Student: Tania Diaz

Date: 09/21/2025

Course: CIST-2881-D1

Assignment: Penetration Testing Tools Assignment

1. What tools are available to administrators?

Some common penetration testing tools are Kali Linux, Nmap, Metasploit, Burp Suite, and Wireshark. These tools help administrators find vulnerabilities and test the security of systems.

2. Comparison Table

Tool	Requirements	How it works	Info it provides	When to use it
Kali Linux	Linux OS, 2GB RAM	Full suite, command-line	Vulnerabilities, scripts	Full penetration tests
Nmap	Windows/Linux/Mac, network access	Network scanner	Open ports, services, network map	Network discovery and scanning
Metasploit	Ruby, 4GB RAM	Exploit framework	Exploit results, logs, payloads	Testing known vulnerabilities
Burp Suite	Java, 2GB RAM	Web app testing	Web traffic, vulnerability reports	Web application security assessments
Wireshark	Windows/Linux/Mac, network access	Packet analyzer	Network traffic, protocols	Network traffic analysis and troubleshooting

3. Requirements to run the tools

Kali Linux: Linux OS, 2GB RAM, basic command line knowledge.

Nmap: Network access, works on Windows, Linux, Mac.

Metasploit: Ruby environment, at least 4GB RAM.

Burp Suite: Java installed, at least 2GB RAM.

Wireshark: Network access, works on Windows, Linux, Mac.

4. Differences in approach

Kali Linux: Comprehensive suite for various penetration testing tasks.

Nmap: Focuses on network scanning and discovery.

Metasploit: Specializes in exploiting known vulnerabilities.

Burp Suite: Designed for web application security testing.

Wireshark: Analyzes network traffic and protocols.

5. Information produced for the administrator

Kali Linux: Provides vulnerability reports and scripts for testing.

Nmap: Outputs open ports, services, and network topology.

Metasploit: Generates exploit results, session logs, and payload information.

Burp Suite: Delivers web application vulnerabilities and HTTP/HTTPS traffic analysis.

Wireshark: Captures network packets and provides protocol details.

6. When should the administrator use it

Kali Linux: For comprehensive penetration testing.

Nmap: To discover devices and check open ports.

Metasploit: To test defenses against known vulnerabilities.

Burp Suite: For testing web applications for security issues.

Wireshark: To analyze network traffic or troubleshoot network problems.

References

Kali Linux: https://www.kali.org/?utm_source=chatgpt.com

Nmap: https://nmap.org/book/toc.html?utm_source=chatgpt.com

Metasploit: https://www.metasploit.com/?utm_source=chatgpt.com

Burp Suite: https://portswigger.net/burp/pro?utm_source=chatgpt.com

Wireshark:
https://www.wireshark.org/docs/wsug_html_chunked/ChIntroPlatforms.html?utm_source=chatgpt.com