Advanced Network Defense Infrastructure

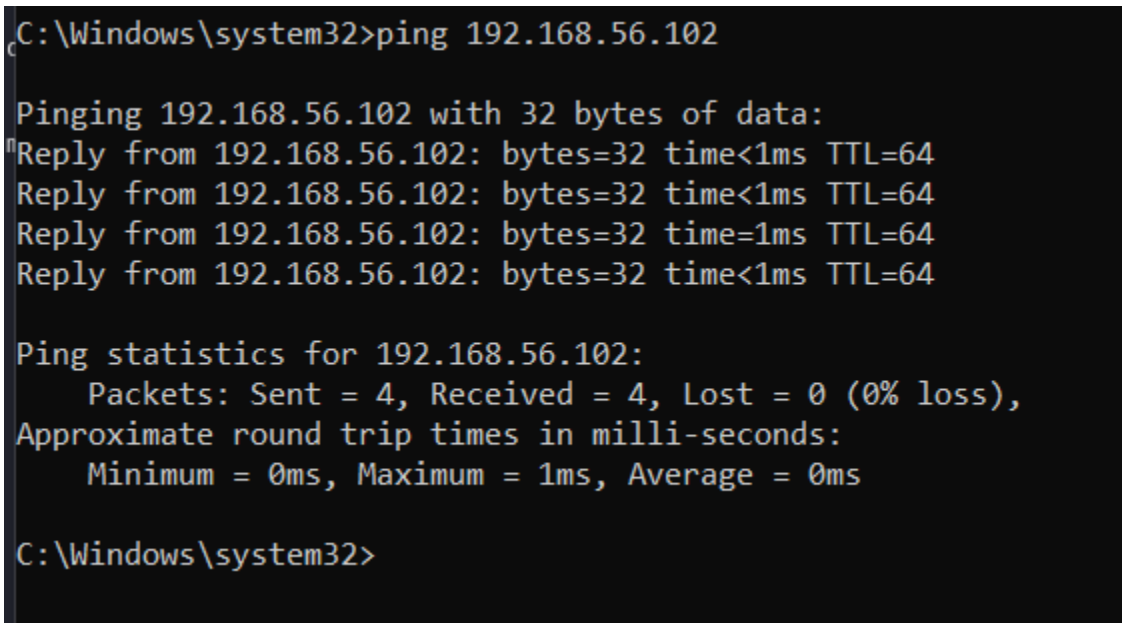
Installation

2 Custom Rules

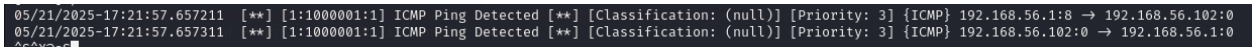
These rules generate alerts when:

- Any ICMP packet is detected (simulates basic ping sweep)
- An HTTP request targets a specific host (basic application layer detection

Connectivity



IDS Detection



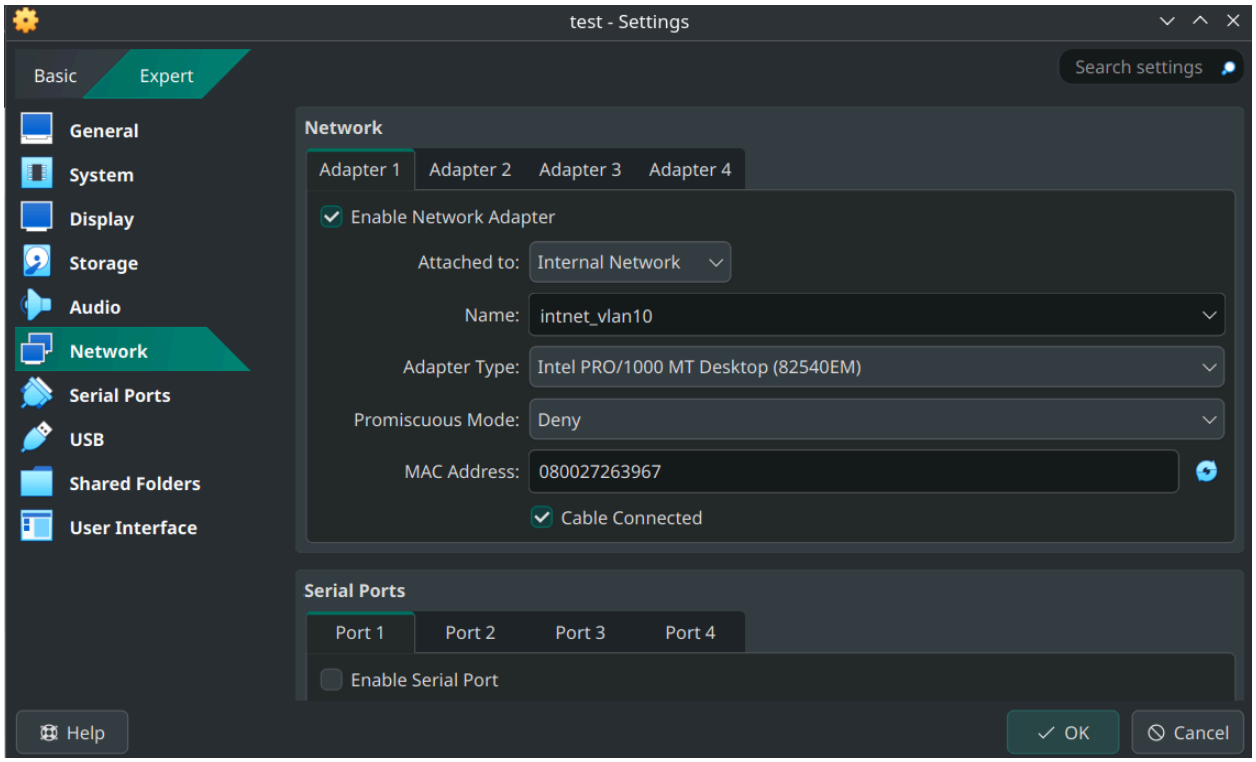
The ICMP rule was generating alerts for all ICMP traffic, including benign network monitoring tools or legitimate pings.

