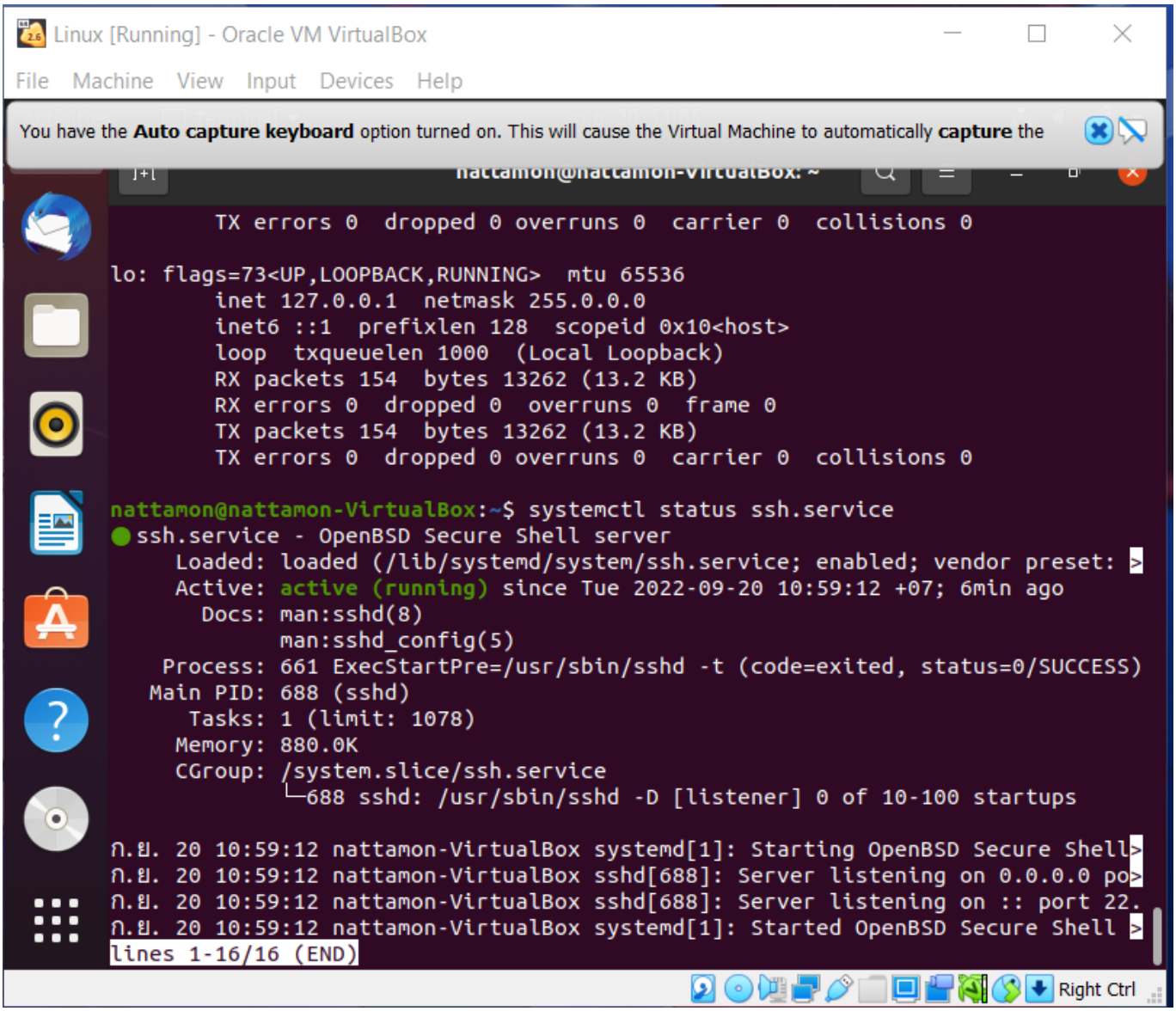
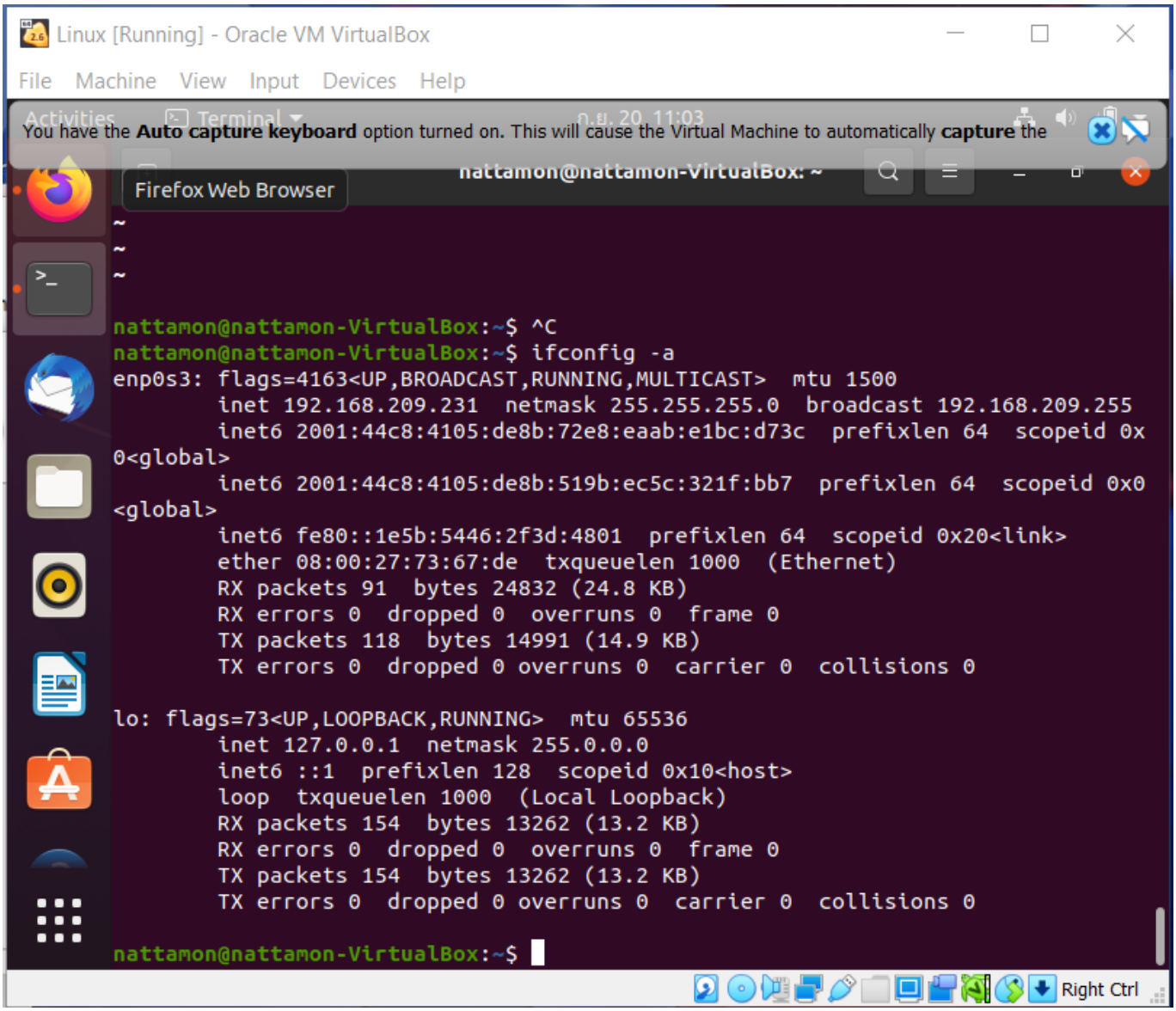
Activity 7 - Recon and Defense (Network Security I)

