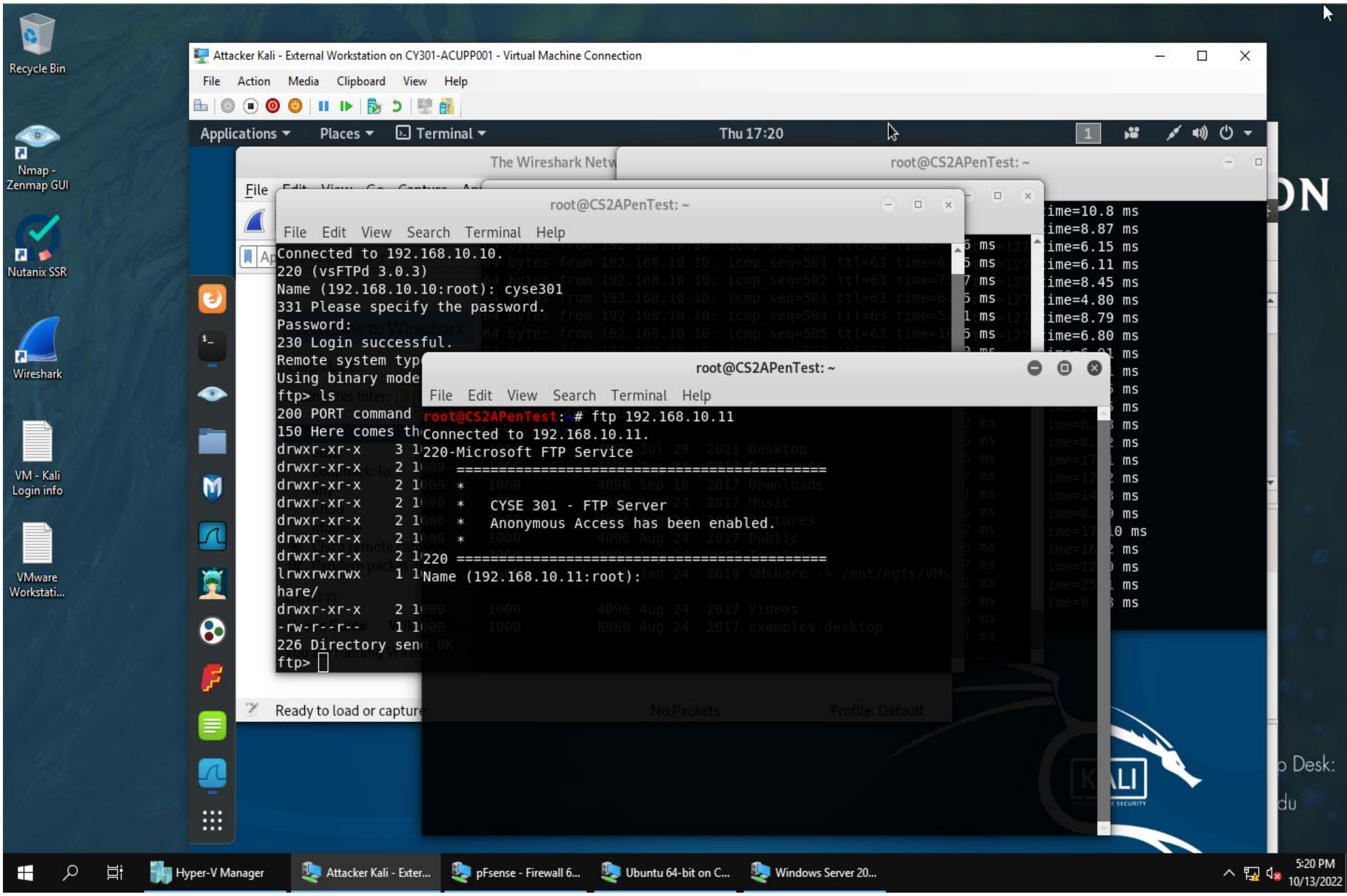
OLD DOMINION

CYSE301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #2 – Traffic Tracing and Sniffing