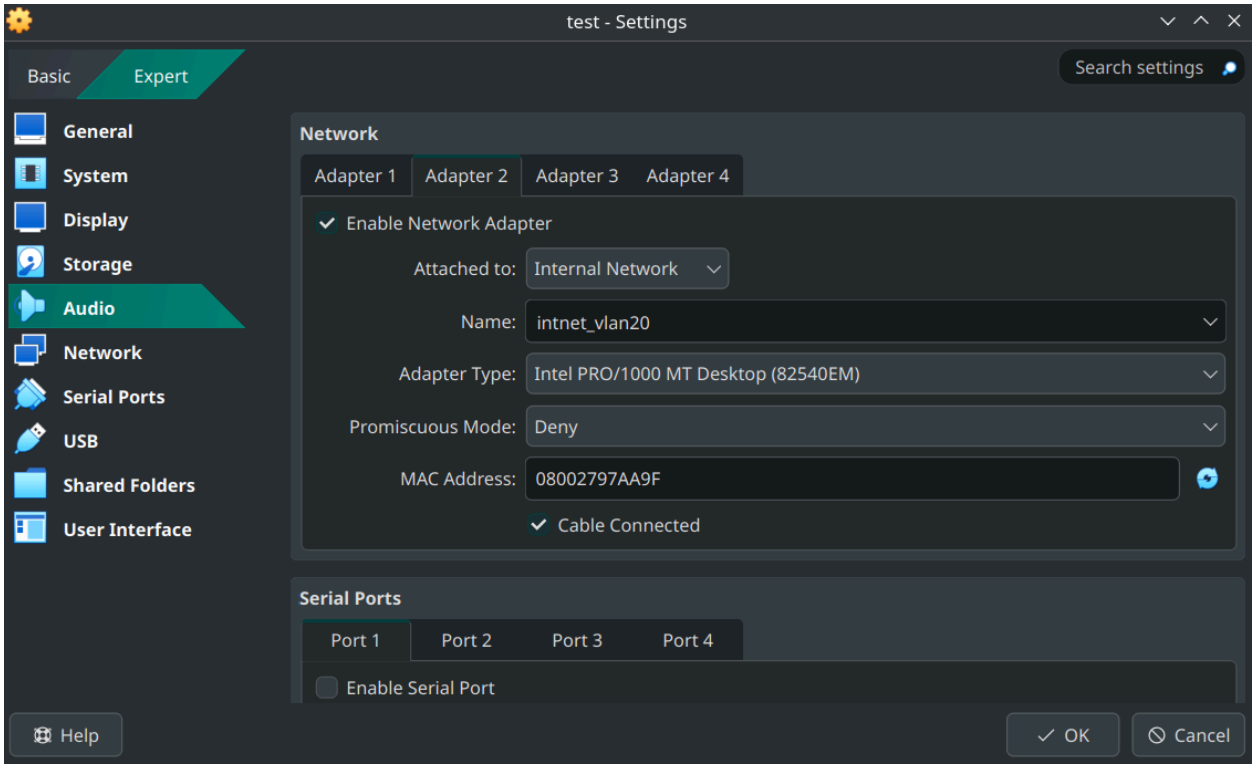
Defense Automation Script

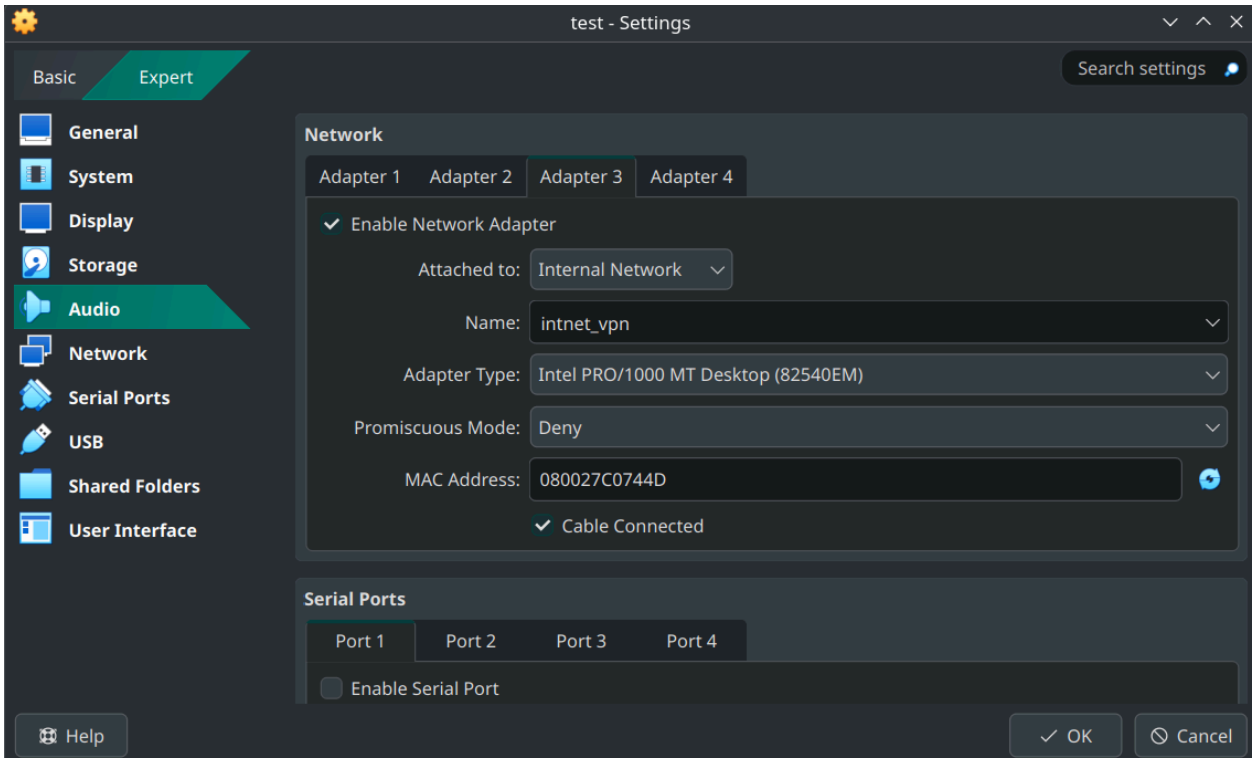
```
#!/bin/bash

LOGFILE="/var/log/suricata/fast.log"

tail -Fn0 $LOGFILE | \
while read line ; do
    if echo "$line" | grep -q "ICMP Echo Request Detected"; then
        # Extract source IP (6th field in log line, before colon)
        IP=$(echo "$line" | awk '{print $6}' | cut -d':' -f1)
        echo "$(date): Blocking IP $IP due to suspicious activity."
        sudo iptables -A INPUT -s $IP -j DROP
    fi
done
```

Advanced Network Architecture

Network Setup in Virtual Box







IP Configuration

```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 192.168.1.79/24
                                  v6/DHCP6: 2600:480a:2a11:6300:a00:27ff:fe4e:a2
a3/64
 LAN (lan)       -> em1        -> v4: 192.168.1.1/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure:
```

