CLab 9: Secure Networked Applications

Joshua Ludolf
CSCI 4406 – Computer Networks

- To start this lab, I had to configure my fabric by running utilizing the blogs GitHub repo (git checkout, additionally had to modify cell 14):

```
import pandas as pd
pd.set_option('display.max_colwidth', None)

# Assuming fablib is an instance of FablibManager
ssh_str = 'ssh -i ' + slice.get_slice_private_key_file() + \
    ' -J ' + fablib.get_bastion_username() + '@' + fablib.get_bastion_host() + \
    ' -F /home/fabric/work/fabric_config/ssh_config '

slice_info = [{'Name': n.get_name(), 'SSH command': ssh_str + n.get_username() + '@' + str(n.get_management_ip())} for n in slice.get_nodes()]
pd.DataFrame(slice_info).set_index('Name')
```

```
Retry: 11, Time: 272 sec
```

Slice

ID	8d6c8390-a291-4545-b1ce-ccea9955ae19
Name	Joshua Ludolf Secure-Applications_jludo01
Lease Expiration (UTC)	2024-11-07 15:39:47 +0000
Lease Start (UTC)	2024-11-06 15:39:47 +0000
Project ID	a70de2f5-9e12-4b6b-b412-0ae1a2c553b0
State	StableOK

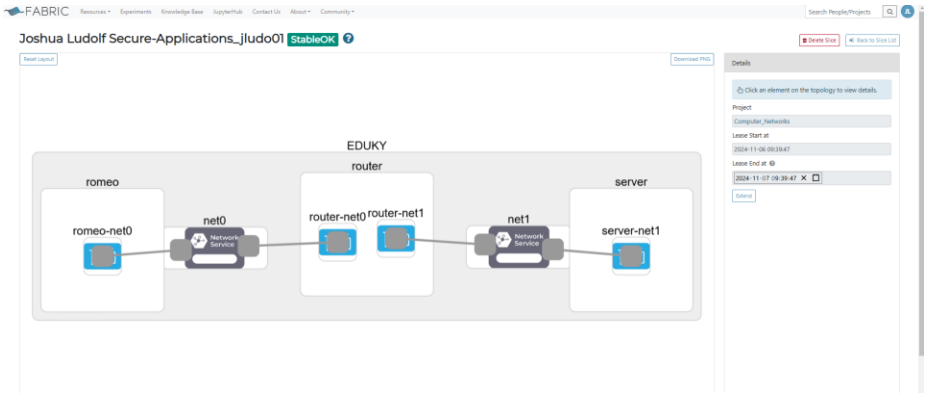
Networks

ID	Name	Layer	Type	Site	Subnet	Gateway	State	Error
669d50c7-3808-409f-a7ad-c3a89547f860	net0	L2	L2Bridge	EDUKY	None	None	Active	
3d8a0a55-64a0-42e5-8c43-b2bee86d5371	net1	L2	L2Bridge	EDUKY	None	None	Active	

Interfaces

Name	Short Name	Node	Network	Bandwidth	Mode	VLAN	MAC	Physical Device	Device	IP Address	Numa Node	Switch Port
romeo-net0-p1	p1	romeo	net0	100	config		1E:A5:A4:33:B4:B1	enp7s0	enp7s0	fe80::1ca5:a4ff:fe33:b4b1	1	HundredGigE0/0/0/34
router-net0-p1	p1	router	net0	100	config		1A:B3:86:14:30:B0	enp8s0	enp8s0	fe80::18b3:86ff:fe14:30b0	1	HundredGigE0/0/0/29
router-net1-p1	p1	router	net1	100	config		1A:78:5D:39:3D:D6	enp7s0	enp7s0	fe80::1878:5dff:fe39:3dd6	1	HundredGigE0/0/0/29
server-net1-p1	p1	server	net1	100	config		1A:79:0A:04:A3:DA	enp7s0	enp7s0	fe80::1879:aff:fe04:a3da	1	HundredGigE0/0/0/21

```
Time to print interfaces 288 seconds
'8d6c8390-a291-4545-b1ce-ccea9955ae19'
```



