**CSCE 629 Lab 2**

**Winter 2019**

**Scanning**

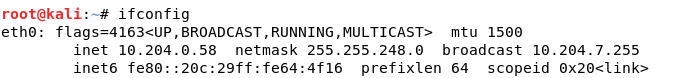
**Assigned: Lesson 5, 10 Jan**

**Due: Lesson 11, 22 Jan, 1400**

**Network Mapping**

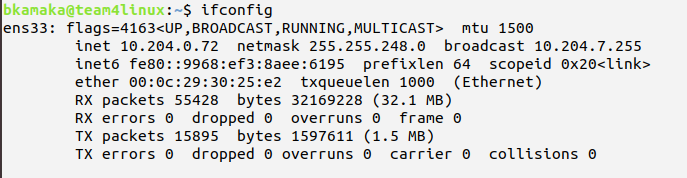
1. What is the IP address and host name of your machine? What is the IP address and host name of your partner’s machine?

Flack: **10.204.0.58/kali**



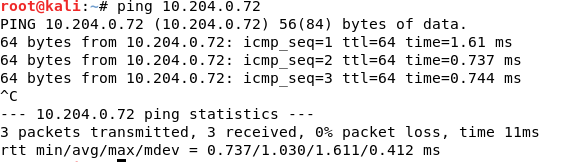


Kamaka: **10.204.0.72/team4linux**

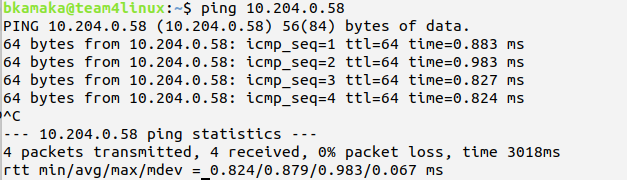


2. Using ping, determine if your partner’s workstation is up. Is your partner’s workstation up?

**Flack: Yes**

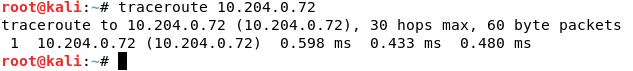


**Kamaka: Yes**

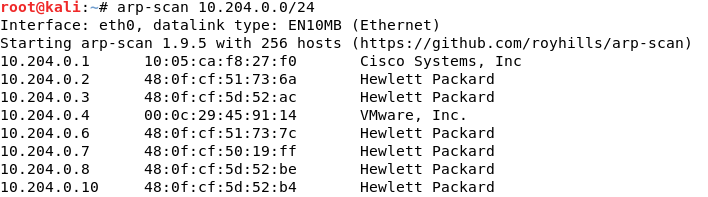


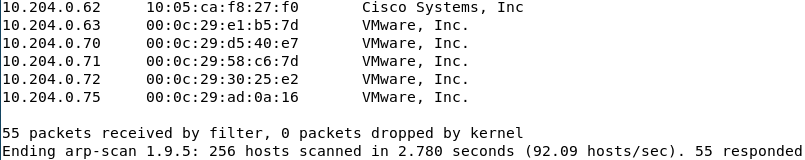
3. Using traceroute, determine the number of hops between your two machines. How many hops are there between the two computers?

**There is 1 hop between the two machines**



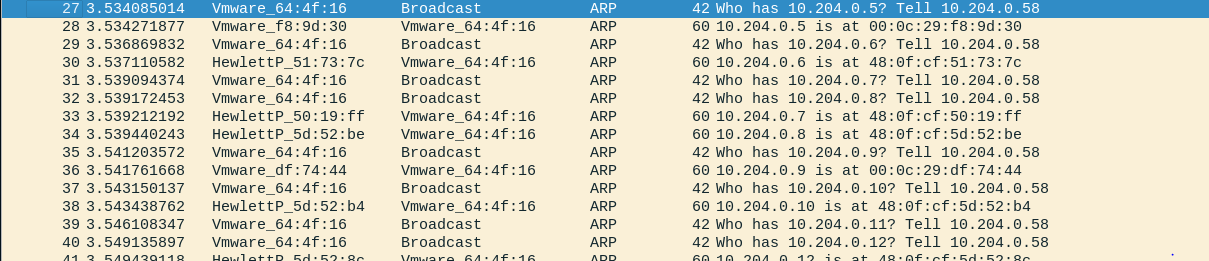
**Kamaka: Same. Screenshot left out because it was exactly the same, with different IP address. This makes sense as they are both one hop away from one another.**

4. Perform a network sweep using arp-scan to identify potential targets/IPs quickly. 

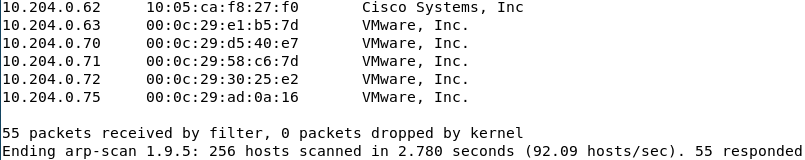


What type of packet is the tool sending? Provide a Wireshark screenshot showing some of the captured packets.