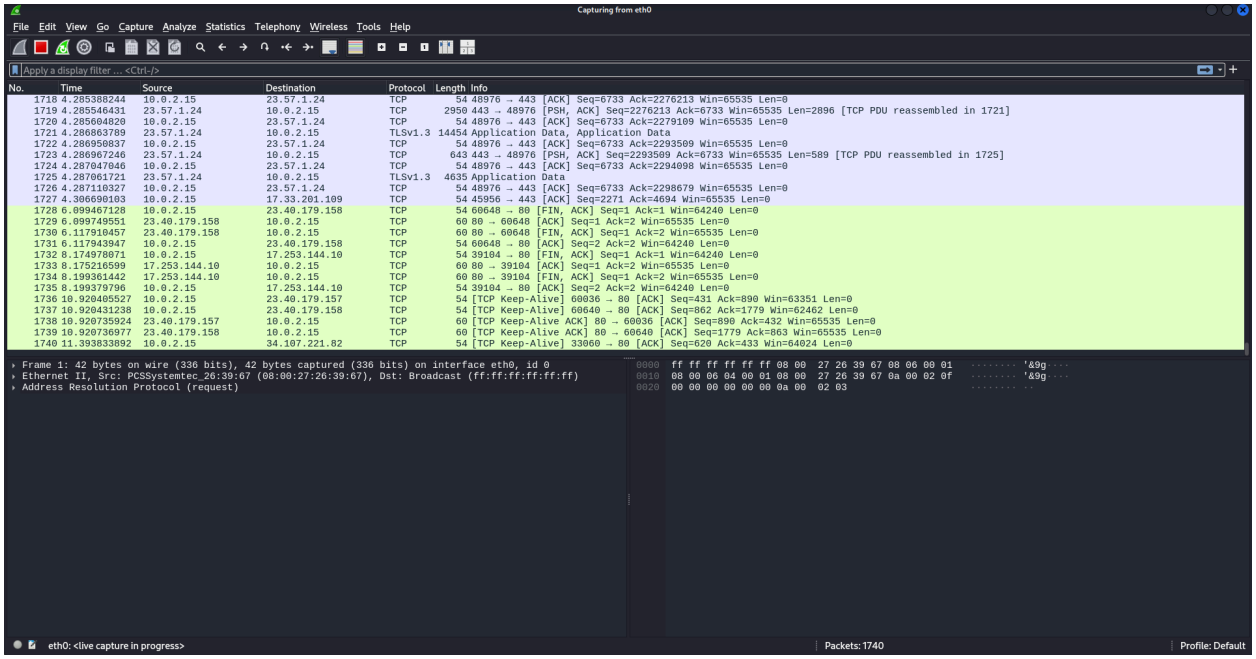
Logs

```
Jun  2 10:13:13 pfSense filterlog[61235]: 69,,,12009,em0,match,block,in,4,0xc0,,
1,6333,0,none,2,igmp,32,192.168.1.1,224.0.0.1,datalength=8
Jun  2 10:13:26 pfSense filterlog[61235]: 69,,,12009,em0,match,block,in,4,0xc0,,
1,16768,0,none,2,igmp,32,192.168.1.1,224.0.0.1,datalength=8
Jun  2 10:13:41 pfSense filterlog[61235]: 69,,,12009,em0,match,block,in,4,0xc0,,
1,27967,0,none,2,igmp,32,192.168.1.1,224.0.0.1,datalength=8
Jun  2 10:13:59 pfSense filterlog[61235]: 69,,,12009,em0,match,block,in,4,0xc0,,
1,38344,0,none,2,igmp,32,192.168.1.1,224.0.0.1,datalength=8
Jun  2 10:14:12 pfSense filterlog[61235]: 69,,,12009,em0,match,block,in,4,0xc0,,
1,40376,0,none,2,igmp,32,192.168.1.1,224.0.0.1,datalength=8
Jun  2 10:14:32 pfSense filterlog[61235]: 69,,,12009,em0,match,block,in,4,0xc0,,
1,50911,0,none,2,igmp,32,192.168.1.1,224.0.0.1,datalength=8
Jun  2 10:16:08 pfSense filterlog[46473]: 71,,,12009,em0,match,block,in,4,0xc0,,
1,21648,0,none,2,igmp,32,192.168.1.1,224.0.0.1,datalength=8
Jun  2 10:16:21 pfSense filterlog[46473]: 71,,,12009,em0,match,block,in,4,0xc0,,
1,26297,0,none,2,igmp,32,192.168.1.1,224.0.0.1,datalength=8
Jun  2 10:16:33 pfSense filterlog[46473]: 71,,,12009,em0,match,block,in,4,0xc0,,
1,30813,0,none,2,igmp,32,192.168.1.1,224.0.0.1,datalength=8
Jun  2 10:16:44 pfSense filterlog[46473]: 71,,,12009,em0,match,block,in,4,0xc0,,
1,39357,0,none,2,igmp,32,192.168.1.1,224.0.0.1,datalength=8
Jun  2 10:16:47 pfSense filterlog[46473]: 4,,,1000000103,em0,match,block,in,4,0x
c0,,1,57688,0,none,1,icmp,36,1.1.168.192,224.0.0.1,routeradv22:30,1,16
SJun  2 10:16:57 pfSense filterlog[46473]: 71,,,12009,em0,match,block,in,4,0xc0,
,1,46446,0,none,2,igmp,32,192.168.1.1,224.0.0.1,datalength=8
S
```

