Network Reconnaissance

Prepared By:
Kazim Ali Obad

Supervisor:

Anmar Mohammed

MOHAMMED .B. HASSAN

Table of Contents

LAB SCENARIO

You are a junior security analyst tasked with assessing the internal network for vulnerabilities. Your team lead has assigned you to perform a structured reconnaissance exercise against a known-vulnerable virtual machine (Metasploitable 2) at 192.168.100.46 from your Kali Linux attack station at 192.168.100.38. The goal is not exploitation — it is visibility. Before any attack can be launched, an attacker must first understand what is running on the target. Equally, the blue team must understand what reconnaissance looks like in logs so they can detect it.

1. **RED TEAM — Structured Nmap reconnaissance to enumerate all live services**

▼

2. BLUE TEAM — Monitor logs, IDS alerts, and network flows to detect scanning activity

▼

3. PURPLE TEAM — Compare what was done against what was detected; identify and close gaps

This exercise maps to MITRE ATT&CK Techniques T1046 (Network Service Discovery) and T1018 (Remote System Discovery). It represents the earliest phase of the cyber kill chain — reconnaissance — and forms the foundation for all subsequent offensive and defensive work.

Lab Environment

Network Topology	
Kali Linux (Attacker)	192.168.100.38
Metasploitable 2 (Target)	192.168.100.46
Network	192.168.100.0/24 — Isolated VM Network
Tools	Nmap, Wireshark, Zeek, RITA, Suricata, ndiff

SECTION 1 — RED TEAM: Nmap Reconnaissance

1.1 Objective

The red team phase involves a layered series of Nmap scans. Each scan type is chosen to answer a specific question: Is the host alive? What ports are open? What services are running? What operating system is in use? The results build a complete picture of the attack surface.

Recon Objectives	
Live Hosts	Confirm 192.168.100.46 is active and reachable
Open TCP Ports	Identify all listening TCP services
Open UDP Ports	Identify DNS, NFS, RPC and other UDP services
Service Versions	Determine exact software versions for vulnerability matching
Operating System	Fingerprint the OS for targeted attack planning

1.2 Host Discovery

Before performing any port scanning, the target host must first be confirmed as alive on the network. A ping scan (-sn) sends ICMP echo requests and TCP probes without scanning any ports. This confirms that 192.168.100.46 is reachable from the Kali machine at 192.168.100.38 before any further scanning begins. It is the least intrusive active check and produces no port-level noise in target logs.

```
sudo nmap -sn 192.168.100.46
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -sn 192.168.100.46
[sudo] password for kali:
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-28 08:42 -0500
Nmap scan report for 192.168.100.46
Host is up (0.00062s latency).
MAC Address: 00:0C:29:71:14:98 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.66 seconds
```

Figure 1: Host Discovery — sudo nmap -sn 192.168.100.46 confirming the target is alive

1.3 Basic TCP Connect Scan (-sT)

A TCP Connect scan completes the full three-way handshake for each probed port. Unlike a SYN scan . This scan type is more detectable since it generates complete connection entries in target logs, but it is useful as a baseline. This scan was saved to XML for later comparison with ndiff.

```
nmap -sT --top-ports 1000 192.168.100.46 -oA essential_scan
```

```
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
```

Figure 2: TCP Connect Scan (-sT) — open ports identified on the target host

1.4 SYN Scan with Version and OS Detection (-sS -sV -O)

The SYN scan (half-open scan) sends TCP SYN packets without completing the handshake resulting in less log noise on the target than a Connect scan . Combined with -sV (version detection) and -O (OS fingerprinting), this is the most informative standard Nmap scan. The -A flag enables additional scripts and traceroute. Output is saved in all formats for archiving and comparison.

```
sudo nmap -sS -sV -O -A -T5 -p- --reason --max-retries 5 192.168.100.46 -oA essential_syn
```

```
└─$ sudo nmap -sS -sV -O -A -T5 -p- --reason --max-retries 5 192.168.100.46

[sudo] password for kali:
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-28 07:29 -0500
Nmap scan report for 192.168.100.46
Host is up, received arp-response (0.00076s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE     REASON         VERSION
21/tcp    open  ftp         syn-ack ttl 64 vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.100.38
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh         syn-ack ttl 64 OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| 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)
```

Figure 3: SYN Scan Part 1

```
|   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)
23/tcp    open  telnet      syn-ack ttl 64 Linux telnetd
25/tcp    open  smtp        syn-ack ttl 64 Postfix smtpd
|_ssl-date: 2026-02-25T04:33:19+00:00; -3d07h59m03s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is n
o such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|_    SSL2_RC2_128_CBC_WITH_MD5
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODE
S, 8BITMIME, DSN
53/tcp    open  domain      syn-ack ttl 64 ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp    open  http        syn-ack ttl 64 Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
```

Figure 4: SYN Scan Part 2

```
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp   open  rpcbind     syn-ack ttl 64 2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      44917/tcp   mountd
|   100005  1,2,3      54376/udp   mountd
|   100021  1,3,4      50870/udp   nlockmgr
|   100021  1,3,4      52765/tcp   nlockmgr
|   100024  1          37888/udp   status
|_  100024  1          40331/tcp   status
139/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp   open  exec        syn-ack ttl 64 netkit-rsh rexecd
513/tcp   open  login?      syn-ack ttl 64
514/tcp   open  tcpwrapped  syn-ack ttl 64
1099/tcp  open  java-rmi    syn-ack ttl 64 GNU Classpath grmiregistry
1524/tcp  open  bindshell   syn-ack ttl 64 Metasploitable root shell
2049/tcp  open  nfs         syn-ack ttl 64 2-4 (RPC #100003)
2121/tcp  open  ftp         syn-ack ttl 64 ProFTPD 1.3.1
3306/tcp  open  mysql       syn-ack ttl 64 MySQL 5.0.51a-3ubuntu5
```

