# Performing Active Reconnaissance (4e)

Ethical Hacking, Fourth Edition - Lab 02

| Student: | Email: |
|---|---|
| Isaiah Mosley | isaiahmosley80@gmail.com |

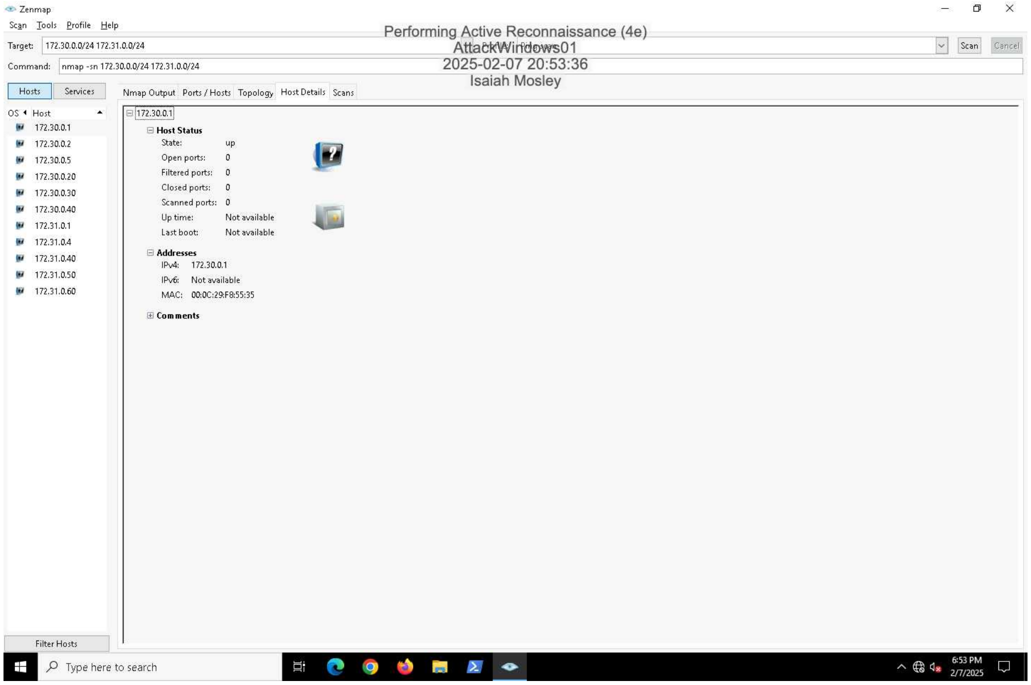
| Time on Task: | Progress: |
|---|---|
| 110 hours, 29 minutes | 100% |

Report Generated: Tuesday, December 2, 2025 at 1:22 PM

## Section 1: Hands-On Demonstration

### Part 1: Use Zenmap to Scan a Target Network

8. **Make a screen capture** showing the **hosts identified by the Ping scan**.



Performing Active Reconnaissance (4e)
AttackWindows01
2025-02-07 20:53:36
Isaiah Mosley

Target: 172.30.0.0/24 172.31.0.0/24

Command: nmap -sn 172.30.0.0/24 172.31.0.0/24

Host:
172.30.0.1
172.30.0.2
172.30.0.5
172.30.0.20
172.30.0.30
172.30.0.40
172.31.0.1
172.31.0.4
172.31.0.40
172.31.0.50
172.31.0.60

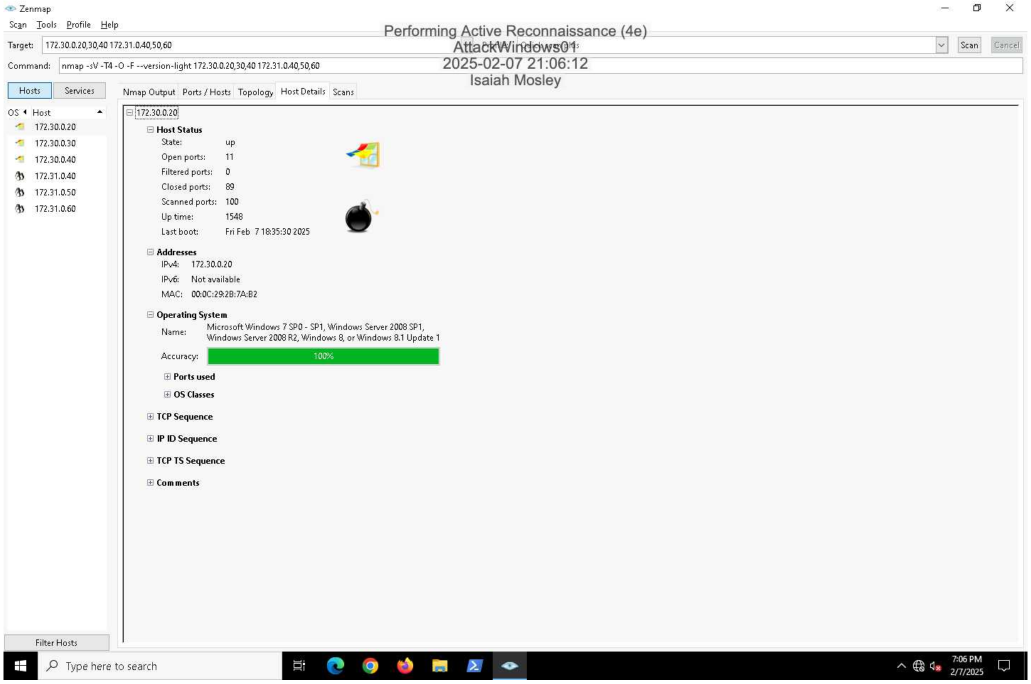
172.30.0.1

Host Status
State: up
Open ports: 0
Filtered ports: 0
Closed ports: 0
Scanned ports: 0
Up time: Not available
Last boot: Not available

Addresses
IPv4: 172.30.0.1
IPv6: Not available
MAC: 00:0C:29:F8:55:35

Comments

15. **Make a screen capture** showing the **host details for 172.30.0.20 from Quick scan plus**.



