Homework #2

Mike Pendleton

John Hulett

West Texas A@M University

**CIDM 6340 Network Management & Information Security – Fall 2021**

**West Texas A&M University**

Homework #3

***[N.B: You can work with a team/group of MAX 5 students, but you need to submit your own Homework report. Also, please mention all group members name in the cover page]***

**Name : \_\_\_\_\_\_\_Mike Pendleton\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Id:\_\_\_\_\_** **1058201\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Rubrics:**

*Full points:* Correct and complete answer.

*Partial points:* Correct but not complete answer.

*No points:* No answer or Incorrect AND incomplete answers.

**Q1. [10 points]** Using CISA website write white how to choose a good password and how to protect the password? Also, explain how can you protect yourself against malicious code?

<https://www.cisa.gov/tips/>

Answer: Avoid common mistakes by avoiding birthdays, common words(dictionary), as well to misspell the words by changing certain letters. For instance using @ for a or $ for s…etc. Length and how complex it is made, as the recommendation is 8 -64 characters long. Avoid spaces, but you can combine phrases combined into one word.

To protect against malicious code:

1. Install and maintain anti malware programs
2. Be careful with links and attachments, validate where they come from prior to clicking on them.
3. Blocking popups
4. Surfing the web with highly restrictive accounts in order to prevent installations from downloaders.
5. Disable autorun as well as auto play
6. Keep security patches up to date so that the latest vulnerabilities are patched.
7. Backing up data is extremely important, more so for ransomware attacks.
8. Enable firewalls and maintain the ACL’s
9. Utilize anti-spyware tools
10. Monitor all accounts used on line consistently to notice if there has been a change. If options for notifications on any change with the account, this should be enabled.
11. Avoid using public wifi. This is a way to avoid being impacted from someone else on the guest network that could be potentially infected.

**Q2. [10 points]** What are major security issues in wireless networks? Write some tips on how to secure 5G/6G Wireless Network?

**Answer:** The major security issues for wireless networks are: 1) Piggybacking, Wardriving, Wireless sniffing, unauthorized computer access, shoulder surfing, and theft of mobile devices. Some tips to secure a wireless network and minimize the risks are: Change the default administrator password, restrict the access to the network to authorized users. This means filtering the MAC addresses. You can encrypt the data on the network using one of the following protocols; WPA2 or WPA3. You can also protect your Service set identifier (SSID). Other options are; install a firewall, keep your antivirus software updated, keep your access point software patched and updated, utilize the internet provides or router manufacturing wireless security options, and connect to the internet using a virtual private network (VPN)

**Q3. [10 points]** What is ethical hacking? Use the *Hacker’s Dictionary* at <http://www.hackersdictionary.com/> to define the following hacker terms:

**Answer:**

Ethical hacking is also known as white hat hacking or penetration testing. Ethical hackers spend their workday learning how computer systems work, discovering their vulnerabilities, and breaking into them with no fear of being arrested.

1. Alpha geek – The person that has the highest skill level and is technically accomplished.
2. Grok – having exhaustive knowledge.
3. Red Book – Informal name for standard references to postscript.
4. Wank – An individual that is extremely clever.
5. Sanity check – checking code for mistakes in order to make sure that the code executes as expected.

**Q4. [10 points]** What do you mean by cyber Crime? Using the Web, journals, books, or other resources, find out if your state or territory has any laws specific to computer security. You might find the following websites helpful:

[www.pbs.org/wgbh/pages/frontline/shows/hackers/blame/crimelaws.html](http://www.pbs.org/wgbh/pages/frontline/shows/hackers/blame/crimelaws.html)

[www.cybercrime.gov](http://www.cybercrime.gov/)

List three laws that you find for your region and provide a brief one- or two-sentence description of each.

