Assignment 3.1: Event Analysis and Verification of Snort Alerts in Splunk

Julia Andersen, Kayvon Karimi, Jacob Napierskie and Dale Whitehead

Shiley-Marcos School of Engineering, University of San Diego

CYBR-512: Incident Detection and Handling

Professor Mark Heckman, Ph.D.

November 09, 2024

Environment Setup

- **Network Configuration for Ubuntu**

  In this setup, Snort is running on an Ubuntu VM. To ensure stable communication and prevent IP conflicts, the network interface on this VM was configured with a static IP address. Specifically, the IP address was set to 10.0.2.110 in order to place it at a high and less likely-to-be-used address within the VirtualBox NAT network range (10.0.2.0/24).

```
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 08:00:27:95:19:81 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.110/24 brd 10.0.2.255 scope global noprefixroute enp0s3
```

  The static IP configuration was applied using Ubuntu's *Settings* tool, where the IPv4 address was manually assigned. This static IP ensures that the Snort VM consistently uses the same IP address, preventing DHCP from reassigning it to another device in the network. The configuration takes effect after a reboot, solidifying the network setup for reliable data flow between Snort and Splunk on this Ubuntu VM.

  Steps Taken:

  1. Go to Ubuntu Settings > Network.
  2. Select Network Interface (Wired or Ethernet)
  3. Set IPv4 to Manual
  4. Assign a Static IP Address of 10.0.2.110 with subnet mask (255.255.255.0)
  5. Save and Apply Changes
  6. Reboot VM for changes to take effect

- **Snort Configuration**

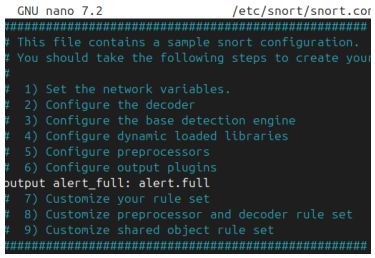
  To ensure compatibility with Splunk, Snort's configuration was adjusted to log alerts in a readable format. Within "/etc/snort/snort.conf", the following line was added to direct Snort to output logs in the "alert.full" format: *output alert_full: alert.full.* This directs Snort to log alerts in a detailed "full" format.

  Steps Taken:

  1. Install Snort if necessary
     - Sudo apt-get update
     - Sudo apt-get install snort
  2. Open the Snort configuration file in a text editor:

- *sudo nano /etc/snort/snort.conf*

3. Add this line below were it says “6) Configure output plugins”
    - *output alert_full: alert.full*



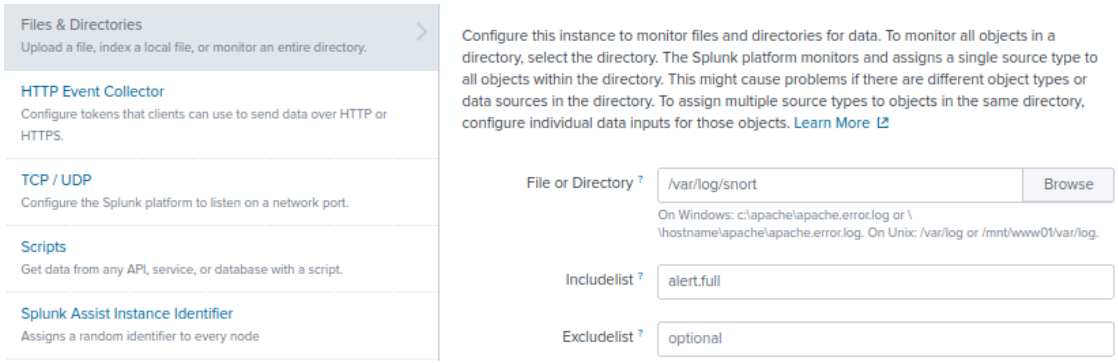
- **Install and Configure Splunk**

  Splunk Enterprise was installed on the same VM as Snort. After setup, the "Snort Alert for Splunk" plugin was installed via the “Find More Apps” section in Splunk. This plugin enables Splunk to capture, interpret, and display Snort alerts in a structured format.

  Steps Taken:

  1. Visit Splunk Website and Sign Up: “www.splunk.com”
  2. Download Splunk Enterprise
     - Select “Splunk Enterprise” from the “Downloads” section and choose the ".deb” package for Ubuntu.
  3. Install Splunk:
     - Open a terminal and navigate to the directory where the Splunk package was downloaded.
     - Use the “.deb” package format command:
       - *sudo dpkg -i splunk_package_name.deb*
  4. Start Splunk
     - Navigate to the Splunk directory:
       - *cd /opt/splunk/bin/*
     - Start the Splunk Service:
       - *sudo ./splunk start*
  5. Access Splunk Web Interface at http://127.0.0.1:8000 through a web browser
     - Log in with the admin credentials previously created
  6. Install Splunk Plugin
     - Navigate to the Splunk start page and click on “+Find More Apps”
     - Search for “snort” and click on the green “Install” button for “Snort Alert for Splunk”
  7. Configure Splunk to use the Plugin
     - Go to Settings > Add Data Inputs > Monitor > Files & Directories

- In the textbox, enter */var/log/snort*
- For include list, type “alert.full”
- On the next page, click on “Select”
- For the “Select Source Type” search for “snort” and select “snort_alert_full”.
- For “App Context, select “Snort Alert for Splunk (snortalert)”
- Select “Constant value”
- Enter a Host field value, it can be “snort”
- Reboot VM for changed to take effect



Attack Execution and Data Generation Phase

Scans and Metasploit attacks were executed from the Kali VM targeting the Metasploitable2 VM. These attacks simulated security threats, generating alerts in Snort that could then be analyzed in Splunk. The methods used included reconnaissance scans and exploitation attempts, designed to produce various alerts for further analysis. This lab explores the differences in Snort alerts generated during an attack simulation using Splunk’s Snort Event Summary, compared to the previous assignment’s enumeration phase results.

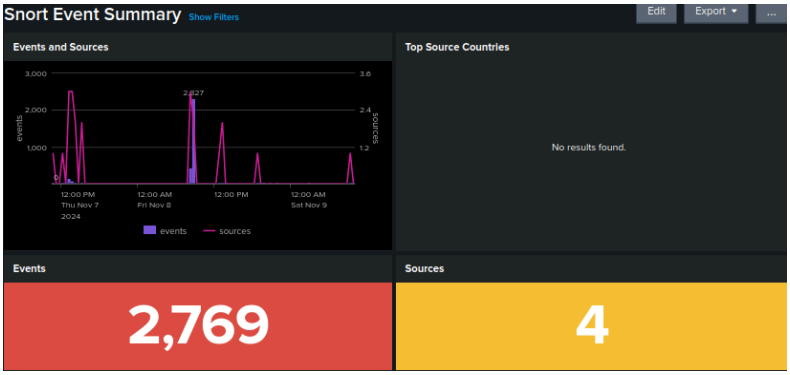
Execute Attack Simulation

1. Start Splunk
   - *cd /opt/splunk/bin/*
   - *sudo ./splunk start*
2. Click on the Splunk web interface link given in the terminal and navigate to the “Snort Event Summary” in the “Snort Alert for Slunk”
3. Start Snort in IDS Mode
   - *sudo snort -A console -q -c /etc/snort/snort.conf -i <interface>*

```
Waiting for web server at http://127.0.0.1:8000 to be available.............
......... Done


If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com

The Splunk web interface is at http://kayvon-VirtualBox:8000
```



4. Repeat Nmap Scans from Enumeration Phase
    - Basic Ping from Kali to Metasploitable2 VM
        - *ping -C 4 {target host}*

```
└─$ ping -c 4 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.
64 bytes from 10.0.2.4: icmp_seq=1 ttl=64 time=17.4 ms
64 bytes from 10.0.2.4: icmp_seq=2 ttl=64 time=3.30 ms
64 bytes from 10.0.2.4: icmp_seq=3 ttl=64 time=1.73 ms
64 bytes from 10.0.2.4: icmp_seq=4 ttl=64 time=1.35 ms

── 10.0.2.4 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3311ms
rtt min/avg/max/mdev = 1.345/5.936/17.370/6.641 ms
```