Figure 5: SYN Scan Part 3

1.5 UDP Scan (-sU)

UDP services are often overlooked in reconnaissance because they do not respond with a SYN/ACK like TCP does. This scan targets the top 50 UDP ports and identified several open services including DNS (53), rpcbind (111), NetBIOS-NS

(137), and NFS (2049). These services represent potential attack vectors that would be invisible to TCP-only scans.

```
sudo nmap -sU -n --top-ports 50 192.168.100.46 -oA udp_top50
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -sU --top-ports 50 --reason --max-retries 3 192.168.100.46 -oA udp_top50_noscripts
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-28 09:02 -0500
Warning: 192.168.100.46 giving up on port because retransmission cap hit (3).
Nmap scan report for 192.168.100.46
Host is up, received arp-response (0.0025s latency).
Not shown: 34 open|filtered udp ports (no-response)
PORT      STATE  SERVICE       REASON
53/udp    open   domain        udp-response ttl 64
67/udp    closed dhcps         port-unreach ttl 64
80/udp    closed http          port-unreach ttl 64
111/udp   open   rpcbind       udp-response ttl 64
136/udp   closed profile       port-unreach ttl 64
137/udp   open   netbios-ns    udp-response ttl 64
139/udp   closed netbios-ssn   port-unreach ttl 64
445/udp   closed microsoft-ds  port-unreach ttl 64
631/udp   closed ipp           port-unreach ttl 64
1646/udp  closed radacct       port-unreach ttl 64
2049/udp  open   nfs           udp-response ttl 64
2222/udp  closed msantipiracy  port-unreach ttl 64
3456/udp  closed IISrpc-or-vat port-unreach ttl 64
5060/udp  closed sip           port-unreach ttl 64
49153/udp closed unknown       port-unreach ttl 64
49154/udp closed unknown       port-unreach ttl 64
MAC Address: 00:0C:29:71:14:98 (VMware)
```

Figure 6: UDP Scan (-sU) — ports 53, 111, 137, and 2049 confirmed open on UDP

1.6 Scan Comparison with ndiff

ndiff compares two saved Nmap XML output files and produces a difference report. Lines prefixed with a minus sign (-) appear only in the first scan; lines prefixed with a plus sign (+) appear only in the second. This confirms that the UDP scan revealed DNS, rpcbind, NetBIOS, and NFS services that were invisible to the TCP-only scan, validating the importance of multi-protocol reconnaissance.

```
ndiff essential_syn_noscripts.xml udp_top50_noscripts.xml | tee comparebetweenports.txt
```

```
+Nmap 7.98 scan initiated Sat Feb 28 09:02:04 2026 as: /usr/lib/nmap/nmap -sU

 192.168.100.46, 00:0C:29:71:14:98:
-Not shown: 65505 closed ports
+Not shown: 34 open|filtered ports
 PORT      STATE  SERVICE       VERSION
-21/tcp    open   ftp           vsftpd 2.3.4
-22/tcp    open   ssh           OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
-23/tcp    open   telnet        Linux telnetd
-25/tcp    open   smtp          Postfix smtpd
-53/tcp    open   domain        ISC BIND 9.4.2
+53/udp    open   domain
+67/udp    closed dhcps
-80/tcp    open   http          Apache httpd 2.2.8 ((Ubuntu) DAV/2)
+80/udp    closed http
-111/tcp   open   rpcbind       2 (RPC #100000)
+111/udp   open   rpcbind
+136/udp   closed profile
+137/udp   open   netbios-ns
-139/tcp   open   netbios-ssn   Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
+139/udp   closed netbios-ssn
-445/tcp   open   netbios-ssn   Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
+445/udp   closed microsoft-ds
-512/tcp   open   exec          netkit-rsh rexecd
-513/tcp   open   login
-514/tcp   open   tcpwrapped
+631/udp   closed ipp
-1099/tcp  open   java-rmi      GNU Classpath grmiregistry
-1524/tcp  open   bindshell     Metasploitable root shell
+1646/udp  closed radacct
-2049/tcp  open   nfs           2-4 (RPC #100003)
+2049/udp  open   nfs
-2121/tcp  open   ftp           ProFTPD 1.3.1
+2222/udp  closed msantipiracy
-3306/tcp  open   mysql         MySQL 5.0.51a-3ubuntu5
+3456/udp  closed IISrpc-or-vat
```

Figure 7: ndiff output comparing TCP SYN scan results UDP scan result

1.7 Summary of Findings

The combined TCP and UDP scans revealed a heavily exposed attack surface. The target was confirmed as Metasploitable 2.

The table below summarises the most significant services discovered.

Port	Service / Version	Protocol
21/tcp	vsftpd 2.3.4	TCP
22/tcp	OpenSSH 4.7p1	TCP
23/tcp	Linux telnetd	TCP
25/tcp	Postfix / SSLv2	TCP
80/tcp	Apache 2.2.8	TCP
139/445	Samba 3.0.20	TCP
1524/tcp	Metasploitable shell	TCP
3306/tcp	MySQL 5.0.51a	TCP
5900/tcp	VNC 3.3	TCP
53/udp	ISC BIND 9.4.2	UDP
2049/udp	NFS 2-4	UDP

SECTION 2 — BLUE TEAM: Detection and Log Analysis

2.1 Overview

The blue team perspective focuses on what a defender observes during the reconnaissance activity described in Section 1. Effective detection requires correlating multiple log sources simultaneously — no single tool sees the complete picture. multiple log sources — firewall, IDS, host-based logs, and network flow data to construct a complete picture of the attacker's activity.

