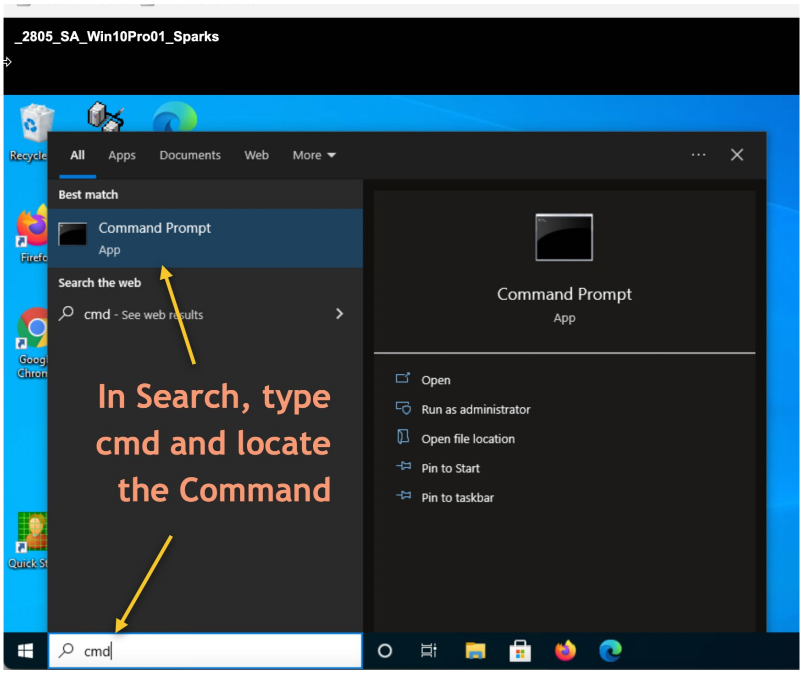
Command Line Lab

Jones, Annie
April 19, 2023

Background:

Many tools used by network administrators to manage a network are also used in cybersecurity by the team charged to protect the network as well as attackers who are attempting to gain access to the network. This lab is designed to introduce the typical command line tools used in cybersecurity to discover information about a network.

Open a browser and navigate to https://infoadc.mccinfo.net. Log into the VM Environment using your MCC credentials and navigate to the VM you have been assigned by your instructor. Log into the VM as admin using the password of Password1. As shown in the graphic, after logging in, open a command line and complete the following parts.



In Search, type cmd and locate the Command

Part 1: ipconfig is used by administrators to discover information about the network interface of a computer system.

1. In the command line, type ipconfig with no parameters.
   a. What information does this display?
      i. Retrieves Basic TCP/IP Network Information (IP, subnet mask, gateway)

   Windows Ip Configuration
   Ethernet adapter Ethernet0 2:
   Connection-specific DNS Suffix . : mccinfo.net
   Link-local IPv6 Adress…..: fe80::411b:ee56:9533:7e96%5
   IPv4 Adress……….: 10.210.17.0

Subnet Mask……..: 255.255.240.0
Default Gateway………: 10.210.31.254

2. Type cls to clear the screen. Type “ipconfig /all” and press enter.
   a. How does the output change?
      i. Retrieves All TCP/IP Network Information (MAC address, adapter description, DHCP details)

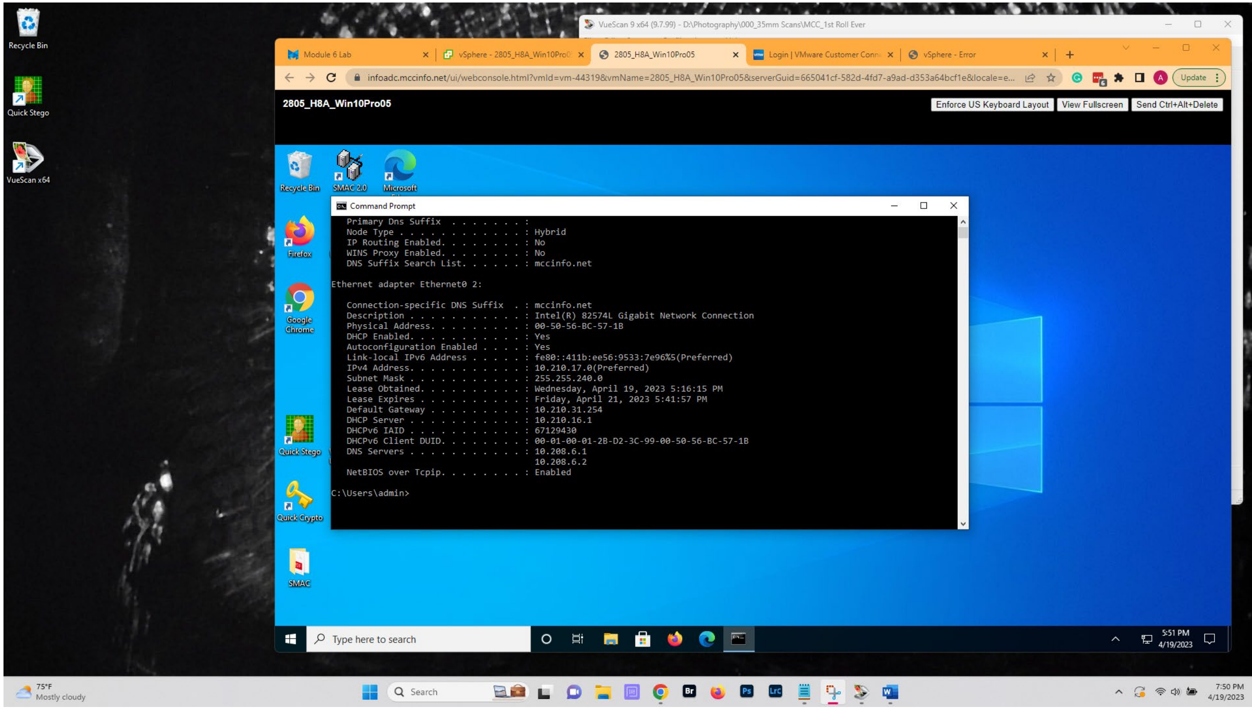
   b. What does it mean if the DHCP is set to yes?
      i. Yes means the device receives its IP address configuration from a DHCP server

   c. What is the subnet mask?

      i. 255.255.240.0

   d. What is your computer’s IP address?
      i. 10.210.17.0(preferred)

   e. **Copy and Paste a capture of the screen below this line (NOTE: your machine name must be visible in the capture.)**

