OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

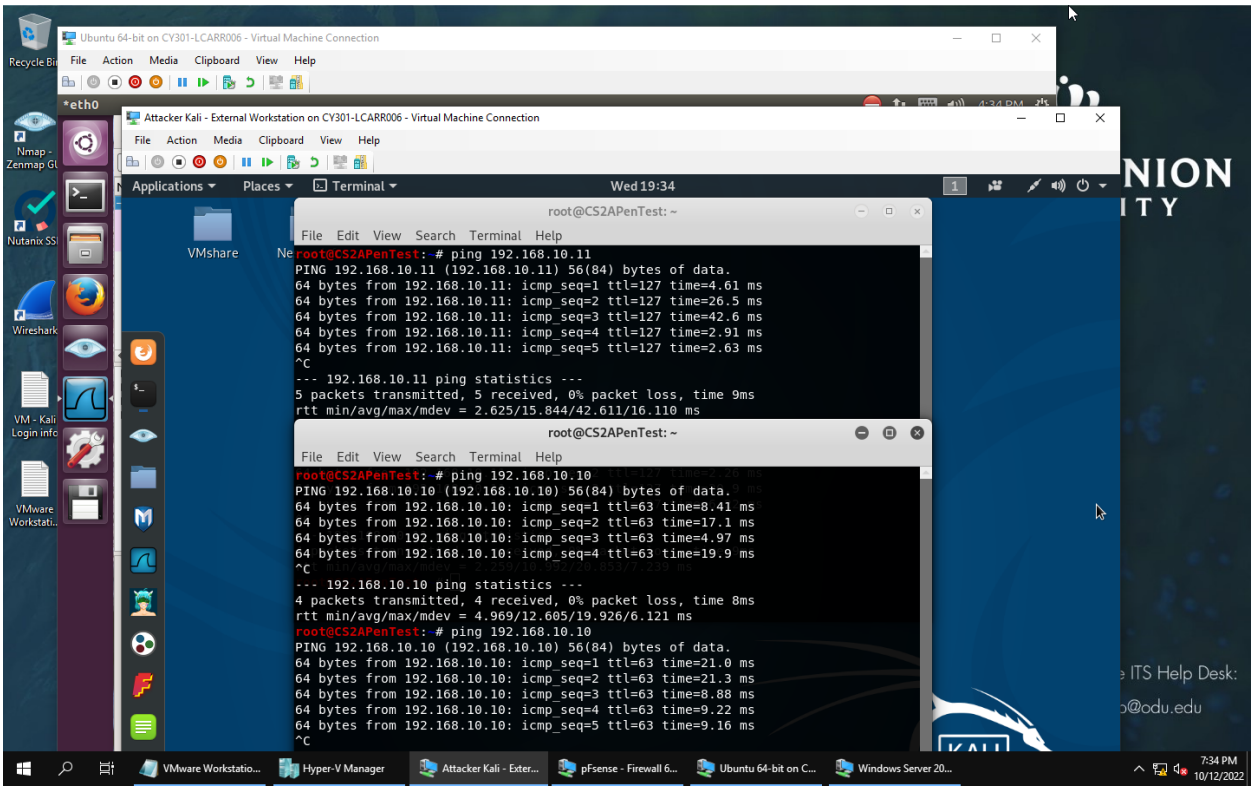
