CIST 3381: Information Assurance and Security

Spring 2022

Reflection: Ethical Hacking Lab 4

Name: Michael Chillemi

1. What is Nmap? What is it used for? *Minimum 150 words*

Nmap is a reconnaissances tool used for scanning networks to show valuable information. Using Nmap is prime tool in for gathering information. When using this tool you can find important information like available ports. Doing port scans is very important so you can visually see a possible pathway to get inside a network or device. In Nmap you can also find valuable information like how many devices are live and what operating system they are running. This kind of information is useful because once you are able to determine what kind of operating system is on the device you can do research on what types of exploits can be used against those systems. This tool can also detect what versions these operating systems are running as well. These features are even more useful when conducting reconnaissances. To sum it up Nmap is a tool that has the capabilities to give a user valuable information in order to creating a full mapping of a networks.

1. Reflect on your experience in this lab. *(Read “Writing Your Lab Reflection”, available in the Left Panel on BB Course Homepage).* *Minimum 150 words*

This lab was very useful and enjoyable. In this lab it taught me how to properly use and read Nmap. It has showed me the importance of using reconnaissances tools in order to properly plan a pen test. Without tools like Nmap pen testing would definitely be a lot more trickery. We also learned the difference between how computers communicate with sending packets. When discussing packet exchange we demonstrated the difference between a three way handshake and verifying communication between a device. Diving deep into these skills is very important to learn how the basic steps in reconnaissances. One idea that would have definitely improved the lab if we had more time would be to discussing the different cases when to use certain commands. Becasue when we were going through some of the Nmap commands I noticed that there were some stealth commands and some brute force commands. When would be the best time to use the brute force commands? Or is it always better to use the stealth commands at all times.

Deliverable:

Write and Save the responses in this file. Submit the file