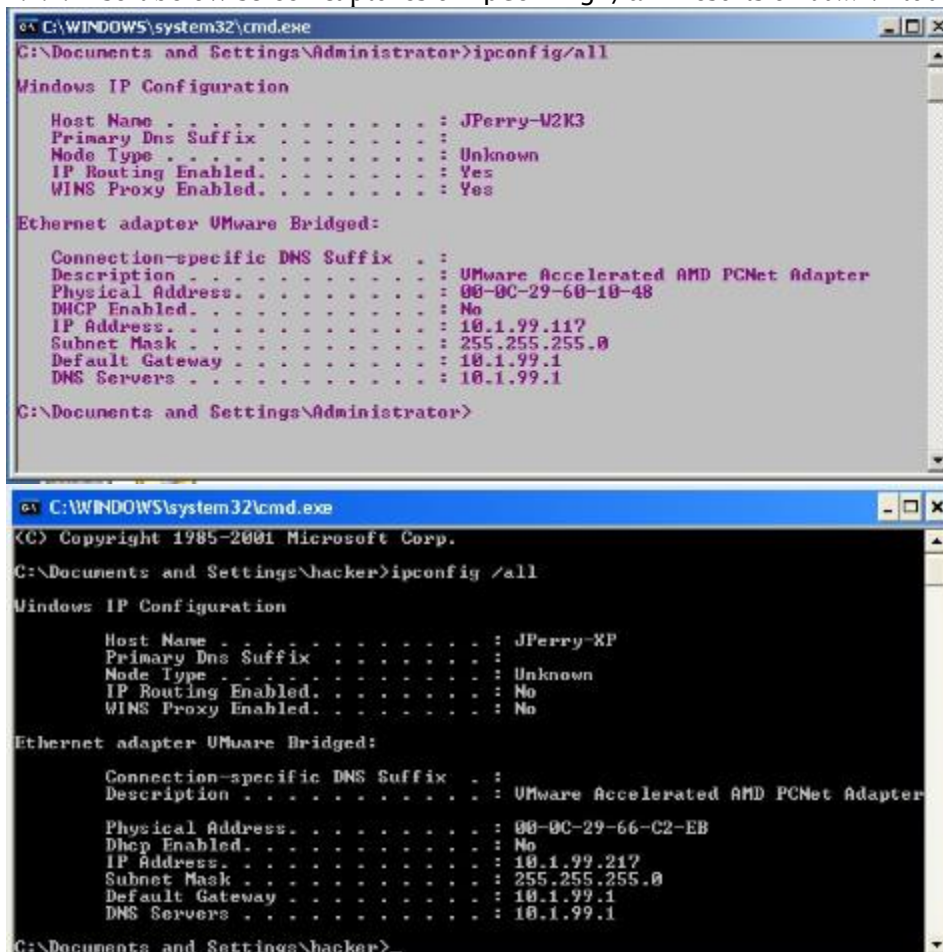


BCIS 4630 Lab 1 Worksheet

Question 1.1

1.1.1. Insert below screen captures of `ipconfig /all` results on *both* virtual machines.



The image contains two screenshots of Windows command prompts. The top screenshot shows the output of `ipconfig /all` for a virtual machine named 'JPerry-U2K3'. The bottom screenshot shows the output for a virtual machine named 'JPerry-XP'.

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>ipconfig/all

Windows IP Configuration

    Host Name . . . . . : JPerry-U2K3
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Unknown
    IP Routing Enabled. . . . . : Yes
    WINS Proxy Enabled. . . . . : Yes

Ethernet adapter VMware Bridged:

    Connection-specific DNS Suffix  . :
    Description . . . . . : VMware Accelerated AMD PCNet Adapter
    Physical Address. . . . . : 08-0C-29-60-10-48
    DHCP Enabled. . . . . : No
    IP Address. . . . . : 10.1.99.117
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.1.99.1
    DNS Servers . . . . . : 10.1.99.1

C:\Documents and Settings\Administrator>
```

```
C:\WINDOWS\system32\cmd.exe
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\hacker>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : JPerry-XP
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Unknown
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

Ethernet adapter VMware Bridged:

    Connection-specific DNS Suffix  . :
    Description . . . . . : VMware Accelerated AMD PCNet Adapter
    Physical Address. . . . . : 08-0C-29-66-C2-EB
    Dhcp Enabled. . . . . : No
    IP Address. . . . . : 10.1.99.217
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.1.99.1
    DNS Servers . . . . . : 10.1.99.1

