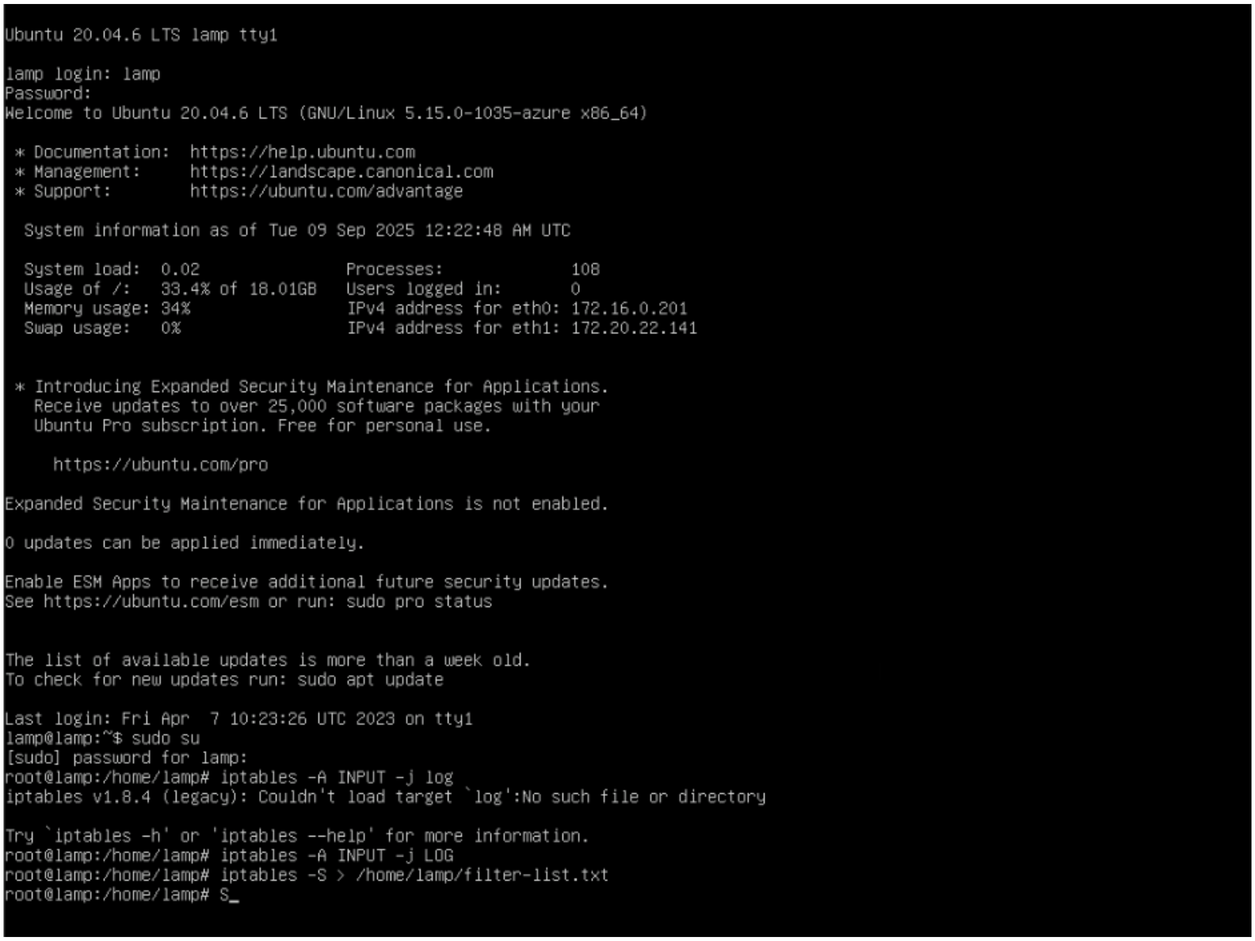
Threat Hunting Network Events

Adrian Cortez

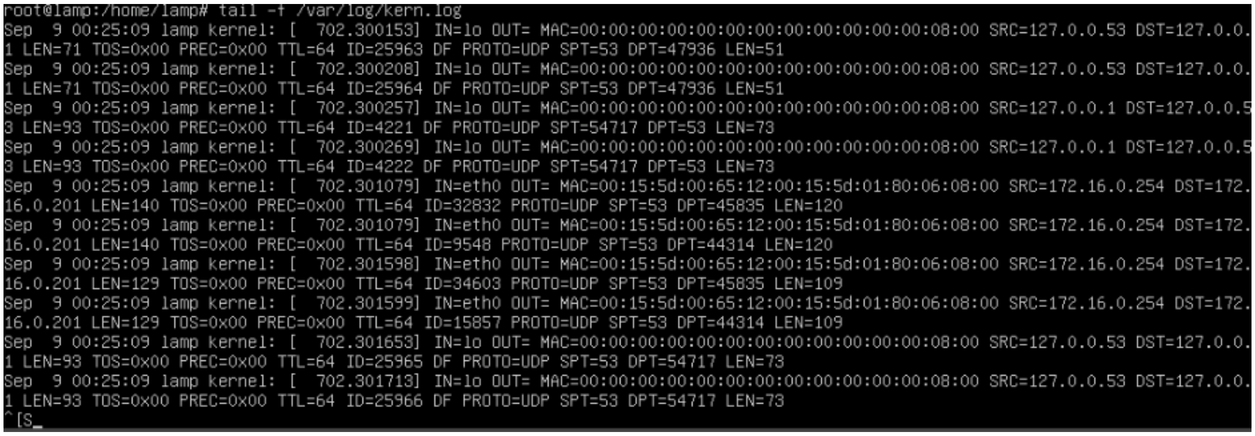
This project demonstrates a typical threat hunting process. In most cases, threat hunting begins with knowledge of an IoC (Indicator of Compromise), which is then used to search for related symptoms or activity within your environment. The objective is to determine whether your systems have already been affected by an exploit or attack technique you've recently identified. In this project, you will analyze network communication logs to uncover an IoC.

Sign into LAMP, our VM hosting the web application, and elevate root privileges.



```
Ubuntu 20.04.6 LTS lamp tty1

lamp login: lamp
Password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-1035-azure x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Tue 09 Sep 2025 12:22:48 AM UTC

  System load:  0.02              Processes:             108
  Usage of /:   33.4% of 18.01GB  Users logged in:       0
  Memory usage: 34%               IPv4 address for eth0: 172.16.0.201
  Swap usage:   0%                IPv4 address for eth1: 172.20.22.141


 * Introducing Expanded Security Maintenance for Applications.
   Receive updates to over 25,000 software packages with your
   Ubuntu Pro subscription. Free for personal use.

     https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Fri Apr  7 10:23:26 UTC 2023 on tty1
lamp@lamp:~$ sudo su
[sudo] password for lamp:
root@lamp:/home/lamp# iptables -A INPUT -j log
iptables v1.8.4 (legacy): Couldn't load target `log':No such file or directory

Try `iptables -h' or 'iptables --help' for more information.
root@lamp:/home/lamp# iptables -A INPUT -j LOG
root@lamp:/home/lamp# iptables -S > /home/lamp/filter-list.txt
root@lamp:/home/lamp# S_
```

The command shown creates a file containing the current filters of iptables. This is necessary because the verification script below is unable to read the filters directly due to permission limitations.