(Snort Output of ping in IDS Console)

```
kayvon@kayvon-VirtualBox:/opt/splunk/bin$ sudo snort -A console -q -c /etc/snort
/snort.conf -i enp0s3
11/10-14:09:53.705378  [**] [1:1000001:1] ICMP Packet detected [**] [Priority: 0
] {ICMP} 10.0.2.5 -> 10.0.2.4
11/10-14:09:53.722439  [**] [1:1000001:1] ICMP Packet detected [**] [Priority: 0
] {ICMP} 10.0.2.4 -> 10.0.2.5
11/10-14:09:54.999105  [**] [1:1000001:1] ICMP Packet detected [**] [Priority: 0
] {ICMP} 10.0.2.5 -> 10.0.2.4
11/10-14:09:55.000135  [**] [1:1000001:1] ICMP Packet detected [**] [Priority: 0
] {ICMP} 10.0.2.4 -> 10.0.2.5
11/10-14:09:56.003594  [**] [1:1000001:1] ICMP Packet detected [**] [Priority: 0
] {ICMP} 10.0.2.5 -> 10.0.2.4
11/10-14:09:56.003598  [**] [1:1000001:1] ICMP Packet detected [**] [Priority: 0
] {ICMP} 10.0.2.4 -> 10.0.2.5
11/10-14:09:57.016547  [**] [1:1000001:1] ICMP Packet detected [**] [Priority: 0
] {ICMP} 10.0.2.5 -> 10.0.2.4
11/10-14:09:57.863418  [**] [1:1000001:1] ICMP Packet detected [**] [Priority: 0
] {ICMP} 10.0.2.4 -> 10.0.2.5
```

(Snort Alert of ping in Splunk Enterprise Web Interface)

Time	Event
11/10/24 2:09:57.016 PM	[**] [1:1000001:1] ICMP Packet detected [**] [Priority: 0] 11/10-14:09:57.016551 10.0.2.5 -> 10.0.2.4 ICMP TTL:64 TOS:0x0 ID:3897 IpLen:20 DgmLen:84 DF Type:8 Code:0 ID:4 Seq:4 ECHO host = snort | source = /var/log/snort/alert.full | sourcetype = snort
11/10/24 2:09:56.003 PM	[**] [1:1000001:1] ICMP Packet detected [**] [Priority: 0] 11/10-14:09:56.003597 10.0.2.5 -> 10.0.2.4 ICMP TTL:64 TOS:0x0 ID:3787 IpLen:20 DgmLen:84 DF Type:8 Code:0 ID:4 Seq:3 ECHO host = snort | source = /var/log/snort/alert.full | sourcetype = snort
11/10/24 2:09:54.999 PM	[**] [1:1000001:1] ICMP Packet detected [**] [Priority: 0] 11/10-14:09:54.999109 10.0.2.5 -> 10.0.2.4 ICMP TTL:64 TOS:0x0 ID:3570 IpLen:20 DgmLen:84 DF Type:8 Code:0 ID:4 Seq:2 ECHO host = snort | source = /var/log/snort/alert.full | sourcetype = snort
11/10/24 2:09:53.705 PM	[**] [1:1000001:1] ICMP Packet detected [**] [Priority: 0] 11/10-14:09:53.705381 10.0.2.5 -> 10.0.2.4 ICMP TTL:64 TOS:0x0 ID:3460 IpLen:20 DgmLen:84 DF Type:8 Code:0 ID:4 Seq:1 ECHO host = snort | source = /var/log/snort/alert.full | sourcetype = snort

- Host Discovery Scan
  - *nmap -sn {target network}*

```
└─$ nmap -sn 10.0.2.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-10 14:32 PST
Nmap scan report for 10.0.2.4
Host is up (0.016s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds
```

(Snort Output of Nmap scan in IDS Console)

```
[**] [1:1000002:1] Possible Nmap SYN scan [**]
[Priority: 0]
11/10-14:32:17.148604 10.0.2.5:46120 -> 10.0.2.4:80
TCP TTL:64 TOS:0x0 ID:33105 IpLen:20 DgmLen:60 DF
******S* Seq: 0xF240476  Ack: 0x0  Win: 0xFAF0  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 1465139605 0 NOP WS: 7

[**] [1:1000002:1] Possible Nmap SYN scan [**]
[Priority: 0]
11/10-14:32:17.148604 10.0.2.5:48132 -> 10.0.2.4:443
TCP TTL:64 TOS:0x0 ID:11824 IpLen:20 DgmLen:60 DF
******S* Seq: 0xFDA40EF5  Ack: 0x0  Win: 0xFAF0  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 1465139605 0 NOP WS: 7
```

(Snort Alert in Splunk Enterprise Web Interface)

Time	Event
11/10/24 2:32:17.148 PM	[**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority: 0] 11/10-14:32:17.148604 10.0.2.5:48132 -> 10.0.2.4:443 TCP TTL:64 TOS:0x0 ID:11824 IpLen:20 DgmLen:60 DF ******S* Seq: 0xFDA40EF5 Ack: 0x0 Win: 0xFAF0 TcpLen: 40 Show all 6 lines host = snort | source = /var/log/snort/alert.full | sourcetype = snort
11/10/24 2:32:17.148 PM	[**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority: 0] 11/10-14:32:17.148604 10.0.2.5:46120 -> 10.0.2.4:80 TCP TTL:64 TOS:0x0 ID:33105 IpLen:20 DgmLen:60 DF ******S* Seq: 0xF240476 Ack: 0x0 Win: 0xFAF0 TcpLen: 40 Show all 6 lines host = snort | source = /var/log/snort/alert.full | sourcetype = snort

(NOTE: Removing 'sudo' allowed Snort to detect the scan, likely due to how 'sudo' interacts with network privileges, or it may have impacted how Nmap was sending packets)

- **TCP Scan**
  - *sudo nmap -sT {target host}*

```
└─$ sudo nmap -sT 10.0.2.4
[sudo] password for kayvon:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-10 14:44 PST
Nmap scan report for 10.0.2.4
Host is up (0.034s latency).
Not shown: 977 closed tcp ports (conn-refused)
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
MAC Address: 08:00:27:6B:C6:41 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.11 seconds
```

