Kelsey Gallo
IST 294 Section W02
10-2-24

Final Project

Penetration Testing

In their textbook *Hands-on ethical hacking and network defense*, Robert S. Wilson and his colleagues (2022, pg. 1) explain that “ethical hackers are employed or contracted by companies to do what illegal hackers do: break in.” An ethical hacker, or penetration tester, imitates a potential cyber-attack by breaking into a company’s network or applications, and produces a penetration test report containing the findings. The purpose of the report is to enable the client to better secure their network and to identify potential security vulnerabilities that might need to be monitored (pg. 2).

No matter if the tester is an independent contractor or an employee of a large security company, he or she must negotiate the scope and rules of engagement of the penetration testing with the client company. It is a good idea to get the agreement written in a contract as a reminder for both parties involved (pg. 14). When conducting a penetration test, a tester should clearly and consistently communicate with management and IT staff about the actions taken during the test and the results. The tester should also possess a knowledge of networking concepts and computer technology, an understanding of applicable federal, state, and local laws regarding cyber-activity, and ability to use the necessary tools to conduct testing (pgs. 15-18).

Reconnaissance

Footprinting is the process of passively collecting information about a company or organization before performing a security test or an attack. It can help pinpoint vulnerabilities in the security system, as well as what types of security measures are being used (pg. 71). *Social engineering* takes advantage of human nature to extract information from individuals. Attackers will attempt to gain login credentials and other types of intelligence through familiarity, politeness, urgency, and sometimes intimidation in social interactions with their victims (pg. 88).

DNS footprinting looks at DNS records, which can be obtained from a zone transfer from a server, to identify connected hosts on a network, as well as their IP addresses and hostnames. Two command-line tools that can perform zone transfers are *nslookup* for Windows and *dig* for Linux. Dig is now preferred over nslookup, particularly because it provides a thorough picture of a network’s organization, including the number of hosts and subnets present on it (pg. 86).

Port Scanning and Enumeration

Netstat is a command-line utility that displays open and/or listening ports and network connections (which could potentially be accessed) on a Windows computer (pg. 33). *ICMP* is a protocol used to send messages about network operations to other computers, such as “destination unreachable” (code 3) or “redirect” (code 5). ICMP messages can assist with troubleshooting network connectivity problems or with tracing the route that an IP packet travels between hosts (pg. 34). *Hping3* is a port scanning command tool that can perform ping sweeps as well as bypass filtering devices by crafting IP packets (pg. 105). A ping sweep is the process of using the ping command on a range of IP addresses to locate active hosts on a network (pg. 102). *Banner grabbing* is the act of retrieving a banner, which may contain vital information about the software running on a server, including its name, version, and protocol. It is commonly carried out using Telnet, a command-line tool that establishes an insecure, remote connection to another host’s open port (Vona 2020).

Determining Vulnerabilities

Nessus and *OpenVAS* are both vulnerability scanners for networks and services that enumerate systems, name and rank detected vulnerabilities according to severity or risk score, and suggest actions to take to close the gaps. Leon Yen (2024) advocates using Nessus for large enterprise networks due to the extensive amount of data collection techniques that it employs and the detailed information that it provides in reports. For smaller organizations, Yen also recommends OpenVas, as a no-cost, user-friendly tool that aggregates the results that it obtains and prioritizes weaknesses based on severity and possible impact.

The *Common Vulnerabilities and Exposures (CVE)* website identifies and provides information on current OS and app vulnerabilities and possible attacks. Wilson et al. (2022) also suggest browsing the websites of Packet Storm and Security Focus to learn more about vulnerabilities. In addition, OffSec’s Exploit Database and Carnegie Mellon University’s CERT Coordination Center provide helpful databases containing recently-published exploits and vulnerabilities, respectively (pg. 54).

Solutions to Identified Vulnerabilities

1. Several servers do not have up to date patches. The Web server is also running an old version of IIS.

Wilson et al. recommend system administrators to keep systems patched and use an up-to-date version of IIS (such as version 10 for Windows Server 2019) whenever possible. Older versions of these systems can have many of their features enabled by default, providing more avenues for attacks to occur (pg. 76). To help simplify patch installation on Windows servers, you may wish to use Windows Software Update Services (WSUS) or another patch management tool from a third-party vendor such as BigFix or Tanium (pg. 182).

2. The firewall revealed unused ports which are open.

You should close and protect unused ports, since anyone can gain access to applications provided by open ports and potentially launch attacks using them. However, you should also consider which services are necessary for ease of access, such as Internet and email, and adjust the amount of open and closed ports to allow both security and availability (pg. 33).

3. Several employees and managers were tricked and they entered their username and password into a fake website.

The fake website was likely provided by a phishing email, a form of attack which can entice users into providing their login credentials and use those credentials to steal data or money (pg. 91). You must educate both employees and managers about the dangers of such attacks and how to recognize and avoid them, such as by sending monthly security update emails. You could additionally implement white-listing, which permits only authorized programs and websites to run on computers (pg. 60).

4. Using Social Engineering, it was easy to obtain employee passwords. Based on the results, it was determined the passwords are weak.

"The best defense against social engineering is user training," as Wilson et al. assert, "because the object being hacked for information is a person and not a computer. Employees should be taught to confirm the identity of the person asking the questions, and never give outsiders any information about OSs or credentials, no matter how familiar they may seem (88). As for passwords, users should not use words that can easily be guessed, such as names of relatives or birthdays (pg. 285).

Works Cited

Wilson, R. S., Simpson, M. T., & Antill, N. (2022). *Hands-on ethical hacking and network defense* (4th ed.). Cengage.

Vona, S. (2020, March 2). *Banner grabbing - penetration testing basics*. Putorius. https://www.putorius.net/banner-grabbing.html.

Yen, L. (2024, February 23). *OpenVAS vs. Nessus: top vulnerability scanners compared*. Datamotion. https://www.datamation.com/security/openvas-vs-nessus/.