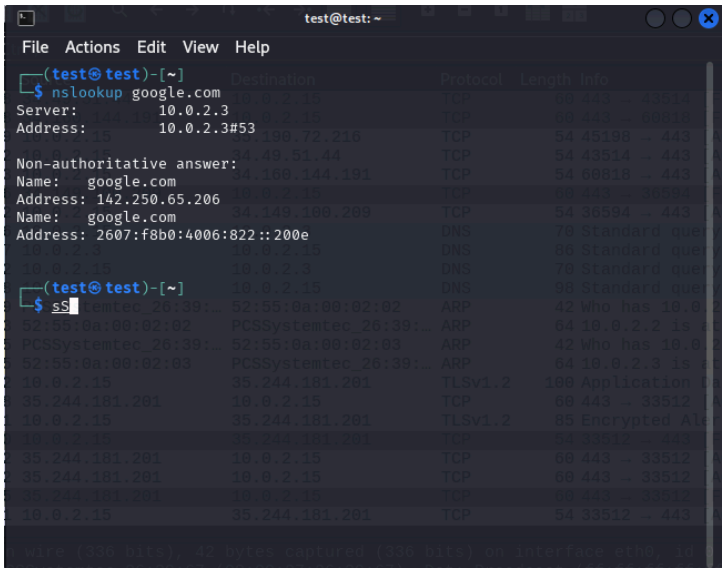
Network Protocol & Traffic Analysis

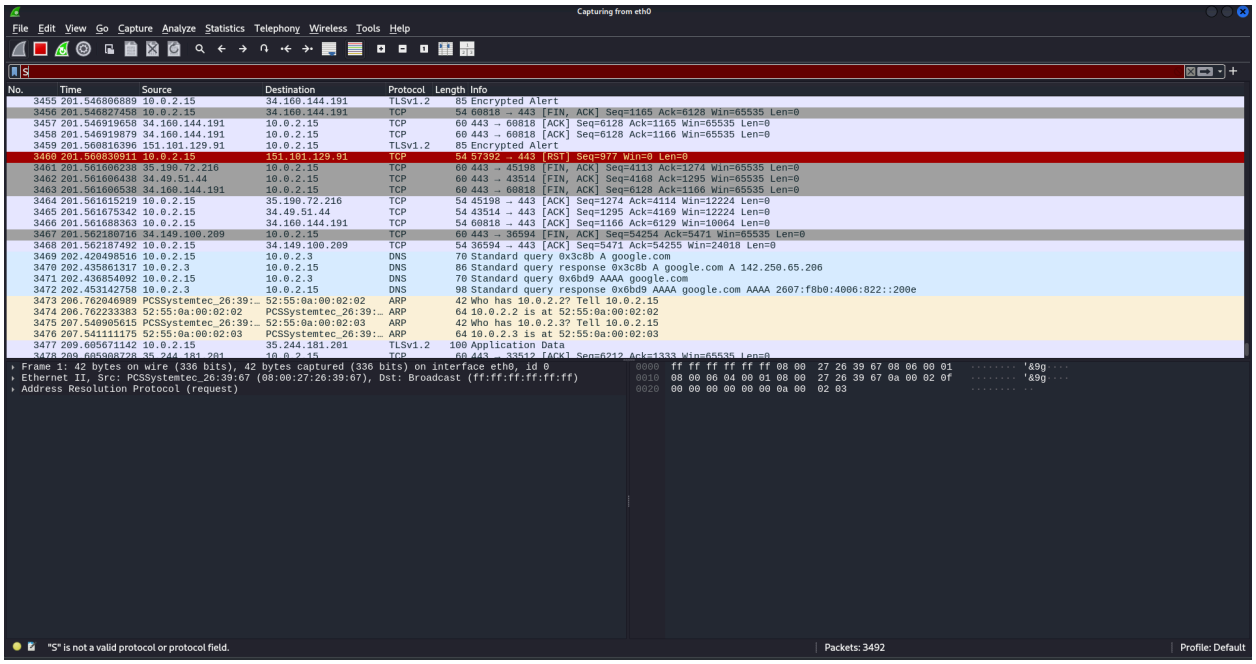
Wireshark Captures

HTTP

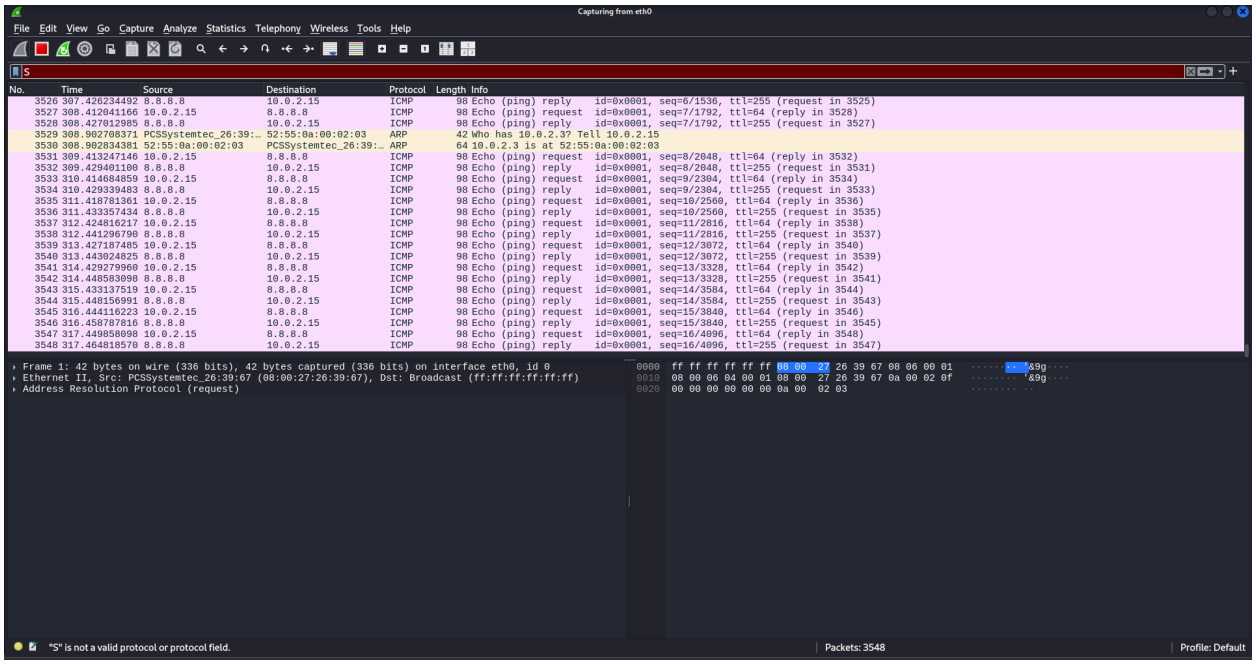

Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1718 4.285388244 10.0.2.15 23.57.1.24 TCP 54 48976 → 443 [ACK] Seq=6733 Ack=2276213 Win=65535 Len=0
1719 4.285546431 23.57.1.24 10.0.2.15 TCP 2950 443 → 48976 [PSH, ACK] Seq=2276213 Ack=6733 Win=65535 Len=2896 [TCP PDU reassembled in 1721]
1720 4.285604820 10.0.2.15 23.57.1.24 TCP 54 48976 → 443 [ACK] Seq=6733 Ack=2279109 Win=65535 Len=0
1721 4.286863789 23.57.1.24 10.0.2.15 TLSv1.3 14454 Application Data, Application Data
1722 4.286950837 10.0.2.15 23.57.1.24 TCP 54 48976 → 443 [ACK] Seq=6733 Ack=2293509 Win=65535 Len=0
1723 4.286967246 23.57.1.24 10.0.2.15 TCP 643 443 → 48976 [PSH, ACK] Seq=2293509 Ack=6733 Win=65535 Len=589 [TCP PDU reassembled in 1725]
1724 4.287047046 10.0.2.15 23.57.1.24 TCP 54 48976 → 443 [ACK] Seq=6733 Ack=2294098 Win=65535 Len=0
1725 4.287061721 23.57.1.24 10.0.2.15 TLSv1.3 4635 Application Data
1726 4.287110327 10.0.2.15 23.57.1.24 TCP 54 48976 → 443 [ACK] Seq=6733 Ack=2298679 Win=65535 Len=0
1727 4.306690103 10.0.2.15 17.33.201.109 TCP 54 45956 → 443 [ACK] Seq=2271 Ack=4694 Win=65535 Len=0
1728 6.099467128 10.0.2.15 23.40.179.158 TCP 54 60648 → 80 [FIN, ACK] Seq=1 Ack=1 Win=64240 Len=0
1729 6.099749551 23.40.179.158 10.0.2.15 TCP 60 80 → 60648 [ACK] Seq=1 Ack=2 Win=65535 Len=0