Performing Active Reconnaissance (4e)
AttackWindows01
2025-02-07 21:06:12
Isaiah Mosley

Target: 172.30.0.20,30,40 172.31.0.40,50,60

Command: nmap -sV -T4 -O -F --version-light 172.30.0.20,30,40 172.31.0.40,50,60

172.30.0.20
172.30.0.30
172.30.0.40
172.31.0.40
172.31.0.50
172.31.0.60

172.30.0.20

Host Status
State: up
Open ports: 11
Filtered ports: 0
Closed ports: 89
Scanned ports: 100
Up time: 1548
Last boot: Fri Feb 7 18:35:30 2025

Addresses
IPv4: 172.30.0.20
IPv6: Not available
MAC: 00:0C:29:2B:7A:B2

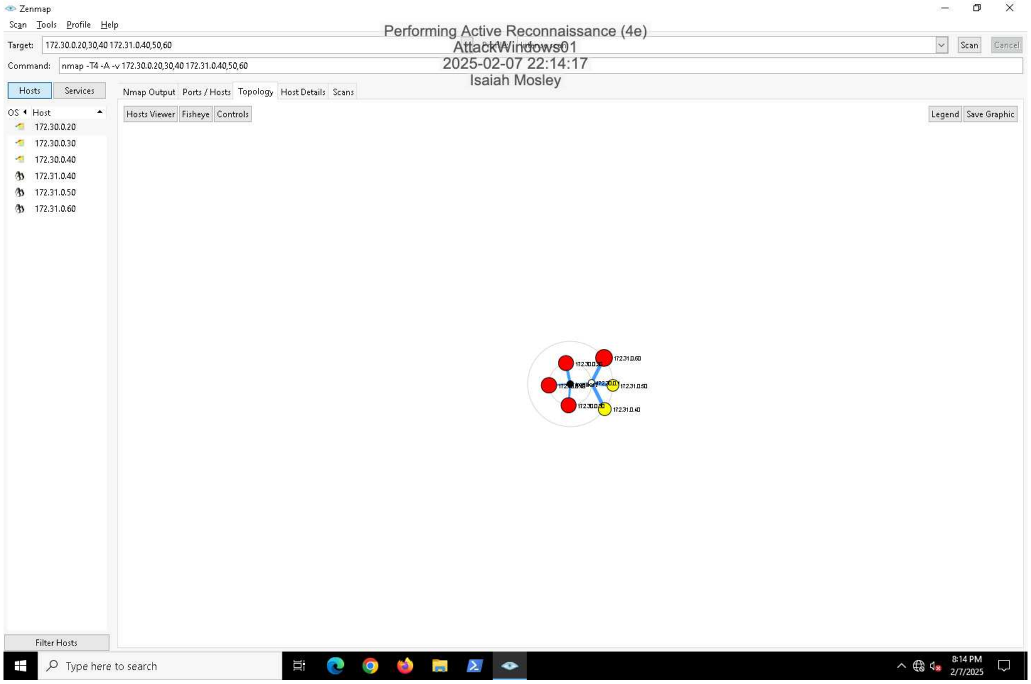
Operating System
Name: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Accuracy: 100%
Ports used
OS Classes

TCP Sequence
IP ID Sequence
TCP TS Sequence
Comments

19. **Document** the **IP addresses and operating systems identified.**

**IPv4**:172.30.0.20 **OS**: Microsoft Window7 SP0-SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1172.30.0.30
**IPv4**:172.30.0.30 **OS**: Microsoft Windows Server R2 Update 1
**IPv4**:172.30.0.40 **OS**: Microsoft Windows Server 2016 build 10586 - 14393
**IPv4**:172.31.0.40 **OS**: Linux 2.6.32
IPv4:172.31.0.50 **OS**: Linux 3.11 - 4.1
**IPv4**172.31.0.60 **OS**: Linux 2.6.15 - 2.6.26 (Likely embedded)

26. **Make a screen capture** showing the **network topology**.



Performing Active Reconnaissance (4e)
AttackWindows01
2025-02-07 22:14:17
Isaiah Mosley

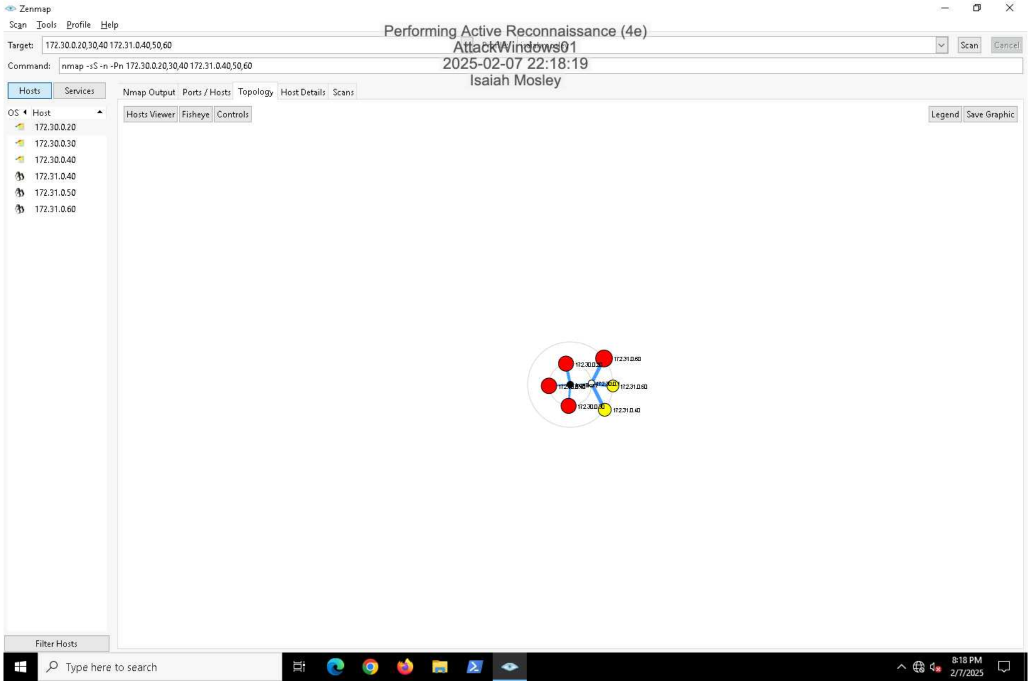
Target: 172.30.0.20,30,40 172.31.0.40,50,60

Command: nmap -T4 -A -v 172.30.0.20,30,40 172.31.0.40,50,60

| OS | Host |
|---|---|
| | 172.30.0.20 |
| | 172.30.0.30 |
| | 172.30.0.40 |
| | 172.31.0.40 |
| | 172.31.0.50 |
| | 172.31.0.60 |

## Part 2: Examine Scan Traffic with Wireshark

11. **Make a screen capture** showing the **new scan profile selected with the corresponding nmap command line**.



