INFORMATION SECURITY MANAGEMENT LAB

NAME: NAMIT MEHROTRA
REG NO:.21BCE0763
SLOT: L29+L30

EXPERIMENT-1
STUDY OF ISM TOOLS

1. Nmap

Description:

Nmap, short for Network Mapper, is your free and open-source network exploration and security auditing tool. Think of it as a powerful flashlight illuminating the hidden devices, services, and vulnerabilities lurking within your network.

Download :

- Link: https://nmap.org/download

Feasibility:

- System Requirements: Runs on major operating systems like Windows, Linux, and macOS. Lightweight and requires minimal resources.
- Skill Level: Beginner-friendly with basic features, but advanced options require network security knowledge and penetration testing methodologies.
- Ethical Use: Authorized scanning on systems you have permission for is crucial. Misuse for illegal purposes can have serious consequences.
- Open source (available under the Nmap Public Source License)
- Platforms: Linux, Windows, Mac OS X, and other UNIX platforms

Applications:

- Network discovery: Identifying active devices on a network
- Port scanning: Discovering open ports and running services
- Service and operating system detection: Fingerprinting applications and identifying underlying OS
- Security auditing: Vulnerability scanning and network security assessment
- Network inventory and monitoring: Tracking changes in network devices and services

Experiments:

- Scan your own network to understand its composition and identify potential vulnerabilities.
- Perform basic port scans on external targets (with proper authorization).

- Use advanced techniques like OS detection and version scanning.
- Experiment with scripting and automation using the Nmap Scripting Engine (NSE).

Basic Skills Needed to Use the Tool:

- Basic understanding of networking concepts like IP addresses, ports, and protocols
- Familiarity with the command line interface (CLI)
- Willingness to learn and experiment
- Important Note: Always use Nmap responsibly and ethically. Do not scan networks without proper authorization.

Additional Resources:

- Nmap documentation: https://nmap.org/docs.html
- Nmap tutorial: https://nmap.org/book/
- Nmap Scripting Engine (NSE): https://nmap.org/book/man-nse.html

Nmap uses different techniques to perform scanning, including: TCP connect() scanning, TCP reverse ident scanning, FTP bounce scanning and so on.

2. Wireshark

Description:

- Wireshark is one of the tools which is used globally by many for analyzing network protocol. This tool will help you to capture using pcap, store and analyze each packet in a detailed fashion. Wireshark supports OS platforms like Windows, Linux, Solaris, macOS etc. Wireshark is also an open-source tool similar to the tcpdump with a user interface option. The main features of Wireshark are that real-time data can be analyzed from different types of protocols. Also colour coding feature is available in the platform to show the packets when it matches any specific rule. This tool will capture packets only from the pcap-supported networks.

DOWNLOAD:

LINK: https://www.wireshark.org/download.html

Feasibility:

- System Requirements: Windows, Linux, macOS, and other Unix-like platforms. Minimum specs are modest, but performance improves with more RAM and a faster CPU.
- Skill Level: Beginner-friendly interface and extensive resources, but understanding network protocols and packet analysis helps for advanced features.

- Ethical Use: Crucial to capture traffic only on authorized networks with proper permission.

Applications:

- Network Troubleshooting: Analyze network traffic to diagnose slowdowns, connection drops, and performance bottlenecks.
- Security Analysis: Monitor traffic for suspicious activity, detect vulnerabilities, and investigate potential threats.
- Software Development: Test and debug network protocols and applications, analyze data flow, and understand network behavior.
- Education and Training: Learn about network protocols, gain practical experience in network analysis, and prepare for network certifications.

Experiments:

- Analyze your internet traffic to understand data exchange and privacy implications.
- Examine website communication to see how data flows and websites operate.
- Study network protocols like TCP/IP, DNS, or HTTP to learn their inner workings.
- Simulate network attacks like ARP spoofing or DNS poisoning for educational purposes.

Open Source or Not:

Wireshark is completely open-source and free to use, making it accessible to everyone. Its open-source nature also fosters continuous development and improvement by the community.