(Snort Output of TCP scan in IDS Console)

```
11/10-14:44:19.683320  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:47294 -> 10.0.2.4:1723
11/10-14:44:19.683324  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:51746 -> 10.0.2.4:3389
11/10-14:44:19.685260  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:54090 -> 10.0.2.4:53
11/10-14:44:19.685265  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:50928 -> 10.0.2.4:8888
11/10-14:44:19.685266  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:35564 -> 10.0.2.4:22
11/10-14:44:19.687066  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:33154 -> 10.0.2.4:25
11/10-14:44:19.692987  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:53064 -> 10.0.2.4:135
11/10-14:44:19.692987  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:41162 -> 10.0.2.4:80
11/10-14:44:19.695987  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:48760 -> 10.0.2.4:1720
11/10-14:44:19.695987  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:57450 -> 10.0.2.4:113
11/10-14:44:19.696438  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:49006 -> 10.0.2.4:143
11/10-14:44:19.696439  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:42656 -> 10.0.2.4:3306
11/10-14:44:19.696440  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:46790 -> 10.0.2.4:139
11/10-14:44:19.698177  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:36574 -> 10.0.2.4:995
11/10-14:44:19.700188  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:59660 -> 10.0.2.4:110
11/10-14:44:19.700496  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:45712 -> 10.0.2.4:111
11/10-14:44:19.700497  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:52018 -> 10.0.2.4:443
11/10-14:44:19.700498  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:57754 -> 10.0.2.4:554
11/10-14:44:19.701472  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:55338 -> 10.0.2.4:5900
11/10-14:44:19.701475  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:39764 -> 10.0.2.4:587
11/10-14:44:19.707498  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:47654 -> 10.0.2.4:8080
11/10-14:44:19.714235  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:39398 -> 10.0.2.4:23
11/10-14:44:19.714236  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:54186 -> 10.0.2.4:993
11/10-14:44:19.714237  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:46904 -> 10.0.2.4:256
11/10-14:44:19.719326  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:35286 -> 10.0.2.4:445
11/10-14:44:19.719327  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:55100 -> 10.0.2.4:21
11/10-14:44:19.720337  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:48052 -> 10.0.2.4:1025
11/10-14:44:19.720340  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
```

```
11/10-14:44:20.410215  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:35460 -> 10.0.2.4:1583
11/10-14:44:20.410424  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:49062 -> 10.0.2.4:49400
11/10-14:44:20.410425  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:48258 -> 10.0.2.4:30718
11/10-14:44:20.412053  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:48460 -> 10.0.2.4:10628
11/10-14:44:20.412058  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:38646 -> 10.0.2.4:1040
11/10-14:44:20.413018  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:56832 -> 10.0.2.4:1126
11/10-14:44:20.414235  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:55602 -> 10.0.2.4:19283
11/10-14:44:20.415104  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:54066 -> 10.0.2.4:50003
11/10-14:44:20.415107  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:35052 -> 10.0.2.4:2013
11/10-14:44:20.415108  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:49628 -> 10.0.2.4:8090
11/10-14:44:20.415109  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:58596 -> 10.0.2.4:1972
11/10-14:44:20.416132  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:39960 -> 10.0.2.4:8291
11/10-14:44:20.417543  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:44388 -> 10.0.2.4:3324
11/10-14:44:20.417613  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:46376 -> 10.0.2.4:2604
11/10-14:44:20.417809  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:52244 -> 10.0.2.4:5666
11/10-14:44:20.417811  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:36022 -> 10.0.2.4:1106
11/10-14:44:20.418709  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:38788 -> 10.0.2.4:7741
11/10-14:44:20.418712  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:40174 -> 10.0.2.4:548
11/10-14:44:20.418713  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:37500 -> 10.0.2.4:1151
11/10-14:44:20.420157  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:35052 -> 10.0.2.4:1074
11/10-14:44:20.420159  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:41030 -> 10.0.2.4:10010
11/10-14:44:20.420160  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:50446 -> 10.0.2.4:340
11/10-14:44:20.420161  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:54188 -> 10.0.2.4:5988
11/10-14:44:20.422610  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:52674 -> 10.0.2.4:1839
11/10-14:44:20.422614  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:57680 -> 10.0.2.4:407
11/10-14:44:20.422615  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:57676 -> 10.0.2.4:1062
11/10-15:00:39.134691  [**] [1:1000001:1] ICMP Packet detected [**] [Priority: 0
] {IPV6-ICMP} fe80::a00:27ff:febf:e82b -> ff02::2
```

(Snort Alert of TCP Scan in Splunk Enterprise Web Interface)

11/10/24 2:44:20.418 PM
[**] [1:1000002:1] Possible Nmap SYN scan [**]
[Priority: 0]
11/10-14:44:20.418710 10.0.2.5:38788 -> 10.0.2.4:7741
TCP TTL:64 TOS:0x0 ID:16505 IpLen:20 DgmLen:60 DF
******S* Seq: 0xB2B3EACE Ack: 0x0 Win: 0xFAF0 TcpLen: 40
Show all 6 lines
host = snort | source = /var/log/snort/alert.full | sourcetype = snort

11/10/24 2:44:20.417 PM
[**] [1:1000002:1] Possible Nmap SYN scan [**]
[Priority: 0]
11/10-14:44:20.417812 10.0.2.5:36022 -> 10.0.2.4:1106
TCP TTL:64 TOS:0x0 ID:26010 IpLen:20 DgmLen:60 DF
******S* Seq: 0x7182EEEA Ack: 0x0 Win: 0xFAF0 TcpLen: 40
Show all 6 lines
host = snort | source = /var/log/snort/alert.full | sourcetype = snort

11/10/24 2:44:20.417 PM
[**] [1:1000002:1] Possible Nmap SYN scan [**]
[Priority: 0]
11/10-14:44:20.417810 10.0.2.5:52244 -> 10.0.2.4:5666
TCP TTL:64 TOS:0x0 ID:37552 IpLen:20 DgmLen:60 DF
******S* Seq: 0x5EA18919 Ack: 0x0 Win: 0xFAF0 TcpLen: 40
Show all 6 lines
host = snort | source = /var/log/snort/alert.full | sourcetype = snort

11/10/24 2:44:20.417 PM
[**] [1:1000002:1] Possible Nmap SYN scan [**]
[Priority: 0]
11/10-14:44:20.417806 10.0.2.5:46376 -> 10.0.2.4:2604
TCP TTL:64 TOS:0x0 ID:33454 IpLen:20 DgmLen:60 DF
******S* Seq: 0xDE20FA1F Ack: 0x0 Win: 0xFAF0 TcpLen: 40
Show all 6 lines
host = snort | source = /var/log/snort/alert.full | sourcetype = snort

11/10/24 2:44:20.417 PM
[**] [1:1000002:1] Possible Nmap SYN scan [**]
[Priority: 0]
11/10-14:44:20.417543 10.0.2.5:44388 -> 10.0.2.4:3324
TCP TTL:64 TOS:0x0 ID:55182 IpLen:20 DgmLen:60 DF
******S* Seq: 0xFE7F91A0 Ack: 0x0 Win: 0xFAF0 TcpLen: 40
Show all 6 lines
host = snort | source = /var/log/snort/alert.full | sourcetype = snort

11/10/24 2:44:20.416 PM
[**] [1:1000002:1] Possible Nmap SYN scan [**]
[Priority: 0]
11/10-14:44:20.416134 10.0.2.5:39960 -> 10.0.2.4:8291
TCP TTL:64 TOS:0x0 ID:23310 IpLen:20 DgmLen:60 DF
******S* Seq: 0xC20046D0 Ack: 0x0 Win: 0xFAF0 TcpLen: 40
Show all 6 lines
host = snort | source = /var/log/snort/alert.full | sourcetype = snort

11/10/24 2:44:20.415 PM
[**] [1:1000002:1] Possible Nmap SYN scan [**]
[Priority: 0]
11/10-14:44:20.415109 10.0.2.5:58596 -> 10.0.2.4:1972
TCP TTL:64 TOS:0x0 ID:26289 IpLen:20 DgmLen:60 DF
******S* Seq: 0x5F3BAFF3 Ack: 0x0 Win: 0xFAF0 TcpLen: 40
Show all 6 lines
host = snort | source = /var/log/snort/alert.full | sourcetype = snort

11/10/24 2:44:20.415 PM
[**] [1:1000002:1] Possible Nmap SYN scan [**]
[Priority: 0]
11/10-14:44:20.415108 10.0.2.5:49628 -> 10.0.2.4:8090
TCP TTL:64 TOS:0x0 ID:42260 IpLen:20 DgmLen:60 DF
******S* Seq: 0x411D265F Ack: 0x0 Win: 0xFAF0 TcpLen: 40
Show all 6 lines
host = snort | source = /var/log/snort/alert.full | sourcetype = snort

11/10/24 2:44:20.415 PM
[**] [1:1000002:1] Possible Nmap SYN scan [**]
[Priority: 0]
11/10-14:44:20.415107 10.0.2.5:35052 -> 10.0.2.4:2013
TCP TTL:64 TOS:0x0 ID:65326 IpLen:20 DgmLen:60 DF
******S* Seq: 0xB84558D4 Ack: 0x0 Win: 0xFAF0 TcpLen: 40
Show all 6 lines
host = snort | source = /var/log/snort/alert.full | sourcetype = snort

11/10/24 2:44:20.422 PM
[**] [1:1000002:1] Possible Nmap SYN scan [**]
[Priority: 0]
11/10-14:44:20.422615 10.0.2.5:57676 -> 10.0.2.4:1062
TCP TTL:64 TOS:0x0 ID:49135 IpLen:20 DgmLen:60 DF
******S* Seq: 0x9E14CE95 Ack: 0x0 Win: 0xFAF0 TcpLen: 40
Show all 6 lines
host = snort | source = /var/log/snort/alert.full | sourcetype = snor

