The nmap-ssh lab

Overview

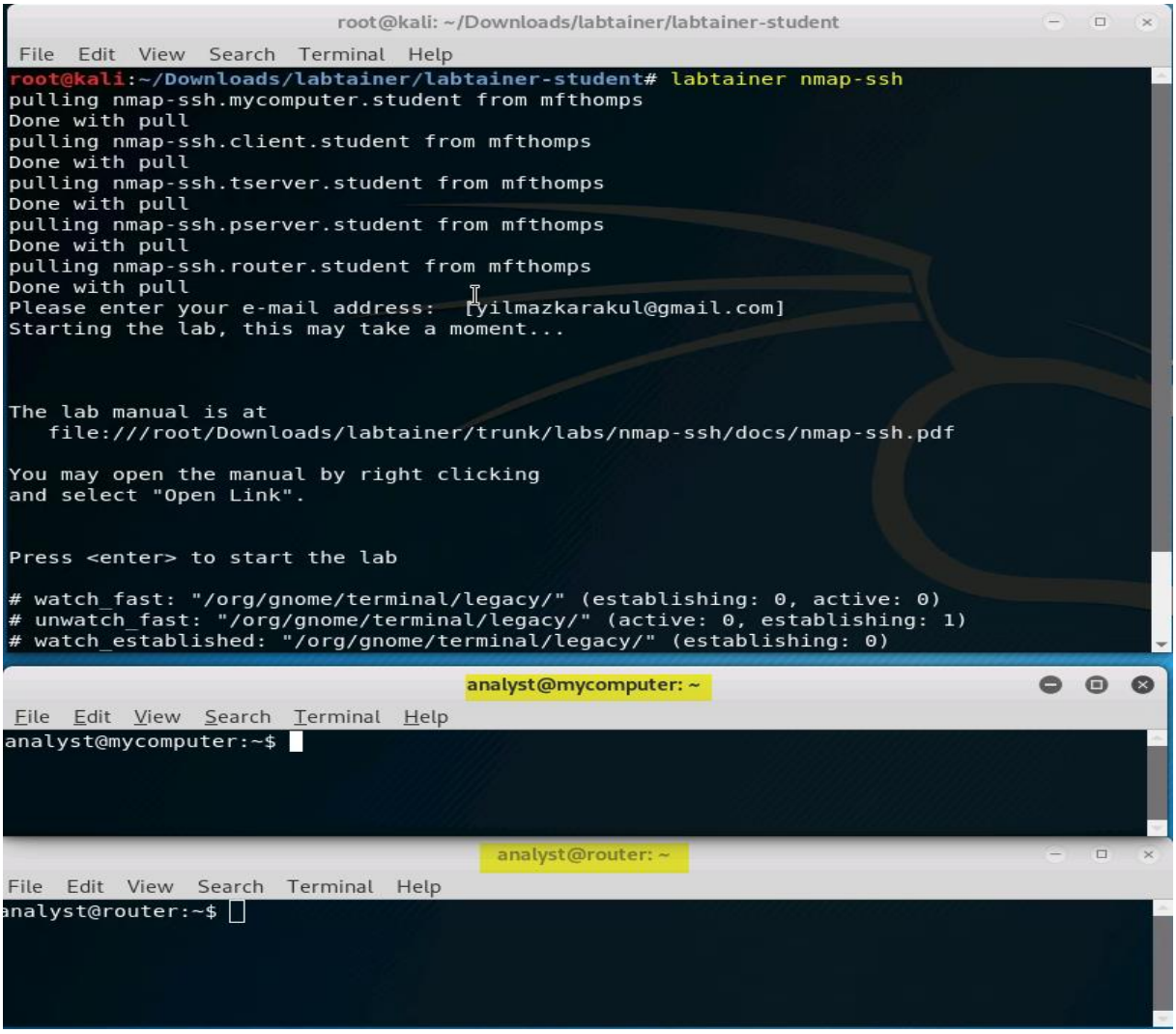
This labtainer exercise uses nmap and skills exercised in previous labtainer labs to identify and exploit a weakness in a system.

You are performing ad-hoc security testing for a client who believes their internal SSH server is relatively secure, but you would like to confirm the validity of this. Your goal is to attempt to remotely access that SSH server and disclose the content of a selected file.

Performing the lab

The lab is started from the labtainer working directory on your Linux host, e.g., a Linux VM. From there, issue the command:

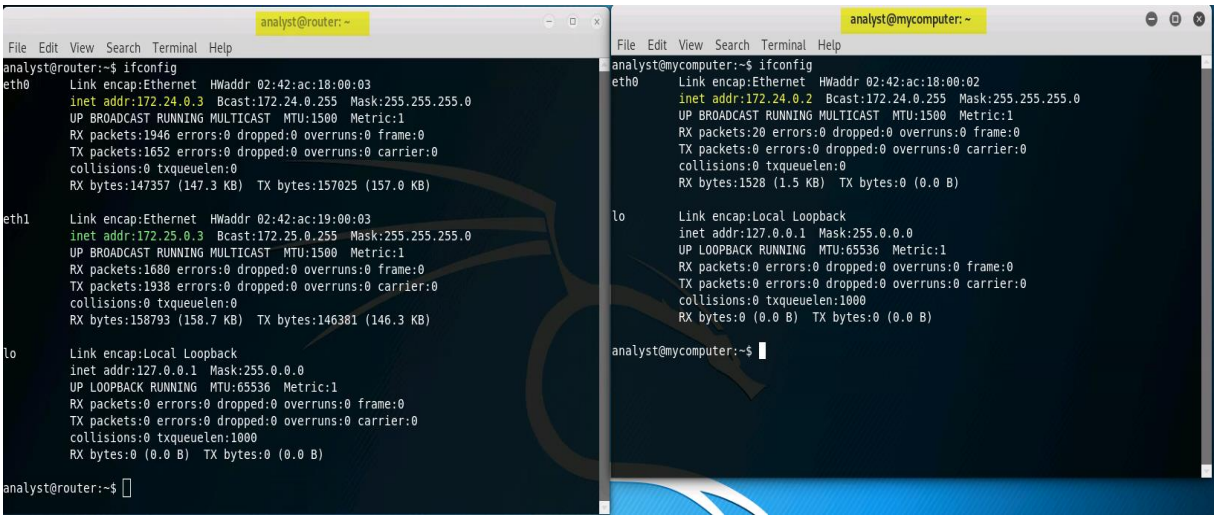
```
labtainer nmap-ssh
```

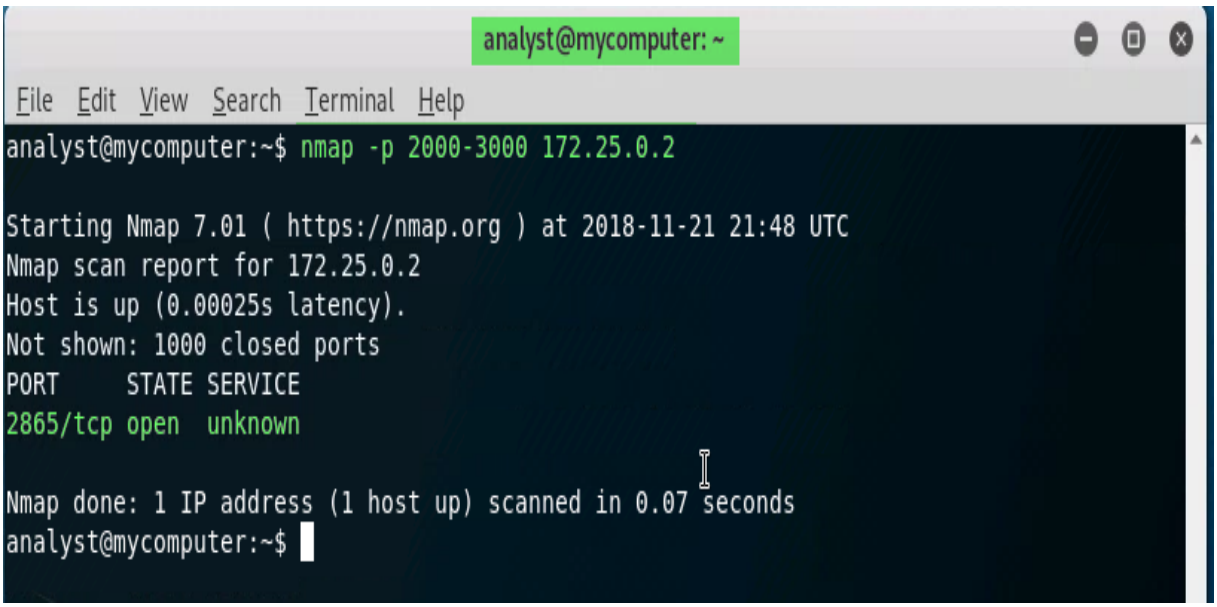


The resulting virtual terminal will include a bash shell on a computer called “MyComputer”. The nmap utility is pre-installed on that computer. You will also have a virtual terminal connected to a “router”, and a bash shell there. You have been told that the router sits between the organization’s client workstations and the servers.

Tasks

You have been told the target SSH server IP address is 172.25.0.2 and the SSH port number changes frequently within the range of 2000-3000. you have been given an account, “analysis” on the client computer and on the router.





Client computers <===> [Router]<===> servers

your goal is to successfully SSH from “MyComputer” into the “ubuntu” account on the SSH server.

```
analyst@router:~$ nmap -p 1-65500 172.24.0.0/24

Starting Nmap 7.01 ( https://nmap.org ) at 2018-12-04 21:54 UTC
Nmap scan report for nmap-ssh.client.student.client_network (172.24.0.1)
Host is up (0.00078s latency).
All 65500 scanned ports on nmap-ssh.client.student.client_network (172.24.0.1) are closed

Nmap scan report for nmap-ssh.mycomputer.student.client_network (172.24.0.2)
Host is up (0.00064s latency).
All 65500 scanned ports on nmap-ssh.mycomputer.student.client_network (172.24.0.2) are closed

Nmap scan report for router (172.24.0.3)
Host is up (0.00013s latency).
All 65500 scanned ports on router (172.24.0.3) are closed

Nmap scan report for 172.24.0.101
Host is up (0.00061s latency).
Not shown: 65497 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
3389/tcp open  ms-wbt-server
5900/tcp open  vnc

Nmap done: 256 IP addresses (4 hosts up) scanned in 11.60 seconds
analyst@router:~$
```

```
analyst@router: ~
File  Edit  View  Search  Terminal  Help
analyst@router:~$ nmap -p 1-65500 172.25.0.0/24

Starting Nmap 7.01 ( https://nmap.org ) at 2018-12-04 21:56 UTC
Nmap scan report for nmap-ssh.tserver.student.server_network (172.25.0.1)
Host is up (0.00073s latency).
Not shown: 65498 closed ports
PORT   STATE SERVICE
23/tcp open  telnet
80/tcp open  http

Nmap scan report for nmap-ssh.pserver.student.server_network (172.25.0.2)
Host is up (0.00076s latency).
Not shown: 65499 closed ports
PORT     STATE SERVICE
2865/tcp open  unknown

Nmap scan report for router (172.25.0.3)
Host is up (0.00012s latency).
All 65500 scanned ports on router (172.25.0.3) are closed

Nmap scan report for 172.25.0.101
Host is up (0.00054s latency).
Not shown: 65497 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
3389/tcp open  ms-wbt-server
5900/tcp open  vnc

Nmap done: 256 IP addresses (4 hosts up) scanned in 11.39 seconds
analyst@router:~$
```