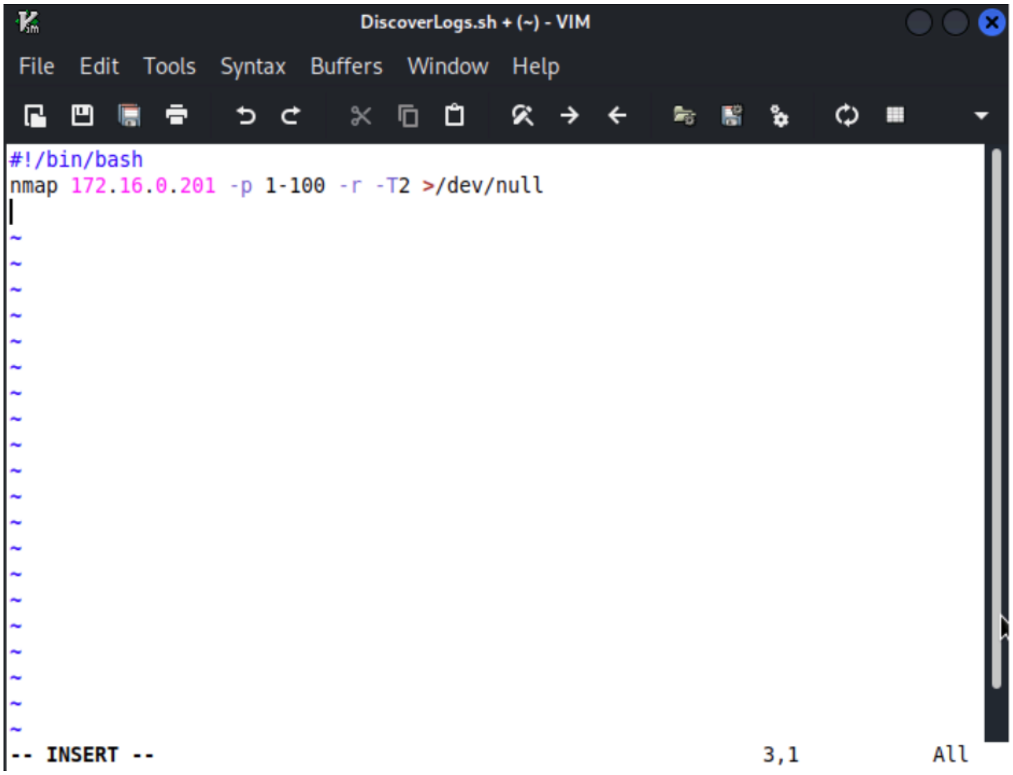
```
root@lamp:/home/lamp# tail -f /var/log/kern.log
Sep  9 00:25:09 lamp kernel: [  702.300153] IN=lo OUT= MAC=00:00:00:00:00:00:00:00:00:00:00:00:08:00 SRC=127.0.0.53 DST=127.0.0.
1 LEN=71 TOS=0x00 PREC=0x00 TTL=64 ID=25963 DF PROTO=UDP SPT=53 DPT=47936 LEN=51
Sep  9 00:25:09 lamp kernel: [  702.300208] IN=lo OUT= MAC=00:00:00:00:00:00:00:00:00:00:00:00:08:00 SRC=127.0.0.53 DST=127.0.0.
1 LEN=71 TOS=0x00 PREC=0x00 TTL=64 ID=25964 DF PROTO=UDP SPT=53 DPT=47936 LEN=51
Sep  9 00:25:09 lamp kernel: [  702.300257] IN=lo OUT= MAC=00:00:00:00:00:00:00:00:00:00:00:00:08:00 SRC=127.0.0.1 DST=127.0.0.5
3 LEN=93 TOS=0x00 PREC=0x00 TTL=64 ID=4221 DF PROTO=UDP SPT=54717 DPT=53 LEN=73
Sep  9 00:25:09 lamp kernel: [  702.300269] IN=lo OUT= MAC=00:00:00:00:00:00:00:00:00:00:00:00:08:00 SRC=127.0.0.1 DST=127.0.0.5
3 LEN=93 TOS=0x00 PREC=0x00 TTL=64 ID=4222 DF PROTO=UDP SPT=54717 DPT=53 LEN=73
Sep  9 00:25:09 lamp kernel: [  702.301079] IN=eth0 OUT= MAC=00:15:5d:00:65:12:00:15:5d:01:80:06:08:00 SRC=172.16.0.254 DST=172.
16.0.201 LEN=140 TOS=0x00 PREC=0x00 TTL=64 ID=32832 PROTO=UDP SPT=53 DPT=45835 LEN=120
Sep  9 00:25:09 lamp kernel: [  702.301079] IN=eth0 OUT= MAC=00:15:5d:00:65:12:00:15:5d:01:80:06:08:00 SRC=172.16.0.254 DST=172.
16.0.201 LEN=140 TOS=0x00 PREC=0x00 TTL=64 ID=9548 PROTO=UDP SPT=53 DPT=44314 LEN=120
Sep  9 00:25:09 lamp kernel: [  702.301598] IN=eth0 OUT= MAC=00:15:5d:00:65:12:00:15:5d:01:80:06:08:00 SRC=172.16.0.254 DST=172.
16.0.201 LEN=129 TOS=0x00 PREC=0x00 TTL=64 ID=34603 PROTO=UDP SPT=53 DPT=45835 LEN=109
Sep  9 00:25:09 lamp kernel: [  702.301599] IN=eth0 OUT= MAC=00:15:5d:00:65:12:00:15:5d:01:80:06:08:00 SRC=172.16.0.254 DST=172.
16.0.201 LEN=129 TOS=0x00 PREC=0x00 TTL=64 ID=15857 PROTO=UDP SPT=53 DPT=44314 LEN=109
Sep  9 00:25:09 lamp kernel: [  702.301653] IN=lo OUT= MAC=00:00:00:00:00:00:00:00:00:00:00:00:08:00 SRC=127.0.0.53 DST=127.0.0.
1 LEN=93 TOS=0x00 PREC=0x00 TTL=64 ID=25965 DF PROTO=UDP SPT=53 DPT=54717 LEN=73
Sep  9 00:25:09 lamp kernel: [  702.301713] IN=lo OUT= MAC=00:00:00:00:00:00:00:00:00:00:00:00:08:00 SRC=127.0.0.53 DST=127.0.0.
1 LEN=93 TOS=0x00 PREC=0x00 TTL=64 ID=25966 DF PROTO=UDP SPT=53 DPT=54717 LEN=73
^[S_
```