C:\Documents and Settings\hacker>
```

1.1.2. Insert below screen captures of `ping` results on *both* virtual machines.

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>ping 10.1.99.217

Pinging 10.1.99.217 with 32 bytes of data:

Reply from 10.1.99.217: bytes=32 time<1ms TTL=128
Reply from 10.1.99.217: bytes=32 time<1ms TTL=128
Reply from 10.1.99.217: bytes=32 time<1ms TTL=128
Reply from 10.1.99.217: bytes=32 time<1ms TTL=128

Ping statistics for 10.1.99.217:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>

C:\WINDOWS\system32\cmd.exe

Connection-specific DNS Suffix . : 
Description . . . . . : VMware Accelerated AMD PCNet Adapter
Physical Address. . . . . : 08-0C-29-66-C2-EB
Dhcp Enabled. . . . . : No
IP Address. . . . . : 10.1.99.217
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.1.99.1
DNS Servers . . . . . : 10.1.99.1

C:\Documents and Settings\hacker>ping 10.1.99.117

Pinging 10.1.99.117 with 32 bytes of data:

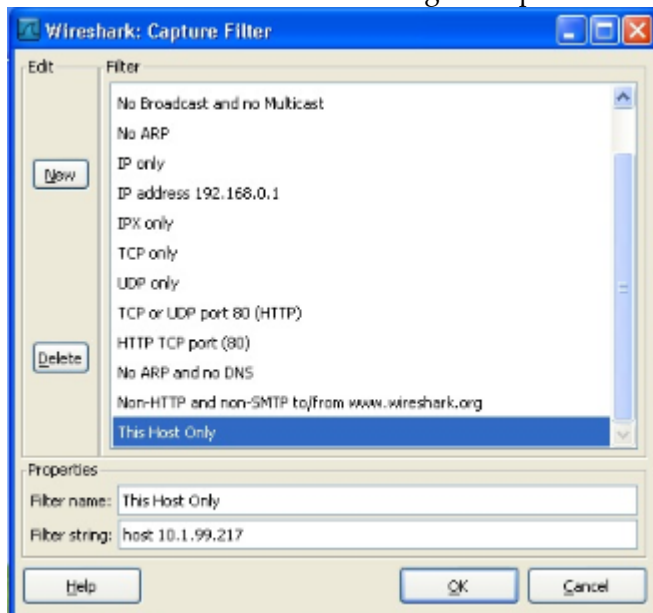
Reply from 10.1.99.117: bytes=32 time<1ms TTL=128
Reply from 10.1.99.117: bytes=32 time<1ms TTL=128
Reply from 10.1.99.117: bytes=32 time<1ms TTL=128
Reply from 10.1.99.117: bytes=32 time<1ms TTL=128

Ping statistics for 10.1.99.117:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\hacker>
```

Question 1.2

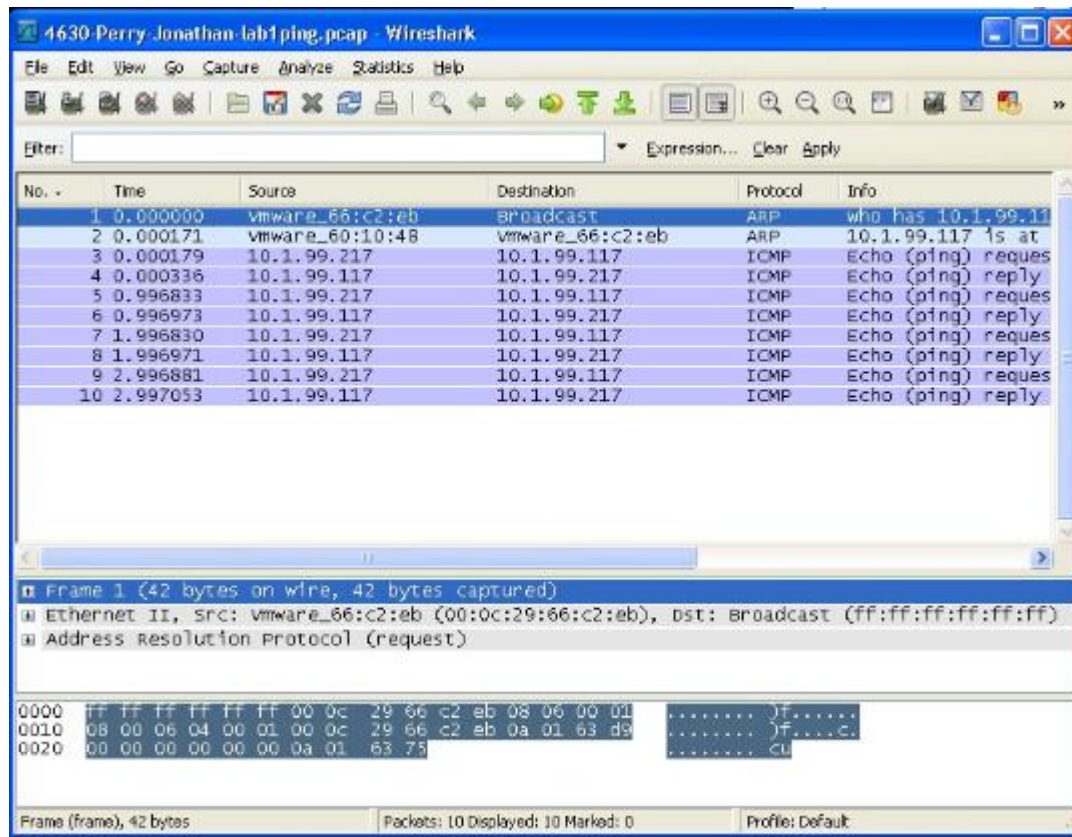
1.2.1. Attach a screen shot showing the capture filter you created.



