

Activity 7 - Recon and Defense (Network Security I)

Part 1: Preparation

1. Check ssh service status

```
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
            RX packets 154 bytes 13262 (13.2 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 154 bytes 13262 (13.2 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

nattamon@nattamon-VirtualBox:~$ systemctl status ssh.service
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: >
  Active: active (running) since Tue 2022-09-20 10:59:12 +07; 6min ago
    Docs: man:sshd(8)
          man:sshd_config(5)
  Process: 661 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
  Main PID: 688 (sshd)
    Tasks: 1 (limit: 1078)
   Memory: 880.0K
      CGroup: /system.slice/ssh.service
              └─688 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

Oct 20 10:59:12 nattamon-VirtualBox systemd[1]: Starting OpenBSD Secure Shell...
Oct 20 10:59:12 nattamon-VirtualBox sshd[688]: Server listening on 0.0.0.0 port 22.
Oct 20 10:59:12 nattamon-VirtualBox sshd[688]: Server listening on :: port 22.
Oct 20 10:59:12 nattamon-VirtualBox systemd[1]: Started OpenBSD Secure Shell >
lines 1-16/16 (END)
```

2. Check VM's IP address

```
nattamon@nattamon-VirtualBox:~$ ^C
nattamon@nattamon-VirtualBox:~$ ifconfig -a
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.209.231 netmask 255.255.255.0 broadcast 192.168.209.255
              inet6 2001:44c8:4105:de8b:72e8:eaab:e1bc:d73c prefixlen 64 scopeid 0x0
0<global>
        inet6 2001:44c8:4105:de8b:519b:ec5c:321f:bb7 prefixlen 64 scopeid 0x0
<global>
        inet6 fe80::1e5b:5446:2f3d:4801 prefixlen 64 scopeid 0x20<link>
ether 08:00:27:73:67:de txqueuelen 1000 (Ethernet)
RX packets 91 bytes 24832 (24.8 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 118 bytes 14991 (14.9 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 154 bytes 13262 (13.2 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 154 bytes 13262 (13.2 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

nattamon@nattamon-VirtualBox:~$
```

Part 2: Reconnaissance

Attacking localhost

Zenmap

Scan Tools Profile Help

Target: localhost Profile: Intense scan plus UDP Scan Cancel

Command: nmap -sS -sU -T4 -A -v localhost

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

- localhost (127.0.0.1)
- 192.168.209.51

```
nmap -sS -sU -T4 -A -v localhost
Starting Nmap 7.93 ( https://nmap.org ) at 2022-09-20 11:15 SE Asia Standard Time
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 11:15
Completed NSE at 11:15, 0.00s elapsed
Initiating NSE at 11:15
Completed NSE at 11:15, 0.00s elapsed
Initiating NSE at 11:15
Completed NSE at 11:15, 0.00s elapsed
Initiating SYN Stealth Scan at 11:15
Scanning localhost (127.0.0.1) [1000 ports]
Discovered open port 135/tcp on 127.0.0.1
Discovered open port 3306/tcp on 127.0.0.1
Discovered open port 445/tcp on 127.0.0.1
Discovered open port 8089/tcp on 127.0.0.1
Discovered open port 8000/tcp on 127.0.0.1
Completed SYN Stealth Scan at 11:15, 0.07s elapsed (1000 total ports)
Initiating UDP Scan at 11:15
Scanning localhost (127.0.0.1) [1000 ports]
Completed UDP Scan at 11:15, 7.16s elapsed (1000 total ports)
Initiating Service scan at 11:15
Scanning 12 services on localhost (127.0.0.1)
Service scan Timing: About 50.00% done; ETC: 11:19 (0:01:38 remaining)
Completed Service scan at 11:17, 102.51s elapsed (12 services on 1 host)
Initiating OS detection (try #1) against localhost (127.0.0.1)
NSE: Script scanning 127.0.0.1.
Initiating NSE at 11:17
NSE ERROR [112.8490s] mksock_bind_addr(): Bind to 0.0.0.0:500 failed (IOD #70): An attempt was made to access a socket in a way forbidden by its access permissions. (10013)
NSE ERROR [113.9830s] mksock_bind_addr(): Bind to 0.0.0.0:500 failed (IOD #93): An attempt was made to access a socket in a way forbidden by its access permissions. (10013)
NSE ERROR [115.1050s] mksock_bind_addr(): Bind to 0.0.0.0:500 failed (IOD #97): An attempt was made to access a socket in a way forbidden by its access permissions. (10013)
NSE ERROR [115.4160s] mksock_bind_addr(): Bind to 0.0.0.0:500 failed (IOD #98): An attempt was made to access a socket in a way forbidden by its access permissions. (10013)
NSE ERROR [116.2270s] mksock_bind_addr(): Bind to 0.0.0.0:500 failed (IOD #101): An attempt was made to access a socket in a way forbidden by its access permissions. (10013)
NSE ERROR [119.1870s] mksock_bind_addr(): Bind to 0.0.0.0:500 failed (IOD #109): An attempt was made to access a socket in a way forbidden by its access permissions. (10013)
```

< >

Filter Hosts

Zenmap

Scan Tools Profile Help

Target: localhost Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v localhost

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

- localhost (127.0.0.1)
- 192.168.209.51

```
nmap -sS -sU -T4 -A -v localhost
NSE: Script scanning 127.0.0.1.
Completed NSE at 11:19, 98.36s elapsed
Initiating NSE at 11:19
Completed NSE at 11:19, 1.95s elapsed
Initiating NSE at 11:19
Completed NSE at 11:19, 0.00s elapsed
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00042s latency).
Other addresses for localhost (not scanned): ::1
rDNS record for 127.0.0.1: kubernetes.docker.internal
Not shown: 995 closed tcp ports (reset), 993 closed udp ports (port-unreach)
```

```
PORT      STATE     SERVICE      VERSION
135/tcp    open      msrpc        Microsoft Windows RPC
445/tcp    open      microsoft-ds?
3306/tcp   open      mysql        MySQL 8.0.27
| mysql-info:
|   Protocol: 10
|   Version: 8.0.27
|   Thread ID: 9
|   Capabilities flags: 65535
|   Some Capabilities: SupportsLoadDataLocal, FoundRows,
|   DontAllowDatabaseTableColumn, InteractiveClient, LongPassword, Support41Auth,
|   SupportsTransactions, IgnoreSigpipes, Speaks41ProtocolOld, LongColumnFlag,
|   SwitchToSSLAfterHandshake, ODBCClient, Speaks41ProtocolNew, SupportsCompression,
|   ConnectWithDatabase, IgnoreSpaceBeforeParenthesis, SupportsMultipleStatements,
|   SupportsAuthPlugins, SupportsMultipleResults
|   Status: Autocommit
|   Salt: ##\x1F\zlw/7]iaZ\x15e"cN\x1E`  

|_ Auth Plugin Name: caching_sha2_password
| ssl-cert: Subject:
commonName=MySQL_Server_8.0.27_Auto_Generated_Server_Certificate
| Issuer: commonName=MySQL_Server_8.0.27_Auto_Generated_CA_Certificate
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-10-23T10:36:53
| Not valid after: 2031-10-21T10:36:53
| MD5: 25c133d3abd2b47a99e55e0b43f3c607
| SHA-1: 1fd1ffe62466308aaed2cff9f0ab30029feab8135
| _ssl-date: TLS randomness does not represent time
8000/tcp   open      http        Splunkd httpd
| http-robots.txt: 1 disallowed entry
|_/
| http-title: Site doesn't have a title (text/html; charset=UTF-8).
| Requested resource was http://localhost:8000/en-US/account/login?return_to=%2Fen-US%2F
|_...
```