Zenmap

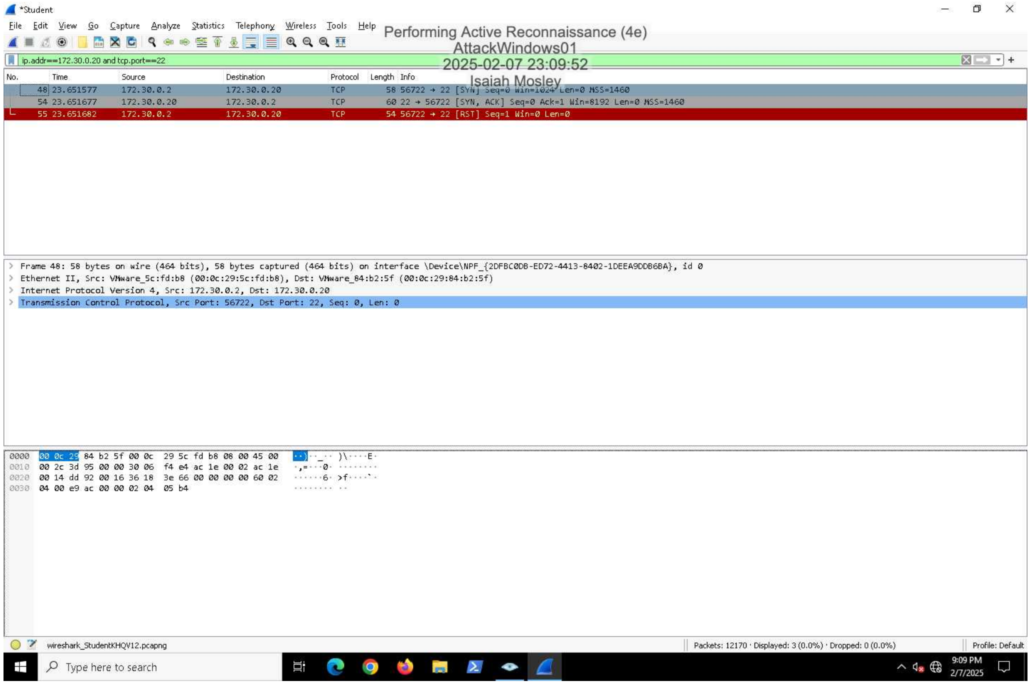
Target: 172.30.0.20,30,40 172.31.0.40,50,60

Command: nmap -sS -n -Pn 172.30.0.20,30,40 172.31.0.40,50,60

Performing Active Reconnaissance (4e)
AttackWindows01
2025-02-07 22:18:19
Isaiah Mosley

| OS | Host |
|---|---|
| | 172.30.0.20 |
| | 172.30.0.30 |
| | 172.30.0.40 |
| | 172.31.0.40 |
| | 172.31.0.50 |
| | 172.31.0.60 |

21. **Make a screen capture** showing the **3-packet sequence for the SYN scan of 172.30.0.20 port 22**.



*Student

ip.addr==172.30.0.20 and tcp.port==22

Performing Active Reconnaissance (4e)
AttackWindows01
2025-02-07 23:09:52
Isaiah Mosley

```
No.  Time       Source       Destination  Protocol  Length  Info
  48 23.651577  172.30.0.2   172.30.0.20  TCP       58 56722 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  54 23.651677  172.30.0.20  172.30.0.2   TCP       60 22 → 56722 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
  55 23.651682  172.30.0.2   172.30.0.20  TCP       54 56722 → 22 [RST] Seq=1 Win=0 Len=0
```

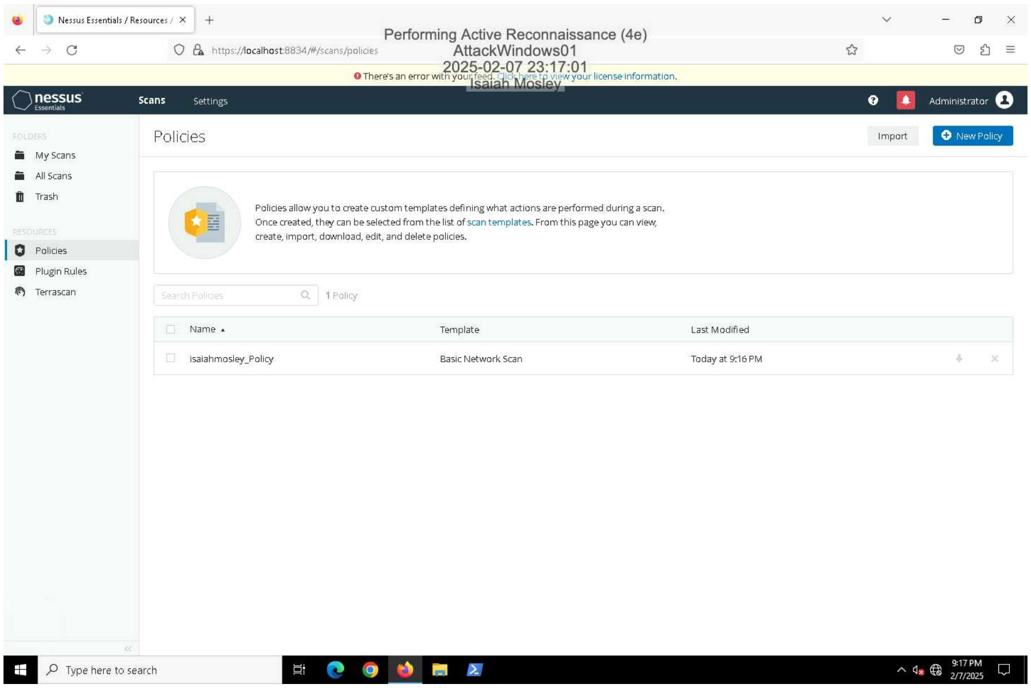
```
> Frame 48: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface \Device\NPF_{2DFBC0DB-ED72-4413-8402-1DEEA9DDB6BA}, id 0
> Ethernet II, Src: VMware_5c:fd:b8 (00:0c:29:5c:fd:b8), Dst: VMware_84:b2:5f (00:0c:29:84:b2:5f)
> Internet Protocol Version 4, Src: 172.30.0.2, Dst: 172.30.0.20
> Transmission Control Protocol, Src Port: 56722, Dst Port: 22, Seq: 0, Len: 0
```

```
0000  00 0c 29 84 b2 5f 00 0c  29 5c fd b8 08 00 45 00   ··)··_·· )\····E·
0010  00 2c 3d 95 00 00 30 06  f4 e4 ac 1e 00 02 ac 1e   ·,=···0· ········
0020  00 14 dd 92 00 16 36 18  3e 66 00 00 00 00 60 02   ······6· >f····`·
0030  04 00 e9 ac 00 00 02 04  05 b4                     ········ ··
```