1.2.2. How many packets were used by the Address Resolution Protocol?

Two packet were used by Address Resolution Protocol.

1.2.3. Attach a screen shot showing the result of applying the display filter.



1.2.4. How many packets were used by ICMP?

8 packets were used by ICMP.

1.2.5. How did the ping host know the pinged host's MAC address?

Because the ping host used a process called ARP, where it broadcasted "who has 10.1.99.117?", and 10.1.99.117 responded with its MAC address.

1.2.6. Which kind of ICMP message does a ping request use?

For the ping request, ICMP used a type: 8 (echo(ping) request).

1.2.7. Which kind of ICMP message does a ping reply use?

For the ping reply, ICMP used a type: 0 (echo(ping) reply).

Question 1.3

1.3.1. How many open ports did Nmap detect?

Nmap appears to have found 9 open ports.

1.3.2. What are the open ports? What are the services running on those ports?

The open ports appear to be 21, 80, 135, 139, 445, 1025, 1026, 1723, 3306, 8009, and 8080. The services running are ftp, http, msrpc, netbios-ssn, NFS-or-IIS, LSA-or-nterm, pptp, mysql, and http-proxy.

1.3.3. For the rest of the ports scanned, what was the status reported by Nmap?

Nmap shows that there are 991 filtered ports not shown.

Question 1.4

Note: There may be more than one set of packets that are used to scan a port. You only need to analyze one set.

1.4.1. Analyze the SEQ and ACK numbers and the control bits. When answering these questions, if a control bit is not on or SEQ/ACK number is not present, say so. In other words, that I ask about a particular bit or number does not mean that it must be on or present.

(a) Find the packet with the SYN bit turned on. Are there any other control bits on in this packet? What is the purpose of this packet?

There are no other control bits on in this packet, the point of this packet is for the XP machine to establish the connection (handshake) to the server.

(b) What is the SEQ number of the packet you identified in (a)? ACK number?

The SEQ number of the packet identified in (a) is 173488027, there is no ACK number because you have just sent an initial packet. The ACK control bit comes into play when responding to each other's packet.

(c) Find the packet with the SYN/ACK bits turned on. What is the purpose of this packet?

The purpose of this packet is to show that the server has obtained the packet from using forward acknowledgement, and for the server to establish its initial SEQ number.

(d) What are the SEQ number and ACK number of the packet you identified in (c)? How are they related to the number(s) you found in (b)?

SEQ = 2096205802, ACK = 173488028. The ACK number is related to the initial SEQ number identified in (b), because the server has responded with the initial SEQ number of the attacker XP machine but added 1. This lets the XP Machine know that the server has gotten the packet. The SEQ is unrelated to the numbers found in (b), because this is the server's initial SEQ number.

(e) Find the third packet that is related to the above two. Which control bit(s) are on in this packet? What is the purpose of this packet?

Only the ACK control bit is on for this packet, the XP machine is just responding back. The purpose of this packet is to let the server know it has received its previous packet and to proceed on.

(f) What are the SEQ number and ACK number of the packet you identified in (e)? How are they related to the number(s) you found in (d)?

The SEQ number of this packet is 173488028, and the ACK number of this packet is 2096205803. This packet is related to the previous packet because the XP machine has acknowledged the server's initial SEQ by adding 1 in its ACK number. The SEQ is related to part (d) because in the 2nd segment the server acknowledged the XP machine's previous SEQ number by adding 1, which is the next segment the server is expecting from the XP machine (forward acknowledgement).

1.4.2. Has a three-way handshake been established between the two machines?

A three-way handshake has been established between the two machines. For a three-way handshake to be established between the two machines, the SYN bit has to be on in the 1st packet, the SYN/ACK bit has to be on in the 2nd packet, and the 3rd packet has to have the ACK bit on.