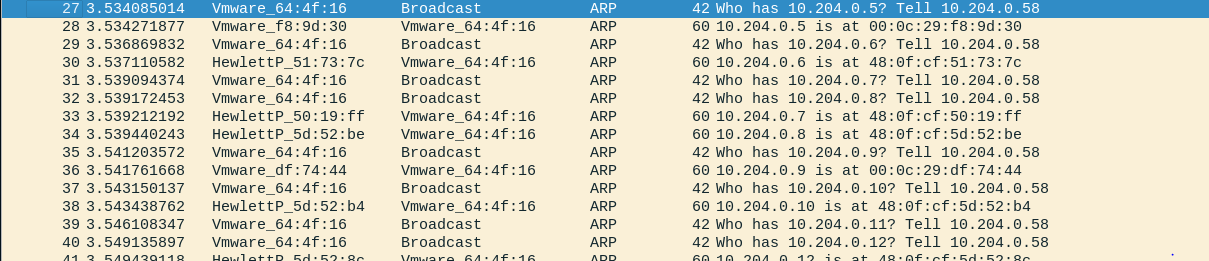
**Address Resolution Protocol (ARP) Packets:**



How many IPs did the tool discover? **55 machines**

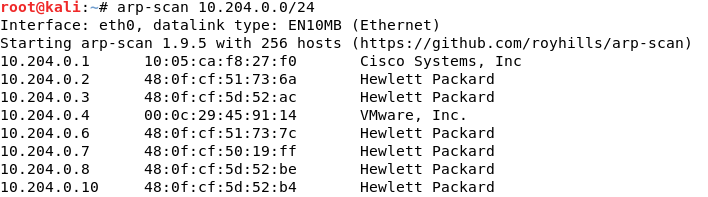


Did the tool scan sequentially? **Yes. You can see from the “who has 10.204.0.X” that the last number increases by 1 for each packet**



What are does the third column represent, and how is that information learned?

**"Vendor Details" relative to the NIC manufacturer, based on the MAC address on the interface that responded to the ARP packet.**



**Nmap**

You will use Wireshark to watch nmap as it performs its magic.

One person will be the target, and the other is the Blackhat. Your assignment is for the Blackhat to scan the target machine. The Blackhat starts nmap and Wireshark. The target starts Wireshark. Be prepared for 1000s of packets, and remember Wireshark can filter the data for you. J

5. Blackhat: Start Wireshark and perform a SYN scan using nmap or zenmap. Use aggressive timing and turn on verbose output. You may add other options as needed to provide the following information about the target. Using just the nmap results, answer the following questions; in other words, you cannot ask your partner for the name of his/her machine.

a. What nmap command did you use? Describe all options used and how they affect the scan.

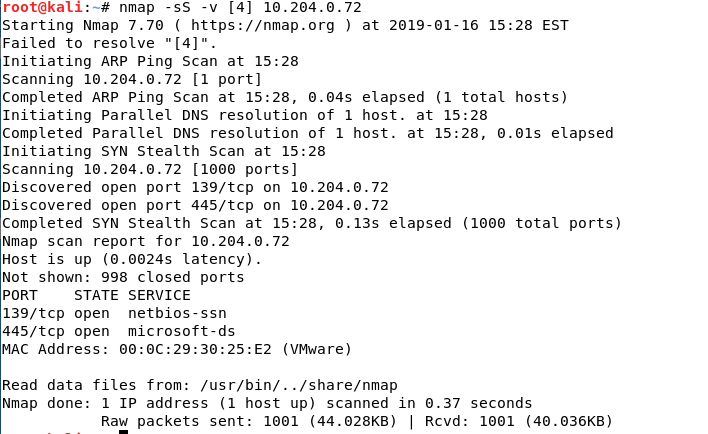
**“nmap -sS 10.204.0.72” (-sS specifies a SYN scan, the IP address is the target)**

**“nmap -sS -v [4] 20.204.0.72” (-v [<level>] tells Nmap how verbose to be. The higher the level the more information the scan will usually provide)**

**“****nmap -T5 -A 10.204.0.72” (This scan revealed the hostname; -T5 set the timing option to very fast; -A enabled OS detection, virus detection, script scanning, and traceroute)**

b. Which ports are open? Provide a screenshot.

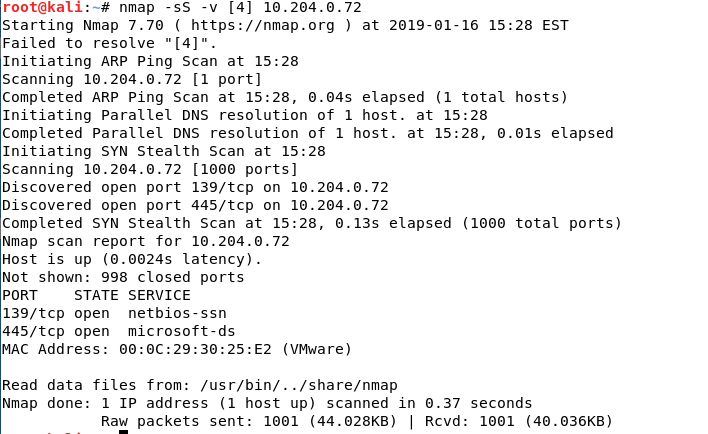
**Ports 139 and 445 are open**



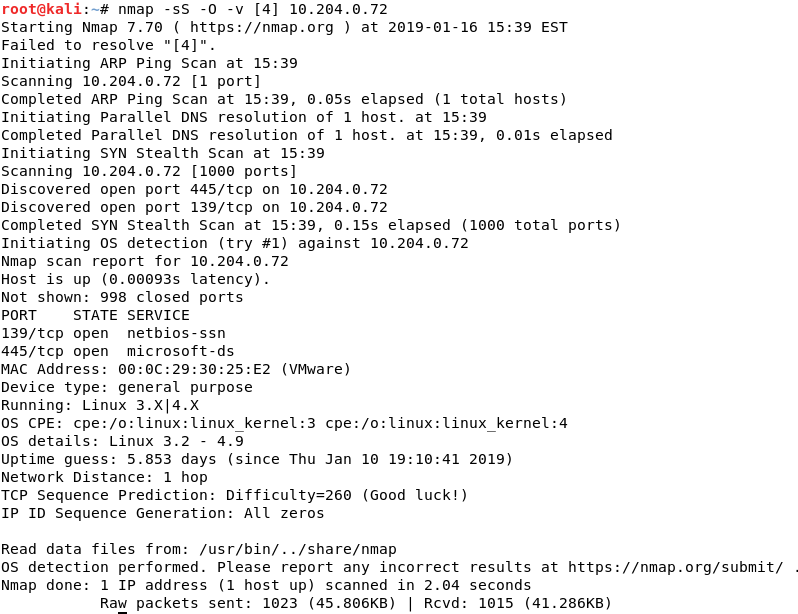
c. What services are being offered? Spell out all acronyms.

