PenTest Lab Exercise Ex050 – nmap

Goal

Use nmap to explore the services available on host www.artstailor.com.

Tasks

1. Log in to the Netlab server, schedule the PenTest Ex050 Lab, start up the lab, and login to your Kali VM.

2. Run an nmap TCP version scan on machine www.artstailor.com. Note the OS type and any open ports and running services. Use Wireshark to inspect the behavior of this scan. Expect to see plenty of packets.

3. Run an nmap UDP version scan on the same machine for ports 1-256. Identify any open ports . Again, use Wireshark to investigate the behavior of this scan.

4. Which scan took longer, the TCP scan or the UDP scan? Which scan scanned more ports? Explain the outcome in the attack narrative section of your report. If you're not sure which scan took longer, find out how you could determine this! (Check out the linux time command.)

5. Point out any interesting or odd ports in both the scans, check out the traffic generated by nmap for those ports to help you identify any oddities.

6. Use the command searchsploit on kali or for services and their versions that were identified to determine if any vulnerabilities exist. You could make the same search on the internet using search terms that include service names, version numbers, and keywords like CVE, vulnerability, or exploit, but don't report on any vulnerabilities you don't find in searchsploit lest your report grow seemingly without bound.

7. If there are any vulnerable services (check the versions), Google is your friend. There may be exploit-db.com exploits or there may be Metasploit modules for any vulnerabilities that exist. You should look for these, but don't report these exploits.

8. Write a report that discusses your activities and provides the information you were asked to note above. Make sure not to add information about exploits you find via google. Make sure to include one or more Mitre ATT&CK TTPs for your activities. Identify a finding associated with each of those unique services that appears to have one or more vulnerabilities. Findings always must include a CVSS score. The information you provide may form the basis of a more complete penetration test report.

9. Yes, there was a key available with this exercise.