This command:

`Tail –f /var/log/kern.log`

displays the last ten (10) entries in the log file. The -f parameter will auto-update the result as new entries are added to the log file. Leave that running.

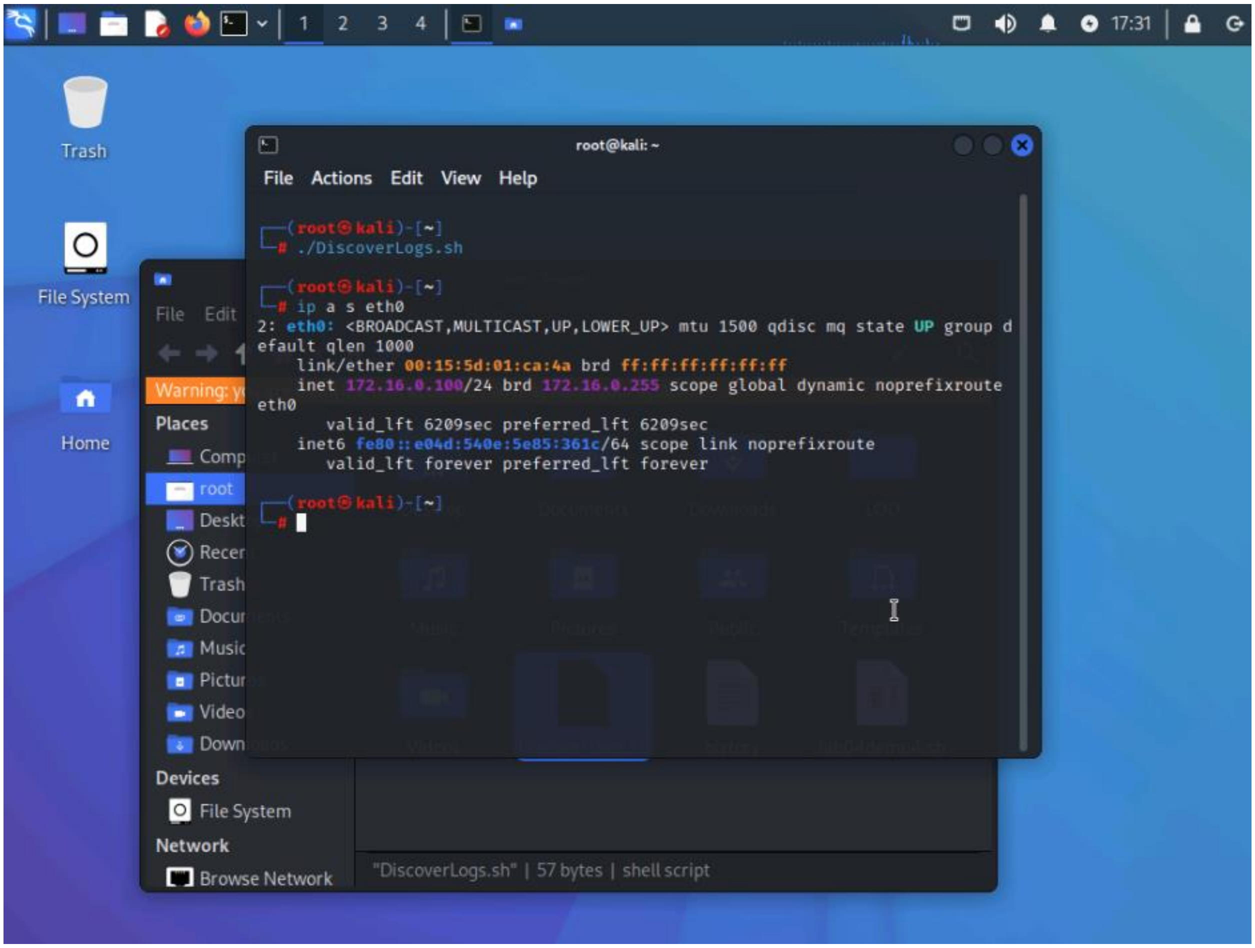
Go to Kali and write the following script to perform an operation for you to discover in the log on LAMP.