wireshark_StudentKHQV12.pcapng | Packets: 12170 · Displayed: 3 (0.0%) · Dropped: 0 (0.0%) | Profile: Default

## Part 3: Run a Vulnerability Scan with Nessus

10. **Make a screen capture** showing **the new Nessus policy**.



Performing Active Reconnaissance (4e)
AttackWindows01
2025-02-07 23:17:01
Isaiah Mosley

There's an error with your feed. Click here to view your license information.

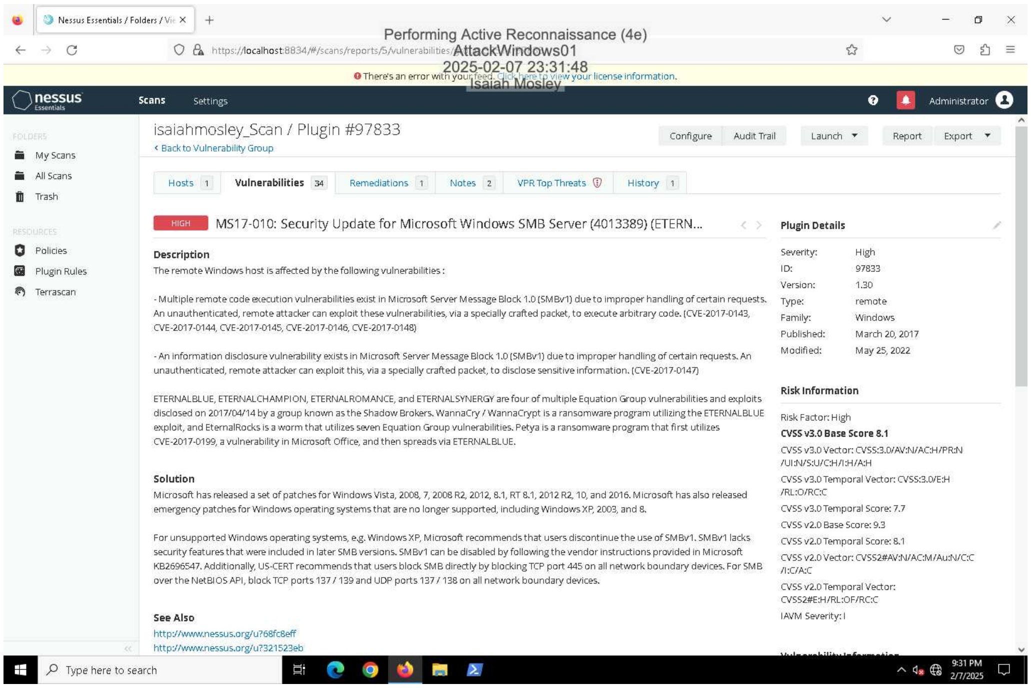
Policies

Policies allow you to create custom templates defining what actions are performed during a scan. Once created, they can be selected from the list of scan templates. From this page you can view, create, import, download, edit, and delete policies.

1 Policy

| Name | Template | Last Modified |
|---|---|---|
| isaiahmosley_Policy | Basic Network Scan | Today at 9:16 PM |

22. **Make a screen capture** showing the **vulnerability title** and the **Plugin information** for MS17-010.



Performing Active Reconnaissance (4e)
AttackWindows01
2025-02-07 23:31:48
Isaiah Mosley

There's an error with your feed. Click here to view your license information.

isaiahmosley_Scan / Plugin #97833

‹ Back to Vulnerability Group

HIGH MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERN...

**Description**

The remote Windows host is affected by the following vulnerabilities :

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)

- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

**Solution**

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.

For unsupported Windows operating systems, e.g. Windows XP, Microsoft recommends that users discontinue the use of SMBv1. SMBv1 lacks security features that were included in later SMB versions. SMBv1 can be disabled by following the vendor instructions provided in Microsoft KB2696547. Additionally, US-CERT recommends that users block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

**See Also**

http://www.nessus.org/u?68fc8eff
http://www.nessus.org/u?321523eb

**Plugin Details**

| | |
|---|---|
| Severity: | High |
| ID: | 97833 |
| Version: | 1.30 |
| Type: | remote |
| Family: | Windows |
| Published: | March 20, 2017 |
| Modified: | May 25, 2022 |