11/10/24 2:44:20.422 PM
[**] [1:1000002:1] Possible Nmap SYN scan [**]
[Priority: 0]
11/10-14:44:20.422614 10.0.2.5:57680 -> 10.0.2.4:407
TCP TTL:64 TOS:0x0 ID:30935 IpLen:20 DgmLen:60 DF
******S* Seq: 0x938A7B2E Ack: 0x0 Win: 0xFAF0 TcpLen: 40
Show all 6 lines
host = snort | source = /var/log/snort/alert.full | sourcetype = snor

11/10/24 2:44:20.422 PM
[**] [1:1000002:1] Possible Nmap SYN scan [**]
[Priority: 0]
11/10-14:44:20.422612 10.0.2.5:52674 -> 10.0.2.4:1839
TCP TTL:64 TOS:0x0 ID:36001 IpLen:20 DgmLen:60 DF
******S* Seq: 0x59361F56 Ack: 0x0 Win: 0xFAF0 TcpLen: 40
Show all 6 lines
host = snort | source = /var/log/snort/alert.full | sourcetype = snor

11/10/24 2:44:20.420 PM
[**] [1:1000002:1] Possible Nmap SYN scan [**]
[Priority: 0]
11/10-14:44:20.420161 10.0.2.5:54188 -> 10.0.2.4:5988
TCP TTL:64 TOS:0x0 ID:4126 IpLen:20 DgmLen:60 DF
******S* Seq: 0xB5A66730 Ack: 0x0 Win: 0xFAF0 TcpLen: 40
Show all 6 lines
host = snort | source = /var/log/snort/alert.full | sourcetype = snor

11/10/24 2:44:20.420 PM
[**] [1:1000002:1] Possible Nmap SYN scan [**]
[Priority: 0]
11/10-14:44:20.420161 10.0.2.5:50446 -> 10.0.2.4:340
TCP TTL:64 TOS:0x0 ID:5166 IpLen:20 DgmLen:60 DF
******S* Seq: 0xCD2126B8 Ack: 0x0 Win: 0xFAF0 TcpLen: 40
Show all 6 lines
host = snort | source = /var/log/snort/alert.full | sourcetype = snor

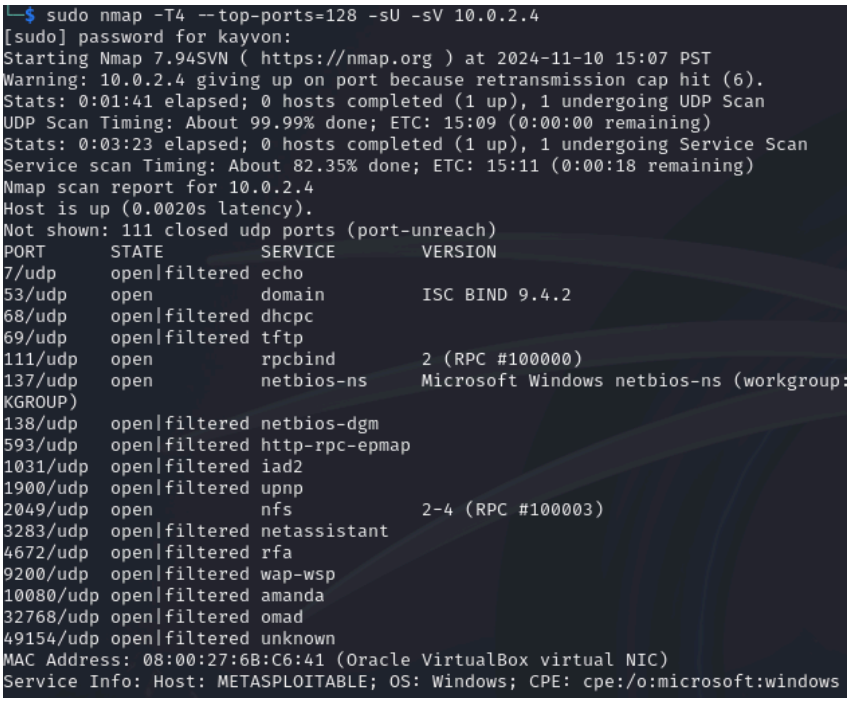
11/10/24 2:44:20.420 PM
[**] [1:1000002:1] Possible Nmap SYN scan [**]
[Priority: 0]
11/10-14:44:20.420160 10.0.2.5:41030 -> 10.0.2.4:10010
TCP TTL:64 TOS:0x0 ID:56994 IpLen:20 DgmLen:60 DF
******S* Seq: 0x83E690DE Ack: 0x0 Win: 0xFAF0 TcpLen: 40
Show all 6 lines
host = snort | source = /var/log/snort/alert.full | sourcetype = snor

11/10/24 2:44:20.420 PM
[**] [1:1000002:1] Possible Nmap SYN scan [**]
[Priority: 0]
11/10-14:44:20.420159 10.0.2.5:35052 -> 10.0.2.4:1074
TCP TTL:64 TOS:0x0 ID:12628 IpLen:20 DgmLen:60 DF
******S* Seq: 0x473D09E1 Ack: 0x0 Win: 0xFAF0 TcpLen: 40
Show all 6 lines
host = snort | source = /var/log/snort/alert.full | sourcetype = snor

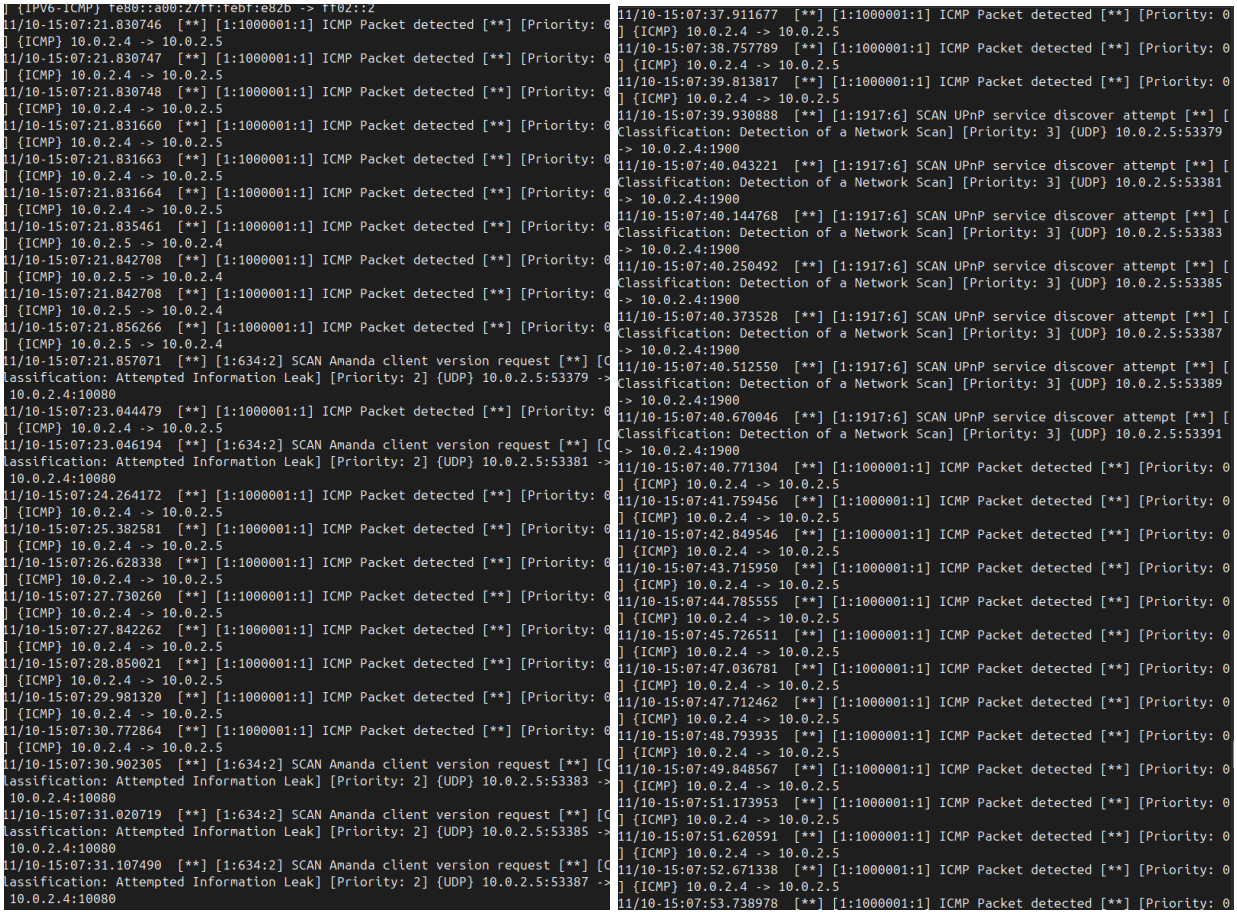
11/10/24 2:44:20.418 PM
[**] [1:1000002:1] Possible Nmap SYN scan [**]
[Priority: 0]
11/10-14:44:20.418713 10.0.2.5:37500 -> 10.0.2.4:1151
TCP TTL:64 TOS:0x0 ID:26279 IpLen:20 DgmLen:60 DF
******S* Seq: 0x296D641C Ack: 0x0 Win: 0xFAF0 TcpLen: 40
Show all 6 lines
host = snort | source = /var/log/snort/alert.full | sourcetype = snor

