST/ACK-----192.5.5.110:23
```

Máy A gửi tới máy B gói dữ liệu với các cờ (FIN, URG, PSH ...) được bật. Như vậy, với những cổng mở thì yêu cầu này sẽ bị loại bỏ, còn cổng đóng thì máy B gửi trả lại gói tín RST, qua đó máy A có thể đánh giá được cổng đang quét đóng/ cổng mở.



# SCAN (cont)

## Giới thiệu cụ Nmap

Nmap Scan	Command Syntax	Requires Privileged Access	Identifies TCP Ports	Identifies UDP Ports
TCP SYN Scan	-sS	YES	YES	NO
TCP connect() Scan	-sT	NO	YES	NO
FIN Scan	-sF	YES	YES	NO
Xmas Tree Scan	-sX	YES	YES	NO
Null Scan	-sN	YES	YES	NO
Ping Scan	-sP	NO	NO	NO
Version Detection	-sV	NO	NO	NO
UDP Scan	-sU	YES	NO	YES
IP Protocol Scan	-sO	YES	NO	NO
ACK Scan	-sA	YES	YES	NO
Window Scan	-sW	YES	YES	NO
RPC Scan	-sR	NO	NO	NO
List Scan	-sL	NO	NO	NO
Idlescan	-sI	YES	YES	NO
FTP Bounce Attack	-b	NO	YES	NO

---

**Quét các lỗ hổng hệ điều hành**

# Thu thập thông tin hệ điều hành

---

Thông tin về hệ điều hành hiển nhiên là rất hữu ích đối với hacker. Bởi rõ ràng các phiên bản về hệ điều hành khác nhau thì có các điểm yếu bảo mật khác nhau.

Những lỗ hổng đối với mỗi phiên bản của hệ điều hành, Attacker có thể dễ dàng tìm kiếm được và khai thác và rút ngắn được thời gian triển khai tấn công

---

## Một số công cụ:

Công cụ tìm kiếm thông tin hệ thống mục tiêu

Netcraft - Banner Grabbing

<https://www.netcraft.com/>

Công cụ tìm kiếm lỗ hổng hệ điều hành

Nessus

NMAP

MBSA

Retina

# SCAN

## Công cụ Netcraft - Banner Grabbing

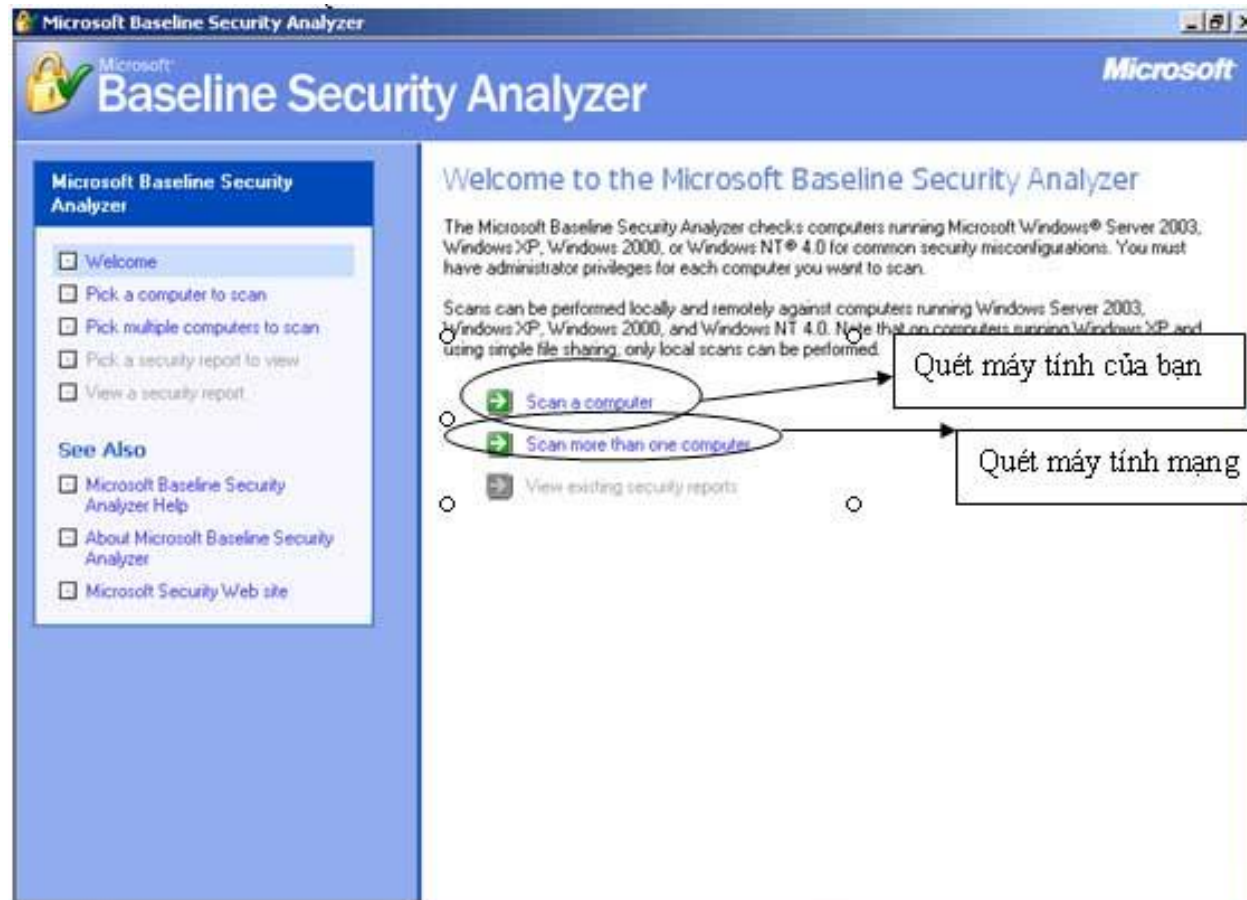
Là công cụ sử dụng kỹ thuật Aactive Stack Fingerprinting.  