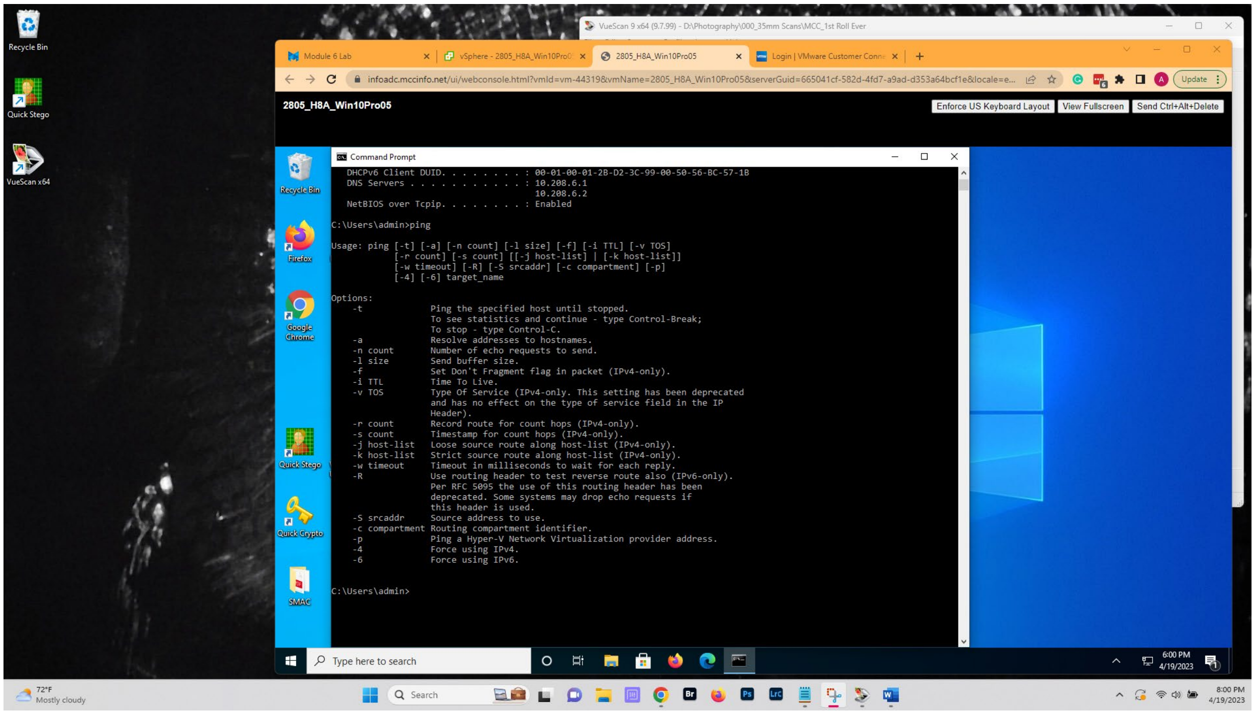


```
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : mccinfo.net

Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . : mccinfo.net
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-50-56-BC-57-1B
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::411b:ee56:9533:7e96%5(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.210.17.0(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Lease Obtained. . . . . . . . . . : Wednesday, April 19, 2023 5:16:15 PM
   Lease Expires . . . . . . . . . . : Friday, April 21, 2023 5:41:57 PM
   Default Gateway . . . . . . . . . : 10.210.31.254
   DHCP Server . . . . . . . . . . . : 10.210.16.1
   DHCPv6 IAID . . . . . . . . . . . : 67129430
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2B-D2-3C-99-00-50-56-BC-57-1B
   DNS Servers . . . . . . . . . . . : 10.208.6.1
                                       10.208.6.2
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Users\admin>
```

Command Line Lab

Part 2: The PING (Packet Internet Groper) is a command used to determine if a computer or network device is online and communicating.

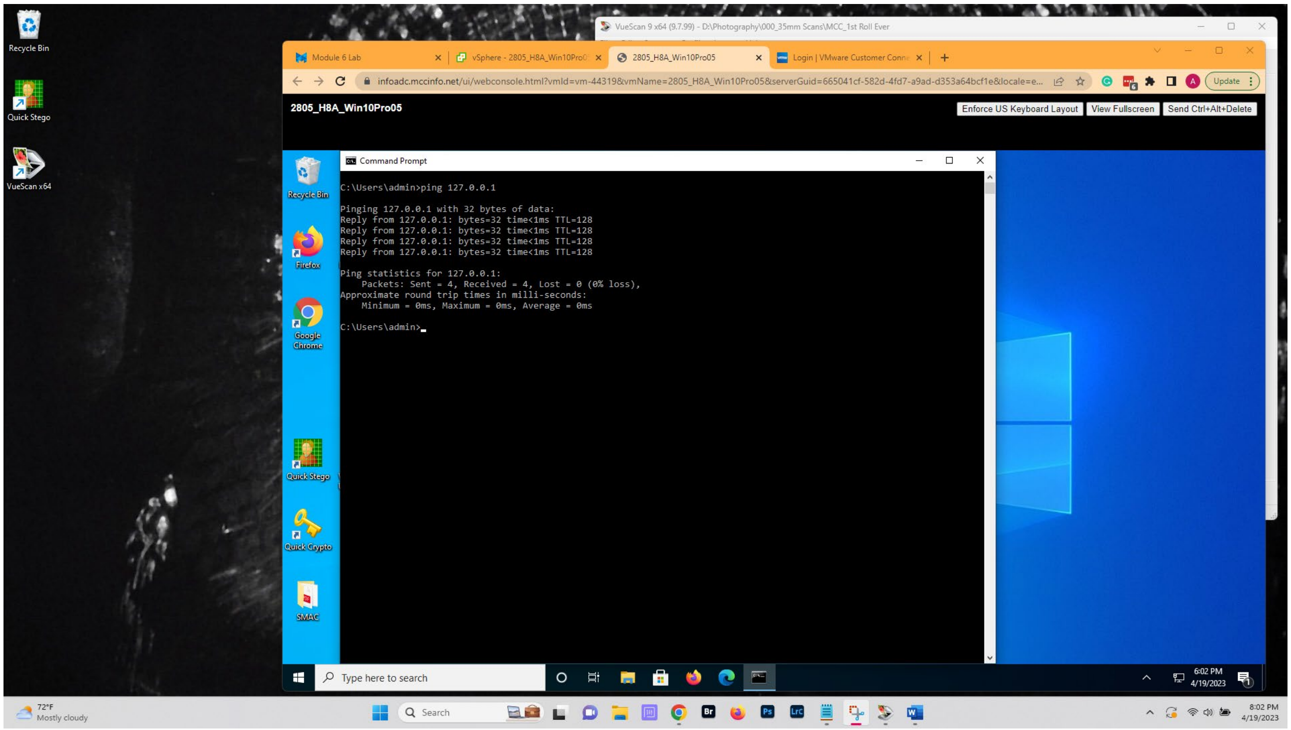
1. In the command line type the command ping with no parameters. **Copy and Paste a capture of the screen below this line (NOTE: your machine name must be visible in the capture.)**


infoadc.mccinfo.net/ui/webconsole.html?vmId=vm-44319&vmName=2805_H8A_Win10Pro05&serverGuid=665041cf-582d-4fd7-a9ad-d353a64bcf1e&locale=e...
2805_H8A_Win10Pro05
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Command Prompt
Type here to search

```
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2B-D2-3C-99-00-50-56-BC-57-1B
   DNS Servers . . . . . . . . . . . : 10.208.6.1
                                       10.208.6.2
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Users\admin>ping

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
            [-4] [-6] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet (IPv4-only).
    -i TTL         Time To Live.
    -v TOS         Type Of Service (IPv4-only. This setting has been deprecated
                   and has no effect on the type of service field in the IP
                   Header).
    -r count       Record route for count hops (IPv4-only).
    -s count       Timestamp for count hops (IPv4-only).
    -j host-list   Loose source route along host-list (IPv4-only).
    -k host-list   Strict source route along host-list (IPv4-only).
    -w timeout     Timeout in milliseconds to wait for each reply.
    -R             Use routing header to test reverse route also (IPv6-only).
                   Per RFC 5095 the use of this routing header has been
                   deprecated. Some systems may drop echo requests if
                   this header is used.
    -S srcaddr     Source address to use.
    -c compartment Routing compartment identifier.
    -p             Ping a Hyper-V Network Virtualization provider address.
    -4             Force using IPv4.
    -6             Force using IPv6.


C:\Users\admin>
```

