

Traffic Tracing and Sniffing

1. Open two terminals on External Kali VM. Use one to ping Ubuntu VM, and use the other to ping Internal Kali

```
Attacker Kali - External Workstation on CY301-IHENR002 - Virtual Machine Connection
File Action Media View Help

root@kali: ~
File Actions Edit View Help
64 bytes from 192.168.10.18: icmp_seq=51 ttl=63 time=684 ms
64 bytes from 192.168.10.18: icmp_seq=52 ttl=63 time=274 ms
64 bytes from 192.168.10.18: icmp_seq=53 ttl=63 time=269 ms
64 bytes from 192.168.10.18: icmp_seq=54 ttl=63 time=2.63 ms
64 bytes from 192.168.10.18: icmp_seq=55 ttl=63 time=11.8 ms
64 bytes from 192.168.10.18: icmp_seq=56 ttl=63 time=4.26 ms
64 bytes from 192.168.10.18: icmp_seq=57 ttl=63 time=7.01 ms
64 bytes from 192.168.10.18: icmp_seq=58 ttl=63 time=5.82 ms
64 bytes from 192.168.10.18: icmp_seq=59 ttl=63 time=5.36 ms
64 bytes from 192.168.10.18: icmp_seq=60 ttl=63 time=10.3 ms
64 bytes from 192.168.10.18: icmp_seq=61 ttl=63 time=3.48 ms
64 bytes from 192.168.10.18: icmp_seq=62 ttl=63 time=2.86 ms
64 bytes from 192.168.10.18: icmp_seq=63 ttl=63 time=2.89 ms
64 bytes from 192.168.10.18: icmp_seq=64 ttl=63 time=3.57 ms
64 bytes from 192.168.10.18: icmp_seq=65 ttl=63 time=2.92 ms
64 bytes from 192.168.10.18: icmp_seq=66 ttl=63 time=6.36 ms
64 bytes from 192.168.10.18: icmp_seq=67 ttl=63 time=4.55 ms
64 bytes from 192.168.10.18: icmp_seq=68 ttl=63 time=2.74 ms
64 bytes from 192.168.10.18: icmp_seq=69 ttl=63 time=3.70 ms
64 bytes from 192.168.10.18: icmp_seq=70 ttl=63 time=8.68 ms
^C
--- 192.168.10.18 ping statistics ---
70 packets transmitted, 70 received, 0% packet loss, time 69146ms
rtt min/avg/max/mdev = 2.251/23.744/684.197/91.043 ms

root@kali: ~
File Actions Edit View Help
64 bytes from 192.168.10.13: icmp_seq=12 ttl=63 time=4.25 ms
64 bytes from 192.168.10.13: icmp_seq=13 ttl=63 time=4.13 ms
64 bytes from 192.168.10.13: icmp_seq=14 ttl=63 time=3.11 ms
64 bytes from 192.168.10.13: icmp_seq=15 ttl=63 time=2.63 ms
64 bytes from 192.168.10.13: icmp_seq=16 ttl=63 time=6.61 ms
64 bytes from 192.168.10.13: icmp_seq=17 ttl=63 time=2.82 ms
64 bytes from 192.168.10.13: icmp_seq=18 ttl=63 time=5.79 ms
64 bytes from 192.168.10.13: icmp_seq=19 ttl=63 time=4.04 ms
64 bytes from 192.168.10.13: icmp_seq=20 ttl=63 time=2.37 ms
64 bytes from 192.168.10.13: icmp_seq=21 ttl=63 time=10.2 ms
64 bytes from 192.168.10.13: icmp_seq=22 ttl=63 time=20.3 ms
64 bytes from 192.168.10.13: icmp_seq=23 ttl=63 time=10.9 ms
64 bytes from 192.168.10.13: icmp_seq=24 ttl=63 time=7.51 ms
64 bytes from 192.168.10.13: icmp_seq=25 ttl=63 time=14.0 ms
64 bytes from 192.168.10.13: icmp_seq=26 ttl=63 time=17.6 ms
64 bytes from 192.168.10.13: icmp_seq=27 ttl=63 time=2.91 ms
64 bytes from 192.168.10.13: icmp_seq=28 ttl=63 time=9.18 ms
64 bytes from 192.168.10.13: icmp_seq=29 ttl=63 time=18.6 ms
64 bytes from 192.168.10.13: icmp_seq=30 ttl=63 time=4.19 ms
64 bytes from 192.168.10.13: icmp_seq=31 ttl=63 time=7.16 ms
^C
--- 192.168.10.13 ping statistics ---
31 packets transmitted, 31 received, 0% packet loss, time 30896ms
rtt min/avg/max/mdev = 2.372/6.863/20.274/5.152 ms
```

In external kali, I opened two terminals to ping ubuntu (left) and internal kali (right) I did ping them again after I took the screenshots

- a. Apply proper display or capture filter on Internal Kali VM to show active ICMP traffic