Ta sẽ được một số thông tin về máy chủ web như hệ điều hành, phiên bản

The screenshot shows the Netcraft website interface. At the top, there's a search bar with the text "What's that site running?" and a search button. Below this, the results for "vtexpress.net" are displayed. The main section is titled "OS, Web Server and Hosting History for vtexpress.net". It shows a table with columns: OS, Server, Last changed, IP address, and Netblock Owner. The table lists several historical entries for the website, all running on Windows Server 2003 with Microsoft-IIS/6.0. The IP address is consistently 210.245.0.21, and the Netblock Owner is "Đại IP sử dụng cho Infrastructure".

OS	Server	Last changed	IP address	Netblock Owner
Windows Server 2003	Microsoft-IIS/6.0	27-May-2009	210.245.0.21	Đại IP sử dụng cho Infrastructure
Windows Server 2003	Microsoft-IIS/6.0	25-Feb-2009	210.245.0.21	Đại IP sử dụng cho Infrastructure
Windows Server 2003	Microsoft-IIS/6.0	23-Feb-2009	210.245.86.175	Đại IP cho Hosting Game
Windows Server 2003	Microsoft-IIS/6.0	27-Jan-2009	210.245.0.21	Đại IP sử dụng cho Infrastructure
Windows Server 2003	Microsoft-IIS/6.0	27-Oct-2008	210.245.0.21	Đại IP sử dụng cho Infrastructure
Windows Server 2003	Microsoft-IIS/6.0	26-Jul-2008	210.245.0.21	Đại IP sử dụng cho Infrastructure
Windows Server 2003	Microsoft-IIS/6.0	21-Jul-2008	210.245.31.22	Đại IP cho kết nối Router, Switch, Server