Hints:

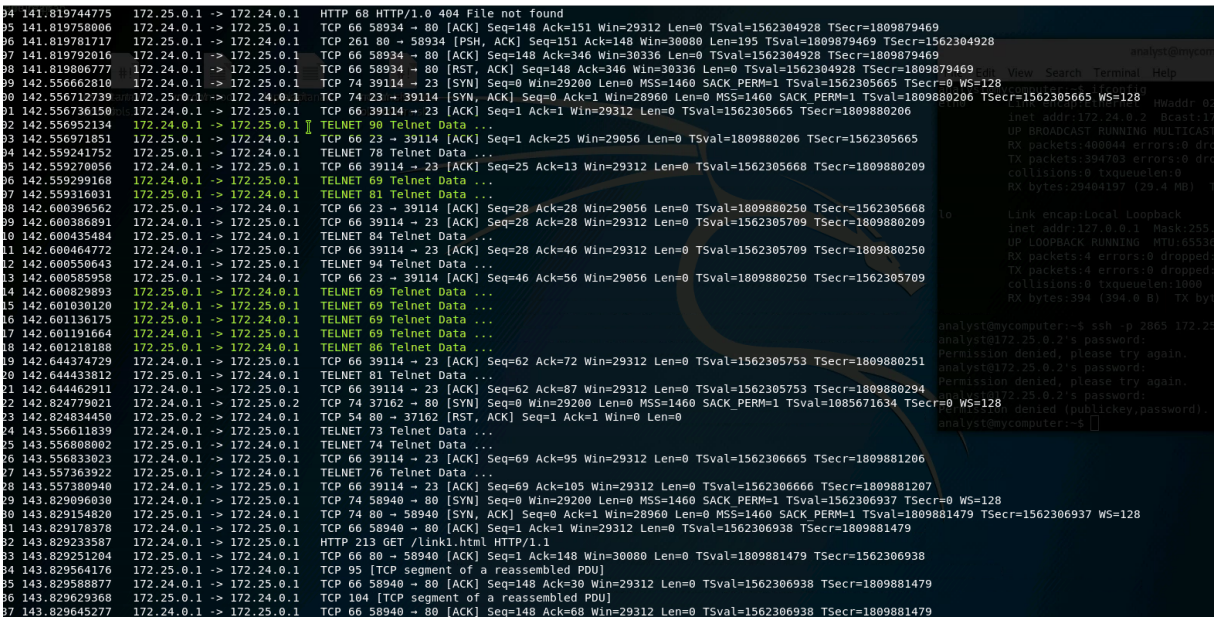
- nmap is installed on mycomputer.
- tshark and tcpdump are installed on the router
- What other password protected network services are being used on the network? And by who?

```
analyst@router: ~
File  Edit  View  Search  Terminal  Help
analyst@router:~$ sudo tcpdump -i eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
22:02:38.590135 IP nmap-ssh.client.student.client_network.35306 > nmap-ssh.pserver.student.server_network.http: Flags [S], seq 2199971567, win 29200, options [mss 1460,sackOK,TS val 1084830689 ecr 0,nop,wscal
], length 0
22:02:38.590216 IP nmap-ssh.pserver.student.server_network.http > nmap-ssh.client.student.client_network.35306: Flags [R.], seq 0, ack 2199971568, win 0, length 0
22:02:39.594779 IP nmap-ssh.client.student.client_network.57084 > nmap-ssh.tserver.student.server_network.http: Flags [S], seq 3550080221, win 29200, options [mss 1460,sackOK,TS val 1561465992 ecr 0,nop,wscal
], length 0
22:02:39.594849 IP nmap-ssh.tserver.student.server_network.http > nmap-ssh.client.student.client_network.57084: Flags [S.], seq 2991428284, ack 3550080222, win 28960, options [mss 1460,sackOK,TS val 180904053
cr 1561465992,nop,wscale 7], length 0
22:02:39.594872 IP nmap-ssh.client.student.client_network.57084 > nmap-ssh.tserver.student.server_network.http: Flags [.], ack 1, win 229, options [nop,nop,TS val 1561465992 ecr 1809040533], length 0
22:02:39.594928 IP nmap-ssh.client.student.client_network.57084 > nmap-ssh.tserver.student.server_network.http: Flags [P.], seq 1:148, ack 1, win 229, options [nop,nop,TS val 1561465992 ecr 1809040533], lengt
47: HTTP: GET /link1.html HTTP/1.1
22:02:39.594945 IP nmap-ssh.tserver.student.server_network.http > nmap-ssh.client.student.client_network.57084: Flags [.], ack 148, win 235, options [nop,nop,TS val 1809040533 ecr 1561465992], length 0
22:02:39.595415 IP nmap-ssh.tserver.student.server_network.http > nmap-ssh.client.student.client_network.57084: Flags [P.], seq 1:30, ack 148, win 235, options [nop,nop,TS val 1809040534 ecr 1561465992], leng
29: HTTP: HTTP/1.0 404 File not found
22:02:39.595453 IP nmap-ssh.client.student.client_network.57084 > nmap-ssh.tserver.student.server_network.http: Flags [.], ack 30, win 229, options [nop,nop,TS val 1561465993 ecr 1809040534], length 0
22:02:39.595507 IP nmap-ssh.tserver.student.server_network.http > nmap-ssh.client.student.client_network.57084: Flags [P.], seq 30:68, ack 148, win 235, options [nop,nop,TS val 1809040534 ecr 1561465993], len
 38: HTTP
22:02:39.595528 IP nmap-ssh.client.student.client_network.57084 > nmap-ssh.tserver.student.server_network.http: Flags [.], ack 68, win 229, options [nop,nop,TS val 1561465993 ecr 1809040534], length 0
22:02:39.595604 IP nmap-ssh.tserver.student.server_network.http > nmap-ssh.client.student.client_network.57084: Flags [P.], seq 68:105, ack 148, win 235, options [nop,nop,TS val 1809040534 ecr 1561465993], le
h 37: HTTP
22:02:39.595620 IP nmap-ssh.client.student.client_network.57084 > nmap-ssh.tserver.student.server_network.http: Flags [.], ack 105, win 229, options [nop,nop,TS val 1561465993 ecr 1809040534], length 0
22:02:39.595667 IP nmap-ssh.tserver.student.server_network.http > nmap-ssh.client.student.client_network.57084: Flags [P.], seq 105:124, ack 148, win 235, options [nop,nop,TS val 1809040534 ecr 1561465993], l
th 19: HTTP
22:02:39.595685 IP nmap-ssh.client.student.client_network.57084 > nmap-ssh.tserver.student.server_network.http: Flags [.], ack 124, win 229, options [nop,nop,TS val 1561465993 ecr 1809040534], length 0
22:02:39.595747 IP nmap-ssh.tserver.student.server_network.http > nmap-ssh.client.student.client_network.57084: Flags [P.], seq 124:149, ack 148, win 235, options [nop,nop,TS val 1809040534 ecr 1561465993], l
th 25: HTTP
22:02:39.595767 IP nmap-ssh.client.student.client_network.57084 > nmap-ssh.tserver.student.server_network.http: Flags [.], ack 149, win 229, options [nop,nop,TS val 1561465993 ecr 1809040534], length 0
22:02:39.595816 IP nmap-ssh.tserver.student.server_network.http > nmap-ssh.client.student.client_network.57084: Flags [P.], seq 149:151, ack 148, win 235, options [nop,nop,TS val 1809040534 ecr 1561465993], l