1730 6.117910457 23.40.179.158 10.0.2.15 TCP 60 80 → 60648 [FIN, ACK] Seq=1 Ack=2 Win=65535 Len=0
1731 6.117943947 10.0.2.15 23.40.179.158 TCP 54 60648 → 80 [ACK] Seq=2 Ack=2 Win=64240 Len=0
1732 8.174978071 10.0.2.15 17.253.144.10 TCP 54 39104 → 80 [FIN, ACK] Seq=1 Ack=1 Win=64240 Len=0
1733 8.175216599 17.253.144.10 10.0.2.15 TCP 60 80 → 39104 [ACK] Seq=1 Ack=2 Win=65535 Len=0
1734 8.199361442 17.253.144.10 10.0.2.15 TCP 60 80 → 39104 [FIN, ACK] Seq=1 Ack=2 Win=65535 Len=0
1735 8.199379796 10.0.2.15 17.253.144.10 TCP 54 39104 → 80 [ACK] Seq=2 Ack=2 Win=64240 Len=0
1736 10.920405527 10.0.2.15 23.40.179.157 TCP 54 [TCP Keep-Alive] 60036 → 80 [ACK] Seq=431 Ack=890 Win=63351 Len=0
1737 10.920431238 10.0.2.15 23.40.179.158 TCP 54 [TCP Keep-Alive] 60640 → 80 [ACK] Seq=862 Ack=1779 Win=62462 Len=0
1738 10.920735924 23.40.179.157 10.0.2.15 TCP 60 [TCP Keep-Alive ACK] 80 → 60036 [ACK] Seq=890 Ack=432 Win=65535 Len=0
1739 10.920736977 23.40.179.158 10.0.2.15 TCP 60 [TCP Keep-Alive ACK] 80 → 60640 [ACK] Seq=1779 Ack=863 Win=65535 Len=0
1740 11.393833892 10.0.2.15 34.107.221.82 TCP 54 [TCP Keep-Alive] 33060 → 80 [ACK] Seq=620 Ack=433 Win=64024 Len=0
Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_26:39:67 (08:00:27:26:39:67), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
0000 ff ff ff ff ff ff 08 00 27 26 39 67 08 06 00 01 .... '&9g....
0010 08 00 06 04 00 01 08 00 27 26 39 67 0a 00 02 0f .... '&9g....
0020 00 00 00 00 00 00 0a 00 02 03 ....
eth0: <live capture in progress>
Packets: 1740
Profile: Default