Windows Server 2003	Microsoft-IIS/6.0	15-Jul-2008	210.245.0.21	Đại IP sử dụng cho Infrastructure
Windows Server 2003	Microsoft-IIS/6.0	11-Jul-2008	210.245.31.22	Đại IP cho kết nối Router, Switch, Server
Windows Server 2003	Microsoft-IIS/6.0	1-Jul-2008	210.245.0.21	Đại IP sử dụng cho Infrastructure

# SCAN (cont)

## ❖ Công cụ Microsoft Baseline Security Analyzer (MBSA)

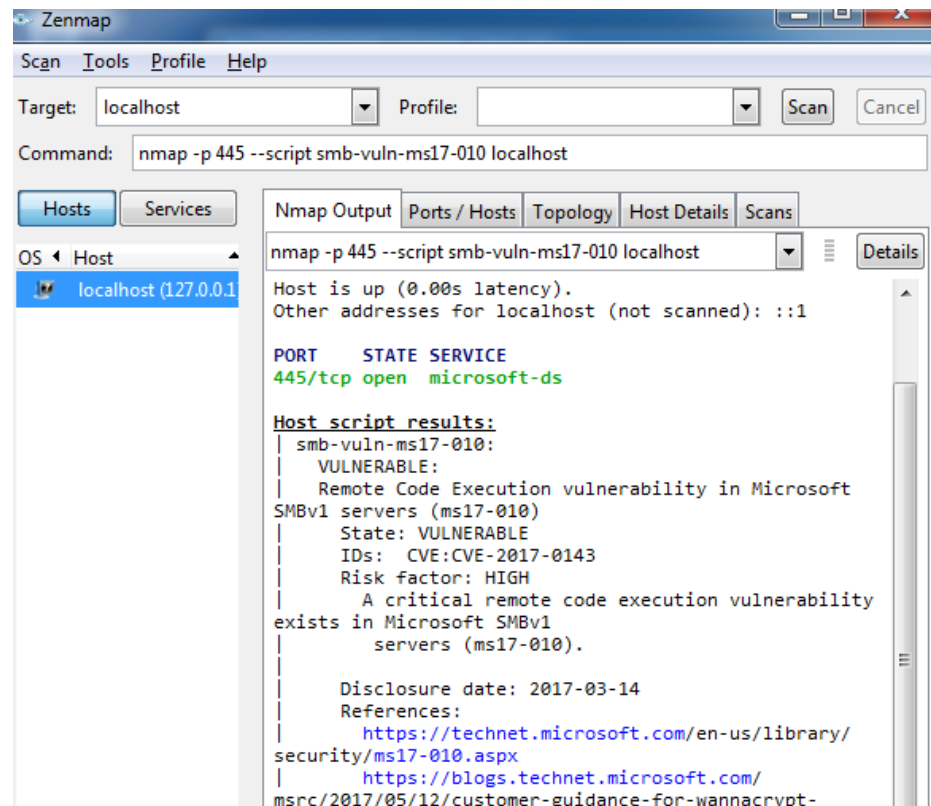
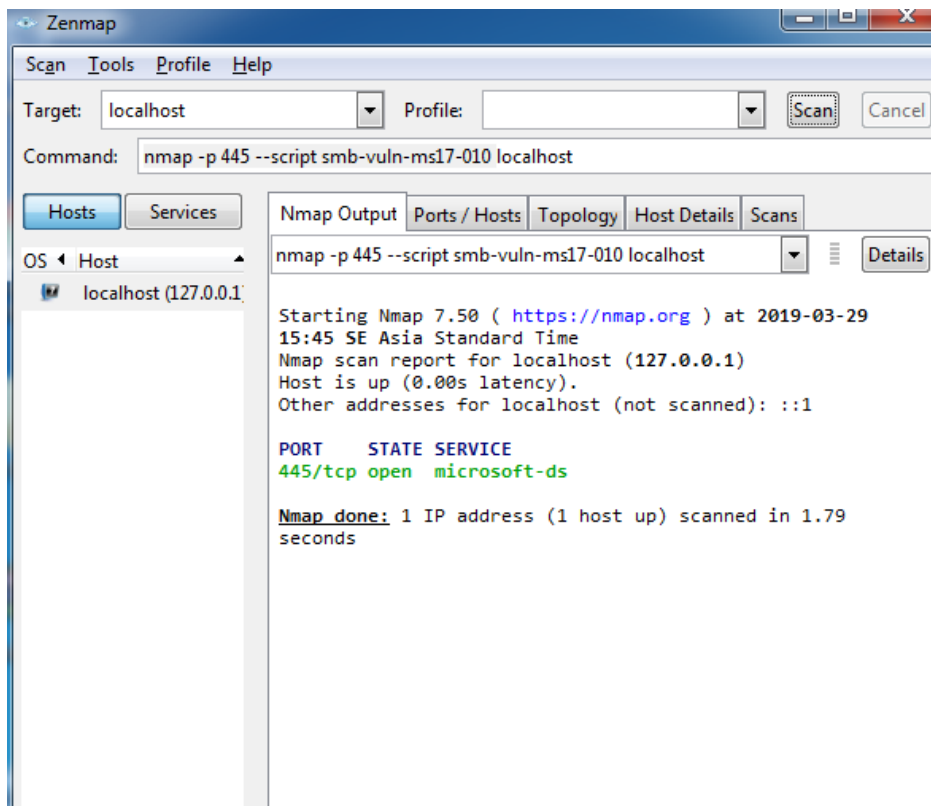


# NMAP - SCRIPT

Scan: `nmap -p 445 --script smb-vuln-ms17-010`

Disable SMB:

`Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SMB1 -Type DWORD -Value 0 -Force`



---

# Kiểm tra lỗi hỏng ứng dụng web



# Giới thiệu công cụ

Mất phí

IBM AppScan

Acunetix

Nguồn mở

W3AF

IronWASP

Arachni

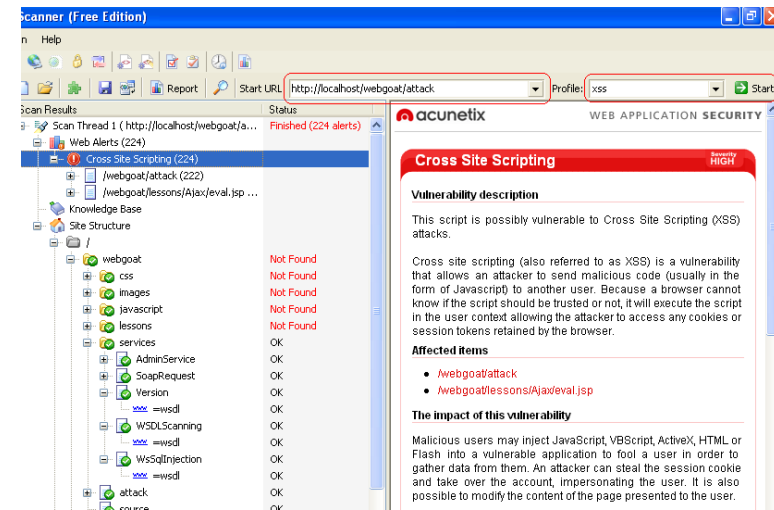
Link tham khảo:

<http://www.sectoolmarket.com/price-and-feature-comparison-of-web-application-scanners-unified-list.html>

# SCAN (cont)

## ❖ Acunetix WVS

Là chương trình tự động kiểm tra các ứng dụng web để tìm kiếm lỗ hổng bảo mật như: SQL Injection, hay Cross-Site Scripting,... đồng thời cũng tìm những chính sách đối với mật đăng nhập



# SCAN (cont)

## Các biện pháp phòng chống Scan

- Thường xuyên rà soát lại những điểm yếu hệ thống
- Chỉ mở những cổng (Port) cần thiết,
- Những thông tin nhạy cảm không nên đưa ra internet.  