Name	SSH command
romeo	ssh -i /home/fabric/work/fabric_config/slice_key -J jludo01_0000228382@bastion.fabric-testbed.net -F /home/fabric/work/fabric_config/ssh_config ubuntu@2610:1e0:1700:206:f816:3eff:fee8:f504
router	ssh -i /home/fabric/work/fabric_config/slice_key -J jludo01_0000228382@bastion.fabric-testbed.net -F /home/fabric/work/fabric_config/ssh_config ubuntu@2610:1e0:1700:206:f816:3eff:fe6c:6c20
server	ssh -i /home/fabric/work/fabric_config/slice_key -J jludo01_0000228382@bastion.fabric-testbed.net -F /home/fabric/work/fabric_config/ssh_config ubuntu@2610:1e0:1700:206:f816:3eff:fe1a:2dc5

- From there, I followed the instructions from https://witestlab.poly.edu/blog/secure-networked-applications/ , starting from Remote login section:
  - First, I needed to install and configure these services on the "server" node. Before that I needed to ssh into “server” node (no issues at all 😍).

```
fabric@spring:secure_applications-167$ ssh -i /home/fabric/work/fabric_config/slice_key -J jludo01_0000228382@bastion.fabric-testbed.net -F /home/fabric/work/fabric_config/ssh_config ubuntu@2610:1e0:1700:206:f816:3eff:fe1a:2dc5
Warning: Permanently added 'bastion.fabric-testbed.net' (ED25519) to the list of known hosts.
Warning: Permanently added '2610:1e0:1700:206:f816:3eff:fe1a:2dc5' (ED25519) to the list of known hosts.
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-186-generic x86_64)

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

 System information as of Wed Nov  6 16:05:53 UTC 2024

  System load:           0.0
  Usage of /:            14.9% of 9.51GB
  Memory usage:          5%
  Swap usage:            0%
  Processes:             165
  Users logged in:       0
  IPv4 address for enp3s0: 10.30.8.189
  IPv6 address for enp3s0: 2610:1e0:1700:206:f816:3eff:fe1a:2dc5


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
New release '22.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Wed Nov  6 15:41:39 2024 from 2610:1e0:1700:205::51
ubuntu@server:~$
ubuntu@server:~$ sudo apt update
Get:1 http://security.ubuntu.com/ubuntu focal-security InRelease [128 kB]
Get:2 http://nova.clouds.archive.ubuntu.com/ubuntu focal InRelease [265 kB]
Get:3 http://security.ubuntu.com/ubuntu focal-security/main amd64 Packages [3284 kB]
Get:4 http://security.ubuntu.com/ubuntu focal-security/main Translation-en [482 kB]
Get:5 http://security.ubuntu.com/ubuntu focal-security/main amd64 c-n-f Metadata [14.3 kB]
Get:6 http://security.ubuntu.com/ubuntu focal-security/restricted amd64 Packages [3222 kB]
Get:7 http://security.ubuntu.com/ubuntu focal-security/restricted Translation-en [451 kB]
Get:8 http://security.ubuntu.com/ubuntu focal-security/restricted amd64 c-n-f Metadata [548 B]
Get:9 http://security.ubuntu.com/ubuntu focal-security/universe amd64 Packages [1014 kB]
Get:10 http://security.ubuntu.com/ubuntu focal-security/universe Translation-en [214 kB]
Get:11 http://security.ubuntu.com/ubuntu focal-security/universe amd64 c-n-f Metadata [21.4 kB]
Get:12 http://security.ubuntu.com/ubuntu focal-security/multiverse amd64 Packages [24.8 kB]
Get:13 http://security.ubuntu.com/ubuntu focal-security/multiverse Translation-en [5968 B]
Get:14 http://security.ubuntu.com/ubuntu focal-security/multiverse amd64 c-n-f Metadata [540 B]
Get:15 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates InRelease [128 kB]
Get:16 http://nova.clouds.archive.ubuntu.com/ubuntu focal-backports InRelease [128 kB]
Get:17 http://nova.clouds.archive.ubuntu.com/ubuntu focal/universe amd64 Packages [8628 kB]
Get:18 http://nova.clouds.archive.ubuntu.com/ubuntu focal/universe Translation-en [5124 kB]
Get:19 http://nova.clouds.archive.ubuntu.com/ubuntu focal/universe amd64 c-n-f Metadata [265 kB]
Get:20 http://nova.clouds.archive.ubuntu.com/ubuntu focal/multiverse amd64 Packages [144 kB]
Get:21 http://nova.clouds.archive.ubuntu.com/ubuntu focal/multiverse Translation-en [104 kB]
Get:22 http://nova.clouds.archive.ubuntu.com/ubuntu focal/multiverse amd64 c-n-f Metadata [9136 B]
Get:23 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/main amd64 Packages [3658 kB]
Get:24 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/main Translation-en [560 kB]
Get:25 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/main amd64 c-n-f Metadata [17.8 kB]
Get:26 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/restricted amd64 Packages [3346 kB]
Get:27 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/restricted Translation-en [468 kB]
Get:28 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/restricted amd64 c-n-f Metadata [548 B]
Get:29 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/universe amd64 Packages [1237 kB]
Get:30 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/universe Translation-en [297 kB]
Get:31 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/universe amd64 c-n-f Metadata [28.3 kB]
Get:32 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/multiverse amd64 Packages [27.0 kB]
Get:33 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/multiverse Translation-en [7936 B]
Get:34 http://nova.clouds.archive.ubuntu.com/ubuntu focal-updates/multiverse amd64 c-n-f Metadata [612 B]
Get:35 http://nova.clouds.archive.ubuntu.com/ubuntu focal-backports/main amd64 Packages [45.7 kB]
Get:36 http://nova.clouds.archive.ubuntu.com/ubuntu focal-backports/main Translation-en [16.3 kB]
Get:37 http://nova.clouds.archive.ubuntu.com/ubuntu focal-backports/main amd64 c-n-f Metadata [1420 B]
Get:38 http://nova.clouds.archive.ubuntu.com/ubuntu focal-backports/restricted amd64 c-n-f Metadata [116 B]
Get:39 http://nova.clouds.archive.ubuntu.com/ubuntu focal-backports/universe amd64 Packages [25.0 kB]
Get:40 http://nova.clouds.archive.ubuntu.com/ubuntu focal-backports/universe Translation-en [16.3 kB]
Get:41 http://nova.clouds.archive.ubuntu.com/ubuntu focal-backports/universe amd64 c-n-f Metadata [880 B]
Get:42 http://nova.clouds.archive.ubuntu.com/ubuntu focal-backports/multiverse amd64 c-n-f Metadata [116 B]
Fetched 33.4 MB in 4s (8123 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
73 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

- Next, I installed telnet service on “server” node (yay, no issues with installation is always a wonderful sign 😍):