11/10/24 2:44:20.418 PM
[**] [1:1000002:1] Possible Nmap SYN scan [**]
[Priority: 0]
11/10-14:44:20.418713 10.0.2.5:40174 -> 10.0.2.4:548
TCP TTL:64 TOS:0x0 ID:28962 IpLen:20 DgmLen:60 DF
******S* Seq: 0x3F9716FA Ack: 0x0 Win: 0xFAF0 TcpLen: 40
Show all 6 lines

- **UDP Scan**
  - *sudo nmap -T5 --top-ports=128 -sU -sV {target host}*



```
└─$ sudo nmap -T4 --top-ports=128 -sU -sV 10.0.2.4
[sudo] password for kayvon:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-10 15:07 PST
Warning: 10.0.2.4 giving up on port because retransmission cap hit (6).
Stats: 0:01:41 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 99.99% done; ETC: 15:09 (0:00:00 remaining)
Stats: 0:03:23 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 82.35% done; ETC: 15:11 (0:00:18 remaining)
Nmap scan report for 10.0.2.4
Host is up (0.0020s latency).
Not shown: 111 closed udp ports (port-unreach)
PORT      STATE         SERVICE        VERSION
7/udp     open|filtered echo
53/udp    open          domain         ISC BIND 9.4.2
68/udp    open|filtered dhcpc
69/udp    open|filtered tftp
111/udp   open          rpcbind        2 (RPC #100000)
137/udp   open          netbios-ns     Microsoft Windows netbios-ns (workgroup:
KGROUP)
138/udp   open|filtered netbios-dgm
593/udp   open|filtered http-rpc-epmap
1031/udp  open|filtered iad2
1900/udp  open|filtered upnp
2049/udp  open          nfs            2-4 (RPC #100003)
3283/udp  open|filtered netassistant
4672/udp  open|filtered rfa
9200/udp  open|filtered wap-wsp
10080/udp open|filtered amanda
32768/udp open|filtered omad
49154/udp open|filtered unknown
MAC Address: 08:00:27:6B:C6:41 (Oracle VirtualBox virtual NIC)
Service Info: Host: METASPLOITABLE; OS: Windows; CPE: cpe:/o:microsoft:windows
```



("Partial View of UDP Alerts from Nmap Scan Detected by Snort")

```
sourcetype="snort" signature=1000001 name="ICMP Packet detected"
| table _time src_ip src_port dest_ip dest_port count
| sort - _time
```

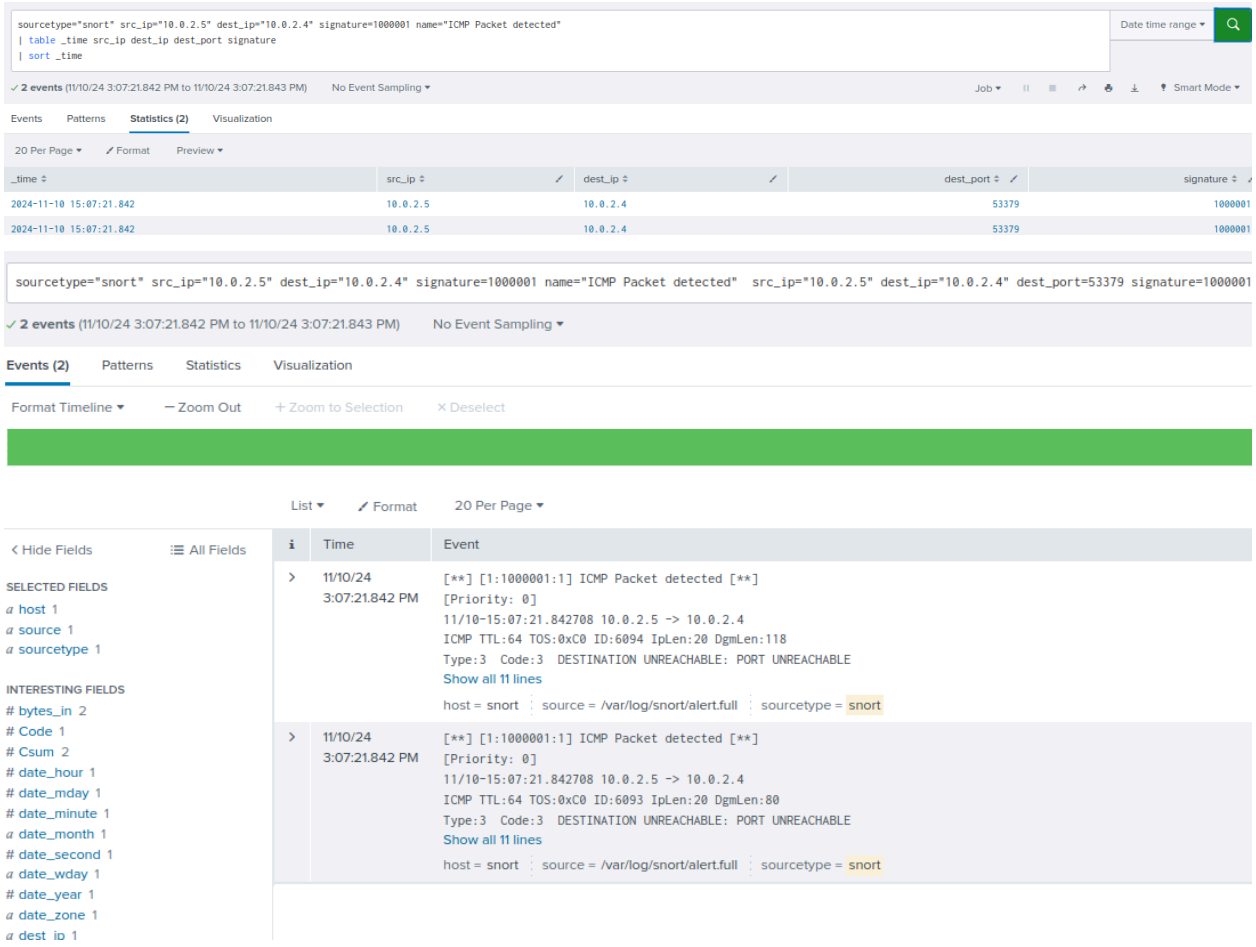
213 of 213 events matched No Event Sampling Job