Ví dụ thông tin về hệ điều hành, phiên bản phần mềm đang dùng....
- Triển khai các thiết bị an ninh mạng IDS/IPS, Firewall ....

## **KHAI THÁC LỖ HỒNG HỆ ĐIỀU HÀNH**

- Tìm hiểu chung về lỗ hồng HĐH và cách thức đánh giá**
- MS17\_010**
- MS11\_003**
- MS03\_026**

# Tìm hiểu chung về lỗ hổng HĐH và cách thực đánh giá

## 1- Thu thập thông tin về máy chủ/ máy trạm

- Xác định địa chỉ ip:
- Xác định tên miền:
- Xác định thông tin HĐH (Loại HĐH, phiên bản)

### Sử dụng công cụ

- Netcraft - Banner Grabbing

## 2- Tìm kiếm lỗ hổng bảo mật

### Sử dụng công cụ quét lỗ hổng HĐH

- Nessus
- MBSA (Microsoft Baseline Security Analyzer)
- Nmap

### Notes:

- Các lỗi rò quét được bằng việc sử dụng các tools trên thường có độ chính xác cao.

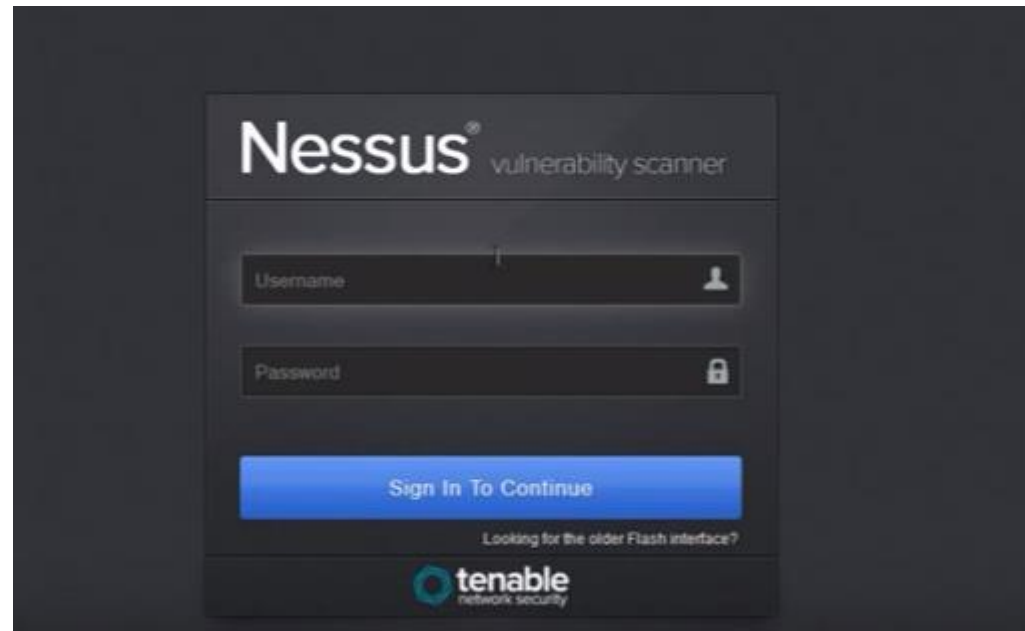
# Tìm hiểu chung về lỗ hổng HĐH

Lỗ hổng	Khả năng khai thác	Tác động
Đặt mật khẩu yếu	Sử dụng công cụ Brute force hoặc Dictionary Attack	Lộ mật khẩu hệ thống, chiếm quyền điều khiển hệ thống => ảnh hưởng đến tính bí mật
Mở Port	Sử dụng công cụ: <ul style="list-style-type: none"><li>• metasploit</li><li>• Malware</li></ul>	Tấn công lỗ hổng dịch vụ (SMB), chiếm quyền điều khiển => ảnh hưởng đến tính bí mật
Không cập nhật bản vá lỗi	Tùy từng lỗ hổng mà có thể khai thác khó hay dễ: Có thể trực tiếp chiếm quyền điều khiển bằng remote code (vd: MS17_010) Cần kết hợp kỹ thuật Social Engineering Có các công cụ hỗ trợ khai thác	Chiếm quyền điều khiển hệ thống; Leo thang đặc quyền admin; ảnh hưởng đến tính bí mật

**Tham khảo:** <http://www.cvedetails.com>

# Công cụ Nessus

- Công cụ Nessus cho phép kiểm tra các lỗ hổng trên hệ thống
- Có hai phiên bản: có phí và không có phí



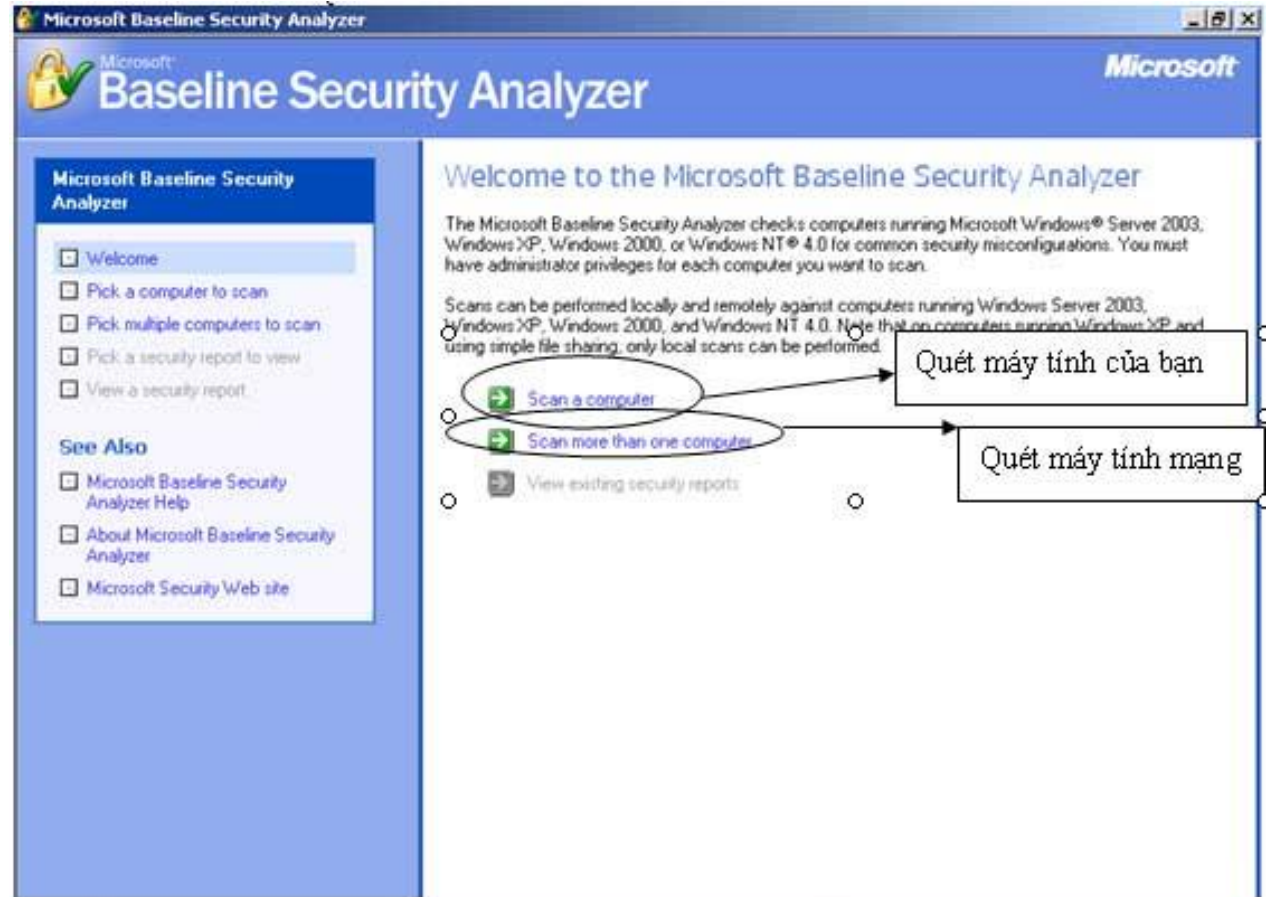