AUSTIN CUPP

01183567

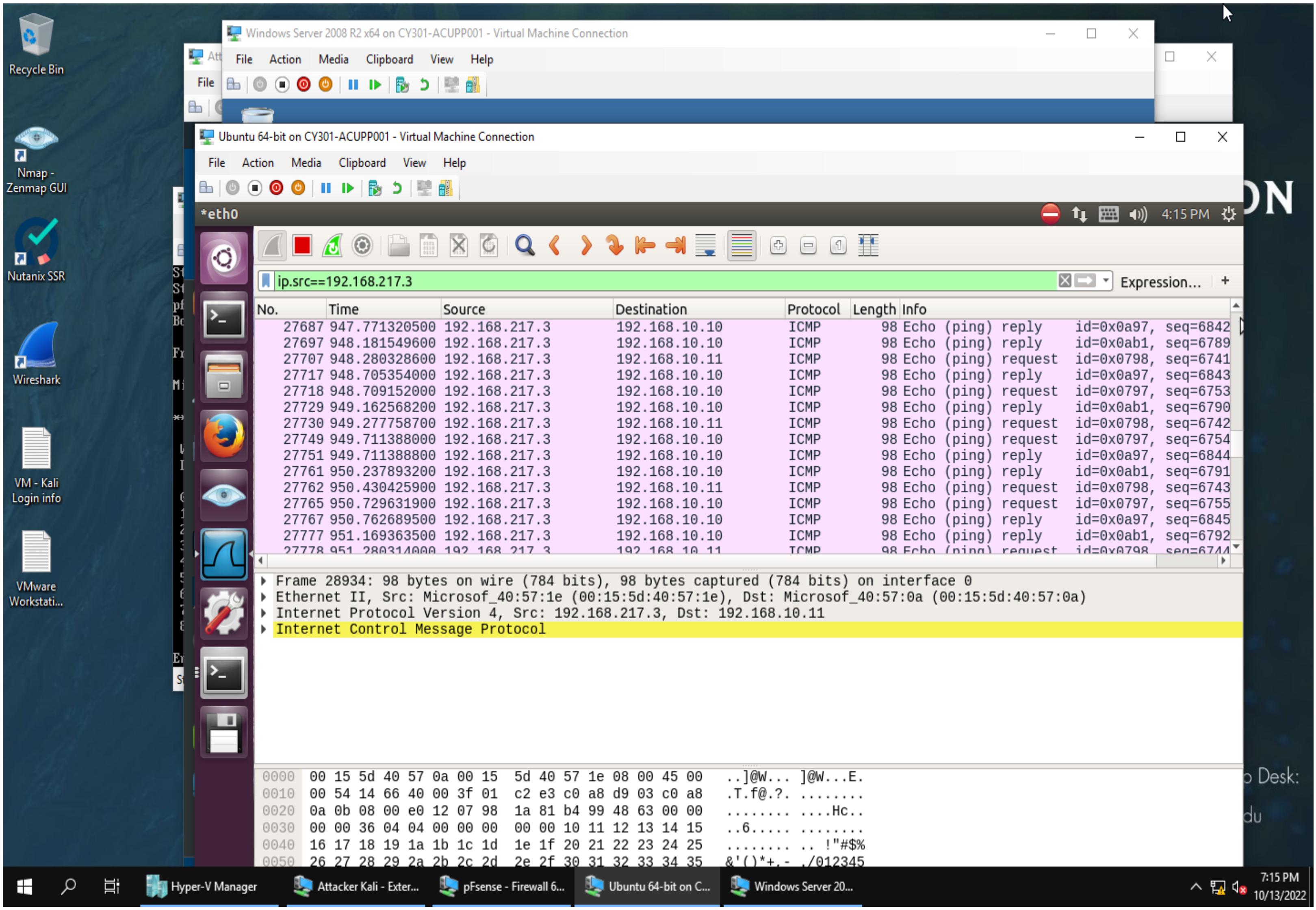


```
Connected to 192.168.10.10.
220 (vsFTPd 3.0.3)
Name (192.168.10.10:root): cyse301
331 Please specify the password.
Password:
230 Login successful.
Remote system typ
Using binary mode
ftp> ls
200 PORT command
150 Here comes th
drwxr-xr-x    3 1
drwxr-xr-x    2 1
drwxr-xr-x    2 1
drwxr-xr-x    2 1
drwxr-xr-x    2 1
drwxr-xr-x    2 1
drwxr-xr-x    2 1
lrwxrwxrwx    1 1
hare/
drwxr-xr-x    2 1
-rw-r--r--    1 1
226 Directory sen
ftp> 
```

```
root@CS2APenTest:~# ftp 192.168.10.11
Connected to 192.168.10.11.
220-Microsoft FTP Service
    ============================================
    *
    *    CYSE 301 - FTP Server
    *    Anonymous Access has been enabled.
    *
220 ============================================
Name (192.168.10.11:root):
```

```
ime=10.8 ms
ime=8.87 ms
ime=6.15 ms
ime=6.11 ms
ime=8.45 ms
ime=4.80 ms
ime=8.79 ms
ime=6.80 ms
```