Part 1: Preparation

1. Check ssh service status

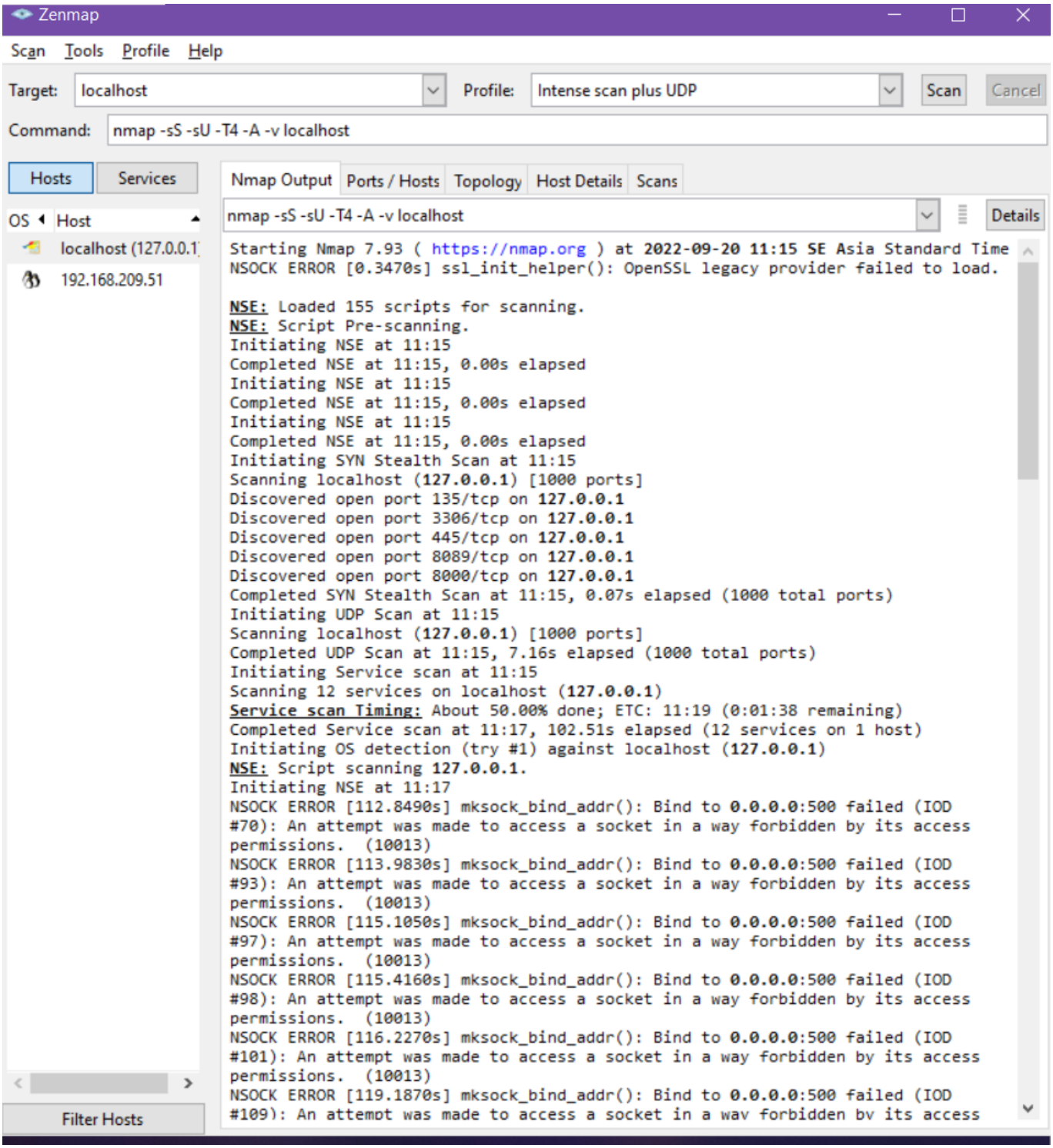


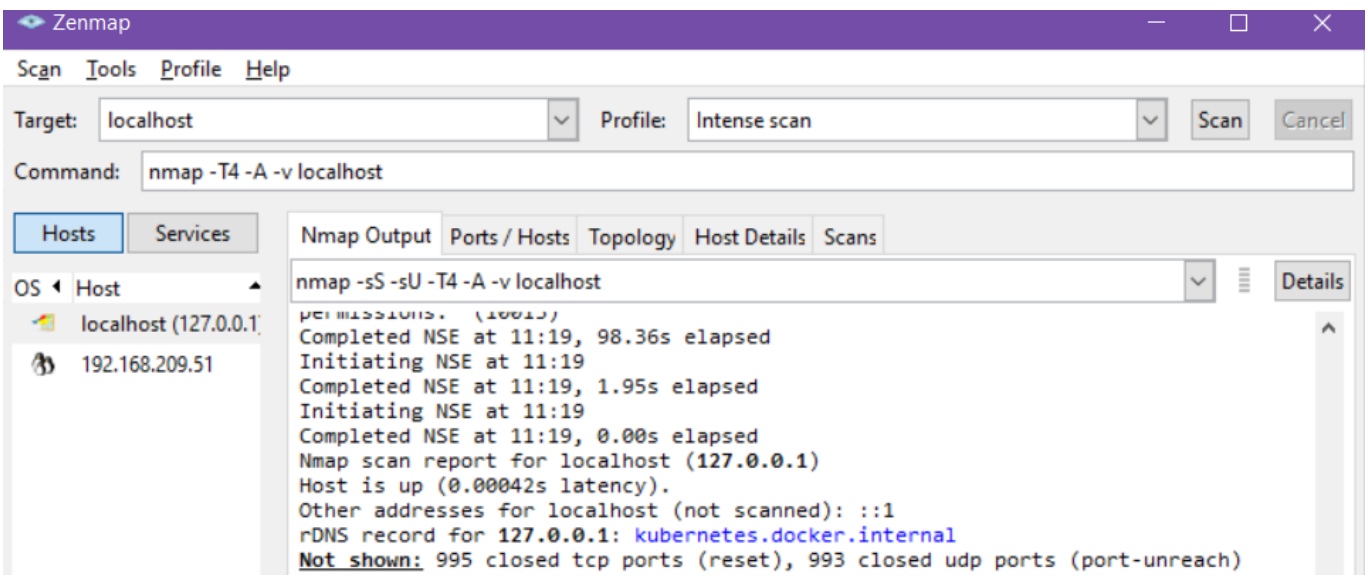
2. Check VM's IP address

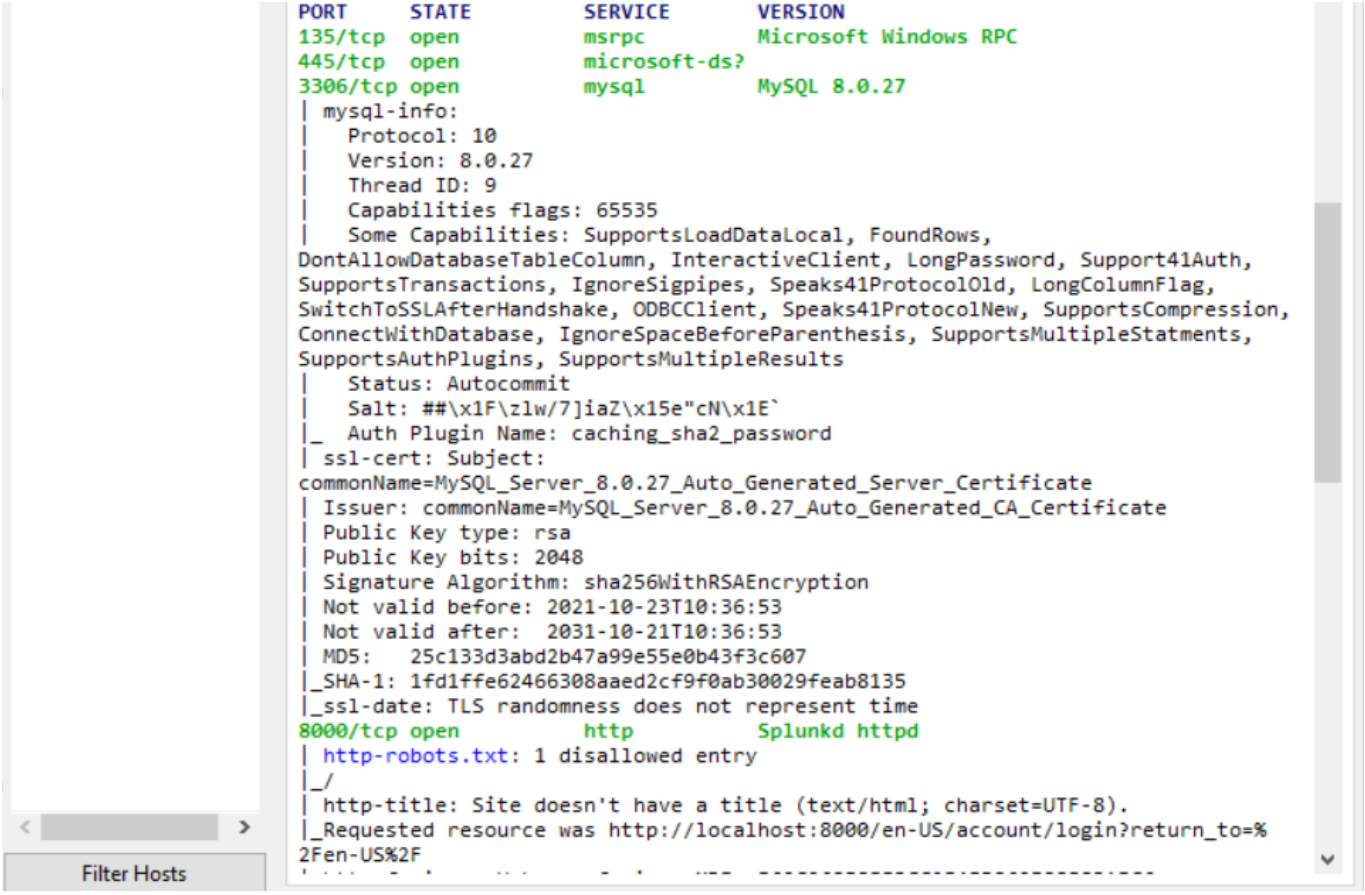


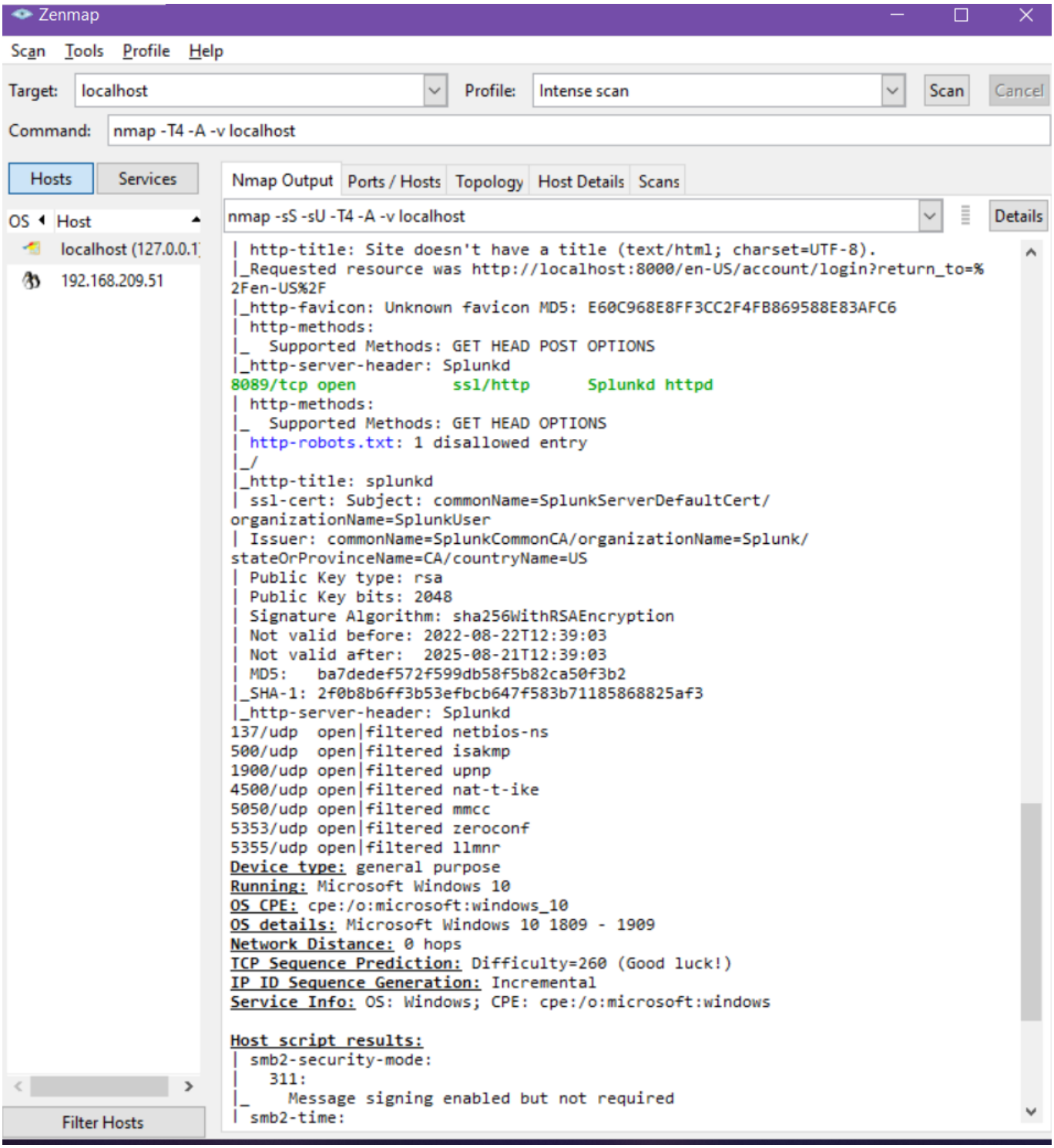
Part 2: Reconnaissance

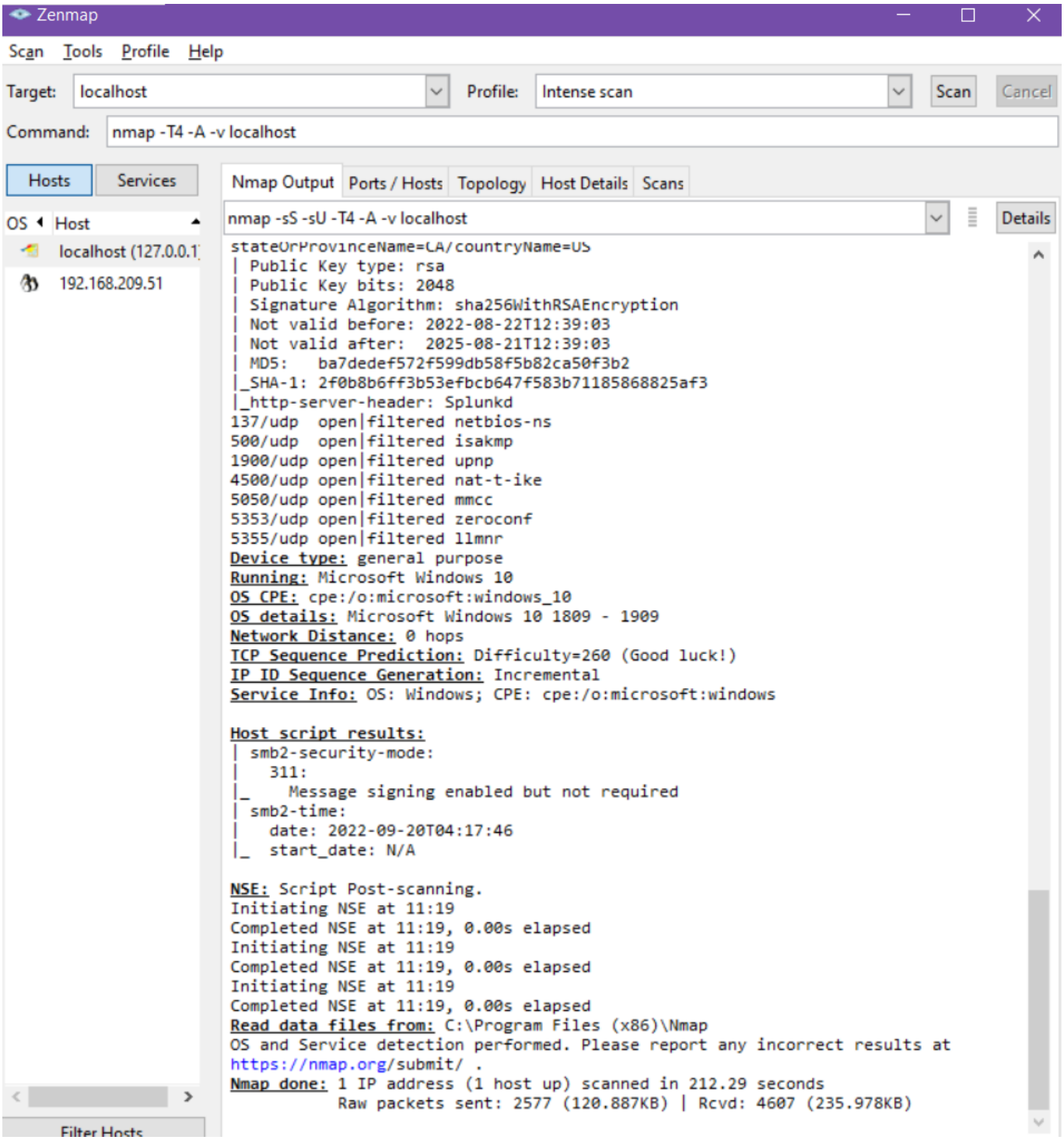
Attacking localhost


Zenmap
Scan Tools Profile Help
Target: localhost
Profile: Intense scan plus UDP
Scan
Cancel
Command: nmap -sS -sU -T4 -A -v localhost
Hosts
Services
OS Host
localhost (127.0.0.1)
192.168.209.51
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -sS -sU -T4 -A -v localhost
Details
Starting Nmap 7.93 (https://nmap.org) at 2022-09-20 11:15 SE Asia Standard Time
NSOCK ERROR [0.3470s] ssl_init_helper(): OpenSSL legacy provider failed to load.