<https://www.tenable.com>

# Công cụ MBSA

**Công cụ MBSA:**  
**cho biết thông tin về hệ thống như:**

- FW ko được bật
- Mật khẩu yếu
- Trạng thái cập nhật bản vá lỗi

**Là phần mềm miễn phí của Microsoft**



<https://www.microsoft.com/en-us/download/details.aspx?id=7558>



# Công cụ Nmap

- Nmap là phần mềm miễn phí
- Kiểm tra các port đang được mở
- Kiểm tra các lỗ hổng bảo mật chưa được cập nhật bản vá

<https://nmap.org/>

Nmap Scan	Command Syntax	Requires Privileged Access	Identifies TCP Ports	Identifies UDP Ports
TCP SYN Scan	-sS	YES	YES	NO
TCP connect() Scan	-sT	NO	YES	NO
FIN Scan	-sF	YES	YES	NO
Xmas Tree Scan	-sX	YES	YES	NO
Null Scan	-sN	YES	YES	NO
Ping Scan	-sP	NO	NO	NO
Version Detection	-sV	NO	NO	NO
UDP Scan	-sU	YES	NO	YES
IP Protocol Scan	-sO	YES	NO	NO
ACK Scan	-sA	YES	YES	NO
Window Scan	-sW	YES	YES	NO
RPC Scan	-sR	NO	NO	NO
List Scan	-sL	NO	NO	NO
Idlescan	-sI	YES	YES	NO
FTP Bounce Attack	-b	NO	YES	NO

---

**Lỗ hổng MS17\_010**

# Phân tích lỗ hổng MS17\_010 (1)

- **Các phiên bản bị ảnh hưởng**

[illegible]

# Phân tích lỗ hổng MS17\_010 (2)

Module: Doublepulsar

=====

Name	Value
NetworkTimeout	60
TargetIp	208
TargetPort	445
DllPayload	C:\Documents and Settings\Admini ts\Downloads\nsa1.dll
DllOrdinal	1
ProcessName	chrome.exe
ProcessCommandLine	
Protocol	SMB
Architecture	x86
Function	RunDLL

```
[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[+] Selected Protocol SMB
[.] Connecting to target...
[+] Connected to target, pinging backdoor...
    [+] Backdoor returned code: 10 - Success!
    [+] Ping returned Target architecture: x86 (32)
SMB Connection string is: Windows 7 Professional 7
Target OS is: 7 x86
Target SP is: 0
    [+] Backdoor installed
    [+] DLL built