2.2 IDS Alert (Suricata fast.log)

Suricata was active on the network segment during the scan. The fast.log output below shows a dense sequence of TCPv4 invalid checksum alerts generated in response to the Nmap SYN scan packets. The alerts fire at a rate of several per second, clearly distinguishing automated scanning behaviour from normal traffic. The source IP 192.168.100.38 and destination 192.168.100.46 are visible throughout the log, confirming the scan was detected at the IDS layer.

```
kazim@kazim:~$ cat ~/suricata_alerts/fast.log
02/28/2026-12:31:08.414008  [**] [1:2200074:2] SURICATA TCPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.38:52416 -> 192.168.100.46:57171
02/28/2026-12:31:08.414731  [**] [1:2200074:2] SURICATA TCPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.38:52416 -> 192.168.100.46:57171
02/28/2026-12:31:08.414951  [**] [1:2200074:2] SURICATA TCPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.38:52416 -> 192.168.100.46:57171
02/28/2026-12:30:45.884129  [**] [1:2200074:2] SURICATA TCPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.38:53400 -> 192.168.100.46:57171
02/28/2026-12:30:45.884336  [**] [1:2200074:2] SURICATA TCPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.38:53416 -> 192.168.100.46:57171
02/28/2026-12:30:45.884918  [**] [1:2200074:2] SURICATA TCPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.38:53416 -> 192.168.100.46:57171
02/28/2026-12:30:45.885093  [**] [1:2200074:2] SURICATA TCPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.38:53416 -> 192.168.100.46:57171
02/28/2026-12:30:53.392513  [**] [1:2200074:2] SURICATA TCPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.38:53416 -> 192.168.100.46:57171
02/28/2026-12:30:53.392709  [**] [1:2200074:2] SURICATA TCPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.38:58074 -> 192.168.100.46:57171
02/28/2026-12:30:53.393129  [**] [1:2200074:2] SURICATA TCPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.38:58074 -> 192.168.100.46:57171
02/28/2026-12:30:53.393314  [**] [1:2200074:2] SURICATA TCPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.38:58074 -> 192.168.100.46:57171
02/28/2026-12:31:13.420292  [**] [1:2200074:2] SURICATA TCPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.38:52416 -> 192.168.100.46:57171
02/28/2026-12:30:53.668053  [**] [1:2200075:2] SURICATA UDPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {UDP} 192.168.100.38:43013 -> 194.225.150.25:123
02/28/2026-12:31:13.420526  [**] [1:2200074:2] SURICATA TCPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.38:52432 -> 192.168.100.46:57171
02/28/2026-12:31:13.421132  [**] [1:2200074:2] SURICATA TCPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.38:52432 -> 192.168.100.46:57171
02/28/2026-12:30:58.399271  [**] [1:2200074:2] SURICATA TCPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.38:58074 -> 192.168.100.46:57171
02/28/2026-12:31:13.421341  [**] [1:2200074:2] SURICATA TCPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.38:52432 -> 192.168.100.46:57171
02/28/2026-12:30:58.399476  [**] [1:2200074:2] SURICATA TCPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.38:58088 -> 192.168.100.46:57171
02/28/2026-12:30:58.400008  [**] [1:2200074:2] SURICATA TCPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.38:58088 -> 192.168.100.46:57171
02/28/2026-12:30:58.400243  [**] [1:2200074:2] SURICATA TCPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.38:58088 -> 192.168.100.46:57171
02/28/2026-12:31:18.425813  [**] [1:2200074:2] SURICATA TCPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.38:52432 -> 192.168.100.46:57171
02/28/2026-12:31:03.405928  [**] [1:2200074:2] SURICATA TCPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.38:58088 -> 192.168.100.46:57171
02/28/2026-12:31:03.406280  [**] [1:2200074:2] SURICATA TCPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.38:58090 -> 192.168.100.46:57171
02/28/2026-12:31:03.407426  [**] [1:2200074:2] SURICATA TCPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.38:58090 -> 192.168.100.46:57171
02/28/2026-12:31:03.407912  [**] [1:2200074:2] SURICATA TCPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.38:58090 -> 192.168.100.46:57171
02/28/2026-12:31:03.613585  [**] [1:2200074:2] SURICATA TCPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.38:58088 -> 192.168.100.46:57171
02/28/2026-12:31:08.413738  [**] [1:2200074:2] SURICATA TCPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.38:58090 -> 192.168.100.46:57171
02/28/2026-12:31:18.426072  [**] [1:2200074:2] SURICATA TCPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.38:58754 -> 192.168.100.46:57171
02/28/2026-12:31:18.426578  [**] [1:2200074:2] SURICATA TCPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.38:58754 -> 192.168.100.46:57171
02/28/2026-12:31:18.426830  [**] [1:2200074:2] SURICATA TCPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.38:58754 -> 192.168.100.46:57171
02/28/2026-12:31:25.918022  [**] [1:2200075:2] SURICATA UDPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {UDP} 192.168.100.38:34090 -> 194.225.150.25:123
02/28/2026-12:31:23.432164  [**] [1:2200074:2] SURICATA TCPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.38:58754 -> 192.168.100.46:57171
02/28/2026-12:31:23.432357  [**] [1:2200074:2] SURICATA TCPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.38:58762 -> 192.168.100.46:57171
02/28/2026-12:31:23.432796  [**] [1:2200074:2] SURICATA TCPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.38:58762 -> 192.168.100.46:57171
02/28/2026-12:31:23.433013  [**] [1:2200074:2] SURICATA TCPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.38:58762 -> 192.168.100.46:57171
02/28/2026-12:31:28.439118  [**] [1:2200074:2] SURICATA TCPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.38:58762 -> 192.168.100.46:57171
02/28/2026-12:31:28.439321  [**] [1:2200074:2] SURICATA TCPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.38:57756 -> 192.168.100.46:57171
02/28/2026-12:31:28.439943  [**] [1:2200074:2] SURICATA TCPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.38:57756 -> 192.168.100.46:57171
02/28/2026-12:31:28.440233  [**] [1:2200074:2] SURICATA TCPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.38:57756 -> 192.168.100.46:57171
02/28/2026-12:31:38.452487  [**] [1:2200074:2] SURICATA TCPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.38:45790 -> 192.168.100.46:57171
02/28/2026-12:31:33.445822  [**] [1:2200074:2] SURICATA TCPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.38:57756 -> 192.168.100.46:57171
02/28/2026-12:31:38.453144  [**] [1:2200074:2] SURICATA TCPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.38:45790 -> 192.168.100.46:57171
02/28/2026-12:31:33.446079  [**] [1:2200074:2] SURICATA TCPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.38:57770 -> 192.168.100.46:57171
02/28/2026-12:31:38.453342  [**] [1:2200074:2] SURICATA TCPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.38:45790 -> 192.168.100.46:57171
02/28/2026-12:31:33.446781  [**] [1:2200074:2] SURICATA TCPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.38:57770 -> 192.168.100.46:57171
02/28/2026-12:31:33.447071  [**] [1:2200074:2] SURICATA TCPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.38:57770 -> 192.168.100.46:57171
02/28/2026-12:31:38.452282  [**] [1:2200074:2] SURICATA TCPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.38:57770 -> 192.168.100.46:57171
02/28/2026-12:31:50.967479  [**] [1:2200074:2] SURICATA TCPv4 invalid checksum [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.100.38:54346 -> 192.168.100.46:57171
```