Assignment #2: TRAFFIC TRACING/SNIFFING

RITZ CARR

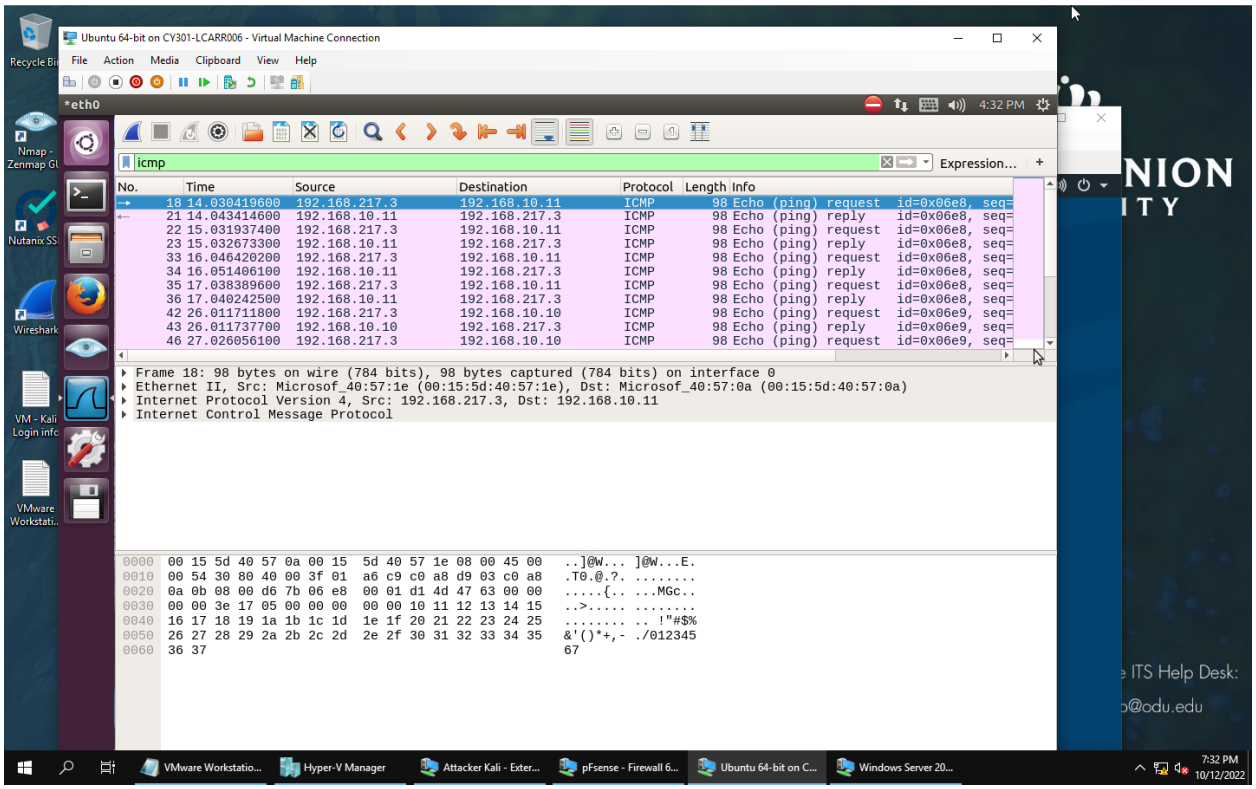
01191227