    [.] Sending shellcode to inject DLL
    [+] Backdoor returned code: 10 - Success!
    [+] Backdoor returned code: 10 - Success!
    [+] Backdoor returned code: 10 - Success!
    [+] Command completed successfully
[+] Doublepulsar Succeeded
```

C:\WINDOWS\system32\cmd.exe - python

```
*0> x86      x86 32-bits
1> x64      x64 64-bits

[?] Architecture [0] :

[*] Function :: Operation for back

*0> OutputInstall      Only output
isk.
1> Ping                Test for p
2> RunDLL              Use an APC
3> RunShellcode        Run raw sh
4> Uninstall           Remove's b

[?] Function [0] : 2
[+] Set Function => RunDLL

[*] DllPayload :: DLL to inject in










[?] DllPayload [1] :

[*] DllPayload :: DLL to inject in

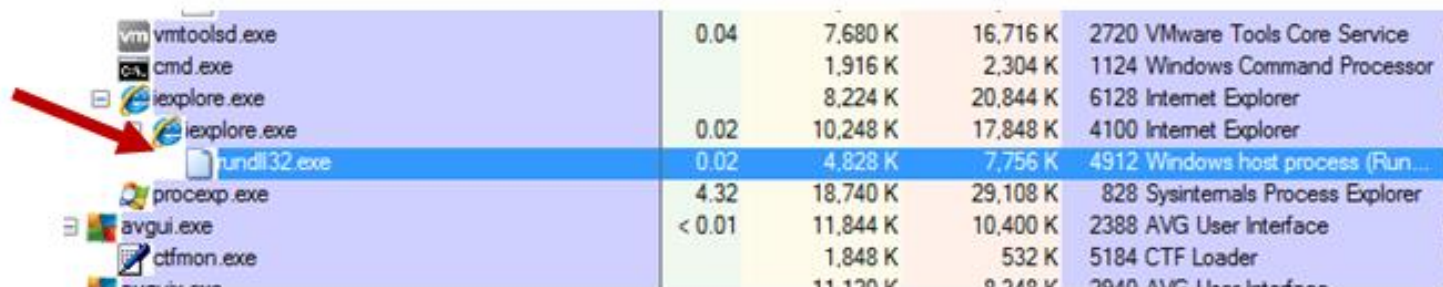
[?] DllPayload [1] : C:\Documents an
ds\nsa1.dll
```

# Phân tích lỗ hổng MS17\_010 (3)

Trước khi inject nsa1.dll vào tiến trình iexplore.exe

	CefHost.exe				
	vmtoolsd.exe	0.07	12,444 K	21,404 K	2720 VMware Tools
	cmd.exe		1,916 K	2,304 K	1124 Windows Command
	iexplore.exe		8,820 K	21,320 K	6128 Internet Explorer
	iexplore.exe	0.02	10,560 K	17,864 K	4100 Internet Explorer
	procexp.exe	0.57	16,904 K	27,704 K	828 Sysinternals Process
	avgui.exe	< 0.01	11,896 K	10,316 K	2388 AVG User Interface
	ctfmon.exe		1,848 K	708 K	5184 CTF Loader
	avgui.exe		11,120 K	9,240 K	2040 AVG User Interface

Sau khi inject nsa1.dll vào tiến trình iexplore.exe. Shell code nsa1.dll sẽ được chạy dưới tiến trình rundll32.exe là tiến trình con của tiến trình iexplore.exe



vmtoolsd.exe		0.04	7,680 K	16,716 K	2720 VMware Tools Core Service
cmd.exe			1,916 K	2,304 K	1124 Windows Command Processor
iexplore.exe			8,224 K	20,844 K	6128 Internet Explorer