**Netbios is offered on port 139. Netbios is Network Basic Input/Output System**

**Microsoft-ds is offered on port 445. Microsoft-ds refers to Microsoft Directory Services**

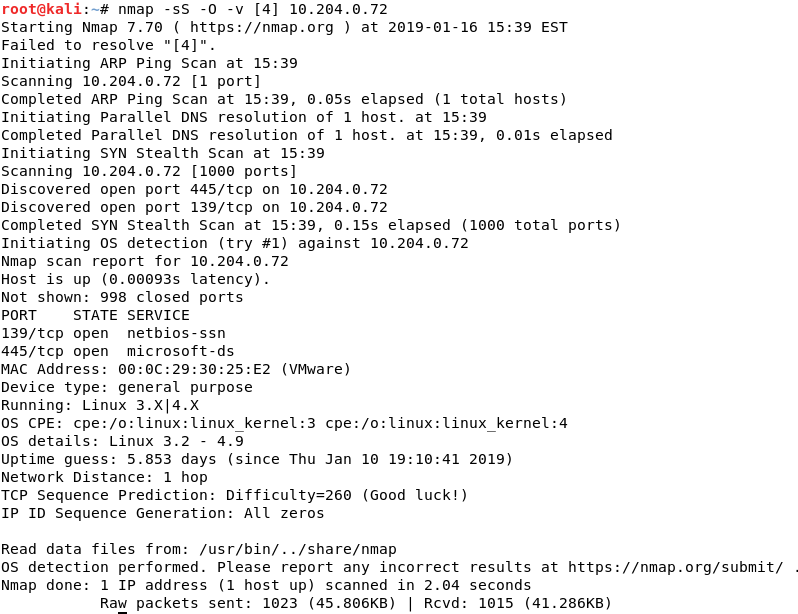


d. What is the MAC address? **00:0C:29:30:25:E2**



e. What is the operating system?

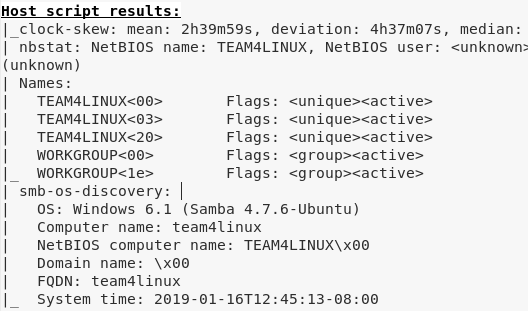
**Linux OS. Version 3.2 through 4.7**



f. What is the hostname of the target (e.g., LISXP33LG)?

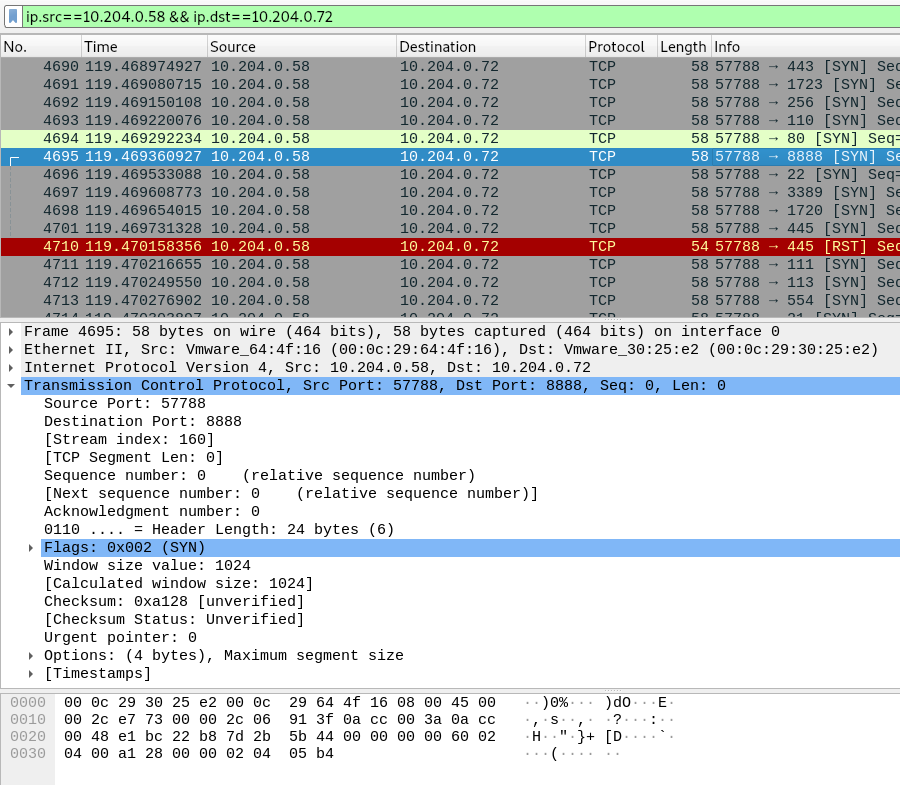
**Blackhat used this scan to find the hostname: “nmap -T5 -A 10.204.0.72”**