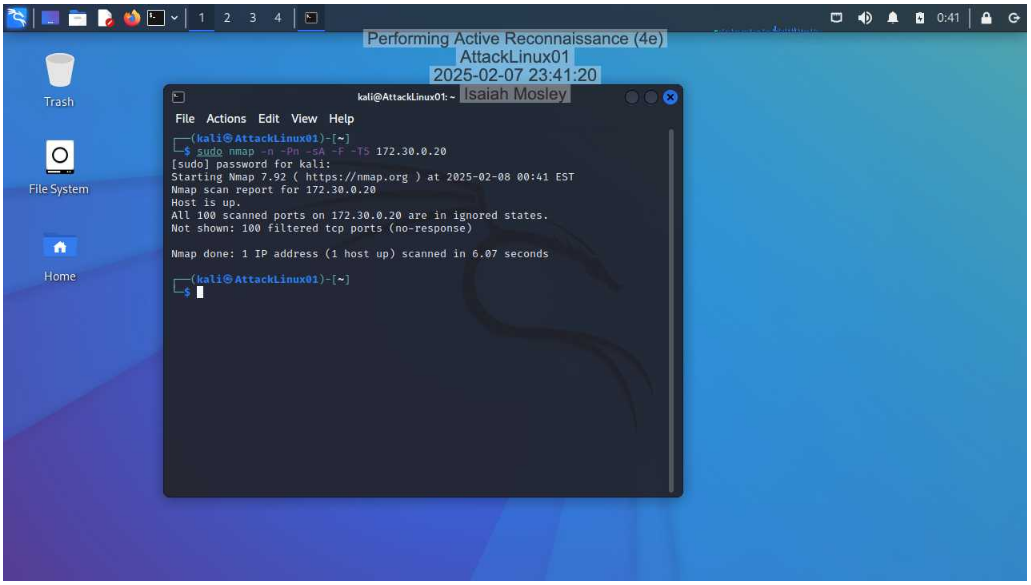
**Risk Information**

Risk Factor: High
**CVSS v3.0 Base Score 8.1**
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS v3.0 Temporal Vector: CVSS:3.0/E:H/RL:O/RC:C
CVSS v3.0 Temporal Score: 7.7
CVSS v2.0 Base Score: 9.3
CVSS v2.0 Temporal Score: 8.1
CVSS v2.0 Vector: CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C
CVSS v2.0 Temporal Vector: CVSS2#E:H/RL:OF/RC:C
IAVM Severity: I

# Section 2: Applied Learning

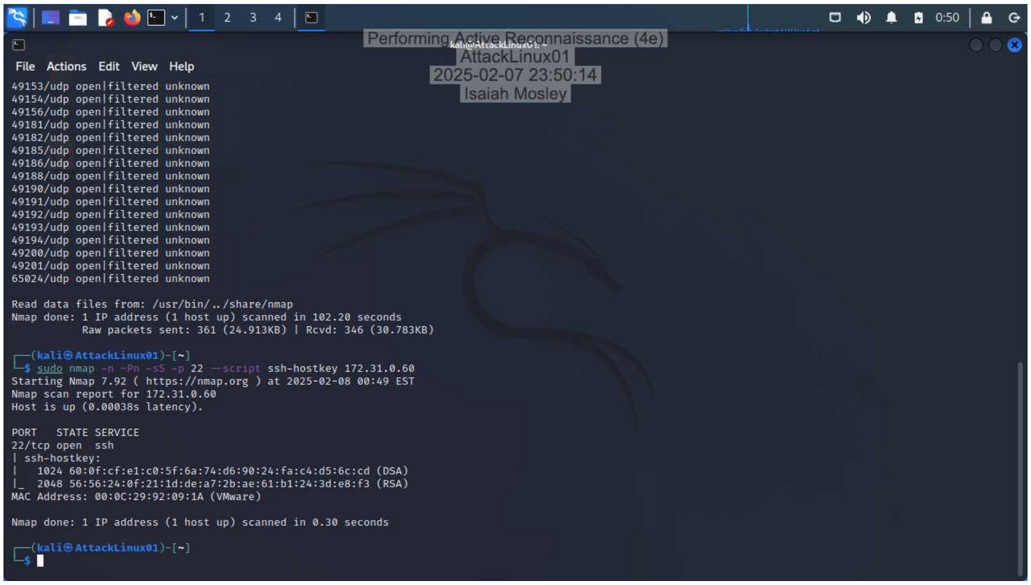
## Part 1: Use Nmap to Scan a Target Network

7. **Make a screen capture** showing the **results of the ACK scan on 172.30.0.20**.



```
┌──(kali㉿AttackLinux01)-[~]
└─$ sudo nmap -n -Pn -sA -F -T5 172.30.0.20
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2025-02-08 00:41 EST
Nmap scan report for 172.30.0.20
Host is up.
All 100 scanned ports on 172.30.0.20 are in ignored states.
Not shown: 100 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 6.07 seconds

┌──(kali㉿AttackLinux01)-[~]
└─$ 
```

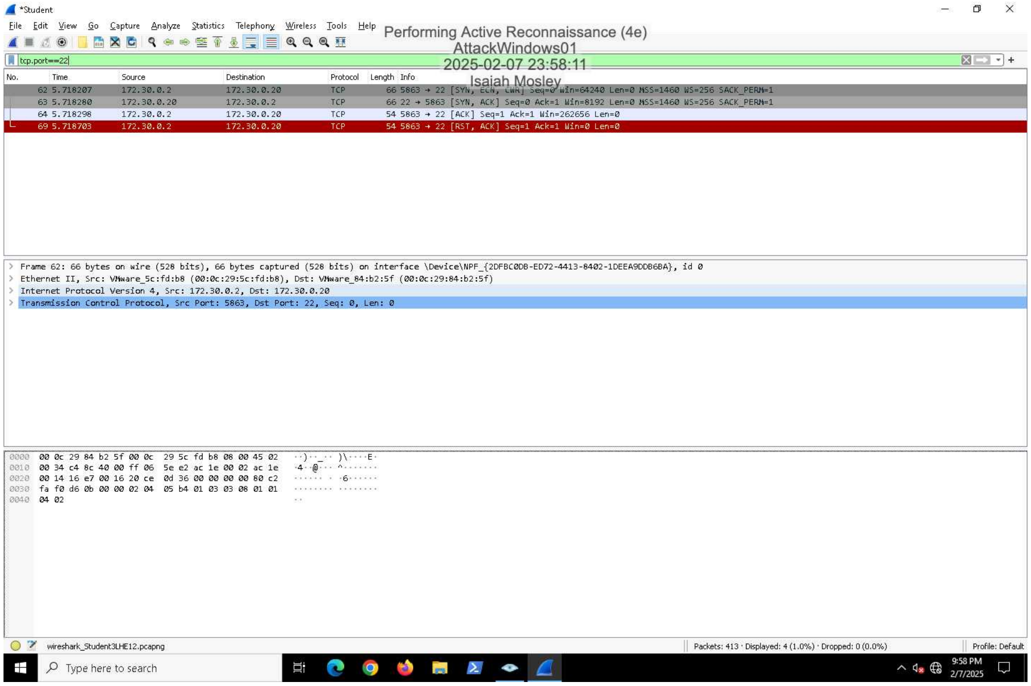
11. **Make a screen capture** showing the **results of the scan with the ssh-hostkey script**.



```
49153/udp open|filtered unknown
49154/udp open|filtered unknown
49156/udp open|filtered unknown
49181/udp open|filtered unknown
49182/udp open|filtered unknown
49185/udp open|filtered unknown
49186/udp open|filtered unknown
49188/udp open|filtered unknown
49190/udp open|filtered unknown
49191/udp open|filtered unknown
49192/udp open|filtered unknown
49193/udp open|filtered unknown
49194/udp open|filtered unknown
49200/udp open|filtered unknown
49201/udp open|filtered unknown
65024/udp open|filtered unknown

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 102.20 seconds
           Raw packets sent: 361 (24.913KB) | Rcvd: 346 (30.783KB)

┌──(kali㉿AttackLinux01)-[~]
└─$ sudo nmap -n -Pn -sS -p 22 --script ssh-hostkey 172.31.0.60
Starting Nmap 7.92 ( https://nmap.org ) at 2025-02-08 00:49 EST
Nmap scan report for 172.31.0.60
Host is up (0.00038s latency).

PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey: 
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
MAC Address: 00:0C:29:92:09:1A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds

┌──(kali㉿AttackLinux01)-[~]
└─$ 
```