**Answer:** Cyber Crime is defined as criminal activity (such as fraud, theft, or distribution of child pornography) committed using a computer especially to illegally access, transmit, or manipulate data

Texas has the following laws

1. Texas Penal Code [§ 33.01](https://codes.findlaw.com/tx/penal-code/penal-sect-33-01.html), et seq. This law covers 5 offenses which include, accessing a computer without consent, soliciting a minor, accessing the voting computers, identify theft of a social networking account and utilizing personal information to defraud a person

The United States of America has the following laws

1. Federal law prohibits the use of the Internet or other interstate facility to lure children for sexual exploitation; prohibits crossing a state line with the intent to engage in a sexual act with a child; and prohibits possession, production or distribution of child pornography.
2. Computer hacking offenses under Title 18, United States Code, Section 1030 (fraud and related activity in connection with computers). Section 1030 prohibits intentional, unauthorized access into a protected computer which causes damage in excess of $5,000

**Q5. [10 points]** What do you mean by penetration testing? Name some scanning tools you might need to use in penetration testing? Open your command prompt or DOS prompt.

* Type in tracert - d [www.chuckeasttom.com](http://www.chuckeasttom.com) .
* Note what hops your computer takes to get to [www.chuckeasttom.com](http://www.chuckeasttom.com/).
* Repeat steps 2 and 3 with <http://home.pearsonhighered.com/>.
* Notice that the first few hops are the same.

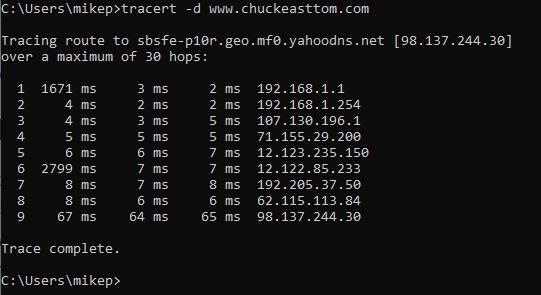
Write down what hops are taken to reach each destination and what hops are the same. Then briefly describe why you think some of the intermediate steps are the same for different destinations.

**Answer:**

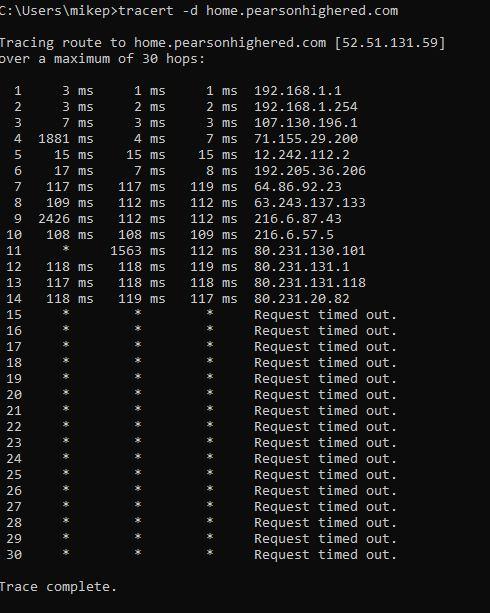
Penetration testing is testing for multiple exploits. Open ports, vulnerabilities both known and unknown. This is common for white hackers to see if they can infiltrate a site and then explain the vulnerabilities found.

Tools used for pen tests would be nmap, wireshark, kali, sqlmap, and others.

Regarding the tracert, I am not finding multiple or the same ip used multiple times across the 9 hops.



For <http://home.pearsonhighered.com/>, the trace was not able to complete and did max out in the 30 hops. But this also shows the same data as the ip’s that did return, none were the same. There are some on the same subnet which would indicate a switch sending traffic to the router. Typically the last octet is .1 for the routers.



**Q.6** **[ 10 points]** Differentiate between traceroute and the ping command. What traceroute offers beyond the ping command? Open your command prompt or DOS prompt.