1.1 The Windows Server 2008 and Ubuntu VM are pinged from two separate terminals and ubuntu and windows 2008 are connected via ftp command



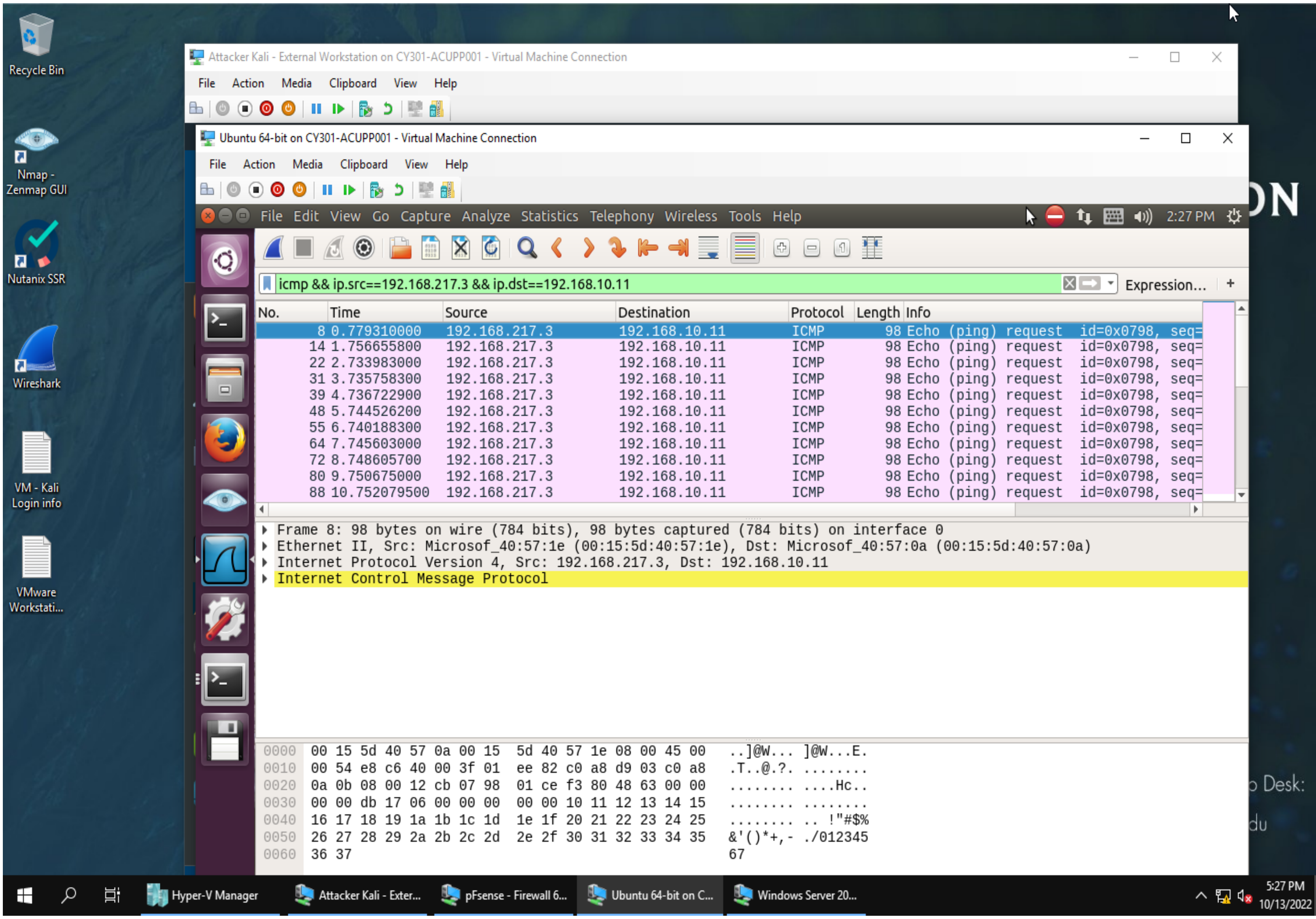
ip.src==192.168.217.3

```
No.   Time         Source          Destination    Protocol Length Info
27687 947.771320500 192.168.217.3  192.168.10.10  ICMP     98 Echo (ping) reply    id=0x0a97, seq=6842
27697 948.181549600 192.168.217.3  192.168.10.10  ICMP     98 Echo (ping) reply    id=0x0ab1, seq=6789
27707 948.280328600 192.168.217.3  192.168.10.11  ICMP     98 Echo (ping) request  id=0x0798, seq=6741
27717 948.705354000 192.168.217.3  192.168.10.10  ICMP     98 Echo (ping) reply    id=0x0a97, seq=6843
27718 948.709152000 192.168.217.3  192.168.10.10  ICMP     98 Echo (ping) request  id=0x0797, seq=6753
27729 949.162568200 192.168.217.3  192.168.10.10  ICMP     98 Echo (ping) reply    id=0x0ab1, seq=6790
27730 949.277758700 192.168.217.3  192.168.10.11  ICMP     98 Echo (ping) request  id=0x0798, seq=6742
27749 949.711388000 192.168.217.3  192.168.10.10  ICMP     98 Echo (ping) request  id=0x0797, seq=6754
27751 949.711388800 192.168.217.3  192.168.10.10  ICMP     98 Echo (ping) reply    id=0x0a97, seq=6844
27761 950.237893200 192.168.217.3  192.168.10.10  ICMP     98 Echo (ping) reply    id=0x0ab1, seq=6791