DNS

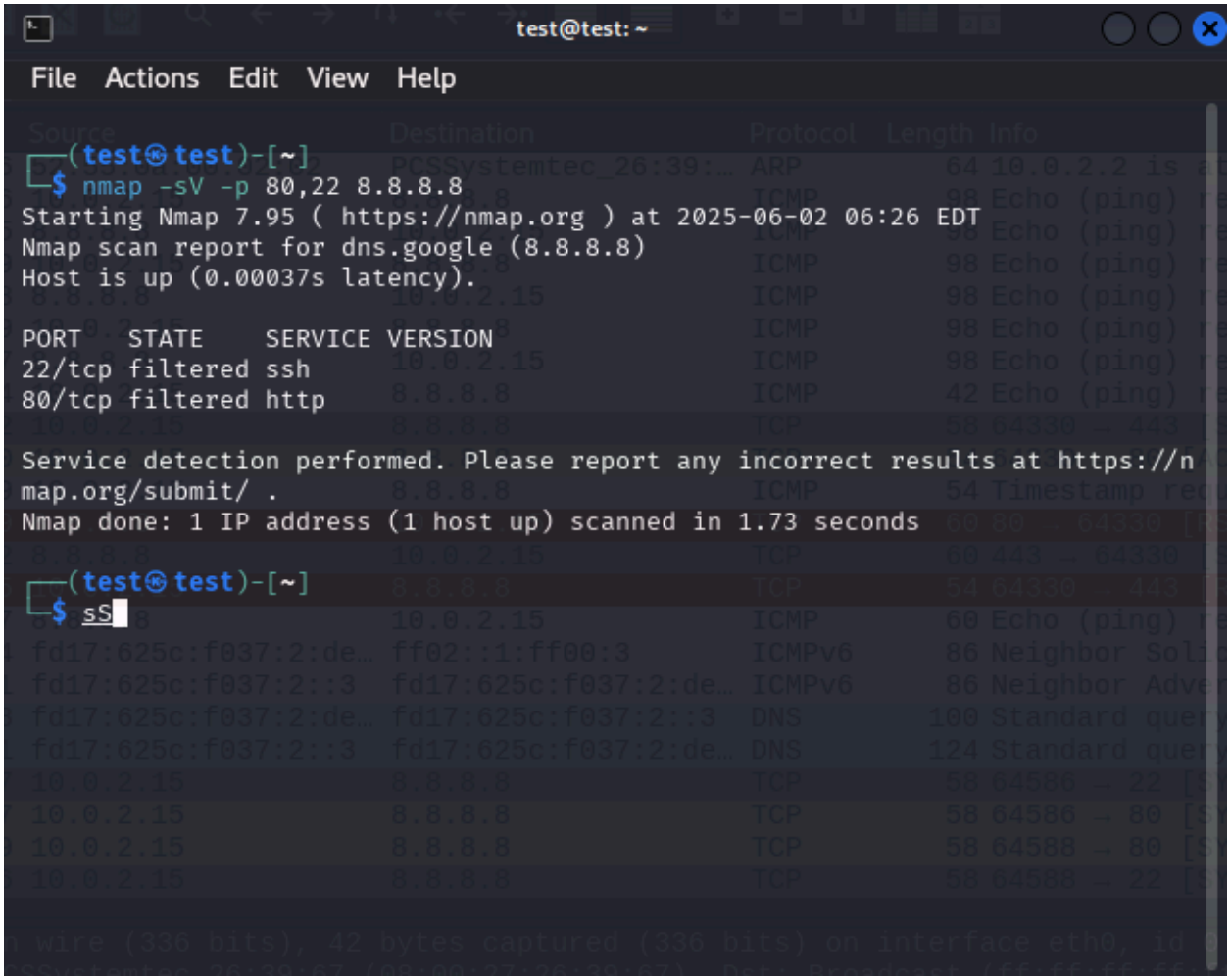

test@test: ~
File Actions Edit View Help
(test㉿test)-[~]
$ nslookup google.com
Server: 10.0.2.3
Address: 10.0.2.3#53
Non-authoritative answer:
Name: google.com
Address: 142.250.65.206
Name: google.com
Address: 2607:f8b0:4006:822::200e
(test㉿test)-[~]
$ sS



ICMP



Basic Vulnerability Assessment



Network Access & Authentication

Lab Environment:

- Hypervisor: Oracle VirtualBox
- VMs:
    - pfSense (Firewall/Router/VPN/NAC)