th 2: HTTP
22:02:39.595838 IP nmap-ssh.client.student.client_network.57084 > nmap-ssh.tserver.student.server_network.http: Flags [.], ack 151, win 229, options [nop,nop,TS val 1561465993 ecr 1809040534], length 0
22:02:39.595896 IP nmap-ssh.tserver.student.server_network.http > nmap-ssh.client.student.client_network.57084: Flags [P.], seq 151:346, ack 148, win 235, options [nop,nop,TS val 1809040534 ecr 1561465993], l
th 195: HTTP
22:02:39.595911 IP nmap-ssh.client.student.client_network.57084 > nmap-ssh.tserver.student.server_network.http: Flags [.], ack 346, win 237, options [nop,nop,TS val 1561465993 ecr 1809040534], length 0
22:02:39.595983 IP nmap-ssh.tserver.student.server_network.http > nmap-ssh.client.student.client_network.57084: Flags [F.], seq 346, ack 148, win 235, options [nop,nop,TS val 1809040535 ecr 1561465993], lengt
22:02:39.596008 IP nmap-ssh.client.student.client_network.57084 > nmap-ssh.tserver.student.server_network.http: Flags [R], seq 3550080369, win 0, length 0
22:02:39.596031 IP nmap-ssh.client.student.client_network.57084 > nmap-ssh.tserver.student.server_network.http: Flags [R.], seq 148, ack 346, win 237, options [nop,nop,TS val 1561465993 ecr 1809040534], lengt
22:02:40.600770 IP nmap-ssh.client.student.client_network.35310 > nmap-ssh.pserver.student.server_network.http: Flags [S], seq 5358689, win 29200, options [mss 1460,sackOK,TS val 1084832699 ecr 0,nop,wscale 7
length 0
```

```
analyst@router: ~
File  Edit  View  Search  Terminal  Help
, length 0
22:02:42.614842 IP nmap-ssh.pserver.student.server_network.http > nmap-ssh.client.student.client_network.35314: Flags [R.], seq 0, ack 965605446, win 0, length 0
22:02:43.281529 IP nmap-ssh.client.student.client_network.37270 > nmap-ssh.tserver.student.server_network.telnet: Flags [S], seq 3158708188, win 29200, options [mss 1460,sackOK,TS val 1561469679 ecr 0,nop,wscale
 7], length 0
22:02:43.281582 IP nmap-ssh.tserver.student.server_network.telnet > nmap-ssh.client.student.client_network.37270: Flags [S.], seq 759731307, ack 3158708189, win 28960, options [mss 1460,sackOK,TS val 1809044220
ecr 1561469679,nop,wscale 7], length 0
22:02:43.281604 IP nmap-ssh.client.student.client_network.37270 > nmap-ssh.tserver.student.server_network.telnet: Flags [.], ack 1, win 229, options [nop,nop,TS val 1561469679 ecr 1809044220], length 0
22:02:43.281854 IP nmap-ssh.client.student.client_network.37270 > nmap-ssh.tserver.student.server_network.telnet: Flags [P.], seq 1:25, ack 1, win 229, options [nop,nop,TS val 1561469679 ecr 1809044220], length
24 [telnet DO SUPPRESS GO AHEAD, WILL TERMINAL TYPE, WILL NAWS, WILL TSPEED, WILL LFLOW, WILL LINEMODE, WILL NEW-ENVIRON, DO STATUS [|telnet]
22:02:43.281887 IP nmap-ssh.tserver.student.server_network.telnet > nmap-ssh.client.student.client_network.37270: Flags [.], ack 25, win 227, options [nop,nop,TS val 1809044221 ecr 1561469679], length 0
22:02:43.284798 IP nmap-ssh.tserver.student.server_network.telnet > nmap-ssh.client.student.client_network.37270: Flags [P.], seq 1:13, ack 25, win 227, options [nop,nop,TS val 1809044223 ecr 1561469679], length
 12 [telnet DO TERMINAL TYPE, DO TSPEED, DO XDISPLOC, DO NEW-ENVIRON [|telnet]
22:02:43.284822 IP nmap-ssh.client.student.client_network.37270 > nmap-ssh.tserver.student.server_network.telnet: Flags [.], ack 13, win 229, options [nop,nop,TS val 1561469682 ecr 1809044223], length 0
22:02:43.284860 IP nmap-ssh.client.student.client_network.37270 > nmap-ssh.tserver.student.server_network.telnet: Flags [P.], seq 25:28, ack 13, win 229, options [nop,nop,TS val 1561469682 ecr 1809044223], lengt
h 3 [telnet WONT XDISPLOC [|telnet]
22:02:43.284867 IP nmap-ssh.tserver.student.server_network.telnet > nmap-ssh.client.student.client_network.37270: Flags [P.], seq 13:28, ack 25, win 227, options [nop,nop,TS val 1809044223 ecr 1561469682], lengt
h 15 [telnet WILL SUPPRESS GO AHEAD, DO NAWS, DO LFLOW, DONT LINEMODE, WILL STATUS [|telnet]
22:02:43.325267 IP nmap-ssh.client.student.client_network.37270 > nmap-ssh.tserver.student.server_network.telnet: Flags [.], ack 28, win 229, options [nop,nop,TS val 1561469723 ecr 1809044223], length 0