```
ubuntu@server:~$ sudo apt -y install xinetd telnetd
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  update-inetd
The following NEW packages will be installed:
  telnetd update-inetd xinetd
0 upgraded, 3 newly installed, 0 to remove and 73 not upgraded.
Need to get 171 kB of archives.
After this operation, 508 kB of additional disk space will be used.
Get:1 http://nova.clouds.archive.ubuntu.com/ubuntu focal/universe amd64 xinetd amd64 1:2.3.15.3-1 [108 kB]
Get:2 http://nova.clouds.archive.ubuntu.com/ubuntu focal/universe amd64 telnetd amd64 0.17-41.2build1 [38.8 kB]
Get:3 http://nova.clouds.archive.ubuntu.com/ubuntu focal/main amd64 update-inetd all 4.50 [24.8 kB]
Fetched 171 kB in 1s (222 kB/s)
Preconfiguring packages ...
Selecting previously unselected package xinetd.
(Reading database ... 64102 files and directories currently installed.)
Preparing to unpack .../xinetd_1%3a2.3.15.3-1_amd64.deb ...
Unpacking xinetd (1:2.3.15.3-1) ...
Selecting previously unselected package telnetd.
Preparing to unpack .../telnetd_0.17-41.2build1_amd64.deb ...
Unpacking telnetd (0.17-41.2build1) ...
Selecting previously unselected package update-inetd.
Preparing to unpack .../update-inetd_4.50_all.deb ...
Unpacking update-inetd (4.50) ...
Setting up xinetd (1:2.3.15.3-1) ...
Setting up update-inetd (4.50) ...
Setting up telnetd (0.17-41.2build1) ...
Adding user telnetd to group utmp
Note: xinetd currently is not fully supported by update-inetd.
Please consult /usr/share/doc/xinetd/README.Debian and itox(8).
update-inetd: warning: cannot add service, /etc/inetd.conf does not exist
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for systemd (245.4-4ubuntu3.23) ...
```

- Next, I created the telnet configuration file, so I will be able to utilize the telnet service and inserted configuration rules for it (no issues, it’s simple nano text editor command and then copy paste as instructions state):