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
NSOCK 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)
NSOCK 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)
NSOCK 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)
NSOCK 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)
NSOCK 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)
NSOCK 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

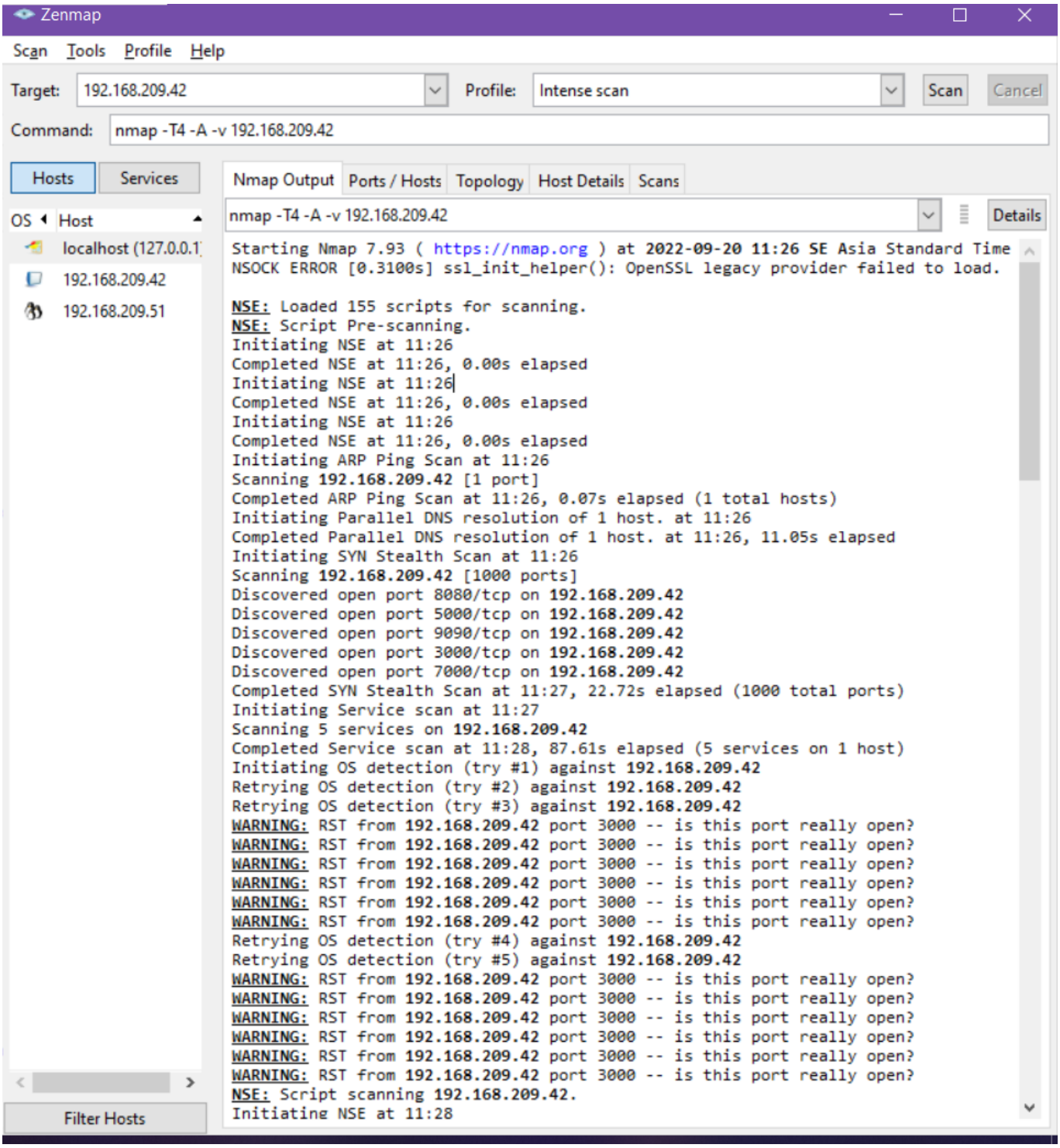

Zenmap
Scan Tools Profile Help
Target: localhost
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v localhost
Hosts
Services
OS Host
localhost (127.0.0.1)
192.168.209.51
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -sS -sU -T4 -A -v localhost
Details
Completed NSE at 11:19, 98.36s 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)

