CYB 552 – CASE STUDY: NMAP

1.) The goal of utilizing a ping sweep during network discovery is to detect active hosts on the network. Sending ICMP echo request packets (ping) to the target IP addresses and noting which hosts respond—indicating that they are active—is how Nmap carries out this work.  
  
2.) The key difference between a TCP SYN scan (-sS) and a complete TCP connect scan (-sT) is how they connect to the target host. The TCP SYN scan sends a SYN packet to the target port and waits for the SYN-ACK response, which signals that the port is open. In contrast, the full TCP connect scan completes the whole three-way TCP handshake. And finally In most cases, the TCP SYN scan is favored since it is more covert and unlikely to be discovered by the target system.

3.) Performing service version detection (-sV) is critical during a vulnerability assessment and it lets the security team determine the precise versions of services operating on the target systems. Accurately identifying known vulnerabilities that have existed in those services requires knowledge of the service versions.

4.) The OpenSSH 7.2 instance in this case study is an example of an outdated software version that provides serious hazards. These older versions includes known security flaws that attackers are used to gain unauthorized access, elevate privileges, or execute malicious code on vulnerable systems.

5.) When analyzing different aspects of the target system's network stack, including the order of TCP/IP packets, the initial time-to-live (TTL) values, and the existence of TCP/IP options, Nmap's OS identification capability operates. Understanding the operating system is essential for vulnerability assessment as many operating systems have unique security flaws that call for distinct mitigating techniques.

6.) After offering a framework for creating unique scripts that may be used for a variety of activities, such as vulnerability scanning, information collection, and exploitation, Nmap's Nmap Scripting Engine (NSE) expands its capabilities. These scripts have the potential to greatly increase Nmap's capability and allow for more thorough security evaluations.

7.) Making the MySQL database available from outside the trusted network raises the danger of unauthorized access, brute-force assaults, and data breaches. By putting in place network-level limitations to guarantee that the databases are accessed from reliable internal IP addresses, this should be reduced.

8.) Using an FTP service with anonymous login makes the network susceptible and it allows unauthorized users to upload, download, and perhaps edit critical data on the system. This can result in data breaches, system vulnerabilities, and the propagation of malware.

9.) A flaw in the Microsoft Server Message Block 1.0 (SMBv1) protocol known as Eternal Blue was used in the WannaCry ransomware assault. Under these circumstances, the antiquated Windows 7 workstations were susceptible to this vulnerability, which provides attackers remote code execution and additional network penetration.  
  
10.) Following a Nmap scan, best methods for maintaining network security include:  
  
a.) Patching or updating any software versions that have been recognized as vulnerable.  
b.) Using access restrictions and network segmentation to prevent unauthorized access to services and systems.  
c.) keeping an eye out for any new vulnerabilities or questionable activities on the network.