ATTACK DEFENSE

by PentesterAcademy

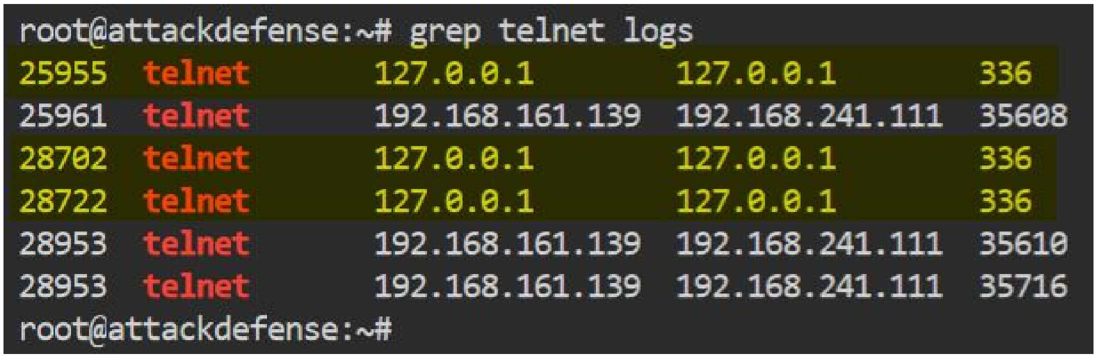
Name	Tcpv4connect: Log Analysis
URL	https://attackdefense.com/challengedetails?cid=1109
Type	Linux Runtime Analysis: Profiling Tools

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Q1. Identify the port on which telnet is running on the server.

Answer: 336

Command: grep telnet logs

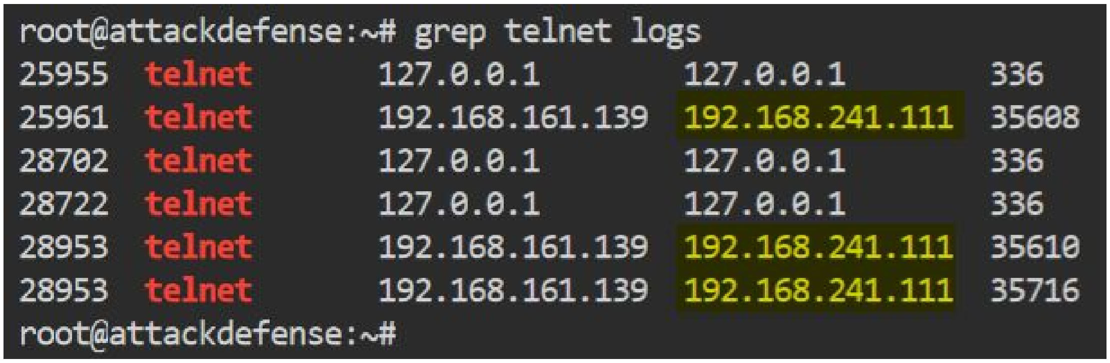


```
root@attackdefense:~# grep telnet logs
25955  telnet      127.0.0.1        127.0.0.1        336
25961  telnet      192.168.161.139  192.168.241.111  35608
28702  telnet      127.0.0.1        127.0.0.1        336
28722  telnet      127.0.0.1        127.0.0.1        336
28953  telnet      192.168.161.139  192.168.241.111  35610
28953  telnet      192.168.161.139  192.168.241.111  35716
root@attackdefense:~#
```

Q2. What the IP address of the remote machine which connected to the server using telnet?

Answer: 192.168.241.111

Command: grep telnet logs

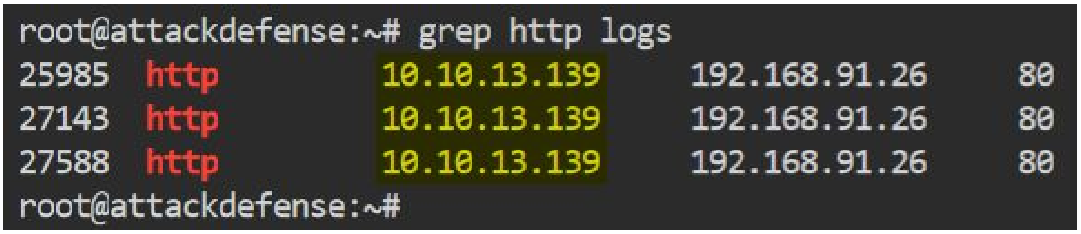


```
root@attackdefense:~# grep telnet logs
25955  telnet      127.0.0.1        127.0.0.1        336
25961  telnet      192.168.161.139  192.168.241.111  35608
28702  telnet      127.0.0.1        127.0.0.1        336
28722  telnet      127.0.0.1        127.0.0.1        336
28953  telnet      192.168.161.139  192.168.241.111  35610
28953  telnet      192.168.161.139  192.168.241.111  35716
root@attackdefense:~#
```

Q3. The server has downloaded data files over HTTP using a different network interface. What is the IP address of that interface?