The screenshot shows the Zenmap interface with the following details:

- Target:** localhost
- Profile:** Intense scan
- Command:** nmap -T4 -A -v localhost

The results pane displays the output of the Nmap scan:

```
nmap -sS -sU -T4 -A -v localhost
| http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_Requested resource was http://localhost:8000/en-US/account/login?return_to=%2Fen-US%2F
| http-favicon: Unknown favicon MD5: E60C968E8FF3CC2F4FB869588E83AFC6
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
| http-server-header: Splunkd
8089/tcp open ssl/http Splunkd httpd
| http-methods:
|_ Supported Methods: GET HEAD OPTIONS
| http-robots.txt: 1 disallowed entry
|_/
| http-title: splunkd
| ssl-cert: Subject: commonName=SplunkServerDefaultCert/
organizationName=SplunkUser
| Issuer: commonName=SplunkCommonCA/organizationName=Splunk/
stateOrProvinceName=CA/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2022-08-22T12:39:03
| Not valid after: 2025-08-21T12:39:03
| MD5: ba7dedef572f599db58f5b82ca50f3b2
| SHA-1: 2f0b8b6ff3b53efbcb647f583b71185868825af3
| http-server-header: Splunkd
137/udp open|filtered netbios-ns
500/udp open|filtered isakmp
1900/udp open|filtered upnp
4500/udp open|filtered nat-t-ike
5050/udp open|filtered mmcc
5353/udp open|filtered zeroconf
5355/udp open|filtered llmnr
Device_type: general purpose
Running: Microsoft Windows 10
OS_CPE: cpe:/o:microsoft:windows_10
OS_details: Microsoft Windows 10 1809 - 1909
Network Distance: 0 hops
TCP_Sequence_Prediction: Difficulty=260 (Good luck!)
IP_ID_Sequence_Generation: Incremental
Service_Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|_ 311:
| Message signing enabled but not required
| smb2-time:
```

The screenshot shows the Zenmap interface. The target is set to 'localhost' with a profile of 'Intense scan'. The command entered is 'nmap -T4 -A -v localhost'. The results tab is selected, displaying the Nmap output. The output shows details about the host, including its OS (Microsoft Windows 10), services (e.g., 137/udp, 500/udp, 1900/udp, 4500/udp, 5050/udp, 5353/udp, 5355/udp), device type (general purpose), and running applications (Microsoft Windows 10). It also shows host script results for SMB security mode and NSE script post-scanning. The scan completed in 212.29 seconds.

```
nmap -sS -sU -T4 -A -v localhost
stateOrProvinceName=CA/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2022-08-22T12:39:03
| Not valid after: 2025-08-21T12:39:03
| MD5: ba7dedef572f599db58f5b82ca50f3b2
|_SHA-1: 2f0b8b6ff3b53efbc647f583b71185868825af3
|_http-server-header: Splunkd
137/udp open|filtered netbios-ns
500/udp open|filtered isakmp
1900/udp open|filtered upnp
4500/udp open|filtered nat-t-ike
5050/udp open|filtered mmcc
5353/udp open|filtered zeroconf
5355/udp open|filtered llmnr
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1809 - 1909
Network Distance: 0 hops
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   311:
|     Message signing enabled but not required
| smb2-time:
|   date: 2022-09-20T04:17:46
|   start_date: N/A

NSE: Script Post-scanning.
Initiating NSE at 11:19
Completed NSE at 11:19, 0.00s elapsed
Initiating NSE at 11:19
Completed NSE at 11:19, 0.00s elapsed
Initiating NSE at 11:19
Completed NSE at 11:19, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 212.29 seconds
    Raw packets sent: 2577 (120.887KB) | Rcvd: 4607 (235.978KB)
```

Attacking target host

Zenmap

Scan Tools Profile Help

Target: 192.168.209.42 Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v 192.168.209.42

Hosts	Services	Nmap Output	Ports / Hosts	Topology	Host Details	Scans	Details
OS Host		nmap -T4 -A -v 192.168.209.42					
localhost (127.0.0.1)		Starting Nmap 7.93 (https://nmap.org) at 2022-09-20 11:26 SE Asia Standard Time					
192.168.209.42		NSOCK ERROR [0.3100s] ssl_init_helper(): OpenSSL legacy provider failed to load.					
192.168.209.51		NSE: Loaded 155 scripts for scanning. NSE: Script Pre-scanning. Initiating NSE at 11:26 Completed NSE at 11:26, 0.00s elapsed Initiating NSE at 11:26 Completed NSE at 11:26, 0.00s elapsed Initiating NSE at 11:26 Completed NSE at 11:26, 0.00s elapsed Initiating ARP Ping Scan at 11:26 Scanning 192.168.209.42 [1 port] Completed ARP Ping Scan at 11:26, 0.07s elapsed (1 total hosts) Initiating Parallel DNS resolution of 1 host. at 11:26 Completed Parallel DNS resolution of 1 host. at 11:26, 11.05s elapsed Initiating SYN Stealth Scan at 11:26 Scanning 192.168.209.42 [1000 ports] Discovered open port 8080/tcp on 192.168.209.42 Discovered open port 5000/tcp on 192.168.209.42 Discovered open port 9090/tcp on 192.168.209.42 Discovered open port 3000/tcp on 192.168.209.42 Discovered open port 7000/tcp on 192.168.209.42 Completed SYN Stealth Scan at 11:27, 22.72s elapsed (1000 total ports) Initiating Service scan at 11:27 Scanning 5 services on 192.168.209.42 Completed Service scan at 11:28, 87.61s elapsed (5 services on 1 host) Initiating OS detection (try #1) against 192.168.209.42 Retrying OS detection (try #2) against 192.168.209.42 Retrying OS detection (try #3) against 192.168.209.42 WARNING: RST from 192.168.209.42 port 3000 -- is this port really open? WARNING: RST from 192.168.209.42 port 3000 -- is this port really open? WARNING: RST from 192.168.209.42 port 3000 -- is this port really open? WARNING: RST from 192.168.209.42 port 3000 -- is this port really open? WARNING: RST from 192.168.209.42 port 3000 -- is this port really open? WARNING: RST from 192.168.209.42 port 3000 -- is this port really open? Retrying OS detection (try #4) against 192.168.209.42 Retrying OS detection (try #5) against 192.168.209.42 WARNING: RST from 192.168.209.42 port 3000 -- is this port really open? WARNING: RST from 192.168.209.42 port 3000 -- is this port really open? WARNING: RST from 192.168.209.42 port 3000 -- is this port really open? WARNING: RST from 192.168.209.42 port 3000 -- is this port really open? WARNING: RST from 192.168.209.42 port 3000 -- is this port really open? WARNING: RST from 192.168.209.42 port 3000 -- is this port really open? NSE: Script scanning 192.168.209.42. Initiating NSE at 11:28					
Filter Hosts							