DiscoverLogs.sh + (~) - VIM
File Edit Tools Syntax Buffers Window Help

```
#!/bin/bash
nmap 172.16.0.201 -p 1-100 -r -T2 >/dev/null
```

```
-- INSERT --                                        3,1          All
```

Go ahead and run it in the terminal.



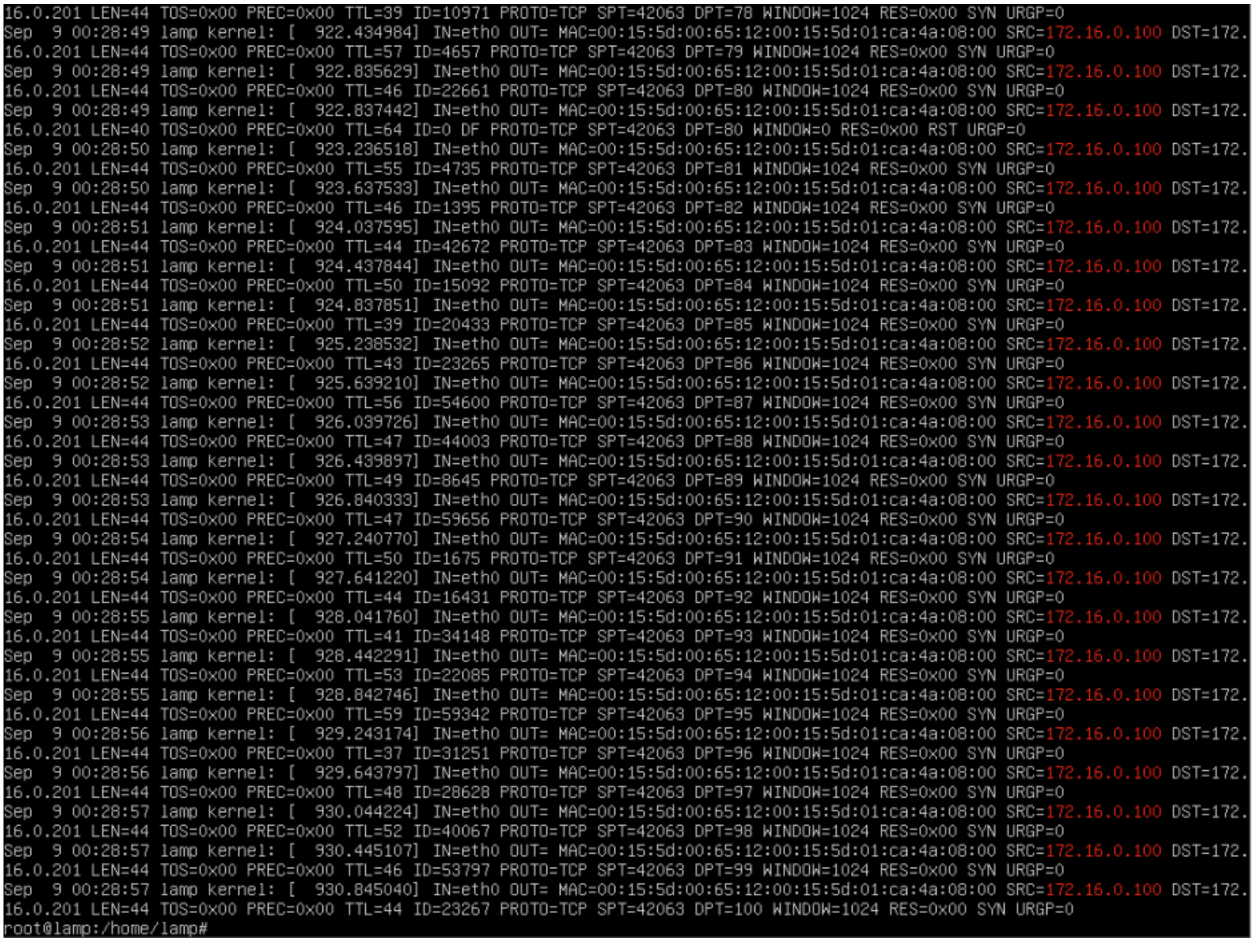
```
┌──(root㉿kali)-[~]
└─# ./DiscoverLogs.sh

┌──(root㉿kali)-[~]
└─# ip a s eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group d
efault qlen 1000
    link/ether 00:15:5d:01:ca:4a brd ff:ff:ff:ff:ff:ff
    inet 172.16.0.100/24 brd 172.16.0.255 scope global dynamic noprefixroute
eth0
       valid_lft 6209sec preferred_lft 6209sec
    inet6 fe80::e04d:540e:5e85:361c/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(root㉿kali)-[~]
└─# 
```