## Part 2: Capture Traffic for a TCP Connect Scan

11. **Make a screen capture** showing the **4-packet sequence for the TCP Connect scan on 172.30.20 port 22**.



Performing Active Reconnaissance (4e)
AttackWindows01
2025-02-07 23:58:11
Isaiah Mosley

tcp.port==22

```
No.  Time      Source       Destination  Protocol Length Info
  62 5.718207  172.30.0.2   172.30.0.20  TCP      66 5863 → 22 [SYN, ECN, CWR] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  63 5.718280  172.30.0.20  172.30.0.2   TCP      66 22 → 5863 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
  64 5.718298  172.30.0.2   172.30.0.20  TCP      54 5863 → 22 [ACK] Seq=1 Ack=1 Win=262656 Len=0
  69 5.718703  172.30.0.2   172.30.0.20  TCP      54 5863 → 22 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

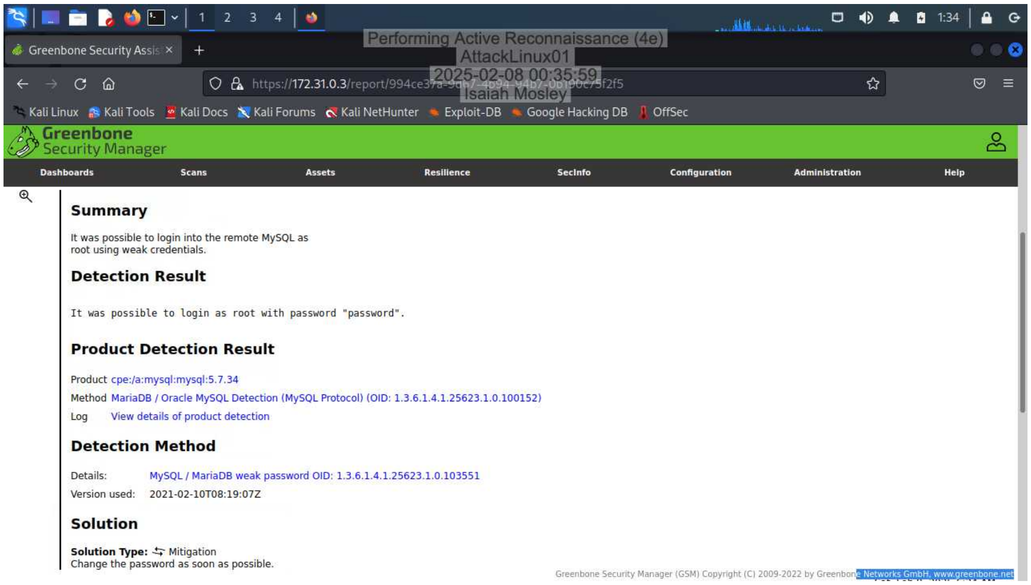
```
> Frame 62: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{2DFBC0DB-ED72-4413-8402-1DEEA9DDB6BA}, id 0
> Ethernet II, Src: VMware_5c:fd:b8 (00:0c:29:5c:fd:b8), Dst: VMware_84:b2:5f (00:0c:29:84:b2:5f)
> Internet Protocol Version 4, Src: 172.30.0.2, Dst: 172.30.0.20
> Transmission Control Protocol, Src Port: 5863, Dst Port: 22, Seq: 0, Len: 0
```

```
0000  00 0c 29 84 b2 5f 00 0c  29 5c fd b8 08 00 45 02   ··)··_··)\····E·
0010  00 34 c4 8c 40 00 ff 06  5e e2 ac 1e 00 02 ac 1e   ·4··@···^·······
0020  00 14 16 e7 00 16 20 ce  0d 36 00 00 00 00 80 c2   ······ ··6······
0030  fa f0 d6 0b 00 00 02 04  05 b4 01 03 03 08 01 01   ················
0040  04 02                                              ··
```

wireshark_Student3LHE12.pcapng | Packets: 413 · Displayed: 4 (1.0%) · Dropped: 0 (0.0%) | Profile: Default

## Part 3: Run a Vulnerability Scan with OpenVAS

17. **Make a screen capture** showing the details of the **MySQL / MariaDB vulnerability**, including the Detection Result and the Solution.



Performing Active Reconnaissance (4e)
AttackLinux01
2025-02-08 00:35:59
Isaiah Mosley

https://172.31.0.3/report/994ce37a-9...-4b94-94b7-0b1b0c75f2f5

### Summary

It was possible to login into the remote MySQL as root using weak credentials.

### Detection Result