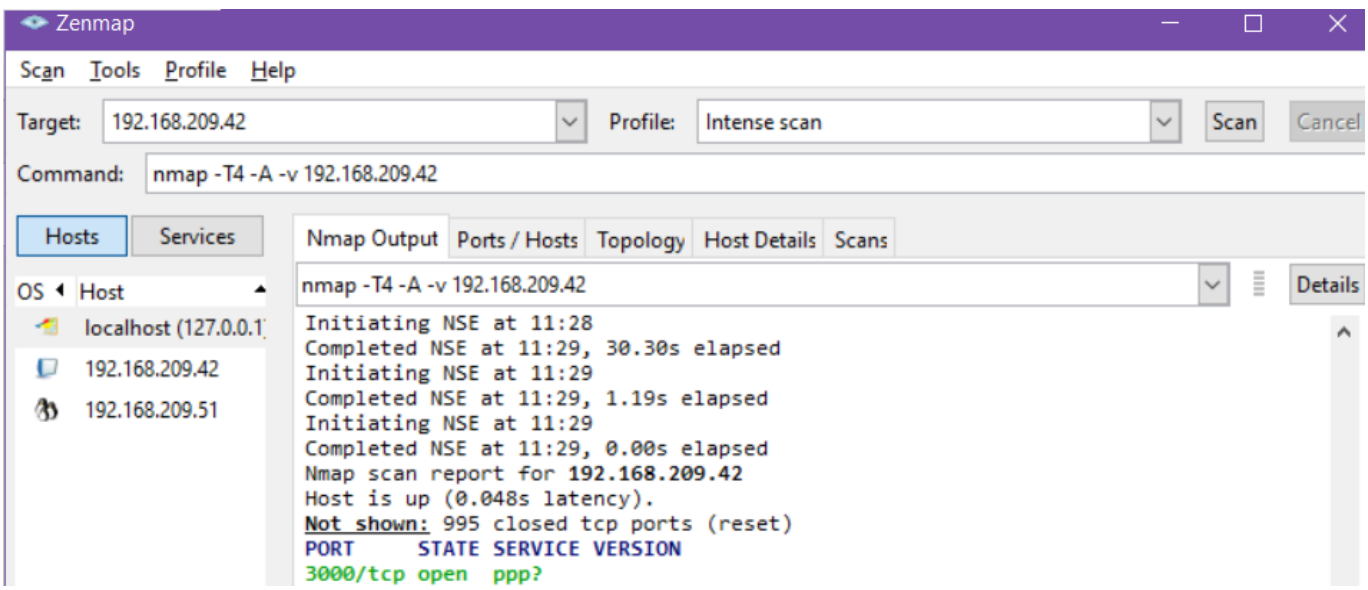

Filter Hosts
PORT STATE SERVICE VERSION
135/tcp open msrpc Microsoft Windows RPC
445/tcp open microsoft-ds?
3306/tcp open mysql MySQL 8.0.27
| mysql-info:
| Protocol: 10
| Version: 8.0.27
| Thread ID: 9
| Capabilities flags: 65535
| Some Capabilities: SupportsLoadDataLocal, FoundRows,
DontAllowDatabaseTableColumn, InteractiveClient, LongPassword, Support41Auth,
SupportsTransactions, IgnoreSigpipes, Speaks41ProtocolOld, LongColumnFlag,
SwitchToSSLAfterHandshake, ODBCClient, Speaks41ProtocolNew, SupportsCompression,
ConnectWithDatabase, IgnoreSpaceBeforeParenthesis, SupportsMultipleStatments,
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: 1fd1ffe62466308aaed2cf9f0ab30029feab8135
|_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

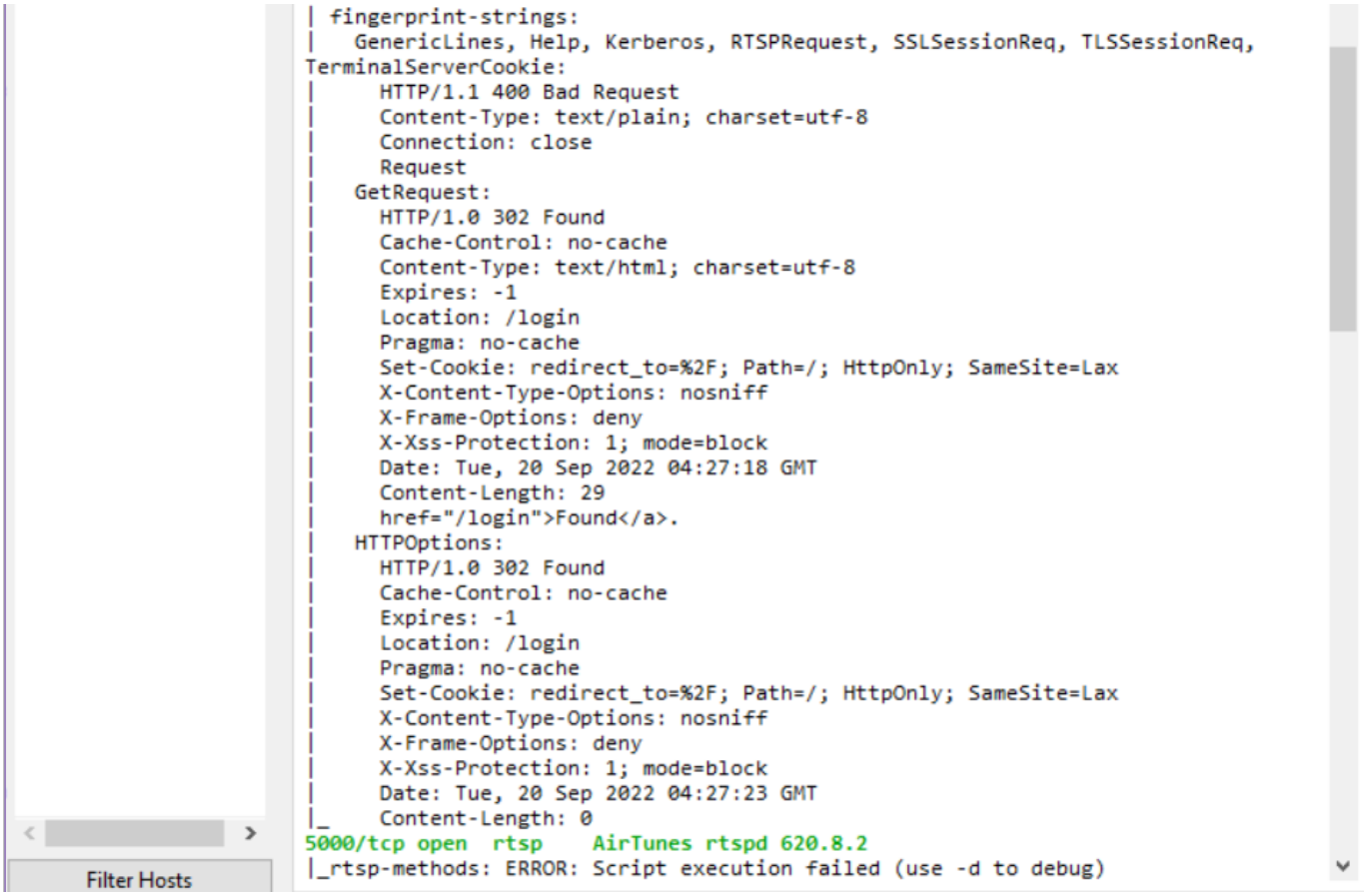

Zenmap
Scan Tools Profile Help
Target: localhost
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v localhost
Hosts
Services
OS Host
localhost (127.0.0.1)
192.168.209.51
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -sS -sU -T4 -A -v localhost
Details
| http-title: Site 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:

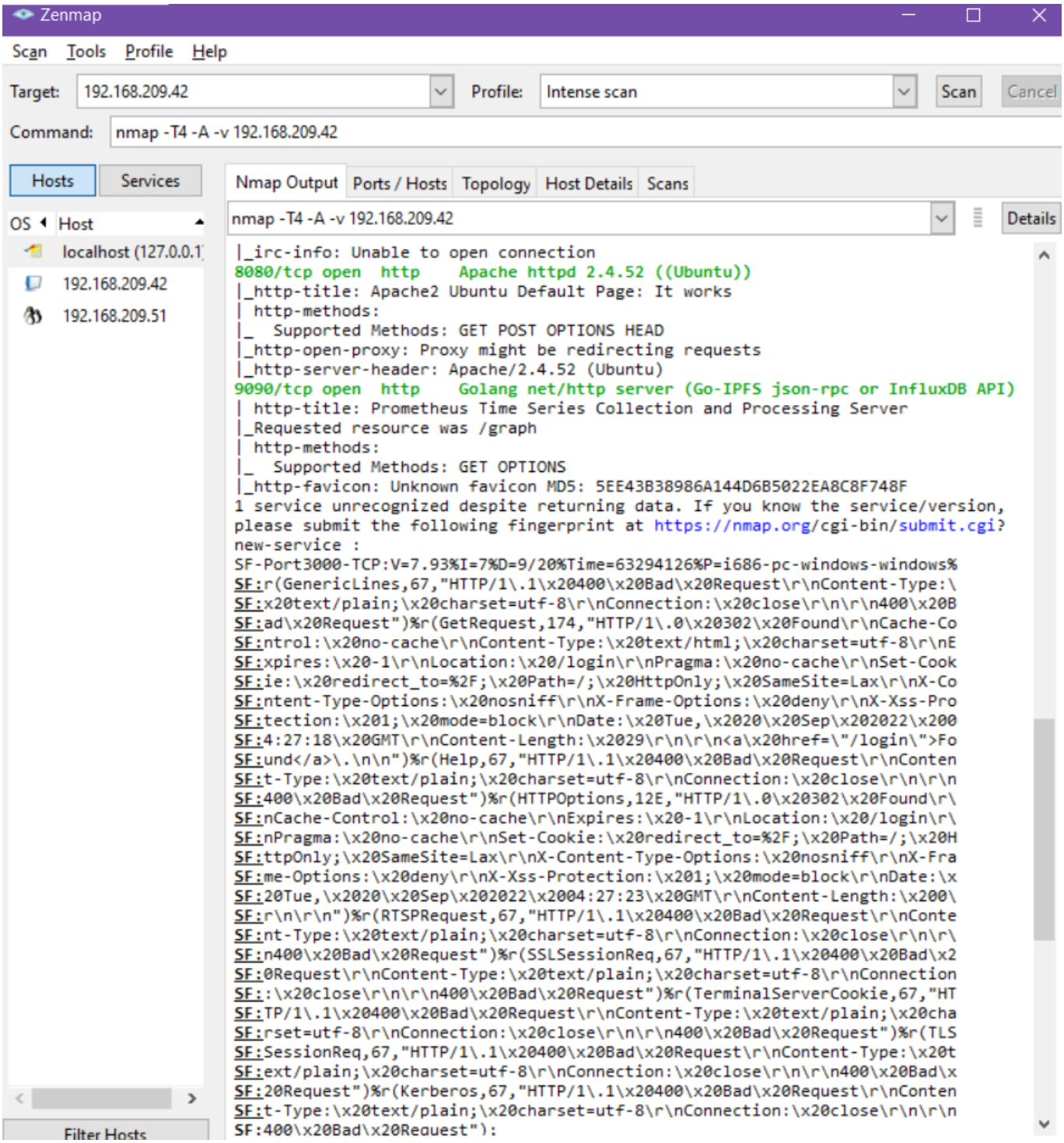


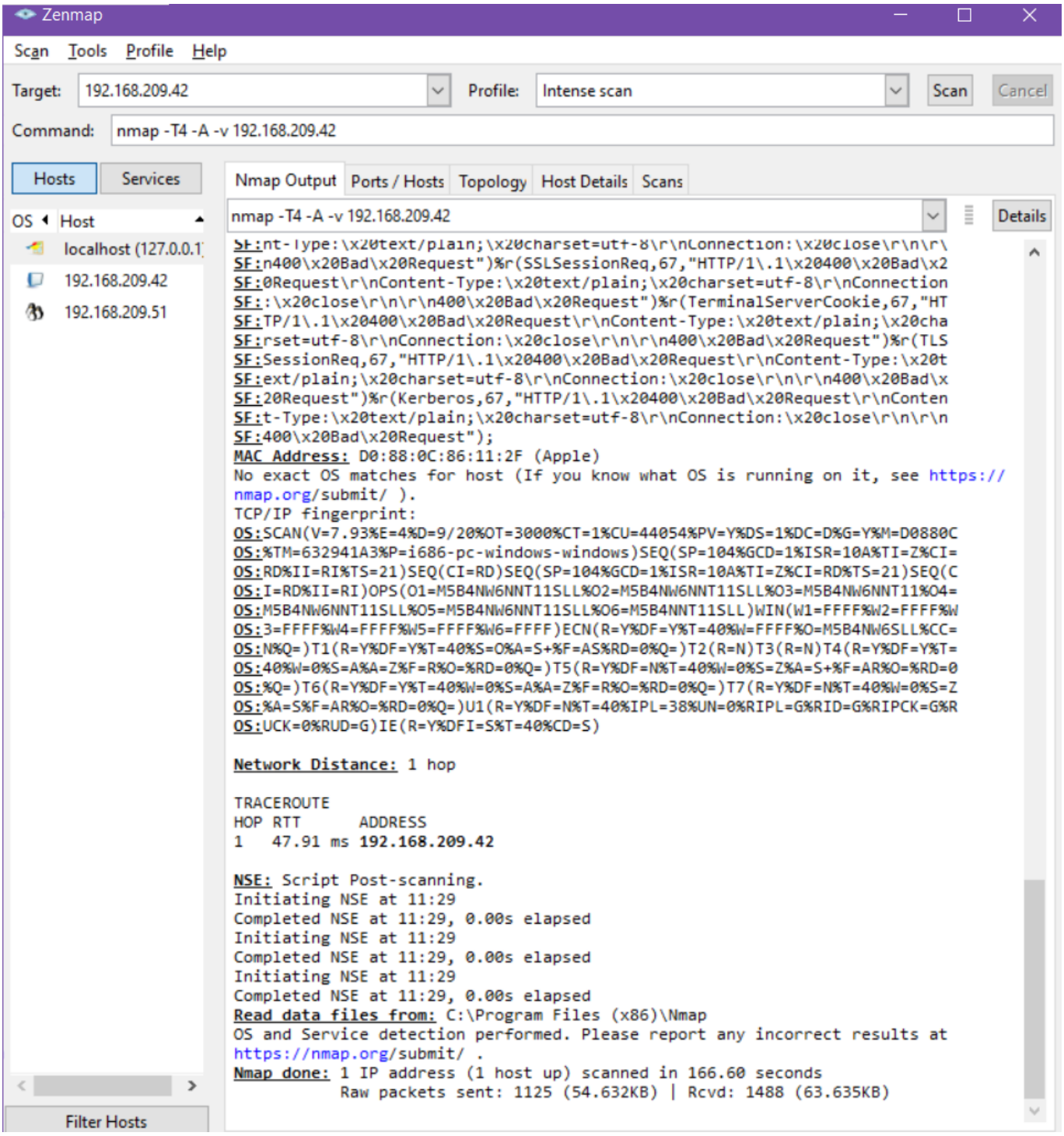
Attacking target host


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
OS Host
localhost (127.0.0.1)
192.168.209.42
192.168.209.51
Filter Hosts
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -T4 -A -v 192.168.209.42
Details
Starting Nmap 7.93 (https://nmap.org) at 2022-09-20 11:26 SE Asia Standard Time
NSOCK ERROR [0.3100s] ssl_init_helper(): OpenSSL legacy provider failed to load.
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

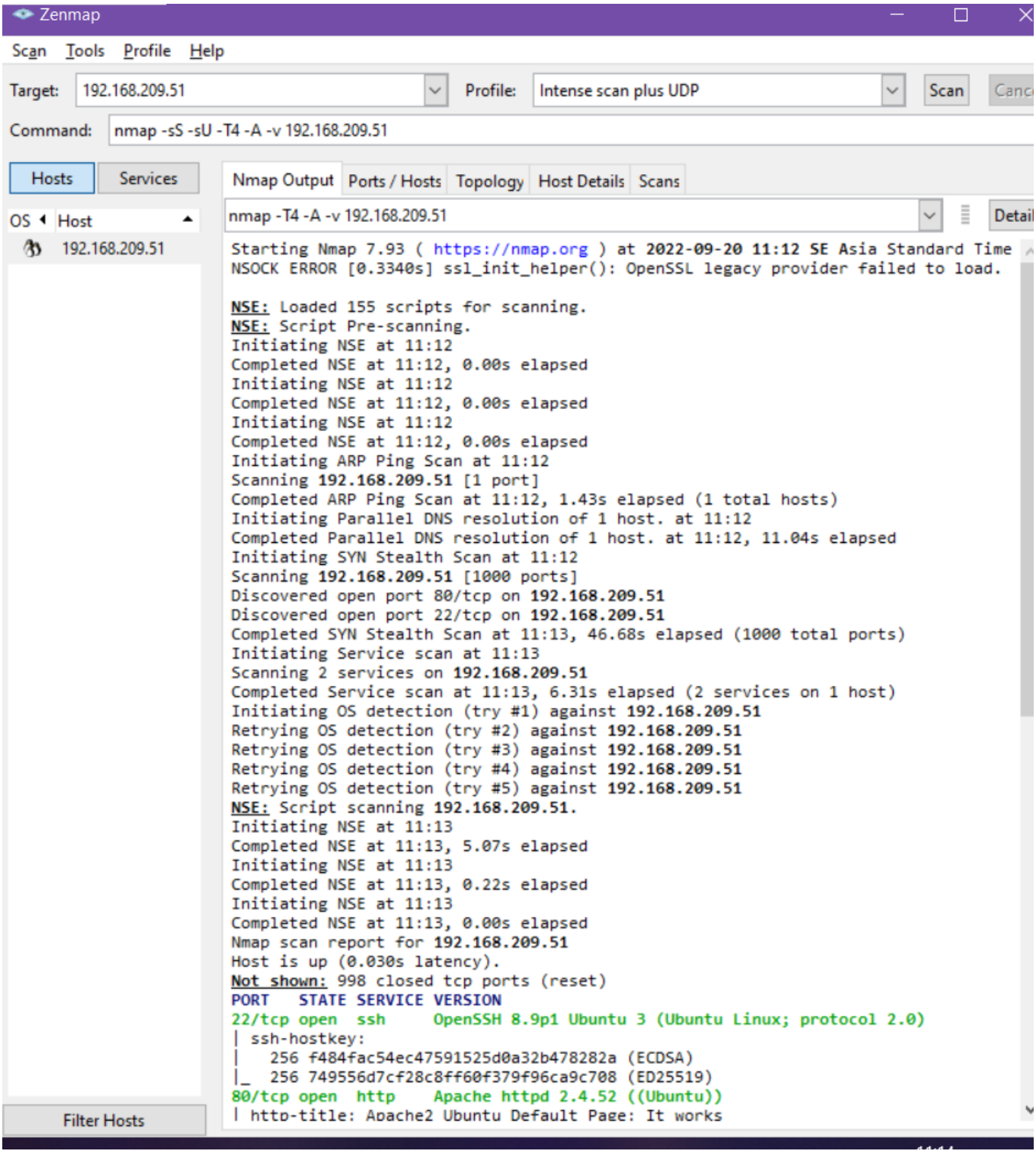

Zenmap
Scan Tools Profile Help
Target: 192.168.209.42
Profile: Intense scan
Scan Cancel
Command: nmap -T4 -A -v 192.168.209.42
Hosts Services
OS Host
localhost (127.0.0.1)
192.168.209.42
192.168.209.51
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -T4 -A -v 192.168.209.42
Details
Initiating NSE at 11:28
Completed NSE at 11:29, 30.30s elapsed
Initiating NSE at 11:29
Completed NSE at 11:29, 1.19s elapsed
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?