**Hostname: team4linux**



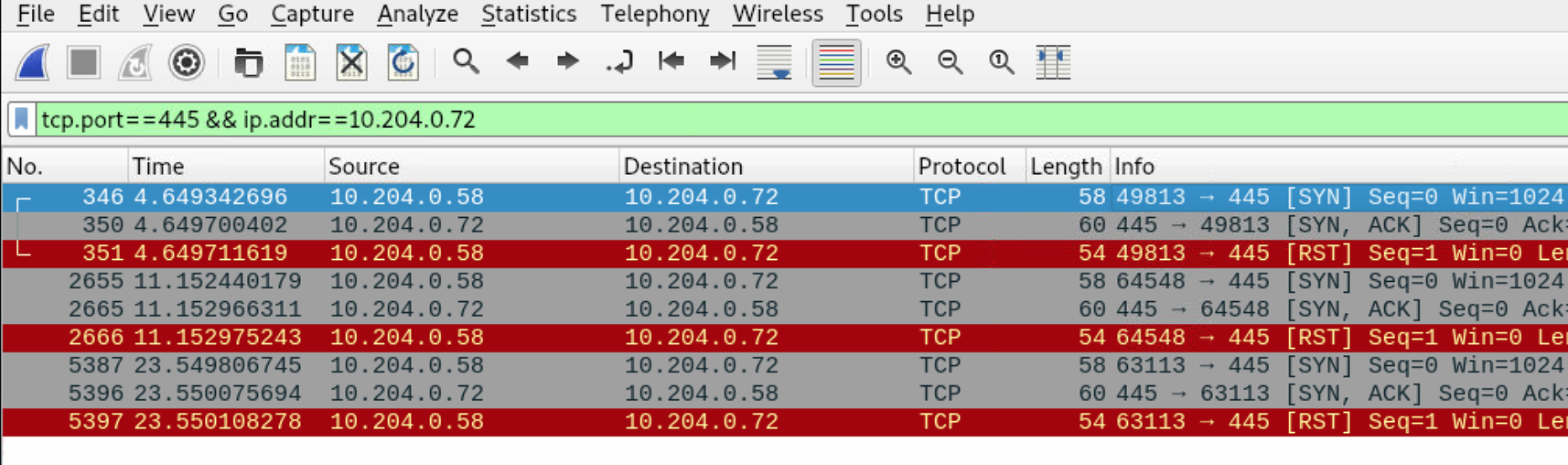
g. Look at the Wireshark data. During the scans, what type of packets did your workstation send to the target (i.e., which flags are set in the packets)?

**Blackhat’s PC sent TCP SYN packets to the victim’s machine on a variety of ports with the “SYN” flag set.**



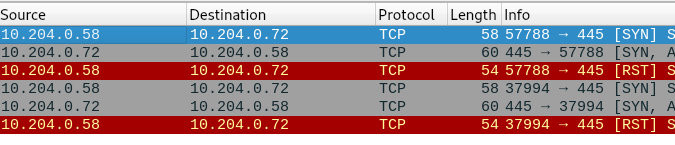
h. Select a port listed as open by nmap. How did the target respond for the open port? How did the Blackhat computer respond to the target’s response? Provide a screenshot of your filtered results. Useful filter: **tcp.port == <port #>**

**When Blackhat sent the TCP SYN packet to port 445 the victim’s machine responded with a TCP packet with the SYN and ACK flags set meaning it was trying to continue the handshake with the Blackhat’s computer.**





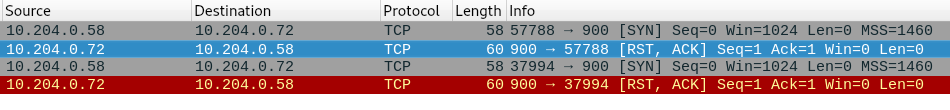
**The Blackhat’s machine then sent a TCP packet with the RST flag set to reset the connection and stop the handshake.**





i. Select a port listed as closed by nmap. How did the target respond for the closed port? Provide a screenshot of your filtered results.

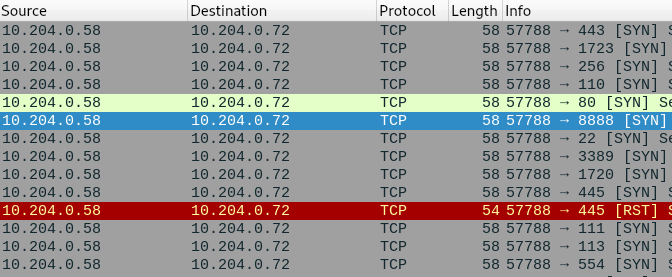
**When Blackhat sent the TCP SYN packet to port 900 the victim’s machine responded with a TCP packet with the RST and ACK flags set meaning it was acknowledging the SYN packet but also closing the connection.**





j. Were the ports scanned sequentially?

**No, the ports were not in sequential order. It looks like it scans the most common ports first.**





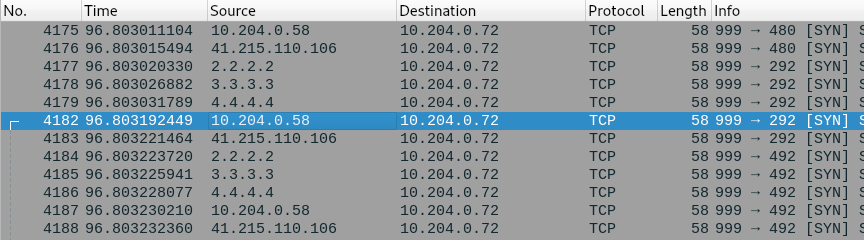
6. Now try nmap’s decoy feature.

Blackhat: Start Wireshark and run a SYN scan against ports 1-500 with decoy addresses of

**2.2.2.2,3.3.3.3,<<your real IP>>,4.4.4.4**. Note there is no space between those addresses, just a comma. Also set your source port number to 999.

a. Provide a screenshot of the Wireshark screen demonstrating the decoy and real IP addresses along with the 999 port number.