27762 950.430425900 192.168.217.3  192.168.10.11  ICMP     98 Echo (ping) request  id=0x0798, seq=6743
27765 950.729631900 192.168.217.3  192.168.10.10  ICMP     98 Echo (ping) request  id=0x0797, seq=6755
27767 950.762689500 192.168.217.3  192.168.10.10  ICMP     98 Echo (ping) reply    id=0x0a97, seq=6845
27777 951.169363500 192.168.217.3  192.168.10.10  ICMP     98 Echo (ping) reply    id=0x0ab1, seq=6792
27778 951.280314000 192.168.217.3  192.168.10.11  ICMP     98 Echo (ping) request  id=0x0798, seq=6744
```

```
▸ Frame 28934: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▸ Ethernet II, Src: Microsof_40:57:1e (00:15:5d:40:57:1e), Dst: Microsof_40:57:0a (00:15:5d:40:57:0a)
▸ Internet Protocol Version 4, Src: 192.168.217.3, Dst: 192.168.10.11
▸ Internet Control Message Protocol
```

```
0000  00 15 5d 40 57 0a 00 15  5d 40 57 1e 08 00 45 00   ..]@W... ]@W...E.
0010  00 54 14 66 40 00 3f 01  c2 e3 c0 a8 d9 03 c0 a8   .T.f@.?. ........
0020  0a 0b 08 00 e0 12 07 98  1a 81 b4 99 48 63 00 00   ........ ....Hc..
0030  00 00 36 04 04 00 00 00  00 00 10 11 12 13 14 15   ..6..... ........
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ........ .. !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
```