Zenmap

Scan Tools Profile Help

Target: 192.168.209.42 Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v 192.168.209.42

Hosts	Services	Nmap Output	Ports / Hosts	Topology	Host Details	Scans	Details
OS Host		nmap -T4 -A -v 192.168.209.42					
localhost (127.0.0.1)		Initiating NSE at 11:28 Completed NSE at 11:29, 30.30s elapsed					
192.168.209.42		Initiating NSE at 11:29 Completed NSE at 11:29, 1.19s elapsed					
192.168.209.51		Initiating NSE at 11:29 Completed NSE at 11:29, 0.00s elapsed Nmap scan report for 192.168.209.42 Host is up (0.048s latency). Not shown: 995 closed tcp ports (reset) PORT STATE SERVICE VERSION 3000/tcp open ppp?					

```
fingerprint-strings:
  GenericLines, Help, Kerberos, RTSPRequest, SSLSessionReq, TLSSessionReq,
TerminalServerCookie:
  HTTP/1.1 400 Bad Request
  Content-Type: text/plain; charset=utf-8
  Connection: close
  Request
GetRequest:
  HTTP/1.0 302 Found
  Cache-Control: no-cache
  Content-Type: text/html; charset=utf-8
  Expires: -1
  Location: /login
  Pragma: no-cache
  Set-Cookie: redirect_to=%2F; Path=/; HttpOnly; SameSite=Lax
  X-Content-Type-Options: nosniff
  X-Frame-Options: deny
  X-Xss-Protection: 1; mode=block
  Date: Tue, 20 Sep 2022 04:27:18 GMT
  Content-Length: 29
  href="/login">Found</a>.
HTTPOptions:
  HTTP/1.0 302 Found
  Cache-Control: no-cache
  Expires: -1
  Location: /login
  Pragma: no-cache
  Set-Cookie: redirect_to=%2F; Path=/; HttpOnly; SameSite=Lax
  X-Content-Type-Options: nosniff
  X-Frame-Options: deny
  X-Xss-Protection: 1; mode=block
  Date: Tue, 20 Sep 2022 04:27:23 GMT
  Content-Length: 0
5000/tcp open rtsp    AirTunes rtspd 620.8.2
|_rtsp-methods: ERROR: Script execution failed (use -d to debug)
```

The screenshot shows the Zenmap interface with the following details:

- Target:** 192.168.209.42
- Profile:** Intense scan
- Command:** nmap -T4 -A -v 192.168.209.42

The main pane displays the Nmap Output for the scanned host:

```
|_irc-info: Unable to open connection
8080/tcp open http Apache httpd 2.4.52 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
| http-methods:
|_ Supported Methods: GET POST OPTIONS HEAD
| http-open-proxy: Proxy might be redirecting requests
| http-server-header: Apache/2.4.52 (Ubuntu)
9090/tcp open http Golang net/http server (Go-IPFS json-rpc or InfluxDB API)
| http-title: Prometheus Time Series Collection and Processing Server
|_Requested resource was /graph
| http-methods:
|_ Supported Methods: GET OPTIONS
|_http-favicon: Unknown favicon MD5: 5EE43B38986A144D6B5022EA8C8F748F
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port3000-TCP:V=7.93%I=7%D=9/20%Time=63294126%P=i686-pc-windows-windows%
SF:r(GenericLines,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n\x400\x20SF:ad\x20Request")%r(GetRequest,174,"HTTP/1\.0\x20302\x20Found\r\nCache-Co
SF:introl:\x20no-cache\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nE
SF:xpires:\x20-1\r\nLocation:\x20/login\r\nPragma:\x20no-cache\r\nSet-Cook
SF:ie:\x20redirect_to=%2F;\x20Path=/; \x20HttpOnly;\x20SameSite=Lax\r\nX-Co
SF:ntent-Type-Options:\x20nosniff\r\nX-Frame-Options:\x20deny\r\nX-Xss-Pro
SF:tection:\x201;\x20mode=block\r\nDate:\x20Tue,\x2020\x20Sep\x202022\x200
SF:4:27:18\x20GMT\r\nContent-Length:\x2029\r\n\r\n>Fo
SF:und</a>.\n\n"\)%r\(Helper,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n\x400\x20Bad\x20Request"\)%r\(HTTPOptions,12E,"HTTP/1\.0\x20302\x20Found\r\nCache-Control:\x20no-cache\r\nExpires:\x20-1\r\nLocation:\x20/login\r\nPragma:\x20no-cache\r\nSet-Cookie:\x20redirect\_to=%2F;\x20Path=/\x20H
SF:ttOnly;\x20SameSite=Lax\r\nX-Content-Type-Options:\x20nosniff\r\nX-Fra
SF:me-Options:\x20deny\r\nX-Xss-Protection:\x201;\x20mode=block\r\nDate:\x20Tue,\x2020\x20Sep\x202022\x2004:27:23\x20GMT\r\nContent-Length:\x200\r\n"\)%r\(HTTSPRequest,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n\x400\x20Bad\x20Request"\)%r\(SSLSessionReq,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n\x400\x20Bad\x20Request"\)%r\(TerminalServerCookie,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n\x400\x20Bad\x20Request"\)%r\(TLS
SF:SessionReq,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n\x400\x20Bad\x20Request"\)%r\(Kerberos,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n\x400\x20Bad\x20Request"\):
```

Hosts **Services** **Nmap Output** **Ports / Hosts** **Topology** **Host Details** **Scans**