**I ran this commend to produce the following output: “nmap -p 1-500 -T5 -A -v -v -v -v -D "2.2.2.2,3.3.3.3,4.4.4.4,ME,RND" -g 999 -S 10.204.0.58 10.204.0.72”**

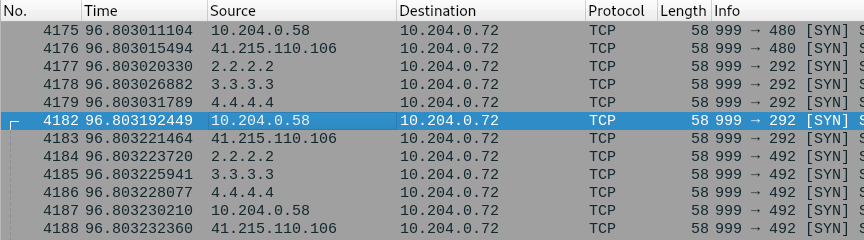


b. Describe how the use of decoys is different than nmap’s idle scanning.

**An idle scan sends packets to the idle (or blamed) machine in order to use it to gather information about the actual target. A decoy uses other IPs to create noise on the network in order to hid the real IP address conducting the scan. No other computers are used except for the Blackhat and victim.**

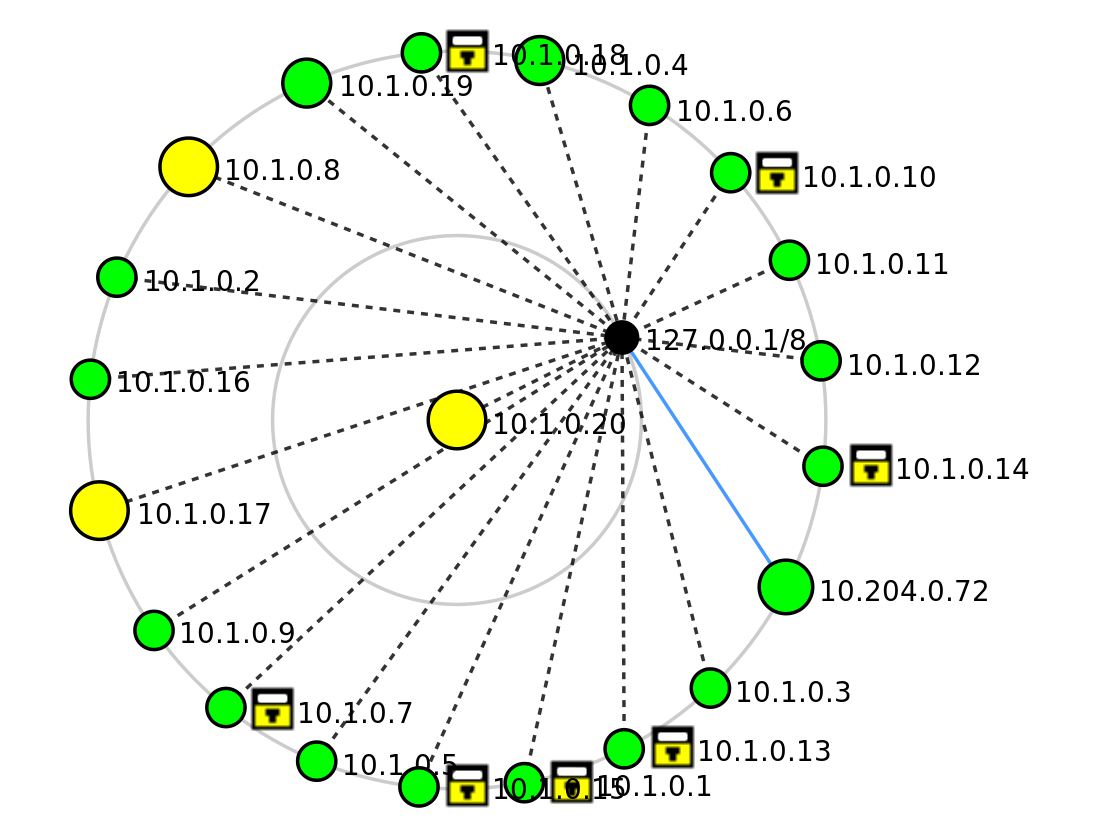
c. Inspect the Wireshark output of your decoy scan. Describe when and how many decoys are sent per real packet

**For each packet sent from the Blackhat’s real IP, there is one packet sent from each of the spoofed IPs sent to the victim's machine.**



7. Scan the IP addresses 10.1.0.1 through 10.1.0.20 looking just for FTP, SSH, or web servers. In the interest of time, I suggest running a simple SYN scan using aggressive timing without OS or version detection. Provide a screenshot showing the topology map generated by nmap. Ensure the text is readable. You may want to uncheck the hostname option in the controls panel to remove the clutter; displaying just IP addresses is fine.

**I used this scan “nmap -p 20,21,22,80,443, -T5 -v -v -v -v -Pn 10.1.0.1-20” to produce the following topology map.**

****

# 

# 

# 

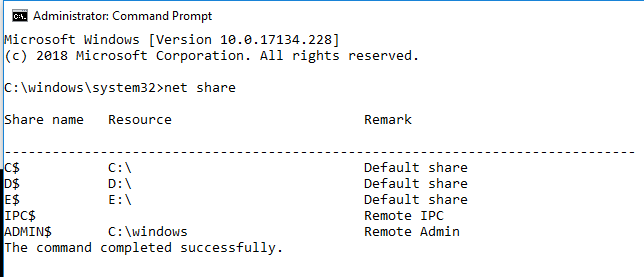
# **Shares**

Both team members perform the following, but only provide answers from one member. Provide a screenshot of your results.