We can also show the IP address of the Kali machine that we will use in LAMP. Go back to LAMP.

As a Cybersecurity Analyst, you suspect that the system using the IPv4 address of 172.16.0.100 is performing unwanted network communications with the lamp system. To investigate this, enter the following:

```
grep 172.16.0.100 /var/log/kern.log
```

This command performs a grep search of the /var/log/kern.log file and displays the entries that match the key term of 172.16.0.100.



```
16.0.201 LEN=44 TOS=0x00 PREC=0x00 TTL=39 ID=10971 PROTO=TCP SPT=42063 DPT=78 WINDOW=1024 RES=0x00 SYN URGP=0
Sep  9 00:28:49 lamp kernel: [  922.434984] IN=eth0 OUT= MAC=00:15:5d:00:65:12:00:15:5d:01:ca:4a:08:00 SRC=172.16.0.100 DST=172.
16.0.201 LEN=44 TOS=0x00 PREC=0x00 TTL=57 ID=4657 PROTO=TCP SPT=42063 DPT=79 WINDOW=1024 RES=0x00 SYN URGP=0
Sep  9 00:28:49 lamp kernel: [  922.835629] IN=eth0 OUT= MAC=00:15:5d:00:65:12:00:15:5d:01:ca:4a:08:00 SRC=172.16.0.100 DST=172.
16.0.201 LEN=44 TOS=0x00 PREC=0x00 TTL=46 ID=22661 PROTO=TCP SPT=42063 DPT=80 WINDOW=1024 RES=0x00 SYN URGP=0
Sep  9 00:28:49 lamp kernel: [  922.837442] IN=eth0 OUT= MAC=00:15:5d:00:65:12:00:15:5d:01:ca:4a:08:00 SRC=172.16.0.100 DST=172.
16.0.201 LEN=40 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=TCP SPT=42063 DPT=80 WINDOW=0 RES=0x00 RST URGP=0
Sep  9 00:28:50 lamp kernel: [  923.236518] IN=eth0 OUT= MAC=00:15:5d:00:65:12:00:15:5d:01:ca:4a:08:00 SRC=172.16.0.100 DST=172.
16.0.201 LEN=44 TOS=0x00 PREC=0x00 TTL=55 ID=4735 PROTO=TCP SPT=42063 DPT=81 WINDOW=1024 RES=0x00 SYN URGP=0
Sep  9 00:28:50 lamp kernel: [  923.637533] IN=eth0 OUT= MAC=00:15:5d:00:65:12:00:15:5d:01:ca:4a:08:00 SRC=172.16.0.100 DST=172.
16.0.201 LEN=44 TOS=0x00 PREC=0x00 TTL=46 ID=1395 PROTO=TCP SPT=42063 DPT=82 WINDOW=1024 RES=0x00 SYN URGP=0
Sep  9 00:28:51 lamp kernel: [  924.037595] IN=eth0 OUT= MAC=00:15:5d:00:65:12:00:15:5d:01:ca:4a:08:00 SRC=172.16.0.100 DST=172.
16.0.201 LEN=44 TOS=0x00 PREC=0x00 TTL=44 ID=42672 PROTO=TCP SPT=42063 DPT=83 WINDOW=1024 RES=0x00 SYN URGP=0
Sep  9 00:28:51 lamp kernel: [  924.437844] IN=eth0 OUT= MAC=00:15:5d:00:65:12:00:15:5d:01:ca:4a:08:00 SRC=172.16.0.100 DST=172.