TASK A

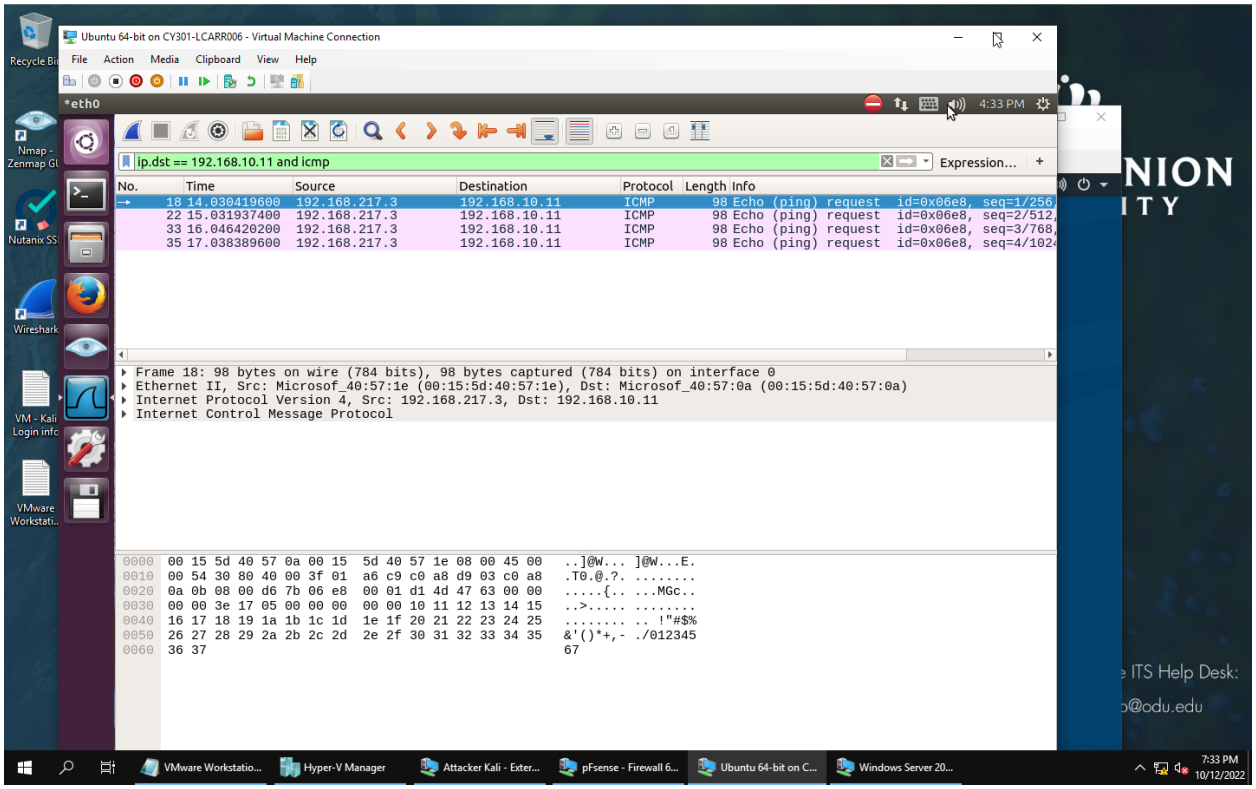
- 1.1: PINGING WINDOWS & UBUNTU FROM KALI:



- 1.2

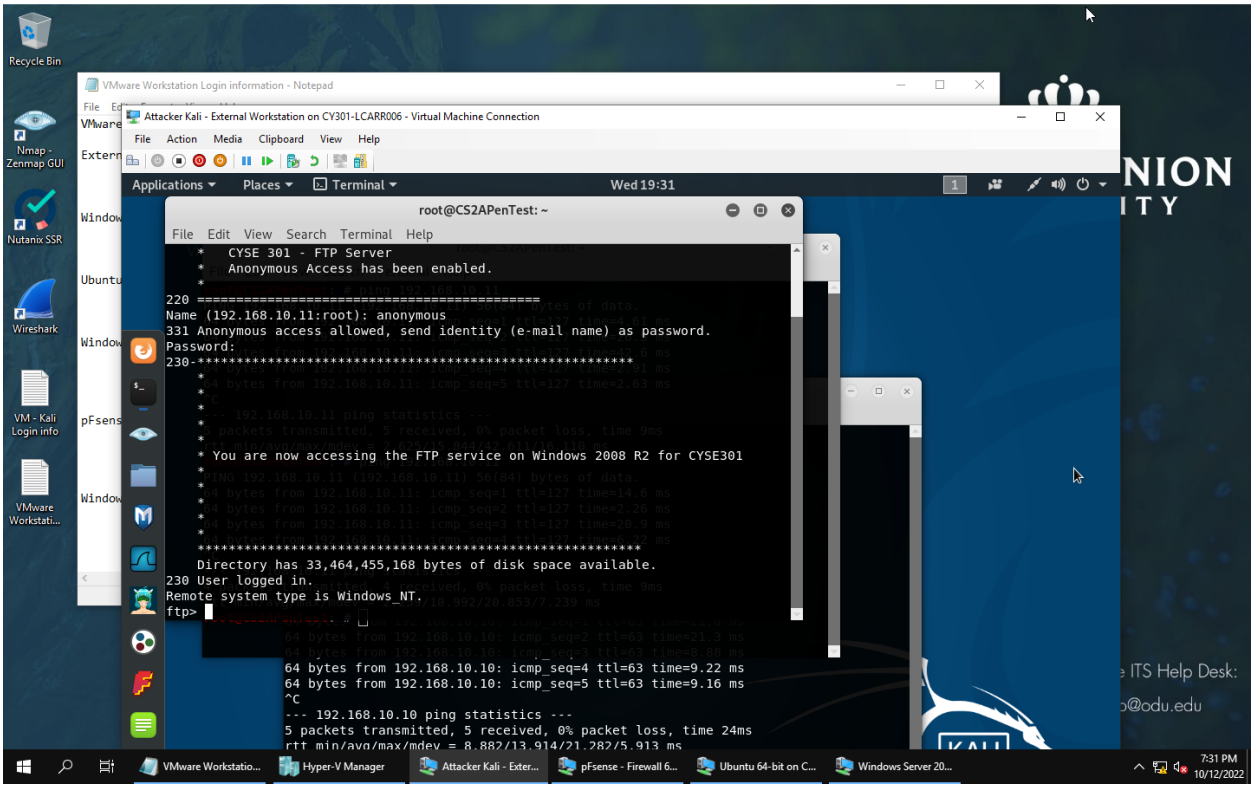

Ubuntu 64-bit on CY301-LCARR006 - Virtual Machine Connection
File Action Media Clipboard View Help
*eth0
4:32 PM
icmp
Expression...
No. Time Source Destination Protocol Length Info
18 14.030419600 192.168.217.3 192.168.10.11 ICMP 98 Echo (ping) request id=0x06e8, seq=
21 14.043414600 192.168.10.11 192.168.217.3 ICMP 98 Echo (ping) reply id=0x06e8, seq=
22 15.031937400 192.168.217.3 192.168.10.11 ICMP 98 Echo (ping) request id=0x06e8, seq=
23 15.032673300 192.168.10.11 192.168.217.3 ICMP 98 Echo (ping) reply id=0x06e8, seq=
33 16.046420200 192.168.217.3 192.168.10.11 ICMP 98 Echo (ping) request id=0x06e8, seq=
34 16.051406100 192.168.10.11 192.168.217.3 ICMP 98 Echo (ping) reply id=0x06e8, seq=
35 17.038389600 192.168.217.3 192.168.10.11 ICMP 98 Echo (ping) request id=0x06e8, seq=
36 17.040242500 192.168.10.11 192.168.217.3 ICMP 98 Echo (ping) reply id=0x06e8, seq=
42 26.011711800 192.168.217.3 192.168.10.10 ICMP 98 Echo (ping) request id=0x06e9, seq=
43 26.011737700 192.168.10.10 192.168.217.3 ICMP 98 Echo (ping) reply id=0x06e9, seq=
46 27.026056100 192.168.217.3 192.168.10.10 ICMP 98 Echo (ping) request id=0x06e9, seq=
Frame 18: 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 30 80 40 00 3f 01 a6 c9 c0 a8 d9 03 c0 a8 .T0.@.?. ....
0020 0a 0b 08 00 d6 7b 06 e8 00 01 d1 4d 47 63 00 00 .....{.. ...MGc..
0030 00 00 3e 17 05 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
Nmap - Zenmap GU
Nutanix SS
Wireshark
VM - Kali Login info
VMware Workstati...
Recycle Bin
VMware Workstatio...
Hyper-V Manager
Attacker Kali - Exter...
pFsense - Firewall 6...
Ubuntu 64-bit on C...
Windows Server 20...
7:32 PM
10/12/2022