Using a command shell (cmd.exe), answer the following:

8. List all (including hidden) shares offered on your local machine.

**C$, D$, E$, IPC$, ADMIN$**



9. List the users on your local machine.

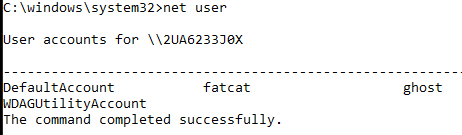
**Default Account**

**WDAGUtilityAccount**

**Fatcat**

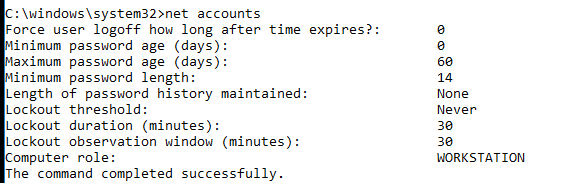
**Ghost**

**(As you can probably tell, I’m running these commands on my host machine)**



10. List the account settings on your local machine.

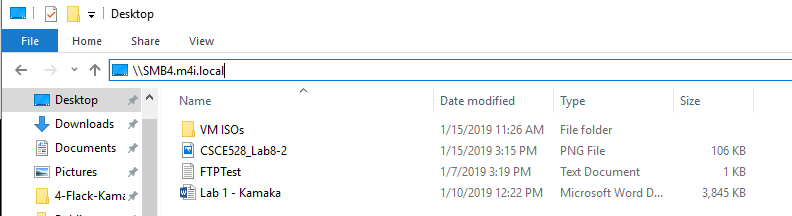
**We used the “net accounts” command to show the following settings:**



11. Using Server Message Block (SMB) and Windows Explorer, connect to the machine called SMB#.m4i.local where # is your team number. Provide screenshots of the windows/commands used.

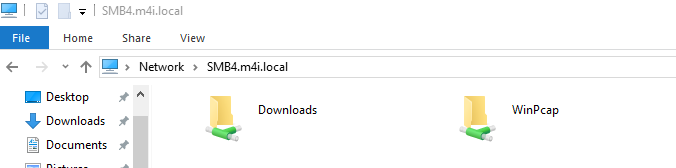
**I used windows explorer to attempt to access the location: \\SMB4.m4i.local**

**I used the username and password: user/Password!123**



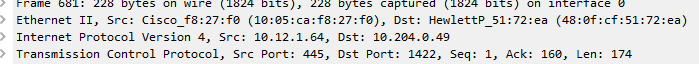
Which folders are being shared?

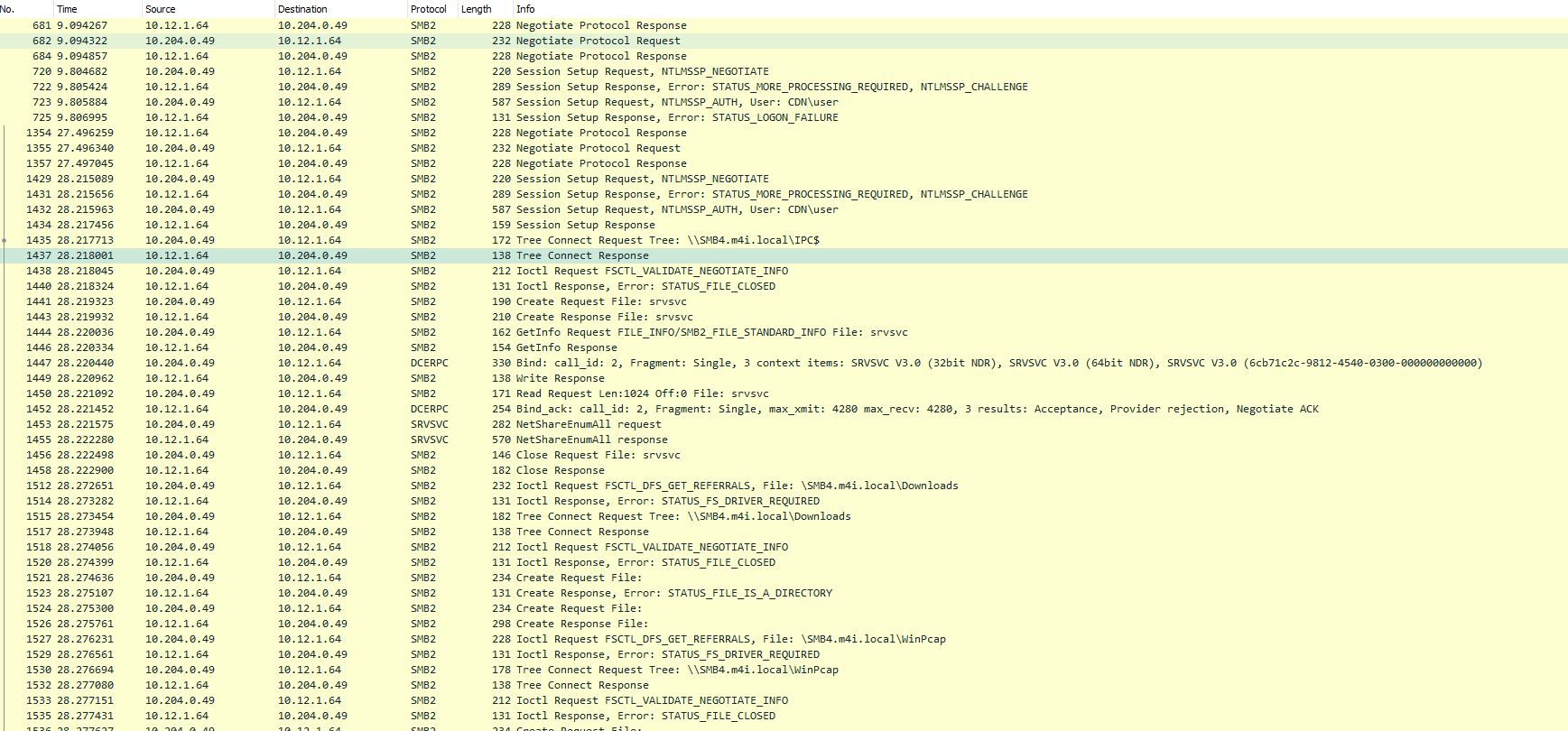
**Downloads and WinPcap**



What transport protocol and port is the SMB server using? Provide a Wireshark screenshot of your computer using the protocol and port listed; filter your Wireshark capture to only include frames involved.