```
It was possible to login as root with password "password".
```

### Product Detection Result

Product cpe:/a:mysql:mysql:5.7.34
Method MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.25623.1.0.100152)
Log View details of product detection

### Detection Method

Details: MySQL / MariaDB weak password OID: 1.3.6.1.4.1.25623.1.0.103551
Version used: 2021-02-10T08:19:07Z

### Solution

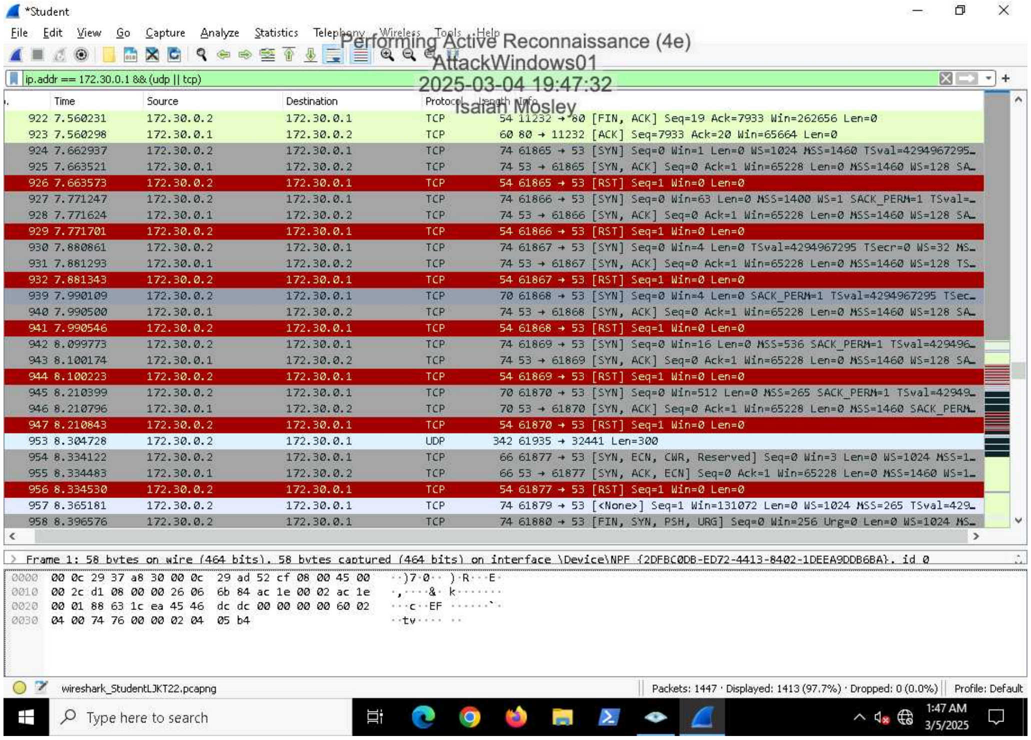
**Solution Type:** Mitigation
Change the password as soon as possible.

Greenbone Security Manager (GSM) Copyright (C) 2009-2022 by Greenbone Networks GmbH, www.greenbone.net

# Section 3: Challenge and Analysis

## Part 1: Capture Traffic for a UDP Scan

**Make a screen capture** showing the **sequence of packets from the UDP scan** of port 53 on 172.30.0.1.



Performing Active Reconnaissance (4e)
AttackWindows01
2025-03-04 19:47:32
Isaiah Mosley