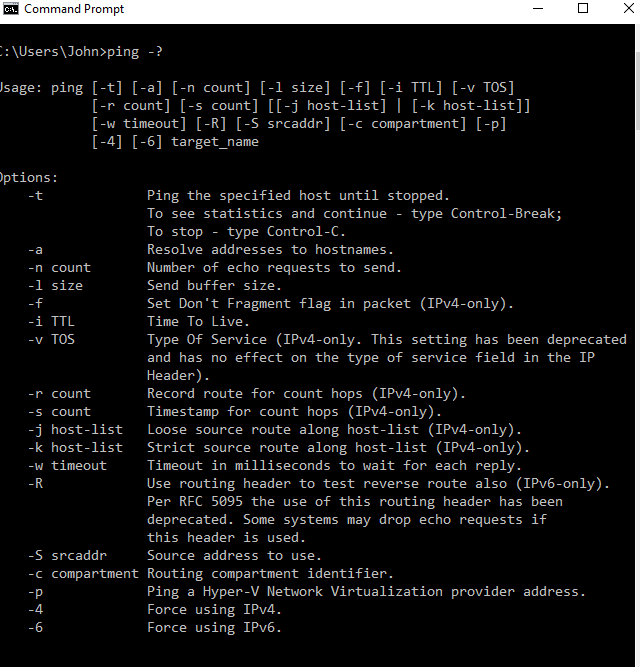
* Use the -? flag on the ping command and find out what other options you have with ping. You should notice several additional options, such as -w, -t, -n, and -i.
* Try ping [www.chuckeasttom.com](http://www.chuckeasttom.com/).
* Try the option ping -n 2 www.chuckeasttom.com. Then try ping -n 7 [www.chuckeasttom.com](http://www.chuckeasttom.com/).

What differences do you notice?

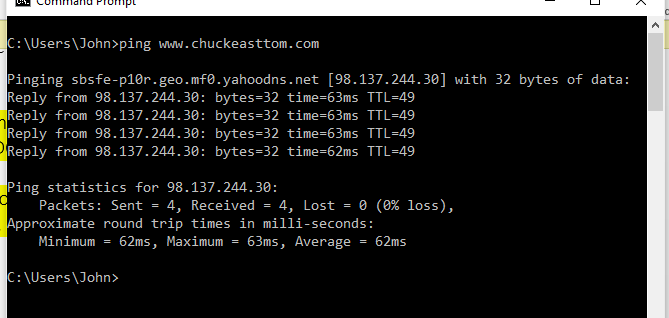
**Answer:**

Traceroute uses ICMP’s Ping command to find out how many different devices are between the computer initiating the traceroute and the target. The ping command sends an Internet Control Message Protocol (ICMP) ECHO\_REQUEST to obtain an ICMP ECHO\_RESPONSE from a host or gateway. To Determining the status of the network and various foreign hosts, Tracking and isolating hardware and software problems, and Testing, measuring, and managing networks.

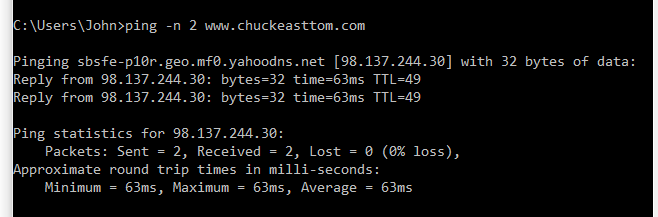
The ping command has 18 options



Ping [www.chuckeasttom.com](http://www.chuckeasttom.com/)



ping -n 2 [www.chuckeasttom.com](http://www.chuckeasttom.com)



Differences between the commands:

* ping with no flags sent 4 echo requests and received 4 responses
* ping with –n 2 flags sent 2 echo requests and received 2 responses
* ping with –n 7 flags sent 7 echo requests and received 7 responses
* All had the basically the same round trip times and all had 0% loss

**Q7. [10 points]** How can you design and protect a network as part of your job? [Case Study] In this case study we will consider a network administrator for a small, family-oriented video store. The store is not part of a chain of stores and has a very limited security budget. It has five machines for employees to use to check out movies and one server on which to keep centralized records. That server is in the manager’s office. The administrator takes the following security precautions:

* Each machine is upgraded to Windows 10, with the personal firewall turned on.
* Antivirus software has been installed on all machines.
* A tape backup is added to the server, and tapes are kept in a file cabinet in the manager’s office.
* Internet access to employee machines is removed.