16.0.201 LEN=44 TOS=0x00 PREC=0x00 TTL=50 ID=15092 PROTO=TCP SPT=42063 DPT=84 WINDOW=1024 RES=0x00 SYN URGP=0
Sep  9 00:28:51 lamp kernel: [  924.837851] IN=eth0 OUT= MAC=00:15:5d:00:65:12:00:15:5d:01:ca:4a:08:00 SRC=172.16.0.100 DST=172.
16.0.201 LEN=44 TOS=0x00 PREC=0x00 TTL=39 ID=20433 PROTO=TCP SPT=42063 DPT=85 WINDOW=1024 RES=0x00 SYN URGP=0
Sep  9 00:28:52 lamp kernel: [  925.238532] IN=eth0 OUT= MAC=00:15:5d:00:65:12:00:15:5d:01:ca:4a:08:00 SRC=172.16.0.100 DST=172.
16.0.201 LEN=44 TOS=0x00 PREC=0x00 TTL=43 ID=23265 PROTO=TCP SPT=42063 DPT=86 WINDOW=1024 RES=0x00 SYN URGP=0
Sep  9 00:28:52 lamp kernel: [  925.639210] IN=eth0 OUT= MAC=00:15:5d:00:65:12:00:15:5d:01:ca:4a:08:00 SRC=172.16.0.100 DST=172.
16.0.201 LEN=44 TOS=0x00 PREC=0x00 TTL=56 ID=54600 PROTO=TCP SPT=42063 DPT=87 WINDOW=1024 RES=0x00 SYN URGP=0
Sep  9 00:28:53 lamp kernel: [  926.039726] IN=eth0 OUT= MAC=00:15:5d:00:65:12:00:15:5d:01:ca:4a:08:00 SRC=172.16.0.100 DST=172.
16.0.201 LEN=44 TOS=0x00 PREC=0x00 TTL=47 ID=44003 PROTO=TCP SPT=42063 DPT=88 WINDOW=1024 RES=0x00 SYN URGP=0
Sep  9 00:28:53 lamp kernel: [  926.439897] IN=eth0 OUT= MAC=00:15:5d:00:65:12:00:15:5d:01:ca:4a:08:00 SRC=172.16.0.100 DST=172.
16.0.201 LEN=44 TOS=0x00 PREC=0x00 TTL=49 ID=8645 PROTO=TCP SPT=42063 DPT=89 WINDOW=1024 RES=0x00 SYN URGP=0
Sep  9 00:28:53 lamp kernel: [  926.840333] IN=eth0 OUT= MAC=00:15:5d:00:65:12:00:15:5d:01:ca:4a:08:00 SRC=172.16.0.100 DST=172.
16.0.201 LEN=44 TOS=0x00 PREC=0x00 TTL=47 ID=59656 PROTO=TCP SPT=42063 DPT=90 WINDOW=1024 RES=0x00 SYN URGP=0
Sep  9 00:28:54 lamp kernel: [  927.240770] IN=eth0 OUT= MAC=00:15:5d:00:65:12:00:15:5d:01:ca:4a:08:00 SRC=172.16.0.100 DST=172.
16.0.201 LEN=44 TOS=0x00 PREC=0x00 TTL=50 ID=1675 PROTO=TCP SPT=42063 DPT=91 WINDOW=1024 RES=0x00 SYN URGP=0
Sep  9 00:28:54 lamp kernel: [  927.641220] IN=eth0 OUT= MAC=00:15:5d:00:65:12:00:15:5d:01:ca:4a:08:00 SRC=172.16.0.100 DST=172.
16.0.201 LEN=44 TOS=0x00 PREC=0x00 TTL=44 ID=16431 PROTO=TCP SPT=42063 DPT=92 WINDOW=1024 RES=0x00 SYN URGP=0
Sep  9 00:28:55 lamp kernel: [  928.041760] IN=eth0 OUT= MAC=00:15:5d:00:65:12:00:15:5d:01:ca:4a:08:00 SRC=172.16.0.100 DST=172.
16.0.201 LEN=44 TOS=0x00 PREC=0x00 TTL=41 ID=34148 PROTO=TCP SPT=42063 DPT=93 WINDOW=1024 RES=0x00 SYN URGP=0