Figure 8: Suricata fast.log — TCPv4

2.3 Firewall Logs

Two sources of firewall evidence were captured. The first shows the Windows Defender Firewall configuration confirming that inbound connections that do not match a rule are blocked across Domain, Private, and Public profiles — meaning the scan traffic would have been visible and partially blocked at the host firewall level. The second shows the pfirewall.log file capturing detailed entries of allowed and dropped TCP connections, with DROP entries visible for traffic from 192.168.100.38 to the target on port 37325 and sequential ports.

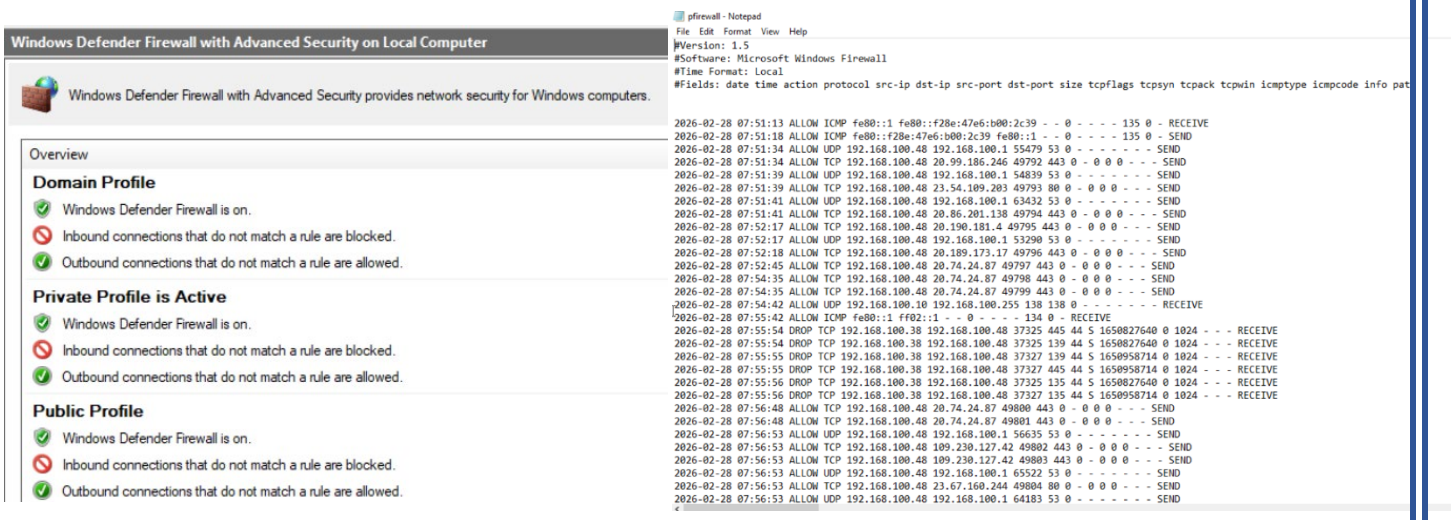
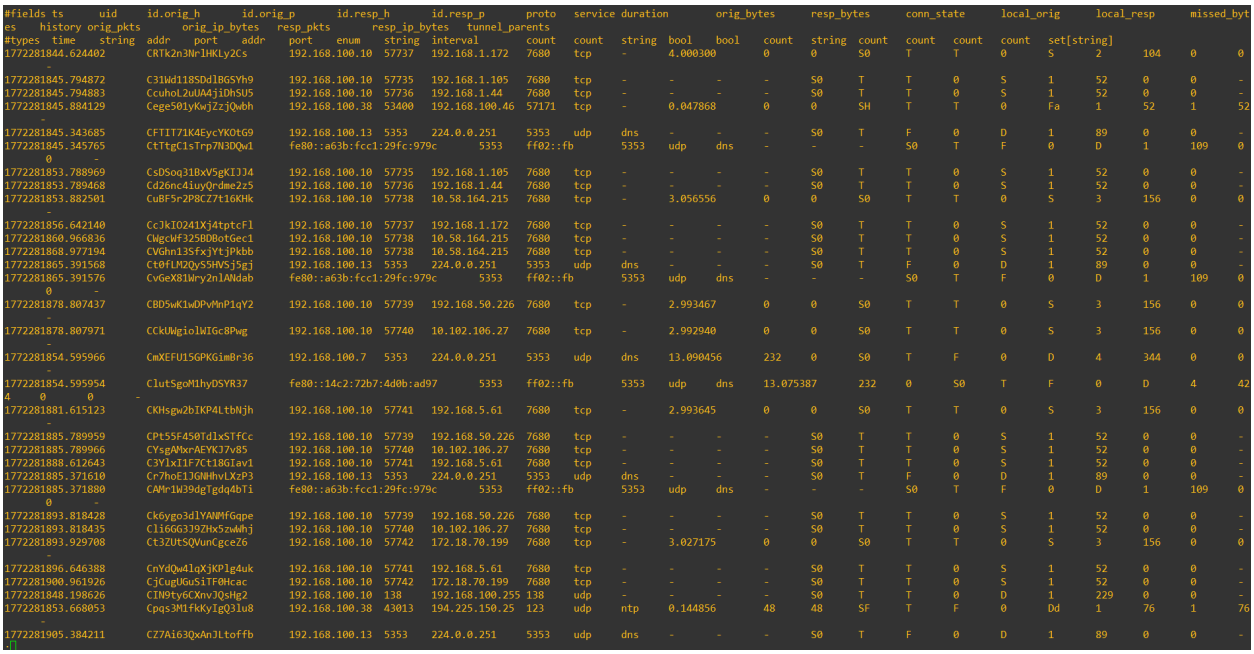