```
ubuntu@server:~$ sudo nano /etc/xinetd.d/telnet
```

setup.ipynb | ubuntu@server: ~

```
  GNU nano 4.8
# default: on
# description: telnet server
service telnet
{
disable = no
flags = REUSE
socket_type = stream
wait = no
user = root
only_from = 10.0.0.0/8
server = /usr/sbin/in.telnetd
log_on_failure += USERID
}
```

- Then I restarted the telnet service on “server” node for the configuration file to take effect, using following command - sudo service xinetd restart, additionally I checked the status of the telnet service (it was “active (running)” state so it’s operating as intended ☺):

```
ubuntu@server:~$ sudo service xinetd restart
ubuntu@server:~$
```

```
ubuntu@server:~$ service xinetd status
● xinetd.service - LSB: Starts or stops the xinetd daemon.
     Loaded: loaded (/etc/init.d/xinetd; generated)
     Active: active (running) since Wed 2024-11-06 16:24:02 UTC; 2min 12s ago
       Docs: man:systemd-sysv-generator(8)
    Process: 15084 ExecStart=/etc/init.d/xinetd start (code=exited, status=0/SUCCESS)
      Tasks: 1 (limit: 4663)
     Memory: 836.0K
     CGroup: /system.slice/xinetd.service
             └─15116 /usr/sbin/xinetd -pidfile /run/xinetd.pid -stayalive -inetd_compat -inetd_ipv6

Nov 06 16:24:02 server xinetd[15116]: Reading included configuration file: /etc/xinetd.d/discard-udp [file=/etc/xinetd.d/discard-udp] [line=25]
Nov 06 16:24:02 server xinetd[15116]: Reading included configuration file: /etc/xinetd.d/echo [file=/etc/xinetd.d/echo] [line=14]
Nov 06 16:24:02 server xinetd[15116]: Reading included configuration file: /etc/xinetd.d/echo-udp [file=/etc/xinetd.d/echo-udp] [line=26]
Nov 06 16:24:02 server xinetd[15116]: Reading included configuration file: /etc/xinetd.d/servers [file=/etc/xinetd.d/servers] [line=14]
Nov 06 16:24:02 server xinetd[15116]: Reading included configuration file: /etc/xinetd.d/services [file=/etc/xinetd.d/services] [line=13]
Nov 06 16:24:02 server xinetd[15116]: Reading included configuration file: /etc/xinetd.d/telnet [file=/etc/xinetd.d/telnet] [line=13]
Nov 06 16:24:02 server xinetd[15116]: Reading included configuration file: /etc/xinetd.d/time [file=/etc/xinetd.d/time] [line=13]
Nov 06 16:24:02 server xinetd[15116]: Reading included configuration file: /etc/xinetd.d/time-udp [file=/etc/xinetd.d/time-udp] [line=28]
Nov 06 16:24:02 server xinetd[15116]: 2.3.15.3 started with libwrap loadavg labeled-networking options compiled in.
Nov 06 16:24:02 server xinetd[15116]: Started working: 1 available service
```

- Next, I started an SSH server process on the "server" host. Hosts on the testbed already have SSH servers on them, but these are configured to allow remote

access to testbed users and administrators. The second ssh on “server” node I, paralleled SSH server process on "server", that will run on port 1000 on the experiment interface, by running following command - sudo /usr/sbin/sshd -o ListenAddress=10.10.2.100 -f /usr/share/openssh/sshd_config -p 1000:

- From there, I added a user account for remote access to the “server” host, named “shakespeare”, and added password to be my user ID (I believe that would be the Fabric Id that is located in User Profile 😍):