Basic Skills Needed to Use That Tool:

To get started with Wireshark, you'll need basic computer literacy and a fundamental understanding of networking concepts. Familiarity with TCP/IP, network protocols, and basic packet analysis principles will be beneficial. As you delve deeper, knowledge of scripting languages like Lua can unlock advanced features.

Wireshark is a powerful tool that can unlock a fascinating world of network communication. Whether you're a seasoned network pro or a curious beginner, Wireshark offers valuable insights and endless learning opportunities.

3. Metasploit

DESCRIPTION:

- Metasploit is a powerful and famous open-source penetration testing tool used in cyber security industry. This tool will be used by cyber attackers and as well as cyber defenders. All that matters is that how they use the tool. Metasploit has many inbuilt modules which can be used for exploiting, payload executions, auxiliary functions, encoding, listening, executing shell codes, Nops. This tool can be used to perform security assessments that enhance the company's security posture.
- Metasploit is a powerful open-source penetration testing framework that helps security professionals identify and exploit vulnerabilities in computer systems. It provides a vast collection of exploits, payloads, auxiliary modules, and encoders that can be used to simulate real-world attacks and assess the security posture of networks and systems.

DOWNLOAD:

Link: https://www.metasploit.com/

Feasibility:

- System Requirements: Windows, Linux, macOS, and other Unix-like platforms. Minimum specs are modest, but performance improves with more RAM and a faster CPU.
- Skill Level: Beginner-friendly interface and extensive resources, but understanding network protocols and packet analysis helps for advanced features.
- Ethical Use: Crucial to capture traffic only on authorized networks with proper permission.

Applications:

- Penetration Testing: Simulate real-world attacks to identify and exploit vulnerabilities in networks and systems.
- Vulnerability Research: Develop and test new exploits for known vulnerabilities.
- Security Awareness Training: Demonstrate the potential consequences of security vulnerabilities to raise awareness among users and administrators.
- Malware Analysis: Analyze malware samples to understand their functionality and how they work.

Experiments:

- Exploiting web applications: Use web-based exploits to gain access to vulnerable web servers.

- Escalating privileges: Once you have gained initial access to a system, use privilege escalation exploits to gain higher levels of access.
- Lateral movement: Move laterally through a network once you have gained access to a single system.
- Developing custom exploits: Use Metasploit's scripting language to develop your own exploits for specific vulnerabilities.

Basic Skills Needed to Use That Tool:

- Strong understanding of network security concepts: This includes knowledge of operating systems, networking protocols,.
- Familiarity with scripting languages like Ruby can be helpful, but not required.
- Strong critical thinking and problem-solving skills.
- Knowledge of ethical hacking principles and responsible use of security tools.

4. Burpsuite:

DESCRIPTION:

Burp suite is a combined platform of several tools which are used in the penetration testing field. This is the favourite tool for all pen testers and bug bounty hunters. This tool was developed by the company “Port Swigger”. There are various tools like Spider, Proxy, Intruder, Repeater, Sequencer, Decoder, Extender, Scanner etc., which are used for different security testing processes. This tool can be used at project-level as well as at user-level.

Download

LINK: https://portswigger.net/burp/download: https://portswigger.net/burp/download

Feasibility (System Requirements and More):

- System Requirements:
- Operating System: Windows, Linux, macOS
- Java: Version 8 or later (required for all editions)
- Memory: 4 GB RAM minimum, 8 GB or more recommended for optimal performance
- CPU: 2 GHz or faster recommended
- Disk Space: 200 MB for installation, additional space for logs and project data
- Skill Level:
- Beginner: Intuitive interface and guided tutorials for learning web security fundamentals. Basic manual testing features are easy to grasp. Requires basic computer literacy and willingness to learn.

