
ATTACK
DEFENSE
by PentesterAcademy

Name	Tcptracer: Log Analysis
URL	https://attackdefense.com/challengedetails?cid=1108
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 SSH is running.

Answer: 3603

Command: grep ssh logs

```
root@attackdefense:~# grep ssh logs
A  1341   sshd            4  192.168.161.139  192.168.161.36   3603   34989
X  1341   sshd            4  192.168.161.139  192.168.161.36   3603   34989
root@attackdefense:~#
```

Q2. What is the IP address of the client that logged into the machine using SSH?

Answer: 192.168.161.36

Command: grep ssh logs

```
root@attackdefense:~# grep ssh logs
A  1341   sshd            4  192.168.161.139  192.168.161.36   3603   34989
X  1341   sshd            4  192.168.161.139  192.168.161.36   3603   34989
root@attackdefense:~#
```

Q3. A remote machine is running a service on port 2701. The local system downloads some files from that service. What is the IP address of the remote machine?

Answer: 10.10.79.35

Command: grep 2701 logs

```
root@attackdefense:~# grep 2701 logs
C  21734  wget            4  192.168.161.139  10.10.79.35     45700  2701
C  21734  wget            4  192.168.161.139  10.10.79.35     45702  2701
X  21734  wget            4  192.168.161.139  10.10.79.35     45700  2701
X  21734  wget            4  192.168.161.139  10.10.79.35     45702  2701
root@attackdefense:~#
```

Q4. What the name of the utility used to download the files from the remote service running on port 2701?

Answer: wget

Command: grep 2701 logs

```
root@attackdefense:~# grep 2701 logs
C  21734  wget            4  192.168.161.139  10.10.79.35     45700  2701
C  21734  wget            4  192.168.161.139  10.10.79.35     45702  2701
X  21734  wget            4  192.168.161.139  10.10.79.35     45700  2701
X  21734  wget            4  192.168.161.139  10.10.79.35     45702  2701
root@attackdefense:~#
```

Q5. The machine sends system metrics to a remote machine using curl. What is the IP address of the remote machine?

Answer: 172.17.3.36

Command: grep curl logs

```
root@attackdefense:~# grep curl logs
C  21735  curl            4  192.168.161.139  172.17.3.36     42670  80
X  21735  curl            4  192.168.161.139  172.17.3.36     42670  80
root@attackdefense:~#
```

References:

1. Tcptracer script (https://github.com/iovisor/bcc/blob/master/tools/tcptracer.py)
2. Tcptracer Examples (https://github.com/iovisor/bcc/blob/master/tools/tcptracer_example.txt)
3. BCC Tools (https://github.com/iovisor/bcc)