Answer: 10.10.13.139

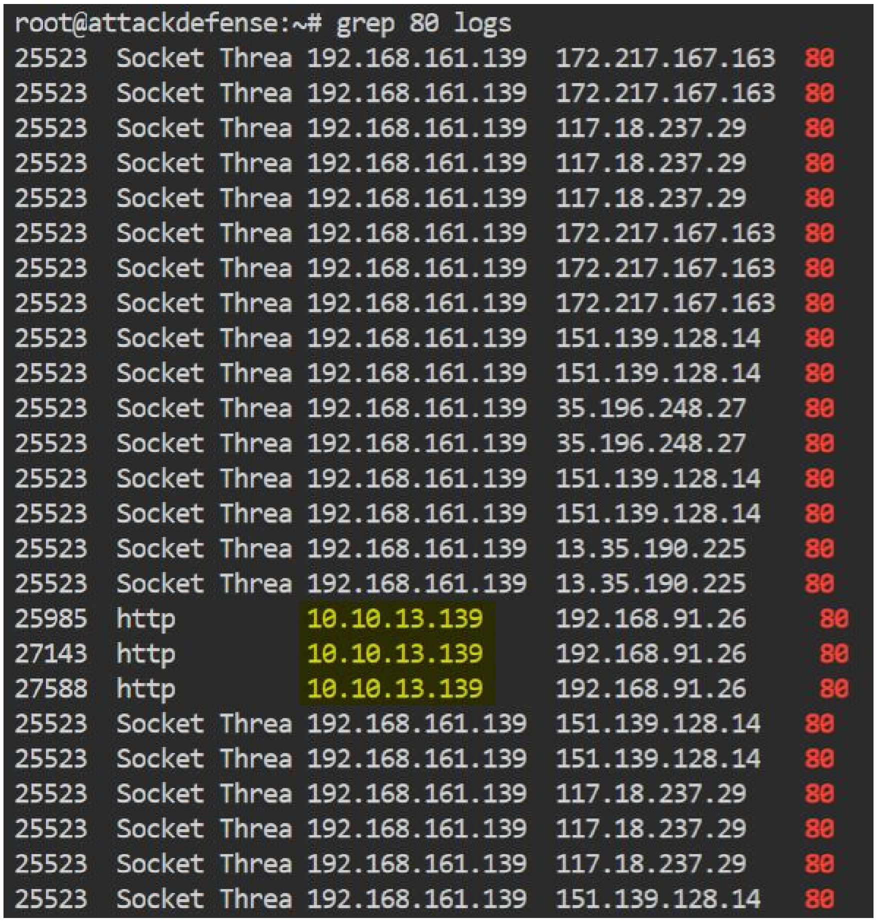
Command: grep http logs



```
root@attackdefense:~# grep http logs
25985  http          10.10.13.139     192.168.91.26     80
27143  http          10.10.13.139     192.168.91.26     80
27588  http          10.10.13.139     192.168.91.26     80
root@attackdefense:~#
```

OR

Command: grep 80 logs

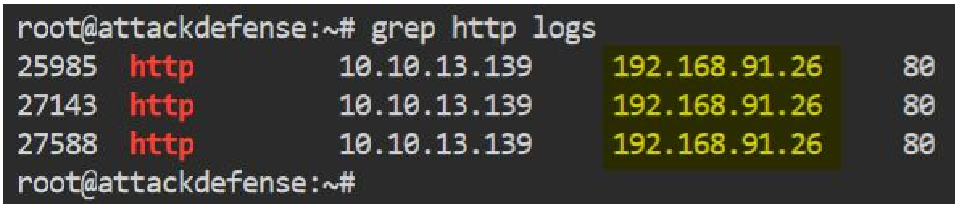


```
root@attackdefense:~# grep 80 logs
25523  Socket Threa 192.168.161.139  172.217.167.163  80
25523  Socket Threa 192.168.161.139  172.217.167.163  80
25523  Socket Threa 192.168.161.139  117.18.237.29    80
25523  Socket Threa 192.168.161.139  117.18.237.29    80
25523  Socket Threa 192.168.161.139  117.18.237.29    80
25523  Socket Threa 192.168.161.139  172.217.167.163  80
25523  Socket Threa 192.168.161.139  172.217.167.163  80
25523  Socket Threa 192.168.161.139  172.217.167.163  80
25523  Socket Threa 192.168.161.139  151.139.128.14   80
25523  Socket Threa 192.168.161.139  151.139.128.14   80
25523  Socket Threa 192.168.161.139  35.196.248.27    80
25523  Socket Threa 192.168.161.139  35.196.248.27    80
25523  Socket Threa 192.168.161.139  151.139.128.14   80
25523  Socket Threa 192.168.161.139  151.139.128.14   80
25523  Socket Threa 192.168.161.139  13.35.190.225    80
25523  Socket Threa 192.168.161.139  13.35.190.225    80
25985  http         10.10.13.139     192.168.91.26     80
27143  http         10.10.13.139     192.168.91.26     80
27588  http         10.10.13.139     192.168.91.26     80
25523  Socket Threa 192.168.161.139  151.139.128.14   80
25523  Socket Threa 192.168.161.139  151.139.128.14   80
25523  Socket Threa 192.168.161.139  117.18.237.29    80
25523  Socket Threa 192.168.161.139  117.18.237.29    80
25523  Socket Threa 192.168.161.139  117.18.237.29    80
25523  Socket Threa 192.168.161.139  151.139.128.14   80
```

Q4. What is the IP address of the remote machine from which the packages were downloaded?

Answer: 192.168.91.26

Command: grep http logs



```
root@attackdefense:~# grep http logs
25985  http         10.10.13.139     192.168.91.26      80
27143  http         10.10.13.139     192.168.91.26      80
27588  http         10.10.13.139     192.168.91.26      80
root@attackdefense:~#
```

References:

1. Tcpv4connect script (https://github.com/iovisor/bcc/blob/master/examples/tracing/tcpv4connect.py)
2. Tcpv4connect Examples (https://github.com/iovisor/bcc/blob/master/examples/tracing/tcpv4connect_example.txt)
3. BCC Tools (https://github.com/iovisor/bcc)