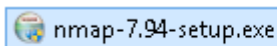


LAB02 step01-Window Nmap

Name	Tran Dang Khoa
Email address	Khoab2014926@student.cu.edu.vn
OS	Windows
Web bro	Chrome

Its illegal to scan outside network

1. Install Windows Nmap



2. Confirm Windows Nmap installation

- 1 CMD nmap

```
C:\Users\student>nmap
Nmap 7.94 < https://nmap.org >
Usage: nmap [Scan Type(s)] [Options] <target specification>
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  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]
  --dns-servers <serv1[,serv2[,...]]>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
```

- 2 CMD nmap-h

```

C:\Users\student>nmap-h
'nmap-h' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\student>nmap h
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-22 15:13 SE Asia Standard Time
Failed to resolve "h".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 2.38 seconds

C:\Users\student>nmap -h
Nmap 7.94 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] <target specification>
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  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:

```

3. Design Nmap scanning pen-test scenario under Windows

	scanner	target
OS	Windows	Windows, Linux
IP address	Test - bed host IP	<ul style="list-style-type: none"> • Localhost • CTU IP • CICT IP • Neighboring PC IP • VM IP(Ubuntu, Centos)
scanning program	Windows <u>Nmap</u>	
scanning types	-sT: -sS: -sP: -sU: -sF -P-PB -O -PS	

4. Execute Windows Nmap based on upper 3.scenario (screenshot and explain the scanning)

1 nmap -sT CTU, explain the meaning of nmap -sT

```

7741/tcp open  scriptview
7777/tcp open  cbt
7778/tcp open  interwise
7800/tcp open  asr
7911/tcp open  unknown
7920/tcp open  unknown
7921/tcp open  unknown
7937/tcp open  nsrexecd
7938/tcp open  lgtoMapper
7999/tcp open  irdmi2
8000/tcp open  http-alt
8001/tcp open  vcom-tunnel
8002/tcp open  teradataordbms
8007/tcp open  ajp12
8008/tcp open  http
8009/tcp open  ajp13
8010/tcp open  xmpp
8011/tcp open  unknown
8021/tcp open  ftp-proxy
8022/tcp open  oa-system
8031/tcp open  unknown
8042/tcp open  fs-agent
8045/tcp open  unknown
8080/tcp open  http-proxy
8081/tcp open  blackice-icecap

```

- 2 nmap -sS CTU, explain the meaning of nmap -sS

```

C:\Users\student>nmap -sS ctu.edu.vn
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-22 15:55 SE Asia Standard Time
Nmap scan report for ctu.edu.vn (172.18.45.2)
Host is up (0.0013s latency).
Other addresses for ctu.edu.vn (not scanned): 172.18.45.6 172.18.27.2 172.18.27.
6 10.16.36.54
rDNS record for 172.18.45.2: CTUAD3.ctu.edu.vn
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
389/tcp   open  ldap
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl

Nmap done: 1 IP address (1 host up) scanned in 5.14 seconds
C:\Users\student>

```

- 3 nmap -sP CICT, explain the meaning of nmap -sP

```

C:\Users\student>nmap -sP cit.ctu.edu.vn
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-22 15:58 SE Asia Standard Time
Nmap scan report for cit.ctu.edu.vn (10.16.63.194)
Host is up (0.0030s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
C:\Users\student>

```

- 4 nmap -sU CICT, explain the meaning of nmap -sU

```

C:\Users\student>nmap -sU 172.18.45.6
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-22 16:24 SE Asia Standard Time
Nmap scan report for CTUAD8.ctu.edu.vn (172.18.45.6)
Host is up (0.0028s latency).
Not shown: 998 open|filtered udp ports (no-response)
PORT      STATE SERVICE
53/udp    open  domain
123/udp   open  ntp

Nmap done: 1 IP address (1 host up) scanned in 7.03 seconds
C:\Users\student>

```

- 5 nmap -sF VM IP, explain the meaning of nmap -sF

```

C:\Users\student>nmap -sF 192.168.56.1
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-22 16:07 SE Asia Standard Time
Nmap scan report for 192.168.56.1
Host is up (0.00081s latency).
All 1000 scanned ports on 192.168.56.1 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
C:\Users\student>

```

- 6 nmap -PB VM IP, explain the meaning of nmap -PB

```

C:\Users\student>nmap -PB 192.168.56.1
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-22 16:08 SE Asia Standard Time
Nmap scan report for 192.168.56.1
Host is up (0.0011s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
1025/tcp   open  NFS-or-IIS
1026/tcp   open  LSA-or-nterm
1027/tcp   open  IIS
1028/tcp   open  unknown

```

- 7 nmap -O VM IP IP, explain the meaning of nmap -O

```

C:\Users\student>nmap -O 192.168.56.1
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-22 16:09 SE Asia Standard Time
Nmap scan report for 192.168.56.1
Host is up (0.00047s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
1025/tcp   open  NFS-or-IIS
1026/tcp   open  LSA-or-nterm
1027/tcp   open  IIS
1028/tcp   open  unknown
1029/tcp   open  ms-lsa
1031/tcp   open  iad2
1033/tcp   open  netinfo
3389/tcp   open  ms-wbt-server
5405/tcp   open  pcduo

```

- 8 nmap -PS VM IP, explain the meaning of nmap -PS

```

C:\Users\student>nmap -PS 192.168.56.1
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-22 16:09 SE Asia Standard Time
Nmap scan report for 192.168.56.1
Host is up (0.0012s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
1025/tcp   open  NFS-or-IIS
1026/tcp   open  LSA-or-nterm
1027/tcp   open  IIS
1028/tcp   open  unknown
1029/tcp   open  ms-lsa
1031/tcp   open  iad2
1033/tcp   open  netinfo
3389/tcp   open  ms-wbt-server
5405/tcp   open  pcduo

```

<https://nmap.org/download.html>

<http://www.insecure.org/nmap/>