Now consider these questions:

* What have these actions accomplished?
* What additional actions might you recommend?

**Answer:**

What have these actions accomplished?

The actions have limited the ability to access the network since the wan link has been severed, therefore nothing can be downloaded from the net.

The latest supported Microsoft client is in use in order to keep up to date with security patches.

Tape backups will help with disaster recovery for user profiles as long as roaming profiles are enabled and in use and stored on the servers where the backup takes place.

What additional actions might you recommend?

Isolated environments are considered secure, but they also require additional resources and are not easily managed. For instance, the data for the anti virus products would have to be brought into the environment manually since there is not a connection to the wan. For the same reason, the security patches would have to be brought in manually.

This is not a major issue, but there is more time in implementation depending on how many days and patches the systems will be behind since automatic updates would not be possible for both data and patches.

The key to the manager’s office would have to also be placed in a secure location where a designated amount of people can gain access. Because if not, then if needed and the manager is not available, the backups would not be accessible.

Security video could still be used for the store, but would have to be stored on the server to be included in the backups. This is because an online storage or sass solution could not be used in this use case.

**Q8. [10 points]** What is cyber stalking? Explain “Cyberstalking is often accompanied by real-time or offline stalking”. Using the Web, find a case of cyber stalking that is not mentioned in this chapter (in the lecture slides). You may find some of the following websites helpful:

[www.safetyed.org/help/stalking/](http://www.safetyed.org/help/stalking/)

Write a brief paper discussing this case, with particular attention to steps you think might have helped avoid or ameliorate the situation.

“Man Relentlessly Harassed Law School interviewer.”

The interviewer’s role was to interview potential school candidates for enrollment purposes. The school or victim was renamed anonymous in the website, but Ho Ka Terence Yung in 2014 was rejected from attending the school. He was accepted at a Texas University on a full ride.

Ho Ka Terence Yung began making threats to the interviewer by placing ads and using the interviewers’ home address stating in the ad’s that the victim was looking for sex with men. These advertisements also were made public on prostitution web sites. This is a clear definition of a form of cyberstalking. Simply because Ho Ka Terence Yung was upset that he was not able to attend his first choice University, he decided to torment the victim through the web and did not have to see the victim in person in order to do so.

Local law enforcement was involved, but requested the help of the FBI because the cyber stalking spanned across multiple states. Ho Ka Terence Yung attempted to mask the location on where the ad’s took place by using a friend's computer and his work computer. This was an attempt in order to assure that there was no way he could be connected to the crimes.

The victim was always on “high alert”, and never knew what to expect when the phone rang or someone was at the door. There is a significant difference from being mean on social media, such as disagreeing to a facebook post and writing things or possible name calling. This becomes a crime once there are threats involved. The victim was scared and was not able to function normally due to the unknown and what might happen if he went outside.

Ho Ka Terence Yung is now serving up to 46 months in prison at the time of the article on “June 10, 2019”. How could this have been prevented? For this specific case, the answer to that question would be difficult to prevent. The reason I state this, is there would have been several interviewees and how could the victim know that this was going to happen if Ho Ka Terence Yung never showed a sign of being upset.

Preventing a crime is difficult for all crimes. This is where digital forensics comes into action. Being able to trace the source on where the ad’s were implemented to the various websites. This is ultimately what linked Ho Ka Terence Yung to the crimes. Even though they were not added from his home, others knew him when traced back; additionally with being the only person who communicated previously with the law school at the friend’s house or his work office.

Source:

*cyberstalker-sentenced-061019*. (2019, 06 10). Retrieved from www.fbi.gov: https://www.fbi.gov/news/stories/cyberstalker-sentenced-061019

**Q.9 [10 points]** What do you mean by DoS attack? Give some recent examples. Using the Web or other tools, find a DoS attack that has occurred in the past 6 months. You might find some resources at [www.f-secure.com](http://www.f-secure.com/).

* Note how that attack was conducted.
* Write a brief explanation of how you might have defended against that specific attack.