OS | **Host**

- localhost (127.0.0.1)
- 192.168.209.42
- 192.168.209.51

```
nmap -T4 -A -v 192.168.209.42
SF:int-type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n
SF:n400\x20Bad\x20Request")%r(SSLSessionReq,67,"HTTP/1\.1\x20400\x20Bad\x20
SF:0Request\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\nConnection
SF:;\x20close\r\n\r\nn400\x20Bad\x20Request")%r(TerminalServerCookie,67,"HT
SF:TP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain;\x20cha
SF:rset=utf-8\r\nConnection:\x20close\r\n\r\nn400\x20Bad\x20Request")%r(TLS
SF:SessionReq,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20t
SF:ext/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\nn400\x20Bad\x20
SF:20Request")%r(Kerberos,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConten
SF:t-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\nn
SF:400\x20Bad\x20Request");
MAC Address: D0:88:0C:86:11:2F (Apple)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).
TCP/IP fingerprint:
OS:SCAN(V=7.93E=4%D=9/20%OT=3000%CT=1%CU=44054%PV=Y%DS=1%DC=D%G=Y%MI=D0880C
OS:%TM=632941A3%P=i686-pc-windows-windows)SEQ(SP=104%GCD=1%ISR=10A%TI=Z%CI=
OS:RD%II=RI%TS=21)SEQ(CI=RD)SEQ(SP=104%GCD=1%ISR=10A%TI=Z%CI=RD%TS=21)SEQ(C
OS:I=RD%II=RI)OPS(O1=M5B4NW6NNT11SLL%O2=M5B4NW6NNT11SLL%O3=M5B4NW6NNT11%O4=
OS:M5B4NW6NNT11SLL%O5=M5B4NW6NNT11SLL%O6=M5B4NNT11SLL)WIN(W1=FFFF%W2=FFFF%W
OS:3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)ECN(R=Y%DF=Y%T=40%W=FFFF%O=M5B4NW6SLL%CC=
OS:N%Q=)T1(R=Y%DF=Y%T=40%W=0%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=
OS:40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=N%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0
OS:%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=N%T=40%W=0%S=Z
OS:%A=S%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=38%UN=0%RIPL=G%RID=G%RIPCK=G%R
OS:UCK=0%RUD=G)IE(R=Y%DFI=S%T=40%CD=S)

Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1  47.91 ms  192.168.209.42

NSE: Script Post-scanning.
Initiating NSE at 11:29
Completed NSE at 11:29, 0.00s elapsed
Initiating NSE at 11:29
Completed NSE at 11:29, 0.00s elapsed
Initiating NSE at 11:29
Completed NSE at 11:29, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 166.60 seconds
Raw packets sent: 1125 (54.632KB) | Rcvd: 1488 (63.635KB)
```

Attacking target VM

Zenmap

Scan Tools Profile Help

Target: 192.168.209.51 Profile: Intense scan plus UDP Scan Cancel

Command: nmap -sS -sU -T4 -A -v 192.168.209.51

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

nmap -T4 -A -v 192.168.209.51

```

Starting Nmap 7.93 ( https://nmap.org ) at 2022-09-20 11:12 SE Asia Standard Time
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 11:12
Completed NSE at 11:12, 0.00s elapsed
Initiating NSE at 11:12
Completed NSE at 11:12, 0.00s elapsed
Initiating NSE at 11:12
Completed NSE at 11:12, 0.00s elapsed
Initiating NSE at 11:12
Completed NSE at 11:12, 0.00s elapsed
Initiating ARP Ping Scan at 11:12
Scanning 192.168.209.51 [1 port]
Completed ARP Ping Scan at 11:12, 1.43s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:12
Completed Parallel DNS resolution of 1 host. at 11:12, 11.04s elapsed
Initiating SYN Stealth Scan at 11:12
Scanning 192.168.209.51 [1000 ports]
Discovered open port 80/tcp on 192.168.209.51
Discovered open port 22/tcp on 192.168.209.51
Completed SYN Stealth Scan at 11:13, 46.68s elapsed (1000 total ports)
Initiating Service scan at 11:13
Scanning 2 services on 192.168.209.51
Completed Service scan at 11:13, 6.31s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 192.168.209.51
Retrying OS detection (try #2) against 192.168.209.51
Retrying OS detection (try #3) against 192.168.209.51
Retrying OS detection (try #4) against 192.168.209.51
Retrying OS detection (try #5) against 192.168.209.51
NSE: Script scanning 192.168.209.51.
Initiating NSE at 11:13
Completed NSE at 11:13, 5.07s elapsed
Initiating NSE at 11:13
Completed NSE at 11:13, 0.22s elapsed
Initiating NSE at 11:13
Completed NSE at 11:13, 0.00s elapsed
Nmap scan report for 192.168.209.51
Host is up (0.030s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 f484fac54ec47591525d0a32b478282a (ECDSA)
|   256 749556d7cf28c8ff60f379f96ca9c708 (ED25519)
80/tcp    open  http   Apache httpd 2.4.52 ((Ubuntu))
| http-title: Apache2 Ubuntu Default Page: It works

```

Filter Hosts

Zenmap

Scan Tools Profile Help

Target: 192.168.209.51 Profile: Intense scan plus UDP Scan Cancel

Command: nmap -sS -sU -T4 -A -v 192.168.209.51

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

nmap -T4 -A -v 192.168.209.51

```

Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 f484fac54ec47591525d0a32b478282a (ECDSA)
|   256 749556d7cf28c8ff60f379f96ca9c708 (ED25519)
80/tcp    open  http   Apache httpd 2.4.52 ((Ubuntu))
| http-title: Apache2 Ubuntu Default Page: It works
| http-methods:
|   Supported Methods: HEAD GET POST OPTIONS

```

```

!_ supported methods: HEAD GET POST OPTIONS
!_ http-server-header: Apache/2.4.52 (Ubuntu)
MAC Address: D0:88:0C:86:11:2F (Apple)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=9/20%OT=22%CT=1%CU=44144%PV=Y%DS=1%DC=D%G=Y%M=D0880C%T
OS:M=63293DEC%P=i686-pc-windows-windows)SEQ(SP=106%GCD=1%ISR=108%TI=Z%CI=Z%
OS:II=I%TS=B)SEQ(CI=Z%II=I)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNNT11NW
OS:7%O4=M5B4ST11NW7%O5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%
OS:W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNNSNW7%CC=Y%Q=)T1
OS:(R=Y%DF=Y%T=40%S=0%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%
OS:S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(
OS:R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F
OS:=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G
OS:%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1  30.10 ms  192.168.209.51

NSE: Script Post-scanning.
Initiating NSE at 11:13
Completed NSE at 11:13, 0.00s elapsed
Initiating NSE at 11:13
Completed NSE at 11:13, 0.00s elapsed
Initiating NSE at 11:13
Completed NSE at 11:13, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 87.52 seconds
Raw packets sent: 1114 (53.066KB) | Rcvd: 1107 (48.022KB)

```

[Filter Hosts](#)

1. Notice the open ports on all 3 devices (the attacker notebook, the target notebook, and the target Linux VM). Does anything look suspicious, i.e., some ports that you are not aware of that are open on the VM or on your notebooks?

- Attacker notebook (localhost) : Ports 135, 3306, 445, 8089, and 8000 are open. Port 135 is Microsoft Windows RPC, 445 is also Microsoft Windows', but port 3306 was MySQL and port 8000 was Splunk which was open unknowingly.
- Target notebook : Ports 3000, 5000, 7000, 8080, and 9090 are open. 8080 is Apache and 9090 is Golang http server.
- Target VM : Ports 22 and 80 are open. 22 is OpenSSH Ubuntu 3 amd 80 is Apache.