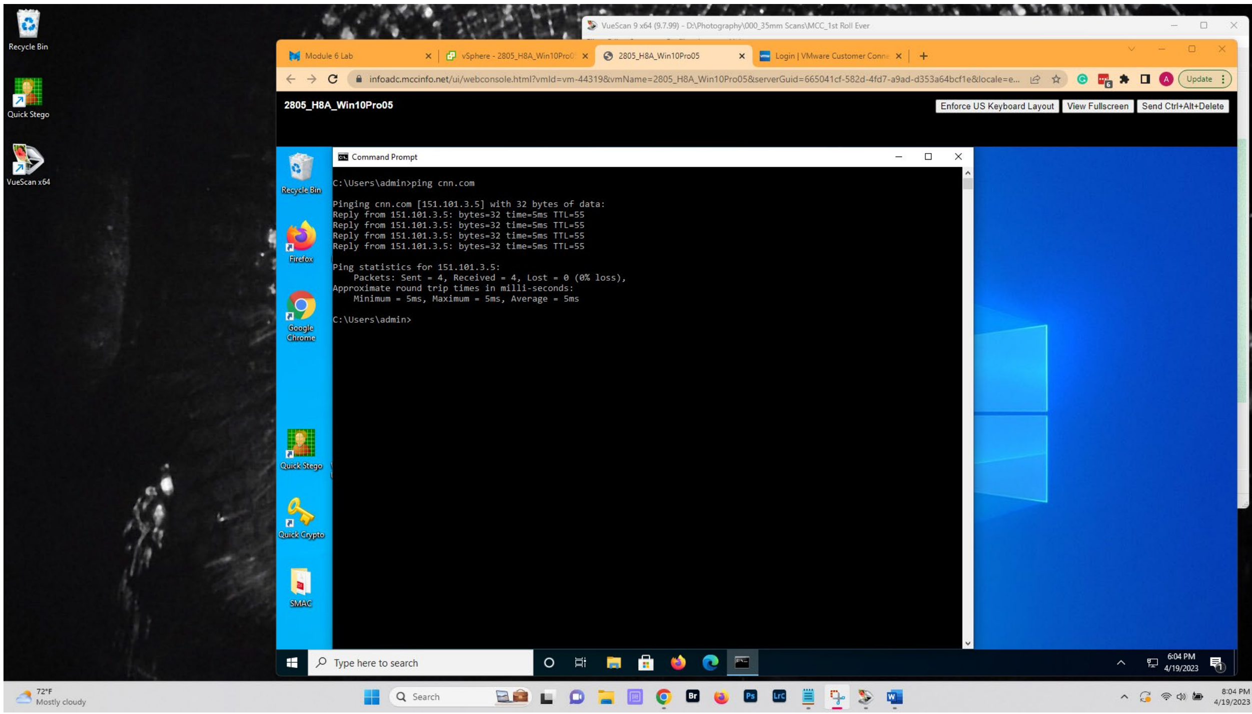
2. Type cls in the command line to clear the screen. Then, type the following command: ping 127.0.0.1. **Copy and Paste a capture of the screen below this line (NOTE: your machine name must be visible in the capture.)**

Command Line Lab



```
C:\Users\admin>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\admin>
```

3. Type cls to clear the screen. Type ping cnn.com and press enter.
   a. What are the IP addresses listed?
      i. 151.101.3.5
   b. What does the information returned tell you?
      i. This tells me the connectivity to cnn.com is 5ms after testing it 4 times and averaging the connectivity time out
   c. **Copy and paste a capture of the screen below this line (NOTE: your machine name must be visible in the capture.)**

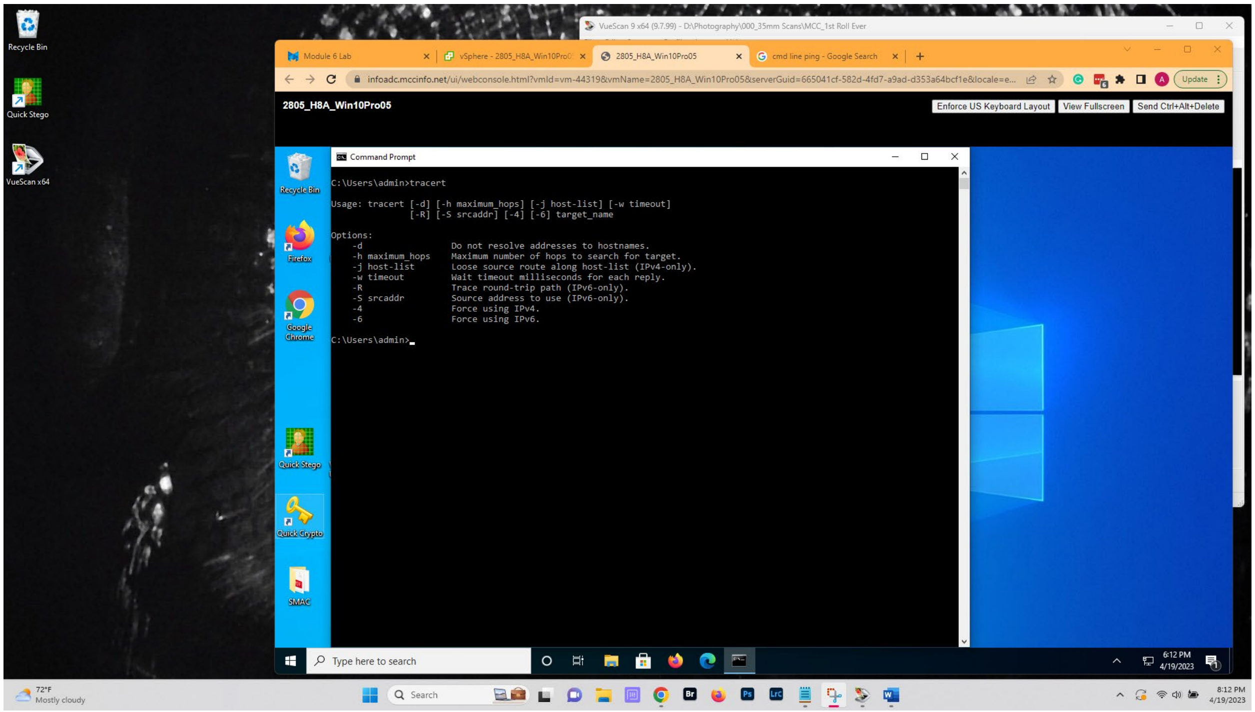


```
C:\Users\admin>ping cnn.com

Pinging cnn.com [151.101.3.5] with 32 bytes of data:
Reply from 151.101.3.5: bytes=32 time=5ms TTL=55
Reply from 151.101.3.5: bytes=32 time=5ms TTL=55
Reply from 151.101.3.5: bytes=32 time=5ms TTL=55
Reply from 151.101.3.5: bytes=32 time=5ms TTL=55

Ping statistics for 151.101.3.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 5ms, Average = 5ms

C:\Users\admin>
```

Part 3: Tracert is a command used to determine the path data takes between two points. From a cybersecurity standpoint, an attacker can discover what routers or Layer 3 Switches the data travels through.

