Homework 1

Mengxiang Jiang
CSEN 5303 Cybersecurity

September 25, 2023

Problem 1. Searching on google for "free hacking tools" and write about two of them.

Two of the most cited tools on google results are Nmap and Metasploit.

1. Nmap, short for "Network Mapper," is a powerful open-source network scanning and security auditing tool. It's designed to discover and map devices, services, and vulnerabilities on computer networks. Nmap operates by sending packets to target hosts and analyzing their responses. This information helps administrators and security professionals gain insights into the network's topology, identify active hosts, discover open ports, and assess potential security risks.

2. Metasploit is a widely used penetration testing and exploitation framework that helps security professionals and researchers test the vulnerabilities of computer systems, networks, and software applications. Metasploit provides a vast collection of pre-built exploits, payloads, and auxiliary modules. These components can be used to simulate attacks on various vulnerabilities in order to assess the security posture of a system.

Both tools, however, can also be misused by malicious actors to exploit vulnerabilities for unauthorized access and attacks. To prevent this, security professionals and ethical hackers must use these tools in controlled and authorized environments to identify and address vulnerabilities before they can be exploited by these malicious actors.