Figure 9: Windows Defender Firewall active on all profiles and Windows pfirewall.log

2.4 Zeek Network Logs

Zeek was deployed to capture and parse all traffic during the exercise. The conn.log table below records every observed connection attempt. Key indicators of port scanning are visible: source port 53422 remains constant across all entries, all durations are zero or near-zero, and the orig_bytes and resp_bytes fields are 0 for almost every entry confirming that no data was transferred.

```
/usr/bin/zeek -r ~/logs.pcap | cat conn.log
```



```
#fields ts      uid     id.orig_h       id.orig_p       id.resp_h       id.resp_p       proto   service duration        orig_bytes      resp_bytes      conn_state      local_orig      local_resp      missed_byt
es      history orig_pkts       orig_ip_bytes   resp_pkts       resp_ip_bytes   tunnel_parents
#types  time    string  addr    port    addr    port    enum    string  interval        count   count   string  bool    bool    count   string  count   count   count   count   set[string]
1772281844.624402       CRTk2n3NrlHKLy2Cs       192.168.100.10  57737   192.168.1.172   7680    tcp     -       4.000300        0       0       S0      T       T       0       S       2       104     0       0
       -
1772281845.794872       C31Wd118SDdlBGSYh9      192.168.100.10  57735   192.168.1.105   7680    tcp     -       -       -       -       S0      T       T       0       S       1       52      0       0       -
1772281845.794883       CcuhoL2uUA4jiDhSU5      192.168.100.10  57736   192.168.1.44    7680    tcp     -       -       -       -       S0      T       T       0       S       1       52      0       0       -
1772281845.884129       Cege501yKwjZzjQwbh      192.168.100.38  53400   192.168.100.46  57171   tcp     -       0.047868        0       0       SH      T       T       0       Fa      1       52      1       52
       -
1772281845.343685       CFTIT71K4EycYKOtG9      192.168.100.13  5353    224.0.0.251     5353    udp     dns     -       -       -       S0      T       F       0       D       1       89      0       0       -
1772281845.345765       CtTtgC1sTrp7N3DQw1      fe80::a63b:fcc1:29fc:979c       5353    ff02::fb        5353    udp     dns     -       -       -       S0      T       F       0       D       1       109     0
       0       -
1772281853.788969       CsDSoq31BxV5gKIJ34      192.168.100.10  57735   192.168.1.105   7680    tcp     -       -       -       -       S0      T       T       0       S       1       52      0       0       -
1772281853.789468       Cd26nc4iuyQrdme2z5      192.168.100.10  57736   192.168.1.44    7680    tcp     -       -       -       -       S0      T       T       0       S       1       52      0       0       -
1772281853.882501       CuBF5r2P8CZ7t16KHk      192.168.100.10  57738   10.58.164.215   7680    tcp     -       3.056556        0       0       S0      T       T       0       S       3       156     0       0
       -
1772281856.642140       CcJkIO241Xj4tptcFl      192.168.100.10  57737   192.168.1.172   7680    tcp     -       -       -       -       S0      T       T       0       S       1       52      0       0       -
1772281860.966836       CWgcWf325BDBotGec1      192.168.100.10  57738   10.58.164.215   7680    tcp     -       -       -       -       S0      T       T       0       S       1       52      0       0       -
1772281868.977194       CVGhn13SfxjYtjPkbb      192.168.100.10  57738   10.58.164.215   7680    tcp     -       -       -       -       S0      T       T       0       S       1       52      0       0       -
1772281865.391568       Ct0flM2QyS5HVSj5gj      192.168.100.13  5353    224.0.0.251     5353    udp     dns     -       -       -       S0      T       F       0       D       1       89      0       0       -
1772281865.391576       CvGeX81Wry2nlANdab      fe80::a63b:fcc1:29fc:979c       5353    ff02::fb        5353    udp     dns     -       -       -       S0      T       F       0       D       1       109     0
       0       -
1772281878.807437       CBD5wK1wDPvMnP1qY2      192.168.100.10  57739   192.168.50.226  7680    tcp     -       2.993467        0       0       S0      T       T       0       S       3       156     0       0
       -
1772281878.807971       CCkUWgiolWIGc8Pwg       192.168.100.10  57740   10.102.106.27   7680    tcp     -       2.992940        0       0       S0      T       T       0       S       3       156     0       0
       -
1772281854.595966       CmXEFU1SGPKGimBr36      192.168.100.7   5353    224.0.0.251     5353    udp     dns     13.090456       232     0       S0      T       F       0       D       4       344     0       0
       -
1772281854.595954       ClutSgoM1hyDSYR37       fe80::14c2:72b7:4d0b:ad97       5353    ff02::fb        5353    udp     dns     13.075387       232     0       S0      T       F       0       D       4       42
4       0       0       -
1772281881.615123       CKHsgw2bIKP4LtbNjh      192.168.100.10  57741   192.168.5.61    7680    tcp     -       2.993645        0       0       S0      T       T       0       S       3       156     0       0
       -
1772281885.789959       CPt55F450Td1xSTfCc      192.168.100.10  57739   192.168.50.226  7680    tcp     -       -       -       -       S0      T       T       0       S       1       52      0       0       -
1772281885.789966       CYsgAMxrAEYKJ7v85       192.168.100.10  57740   10.102.106.27   7680    tcp     -       -       -       -       S0      T       T       0       S       1       52      0       0       -
1772281888.612643       C3YlxI1F7Ct18GIav1      192.168.100.10  57741   192.168.5.61    7680    tcp     -       -       -       -       S0      T       T       0       S       1       52      0       0       -
1772281885.371610       Cr7hoE1JGNHhvLXzP3      192.168.100.13  5353    224.0.0.251     5353    udp     dns     -       -       -       S0      T       F       0       D       1       89      0       0       -
1772281885.371880       CAMr1W39dgTgdq4bTi      fe80::a63b:fcc1:29fc:979c       5353    ff02::fb        5353    udp     dns     -       -       -       S0      T       F       0       D       1       109     0
       0       -
1772281893.818428       Ck6ygo3dlYANMfGqpe      192.168.100.10  57739   192.168.50.226  7680    tcp     -       -       -       -       S0      T       T       0       S       1       52      0       0       -
1772281893.818435       Cli6GG3J9ZHx5zwWhj      192.168.100.10  57740   10.102.106.27   7680    tcp     -       -       -       -       S0      T       T       0       S       1       52      0       0       -
1772281893.929708       Ct3ZUtSQVunCgceZ6       192.168.100.10  57742   172.18.70.199   7680    tcp     -       3.027175        0       0       S0      T       T       0       S       3       156     0       0
       -
1772281896.646388       CnYdQw41qXjKPlg4uk      192.168.100.10  57741   192.168.5.61    7680    tcp     -       -       -       -       S0      T       T       0       S       1       52      0       0       -
1772281900.961926       CjCugUGuSiTF0Hcac       192.168.100.10  57742   172.18.70.199   7680    tcp     -       -       -       -       S0      T       T       0       S       1       52      0       0       -
1772281848.198626       CIN9ty6CXnvJQsHg2       192.168.100.10  138     192.168.100.255 138     udp     -       -       -       -       S0      T       T       0       D       1       229     0       0       -
1772281853.668053       Cpqs3M1fkKyIgQ3lu8      192.168.100.38  43013   194.225.150.25  123     udp     ntp     0.144856        48      48      SF      T       F       0       Dd      1       76      1       76
       -
1772281905.384211       CZ7Ai63QxAnJLtoffb      192.168.100.13  5353    224.0.0.251     5353    udp     dns     -       -       -       S0      T       F       0       D       1       89      0       0       -
```

