CIST 3381: Information Assurance and Security

Spring 2022

Reflection: Ethical Hacking Lab 3

Name: Michael Chillemi

1. Explain the difference between Active Reconnaissance and Passive Reconnaissance *Minimum 150 words*

The term "passive reconnaissance" refers to a method of gathering information about computers and networks without actively engaging with them. This means that you don’t exactly engage with the target so you don’t trigger any alarms. A lot of the times passive reconnasissance is used to gather public information about the target. This type of information is called OSINT which stands for Open-Scource-Intelligence. When gathering open source intelligence you can acquire useful information like IP address,domain names,targets names, hostnames, email addresses, and dns records.Passive reconnasissance is a very important tactic to utilize when you are conducting a pen test on a organization. In active reconnaissance, on the other hand, the attacker interacts with the target system, usually by running a port scan to see if any open ports are there. When conducting active reconaissanceyou directly work with the computer system to gather very specific information about the target. Some of the tools used in active reconnaissance will send requests to the targets to gather information like what devices are connected to the network,what ports are open, what kind of operating system is running on the devices and many more useful info. Active reconnaissance is a important tactic that hackers and pentester utilize t ocomplete their mission.

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 really exciting and tons of fun. It showed us a tool that can mirror webpages which was really cool but scary at the same time. Before coming into this lab I always wondered how blackhat hackers or scammers replicate webpages to fool people. My first thought was that they spent tons of time creating the webpages on their own. Which I thought was very tedious and a waste of time. But after going through this lab it made me realize how fast and easy it was to duplicate a webpage. Then all the hacker/scammer would need to do is modify the code a little bit to use it for wherever they want. This lab is also giving me great ideas on how I want to do showcase my project for this course.

Deliverable:

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