Events Patterns **Statistics (213)** Visualization

20 Per Page Format Prev 1 … 4 5 6

_time	src_ip	src_port	dest_ip	dest_port
2024-11-10 15:07:43.715	10.0.2.4	53391	10.0.2.5	1025
2024-11-10 15:07:42.849	10.0.2.4	53391	10.0.2.5	49162
2024-11-10 15:07:41.759	10.0.2.4	53379	10.0.2.5	32769
2024-11-10 15:07:40.771	10.0.2.4	53379	10.0.2.5	49191
2024-11-10 15:07:39.813	10.0.2.4	53381	10.0.2.5	49193
2024-11-10 15:07:38.757	10.0.2.4	53391	10.0.2.5	20031
2024-11-10 15:07:37.911	10.0.2.4	53381	10.0.2.5	443
2024-11-10 15:07:36.756	10.0.2.4	53379	10.0.2.5	49189
2024-11-10 15:07:35.795	10.0.2.4	53379	10.0.2.5	989
2024-11-10 15:07:34.785	10.0.2.4	53391	10.0.2.5	4444
2024-11-10 15:07:33.831	10.0.2.4	53387	10.0.2.5	1645
2024-11-10 15:07:32.769	10.0.2.4	53391	10.0.2.5	2000
2024-11-10 15:07:31.914	10.0.2.4	53385	10.0.2.5	1030
2024-11-10 15:07:30.772	10.0.2.4	53389	10.0.2.5	3456
2024-11-10 15:07:29.981	10.0.2.4	53391	10.0.2.5	32771
2024-11-10 15:07:28.850	10.0.2.4	53389	10.0.2.5	2148
2024-11-10 15:07:27.842	10.0.2.4	53385	10.0.2.5	5353
2024-11-10 15:07:27.730	10.0.2.4	53385	10.0.2.5	158
2024-11-10 15:07:26.628	10.0.2.4	53387	10.0.2.5	3703
2024-11-10 15:07:25.382	10.0.2.4	53385	10.0.2.5	497

(Snort Detection of ICMP 'Port Unreachable' Alerts During Nmap Scan: Matching 'Host Unreachable' Messages Observed in Kali)



- OS Detection Scan
  - *sudo nmap -O {target host}*

```
└─$ sudo nmap -O 10.0.2.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-08 08:30 PST
Nmap scan report for 10.0.2.4
Host is up (0.0012s latency).
Not shown: 977 closed tcp ports (reset)
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
MAC Address: 08:00:27:6B:C6:41 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at htt
Nmap done: 1 IP address (1 host up) scanned in 1.98 seconds
```

```
] {ICMP} 10.0.2.5 -> 10.0.2.4
11/08-08:30:45.918428  [**] [1:1000001:1] ICMP Packet detected [**] [Priority: 0
] {ICMP} 10.0.2.4 -> 10.0.2.5
11/08-08:30:45.944826  [**] [1:1000001:1] ICMP Packet detected [**] [Priority: 0
] {ICMP} 10.0.2.5 -> 10.0.2.4
11/08-08:30:45.945421  [**] [1:1000001:1] ICMP Packet detected [**] [Priority: 0
] {ICMP} 10.0.2.4 -> 10.0.2.5
11/08-08:30:45.973343  [**] [1:1000001:1] ICMP Packet detected [**] [Priority: 0
] {ICMP} 10.0.2.4 -> 10.0.2.5
11/08-08:30:46.023862  [**] [1:1000004:1] Possible Nmap NULL scan [**] [Priority
: 0] {TCP} 10.0.2.5:49326 -> 10.0.2.4:21
11/08-08:30:46.105498  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:49329 -> 10.0.2.4:1
11/08-08:30:46.157478  [**] [1:1000005:1] Possible Nmap XMAS scan [**] [Priority
: 0] {TCP} 10.0.2.5:49331 -> 10.0.2.4:1
11/08-08:30:46.157478  [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Atte
mpted Information Leak] [Priority: 2] {TCP} 10.0.2.5:49331 -> 10.0.2.4:1
11/08-08:30:46.183833  [**] [1:1000004:1] Possible Nmap NULL scan [**] [Priority
: 0] {TCP} 10.0.2.5:49326 -> 10.0.2.4:21
11/08-08:30:46.285207  [**] [1:1000004:1] Possible Nmap NULL scan [**] [Priority
: 0] {TCP} 10.0.2.5:49326 -> 10.0.2.4:21
11/08-08:30:46.387474  [**] [1:1000004:1] Possible Nmap NULL scan [**] [Priority
: 0] {TCP} 10.0.2.5:49326 -> 10.0.2.4:21
```

- Service Version Detection
  - sudo nmap -sV {target host}
- Aggressive Scan
  - sudo nmap -A {target host}

```
sudo nmap -T5 --top-ports=128 -sU -sV {target host}
```

```
└─$ sudo nmap -T5 --top-ports=128 -sU -sV --max-retries 5 10.0.2.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-08 08:26 PST
```

```
pted Information Leak] [Priority: 2] {UDP} 10.0.2.5:43359 -> 10.0.2.4:162
11/08-08:26:43.941845  [**] [1:1000001:1] ICMP Packet detected [**] [Priority:
] {ICMP} 10.0.2.4 -> 10.0.2.5
11/08-08:26:43.941849  [**] [1:1000001:1] ICMP Packet detected [**] [Priority:
] {ICMP} 10.0.2.4 -> 10.0.2.5
11/08-08:26:46.509220  [**] [1:2339:2] TFTP NULL command attempt [**] [Classifi
ation: Potentially Bad Traffic] [Priority: 2] {UDP} 10.0.2.5:49404 -> 10.0.2.4:
9
11/08-08:26:46.510190  [**] [1:1000001:1] ICMP Packet detected [**] [Priority:
] {ICMP} 10.0.2.4 -> 10.0.2.5
11/08-08:26:46.510191  [**] [1:1000001:1] ICMP Packet detected [**] [Priority:
] {ICMP} 10.0.2.4 -> 10.0.2.5
11/08-08:26:46.510191  [**] [1:1000001:1] ICMP Packet detected [**] [Priority:
] {ICMP} 10.0.2.4 -> 10.0.2.5
11/08-08:26:46.513125  [**] [1:1419:9] SNMP trap udp [**] [Classification: Atte
pted Information Leak] [Priority: 2] {UDP} 10.0.2.5:54234 -> 10.0.2.4:162
11/08-08:26:49.195897  [**] [1:1000001:1] ICMP Packet detected [**] [Priority:
] {ICMP} 10.0.2.4 -> 10.0.2.5
11/08-08:26:49.195898  [**] [1:1000001:1] ICMP Packet detected [**] [Priority:
] {ICMP} 10.0.2.4 -> 10.0.2.5
11/08-08:26:49.195984  [**] [1:1000001:1] ICMP Packet detected [**] [Priority:
] {ICMP} 10.0.2.4 -> 10.0.2.5
11/08-08:26:51.512194  [**] [1:2339:2] TFTP NULL command attempt [**] [Classifi
ation: Potentially Bad Traffic] [Priority: 2] {UDP} 10.0.2.5:40770 -> 10.0.2.4:
```

11/8/24 8:26:56.518 AM
[**] [1:1419:9] SNMP trap udp [**]
[Classification: Attempted Information Leak] [Priority: 2]
11/08-08:26:56.518420 10.0.2.5:53534 -> 10.0.2.4:162
UDP TTL:64 TOS:0x0 ID:24007 IpLen:20 DgmLen:89 DF
Len: 61
Show all 6 lines
host = snort | source = /var/log/snort/alert.full | sourcetype = snort