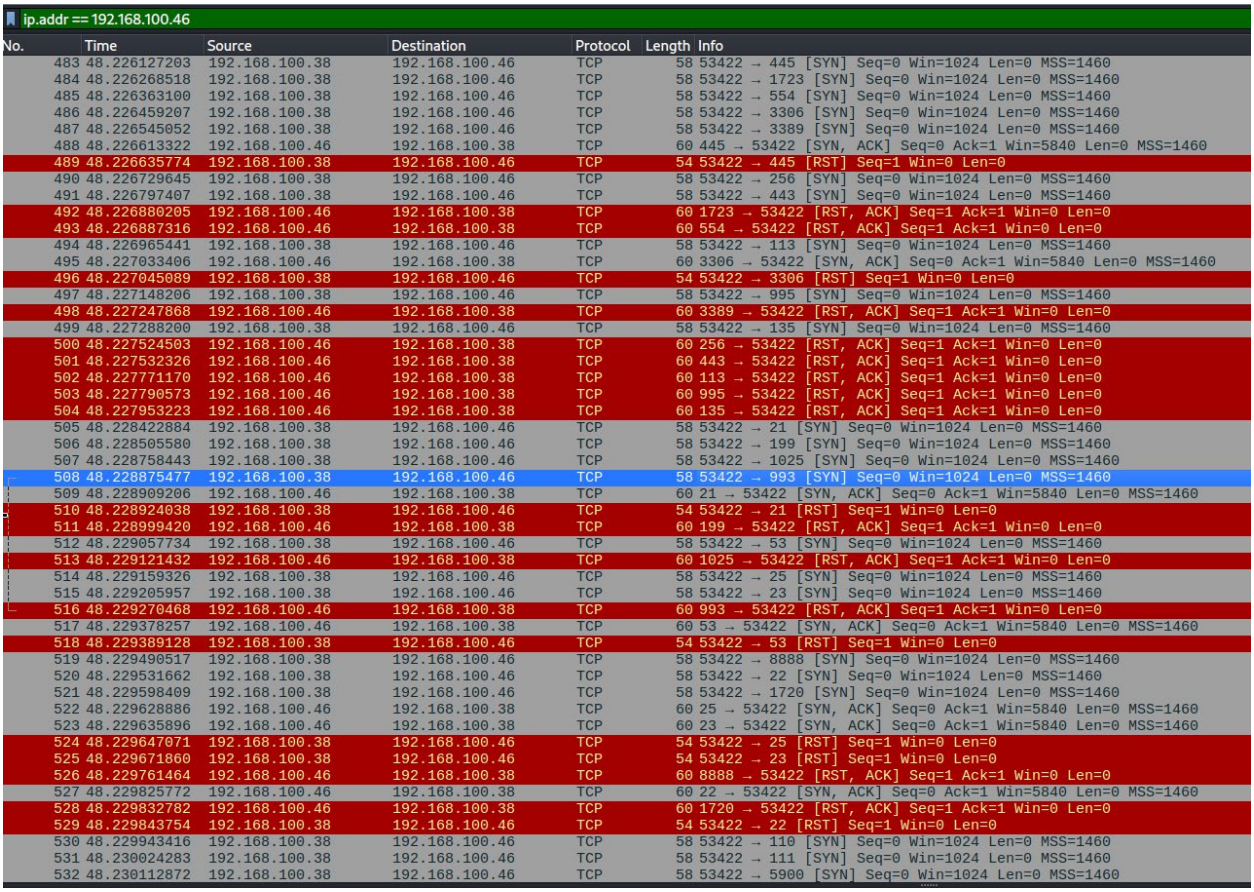
Figure 11: Zeek conn.log

Zeek Connection States — What They Mean During a Scan	
S0	SYN sent, no response — port is filtered or host unreachable
REJ	Port closed — target sent RST; probe rejected
RSTO	Scanner sent RST after receiving SYN/ACK — half-open scan
SF	Full connection established — port is open and service responded
SH	SYN sent, SYN/ACK received, half-open (no final ACK from scanner)

2.5 Wireshark Packet Capture Analysis

The Wireshark capture confirms the half-open SYN scan pattern at the packet level. The scanner at 192.168.100.38 sends SYN packets to sequential destination ports on 192.168.100.46. When an open port (such as port 445) responds with SYN/ACK, the scanner immediately sends RST rather than completing the handshake the

defining characteristic of an Nmap -sS scan. Closed ports respond with RST/ACK directly. The rapid succession of packets within milliseconds confirms automated rather than human activity.



ip.addr == 192.168.100.46

No.	Time	Source	Destination	Protocol	Length	Info
483	48.226127203	192.168.100.38	192.168.100.46	TCP	58	53422 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
484	48.226268518	192.168.100.38	192.168.100.46	TCP	58	53422 → 1723 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
485	48.226363100	192.168.100.38	192.168.100.46	TCP	58	53422 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
486	48.226459207	192.168.100.38	192.168.100.46	TCP	58	53422 → 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
487	48.226545052	192.168.100.38	192.168.100.46	TCP	58	53422 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
488	48.226613322	192.168.100.46	192.168.100.38	TCP	60	445 → 53422 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
489	48.226635774	192.168.100.38	192.168.100.46	TCP	54	53422 → 445 [RST] Seq=1 Win=0 Len=0
490	48.226729645	192.168.100.38	192.168.100.46	TCP	58	53422 → 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
491	48.226797407	192.168.100.38	192.168.100.46	TCP	58	53422 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
492	48.226880205	192.168.100.46	192.168.100.38	TCP	60	1723 → 53422 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
493	48.226887316	192.168.100.46	192.168.100.38	TCP	60	554 → 53422 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
494	48.226965441	192.168.100.38	192.168.100.46	TCP	58	53422 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
495	48.227033406	192.168.100.46	192.168.100.38	TCP	60	3306 → 53422 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
496	48.227045089	192.168.100.38	192.168.100.46	TCP	54	53422 → 3306 [RST] Seq=1 Win=0 Len=0
497	48.227148206	192.168.100.38	192.168.100.46	TCP	58	53422 → 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
498	48.227247868	192.168.100.46	192.168.100.38	TCP	60	3389 → 53422 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
499	48.227288200	192.168.100.38	192.168.100.46	TCP	58	53422 → 135 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
500	48.227524503	192.168.100.46	192.168.100.38	TCP	60	256 → 53422 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
501	48.227532326	192.168.100.46	192.168.100.38	TCP	60	443 → 53422 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
502	48.227771170	192.168.100.46	192.168.100.38	TCP	60	113 → 53422 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