2. Look at the information provided by nmap about your OS's on all 3 devices. Is the information correct? Why is it or why is it not correct?

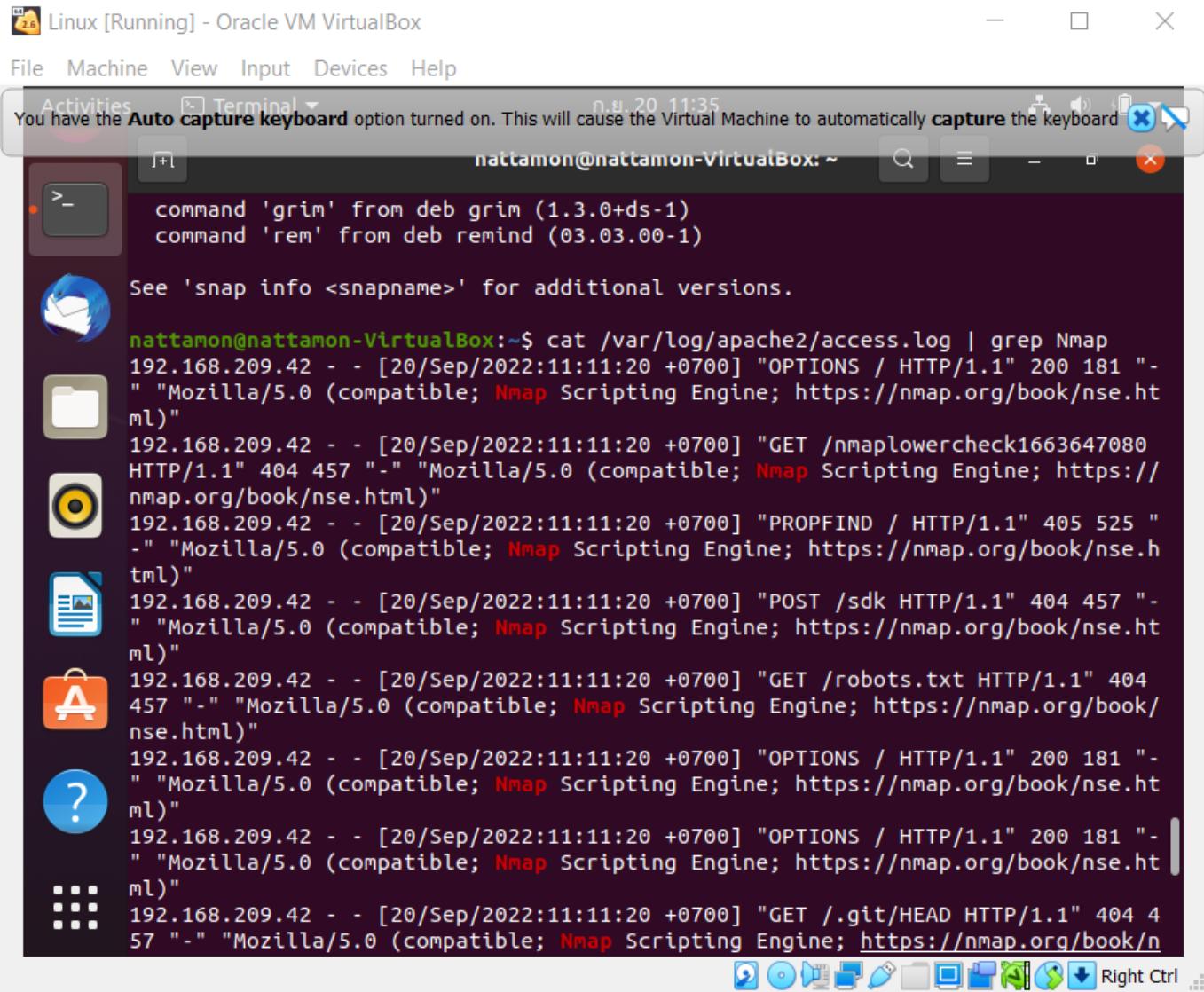
The information is correct for Windows but not for MacOS and Linux where the OS was unable to be detected. However, the MAC address was identified as Apple.

3. What do you think about the information you can get using nmap? Scary?

You can get a *lot* of information from nmap, including

- open ports
- what those ports are, the versions, protocols and such
- supported capabilities or http options
- the device type, OS, and network distance of the host The information is certainly useful for malicious purposes.

4. Look at the access.log file for the web server in your Linux VM. What IP addresses do you see accessing the web server? Which devices do these IP addresses belong to?



```
Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal 20 11:35
You have the Auto capture keyboard option turned on. This will cause the Virtual Machine to automatically capture the keyboard
nattamon@nattamon-VirtualBox: ~
command 'grim' from deb grim (1.3.0+ds-1)
command 'rem' from deb remind (03.03.00-1)

See 'snap info <snapname>' for additional versions.

nattamon@nattamon-VirtualBox:~$ cat /var/log/apache2/access.log | grep Nmap
192.168.209.42 - - [20/Sep/2022:11:11:20 +0700] "OPTIONS / HTTP/1.1" 200 181 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.209.42 - - [20/Sep/2022:11:11:20 +0700] "GET /nmaplowercheck1663647080
HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.209.42 - - [20/Sep/2022:11:11:20 +0700] "PROPFIND / HTTP/1.1" 405 525 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.209.42 - - [20/Sep/2022:11:11:20 +0700] "POST /sdk HTTP/1.1" 404 457 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.209.42 - - [20/Sep/2022:11:11:20 +0700] "GET /robots.txt HTTP/1.1" 404
457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.209.42 - - [20/Sep/2022:11:11:20 +0700] "OPTIONS / HTTP/1.1" 200 181 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.209.42 - - [20/Sep/2022:11:11:20 +0700] "OPTIONS / HTTP/1.1" 200 181 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.209.42 - - [20/Sep/2022:11:11:20 +0700] "GET /.git/HEAD HTTP/1.1" 404 4
57 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
```

The IP address is 192.168.209.42, which is the IP address of the target notebook (which was also attacking this VM).

5. Find the nmap scan in the web server log. Copy the lines from the log file that were created because of the nmap scan.