- Intermediate: Advanced features like automated scanning and vulnerability identification may require experience with web security concepts and tools. Understanding of HTTP and web technologies is beneficial.
- Security Professional: Comprehensive customization options and extension capabilities cater to specific needs and advanced penetration testing. Strong technical expertise and knowledge of web application security are essential.
- **Open Source or Not:**
- Community Edition: Free and open-source, offering core features like manual interception, proxy, and basic scanning.
- Professional Edition: Paid version with additional features like automated scanners, intruder for fuzzing, and advanced extensions.
- Enterprise Edition: Scaled version for large organizations with advanced collaboration features and centralized management.
- **Applications:**
- Manual Testing: Intercept and analyze HTTP requests and responses to identify vulnerabilities like SQL injection or XSS.
- Automated Scanning: Utilize built-in or custom scanners to detect common vulnerabilities in web applications.
- Fuzzing: Test applications with invalid data to uncover unexpected behavior and potential vulnerabilities.
- Penetration Testing: Simulate real-world attack scenarios to assess the overall security posture of web applications.
- Security Awareness Training: Demonstrate vulnerabilities and attack techniques to educate users and developers.
- **Experiments Available:**
- Analyze your own website traffic to understand data exchange and identify potential security concerns.
- Test a public vulnerability in a publicly available web application for educational purposes (with proper permission).
- Build your own custom extension to automate specific tasks or analyze data in new ways.
- **Basic Skills Needed:**
- Basic understanding of HTTP and web technologies: Familiarity with how web applications work and communicate will be helpful.
- Computer literacy and ability to learn new tools: Burp Suite offers extensive documentation and tutorials, but basic tech skills are necessary.

- Ethical mindset: Remember, responsible use is crucial. Always use Burp Suite on authorized systems and networks with proper permission.

5. Aircrack-NG:

DESCRIPTION:

Aircrack-ng is an open-source project, and its source code is available on various platforms, including GitHub. You can obtain the latest version of the software by visiting the official repository. The source code is typically distributed under the GNU General Public License (GPL), ensuring that it remains free and open for users to modify and distribute .

DOWNLOAD:

Link: https://www.aircrack-ng.org/

Feasibility:

System Requirements:

- OperatingSystem: Windows, Linux, macOS, FreeBSD, OpenBSD, NetBSD, Solaris, eCo mStation 2
- Hardware: Requires a wireless network interface controller (NIC) that supports raw monitoring mode.

Skill Level:

- Basic: Aircrack-NG has a simple interface that makes it easy to use for basic tasks like monitoring traffic and cracking WEP keys.
- Intermediate: Advanced features like WPA/WPA2 cracking and packet injection require more technical knowledge and experience.

Ethical Use:

- Only use Aircrack-NG on authorized networks with proper permission. Misuse for illegal or unauthorized purposes can have serious consequences.

Applications:

- Network Analysis: Monitor traffic to identify vulnerabilities and potential threats.
- Penetration Testing: Simulate real-world attacks to assess network security.
- Security Auditing: Identify and fix security vulnerabilities.
- Research: Develop new security tools and techniques.

Experiments:

- Analyze traffic from your own network to understand how it works and identify potential security concerns.
- Crack a WEP key from a public wireless network for educational purposes (with proper permission).

- Simulate a WPA/WPA2 attack on a vulnerable network.

Basic Skills Needed:

- Basic understanding of network protocols: Familiarity with how wireless networks work will be helpful.
- Computer literacy and ability to learn new tools: Aircrack-NG offers extensive documentation and tutorials, but basic tech skills are necessary.
- Ethical mindset: Remember, responsible use is crucial. Always use Aircrack-NG on authorized networks and with proper permission.

Basic Skills Required:

Basic understanding of networking concepts (TCP/IP, OSI Model, protocols (TCP, UDP, IP, Ethernet))

- Familiarity with wireless security concepts (WEP, WPA/WPA2-PSK)
- Ability to interpret packet capture data
- Strong critical thinking and problem-solving skills

• A security analyst can use Aircrack-ng to identify wireless networks that are using weak or default passwords.

• A penetration tester can use Aircrack-ng to crack the password of a wireless network as part of a security assessment.

• A forensic investigator can use Aircrack-ng to collect evidence of a wireless attack.

• Aircrack-ng is a valuable tool for anyone who needs to assess the security of wireless networks. It is a powerful tool, but it should be used responsibly