    - Windows 10 (Client Machine)
- Internal Networks:

    - `LAN1`: Simulated internal site
    - `LAN2`: Simulated remote site

Setup:

- **pfSense Interface Configuration:**
    - LAN IP: `192.168.1.1/24`
    - DHCP Range: `192.168.1.100 – 192.168.1.200`
    - WAN: NAT (Internet access)
    - LAN: Internal Network `LAN1`
- **Captive Portal:**
    - Enabled on LAN interface
    - Authentication using local pfSense users

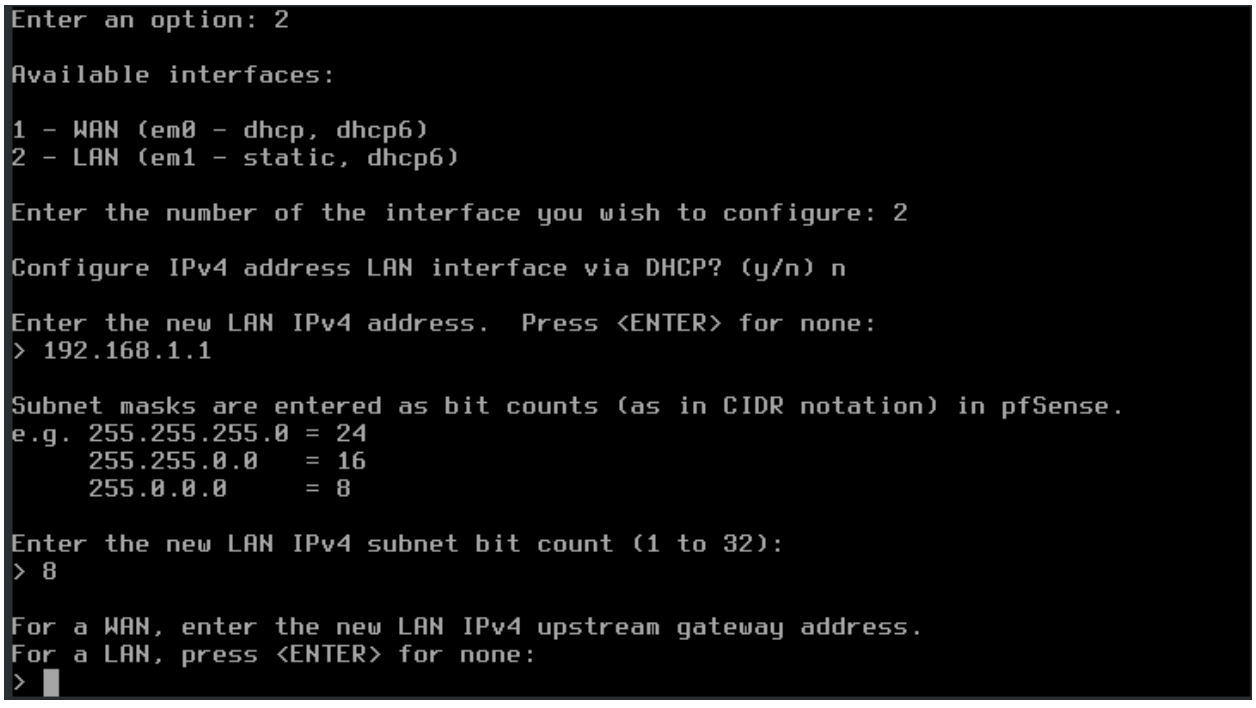
Phase 1:

- Key Exchange: IKEv2
- Authentication: Pre-shared key
- Local network: 192.168.1.0/24
- Remote network: 192.168.2.0/24

Phase 2:

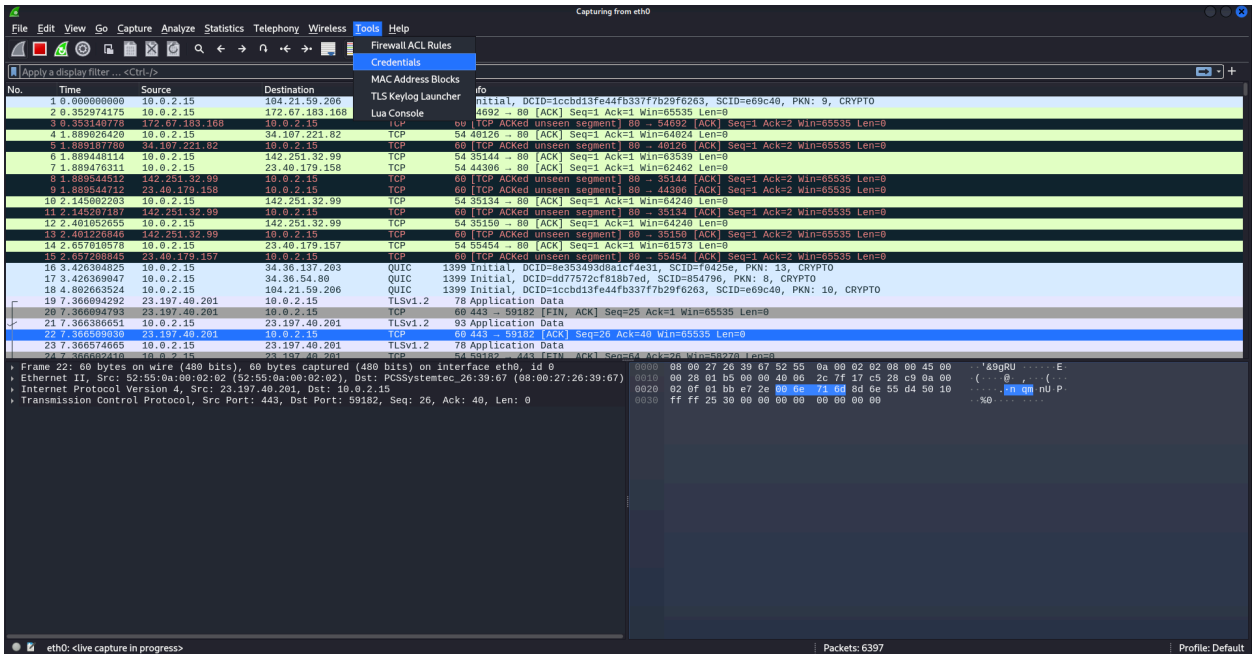
- Encryption: AES-256
- Protocol: ESP
- Lifetime: 3600 seconds

PFSENSE setup



Network Security Operations

Web Browsing



Steps:

1. Go to **pfSense Web UI > Firewall > Rules > LAN**.
2. Add a new rule:
    - Action: **Block**
    - Protocol: **TCP**
    - Destination Port: **3389 (RDP)**
    - Description: "Block RDP from LAN"
3. Apply changes.
4. On Windows VM:
    - Try running `mstsc` or RDP to another IP (or simulate attempt).
    - Use command: `telnet 192.168.1.1 3389` → should fail.

5. Check **Status > System Logs > Firewall** to confirm block event.

1. Simulate incident:
    - Try logging into the captive portal with **wrong username/password**
2. Go to **pfSense Web UI > Status > System Logs > Captive Portal**
3. Document:
    - Time of attempt
    - Source IP (e.g., `192.168.1.101`)
    - Usernames used
    - Number of attempts
4. Optional: Add response (e.g., lock IP, notify admin)