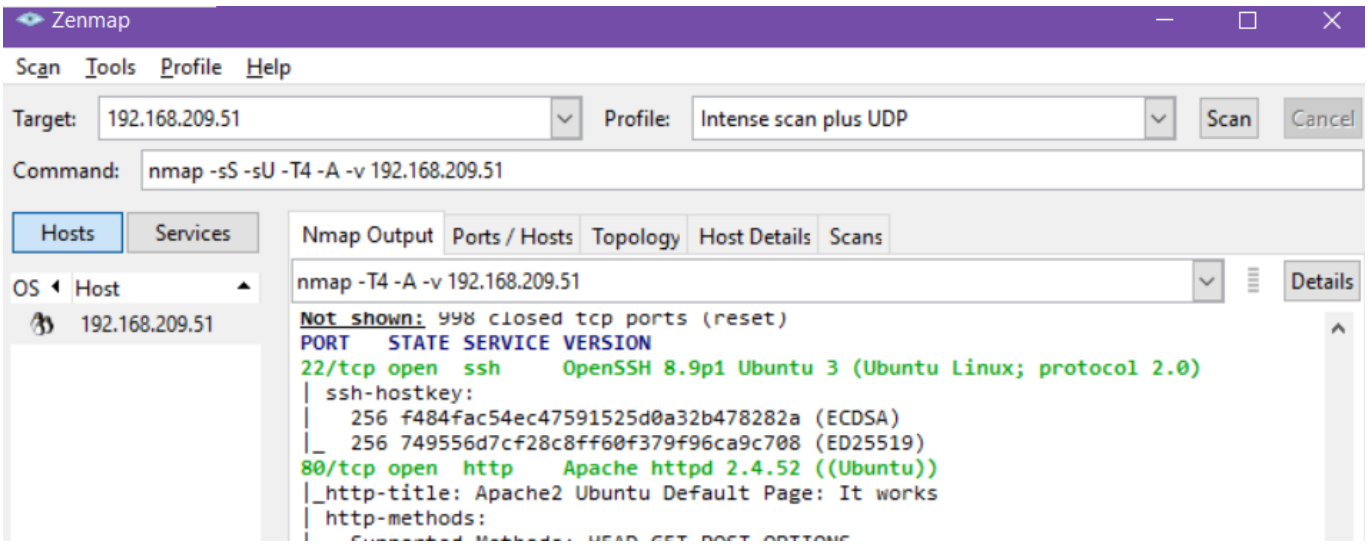

| fingerprint-strings:
| GenericLines, Help, Kerberos, RTSPRequest, SSLSessionReq, TLSSessionReq,
TerminalServerCookie:
| HTTP/1.1 400 Bad Request
| Content-Type: text/plain; charset=utf-8
| Connection: close
| Request
| GetRequest:
| HTTP/1.0 302 Found
| Cache-Control: no-cache
| Content-Type: text/html; 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.
| 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)
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
OS Host
localhost (127.0.0.1)
192.168.209.42
192.168.209.51
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T4 -A -v 192.168.209.42
Details
|_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:\
SF:x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20B
SF:ad\x20Request")%r(GetRequest,174,"HTTP/1\.0\x20302\x20Found\r\nCache-Co
SF:ntrol:\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<a\x20href=\"/login\">Fo
SF:und\.\n\n")%r(Help,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConten
SF:t-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n
SF:400\x20Bad\x20Request")%r(HTTPOptions,12E,"HTTP/1\.0\x20302\x20Found\r\
SF:nCache-Control:\x20no-cache\r\nExpires:\x20-1\r\nLocation:\x20/login\r\
SF:nPragma:\x20no-cache\r\nSet-Cookie:\x20redirect_to=%2F;\x20Path=/;\x20H
SF:ttpOnly;\x20SameSite=Lax\r\nX-Content-Type-Options:\x20nosniff\r\nX-Fra
SF:me-Options:\x20deny\r\nX-Xss-Protection:\x201;\x20mode=block\r\nDate:\x
SF:20Tue,\x2020\x20Sep\x202022\x2004:27:23\x20GMT\r\nContent-Length:\x200\
SF:r\n\r\n")%r(RTSPRequest,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConte
SF:nt-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\
SF:n400\x20Bad\x20Request")%r(SSLSessionReq,67,"HTTP/1\.1\x20400\x20Bad\x2
SF:0Request\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\nConnection
SF:;\x20close\r\n\r\n400\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\n400\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\n400\x20Bad\x
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\n
SF:400\x20Bad\x20Request");



Attacking target VM


Zenmap
Scan Tools Profile Help
Target: 192.168.209.51
Profile: Intense scan plus UDP
Scan
Command: nmap -sS -sU -T4 -A -v 192.168.209.51
Hosts Services
OS Host
192.168.209.51
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
NSOCK ERROR [0.3340s] ssl_init_helper(): OpenSSL legacy provider failed to load.
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 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
OS Host
192.168.209.51
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -T4 -A -v 192.168.209.51
Details
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:

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?

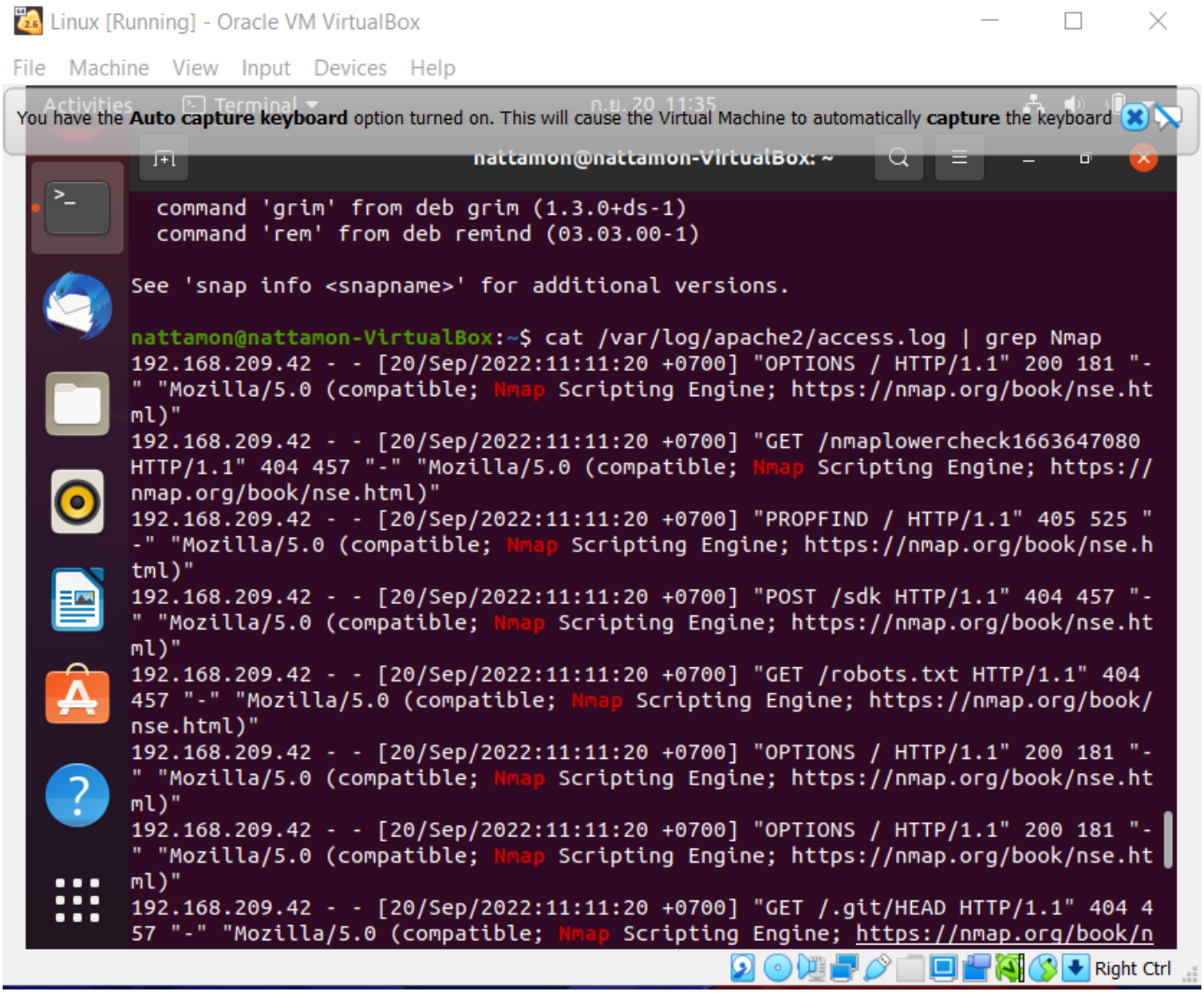
The information is correct for Windows but not for MacOS and Linux where the OS was unable to be detected. However, the MAC address was identified as Apple.

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

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

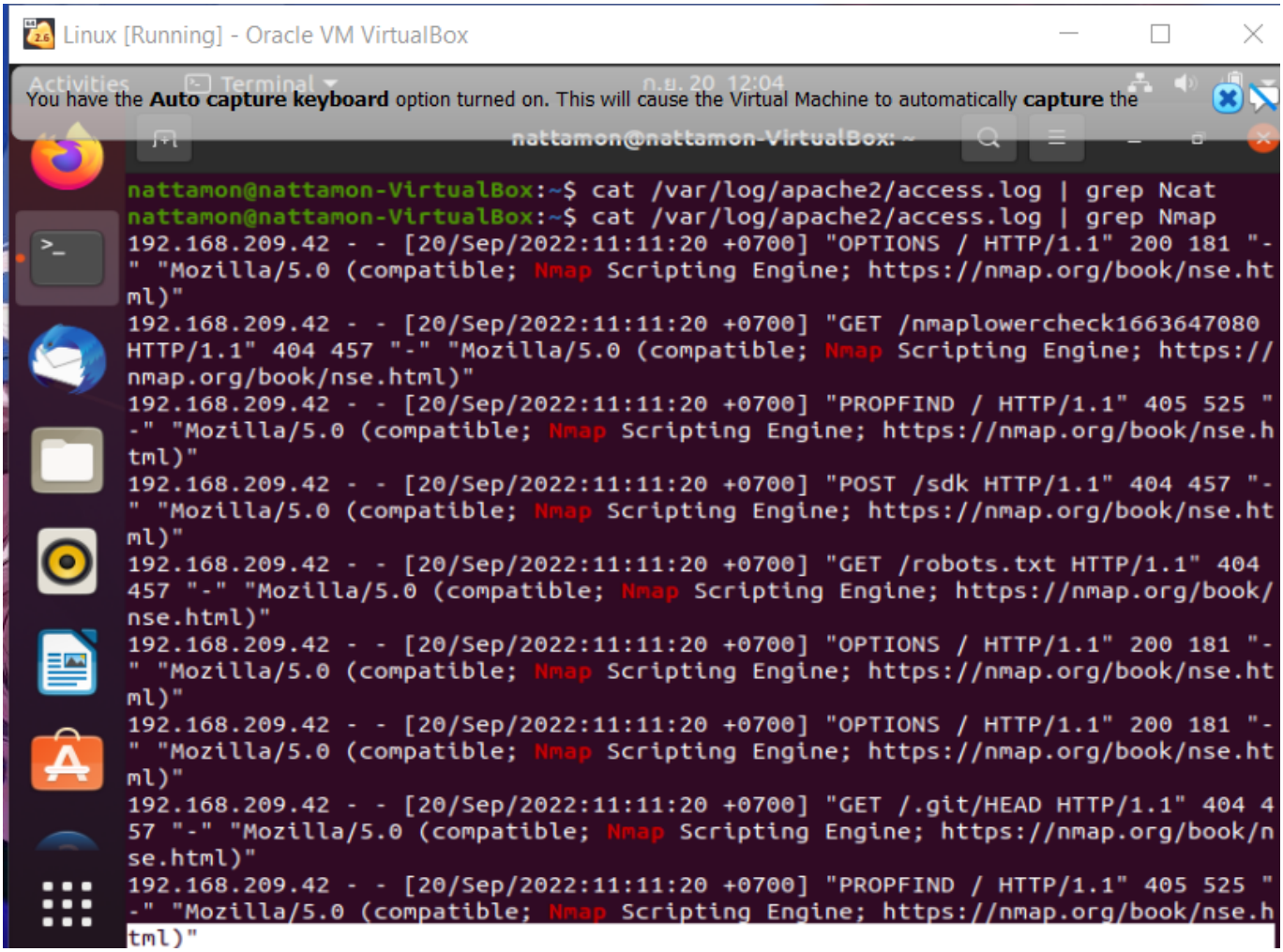
- open ports
- what those ports are, the versions, protocols and such
- supported capabilities or http options
- the device type, OS, and network distance of the host The information is certainly useful for malicious purposes.