Linux [Running] - Oracle VM VirtualBox

Activities Terminal n.b. 20 12:04 nattamon@nattamon-VirtualBox: ~

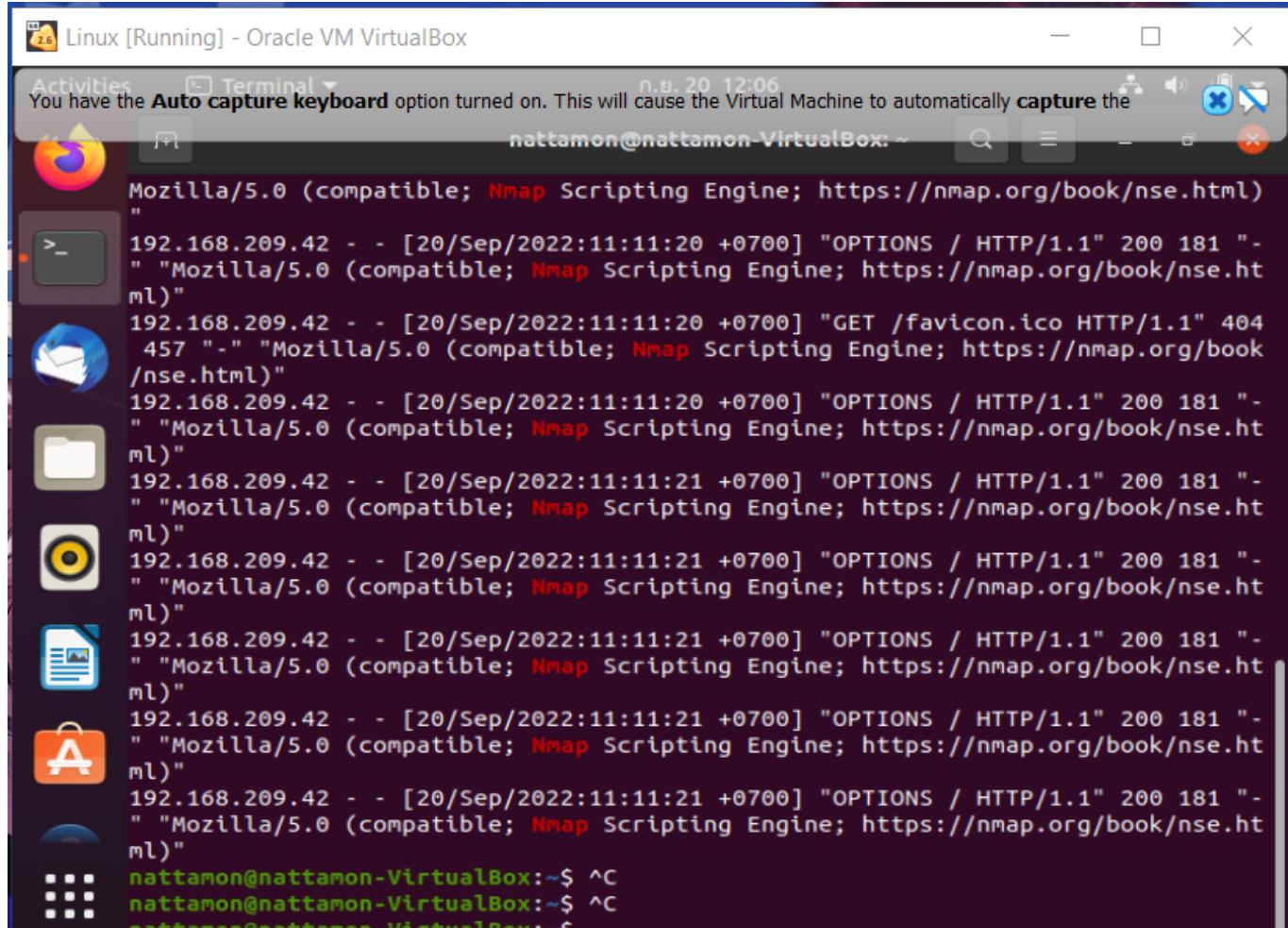
```
nattamon@nattamon-VirtualBox:~$ cat /var/log/apache2/access.log | grep Ncat
nattamon@nattamon-VirtualBox:~$ cat /var/log/apache2/access.log | grep Nmap
192.168.209.42 - - [20/Sep/2022:11:11:20 +0700] "OPTIONS / HTTP/1.1" 200 181 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.209.42 - - [20/Sep/2022:11:11:20 +0700] "GET /nmaplowercheck1663647080
HTTP/1.1" 404 457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.209.42 - - [20/Sep/2022:11:11:20 +0700] "PROPFIND / HTTP/1.1" 405 525 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.209.42 - - [20/Sep/2022:11:11:20 +0700] "POST /sdk HTTP/1.1" 404 457 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.209.42 - - [20/Sep/2022:11:11:20 +0700] "GET /robots.txt HTTP/1.1" 404
457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.209.42 - - [20/Sep/2022:11:11:20 +0700] "OPTIONS / HTTP/1.1" 200 181 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.209.42 - - [20/Sep/2022:11:11:20 +0700] "OPTIONS / HTTP/1.1" 200 181 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.209.42 - - [20/Sep/2022:11:11:20 +0700] "GET /.git/HEAD HTTP/1.1" 404 4
57 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.209.42 - - [20/Sep/2022:11:11:20 +0700] "PROPFIND / HTTP/1.1" 405 525 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
```

Linux [Running] - Oracle VM VirtualBox

Activities Terminal n.b. 20 12:05 nattamon@nattamon-VirtualBox: ~

```
Firefox Web Browser nattamon@nattamon-VirtualBox: ~
```

```
-"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.209.42 - - [20/Sep/2022:11:11:20 +0700] "POST / HTTP/1.1" 200 11192 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.209.42 - - [20/Sep/2022:11:11:20 +0700] "GET / HTTP/1.1" 200 11192 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.209.42 - - [20/Sep/2022:11:11:20 +0700] "PROPFIND / HTTP/1.1" 405 525 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.209.42 - - [20/Sep/2022:11:11:20 +0700] "OPTIONS / HTTP/1.1" 200 181 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.209.42 - - [20/Sep/2022:11:11:20 +0700] "GET /HNAP1 HTTP/1.1" 404 457 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.209.42 - - [20/Sep/2022:11:11:20 +0700] "GET /evox/about HTTP/1.1" 404
457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.209.42 - - [20/Sep/2022:11:11:20 +0700] "VKUU / HTTP/1.1" 501 501 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.209.42 - - [20/Sep/2022:11:11:20 +0700] "OPTIONS / HTTP/1.1" 200 181 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.209.42 - - [20/Sep/2022:11:11:20 +0700] "GET /favicon.ico HTTP/1.1" 404
457 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
```



The screenshot shows a Linux desktop environment running in Oracle VM VirtualBox. The terminal window displays the following nmap scan output:

```
 Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
"
192.168.209.42 - - [20/Sep/2022:11:11:20 +0700] "OPTIONS / HTTP/1.1" 200 181 "-"
" Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.209.42 - - [20/Sep/2022:11:11:20 +0700] "GET /favicon.ico HTTP/1.1" 404
457 "-" Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.209.42 - - [20/Sep/2022:11:11:20 +0700] "OPTIONS / HTTP/1.1" 200 181 "-"
" Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.209.42 - - [20/Sep/2022:11:11:21 +0700] "OPTIONS / HTTP/1.1" 200 181 "-"
" Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.209.42 - - [20/Sep/2022:11:11:21 +0700] "OPTIONS / HTTP/1.1" 200 181 "-"
" Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.209.42 - - [20/Sep/2022:11:11:21 +0700] "OPTIONS / HTTP/1.1" 200 181 "-"
" Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.209.42 - - [20/Sep/2022:11:11:21 +0700] "OPTIONS / HTTP/1.1" 200 181 "-"
" Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.209.42 - - [20/Sep/2022:11:11:21 +0700] "OPTIONS / HTTP/1.1" 200 181 "-"
" Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
nattamon@nattamon-VirtualBox:~$ ^C
nattamon@nattamon-VirtualBox:~$ ^C
nattamon@nattamon-VirtualBox:~$
```

Q6. After you successfully install your iptable rule(s), how do the reported results from your new nmap scan compare to your previous scan before using iptables? Look to see if OS detection, port open results, etc. have changed. Something(s) have definitely changed.

