Kobe Coleman

Professor Duvall

CYSE 368

7/5/2024

Reflection Paper 4

For these next 50 hours I looked over my Nmap and Nessus Scans to see what ports open and what vulnerabilities can be possibly exploited. When looking at Nmap scans my coworkers have told me that there are always certain ports that if open have a multitude of exploits. Some of these open ports can be port "20, 21, 22, 23, 25, 53, 137, 445, 80, 443, 1433, and 3389" (Netwrix). For the Nessus scans they were trickier since it gives the user so much information. I had to rely on more coworker's experience and google to figure out what can be exploited and what is patched from the system latest updates. The good thing about Nessus scans is that the tool will tell you what CVE was used to exploited the vulnerability. CVEs are " CVE stands for Common Vulnerabilities and Exposures. CVE is a glossary that classifies vulnerabilities. The glossary analyzes vulnerabilities and then uses the Common Vulnerability Scoring System (CVSS) to evaluate the threat level of a vulnerability. A CVE score is often used for prioritizing the security of vulnerabilities" (Imperva). After getting my scans we use a tool called Eyewitness which "EyeWitness is designed to take screenshots of websites provide some server header info, and identify default credentials if known. EyeWitness is designed to run on Kali Linux. It will auto detect the file you give it with the -f flag as either being a text file with URLs on each new line, nmap xml output, or nessus xml output. The --timeout flag is completely optional, and lets you provide the max time to wait when trying to render and screenshot a web page." (Github)

Work Cited

RedSiege. “Redsiege/Eyewitness: Eyewitness Is Designed to Take Screenshots of Websites, Provide Some Server Header Info, and Identify Default Credentials If Possible.” *GitHub*, github.com/RedSiege/EyeWitness. Accessed 5 July 2024.

Schrader, Dirk, and Dirk Schrader Dirk Schrader is a Resident CISO (EMEA) and VP of Security Research at Netwrix. A 25-year veteran in IT security with certifications as CISSP (ISC2) an. “Open Port Vulnerabilities List.” *Common*, blog.netwrix.com/2022/08/04/open-port-vulnerabilities-list/. Accessed 5 July 2024.

“What Is CVE and CVSS: Vulnerability Scoring Explained: Imperva.” *Learning Center*, 21 Dec. 2023, www.imperva.com/learn/application-security/cve-cvss-vulnerability/#:~:text=CVE%20stands%20for%20Common%20Vulnerabilities,threat%20level%20of%20a%20vulnerability.