```
ubuntu@server:~$ sudo useradd -m shakespeare -s /bin/sh
ubuntu@server:~$
```

FABRIC ID	FABRIC1001778

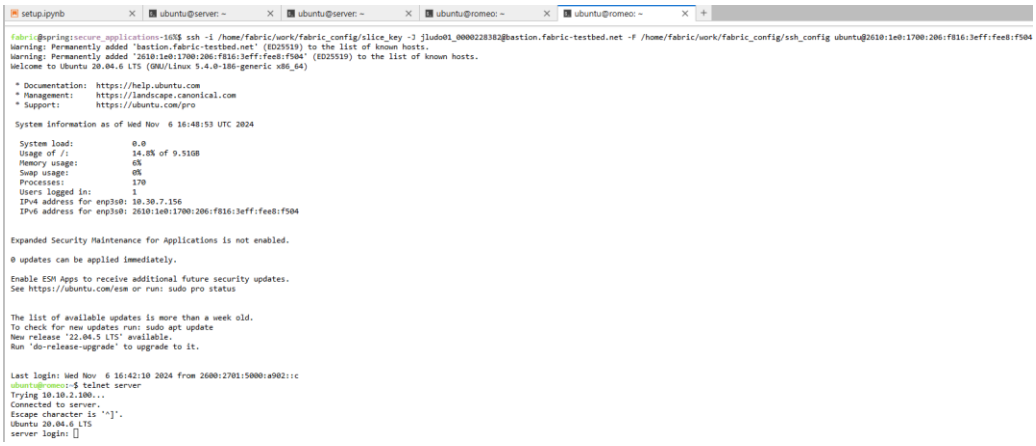
```
ubuntu@server:~$ sudo passwd shakespeare
New password:
Retype new password:
passwd: password updated successfully
```

- Now I am ready to compare the two remote access applications, with respect to security. On the "romeo" host, I ran - sudo tcpdump -i $(ip route get 10.10.2.100 | grep -oP "(?<=dev)[^]+") -w security-telnet-$(hostname -s).pcap :

```
ubuntu@romeo:~$ sudo tcpdump -i $(ip route get 10.10.2.100 | grep -oP "(?<=dev )[^ ]+") -w security-telnet-$(hostname -s).pcap
tcpdump: listening on enp7s0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

- From there I initiated a telnet connection from “romeo” node to “server” node by running the following command - telnet server (additionally requires another

instance of “romeo” node 😊):



- For the server login is the name I gave it earlier – “shakespeare” and password is my Fabric ID – FABRIC10001778 (no issues 😊) :

```
server login: shakespeare
Password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-186-generic x86_64)

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

 System information as of Wed Nov  6 16:50:43 UTC 2024

  System load:             0.0
  Usage of /:              16.7% of 9.51GB
  Memory usage:            6%
  Swap usage:              0%
  Processes:               153
  Users logged in:         1
  IPv4 address for enp3s0: 10.30.8.189
  IPv6 address for enp3s0: 2610:1e0:1700:206:f816:3eff:fe1a:2dc5


Expanded Security Maintenance for Applications is not enabled.

79 updates can be applied immediately.
52 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

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

New release '22.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.



The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

$
```

- After successfully logging in using telnet, I ran date command and stopped the tcdump from the “romeo” node:

```
$ date
Wed Nov  6 16:53:32 UTC 2024


^C186 packets captured
186 packets received by filter
0 packets dropped by kernel
ubuntu@romeo:~$
```

- Next, on the “romeo” node, I ran a different tcpdump command that would capture traffic on the network segment. This packet capture will show you what is visible to anyone eavesdropping on the network segment. Right after that I initiate an SSH connection from "romeo" to "server" on port 1000 - on "romeo" (this was painful as apparently my public key wasn’t setup right though, even though I had no issues with the keys until now, I basically had to generate new key pair and manually add it to the node then to the server (way too many steps to show), but eventually got it to work 😳…):

```
ubuntu@romeo:~$ sudo tcpdump -i $(ip route get 10.10.2.100 | grep -oP "(?<=dev )[^ ]+") -w security-ssh-$(hostname -s).pcap
tcpdump: listening on enp7s0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

```
ubuntu@romeo:~$ ssh -i ~/.ssh/id_rsa shakespeare@server -p 1000
Enter passphrase for key '/home/ubuntu/.ssh/id_rsa':
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-186-generic x86_64)

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

 System information as of Wed Nov  6 17:39:17 UTC 2024

  System load:             0.0
  Usage of /:              16.8% of 9.51GB
  Memory usage:            6%
  Swap usage:              0%
  Processes:               160
  Users logged in:         2
  IPv4 address for enp3s0: 10.30.8.189
  IPv6 address for enp3s0: 2610:1e0:1700:206:f816:3eff:fe1a:2dc5


Expanded Security Maintenance for Applications is not enabled.