1. Type cls to clear the screen. Type tracert with no parameteers. **Copy and Paste a capture of the screen below this line (NOTE: your machine name must be visible in the capture.)**

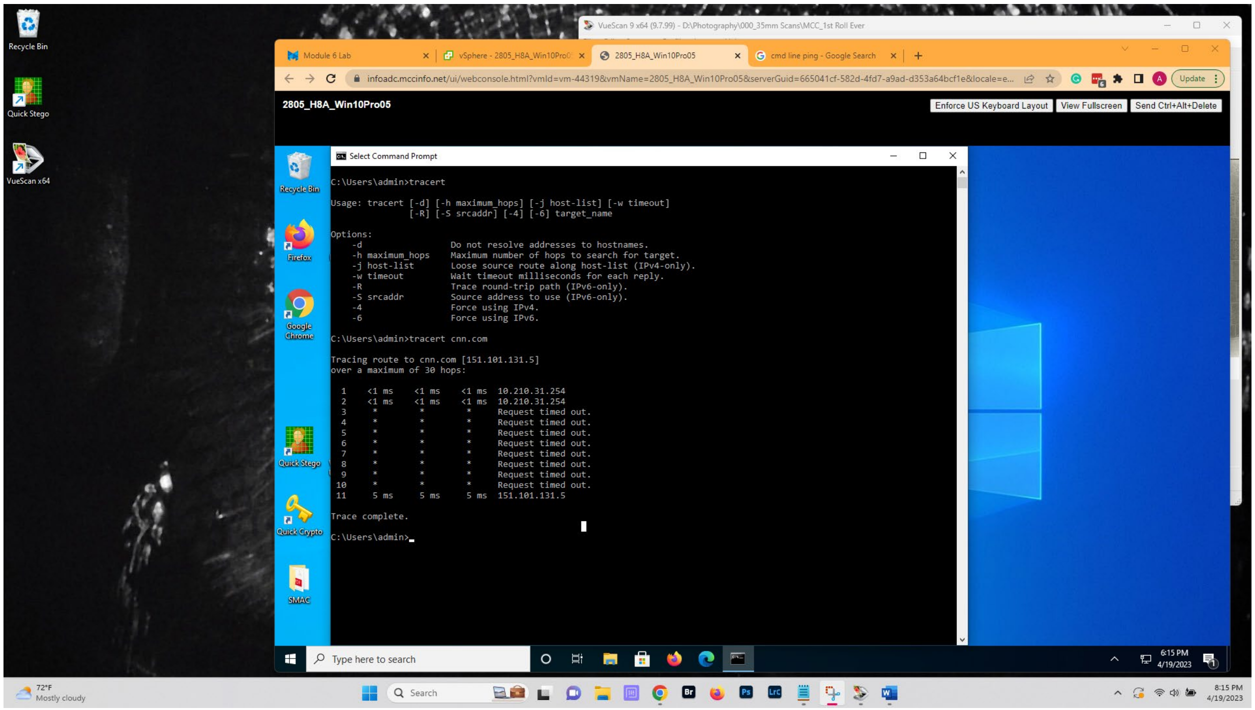
Command Line Lab



```
C:\Users\admin>tracert

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -d                 Do not resolve addresses to hostnames.
    -h maximum_hops    Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list (IPv4-only).
    -w timeout         Wait timeout milliseconds for each reply.
    -R                 Trace round-trip path (IPv6-only).
    -S srcaddr         Source address to use (IPv6-only).
    -4                 Force using IPv4.
    -6                 Force using IPv6.

C:\Users\admin>
```

2. Type cls to clear the screen. Type “tracert cnn.com” and press enter.
    a. What are the public IP addresses?
        i. 151.101.131.5
    b. What are the private IP addresses?
        i. 10.210.31.254

    c. **Copy and Paste a capture of the screen below this line (NOTE: your machine name must be visible in the capture.)**

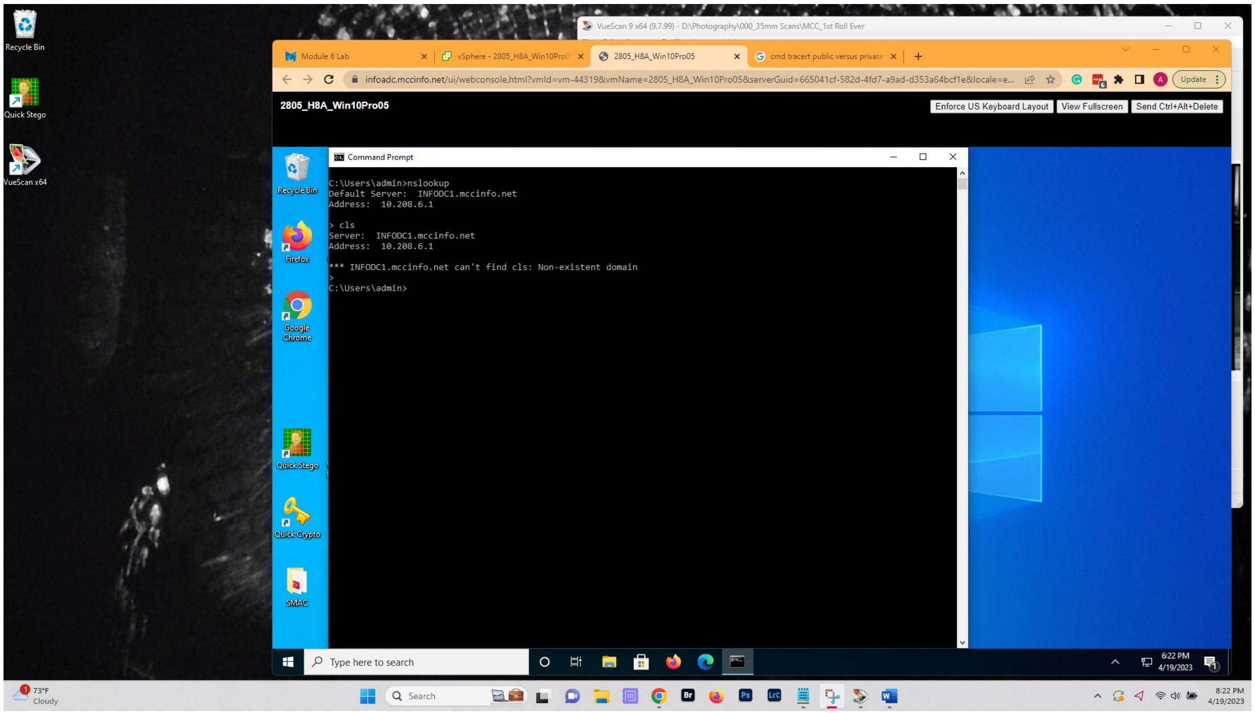


```
C:\Users\admin>tracert

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -d                 Do not resolve addresses to hostnames.
    -h maximum_hops    Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list (IPv4-only).
    -w timeout         Wait timeout milliseconds for each reply.
    -R                 Trace round-trip path (IPv6-only).
    -S srcaddr         Source address to use (IPv6-only).
    -4                 Force using IPv4.
    -6                 Force using IPv6.

C:\Users\admin>tracert cnn.com

Tracing route to cnn.com [151.101.131.5]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  10.210.31.254
  2    <1 ms    <1 ms    <1 ms  10.210.31.254
  3     *        *        *     Request timed out.
  4     *        *        *     Request timed out.
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     5 ms     5 ms     5 ms  151.101.131.5

Trace complete.

C:\Users\admin>_
```