Zenmap

Scan Tools Profile Help

Target: 192.168.209.51 Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v 192.168.209.51

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host 192.168.209.51

```
nmap -T4 -A -v 192.168.209.51
Starting Nmap 7.93 ( https://nmap.org ) at 2022-09-20 12:00 SE Asia Standard Time
N SOCK ERROR [0.6250s] ssl_init_helper(): OpenSSL legacy provider failed to load.

NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 12:00
Completed NSE at 12:00, 0.00s elapsed
Initiating NSE at 12:00
Completed NSE at 12:00, 0.00s elapsed
Initiating NSE at 12:00
Completed NSE at 12:00, 0.00s elapsed
Initiating ARP Ping Scan at 12:00
Scanning 192.168.209.51 [1 port]
Completed ARP Ping Scan at 12:00, 0.23s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:00
Completed Parallel DNS resolution of 1 host. at 12:01, 11.07s elapsed
Initiating SYN Stealth Scan at 12:01
Scanning 192.168.209.51 [1000 ports]
Discovered open port 80/tcp on 192.168.209.51
Completed SYN Stealth Scan at 12:01, 20.00s elapsed (1000 total ports)
Initiating Service scan at 12:01
Scanning 1 service on 192.168.209.51
Completed Service scan at 12:01, 6.06s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against 192.168.209.51
NSE: Script scanning 192.168.209.51.
Initiating NSE at 12:01
Completed NSE at 12:01, 5.04s elapsed
Initiating NSE at 12:01
Completed NSE at 12:01, 0.10s elapsed
Initiating NSE at 12:01
Completed NSE at 12:01, 0.00s elapsed
Nmap scan report for 192.168.209.51
Host is up (0.092s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.52 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-methods:
|_ Supported Methods: HEAD GET POST OPTIONS
|_http-server-header: Apache/2.4.52 (Ubuntu)
MAC Address: D0:88:0C:86:11:2F (Apple)
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux kernel:4 cpe:/o:linux:linux kernel:5
```

Filter Hosts

Zenmap

Scan Tools Profile Help

Target: 192.168.209.51 Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v 192.168.209.51

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host 192.168.209.51

```
nmap -T4 -A -v 192.168.209.51
Initiating OS detection (try #1) against 192.168.209.51
NSE: Script scanning 192.168.209.51.
Initiating NSE at 12:01
Completed NSE at 12:01, 5.04s elapsed
Initiating NSE at 12:01
Completed NSE at 12:01, 0.10s elapsed
Initiating NSE at 12:01
Completed NSE at 12:01, 0.00s elapsed
Nmap scan report for 192.168.209.51
Host is up (0.092s latency).
Not shown: 999 filtered tcp ports (no-response)
```

```

PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.52 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
| http-methods:
|_ Supported Methods: HEAD GET POST OPTIONS
|_http-server-header: Apache/2.4.52 (Ubuntu)
MAC Address: D0:88:0C:86:11:2F (Apple)
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Uptime guess: 15.703 days (since Sun Sep 4 19:09:34 2022)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=256 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE
HOP RTT      ADDRESS
1  92.28 ms 192.168.209.51

NSE: Script Post-scanning.
Initiating NSE at 12:01
Completed NSE at 12:01, 0.00s elapsed
Initiating NSE at 12:01
Completed NSE at 12:01, 0.00s elapsed
Initiating NSE at 12:01
Completed NSE at 12:01, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 49.98 seconds
Raw packets sent: 2053 (92.836KB) | Rcvd: 72 (5.525KB)

```

Filter Hosts

Only port 80 (Apache) is open, and the OS is now correctly detected as Linux.

Q7. Notice that nmap can still figure out you have Apache httpd running. Look at the access.log file for the web server in your Linux VM. Are the logs the same as in Part II?

There are more logs after the firewall is up.

```

192.168.209.70 - - [20/Sep/2022:05:01:38 +0000] "GET /nmaplowercheck1663650099
HTTP/1.1" 404 456 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine;
https://nmap.org/book/nse.html)"
192.168.209.70 - - [20/Sep/2022:05:01:38 +0000] "POST / HTTP/1.1" 200 10945 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.209.70 - - [20/Sep/2022:05:01:38 +0000] "GET / HTTP/1.1" 200 10945 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.209.70 - - [20/Sep/2022:05:01:38 +0000] "OPTIONS / HTTP/1.1" 200 181 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.209.70 - - [20/Sep/2022:05:01:38 +0000] "GET /robots.txt HTTP/1.1" 404 456
"-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine;
https://nmap.org/book/nse.html)"
192.168.209.70 - - [20/Sep/2022:05:01:38 +0000] "OPTIONS / HTTP/1.1" 200 181 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.209.70 - - [20/Sep/2022:05:01:38 +0000] "OPTIONS / HTTP/1.1" 200 181 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.209.70 - - [20/Sep/2022:05:01:38 +0000] "POST /sdk HTTP/1.1" 404 456 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.209.70 - - [20/Sep/2022:05:01:38 +0000] "GET /.git/HEAD HTTP/1.1" 404 456
"-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine;
https://nmap.org/book/nse.html)"
192.168.209.70 - - [20/Sep/2022:05:01:38 +0000] "PROPFIND / HTTP/1.1" 405 524 "-"