```
ip.addr == 172.30.0.1 && (udp || tcp)
```

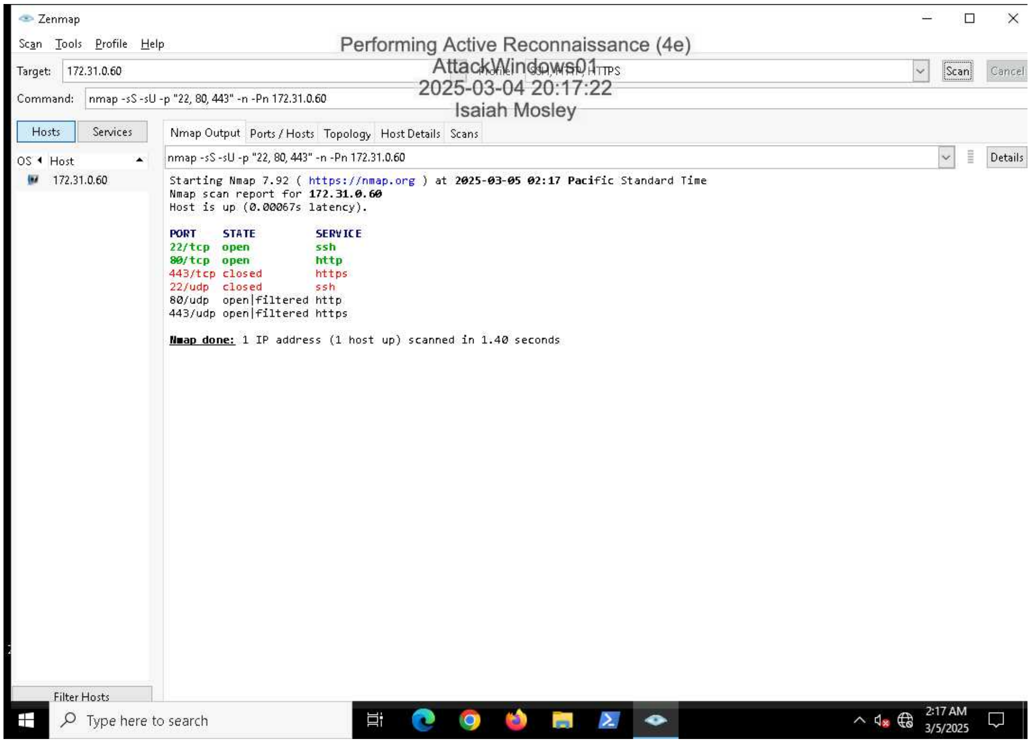
```
.    Time         Source        Destination   Protocol  Length  Info
  922 7.560231    172.30.0.2    172.30.0.1    TCP        54 11232 → 80 [FIN, ACK] Seq=19 Ack=7933 Win=262656 Len=0
  923 7.560298    172.30.0.1    172.30.0.2    TCP        60 80 → 11232 [ACK] Seq=7933 Ack=20 Win=65664 Len=0
  924 7.662937    172.30.0.2    172.30.0.1    TCP        74 61865 → 53 [SYN] Seq=0 Win=1 Len=0 WS=1024 MSS=1460 TSval=4294967295…
  925 7.663521    172.30.0.1    172.30.0.2    TCP        74 53 → 61865 [SYN, ACK] Seq=0 Ack=1 Win=65228 Len=0 MSS=1460 WS=128 SA…
  926 7.663573    172.30.0.2    172.30.0.1    TCP        54 61865 → 53 [RST] Seq=1 Win=0 Len=0
  927 7.771247    172.30.0.2    172.30.0.1    TCP        74 61866 → 53 [SYN] Seq=0 Win=63 Len=0 MSS=1400 WS=1 SACK_PERM=1 TSval=…
  928 7.771624    172.30.0.1    172.30.0.2    TCP        74 53 → 61866 [SYN, ACK] Seq=0 Ack=1 Win=65228 Len=0 MSS=1460 WS=128 SA…
  929 7.771701    172.30.0.2    172.30.0.1    TCP        54 61866 → 53 [RST] Seq=1 Win=0 Len=0
  930 7.880861    172.30.0.2    172.30.0.1    TCP        74 61867 → 53 [SYN] Seq=0 Win=4 Len=0 TSval=4294967295 TSecr=0 WS=32 MS…
  931 7.881293    172.30.0.1    172.30.0.2    TCP        74 53 → 61867 [SYN, ACK] Seq=0 Ack=1 Win=65228 Len=0 MSS=1460 WS=128 TS…
  932 7.881343    172.30.0.2    172.30.0.1    TCP        54 61867 → 53 [RST] Seq=1 Win=0 Len=0
  939 7.990109    172.30.0.2    172.30.0.1    TCP        70 61868 → 53 [SYN] Seq=0 Win=4 Len=0 SACK_PERM=1 TSval=4294967295 TSec…
  940 7.990500    172.30.0.1    172.30.0.2    TCP        74 53 → 61868 [SYN, ACK] Seq=0 Ack=1 Win=65228 Len=0 MSS=1460 WS=128 SA…
  941 7.990546    172.30.0.2    172.30.0.1    TCP        54 61868 → 53 [RST] Seq=1 Win=0 Len=0
  942 8.099773    172.30.0.2    172.30.0.1    TCP        74 61869 → 53 [SYN] Seq=0 Win=16 Len=0 MSS=536 SACK_PERM=1 TSval=429496…
  943 8.100174    172.30.0.1    172.30.0.2    TCP        74 53 → 61869 [SYN, ACK] Seq=0 Ack=1 Win=65228 Len=0 MSS=1460 WS=128 SA…
  944 8.100223    172.30.0.2    172.30.0.1    TCP        54 61869 → 53 [RST] Seq=1 Win=0 Len=0
  945 8.210399    172.30.0.2    172.30.0.1    TCP        70 61870 → 53 [SYN] Seq=0 Win=512 Len=0 MSS=265 SACK_PERM=1 TSval=42949…
  946 8.210796    172.30.0.1    172.30.0.2    TCP        70 53 → 61870 [SYN, ACK] Seq=0 Ack=1 Win=65228 Len=0 MSS=1460 SACK_PERM…
  947 8.210843    172.30.0.2    172.30.0.1    TCP        54 61870 → 53 [RST] Seq=1 Win=0 Len=0
  953 8.304728    172.30.0.2    172.30.0.1    UDP       342 61935 → 32441 Len=300
  954 8.334122    172.30.0.2    172.30.0.1    TCP        66 61877 → 53 [SYN, ECN, CWR, Reserved] Seq=0 Win=3 Len=0 WS=1024 MSS=1…
  955 8.334483    172.30.0.1    172.30.0.2    TCP        66 53 → 61877 [SYN, ACK, ECN] Seq=0 Ack=1 Win=65228 Len=0 MSS=1460 WS=1…
  956 8.334530    172.30.0.2    172.30.0.1    TCP        54 61877 → 53 [RST] Seq=1 Win=0 Len=0
  957 8.365181    172.30.0.2    172.30.0.1    TCP        74 61879 → 53 [<None>] Seq=1 Win=131072 Len=0 WS=1024 MSS=265 TSval=429…
  958 8.396576    172.30.0.2    172.30.0.1    TCP        74 61880 → 53 [FIN, SYN, PSH, URG] Seq=0 Win=256 Urg=0 Len=0 WS=1024 MS…
```

```
> Frame 1: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface \Device\NPF_{2DFBC0DB-ED72-4413-8402-1DEEA9DDB6BA}, id 0
0000  00 0c 29 37 a8 30 00 0c  29 ad 52 cf 08 00 45 00   ··)7·0·· )·R···E·
0010  00 2c d1 08 00 00 26 06  6b 84 ac 1e 00 02 ac 1e   ·,····&· k·······
0020  00 01 88 63 1c ea 45 46  dc dc 00 00 00 00 60 02   ···c··EF ······`·
0030  04 00 74 76 00 00 02 04  05 b4                     ··tv···· ··
```

```
wireshark_StudentLJKT22.pcapng    Packets: 1447 · Displayed: 1413 (97.7%) · Dropped: 0 (0.0%)    Profile: Default
```

## Part 2: Create a New Zenmap Profile

**Make a screen capture** showing the new profile selected in Zenmap and the results of using the profile to scan 172.31.0.60.



Target: 172.31.0.60
Profile: SSH, HTTP, HTTPS
Command: nmap -sS -sU -p "22, 80, 443" -n -Pn 172.31.0.60

```
nmap -sS -sU -p "22, 80, 443" -n -Pn 172.31.0.60

Starting Nmap 7.92 ( https://nmap.org ) at 2025-03-05 02:17 Pacific Standard Time
Nmap scan report for 172.31.0.60
Host is up (0.00067s latency).

PORT    STATE         SERVICE
22/tcp  open          ssh
80/tcp  open          http
443/tcp closed        https
22/udp  closed        ssh
80/udp  open|filtered http
443/udp open|filtered https

Nmap done: 1 IP address (1 host up) scanned in 1.40 seconds
```