1.2 External Kali VM IP source filter is applied to show all ping traffic towards Ubuntu and Windows Server 2008.


Attacker Kali - External Workstation on CY301-ACUPP001 - Virtual Machine Connection
Ubuntu 64-bit on CY301-ACUPP001 - Virtual Machine Connection
File Action Media Clipboard View Help
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
2:27 PM
Expression...
Recycle Bin
Nmap - Zenmap GUI
Nutanix SSR
Wireshark
VM - Kali Login info
VMware Workstati...
Hyper-V Manager
Attacker Kali - Exter...
pFsense - Firewall 6...
Ubuntu 64-bit on C...
Windows Server 20...
5:27 PM
10/13/2022

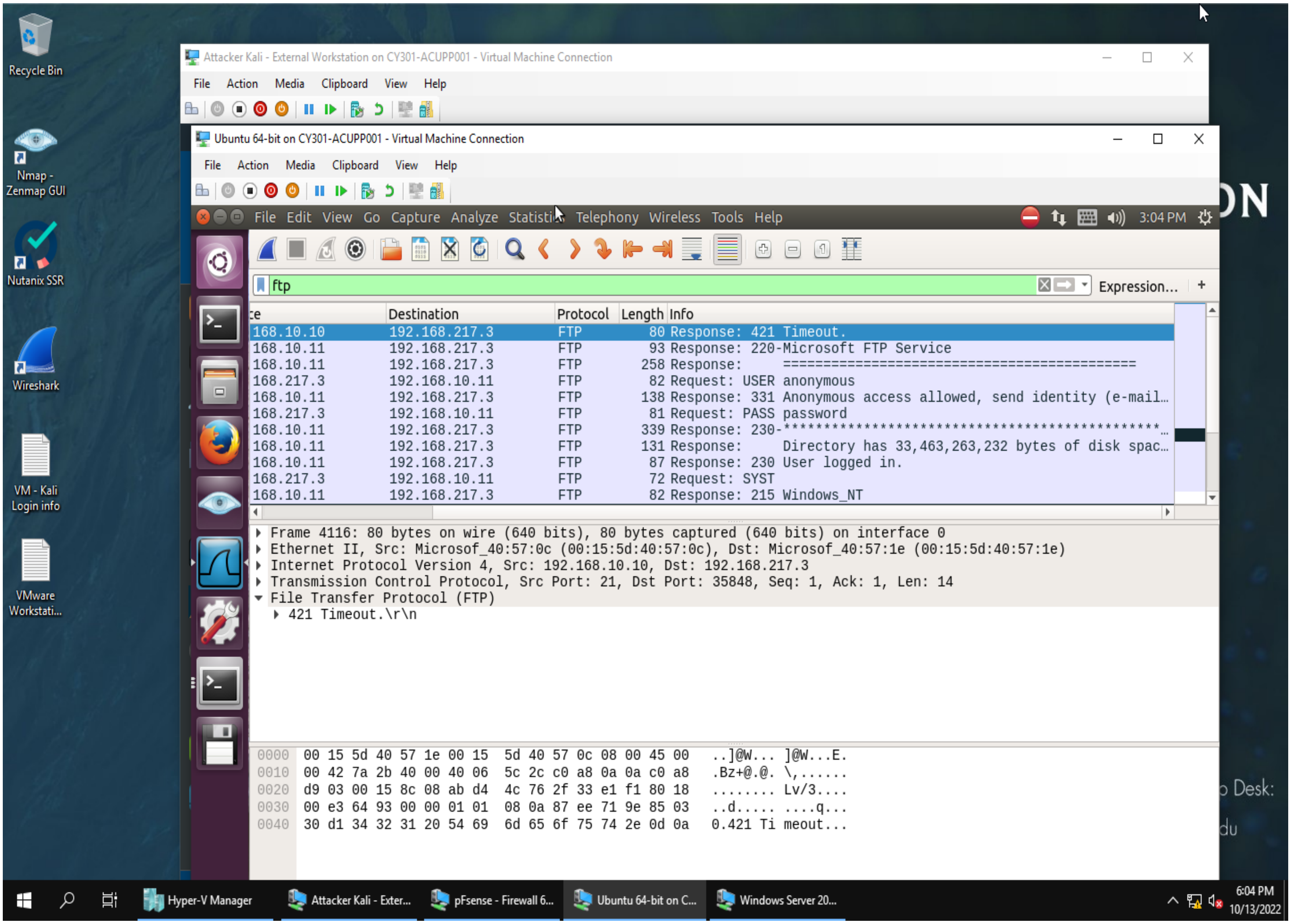
icmp && ip.src==192.168.217.3 && ip.dst==192.168.10.11

```
No.   Time          Source          Destination     Protocol Length Info
    8 0.779310000   192.168.217.3   192.168.10.11   ICMP         98 Echo (ping) request  id=0x0798, seq=
   14 1.756655800   192.168.217.3   192.168.10.11   ICMP         98 Echo (ping) request  id=0x0798, seq=
   22 2.733983000   192.168.217.3   192.168.10.11   ICMP         98 Echo (ping) request  id=0x0798, seq=
