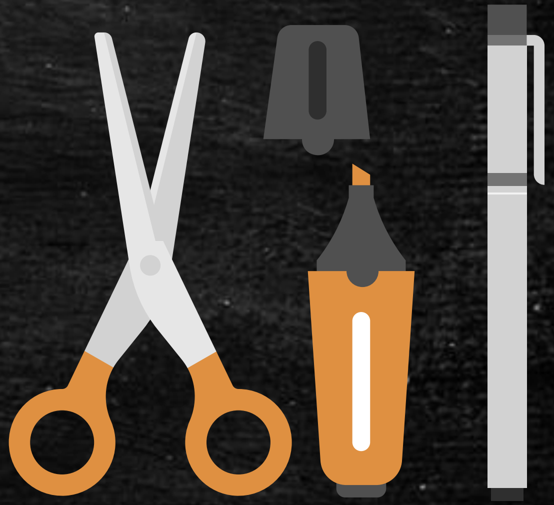
Penetration Tools

Team 1

Penetration tools discussed

- Metasploit
- Nessus Vulnerability Scanner
- Nmap
- Burp Suite
- OWASP ZAP
- SQLmap
- Kali Linux
- Jawfish



Metasploit

- Open source framework
- Support custom modules, test tools that test for weaknesses in operating systems and applications
- Comes with installer
- offers both a Ruby interface and a CLI, GUI available
- License: BSD-3-clause
- Good documentations and learning materials

Nessus Vulnerability Scanner

- signature-based tool for locating vulnerabilities
- can only compare scans to a database of known vulnerability signatures
- GUI available
- More than 450 compliance and configuration templates available
- Available on Raspberry Pi
- Configurable reports
- Easily transferable license between computers

Nmap

- Open source
- Can determine the types of computers, servers, and hardware the enterprise has on its network
- search for hosts, open ports, software versions, operating systems, hardware versions, and vulnerabilities
- has a scripting feature and is useful for enumerating user access
- GUI available
- Installer available

Burp Suite

- maps and analyzes web applications, finding and exploiting vulnerabilities
- automates repetitive functions while retaining user choice where the pen tester needs to have control of individualized options for testing
- investigates cross site scripting and other vulnerabilities using a proxy
- Enterprise edition, professional and community edition

OWASP ZAP

- offers automated and manual web application scanning
- open source tool now available on GitHub
- port scanning, brute force scanning, and fuzzing
- intuitive GUI
- Installer available
- is not as feature rich as Burp Suite, but is free and open source

SQLmap

- open source
- automates the discovery of SQL Injection holes
- python commands in a command line
- installs on Ubuntu Linux, inside a VM

Kali Linux

- all-in-one tool comprising a suite of dedicated, pre-installed penetration testing (and security and forensics) tools
- comes with a lot of user documentation
- free of charge, open source

Jawfish

- uses genetic algorithms
- does not require a signature database
- GUI available
- entirely new and not vetted for enterprise adoption

Comparison

Tool	Ease of install	Ease of use	Flexibility	Licensing	Privacy	Reputation
Metasploit	5	4	5	5	4	5
Nessus Vulnerability Scanner	5	5	3	3	4	4
Nmap	4	3	3	5	4	4
Burp Suite	5	5	3	3	4	5
OWASP ZAP	5	5	4	5	4	4
SQLmap	4	3	5	5	4	4
Kali Linux	5	4	5	5	4	4
Jawfish						3

References

Geer, D. (2015) 8 Penetration Testing Tools That Will Do the Job. (Network World)

Metasploit. (N.D.) Metatsploit. Available from: https://www.metasploit.com/ [Accessed on 15 Apr 2022]

Tenable (N.D.) DataSheet - Nessus Professional. Available from: https://static.tenable.com/marketing/datasheets/DataSheet-Nessus_Professional.pdf [Accessed on 15 Apr 2022]