**Answer:**

A denial-of-service (DoS) attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor. Services affected may include email, websites, online accounts (e.g., banking), or other services that rely on the affected computer or network. A denial-of-service condition is accomplished by flooding the targeted host or network with traffic until the target cannot respond or simply crashes, preventing access for legitimate users. DoS attacks can cost an organization both time and money while their resources and services are inaccessible.

# Massive DDoS Attack Disrupts Belgium Parliament - In May 2021 a massive distributed denial of service (DDos) attack cut off Internet access to numerous government, public, scientific and educational agencies, including Belgium’s Parliament and some law-enforcement agencies. The attack affected “all the institutions connected to the Belnet network. The attack was a coordinated effort targeting the Belgium government–also affected other ISPs in what was the largest [DDoS attack](https://threatpost.com/ddos-attacks-q4-cryptomining-resurgence/163998/) the country has seen, according to reports. Belgium is the headquarters of the European Union (EU) and thus a key hub of activity and decision-making that affects the global political and socio-economic landscape. The attack overwhelmed the web sites with traffic, rendering their public-facing sites unusable for visitors, while the attack overwhelmed internal systems, cutting them off from the internet.

Defending against a DoS attack

To defend against a DoS attack you can do several things. 1) know your networks traffic, understanding the normal traffic pattern (a baseline), will assist with the determination of unusual traffic. 2) Create a DoS of Service Response Plan, having a plan in advance will help you quickly and efficiently respond to an attack. 3) Make your network resilient, 4) Practice Good cyber hygiene, ensuring users are following best practices when accessing the network. 5) Scale up your bandwidth, the more traffic a network can handle the more it can absorb. 6) Utilize anti-DDoS hardware and Software. 7) Use cloud technologies since they have a larger bandwidth then on-premise networks. 8) Understand the symptoms of an attack. And finally ensure you are monitoring the network for usual activity

**Q10. [10 points]** List some job responsibilities of a network security engineer. (you can use examples from indeed or glassdoor, or any other sites) Runa Singh is the network administrator in charge of network security for a medium-sized company. The firm already has a firewall, its network is divided into multiple segments separated by routers, and it has updated virus scanners on all machines. Runa wants to take extra precautions to prevent DoS attacks. She takes the following actions:

* She adjusts her firewall so that no incoming ICMP packets are allowed.
* She changes the web server so that it uses SYN cookies.

Now consider the following questions:

* Are there problems with any of her precautions? If so, what are the problems?
* What additional steps would you recommend to Runa?

**Answer:**

*Network Security Engineer*: The main task of a network security engineer is to plan, design, optimize, implement, audit, and troubleshoot the network security system to improve the efficiency of the organization. The network security job is to protect the network from threats and bugs that could attack the system and also from the existing dangers. Most importantly, they must make sure that the networking systems can bounce back or withstand any type of mishaps such as natural disasters and hacker attacks. They should have a thorough knowledge and a multi-branched background that should include expertise from the fields of information technology, network and engineering, and information security.

*Are there problems with any of her precautions:*

The first thing to consider in defending against a Denial of Service attack is how the attack penetrates the network. This can be done by utilizing the ICMP packets. If firewalls are present then it should be configured to reject ICMP packets from outside the network. DoS attacks are unpredictable and can come in a variety of forms, so a firewall can be configured to prevent any incoming traffic. SYN cookies are used to resist specific kinds of Dos attacks and SYN flood attacks. This technique the network doesn’t develop a buffer space in memory, instead it transmits the SYN/ACK composed a cookie that is generate as a hash that includes the IP address, port # and other data from the client machine. When the client replies with an ACK it will include the SYN cookie for the server to verify. During the process no memory buffer is assigned until the third stage of the handshake process. Thus allowing the network to operate normally.

Additional steps to defend against the DoS attacks are:

1. Utilize virus-scanning software and it must be updated.
2. Keep the operating system and software patches up-to-date.
3. Develop a company policy on internet usage, and email protocol (being able to identify spam email)
4. Develop a cyber security training program so that all employees understand the different threats and attack methods