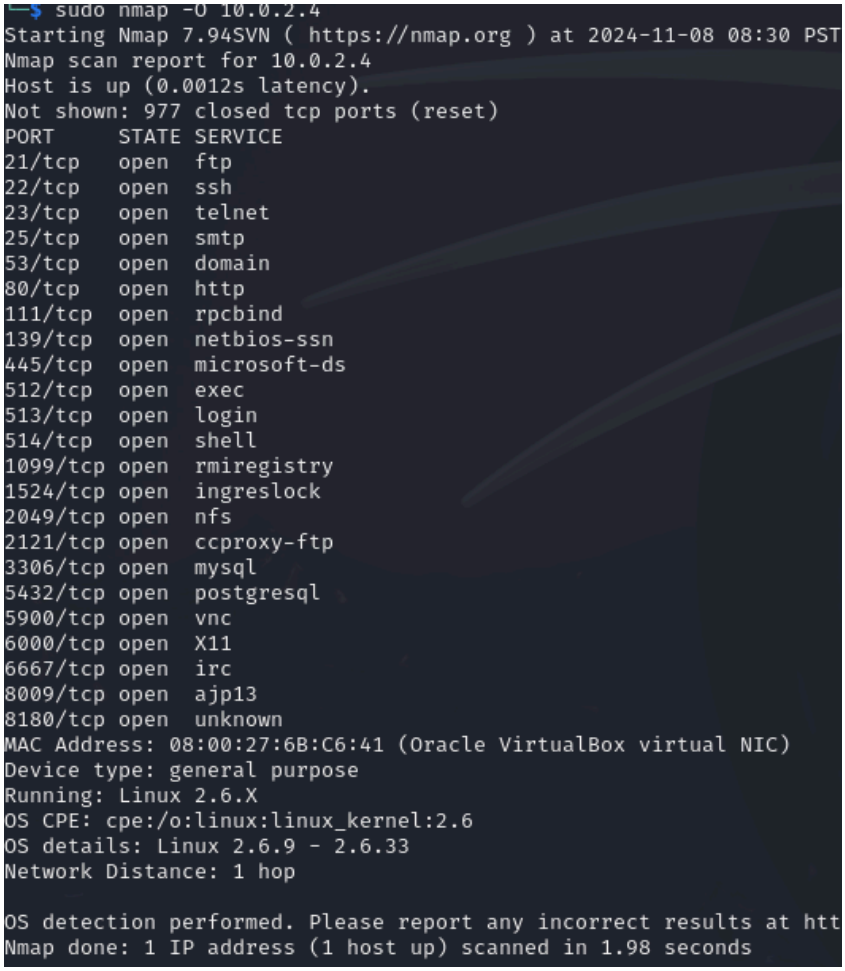
11/8/24 8:26:51.513 AM
[**] [1:1419:9] SNMP trap udp [**]
[Classification: Attempted Information Leak] [Priority: 2]
11/08-08:26:51.513032 10.0.2.5:49606 -> 10.0.2.4:162
UDP TTL:64 TOS:0x0 ID:32876 IpLen:20 DgmLen:141 DF
Len: 113
Show all 6 lines
host = snort | source = /var/log/snort/alert.full | sourcetype = snort

11/8/24 8:26:51.512 AM
[**] [1:2339:2] TFTP NULL command attempt [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
11/08-08:26:51.512196 10.0.2.5:40770 -> 10.0.2.4:69
UDP TTL:64 TOS:0x0 ID:12787 IpLen:20 DgmLen:74 DF
Len: 46
Show all 6 lines
host = snort | source = /var/log/snort/alert.full | sourcetype = snort

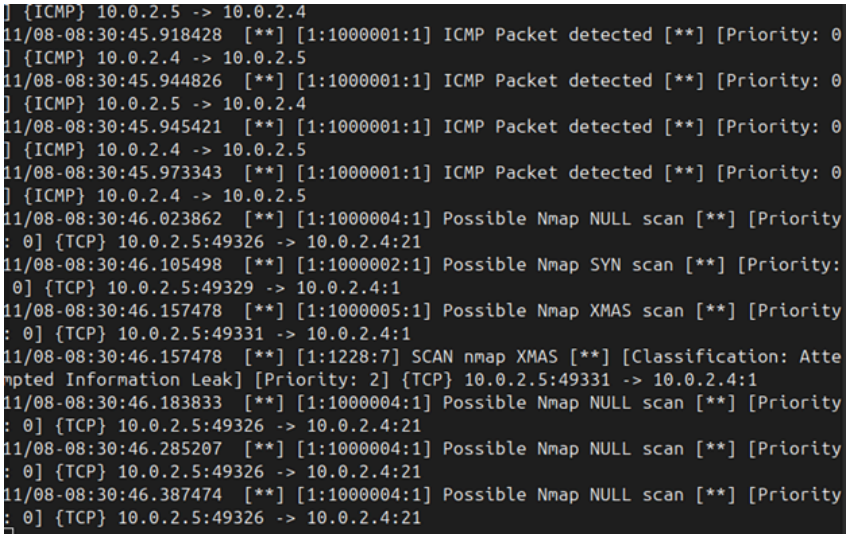
11/8/24 8:26:46.513 AM
[**] [1:1419:9] SNMP trap udp [**]
[Classification: Attempted Information Leak] [Priority: 2]
11/08-08:26:46.513125 10.0.2.5:54234 -> 10.0.2.4:162
UDP TTL:64 TOS:0x0 ID:16991 IpLen:20 DgmLen:58 DF
Len: 30
Show all 6 lines
host = snort | source = /var/log/snort/alert.full | sourcetype = snort

11/8/24 8:26:46.509 AM
[**] [1:2339:2] TFTP NULL command attempt [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
11/08-08:26:46.509222 10.0.2.5:49404 -> 10.0.2.4:69
UDP TTL:64 TOS:0x0 ID:1563 IpLen:20 DgmLen:60 DF
Len: 32
Show all 6 lines
host = snort | source = /var/log/snort/alert.full | sourcetype = snort

sudo nmap -O {target host}



Snort IDS Alert Console



Snort IDS Alerts on Splunk from Nmap Scanning Activity

11/8/24 8:30:46.387 AM	[**] [1:1000004:1] Possible Nmap NULL scan [**] [Priority: 0] 11/08-08:30:46.387476 10.0.2.5:49326 -> 10.0.2.4:21 TCP TTL:55 TOS:0x0 ID:49926 IpLen:20 DgmLen:60 DF ******** Seq: 0xDCDD651D Ack: 0x6F44748D Win: 0x80 TcpLen: 40 Show all 6 lines host = snort ⋮ source = /var/log/snort/alert.full ⋮ sourcetype = snort
11/8/24 8:30:46.285 AM	[**] [1:1000004:1] Possible Nmap NULL scan [**] [Priority: 0] 11/08-08:30:46.285208 10.0.2.5:49326 -> 10.0.2.4:21 TCP TTL:39 TOS:0x0 ID:6554 IpLen:20 DgmLen:60 DF ******** Seq: 0xDCDD651D Ack: 0x6F44748D Win: 0x80 TcpLen: 40 Show all 6 lines host = snort ⋮ source = /var/log/snort/alert.full ⋮ sourcetype = snort
11/8/24 8:30:46.183 AM	[**] [1:1000004:1] Possible Nmap NULL scan [**] [Priority: 0] 11/08-08:30:46.183834 10.0.2.5:49326 -> 10.0.2.4:21 TCP TTL:44 TOS:0x0 ID:33542 IpLen:20 DgmLen:60 DF ******** Seq: 0xDCDD651D Ack: 0x6F44748D Win: 0x80 TcpLen: 40 Show all 6 lines host = snort ⋮ source = /var/log/snort/alert.full ⋮ sourcetype = snort
11/8/24 8:30:46.157 AM	[**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Attempted Information Leak] [Priority: 2] 11/08-08:30:46.157479 10.0.2.5:49331 -> 10.0.2.4:1 TCP TTL:39 TOS:0x0 ID:11032 IpLen:20 DgmLen:60 **U*P**F Seq: 0xDCDD651D Ack: 0x6F44748D Win: 0xFFFF TcpLen: 40 UrgPtr: 0x0 Show all 7 lines host = snort ⋮ source = /var/log/snort/alert.full ⋮ sourcetype = snort
11/8/24 8:30:46.157 AM	[**] [1:1000005:1] Possible Nmap XMAS scan [**] [Priority: 0] 11/08-08:30:46.157479 10.0.2.5:49331 -> 10.0.2.4:1 TCP TTL:39 TOS:0x0 ID:11032 IpLen:20 DgmLen:60 **U*P**F Seq: 0xDCDD651D Ack: 0x6F44748D Win: 0xFFFF TcpLen: 40 UrgPtr: 0x0 Show all 6 lines host = snort ⋮ source = /var/log/snort/alert.full ⋮ sourcetype = snort
11/8/24 8:30:46.105 AM	[**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority: 0] 11/08-08:30:46.105500 10.0.2.5:49329 -> 10.0.2.4:1 TCP TTL:37 TOS:0x0 ID:18409 IpLen:20 DgmLen:60 ******S* Seq: 0xDCDD651D Ack: 0x6F44748D Win: 0x7A69 TcpLen: 40 Show all 6 lines host = snort ⋮ source = /var/log/snort/alert.full ⋮ sourcetype = snort
11/8/24 8:30:46.023 AM	[**] [1:1000004:1] Possible Nmap NULL scan [**] [Priority: 0] 11/08-08:30:46.023864 10.0.2.5:49326 -> 10.0.2.4:21 TCP TTL:53 TOS:0x0 ID:6597 IpLen:20 DgmLen:60 DF ******** Seq: 0xDCDD651D Ack: 0x6F44748D Win: 0x80 TcpLen: 40 Show all 6 lines host = snort ⋮ source = /var/log/snort/alert.full ⋮ sourcetype = snort