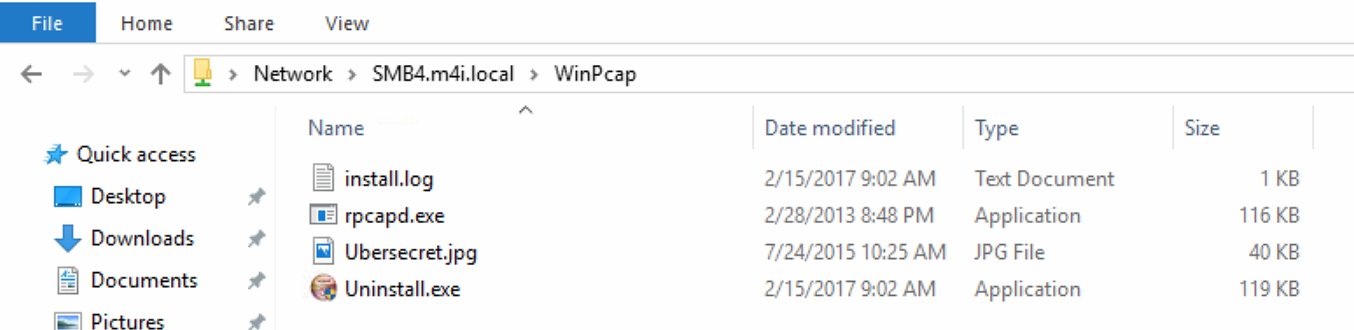
**This SMB session operated over tcp using server port 445 and client port 1422**



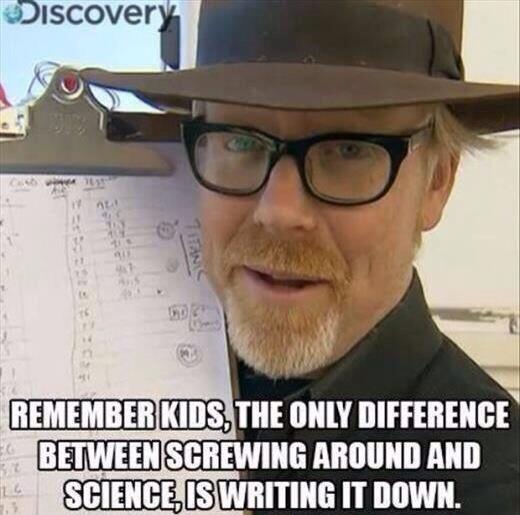


What is the secret message found on the target?

**When we opened the “WinPcap” folder and found the “Ubersecret.jpg” file.**



**The file contained this message:** **“REMEMBER KIDS, THE ONLY DIFFERENCE BETWEEN SCREWING AROUND AND SCIENCE, IS WRITING IT DOWN.”**



12. The Air Force has developed a new cyber attack tool. Your assignment is to find the phrase used to activate the tool. This phrase is contained in a file with a name starting with “flag”. In answering each step, provide detailed instructions or commands used as well as screenshots for each step. In order to actually view the file, you are only authorized to use a command shell; you may not use any other Windows utilities like Windows Explorer. At this point in the course, I do not expect you to crack passwords; therefore, I provide the following hints:

• This computer is on the same subnet as SMB#.m4i.local computers.

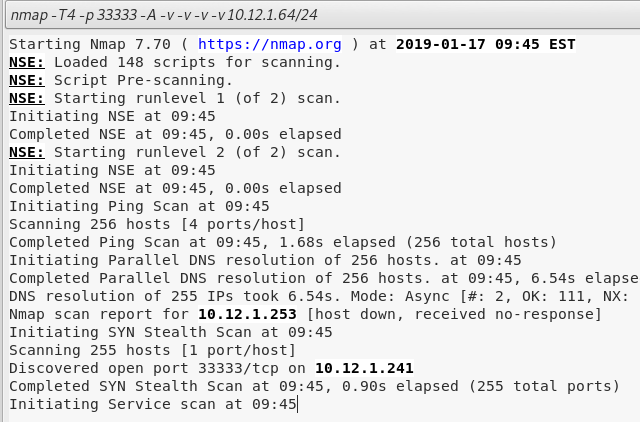
• Users are lazy and often use a password that is the same as their username or one of the top 10 worst passwords.

• The cyber attack tool installation process created a listening socket on TCP/33333.

• The following accounts are typical for Windows systems and are not of interest for this lab: Administrator, Guest, HelpAssistant, and any account with “Support” in the name.

Once again: You are not authorized to attack this machine; you are only authorized to scan and interact with it. Do not alter the target in any way including permissions.

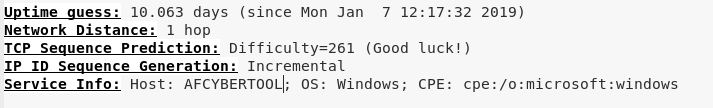
**We used nmap to scan the subnet of SMB4.m4i.local looking for an open port 33333. We found that host 10.12.1.241 has port 33333 open.**



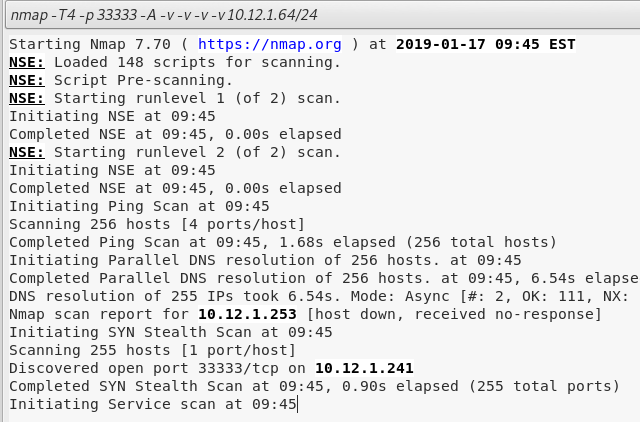
a. What is the name, IP address, and operating system (and version) of this mysterious computer?