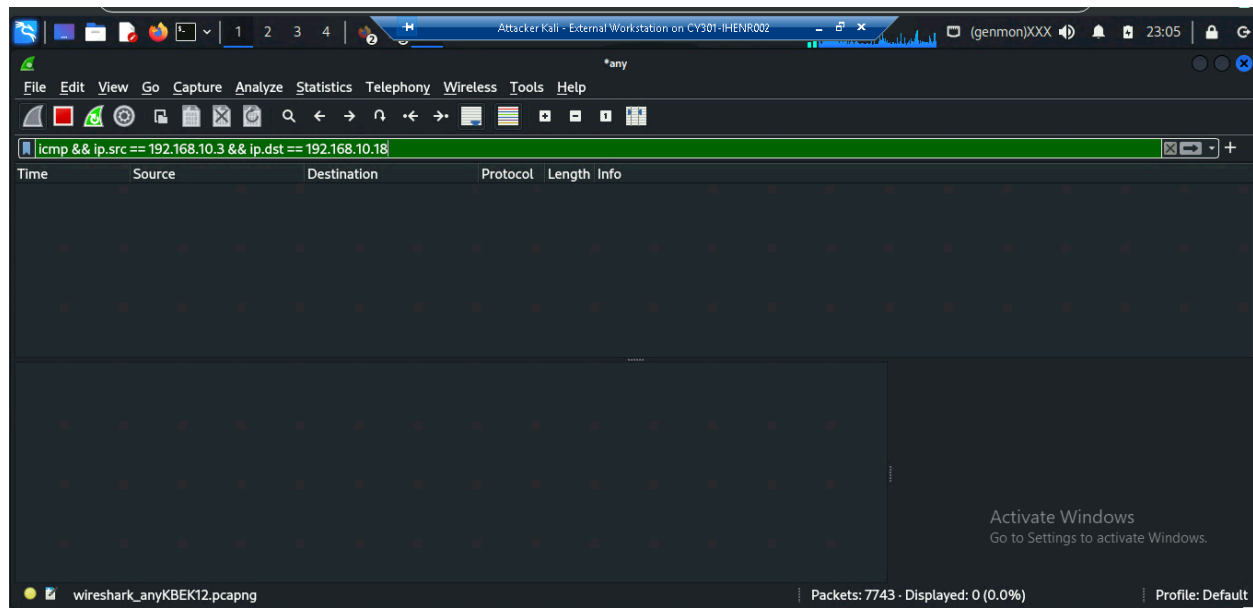
```
Attacker Kali - External Workstation on CY301-IHENR002 - Virtual Machine Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
Time Source Destination Protocol Length Info
56.147210900 192.168.217.3 192.168.10.18 ICMP 100 Echo (ping) request id=0xb31d, seq=86/22016, ttl=64 (reply
56.150099400 192.168.10.18 192.168.217.3 ICMP 100 Echo (ping) reply id=0xb31d, seq=86/22016, ttl=63 (request
56.451723900 192.168.217.3 192.168.10.13 ICMP 100 Echo (ping) request id=0x89cd, seq=77/19712, ttl=64 (reply
56.465471300 192.168.10.13 192.168.217.3 ICMP 100 Echo (ping) reply id=0x89cd, seq=77/19712, ttl=63 (request
57.155329800 192.168.217.3 192.168.10.18 ICMP 100 Echo (ping) request id=0xb31d, seq=87/22272, ttl=64 (reply
57.157406000 192.168.10.18 192.168.217.3 ICMP 100 Echo (ping) reply id=0xb31d, seq=87/22272, ttl=63 (request
57.461209800 192.168.217.3 192.168.10.13 ICMP 100 Echo (ping) request id=0x89cd, seq=78/19968, ttl=64 (reply
57.463489900 192.168.10.13 192.168.217.3 ICMP 100 Echo (ping) reply id=0x89cd, seq=78/19968, ttl=63 (request
58.157177300 192.168.217.3 192.168.10.18 ICMP 100 Echo (ping) request id=0xb31d, seq=88/22528, ttl=64 (reply
58.160350900 192.168.10.18 192.168.217.3 ICMP 100 Echo (ping) reply id=0xb31d, seq=88/22528, ttl=63 (request

> Frame 1: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface any, id
> Linux cooked capture v1
> Internet Protocol Version 4, Src: 192.168.217.3, Dst: 192.168.10.18
> Internet Control Message Protocol
0000 00 04 00 01 00 06 00 15 5d 40 00
0010 45 00 00 54 5b 2f 40 00 40 01 00
0020 c0 a8 0a 12 08 00 68 e2 b3 1d 00
0030 00 00 00 00 9d 90 09 00 00 00 00
0040 14 15 16 17 18 19 1a 1b 1c 1d 1e
0050 24 25 26 27 28 29 2a 2b 2c 2d 2e
0060 34 35 36 37
```

I opened wireshark using another window, listened on the “any” interface, and typed in “icmp” into the filter.

- b. Apply proper display or capture filter on Internal Kali VM that **ONLY** displays ICMP request originated from External Kali VM and goes to Ubuntu 64-bit VM



I typed "icmp" into the filter along with the external kali source ip and the ubuntu destination ip to narrow down any traffic between the VMs.