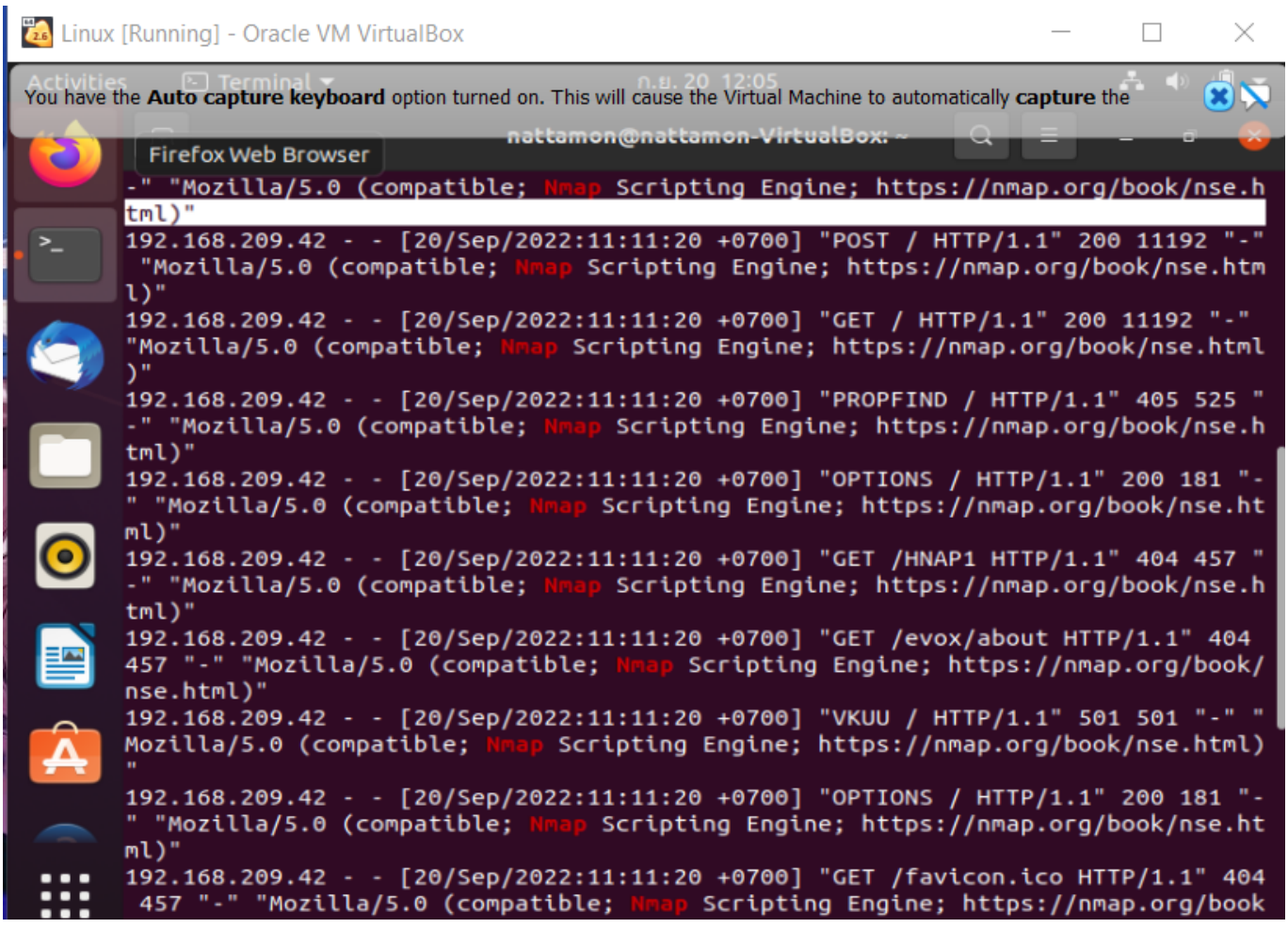
4. Look at the access.log file for the web server in your Linux VM. What IP addresses do you see accessing the web server? Which devices do these IP addresses belong to?

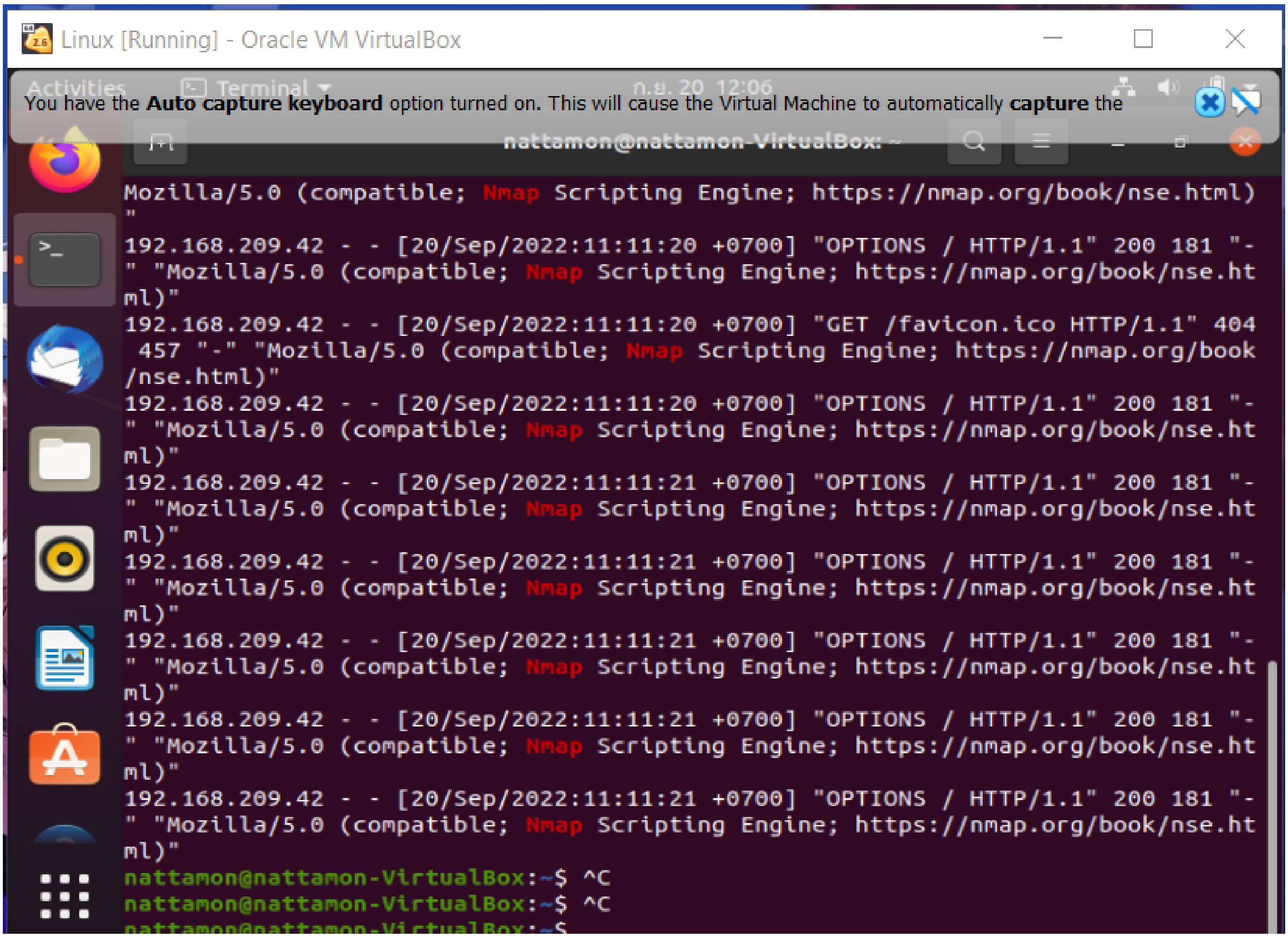


The IP address is 192.168.209.42, which is the IP address of the target notebook (which was also attacking this VM).

