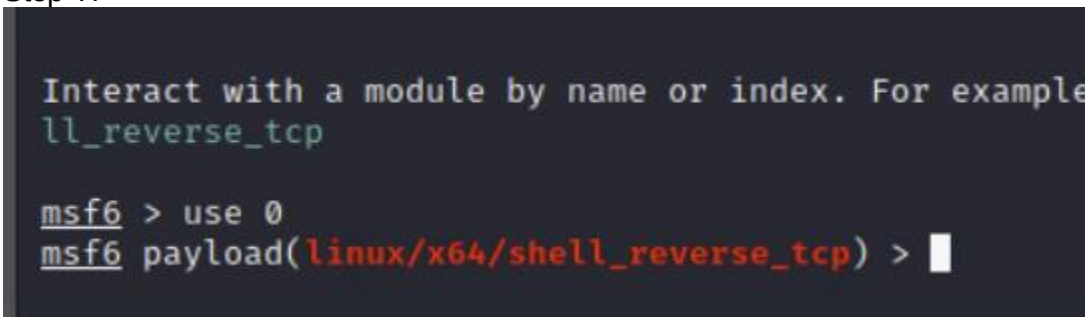
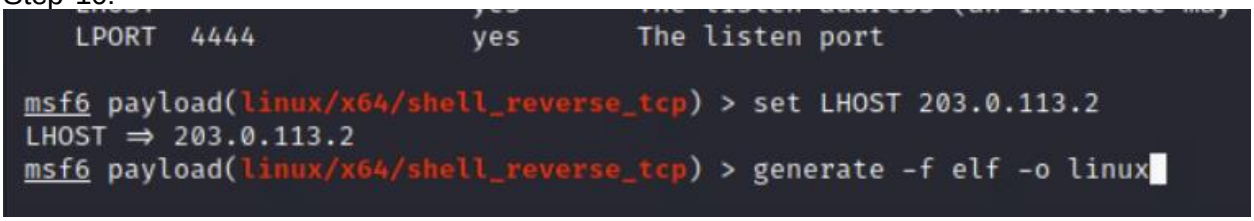
Peter Sanford
IT 2700
NetLab Lab 22
11/04/2023

1.1
Step 7:

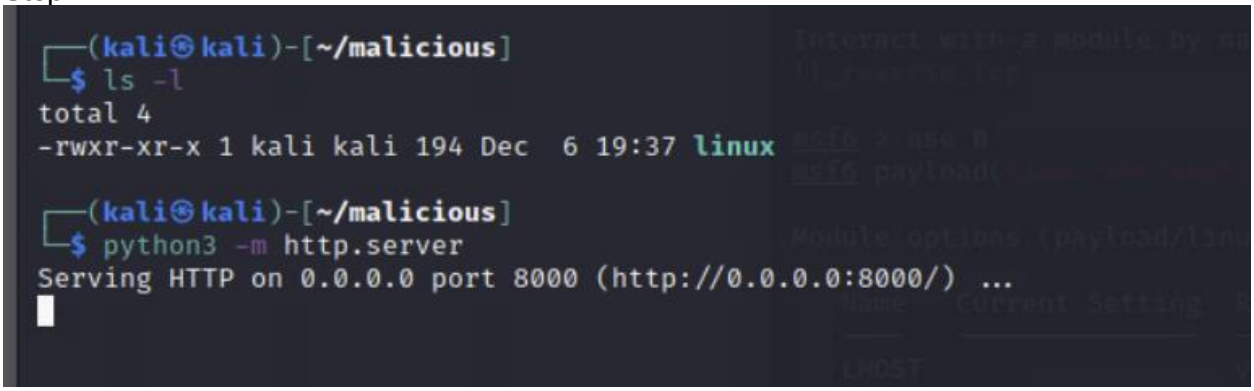


Step 10:

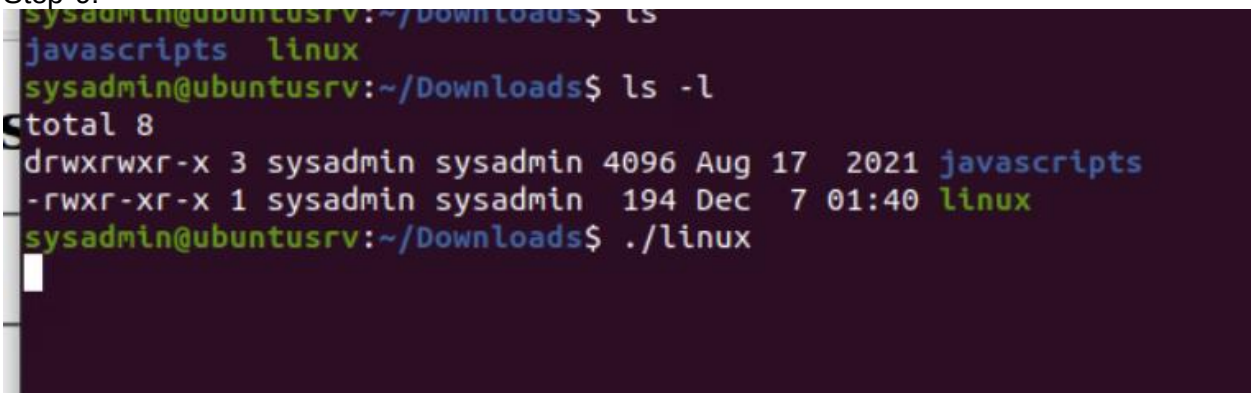


Step 13:

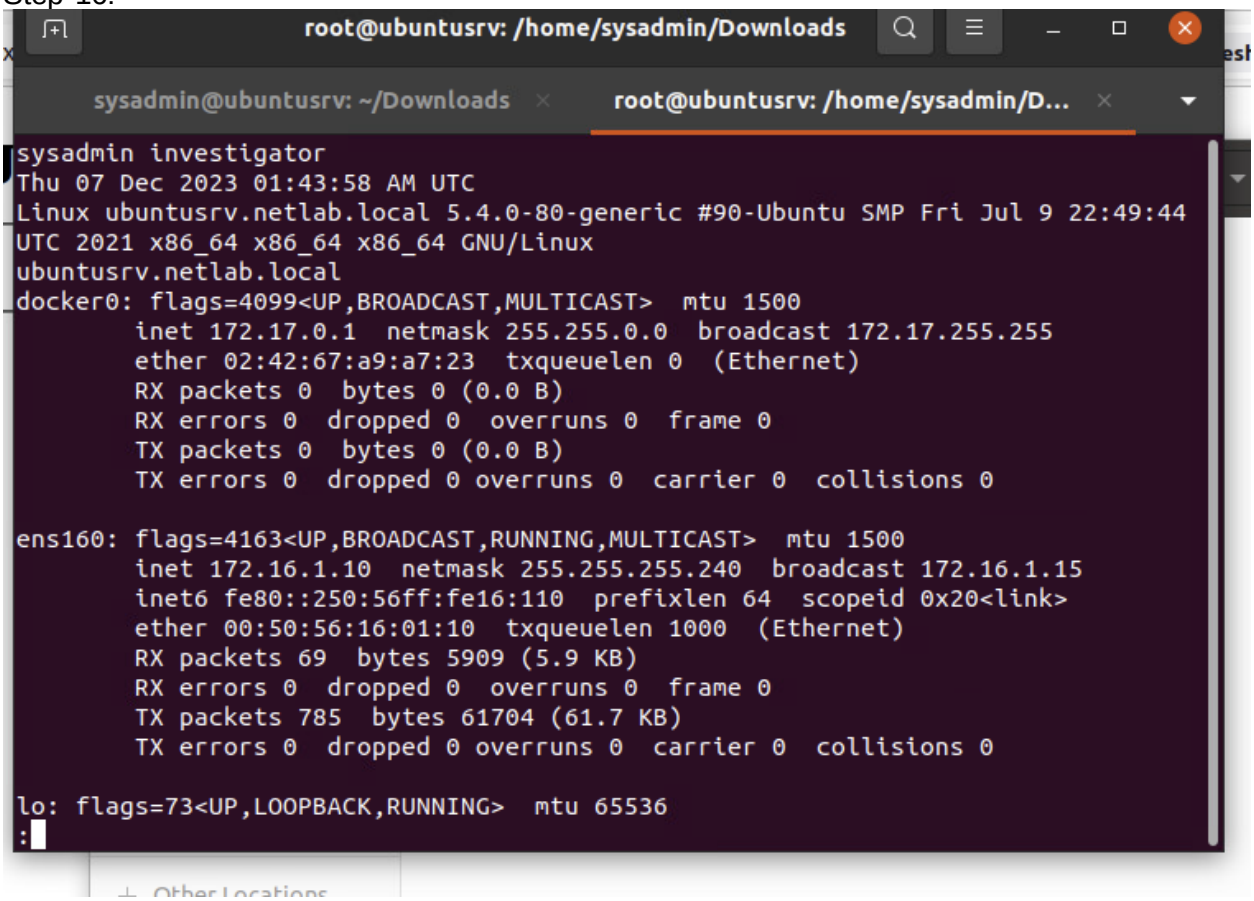
1.2
Step 4:



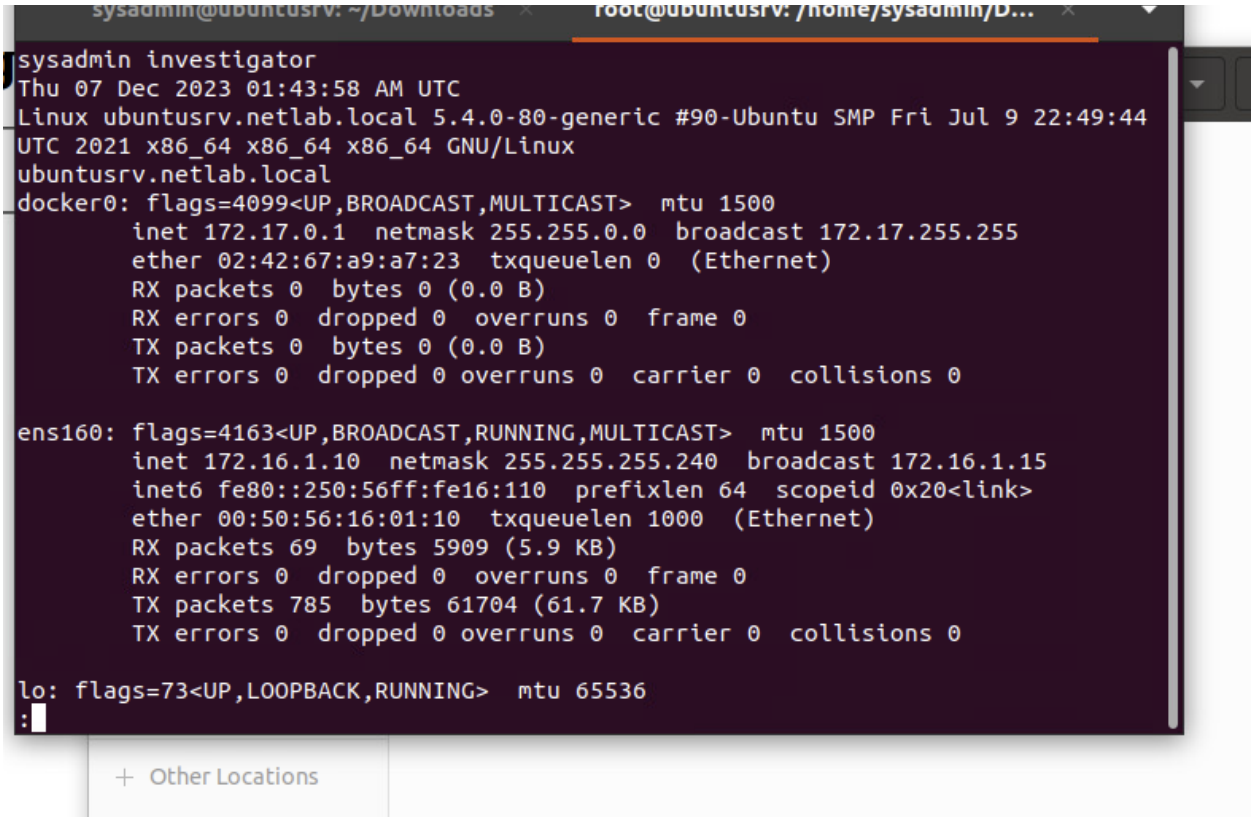
1.3
Step 9:



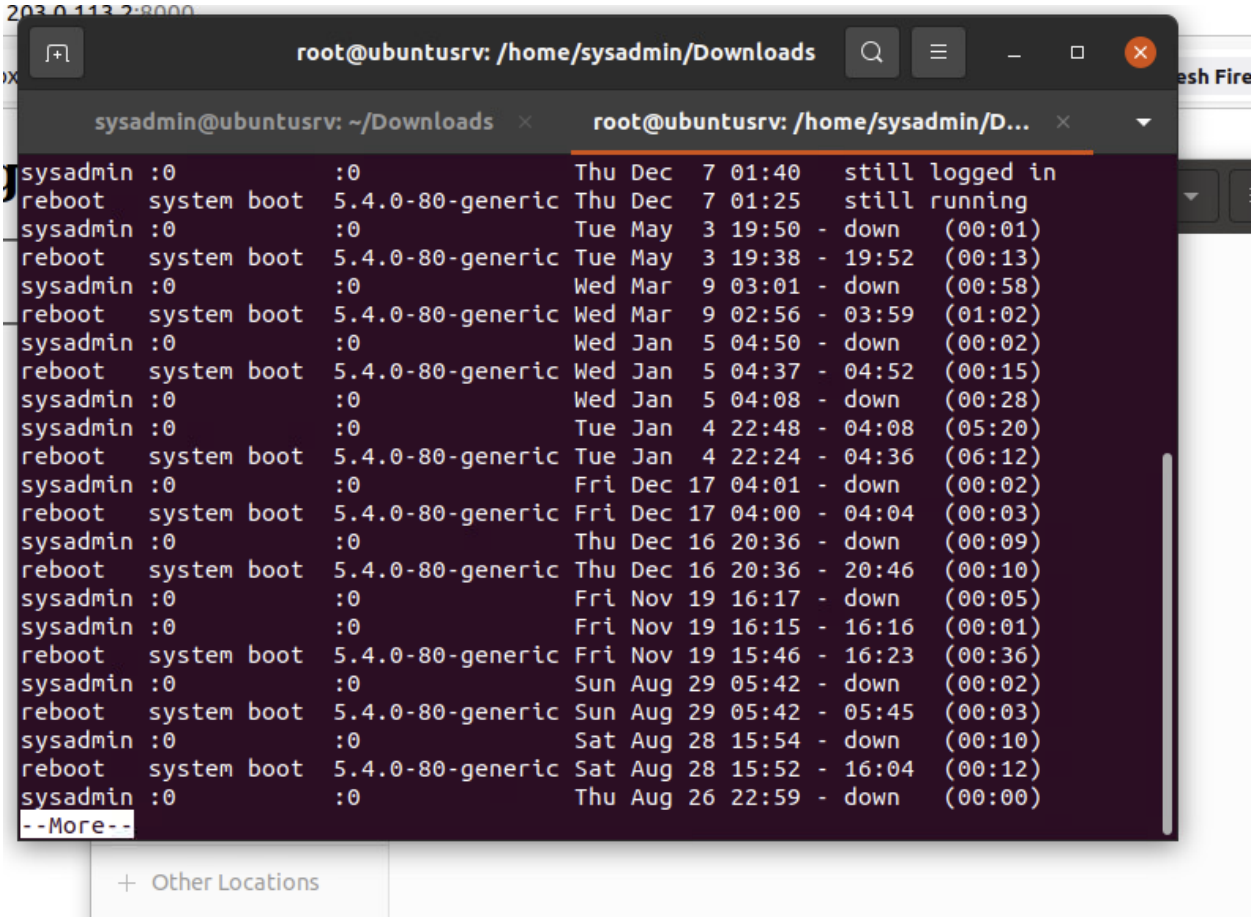
2.1
Step 16:



3.1
Step 1:


sysadmin@ubuntusrv: ~/Downloads
root@ubuntusrv: /home/sysadmin/D...
sysadmin investigator
Thu 07 Dec 2023 01:43:58 AM UTC
Linux ubuntusrv.netlab.local 5.4.0-80-generic #90-Ubuntu SMP Fri Jul 9 22:49:44
UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
ubuntusrv.netlab.local
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
ether 02:42:67:a9:a7:23 txqueuelen 0 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 172.16.1.10 netmask 255.255.255.240 broadcast 172.16.1.15
inet6 fe80::250:56ff:fe16:110 prefixlen 64 scopeid 0x20<link>
ether 00:50:56:16:01:10 txqueuelen 1000 (Ethernet)
RX packets 69 bytes 5909 (5.9 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 785 bytes 61704 (61.7 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
:
Other Locations

Step 4:



Commentary:

In this lab we viewed out linux logs after a compromise to see what clues there are to infiltrators. I learned what the logs look like when there's an infiltrator and someone logged into your account that you don't expect. Knowing this information, companies can go through their log files regularly and make sure there isn't any unexpected entries.