   31 3.735758300   192.168.217.3   192.168.10.11   ICMP         98 Echo (ping) request  id=0x0798, seq=
   39 4.736722900   192.168.217.3   192.168.10.11   ICMP         98 Echo (ping) request  id=0x0798, seq=
   48 5.744526200   192.168.217.3   192.168.10.11   ICMP         98 Echo (ping) request  id=0x0798, seq=
   55 6.740188300   192.168.217.3   192.168.10.11   ICMP         98 Echo (ping) request  id=0x0798, seq=
   64 7.745603000   192.168.217.3   192.168.10.11   ICMP         98 Echo (ping) request  id=0x0798, seq=
   72 8.748605700   192.168.217.3   192.168.10.11   ICMP         98 Echo (ping) request  id=0x0798, seq=
   80 9.750675000   192.168.217.3   192.168.10.11   ICMP         98 Echo (ping) request  id=0x0798, seq=
   88 10.752079500  192.168.217.3   192.168.10.11   ICMP         98 Echo (ping) request  id=0x0798, seq=
```

```
▸ Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▸ Ethernet II, Src: Microsof_40:57:1e (00:15:5d:40:57:1e), Dst: Microsof_40:57:0a (00:15:5d:40:57:0a)
▸ Internet Protocol Version 4, Src: 192.168.217.3, Dst: 192.168.10.11
▸ Internet Control Message Protocol
