Mohammed Abusbeih

IT025: Lab 5

June 27, 2018

Summer, 2018

Table of Contents

[Executive Summary 3](#_Toc517996642)

[Chapter 9: Computer Security Fundamentals 4](#_Toc517996643)

[NMAP 4](#_Toc517996644)

[Extra Credit 5](#_Toc517996645)

[Github 6](#_Toc517996646)

[Security/Ethics 6](#_Toc517996647)

[Conclusion 7](#_Toc517996648)

# Executive Summary

We will be learning how all the security in this field is created and used. I will be able to learn how to hack into certain Wi-Fi protected devices. I will be able to research a very strong authentication process that is widely used today.

I will know the differences between a firewall and an active virus protection software. I will learn about the different methodologies that different virus protections use. I will learn how some companies track network data by using NMAP. I will create a GitHub account and upload my first repositories.

Finally we will learn how we are protected as US citizens when it comes to our technologies and personal data.

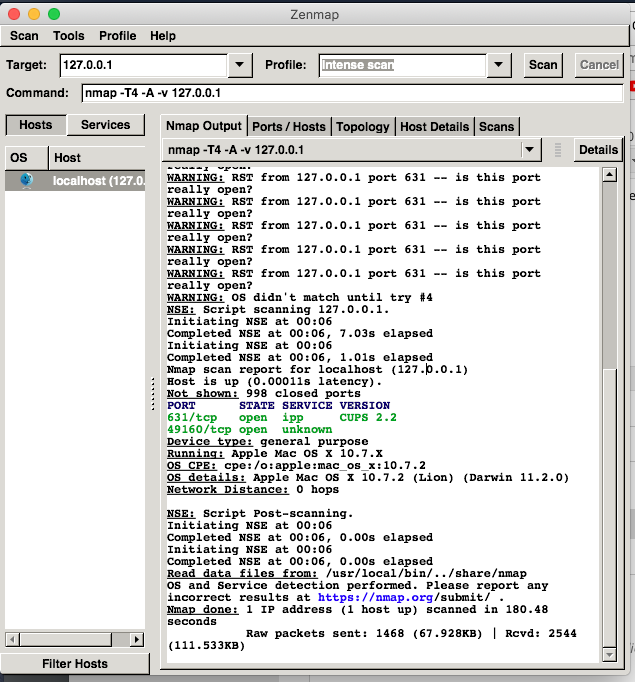
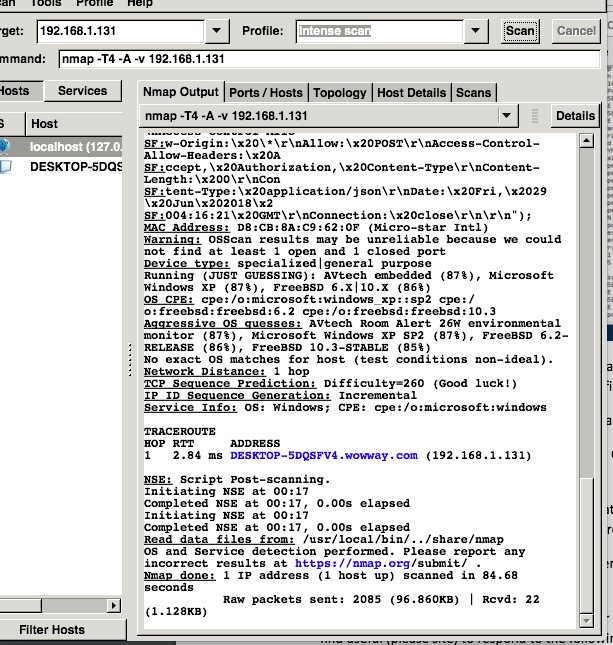
# Chapter 9: Computer Security Fundamentals

1. A Firewall is a barrier between you and the internet. Basically, it is to prevent attacks from other systems to access your network. A virus scanner is preventing software from attack your system or hardware. It is updated almost daily to keep up with all of the new virus being developed.
2. Cerberus is software that is used to scan local network information and hardware to scan for incoming attacks. It scans for patterns of ICMP packets, in other words it reads the error messages produced from the ICMP to look at where the issues are coming from. This is all a form of IDS.
3. Kerberos is software that is used in mainly Microsoft systems. It is an authentication system that allows for extremely accurate and long-lasting security. They have the several levels of security that allow for only certain people to gain access to the information they are allowed to and only for a short period of time before they are required to re-authorize themselves again. This allows for a much more secure work environment in most businesses.
4. Norton:  
   McAfee
5. A digital certificate is usually used to prove that a website is secured by a trusted source. They are also used to access certain websites that could only be accessed if you are given the certificate. Without a certificate some websites would appear as if they aren’t really a website.
6. A packet is any information that is transferred though the internet. A packet is sent anytime you do anything. All traffic is measured through packets. When using a VPN, all the internet access or packets are transferred through a VPN as if all of your information is coming from somewhere else to help hide your information or anonymize your internet access.
7. An algorithm is a set of computer instructions to secure something. There are different types of algorithms depending on how strong you want the connection.  
   WEP: Wired Equivalent Privacy is a secure algorithm in theory but is very easily cracked because it reuses some of the basic parts to receive a new key.  
   WPA is much better then WEB because for each packet it uses a new key. This way if someone was ever to crack it, it would be different very quickly.  
   WPA2 is the most secure of the three since it uses a much more difficult algorithm to crack.

# NMAP

1. NMAP is a network mapper which logs where each packet is going in a network and maps it out. This is used to track if there is any issues and how well the firewalls are working and most network issues are working.
2. It was used in Bourne Ultimatum to find out what mail server one of the characters was using to find out that it had a exploit they had just by finding out what version of mail server the end user was using.
3. Zenmap is a GUI for NMAP – Basically it is skin over a command line instructions to make it easier to read.

# Extra Credit

1.   
   It seemed that I have some open parts that I had no idea about. I am interested on how they are opened and how they are being used.
2.   
   This is my desktop computer in my basement. It is kind of cool to see what kind of information is stored just be sending requests.

# Github

# Security/Ethics

1. The fourth amendment also applies to your technology. This means your computer’s hard drives could not be searched without consent or a warrant.
2. The FAA is the organization in which all of the legislations are enforced by. There was a guy who was charged $50 for flying his drone in a park and he fought it stating that the FAA states that as long as he is not flying above 500 ft or above people, he was not in the wrong.   
   Source: <https://www.dailyherald.com/article/20160907/news/160909125/>
3. The 5th amendment allows for people to have their devices encrypted without having to be worried to be forcefully decrypted.

# Conclusion

Today I learned about how different types of encryption and how they work. I was able to learn how digital certificates work and how they could be used to access hidden websites. I was able to learn how some Wi-Fi networks could be accessed and hacked into quite easily.

VPNs are used to hide your information from sources, so you could be able to access information without either end knowing where you are from as long as your location is not being requested and accepted. We also learned how NMAP and the rest would work to read on whether or not you’re sending information to a location you may not know about it.