**The following information was found using the nmap scan above.**

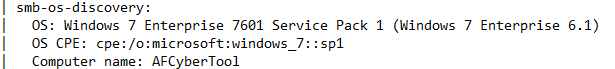
**Hostname: AFCYBERTOOL**



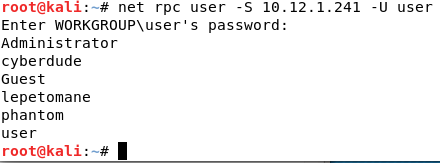
**IP Address: 10.12.1.241**



**Operating System: Windows 7, Enterprise 7601 SP 1**

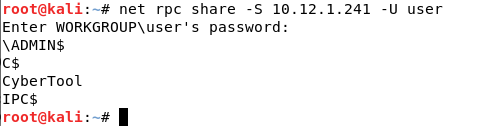


**We found the list of users using the net rpc user command with the username “user” and password “user”. Additionally we had to add the -S command to dictate to the net rpc user command that this is a server “net rpc user -I 10.12.1.241 - U user” did not work.**



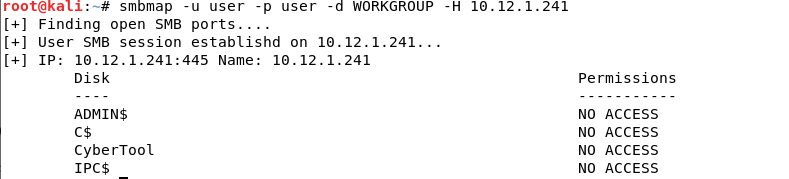
b. Identify shares on this machine. Provide a screenshot of your results.

**Using the same credentials from above (user / user) we were able to display a list of the shares on the machine.**

****

c. Find the secret phrase contained in the file located in the shared folder. List the exact instructions you used to find your answer. Provide a screenshot showing the phrase.

**The user / user login did not provide access to any of the shares on the computer**

****

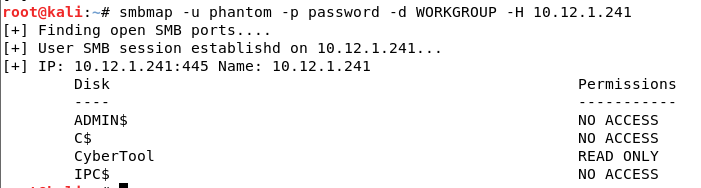
**These password combinations work, however none have permissions to the shares**

**lepetomane / leptomane**

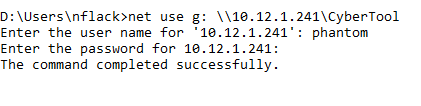
**user / user**

**cyberdude / cyberdude**

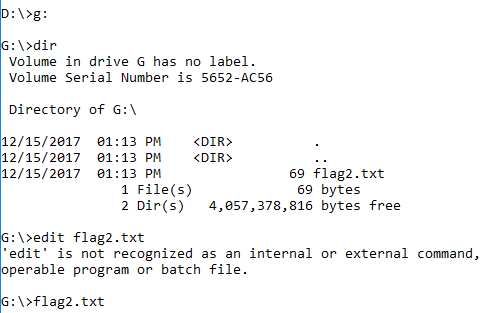
**We discovered “phantom” / “password” is a valid combination and the user phantom has access to the “CyberTool” share**

****

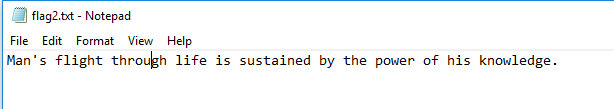
**Then we mapped the share to our computer (on the G drive) using the “net use” command**

****

**We navigated to the G:\ drive using the “g:” command and then listed the contents of the “CyberTool” share. This showed the contents of the directory which contains the flag2.txt file.**

****

**The message in the flag file is “Man’s flight through life is sustained by the power of his knowledge” (we feel accomplished and inspired 🙂)**

****

# **General Observations**

How long did it take you to complete the lab?

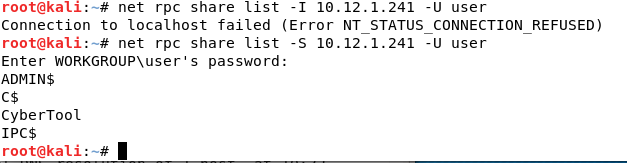
**4 Hours**

Was it an appropriate length lab?

**Good**

What corrections and or improvements do you suggest for this lab? Please be very specific, and if you add new material, provide the exact wording and instructions you would give to future students in the new lab handout. You may cross out and edit the text of the lab on previous pages to make minor corrections/suggestions.

**(Concerning question 12) I don’t know how you might communicate this without giving away too much, but to list the shares from Kali Linux on the server (10.12.1.241) you have to use the -S command for “server” instead of the -I for IP. From the screenshot below you can see that one works and one doesn’t when you provide the same username and password.**



**I know issues like this are just part of the troubleshooting process, but this one threw us for a loop and made us waste a lot of time. All the scanning data pointed toward the mystery machine being a PC and not a server (the OS said that it was a Windows 7 machine). Therefore, it seemed like “-I” was the logical choice. We didn’t try “-S” until we got a tip from a classmate. This might be one of the “nuggets” you drop in class when introducing Lab 2.**