```

```
0000  00 15 5d 40 57 0a 00 15  5d 40 57 1e 08 00 45 00   ..]@W... ]@W...E.
0010  00 54 e8 c6 40 00 3f 01  ee 82 c0 a8 d9 03 c0 a8   .T..@.?. ........
0020  0a 0b 08 00 12 cb 07 98  01 ce f3 80 48 63 00 00   ........ ....Hc..
0030  00 00 db 17 06 00 00 00  00 00 10 11 12 13 14 15   ........ ........
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ........ .. !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

1.3 The proper filter is applied in order to show only IMCP requests that originated from External Kali VM and goes to Windows Server 2008



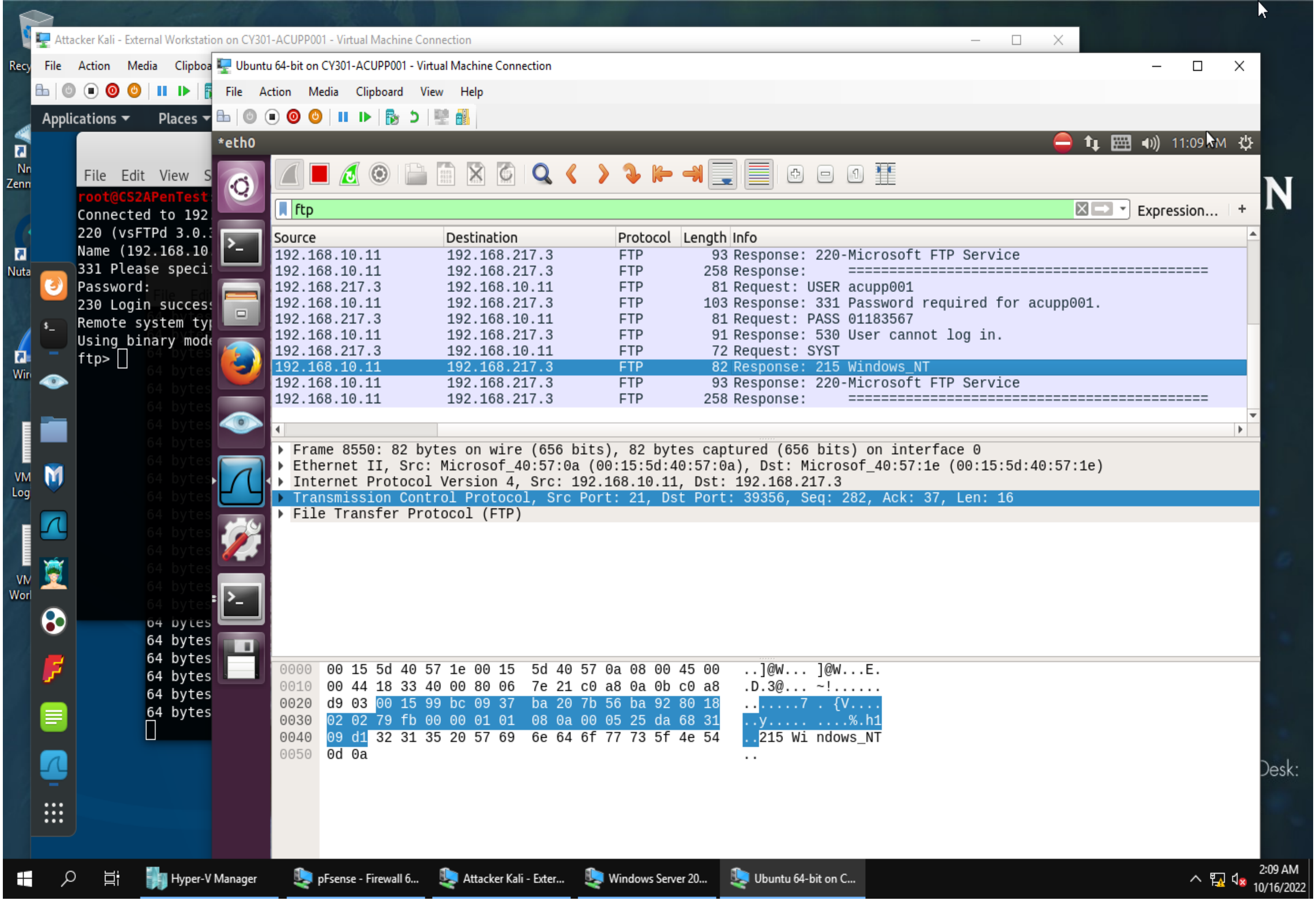
Recycle Bin
Nmap - Zenmap GUI
Nutanix SSR
Wireshark
VM - Kali Login info
VMware Workstati...
Attacker Kali - External Workstation on CY301-ACUPP001 - Virtual Machine Connection
Ubuntu 64-bit on CY301-ACUPP001 - Virtual Machine Connection
File Action Media Clipboard View Help
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
3:04 PM
ftp
Expression...
Hyper-V Manager
Attacker Kali - Exter...
pFsense - Firewall 6...
Ubuntu 64-bit on C...
Windows Server 20...
6:04 PM
10/13/2022