22:02:43.325285 IP nmap-ssh.tserver.student.server_network.telnet > nmap-ssh.client.student.client_network.37270: Flags [.], ack 28, win 227, options [nop,nop,TS val 1809044264 ecr 1561469682], length 0
22:02:43.325313 IP nmap-ssh.tserver.student.server_network.telnet > nmap-ssh.client.student.client_network.37270: Flags [P.], seq 28:46, ack 28, win 227, options [nop,nop,TS val 1809044264 ecr 1561469723], lengt
h 18 [telnet SB TSPEED SEND SE, SB NEW-ENVIRON SEND SE, SB TERMINAL TYPE SEND SE [|telnet]
22:02:43.325328 IP nmap-ssh.client.student.client_network.37270 > nmap-ssh.tserver.student.server_network.telnet: Flags [.], ack 46, win 229, options [nop,nop,TS val 1561469723 ecr 1809044264], length 0
22:02:43.325520 IP nmap-ssh.client.student.client_network.37270 > nmap-ssh.tserver.student.server_network.telnet: Flags [P.], seq 28:56, ack 46, win 229, options [nop,nop,TS val 1561469723 ecr 1809044264], lengt
h 28 [telnet SB TSPEED IS 0x30 0x2c 0x30 SE, SB NEW-ENVIRON IS SE, SB TERMINAL TYPE IS 0x55 0x4e 0x4b 0x4e 0x4f 0x57 0x4e SE [|telnet]
22:02:43.325549 IP nmap-ssh.tserver.student.server_network.telnet > nmap-ssh.client.student.client_network.37270: Flags [.], ack 56, win 227, options [nop,nop,TS val 1809044264 ecr 1561469723], length 0
22:02:43.325859 IP nmap-ssh.tserver.student.server_network.telnet > nmap-ssh.client.student.client_network.37270: Flags [P.], seq 46:49, ack 56, win 227, options [nop,nop,TS val 1809044264 ecr 1561469723], lengt
h 3 [telnet DO ECHO [|telnet]
22:02:43.325913 IP nmap-ssh.client.student.client_network.37270 > nmap-ssh.tserver.student.server_network.telnet: Flags [P.], seq 56:59, ack 49, win 229, options [nop,nop,TS val 1561469724 ecr 1809044264], lengt
h 3 [telnet WONT ECHO [|telnet]
22:02:43.326070 IP nmap-ssh.tserver.student.server_network.telnet > nmap-ssh.client.student.client_network.37270: Flags [P.], seq 49:52, ack 59, win 227, options [nop,nop,TS val 1809044265 ecr 1561469724], lengt
h 3 [telnet WILL ECHO [|telnet]
22:02:43.326130 IP nmap-ssh.client.student.client_network.37270 > nmap-ssh.tserver.student.server_network.telnet: Flags [P.], seq 59:62, ack 52, win 229, options [nop,nop,TS val 1561469724 ecr 1809044265], lengt
h 3 [telnet DO ECHO [|telnet]
```

```
analyst@router:~$ sudo tcpdump -i eth1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
22:09:36.629314 IP nmap-ssh.tserver.student.server_network.telnet > nmap-ssh.client.student.client_network.38180: Flags [.], ack 1800839297, win 227, options [nop,nop,TS val 1809457577 ecr 1561882996], length 0
22:09:36.629345 IP nmap-ssh.client.student.client_network.38180 > nmap-ssh.tserver.student.server_network.telnet: Flags [.], ack 0, win 229, options [nop,nop,TS val 1561883036 ecr 1809457537], length 0
22:09:36.629392 IP nmap-ssh.tserver.student.server_network.telnet > nmap-ssh.client.student.client_network.38180: Flags [P.], seq 0:18, ack 1, win 227, options [nop,nop,TS val 1809457577 ecr 1561883036], length
18 [telnet SB TSPEED SEND SE, SB NEW-ENVIRON SEND SE, SB TERMINAL TYPE SEND SE [|telnet]
22:09:36.629422 IP nmap-ssh.client.student.client_network.38180 > nmap-ssh.tserver.student.server_network.telnet: Flags [.], ack 18, win 229, options [nop,nop,TS val 1561883036 ecr 1809457577], length 0
22:09:36.629543 IP nmap-ssh.client.student.client_network.38180 > nmap-ssh.tserver.student.server_network.telnet: Flags [P.], seq 1:29, ack 18, win 229, options [nop,nop,TS val 1561883036 ecr 1809457577], length
 28 [telnet SB TSPEED IS 0x30 0x2c 0x30 SE, SB NEW-ENVIRON IS SE, SB TERMINAL TYPE IS 0x55 0x4e 0x4b 0x4e 0x4f 0x57 0x4e SE [|telnet]
22:09:36.629586 IP nmap-ssh.tserver.student.server_network.telnet > nmap-ssh.client.student.client_network.38180: Flags [.], ack 29, win 227, options [nop,nop,TS val 1809457577 ecr 1561883036], length 0
22:09:36.629856 IP nmap-ssh.tserver.student.server_network.telnet > nmap-ssh.client.student.client_network.38180: Flags [P.], seq 18:21, ack 29, win 227, options [nop,nop,TS val 1809457577 ecr 1561883036], lengt
h 3 [telnet DO ECHO [|telnet]
22:09:36.630554 IP nmap-ssh.client.student.client_network.38180 > nmap-ssh.tserver.student.server_network.telnet: Flags [P.], seq 32:35, ack 24, win 229, options [nop,nop,TS val 1561883037 ecr 1809457578], lengt
h 3 [telnet DO ECHO [|telnet]