Part 4: NSlookup is another command used to lookup DNS (Domain Name System) information such as IP address.
Cls

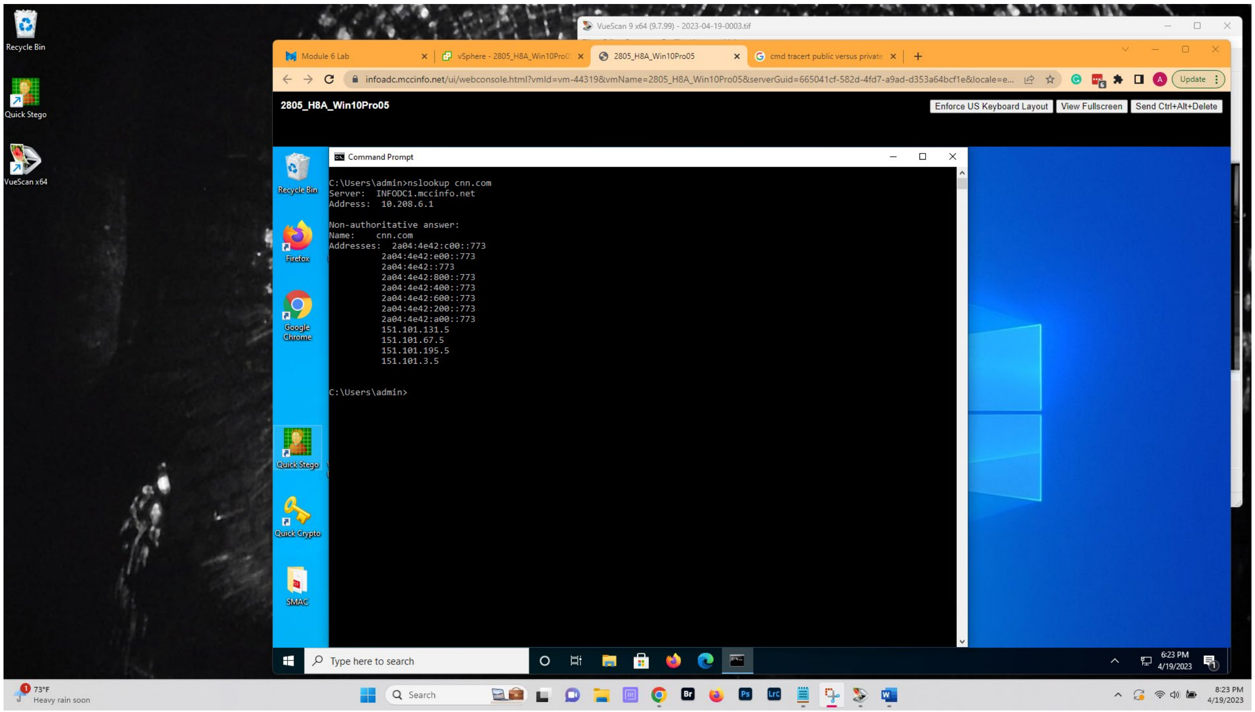
1. Type cls to clear the screen. Type nslookup with no parameters.
    a. What is your default server? Use the fully qualified domain name. Press Ctrl+C to break the command execution.
        i. INFODC1.mccinfo.net
    b. What is the IP address?
        i. 10.208.61
    c. **Copy and Paste a capture of the screen below this line (NOTE: your machine name must be visible in the capture.)**

Command Line Lab


VueScan 9 x64 (9.7.99) - D:\Photography\000_35mm Scans\MCC_1st Roll Ever
Module 6 Lab
vSphere - 2805_H8A_Win10Pro0
2805_H8A_Win10Pro05
cmd tracert public versus private
infoadc.mccinfo.net/ui/webconsole.html?vmId=vm-44319&vmName=2805_H8A_Win10Pro05&serverGuid=665041cf-582d-4fd7-a9ad-d353a64bcf1e&locale=e...
2805_H8A_Win10Pro05
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Command Prompt
Recycle Bin
Quick Stego
VueScan x64
Firefox
Google Chrome
Quick Crypto
SMAC
Type here to search
6:22 PM
4/19/2023
73°F
Cloudy
Search
8:22 PM
4/19/2023

```
C:\Users\admin>nslookup
Default Server:  INFODC1.mccinfo.net
Address:  10.208.6.1

> cls
Server:  INFODC1.mccinfo.net
Address:  10.208.6.1

*** INFODC1.mccinfo.net can't find cls: Non-existent domain
>
C:\Users\admin>
```

2. Type cls to clear the screen. Type “nslookup cnn.com” and press enter.
   a. How many IP addresses do they have assigned?
      i. 12
   b. **Copy and Paste a capture of the screen below this line (NOTE: your machine name must be visible in the capture.)**