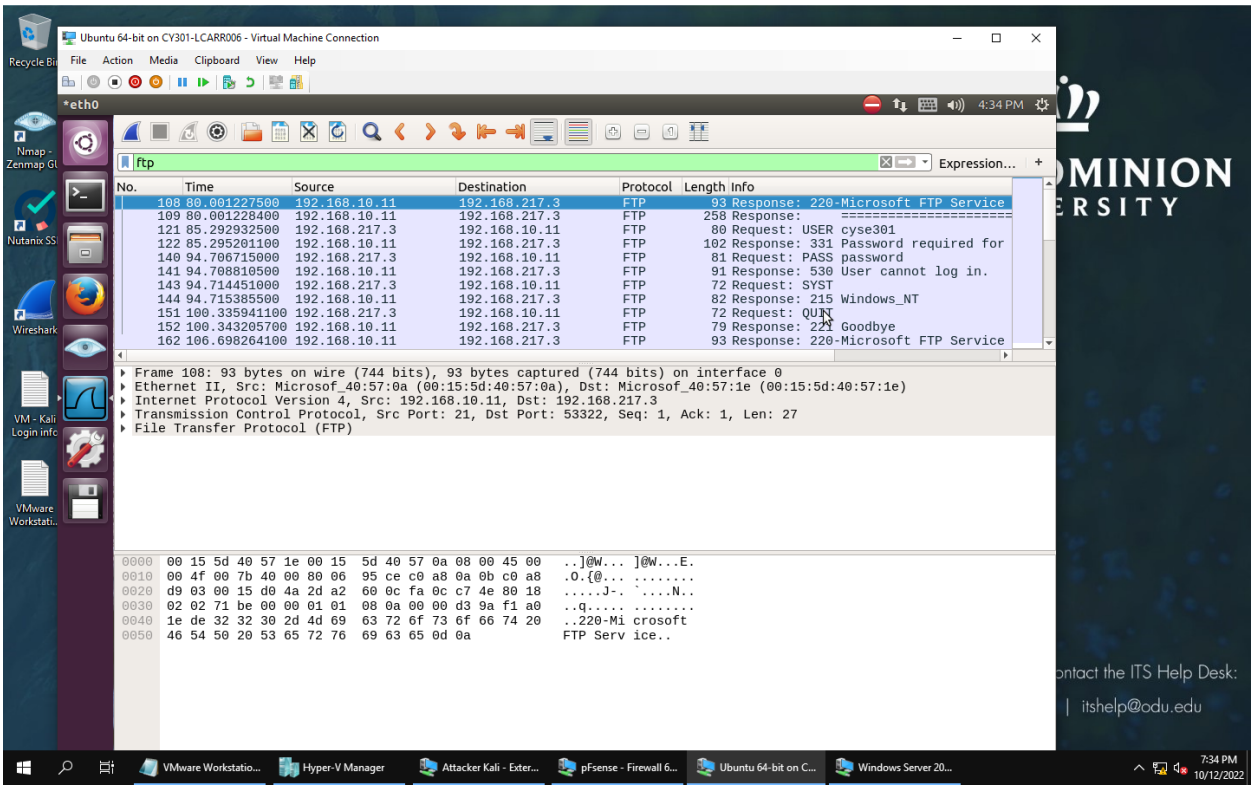
- 1.3


Ubuntu 64-bit on CY301-LCARR006 - Virtual Machine Connection
File Action Media Clipboard View Help
*eth0
4:33 PM
ip.dst == 192.168.10.11 and icmp
Expression...
No. Time Source Destination Protocol Length Info
18 14.030419600 192.168.217.3 192.168.10.11 ICMP 98 Echo (ping) request id=0x06e8, seq=1/256
22 15.031937400 192.168.217.3 192.168.10.11 ICMP 98 Echo (ping) request id=0x06e8, seq=2/512,
33 16.046420200 192.168.217.3 192.168.10.11 ICMP 98 Echo (ping) request id=0x06e8, seq=3/768,
35 17.038389600 192.168.217.3 192.168.10.11 ICMP 98 Echo (ping) request id=0x06e8, seq=4/1024