iexplore.exe		0.02	10,248 K	17,848 K	4100 Internet Explorer
rundll32.exe		0.02	4,828 K	7,756 K	4912 Windows host process (Run...
procexp.exe		4.32	18,740 K	29,108 K	828 Sysinternals Process Explorer
avgui.exe		< 0.01	11,844 K	10,400 K	2388 AVG User Interface
ctfmon.exe			1,848 K	532 K	5184 CTF Loader
			11,120 K	9,240 K	2040 AVG User Interface

# Phân tích lỗ hổng MS17\_010 (4)

Tạo file backdoor tên là nsa1.dll

## Index of /

	<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
	<a href="#">backdoor542017-v2.exe</a>	2017-04-30 05:36	72K	
	<a href="#">backdoor542017.exe</a>	2017-04-30 05:23	74K	
	<a href="#">harvester_2017-04-29 18:33:40.935500.txt</a>	2017-04-29 18:36	896	
	<a href="#">harvester_2017-04-29 18:58:57.764361.txt</a>	2017-04-29 18:58	0	
	<a href="#">in.html</a>	2017-04-29 18:58	122K	
	<a href="#">nsa1.dll</a>	2017-04-29 01:06	5.0K	
	<a href="#">post.php</a>	2017-04-29 18:58	315	

# Khuyến nghị khác phục lỗ hổng

## MS17\_010

- Cần đóng port 445/139 trên hệ thống nếu ko được sử dụng
- Sao lưu dữ liệu
- Sử dụng và cập nhật phần mềm anti-virus
- Cần trọng khi nhận được email có dấu hiệu lạ
- Cập nhật bản vá lỗi hệ điều hành

### Tham khảo

- <https://support.microsoft.com/vi-vn/help/2696547/how-to-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and-windows>
- <http://www.backup-utility.com/anti-ransomware/how-to-block-port-445-in-windows-3889.html>

# NGHE LÉN (SNIFFER - MitM)





# Khái niệm

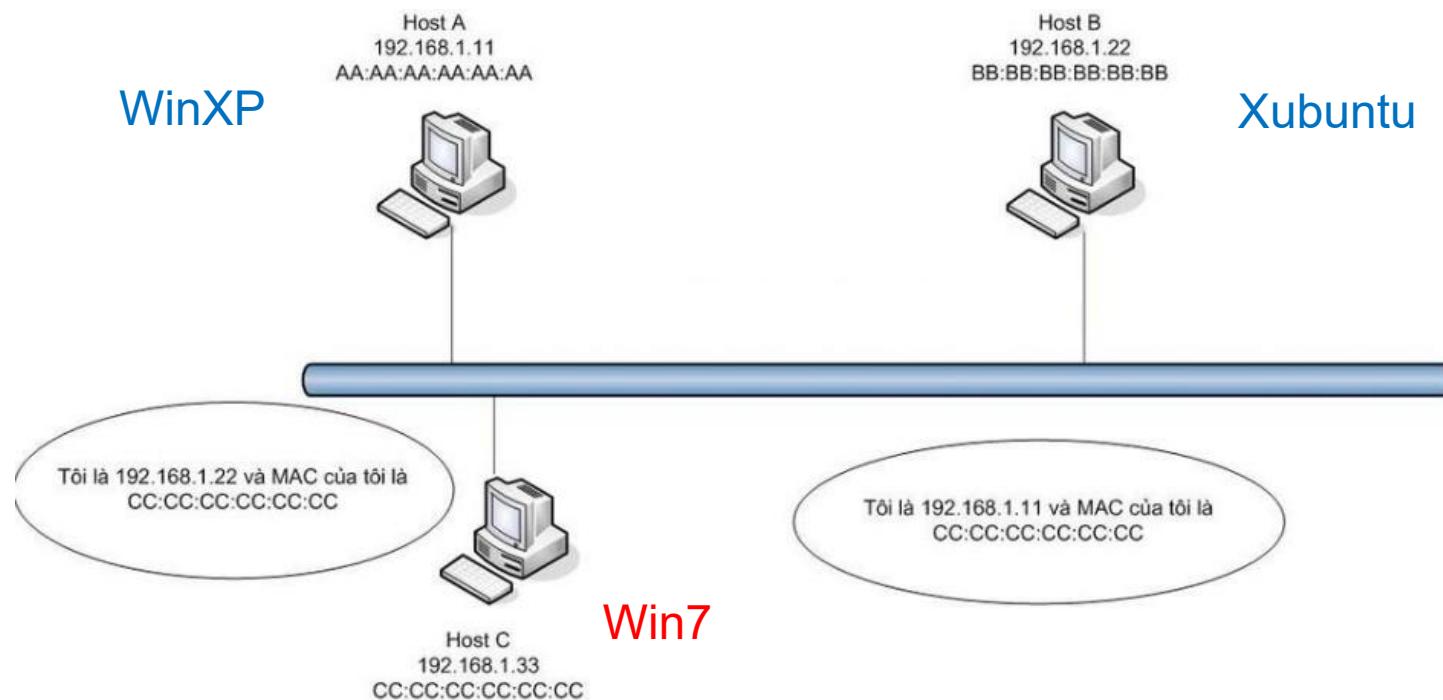
**Là một chương trình hay thiết bị dùng để chặn bắt dữ**

**liệu được truyền trên hệ thống mạng. Kỹ thuật tấn công này còn gọi là Man-in-the-Middle (MitM)**

- **Mục tiêu của việc nghe lén là lấy được:**
  - Mật khẩu (của email, web, ftp ....)
  - Nội dung của các email