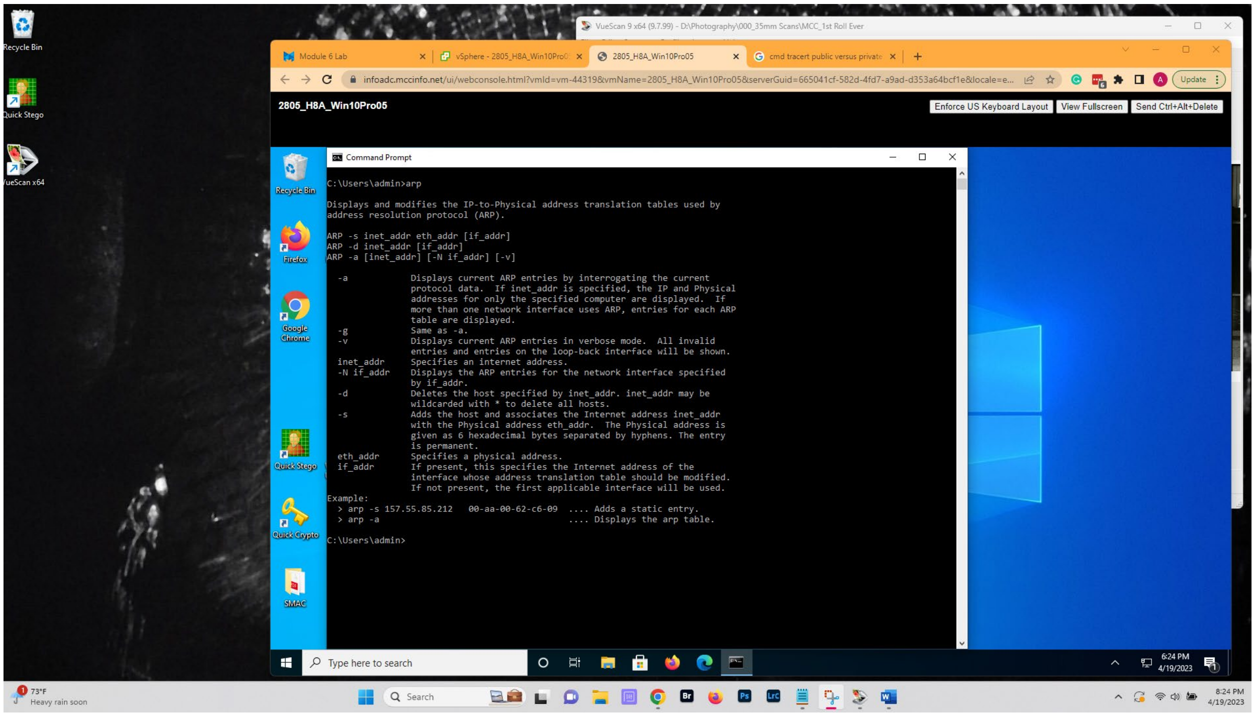
infoadc.mccinfo.net/ui/webconsole.html?vmId=vm-44319&vmName=2805_H8A_Win10Pro05&serverGuid=665041cf-582d-4fd7-a9ad-d353a64bcf1e&locale=e...
2805_H8A_Win10Pro05
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Command Prompt

```
C:\Users\admin>nslookup cnn.com
Server:  INFODC1.mccinfo.net
Address:  10.208.6.1

Non-authoritative answer:
Name:    cnn.com
Addresses:  2a04:4e42:c00::773
          2a04:4e42:e00::773
          2a04:4e42::773
          2a04:4e42:800::773
          2a04:4e42:400::773
          2a04:4e42:600::773
          2a04:4e42:200::773
          2a04:4e42:a00::773
          151.101.131.5
          151.101.67.5
          151.101.195.5
          151.101.3.5


C:\Users\admin>
```

Part 5: ARP (Address Resolution Protocol) is used to displays the ARP table that shows the MAC (Media Access Control) address mapped to the IP address. Additionally, it can show if the address is assigned dynamically or static.

1. Type cls to clear the screen. Type arp with no parameters and press enter. **Copy and Paste a capture of the screen below this line (NOTE: your machine name must be visible in the capture.)**

Command Line Lab



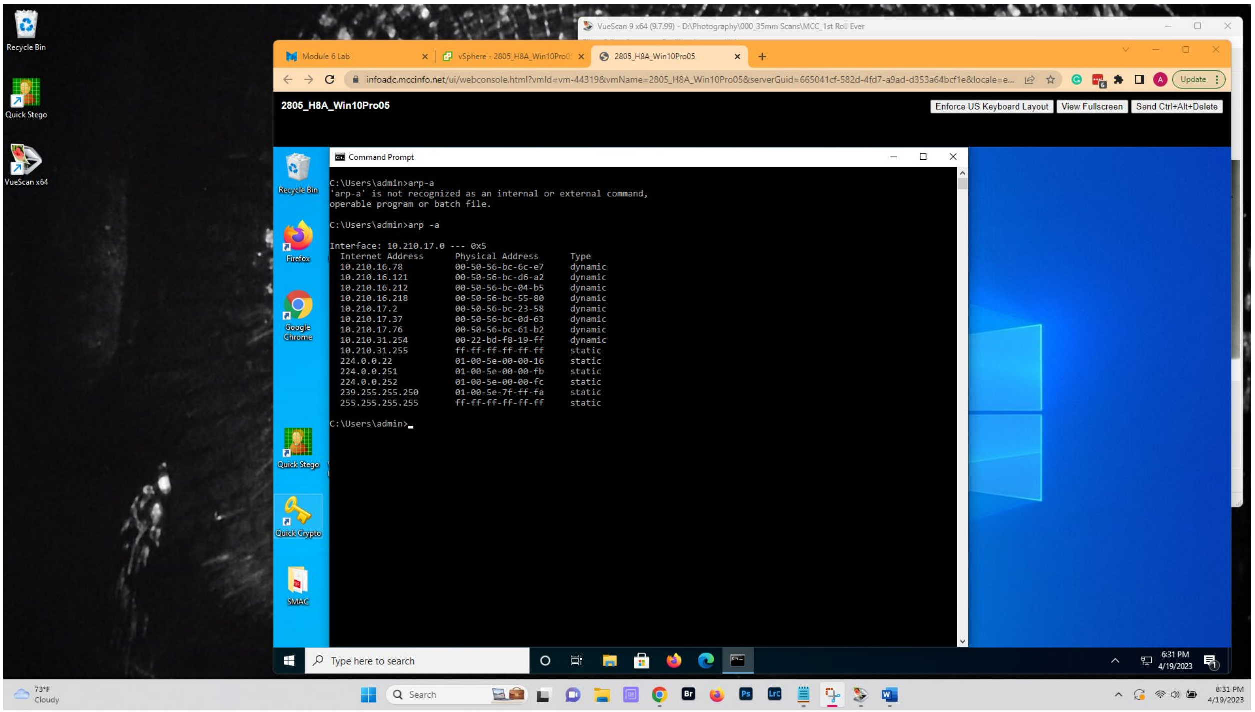
```
C:\Users\admin>arp

Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

  -a            Displays current ARP entries by interrogating the current
                protocol data.  If inet_addr is specified, the IP and Physical
                addresses for only the specified computer are displayed.  If
                more than one network interface uses ARP, entries for each ARP
                table are displayed.
  -g            Same as -a.
  -v            Displays current ARP entries in verbose mode.  All invalid
                entries and entries on the loop-back interface will be shown.
  inet_addr     Specifies an internet address.
  -N if_addr    Displays the ARP entries for the network interface specified
                by if_addr.
  -d            Deletes the host specified by inet_addr. inet_addr may be
                wildcarded with * to delete all hosts.
  -s            Adds the host and associates the Internet address inet_addr
                with the Physical address eth_addr.  The Physical address is
                given as 6 hexadecimal bytes separated by hyphens. The entry
                is permanent.
  eth_addr      Specifies a physical address.
  if_addr       If present, this specifies the Internet address of the
                interface whose address translation table should be modified.
                If not present, the first applicable interface will be used.
Example:
  > arp -s 157.55.85.212   00-aa-00-62-c6-09  .... Adds a static entry.
  > arp -a                                    .... Displays the arp table.

C:\Users\admin>
```

2. Type cls to clear the screen. Type “arp -a” and press enter.
   a. What are the columns used?
      i. Internet Address, Physical Address, Type

   b. What is mean by the physical address?
      i. The MAC address is the physical address that identifies each device on a network using 12 hexidecimal digits used for global identification.

   c. What does it mean on the type as dynamic and static?
      i. Static addresses are manually configured and do not age out. The device creates dynamic addresses from the ARP packets it receives. Dynamic addresses age out after a configured time.

   d. **Copy and Paste a capture of the screen below this line (NOTE: your machine name must be visible in the capture.)**