```

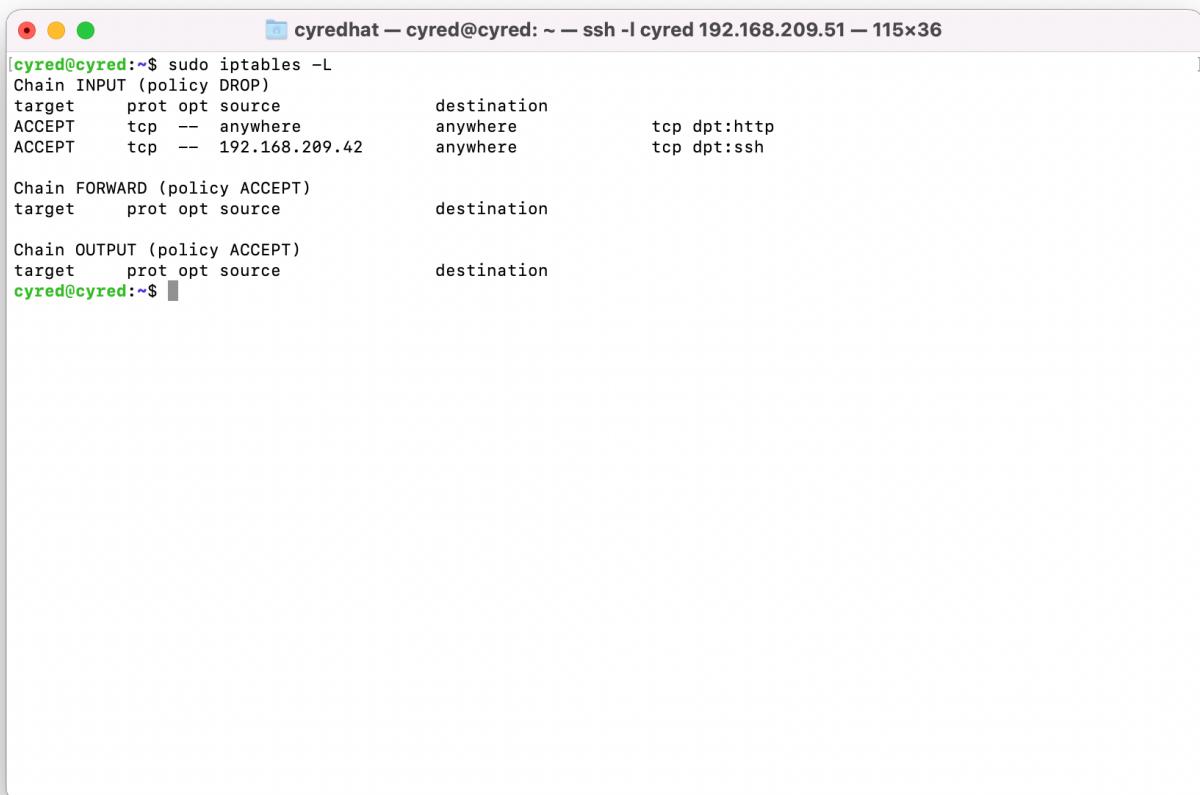
```
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"  
192.168.209.70 - - [20/Sep/2022:05:01:38 +0000] "PROPFIND / HTTP/1.1" 405 524 "-"  
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"  
192.168.209.70 - - [20/Sep/2022:05:01:38 +0000] "GET /HNAP1 HTTP/1.1" 404 456 "-"  
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"  
192.168.209.70 - - [20/Sep/2022:05:01:38 +0000] "OPTIONS / HTTP/1.1" 200 181 "-"  
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"  
192.168.209.70 - - [20/Sep/2022:05:01:38 +0000] "GET /evox/about HTTP/1.1" 404 456  
"-" "Mozilla/5.0 (compatible; Nmap Scripting Engine;  
https://nmap.org/book/nse.html)"  
192.168.209.70 - - [20/Sep/2022:05:01:38 +0000] "PROPFIND / HTTP/1.1" 405 524 "-"  
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"  
192.168.209.70 - - [20/Sep/2022:05:01:38 +0000] "SWOK / HTTP/1.1" 501 499 "-"  
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"  
192.168.209.70 - - [20/Sep/2022:05:01:38 +0000] "OPTIONS / HTTP/1.1" 200 181 "-"  
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"  
192.168.209.70 - - [20/Sep/2022:05:01:38 +0000] "GET / HTTP/1.1" 200 10945 "-"  
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"  
192.168.209.70 - - [20/Sep/2022:05:01:39 +0000] "OPTIONS / HTTP/1.1" 200 181 "-"  
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"  
192.168.209.70 - - [20/Sep/2022:05:01:39 +0000] "OPTIONS / HTTP/1.1" 200 181 "-"  
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"  
192.168.209.70 - - [20/Sep/2022:05:01:39 +0000] "GET /favicon.ico HTTP/1.1" 404  
456 "—" "Mozilla/5.0 (compatible; Nmap Scripting Engine;  
https://nmap.org/book/nse.html)"  
192.168.209.70 - - [20/Sep/2022:05:01:39 +0000] "OPTIONS / HTTP/1.1" 200 181 "-"  
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"  
192.168.209.70 - - [20/Sep/2022:05:01:39 +0000] "OPTIONS / HTTP/1.1" 200 181 "-"  
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"  
192.168.209.70 - - [20/Sep/2022:05:01:39 +0000] "OPTIONS / HTTP/1.1" 200 181 "-"  
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"  
192.168.209.70 - - [20/Sep/2022:05:01:39 +0000] "OPTIONS / HTTP/1.1" 200 181 "-"  
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"  
192.168.209.70 - - [20/Sep/2022:05:01:39 +0000] "GET /nmaplowercheck1663650099  
HTTP/1.1" 404 456 "—" "Mozilla/5.0 (compatible; Nmap Scripting Engine;  
https://nmap.org/book/nse.html)"  
192.168.209.42 - - [20/Sep/2022:05:01:39 +0000] "GET /.git/HEAD HTTP/1.1" 404 456  
"—" "Mozilla/5.0 (compatible; Nmap Scripting Engine;  
https://nmap.org/book/nse.html)"  
192.168.209.42 - - [20/Sep/2022:05:01:39 +0000] "POST /sdk HTTP/1.1" 404 456 "-"  
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"  
192.168.209.42 - - [20/Sep/2022:05:01:39 +0000] "OPTIONS / HTTP/1.1" 200 181 "-"  
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"  
192.168.209.42 - - [20/Sep/2022:05:01:39 +0000] "GET /robots.txt HTTP/1.1" 404 456  
"—" "Mozilla/5.0 (compatible; Nmap Scripting Engine;  
https://nmap.org/book/nse.html)"  
192.168.209.42 - - [20/Sep/2022:05:01:39 +0000] "GET / HTTP/1.1" 200 10945 "-"  
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"  
192.168.209.42 - - [20/Sep/2022:05:01:39 +0000] "PROPFIND / HTTP/1.1" 405 524 "-"  
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
```

```
192.168.209.42 - - [20/Sep/2022:05:01:39 +0000] "POST / HTTP/1.1" 200 10945 "-"
Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
```

Q8. Explain whether or not you could prevent nmap from reaching the web server while still allowing legitimate clients to get service. Will a firewall be sufficient for this? Or do you need some other device? Please think critically about this.

A firewall would be sufficient to prevent nmap from reaching the server, because we can add rules that reject specific IP addresses or packet statuses.

Q9. What are your firewall rules? Run iptables -L on your VM and enter the output here.



```
cyred@cyred:~$ sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source          destination
ACCEPT    tcp  --  anywhere        anywhere          tcp dpt:http
ACCEPT    tcp  --  192.168.209.42  anywhere          tcp dpt:ssh

Chain FORWARD (policy ACCEPT)
target     prot opt source          destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source          destination
cyred@cyred:~$
```