79 updates can be applied immediately.
52 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

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

New release '22.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Wed Nov  6 17:29:21 2024 from romeo
$
```

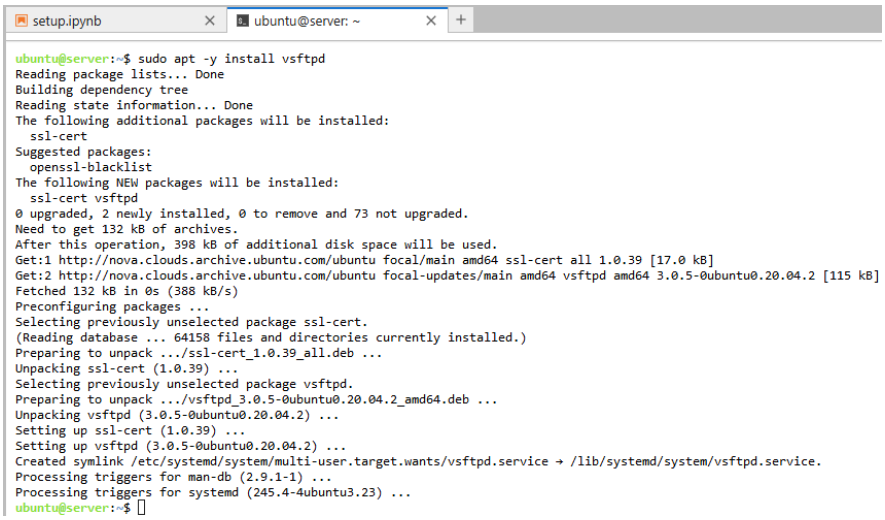
- After successfully logging in using SSH, I ran the date command again and stopped the tcdump in the “romeo” node instance:

```
$ date
Wed Nov  6 17:44:48 UTC 2024
```

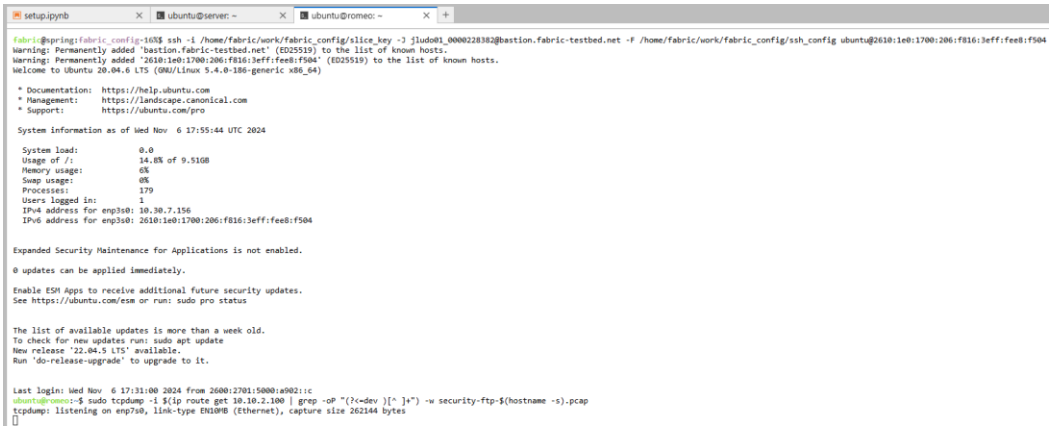
```
ubuntu@romeo:~$ sudo tcpdump -i $(ip route get 10.10.2.100 | grep -oP "(?<=dev )[^ ]+") -w security-ssh-$(hostname -s).pcap
tcpdump: listening on enp7s0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C120 packets captured
120 packets received by filter
0 packets dropped by kernel
```

- Now, after all that, I made it to File Transfer section to learn about how to compare File Transfer Protocol and Secure File Transfer Protocol usage to and from remote host 😍:

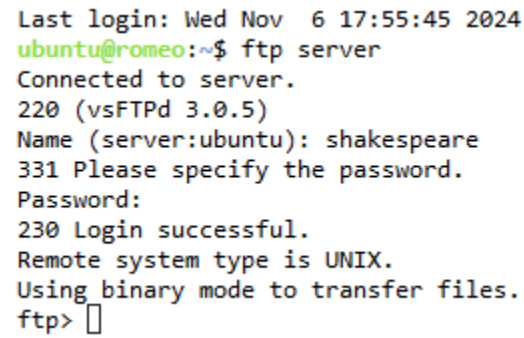
- First, I needed to install the SFTP server on the "server" node (I also cleared my workspace for organization purposes 😊):



- Next, I am going to use “shakespeare” on “server” node, before that I ran - sudo tcpdump -i $(ip route get 10.10.2.100 | grep -oP "(?<=dev)[^]+") -w security-ftp-$(hostname -s).pcap - on “romeo” node:



- On Romeo node I ran – ftp server – command to initiate FTP session from “romeo” node to “server” node (another instance of “romeo” required):



- Next, I ran following command – cd /etc – and got password, as this will transfer a list of all usernames on the remote system over the FTP session:

```
ftp> cd /etc
250 Directory successfully changed.
ftp> get passwd
local: passwd remote: passwd
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for passwd (1993 bytes).
226 Transfer complete.
1993 bytes received in 0.00 secs (57.5961 MB/s)
ftp>
```

- After that, I stopped the tcpdump in "romeo" node instance:

```
ubuntu@romeo:~$ sudo tcpdump -i $(ip route get 10.10.2.100 | grep -oP "(?<=dev )[^ ]+") -w security-ftp-$(hostname -s).pcap
tcpdump: listening on enp7s0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C57 packets captured
57 packets received by filter
0 packets dropped by kernel
```

- This is the contents of passwd file I transferred:

```
ubuntu@romeo:~$ cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
landscape:x:110:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:111:1::/var/cache/pollinate:/bin/false
fwupd-refresh:x:112:116:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
telnetd:x:113:120::/nonexistent:/usr/sbin/nologin
shakespeare:x:1001:1001::/home/shakespeare:/bin/sh
ftp:x:114:122:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
ubuntu@romeo:~$
```

- Then I did sftp connection instead of ftp, additionally started a new tcpdump:

```
ubuntu@romeo:~$ sudo tcpdump -i $(ip route get 10.10.2.100 | grep -oP "(?<=dev )[^ ]+") -w security-sftp-$(hostname -s).pcap
tcpdump: listening on enp7s0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

```
ubuntu@romeo:~$ sftp -P 1000 shakespeare@server
Enter passphrase for key '/home/ubuntu/.ssh/id_rsa':
Connected to server.
sftp>
```

```
sftp> cd /etc
sftp>
sftp> get passwd
Fetching /etc/passwd to passwd
/etc/passwd
sftp> exit
ubuntu@romeo:~$
```

```
ubuntu@romeo:~$ sudo tcpdump -i $(ip route get 10.10.2.100 | grep -oP "(?<=dev )[^ ]+") -w security-sftp-$(hostname -s).pcap
tcpdump: listening on enp7s0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C91 packets captured
91 packets received by filter
0 packets dropped by kernel
```

- Additionally ran same cat command, to see the improve tranfer of using secure file tranfer protocol (sftp) instead of normal file transfer protocol (ftp):

```
ubuntu@romeo:~$ cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
landscape:x:110:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:111:1::/var/cache/pollinate:/bin/false
fwupd-refresh:x:112:116:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
telnetd:x:113:120::/nonexistent:/usr/sbin/nologin
shakespeare:x:1001:1001::/home/shakespeare:/bin/sh
ftp:x:114:122:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
ubuntu@romeo:~$
```

- Summary of what I learned from this lab:

From this lab, I gained a solid understanding of how to securely access and manage remote servers using SSH (Secure Shell) and public key authentication. Initially, I learned the significance of SSH in providing secure communication

channels between my local machine and a remote server. By generating a new SSH key pair with `ssh-keygen`, I explored the process of creating both public and private keys and how they contribute to secure authentication.

Throughout the lab, I encountered various challenges, such as permission issues and key misconfigurations. These hurdles taught me the importance of correctly setting file permissions for `.ssh` directories and key files to ensure security and functionality. I also learned how to transfer my public key to a remote server using tools like `ssh-copy-id` and manual methods when automated solutions failed.

Using the `-v` (verbose) option in SSH commands provided me with detailed insights into the connection process, enabling me to diagnose and resolve issues effectively. This experience highlighted the necessity of understanding server-side configurations, such as the SSH daemon settings, to allow public key authentication and secure access.

Overall, this lab equipped me with essential skills for securely managing remote servers, reinforcing the value of secure practices in systems administration and cloud computing. The hands-on experience and troubleshooting efforts deepened my appreciation for the intricacies of secure remote access, preparing me for practical applications in IT and cybersecurity.