Sep  9 00:28:55 lamp kernel: [  928.442291] IN=eth0 OUT= MAC=00:15:5d:00:65:12:00:15:5d:01:ca:4a:08:00 SRC=172.16.0.100 DST=172.
16.0.201 LEN=44 TOS=0x00 PREC=0x00 TTL=53 ID=22085 PROTO=TCP SPT=42063 DPT=94 WINDOW=1024 RES=0x00 SYN URGP=0
Sep  9 00:28:55 lamp kernel: [  928.842746] IN=eth0 OUT= MAC=00:15:5d:00:65:12:00:15:5d:01:ca:4a:08:00 SRC=172.16.0.100 DST=172.
16.0.201 LEN=44 TOS=0x00 PREC=0x00 TTL=59 ID=59342 PROTO=TCP SPT=42063 DPT=95 WINDOW=1024 RES=0x00 SYN URGP=0
Sep  9 00:28:56 lamp kernel: [  929.243174] IN=eth0 OUT= MAC=00:15:5d:00:65:12:00:15:5d:01:ca:4a:08:00 SRC=172.16.0.100 DST=172.
16.0.201 LEN=44 TOS=0x00 PREC=0x00 TTL=37 ID=31251 PROTO=TCP SPT=42063 DPT=96 WINDOW=1024 RES=0x00 SYN URGP=0
Sep  9 00:28:56 lamp kernel: [  929.643797] IN=eth0 OUT= MAC=00:15:5d:00:65:12:00:15:5d:01:ca:4a:08:00 SRC=172.16.0.100 DST=172.
16.0.201 LEN=44 TOS=0x00 PREC=0x00 TTL=48 ID=28628 PROTO=TCP SPT=42063 DPT=97 WINDOW=1024 RES=0x00 SYN URGP=0
Sep  9 00:28:57 lamp kernel: [  930.044224] IN=eth0 OUT= MAC=00:15:5d:00:65:12:00:15:5d:01:ca:4a:08:00 SRC=172.16.0.100 DST=172.
16.0.201 LEN=44 TOS=0x00 PREC=0x00 TTL=52 ID=40067 PROTO=TCP SPT=42063 DPT=98 WINDOW=1024 RES=0x00 SYN URGP=0
Sep  9 00:28:57 lamp kernel: [  930.445107] IN=eth0 OUT= MAC=00:15:5d:00:65:12:00:15:5d:01:ca:4a:08:00 SRC=172.16.0.100 DST=172.
16.0.201 LEN=44 TOS=0x00 PREC=0x00 TTL=46 ID=53797 PROTO=TCP SPT=42063 DPT=99 WINDOW=1024 RES=0x00 SYN URGP=0
Sep  9 00:28:57 lamp kernel: [  930.845040] IN=eth0 OUT= MAC=00:15:5d:00:65:12:00:15:5d:01:ca:4a:08:00 SRC=172.16.0.100 DST=172.
16.0.201 LEN=44 TOS=0x00 PREC=0x00 TTL=44 ID=23267 PROTO=TCP SPT=42063 DPT=100 WINDOW=1024 RES=0x00 SYN URGP=0
root@lamp:/home/lamp#
```

After reviewing the logs, it is clear that the attacking machine was conducting a port scan—an evident Indicator of Compromise (IoC).

Through this project, I identified the distinct pattern of port scanning, which occurs when a single source IP makes repeated connection attempts across multiple ports. In this case, the attacker systematically scanned ports 1 through 100 in numerical order, highlighting a classic reconnaissance technique used to probe for potential vulnerabilities.