22:09:36.630601 IP nmap-ssh.tserver.student.server_network.telnet > nmap-ssh.client.student.client_network.38180: Flags [P.], seq 24:44, ack 35, win 227, options [nop,nop,TS val 1809457578 ecr 1561883037], lengt
h 20
22:09:36.673275 IP nmap-ssh.client.student.client_network.38180 > nmap-ssh.tserver.student.server_network.telnet: Flags [.], ack 44, win 229, options [nop,nop,TS val 1561883080 ecr 1809457578], length 0
22:09:36.673312 IP nmap-ssh.tserver.student.server_network.telnet > nmap-ssh.client.student.client_network.38180: Flags [P.], seq 44:59, ack 35, win 227, options [nop,nop,TS val 1809457621 ecr 1561883080], lengt
h 15
22:09:36.673341 IP nmap-ssh.client.student.client_network.38180 > nmap-ssh.tserver.student.server_network.telnet: Flags [.], ack 59, win 229, options [nop,nop,TS val 1561883080 ecr 1809457621], length 0
22:09:37.076634 IP nmap-ssh.client.student.client_network.36228 > nmap-ssh.pserver.student.server_network.http: Flags [S], seq 3523908415, win 29200, options [mss 1460,sackOK,TS val 1085249184 ecr 0,nop,wscale 7
], length 0
22:09:37.076674 IP nmap-ssh.pserver.student.server_network.http > nmap-ssh.client.student.client_network.36228: Flags [R.], seq 0, ack 3523908416, win 0, length 0
22:09:37.586966 IP nmap-ssh.client.student.client_network.38180 > nmap-ssh.tserver.student.server_network.telnet: Flags [P.], seq 35:42, ack 59, win 229, options [nop,nop,TS val 1561883993 ecr 1809457621], lengt
h 7
22:09:37.587115 IP nmap-ssh.tserver.student.server_network.telnet > nmap-ssh.client.student.client_network.38180: Flags [P.], seq 59:67, ack 42, win 227, options [nop,nop,TS val 1809458535 ecr 1561883993], lengt
h 8
22:09:37.587152 IP nmap-ssh.client.student.client_network.38180 > nmap-ssh.tserver.student.server_network.telnet: Flags [.], ack 67, win 229, options [nop,nop,TS val 1561883994 ecr 1809458535], length 0
22:09:37.587664 IP nmap-ssh.tserver.student.server_network.telnet > nmap-ssh.client.student.client_network.38180: Flags [P.], seq 67:77, ack 42, win 227, options [nop,nop,TS val 1809458535 ecr 1561883994], lengt
h 10
22:09:37.587690 IP nmap-ssh.client.student.client_network.38180 > nmap-ssh.tserver.student.server_network.telnet: Flags [.], ack 77, win 229, options [nop,nop,TS val 1561883994 ecr 1809458535], length 0
22:09:38.081748 IP nmap-ssh.client.student.client_network.58006 > nmap-ssh.tserver.student.server_network.http: Flags [S], seq 108430931, win 29200, options [mss 1460,sackOK,TS val 1561884488 ecr 0,nop,wscale 7]
, length 0
22:09:38.081788 IP nmap-ssh.tserver.student.server_network.http > nmap-ssh.client.student.client_network.58006: Flags [S.], seq 3335374234, ack 108430932, win 28960, options [mss 1460,sackOK,TS val 1809459029 ec
r 1561884488,nop,wscale 7], length 0
22:09:38.081817 IP nmap-ssh.client.student.client_network.58006 > nmap-ssh.tserver.student.server_network.http: Flags [.], ack 1, win 229, options [nop,nop,TS val 1561884488 ecr 1809459029], length 0
22:09:38.081894 IP nmap-ssh.client.student.client_network.58006 > nmap-ssh.tserver.student.server_network.http: Flags [P.], seq 1:148, ack 1, win 229, options [nop,nop,TS val 1561884488 ecr 1809459029], length 1
47: HTTP: GET /link1.html HTTP/1.1
22:09:38.081906 IP nmap-ssh.tserver.student.server_network.http > nmap-ssh.client.student.client_network.58006: Flags [.], ack 148, win 235, options [nop,nop,TS val 1809459029 ecr 1561884488], length 0
```

```
analyst@router: ~
File  Edit  View  Search  Terminal  Help
analyst@router:~$ sudo tshark -i eth0
Running as user "root" and group "root". This could be dangerous.
tshark: Lua: Error during loading:
 [string "/usr/share/wireshark/init.lua"]:44: dofile has been disabled due to running Wireshark as superuser. See https://wiki.wireshark.org/CaptureSetup/CapturePrivileges for help in
rivileged user.
Capturing on 'eth0'
  1 0.000000000   172.24.0.1 -> 172.25.0.2   TCP 74 36846 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1085528806 TSecr=0 WS=128
  2 0.000071912   172.25.0.2 -> 172.24.0.1   TCP 54 80 → 36846 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  3 1.005513474   172.24.0.1 -> 172.25.0.1   TCP 74 58624 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1562164111 TSecr=0 WS=128