sudo nmap -A {target host}

```
└─$ sudo nmap -A 10.0.2.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-08 08:33 PST
Stats: 0:01:04 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 08:34 (0:00:03 remaining)
Nmap scan report for 10.0.2.4
Host is up (0.0034s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.0.2.5
|      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         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)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY
LS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     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      33453/udp   mountd
|   100005  1,2,3      46178/tcp   mountd
|   100021  1,3,4      35856/udp   nlockmgr
|   100021  1,3,4      53137/tcp   nlockmgr
|   100024  1          46355/tcp   status
|_  100024  1          57784/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
```

```
11/08-08:33:37.121942  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:50688 -> 10.0.2.4:8009
11/08-08:33:37.187564  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:39332 -> 10.0.2.4:8180
11/08-08:33:43.075521  [**] [1:257:9] DNS named version attempt [**] [Classifica
tion: Attempted Information Leak] [Priority: 2] {TCP} 10.0.2.5:43696 -> 10.0.2.4
:53
11/08-08:33:43.075523  [**] [1:2113:3] RSERVICES rexec username overflow attempt
 [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TC
P} 10.0.2.5:33098 -> 10.0.2.4:512
11/08-08:33:43.092795  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:54608 -> 10.0.2.4:5432
11/08-08:33:43.116389  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:36690 -> 10.0.2.4:6000
11/08-08:33:43.118887  [**] [1:1226:4] X11 xopen [**] [Classification: Unknown T
raffic] [Priority: 3] {TCP} 10.0.2.5:36690 -> 10.0.2.4:6000
11/08-08:33:43.125709  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:54622 -> 10.0.2.4:5432
11/08-08:33:43.150396  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:50694 -> 10.0.2.4:8009
11/08-08:33:43.162003  [**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority:
 0] {TCP} 10.0.2.5:50704 -> 10.0.2.4:8009
```

11/8/24 8:33:43.150 AM	[**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority: 0] 11/08-08:33:43.150397 10.0.2.5:50694 -> 10.0.2.4:8009 TCP TTL:64 TOS:0x0 ID:62043 IpLen:20 DgmLen:60 DF ******S* Seq: 0x2952A909 Ack: 0x0 Win: 0xFAF0 TcpLen: 40 Show all 6 lines host = snort ⋮ source = /var/log/snort/alert.full ⋮ sourcetype = snort
11/8/24 8:33:43.125 AM	[**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority: 0] 11/08-08:33:43.125711 10.0.2.5:54622 -> 10.0.2.4:5432 TCP TTL:64 TOS:0x0 ID:46299 IpLen:20 DgmLen:60 DF ******S* Seq: 0x75C74305 Ack: 0x0 Win: 0xFAF0 TcpLen: 40 Show all 6 lines host = snort ⋮ source = /var/log/snort/alert.full ⋮ sourcetype = snort
11/8/24 8:33:43.118 AM	[**] [1:1226:4] X11 xopen [**] [Classification: Unknown Traffic] [Priority: 3] 11/08-08:33:43.118887 10.0.2.5:36690 -> 10.0.2.4:6000 TCP TTL:64 TOS:0x0 ID:63123 IpLen:20 DgmLen:64 DF ***AP*** Seq: 0xE538C6B8 Ack: 0x1C709317 Win: 0x1F6 TcpLen: 32 Show all 7 lines host = snort ⋮ source = /var/log/snort/alert.full ⋮ sourcetype = snort
11/8/24 8:33:43.116 AM	[**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority: 0] 11/08-08:33:43.116389 10.0.2.5:36690 -> 10.0.2.4:6000 TCP TTL:64 TOS:0x0 ID:63121 IpLen:20 DgmLen:60 DF ******S* Seq: 0xE538C6B7 Ack: 0x0 Win: 0xFAF0 TcpLen: 40 Show all 6 lines host = snort ⋮ source = /var/log/snort/alert.full ⋮ sourcetype = snort
11/8/24 8:33:43.092 AM	[**] [1:1000002:1] Possible Nmap SYN scan [**] [Priority: 0] 11/08-08:33:43.092795 10.0.2.5:54608 -> 10.0.2.4:5432 TCP TTL:64 TOS:0x0 ID:21332 IpLen:20 DgmLen:60 DF ******S* Seq: 0xFCC87DCE Ack: 0x0 Win: 0xFAF0 TcpLen: 40 Show all 6 lines host = snort ⋮ source = /var/log/snort/alert.full ⋮ sourcetype = snort
11/8/24 8:33:43.075 AM	[**] [1:2113:3] RSERVICES rexec username overflow attempt [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] 11/08-08:33:43.075523 10.0.2.5:33098 -> 10.0.2.4:512 TCP TTL:64 TOS:0x0 ID:38924 IpLen:20 DgmLen:84 DF ***AP*** Seq: 0x73AEB0C1 Ack: 0x163E8D79 Win: 0x1F6 TcpLen: 32 Show all 6 lines host = snort ⋮ source = /var/log/snort/alert.full ⋮ sourcetype = snort
11/8/24 8:33:43.075 AM	[**] [1:257:9] DNS named version attempt [**] [Classification: Attempted Information Leak] [Priority: 2] 11/08-08:33:43.075521 10.0.2.5:43696 -> 10.0.2.4:53 TCP TTL:64 TOS:0x0 ID:61391 IpLen:20 DgmLen:84 DF ***AP*** Seq: 0xFE678156 Ack: 0x16ECFFEF Win: 0x1F6 TcpLen: 32 Show all 7 lines host = snort ⋮ source = /var/log/snort/alert.full ⋮ sourcetype = snort

Event Analysis in Splunk

1. **Snort Event Summary in Splunk**

   The Snort Event Summary, accessed through the "Snort Alert for Splunk" plugin in Splunk, provided an organized display of the events captured. This summary listed event types, timestamps, and additional metadata. A screenshot of the Snort Event Summary is included to document the total number of events recorded.

2. **Comparison with Previous Assignment**

   The total count of events in the Snort Event Summary was compared with the alert counts from the previous assignment. This comparison aimed to verify consistency between assignments. Any discrepancies were noted, with potential causes examined, such as variations in attack execution, configuration settings, or event handling in Splunk.

3. **Splunk Event Search Results**

   Splunk's search function was used to locate all Snort events generated during the tests. Using the query _host=snort | table *time, src_ip, dst_ip*, events were listed with their timestamps, source IPs, and destination IPs. A **screenshot** of these search results is included for documentation.

4. **Comparison of Search Results and Snort Event Summary**

   Finally, the events from Splunk's search results were compared with those listed in the Snort Event Summary to ensure that all events were accounted for. This comparison helped confirm the accuracy of Splunk's search capabilities in capturing Snort data. Any unaccounted-for events were documented, with potential explanations provided for differences between the two views.

   -