Host Detection and Enumeration

Host detection and enumeration are critical steps in pen testing. Employing the right tools for these tasks will help the tester audit the correct flaws.

Nmap

It is an adaptable command-line tool that can run several scans, such as port scans, operating system detection, and service identification. The NMAP Scripting Engine (NSE) allows users to write scripts, automate several network tasks, and execute them in parallel efficiently, and Zenmap is the visual interface for Nmap. This technology has several limitations: the scan results are based on the packets returned by the target, which will not always accurately show the devices in the network; the scan time can be high if a minimum is not specified. (*Nmap Network Scanning*, n.d.)

Commands:

- nmap -sV -O <ip address> -p <port range>
- nmap -sV -O –script=<scripts> <ip address>.

Nessus

A vulnerability scanner detects and provides detailed reports of out-of-date systems, misconfigurations, and missing patches, letting the tester know which vulnerability should be proofed. This tool complies with security standards such as HIPAA and PCI DSS. However, this technology has several limitations, such as Network Address Translation(NAT), IPS, firewalls, and load balancers or proxies affecting the scan result, possibly missing vulnerabilities; the scan is slow when the network is extensive. (*Deployment Considerations (Tenable Nessus 10.8)*, n.d.)

Commands:

- nessus -T <ip address> -p <port range>.

Nikto

It is an open-source scanner that executes vulnerability scanning against websites. Nitko assesses outdated versions of web server software, server misconfigurations, and any potential vulnerabilities they might have introduced. This application has some limitations, like it doesn't support the testing of authentication areas, has a limited scope by only working with web servers, is not a stealth tool, and can produce inaccurate results.(*Nikto | CISA*, n.d.; *Nikto 2.5 | CIRT.Net*, n.d.)

Commands:

- nikto -h <url> -Tuning <mode> -port <port> -ssl

Wireshark

It is an open-source, multi-platform network protocol analyzer that the pentester uses to learn about the network's services. It captures the packets sent through the network and shows in detail the protocols and the corresponding port that services use, such as SMTP, RADIUS, HTTPS, and FTPS, as well as the devices in the network and their communication patterns. This technology has several limitations, such as it can't capture all the traffic, just the one between the tester computer and the target system, and it can become slow when loading or filtering a large file. The tester can use the command line or the visual interface. (*NCCIC ICS_FactSheet_Packets_S508C.Pdf*, n.d.; *Wireshark · About*, n.d.)

Commands:

- wireshark -i <interface> -f <filter>

Metasploit

Metasploit is a helpful application generally used to find vulnerabilities in the system. It allows the user to search in a database of metasploit a payload corresponding to the protocol and vulnerability detected, and then test if this payload will penetrate the system by setting up the required parameters. This technology has several limitations, such as providing false positives, limited report capabilities to comply with some business needs, reliance on public exploits, no guarantee it always works, and antivirus detection of the metasploit. (Team, 2023)

Commands:

- msfconsole
- search <exploit>
- use <name>
- show options
- set RHOST <IP address>
- info <exploit>
- show payload
- set payload <name>
- run
- exploit

Conclusion

The use of the right tools can help the auditor achieve the goals with efficiency and accuracy, helping the user to analyze and create a strategy to exploit the vulnerabilities.

References

Deployment Considerations (Tenable Nessus 10.8). (n.d.). Retrieved March 9, 2025, from https://docs.tenable.com/nessus/Content/DeploymentConsiderations.htm

NCCIC ICS_FactSheet_Packets_S508C.pdf. (n.d.). Retrieved March 9, 2025, from https://www.cisa.gov/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_Packets_S508C.pdf

Nikto | CISA. (n.d.). Retrieved March 9, 2025, from https://www.cisa.gov/resources-tools/services/nikto

Nikto 2.5 | CIRT.net. (n.d.). Retrieved March 9, 2025, from https://cirt.net/nikto2

Nmap Network Scanning. (n.d.). Retrieved March 9, 2025, from https://nmap.org/book/toc.html

Team, C. W. (2023, June 22). *What is Metasploit: Tools, Uses, History, Benefits, and Limitations*. Cyber Security News. https://cybersecuritynews.com/what-is-metasploit/

Wireshark · About. (n.d.). Wireshark. Retrieved March 9, 2025, from https://www.wireshark.org/about.html