  4 1.005571867   172.25.0.1 -> 172.24.0.1   TCP 74 80 → 58624 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=1809738652 TSecr=1562164111 WS=128
  5 1.005598329   172.24.0.1 -> 172.25.0.1   TCP 66 58624 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1562164111 TSecr=1809738652
  6 1.005652194   172.24.0.1 -> 172.25.0.1   HTTP 213 GET /link1.html HTTP/1.1
  7 1.005675935   172.25.0.1 -> 172.24.0.1   TCP 66 80 → 58624 [ACK] Seq=1 Ack=148 Win=30080 Len=0 TSval=1809738652 TSecr=1562164111
  8 1.006076668   172.25.0.1 -> 172.24.0.1   TCP 95 [TCP segment of a reassembled PDU]
  9 1.006099937   172.24.0.1 -> 172.25.0.1   TCP 66 58624 → 80 [ACK] Seq=148 Ack=30 Win=29312 Len=0 TSval=1562164111 TSecr=1809738652
 10 1.006139270   172.25.0.1 -> 172.24.0.1   TCP 104 [TCP segment of a reassembled PDU]
 11 1.006151874   172.24.0.1 -> 172.25.0.1   TCP 66 58624 → 80 [ACK] Seq=148 Ack=68 Win=29312 Len=0 TSval=1562164112 TSecr=1809738653
 12 1.006191989   172.25.0.1 -> 172.24.0.1   TCP 103 [TCP segment of a reassembled PDU]
 13 1.006217808   172.24.0.1 -> 172.25.0.1   TCP 66 58624 → 80 [ACK] Seq=148 Ack=105 Win=29312 Len=0 TSval=1562164112 TSecr=1809738653
 14 1.006244938   172.25.0.1 -> 172.24.0.1   TCP 85 [TCP segment of a reassembled PDU]
 15 1.006258539   172.24.0.1 -> 172.25.0.1   TCP 66 58624 → 80 [ACK] Seq=148 Ack=124 Win=29312 Len=0 TSval=1562164112 TSecr=1809738653
 16 1.006295664   172.25.0.1 -> 172.24.0.1   TCP 91 [TCP segment of a reassembled PDU]
 17 1.006309514   172.24.0.1 -> 172.25.0.1   TCP 66 58624 → 80 [ACK] Seq=148 Ack=149 Win=29312 Len=0 TSval=1562164112 TSecr=1809738653
 18 1.006343914   172.25.0.1 -> 172.24.0.1   HTTP 68 HTTP/1.0 404 File not found
 19 1.006356093   172.24.0.1 -> 172.25.0.1   TCP 66 58624 → 80 [ACK] Seq=148 Ack=151 Win=29312 Len=0 TSval=1562164112 TSecr=1809738653
 20 1.006379556   172.25.0.1 -> 172.24.0.1   TCP 261 80 → 58624 [PSH, ACK] Seq=151 Ack=148 Win=30080 Len=195 TSval=1809738653 TSecr=1562164112
 21 1.006389331   172.24.0.1 -> 172.25.0.1   TCP 66 58624 → 80 [ACK] Seq=148 Ack=346 Win=30336 Len=0 TSval=1562164112 TSecr=1809738653
 22 1.006433981   172.25.0.1 -> 172.24.0.1   TCP 66 80 → 58624 [FIN, ACK] Seq=346 Ack=148 Win=30080 Len=0 TSval=1809738653 TSecr=1562164112
 23 1.006448124   172.24.0.1 -> 172.25.0.1   TCP 66 58624 → 80 [RST, ACK] Seq=148 Ack=346 Win=30336 Len=0 TSval=1562164112 TSecr=1809738653
 24 1.006450461   172.24.0.1 -> 172.25.0.1   TCP 54 58624 → 80 [RST] Seq=148 Win=0 Len=0
 25 1.752828046   172.24.0.1 -> 172.25.0.1   TCP 74 38804 → 23 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1562164858 TSecr=0 WS=128
 26 1.752873198   172.25.0.1 -> 172.24.0.1   TCP 74 23 → 38804 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=1809739399 TSecr=1562164858 WS=128
 27 1.752894498   172.24.0.1 -> 172.25.0.1   TCP 66 38804 → 23 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1562164858 TSecr=1809739399
 28 1.753097482   172.24.0.1 -> 172.25.0.1   TELNET 90 Telnet Data ...
 29 1.753123754   172.25.0.1 -> 172.24.0.1   TCP 66 23 → 38804 [ACK] Seq=1 Ack=25 Win=29056 Len=0 TSval=1809739400 TSecr=1562164858
 30 1.755655331   172.25.0.1 -> 172.24.0.1   TELNET 78 Telnet Data ...
 31 1.755677392   172.24.0.1 -> 172.25.0.1   TCP 66 38804 → 23 [ACK] Seq=25 Ack=13 Win=29312 Len=0 TSval=1562164861 TSecr=1809739402
 32 1.755705782   172.24.0.1 -> 172.25.0.1   TELNET 69 Telnet Data ...
 33 1.755709722   172.25.0.1 -> 172.24.0.1   TELNET 81 Telnet Data ...
 34 1.796469157   172.24.0.1 -> 172.25.0.1   TCP 66 38804 → 23 [ACK] Seq=28 Ack=28 Win=29312 Len=0 TSval=1562164902 TSecr=1809739402
 35 1.796492196   172.25.0.1 -> 172.24.0.1   TCP 66 23 → 38804 [ACK] Seq=28 Ack=28 Win=29056 Len=0 TSval=1809739443 TSecr=1562164861
 36 1.796521581   172.25.0.1 -> 172.24.0.1   TELNET 84 Telnet Data ...
 37 1.796535411   172.24.0.1 -> 172.25.0.1   TCP 66 38804 → 23 [ACK] Seq=28 Ack=46 Win=29312 Len=0 TSval=1562164902 TSecr=1809739443
 38 1.796599256   172.24.0.1 -> 172.25.0.1   TELNET 94 Telnet Data ...
 39 1.796621042   172.25.0.1 -> 172.24.0.1   TCP 66 23 → 38804 [ACK] Seq=46 Ack=56 Win=29056 Len=0 TSval=1809739443 TSecr=1562164902
 40 1.796860152   172.25.0.1 -> 172.24.0.1   TELNET 69 Telnet Data ...
```

