Nmap scan results

Open ports from scan are as followed:

Port	Protocol	Service
80	tcp	http
135	tcp	msrcp
139	tcp	netbios-ssn
443	tcp	https
445	tcp	microsoft-ds
3306	tcp	mysql

Open ports are an opening for threat actors to take advantage of vulnerabilities. That is why one must be cautious and close ports when they are done utilising the ports.

1.Port 80: Open due to visiting a website. This is something that is basically having double the problem. This port is not secure, and it is open, so it puts the computer at high risk. Using this port is not safe because it stores usernames and passwords in plaintext It would be best to opt for port 443 because it is more secure.

2.Port135: This port is the Microsoft RPC (Remote Procedure Call). Allows programs in Windows to request services from other software on the network. This is open because of my virtual machine. If exploited malware can spread across network. This could also lead to privilege escalation within the network which could increase the level of exploitation.

3.Port139: This is also open because of the virtual machine. If the virtual machine is misconfigured it could lead to exposure of sensitive information. This can also provide domain information, which is a problem, since it gives a threat actor more information about websites we have visited.

4.Port 443: This is open because I was visiting a secure website. This is one of the safest ports for websites. It encrypts the information and makes it difficult for threat actors to exploit. If there. If this port is overwhelmed with traffic this leads to DDoS attacks. This can be used in the first step of active reconnaissance especially if the certificates of websites have expired.

5.Port 445: This is the Microsoft Directory Services which has SMB (Server Message Block). The version installed is not SMBv1-not secure. This allows file sharing and Active Directory communication. If this is misconfigured it can lead to remote execution which can also be part of the command-and-control part of the Cyber Kill Chain. This can increase the attack surfaces like ransomware and Remote Access Trojans (RAT). This can also lead to information being compromised.

6. Port 3306: MySQL this has authentication weaknesses that can allow unauthorized database access. When the database has been accessed, the threat actor can even change privileges to root and can exploit the database further, this can lead to system compromise. This also increases the likelihood of a SQL injection attack to be successful.