503	48.227790573	192.168.100.46	192.168.100.38	TCP	60	995 → 53422 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
504	48.227953223	192.168.100.46	192.168.100.38	TCP	60	135 → 53422 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
505	48.228422884	192.168.100.38	192.168.100.46	TCP	58	53422 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
506	48.228505580	192.168.100.38	192.168.100.46	TCP	58	53422 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
507	48.228758443	192.168.100.38	192.168.100.46	TCP	58	53422 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
508	48.228875477	192.168.100.38	192.168.100.46	TCP	58	53422 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
509	48.228909206	192.168.100.46	192.168.100.38	TCP	60	21 → 53422 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
510	48.228924038	192.168.100.38	192.168.100.46	TCP	54	53422 → 21 [RST] Seq=1 Win=0 Len=0
511	48.228999420	192.168.100.46	192.168.100.38	TCP	60	199 → 53422 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
512	48.229057734	192.168.100.38	192.168.100.46	TCP	58	53422 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
513	48.229121432	192.168.100.46	192.168.100.38	TCP	60	1025 → 53422 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
514	48.229159326	192.168.100.38	192.168.100.46	TCP	58	53422 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
515	48.229205957	192.168.100.38	192.168.100.46	TCP	58	53422 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
516	48.229270468	192.168.100.46	192.168.100.38	TCP	60	993 → 53422 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
517	48.229378257	192.168.100.46	192.168.100.38	TCP	60	53 → 53422 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
518	48.229389128	192.168.100.38	192.168.100.46	TCP	54	53422 → 53 [RST] Seq=1 Win=0 Len=0
519	48.229490517	192.168.100.38	192.168.100.46	TCP	58	53422 → 8888 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
520	48.229531662	192.168.100.38	192.168.100.46	TCP	58	53422 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
521	48.229598409	192.168.100.38	192.168.100.46	TCP	58	53422 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
522	48.229628886	192.168.100.46	192.168.100.38	TCP	60	25 → 53422 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
523	48.229635896	192.168.100.46	192.168.100.38	TCP	60	23 → 53422 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
524	48.229647071	192.168.100.38	192.168.100.46	TCP	54	53422 → 25 [RST] Seq=1 Win=0 Len=0
525	48.229671860	192.168.100.38	192.168.100.46	TCP	54	53422 → 23 [RST] Seq=1 Win=0 Len=0
526	48.229761464	192.168.100.46	192.168.100.38	TCP	60	8888 → 53422 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
527	48.229825772	192.168.100.46	192.168.100.38	TCP	60	22 → 53422 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
528	48.229832782	192.168.100.46	192.168.100.38	TCP	60	1720 → 53422 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
529	48.229843754	192.168.100.38	192.168.100.46	TCP	54	53422 → 22 [RST] Seq=1 Win=0 Len=0
530	48.229943416	192.168.100.38	192.168.100.46	TCP	58	53422 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
531	48.230024283	192.168.100.38	192.168.100.46	TCP	58	53422 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
532	48.230112872	192.168.100.38	192.168.100.46	TCP	58	53422 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Figure 12: Wireshark packet capture