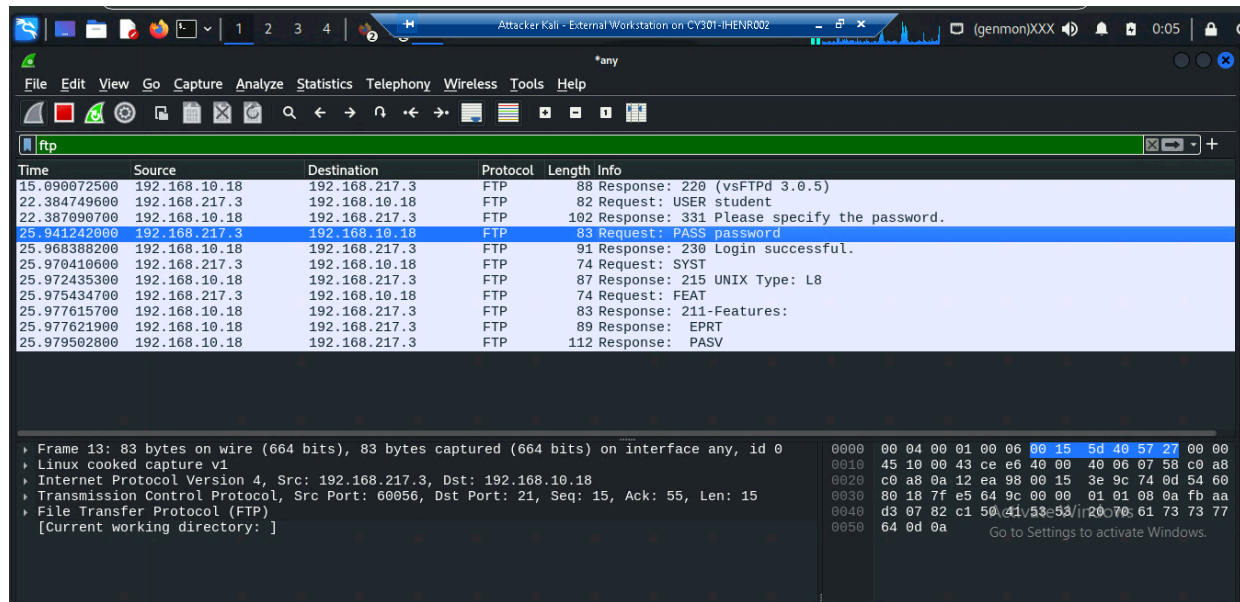
2. Sniff FTP traffic

- a. Ubuntu VM is also serving as an FTP server inside the LAN network. Now, you need to use External Kali to access this FTP server by using the command: `ftp [ip_addr of ubuntu VM]`. The username for the FTP server is `cyse301`, and the password is `password`. You can follow the steps below to access the FTP server.

```
on on CY301-IHENR002 (genmon)XXX 0:06
root@kali: ~
File Actions Edit View Help
(root@kali)-[~]
# ftp 192.168.10.18
Connected to 192.168.10.18.
220 (vsFTPd 3.0.5)
Name (192.168.10.18:root): student
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

In a window in external kali, I typed in ftp and the ip address for ubuntu, then used the given username and password.

- b. **Unfortunately, Internal Kali, the attacker, is also sniffing to the communication. Therefore, all of your communication is exposed to the attacker. Now, you need to find out the password used by External Kali to access the FTP server from the intercepted traffic on Internal Kali. You need to screenshot and explain how you find the password.**



I opened wireshark and listened in under the “any” interface. I filtered it so I could only see ftp traffic. Then I opened a new external kali window and tried to access the ftp server again using the same steps from above. I went back to wireshark and double clicked the password request which gave me the password I typed in.

- c. After you successfully find the username & password from the FTP traffic, repeat the previous step (2a), and use your MIDAS ID as the username and UIN as the password to reassess the FTP server from External Kali. Although External Kali may not access the FTP server, you need to intercept the packets containing these “secrets” from the attacker VM, which is Internal Kali.

```

(root@kali)-[~]
└─# ftp 192.168.10.18
Connected to 192.168.10.18.
220 (vsFTPd 3.0.5)
Name (192.168.10.18:root): ihenr002
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp>
  
```

The screenshot shows a Wireshark capture of network traffic. The top pane displays a list of captured packets. The bottom pane shows the details of the selected packet (packet 36), which is an FTP 'PASS' request. The details pane shows the following information:

- Frame 92: 83 bytes on wire (664 bits), 83 bytes captured (664 bits)
- Linux cooked capture v1
- Internet Protocol Version 4, Src: 192.168.217.3, Dst: 192.168.10.18
- Transmission Control Protocol, Src Port: 44720, Dst Port: 21, Seq: ...
- File Transfer Protocol (FTP)
 - PASS 01256007\r\n
 - Request command: PASS
 - Request arg: 01256007
 - [Current working directory:]

I repeated the steps from part (a), but this time I used my userID and UIN for the username and password. Then I went back to wireshark and looked at the password input to find my UIN.