```
ce              Destination     Protocol Length Info
168.10.10       192.168.217.3   FTP          80 Response: 421 Timeout.
168.10.11       192.168.217.3   FTP          93 Response: 220-Microsoft FTP Service
168.10.11       192.168.217.3   FTP         258 Response:     ==========================================
168.217.3       192.168.10.11   FTP          82 Request: USER anonymous
168.10.11       192.168.217.3   FTP         138 Response: 331 Anonymous access allowed, send identity (e-mail…
168.217.3       192.168.10.11   FTP          81 Request: PASS password
168.10.11       192.168.217.3   FTP         339 Response: 230-************************************************…
168.10.11       192.168.217.3   FTP         131 Response:     Directory has 33,463,263,232 bytes of disk spac…
168.10.11       192.168.217.3   FTP          87 Response: 230 User logged in.
168.217.3       192.168.10.11   FTP          72 Request: SYST
168.10.11       192.168.217.3   FTP          82 Response: 215 Windows_NT
```

```
▸ Frame 4116: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface 0
▸ Ethernet II, Src: Microsof_40:57:0c (00:15:5d:40:57:0c), Dst: Microsof_40:57:1e (00:15:5d:40:57:1e)
▸ Internet Protocol Version 4, Src: 192.168.10.10, Dst: 192.168.217.3
▸ Transmission Control Protocol, Src Port: 21, Dst Port: 35848, Seq: 1, Ack: 1, Len: 14
▾ File Transfer Protocol (FTP)
  ▸ 421 Timeout.\r\n
```

```
0000  00 15 5d 40 57 1e 00 15  5d 40 57 0c 08 00 45 00   ..]@W... ]@W...E.
0010  00 42 7a 2b 40 00 40 06  5c 2c c0 a8 0a 0a c0 a8   .Bz+@.@. \,......
0020  d9 03 00 15 8c 08 ab d4  4c 76 2f 33 e1 f1 80 18   ........ Lv/3....
0030  00 e3 64 93 00 00 01 01  08 0a 87 ee 71 9e 85 03   ..d..... ....q...
0040  30 d1 34 32 31 20 54 69  6d 65 6f 75 74 2e 0d 0a   0.421 Ti meout...
```

2.1 On attacker kali, ftp command is used for Windows 2008 IP Address in an attempt to connect. I entered in the username anonymous, and the password, which is password, and then connected. I then used FTP protocol filter in the Ubuntu Wireshark to sniff the username and password.



```
root@CS2APenTest
Connected to 192
220 (vsFTPd 3.0.3
Name (192.168.10
331 Please speci
Password:
230 Login success
Remote system typ
Using binary mode
ftp>
```

```
64 bytes
64 bytes
64 bytes
64 bytes
64 bytes
64 bytes
64 bytes
64 bytes
64 bytes
64 bytes
64 bytes
64 bytes
64 bytes
64 bytes
64 bytes
64 bytes
64 bytes
64 bytes
64 bytes
64 bytes
64 bytes
```

ftp

```
Source          Destination     Protocol Length Info
192.168.10.11   192.168.217.3   FTP         93 Response: 220-Microsoft FTP Service
192.168.10.11   192.168.217.3   FTP        258 Response:     ==========================================
192.168.217.3   192.168.10.11   FTP         81 Request: USER acupp001
192.168.10.11   192.168.217.3   FTP        103 Response: 331 Password required for acupp001.
192.168.217.3   192.168.10.11   FTP         81 Request: PASS 01183567
192.168.10.11   192.168.217.3   FTP         91 Response: 530 User cannot log in.
192.168.217.3   192.168.10.11   FTP         72 Request: SYST
192.168.10.11   192.168.217.3   FTP         82 Response: 215 Windows_NT
192.168.10.11   192.168.217.3   FTP         93 Response: 220-Microsoft FTP Service
192.168.10.11   192.168.217.3   FTP        258 Response:     ==========================================
```

```
▸ Frame 8550: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface 0
▸ Ethernet II, Src: Microsof_40:57:0a (00:15:5d:40:57:0a), Dst: Microsof_40:57:1e (00:15:5d:40:57:1e)
▸ Internet Protocol Version 4, Src: 192.168.10.11, Dst: 192.168.217.3
▸ Transmission Control Protocol, Src Port: 21, Dst Port: 39356, Seq: 282, Ack: 37, Len: 16
▸ File Transfer Protocol (FTP)
```

```
0000  00 15 5d 40 57 1e 00 15  5d 40 57 0a 08 00 45 00   ..]@W... ]@W...E.
0010  00 44 18 33 40 00 80 06  7e 21 c0 a8 0a 0b c0 a8   .D.3@... ~!......
0020  d9 03 00 15 99 bc 09 37  ba 20 7b 56 ba 92 80 18   .......7 . {V....
0030  02 02 79 fb 00 00 01 01  08 0a 00 05 25 da 68 31   ..y..... ....%.h1
0040  09 d1 32 31 35 20 57 69  6e 64 6f 77 73 5f 4e 54   ..215 Wi ndows_NT
0050  0d 0a                                              ..
```

2.2 The packets containing the secrets are intercepted by repeating step one of 2.1 using my Midas id and UIN