VueScan 9 x64 (9.7.99) - D:\Photography\000_35mm Scans\MCC_1st Roll Ever
Module 6 Lab
vSphere - 2805_H8A_Win10Pro05
2805_H8A_Win10Pro05
infoadc.mccinfo.net/ui/webconsole.html?vmId=vm-44319&vmName=2805_H8A_Win10Pro05&serverGuid=665041cf-582d-4fd7-a9ad-d353a64bcf1e&locale=e...
Update
2805_H8A_Win10Pro05
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Command Prompt
Recycle Bin
Quick Stego
VueScan x64
Firefox
Google Chrome
Quick Crypto
SMAC
Type here to search
6:31 PM
4/19/2023
73°F
Cloudy
Search
8:31 PM
4/19/2023

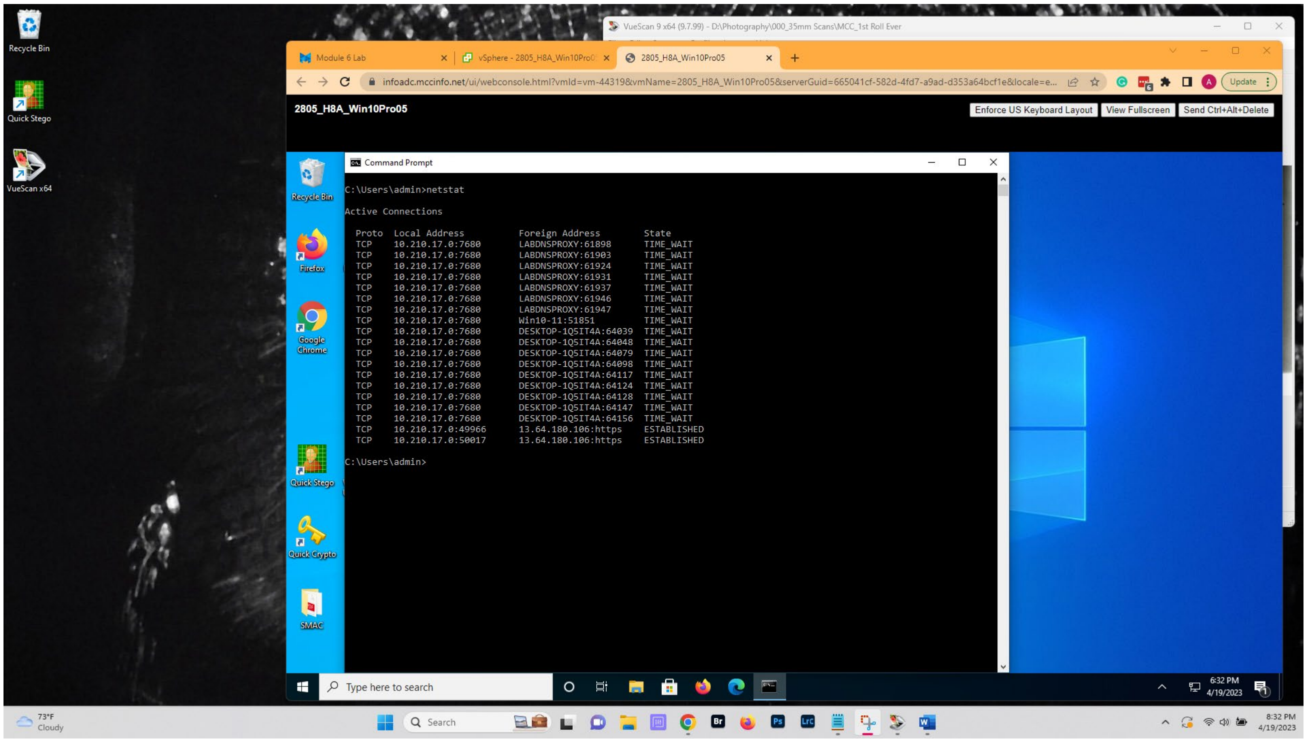
```
C:\Users\admin>arp-a
'arp-a' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\admin>arp -a

Interface: 10.210.17.0 --- 0x5
  Internet Address      Physical Address      Type
  10.210.16.78          00-50-56-bc-6c-e7     dynamic
  10.210.16.121         00-50-56-bc-d6-a2     dynamic
  10.210.16.212         00-50-56-bc-04-b5     dynamic
  10.210.16.218         00-50-56-bc-55-80     dynamic
  10.210.17.2           00-50-56-bc-23-58     dynamic
  10.210.17.37          00-50-56-bc-0d-63     dynamic
  10.210.17.76          00-50-56-bc-61-b2     dynamic
  10.210.31.254         00-22-bd-f8-19-ff     dynamic
  10.210.31.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\admin>_
```

Part 6: Netstat is used to display connections on protocols at Layer 4 of the OSI (Open Systems Interconnection) model.

1. Type cls to clear the screen. Type netstat with no parameters.
   a. How many connections are displayed?
      i. 19

   b. What protocol is displayed?
      i. TCP

   c. **Copy and Paste a capture of the screen below this line (NOTE: your machine name must be visible in the capture.)**


Recycle Bin
Quick Stego
VueScan x64
VueScan 9 x64 (9.7.99) - D:\Photography\000_35mm Scans\MCC_1st Roll Ever
Module 6 Lab
vSphere - 2805_H8A_Win10Pro05
2805_H8A_Win10Pro05
infoadc.mccinfo.net/ui/webconsole.html?vmId=vm-44319&vmName=2805_H8A_Win10Pro05&serverGuid=665041cf-582d-4fd7-a9ad-d353a64bcf1e&locale=e...
Update
2805_H8A_Win10Pro05
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Command Prompt
Firefox
Google Chrome
Quick Crypto
SMAC
Type here to search
6:32 PM
4/19/2023
73°F
Cloudy
Search
8:32 PM
4/19/2023

```
C:\Users\admin>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    10.210.17.0:7680       LABDNSPROXY:61898      TIME_WAIT
  TCP    10.210.17.0:7680       LABDNSPROXY:61903      TIME_WAIT
  TCP    10.210.17.0:7680       LABDNSPROXY:61924      TIME_WAIT
  TCP    10.210.17.0:7680       LABDNSPROXY:61931      TIME_WAIT
  TCP    10.210.17.0:7680       LABDNSPROXY:61937      TIME_WAIT
  TCP    10.210.17.0:7680       LABDNSPROXY:61946      TIME_WAIT
  TCP    10.210.17.0:7680       LABDNSPROXY:61947      TIME_WAIT
  TCP    10.210.17.0:7680       Win10-11:51851         TIME_WAIT
  TCP    10.210.17.0:7680       DESKTOP-1Q5IT4A:64039  TIME_WAIT
  TCP    10.210.17.0:7680       DESKTOP-1Q5IT4A:64048  TIME_WAIT
  TCP    10.210.17.0:7680       DESKTOP-1Q5IT4A:64079  TIME_WAIT
  TCP    10.210.17.0:7680       DESKTOP-1Q5IT4A:64098  TIME_WAIT
  TCP    10.210.17.0:7680       DESKTOP-1Q5IT4A:64117  TIME_WAIT
  TCP    10.210.17.0:7680       DESKTOP-1Q5IT4A:64124  TIME_WAIT
  TCP    10.210.17.0:7680       DESKTOP-1Q5IT4A:64128  TIME_WAIT
  TCP    10.210.17.0:7680       DESKTOP-1Q5IT4A:64147  TIME_WAIT
  TCP    10.210.17.0:7680       DESKTOP-1Q5IT4A:64156  TIME_WAIT
  TCP    10.210.17.0:49966      13.64.180.106:https    ESTABLISHED
  TCP    10.210.17.0:50017      13.64.180.106:https    ESTABLISHED

C:\Users\admin>
```

2. Type cls to clear the screen. Type “netstat -a” and press enter.

    a. How does the output change?

        i. Netstat -a displays all TCP connections including LISTENING and also UDP ports

    b. What protocols are displayed?