Frame 18: 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 30 80 40 00 3f 01 a6 c9 c0 a8 d9 03 c0 a8 .T0.@.?. ....
0020 0a 0b 08 00 d6 7b 06 e8 00 01 d1 4d 47 63 00 00 .....{.. ...MGc..
0030 00 00 3e 17 05 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
Nmap - Zenmap GU
Nutanix SS
Wireshark
VM - Kali Login info
VMware Workstati...
Recycle Bin
VMware Workstatio...
Hyper-V Manager
Attacker Kali - Exter...
pFsense - Firewall 6...
Ubuntu 64-bit on C...
Windows Server 20...
7:33 PM
10/12/2022

TASK B

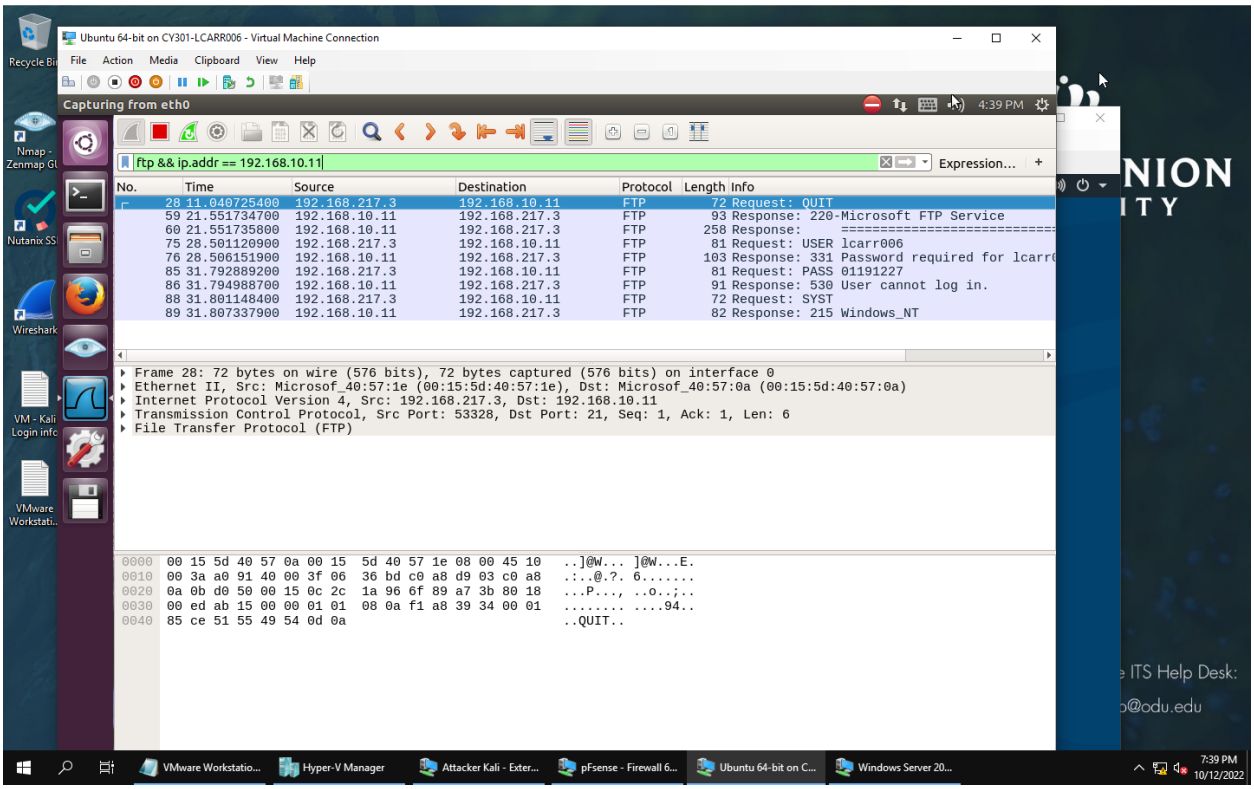
2.1:


Attacker Kali - External Workstation on CY301-LCARR006 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal Wed 19:31
root@CS2APenTest: ~
File Edit View Search Terminal Help
* CYSE 301 - FTP Server
* Anonymous Access has been enabled.
220 ==========
Name (192.168.10.11:root): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230-**********
* You are now accessing the FTP service on Windows 2008 R2 for CYSE301
****
Directory has 33,464,455,168 bytes of disk space available.
230 User logged in.
Remote system type is Windows_NT.
ftp>
64 bytes from 192.168.10.10: icmp_seq=4 ttl=63 time=9.22 ms
64 bytes from 192.168.10.10: icmp_seq=5 ttl=63 time=9.16 ms
^C
--- 192.168.10.10 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 24ms
rtt min/avg/max/mdev = 8.882/13.914/21.282/5.913 ms
Recycle Bin
Nmap - Zenmap GUI
Nutanix SSR
Wireshark
VM - Kali Login info
VMware Workstati...
VMware Workstatio...
Hyper-V Manager
Attacker Kali - Exter...
pFsense - Firewall 6...
Ubuntu 64-bit on C...
Windows Server 20...
7:31 PM
10/12/2022



The password can be found by selecting the FTP display filter and using AND to add in the source IP address, 192.168.10.11. Here, we can see both the username and password enter upon login to the FTP server.

2.2:


Ubuntu 64-bit on CY301-LCARR006 - Virtual Machine Connection
File Action Media Clipboard View Help
Capturing from eth0
4:39 PM
ftp && ip.addr == 192.168.10.11
Expression...
No. Time Source Destination Protocol Length Info
28 11.040725400 192.168.217.3 192.168.10.11 FTP 72 Request: QUIT
59 21.551734700 192.168.10.11 192.168.217.3 FTP 93 Response: 220-Microsoft FTP Service
60 21.551735800 192.168.10.11 192.168.217.3 FTP 258 Response:
75 28.501120900 192.168.217.3 192.168.10.11 FTP 81 Request: USER lcarr006
76 28.506151900 192.168.10.11 192.168.217.3 FTP 103 Response: 331 Password required for lcarr
85 31.792889200 192.168.217.3 192.168.10.11 FTP 81 Request: PASS 01191227
86 31.794988700 192.168.10.11 192.168.217.3 FTP 91 Response: 530 User cannot log in.
88 31.801148400 192.168.217.3 192.168.10.11 FTP 72 Request: SYST
89 31.807337900 192.168.10.11 192.168.217.3 FTP 82 Response: 215 Windows_NT
Frame 28: 72 bytes on wire (576 bits), 72 bytes captured (576 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
Transmission Control Protocol, Src Port: 53328, Dst Port: 21, Seq: 1, Ack: 1, Len: 6
File Transfer Protocol (FTP)
0000 00 15 5d 40 57 0a 00 15 5d 40 57 1e 08 00 45 10 ..]@W...]@W...E.
0010 00 3a a0 91 40 00 3f 06 36 bd c0 a8 d9 03 c0 a8 .:..@.?. 6.....
0020 0a 0b d0 50 00 15 0c 2c 1a 96 6f 89 a7 3b 80 18 ...P..., ..o..;..
0030 00 ed ab 15 00 00 01 01 08 0a f1 a8 39 34 00 01 ....94..
0040 85 ce 51 55 49 54 0d 0a ..QUIT..
Recycle Bin
Nmap - Zenmap GUI
Nutanix SSH
Wireshark
VM - Kali Login info
VMware Workstati...
VMware Workstatio...
Hyper-V Manager
Attacker Kali - Exter...
pFsense - Firewall 6...
Ubuntu 64-bit on C...
Windows Server 20...
7:39 PM
10/12/2022