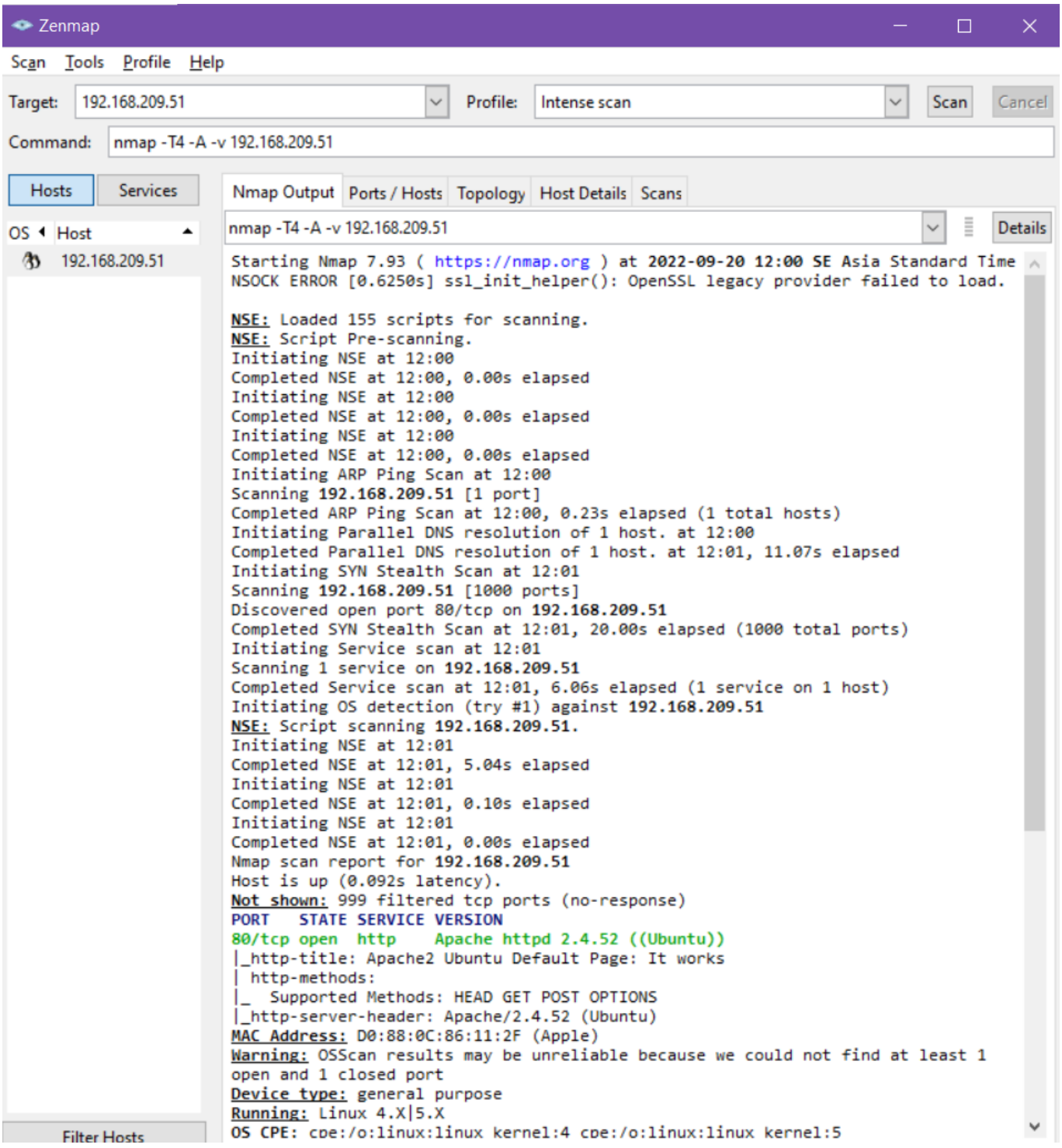
5. Find the nmap scan in the web server log. Copy the lines from the log file that were created because of the nmap scan.

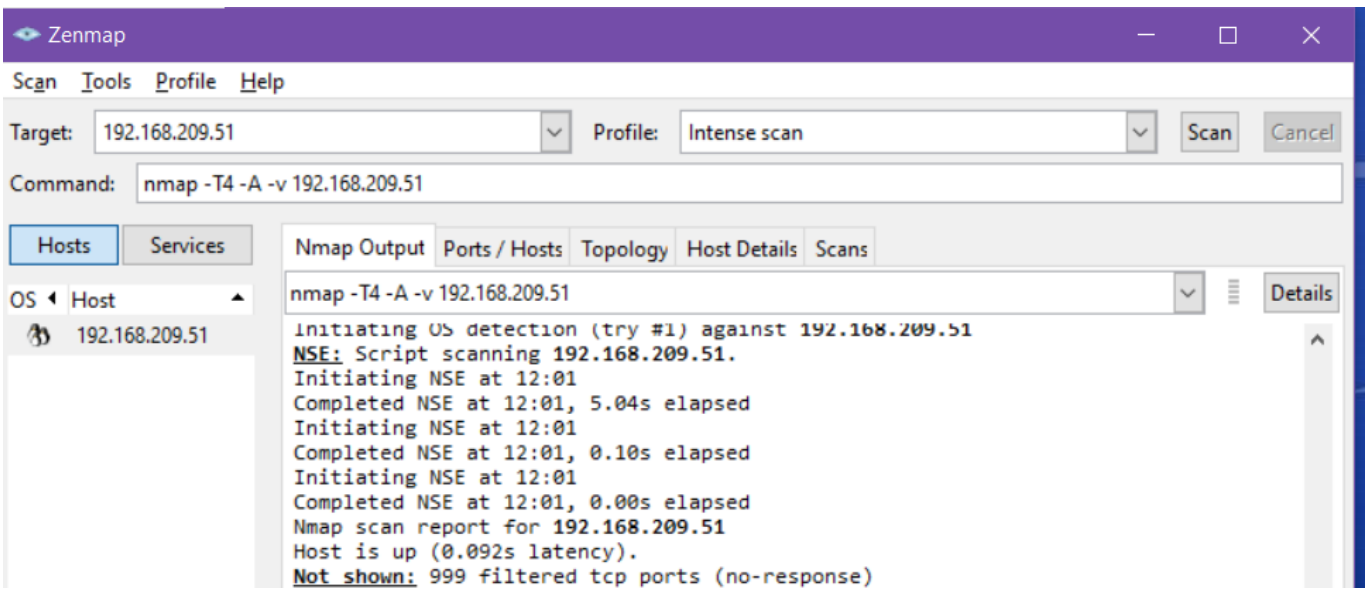

Linux [Running] - Oracle VM VirtualBox
You have the Auto capture keyboard option turned on. This will cause the Virtual Machine to automatically capture the
nattamon@nattamon-VirtualBox: ~
nattamon@nattamon-VirtualBox:~$ cat /var/log/apache2/access.log | grep Ncat
nattamon@nattamon-VirtualBox:~$ cat /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" 404 457 "-" "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)"

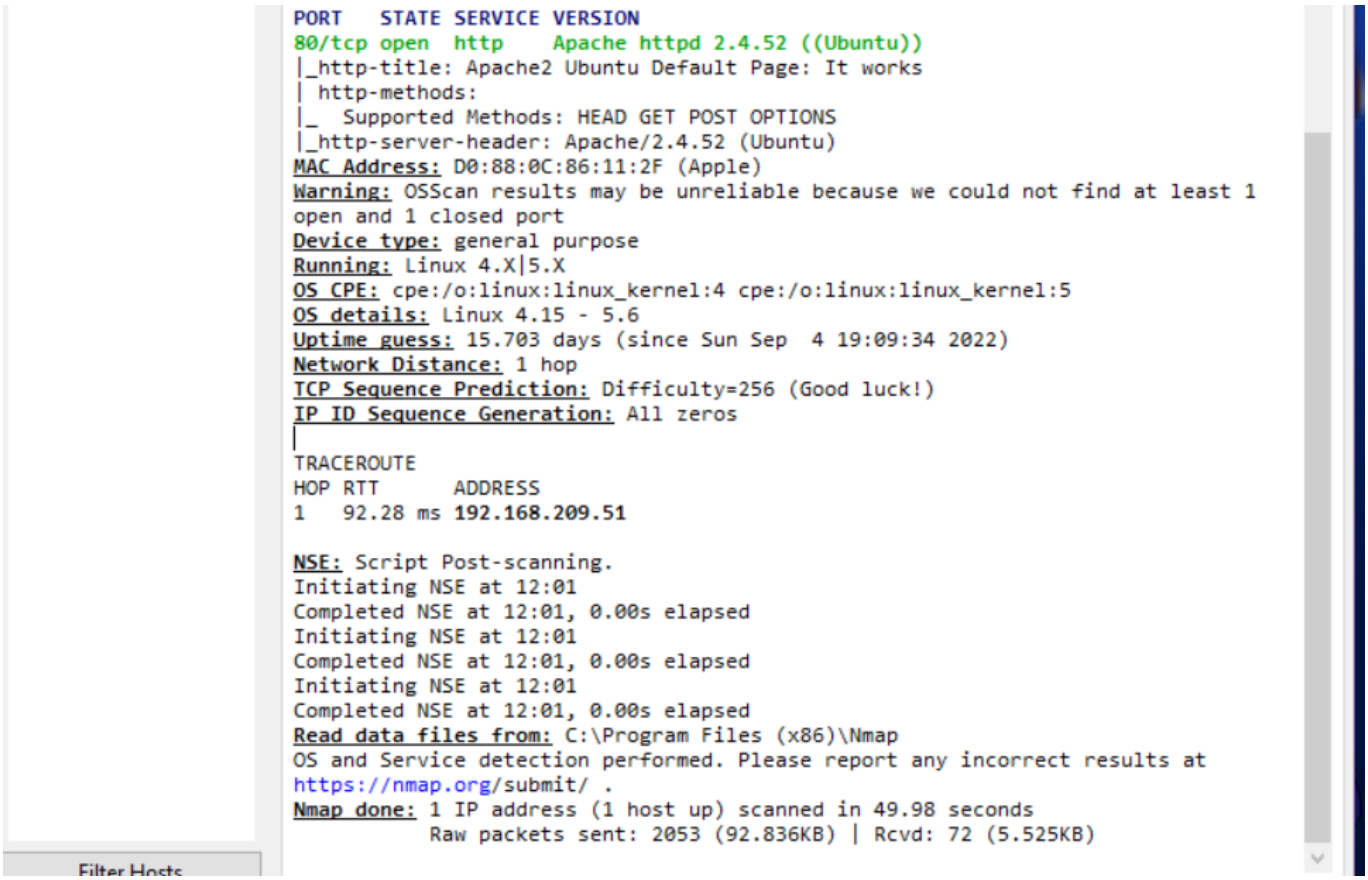

Linux [Running] - Oracle VM VirtualBox
You have the Auto capture keyboard option turned on. This will cause the Virtual Machine to automatically capture the
nattamon@nattamon-VirtualBox: ~
Firefox Web Browser
-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.209.42 - - [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



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
OS Host
192.168.209.51
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T4 -A -v 192.168.209.51
Details
Starting Nmap 7.93 (https://nmap.org) at 2022-09-20 12:00 SE Asia Standard Time
NSOCK 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


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
OS Host
192.168.209.51
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T4 -A -v 192.168.209.51
Details
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)



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)"
192.168.209.42 - - [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] "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] "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 /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.