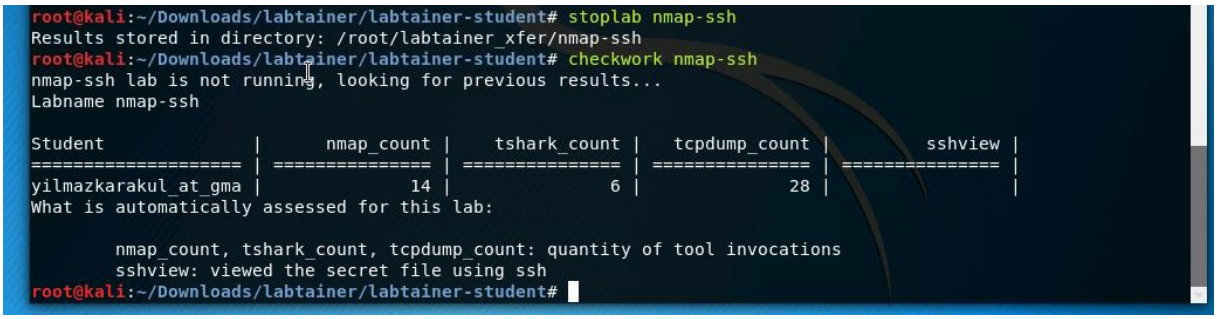


Stop the labtainer

This lab was developed for the Labtainer framework by the Naval Postgraduate School, Center for Cybersecurity and Cyber Operations under National Science Foundation Award No. 1438893. This work is in the public domain, and cannot be copyrighted.

When the lab is completed, or you'd like to stop working for a while, run:

```
Stoplab
```



from the host labtainer working directory. You can always restart the labtainer to continue your work. When the labtainer is stopped, a zip file is created and copied to a location displayed by the stoplab command. When the lab is completed send that zip file to the instructor.