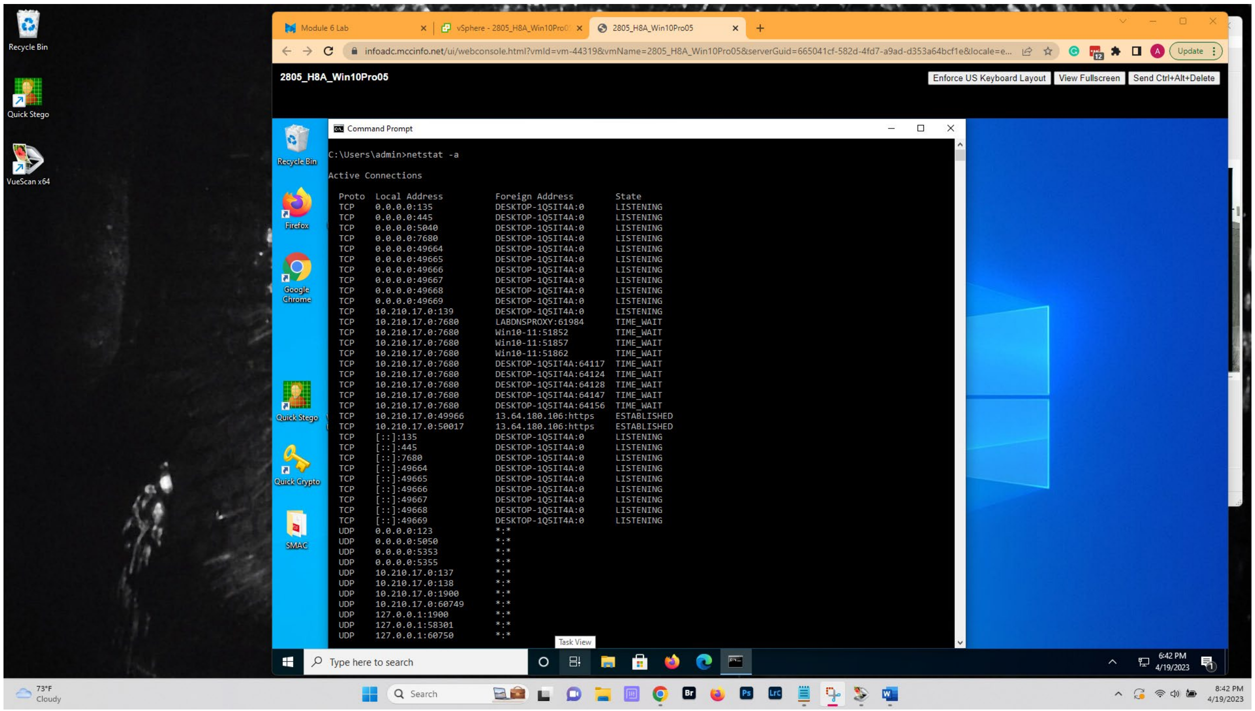
        i. TCP & UDP

    c. What are the two protocols used for?

        i. TCP is a connection-oriented protocol and UDB is a connectionless protocol. UDB is used for time-sensitive applications like DNS lookups, games, videos. TCP is for non0time sensitive data transmissions like FTP & SSH

    d. **Copy and Paste a capture of the screen below this line (NOTE: your machine name must be visible in the capture.)**

Command Line Lab



```
C:\Users\admin>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            DESKTOP-1Q5IT4A:0      LISTENING
  TCP    0.0.0.0:445            DESKTOP-1Q5IT4A:0      LISTENING
  TCP    0.0.0.0:5040           DESKTOP-1Q5IT4A:0      LISTENING
  TCP    0.0.0.0:7680           DESKTOP-1Q5IT4A:0      LISTENING
  TCP    0.0.0.0:49664          DESKTOP-1Q5IT4A:0      LISTENING
  TCP    0.0.0.0:49665          DESKTOP-1Q5IT4A:0      LISTENING
  TCP    0.0.0.0:49666          DESKTOP-1Q5IT4A:0      LISTENING
  TCP    0.0.0.0:49667          DESKTOP-1Q5IT4A:0      LISTENING
  TCP    0.0.0.0:49668          DESKTOP-1Q5IT4A:0      LISTENING
  TCP    0.0.0.0:49669          DESKTOP-1Q5IT4A:0      LISTENING
  TCP    10.210.17.0:139        DESKTOP-1Q5IT4A:0      LISTENING
  TCP    10.210.17.0:7680       LABDNSPROXY:61984      TIME_WAIT
  TCP    10.210.17.0:7680       Win10-11:51852         TIME_WAIT
  TCP    10.210.17.0:7680       Win10-11:51857         TIME_WAIT
  TCP    10.210.17.0:7680       Win10-11:51862         TIME_WAIT
  TCP    10.210.17.0:7680       DESKTOP-1Q5IT4A:64117  TIME_WAIT
  TCP    10.210.17.0:7680       DESKTOP-1Q5IT4A:64124  TIME_WAIT
  TCP    10.210.17.0:7680       DESKTOP-1Q5IT4A:64128  TIME_WAIT
  TCP    10.210.17.0:7680       DESKTOP-1Q5IT4A:64147  TIME_WAIT
  TCP    10.210.17.0:7680       DESKTOP-1Q5IT4A:64156  TIME_WAIT
  TCP    10.210.17.0:49966      13.64.180.106:https    ESTABLISHED
  TCP    10.210.17.0:50017      13.64.180.106:https    ESTABLISHED
  TCP    [::]:135               DESKTOP-1Q5IT4A:0      LISTENING
  TCP    [::]:445               DESKTOP-1Q5IT4A:0      LISTENING
  TCP    [::]:7680              DESKTOP-1Q5IT4A:0      LISTENING
  TCP    [::]:49664             DESKTOP-1Q5IT4A:0      LISTENING
  TCP    [::]:49665             DESKTOP-1Q5IT4A:0      LISTENING
  TCP    [::]:49666             DESKTOP-1Q5IT4A:0      LISTENING
  TCP    [::]:49667             DESKTOP-1Q5IT4A:0      LISTENING
  TCP    [::]:49668             DESKTOP-1Q5IT4A:0      LISTENING
  TCP    [::]:49669             DESKTOP-1Q5IT4A:0      LISTENING
  UDP    0.0.0.0:123            *:*
  UDP    0.0.0.0:5050           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5355           *:*
  UDP    10.210.17.0:137        *:*
  UDP    10.210.17.0:138        *:*
  UDP    10.210.17.0:1900       *:*
  UDP    10.210.17.0:60749      *:*
  UDP    127.0.0.1:1900         *:*
  UDP    127.0.0.1:58301        *:*
  UDP    127.0.0.1:60750        *:*
```