  - Các tệp lưu chuyển
- Các giao thức có thể bị nghe lén bao gồm:
  - HTTP: dữ liệu ở dạng bản rõ (clear text)
  - SMTP, POP, IMAP, FTP, NNTP ,...: gồm mật khẩu và dữ liệu bản rõ

# Các kỹ thuật nghe lén (cont)

- Kiểu tấn công ARP Spoofing:



# Biện pháp phòng chống nghe lén

- Thiết lập hệ thống phát hiện xâm nhập IDS, có thể dùng phần mềm giám sát Snort (miễn phí)
- Sử dụng phần mềm phát hiện nghe lén, như: AntiSniff, Xarp, ARPwatch, Ettercap,...
- Giới hạn miền Broadcast => Chia VLAN
- Hạn chế thiết bị kết nối trái phép bằng cách thiết lập Port Security, áp dụng chính sách giới hạn cài đặt phần mềm
- Với mạng nhỏ có thể sử dụng IP tĩnh, bảng ARP tĩnh
- Áp dụng cơ chế mã hoá trên đường truyền


# Công cụ phát hiện nghe lén

## ❖ Công cụ Xarp

Phát hiện và cảnh báo các thông máy nghe lén và bị nghe lén



**XArp - unregistered version**

File XArp Professional Help

 Status: ARP attacks detected! Security level set to: aggressive

- [View detected attacks](#)
- [Read the 'Handling ARP attacks' help](#)
- [View XArp logfile](#)

[Get XArp Professional now!](#)  
[Register XArp Professional](#)

	IP	MAC	Host	Vendor	Interface
	192.168.0.1	00-25-9c-80-e4-78		Cisco-linksys, Llc	0x5 - Realtek
	192.168.0.2	00-1c-9c-c4-cc-00		Nortel	0x5 - Realtek

OK

< Alert 1 of 1 >

12/1/2006 16:50:55

DirectedRequestFilter: targeted request.  
 destination mac of arp request not set to  
 broadcast/invalid address

Interface : 0x5  
 [ethernet]  
 source mac: 00-25-9c-80-e4-78  
 dest mac : 00-24-8c-c5-76-ff  
 type : 0x806  
 [arp]  
 direction : in  
 type : request  
 source ip : 192.168.0.1  
 dest ip : 192.168.0.14  
 source mac: 00-25-9c-80-e4-78  
 dest mac : 00-00-00-00-00-00

---

**THANK YOU !**