2.6 RITA Beacon Analysis

RITA (Real Intelligence Threat Analytics) analysed the Zeek logs for beaconing behaviour — regular automated outbound communication that may indicate a compromised host. The output below shows that RITA flagged communication from 192.168.100.38 to the external IP 194.225.150.25 on UDP port 123 (NTP) with a severity of High and a beacon score of 99.50%.

```
rita import ~/zeek_logs/ purple_lab_dataset
```

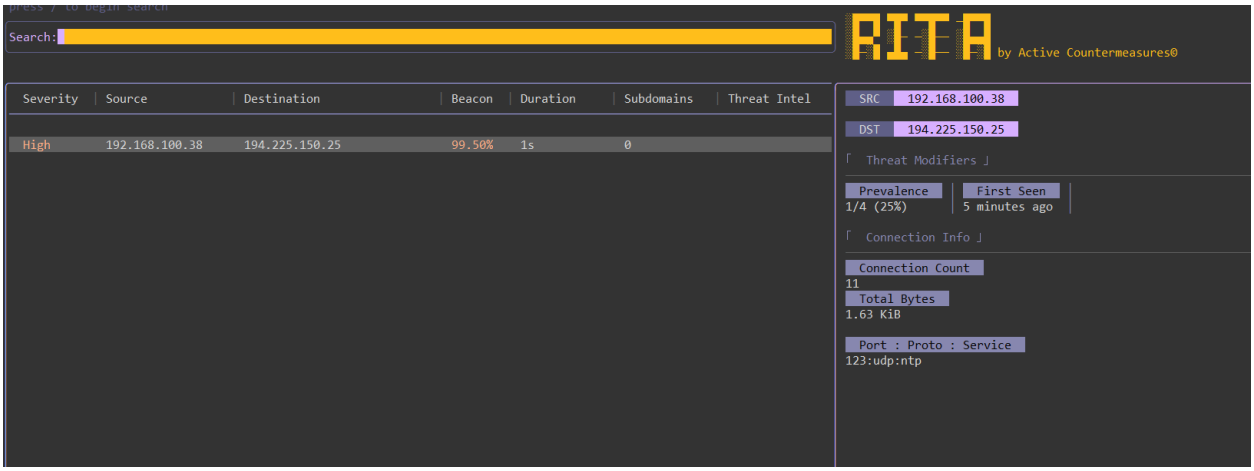


Figure 13: RITA dashboard

Blue Team Detection Summary	
IDS (Suricata)	Detected hundreds of alerts during SYN scan
Firewall	Detected DROP entries visible in pfirewall.log
Zeek conn.log	Detected zero-duration connections across sequential ports
Wireshark	Confirmed SYN/RST half-open handshake pattern visible
RITA	Detected 99.50% beacon score on NTP traffic
UDP Scan	Partial Zeek logged, IDS had fewer alerts

SECTION 3 — PURPLE TEAM: Detection Gap Analysis

3.1 Purpose of the Purple Team Exercise

The purple team phase brings red and blue team findings together. Rather than operating in isolation, both sides compare what the attacker did against what the defender detected. The objective is to identify gaps — attacks that succeeded without triggering any alert and to improve detection coverage as a result.

3.2 Detection Coverage

Red Team Action	Detection Status
TCP SYN scan (-sS)	Detected — Suricata + Wireshark
TCP Connect scan (-sT)	Detected — Firewall + Zeek
UDP scan (-sU)	Partial — Zeek logged, fewer IDS hits
OS detection (-O)	Partially detected
Version detection (-sV)	Often missed
NTP beaconing	Detected by RITA (99.50%)

SECTION 4 — CONCLUSION

Summary

This laboratory exercise demonstrated the complete reconnaissance lifecycle against a vulnerable target host. The red team successfully enumerated over 30 open services using a structured sequence of Nmap scans. Blue team monitoring confirmed that TCP SYN scanning is reliably detected when Suricata rules and firewall logging are properly configured. Zeek and Wireshark provided packet-level and flow-level confirmation of the half-open scan pattern. RITA detected high-confidence beaconing in the Zeek logs with a 99.50% score. The purple team exercise identified UDP scanning and service version detection as persistent blind spots requiring rule additions and baselining work.

The central lesson is that no single tool provides complete visibility. Effective defence requires IDS, firewall logging, network flow analysis, and behavioural analytics working together . The screenshots in this report demonstrate that monitoring was active and functional throughout the exercise, with evidence of scan detection across four independent tool categories.