Information Security Lab
Lab 1

Report

The following tools were studied and analyzed in this lab:

- **Kali Linux**

A Debian-based Linux Distribution, designed for use in information security, digital forensics, penetration testing and ethical hacking.

Features:

1. Pre-installed with hundreds of security and ethical hacking tools.
2. Highly customizable, allowing users to tailor the environment to specific testing needs.
3. Supports multiple platforms including ARM devices, making it useful for several types of hardware devices.
4. Regularly updated to include the latest security patches and tools.
5. Has a live boot option, enabling users to run the system without installation.
6. A large community and extensive documentation are provided to users.

- **Metasploit**

  An open-source framework to develop test and use exploit code against remote targets. Often used in penetration testing and ethical hacking to find vulnerabilities.

  Features:

  1. Huge library of exploits, payloads etc. for automated security assessment.

2. Supports automation to allow users to create automated and repeatable testing workflows.
3. Integration with other tools allows for more versatility.
4. Both command line and GUI options for a user-friendly interface.

- **Burp Suite**
  A proprietary tool for security assessment and penetration testing of web applications.

  Features:

  1. Acts as a proxy server to intercept and modify HTTP requests in real-time.
  2. Captures site maps via automatic or manual web crawling.
  3. Logs HTTP request and response history for review.
  4. Burp Repeater allows repeated sending of customized HTTP requests quickly to test vulnerabilities, especially those caused by race conditions.
  5. Burp Decoder automates encoding and decoding of formats like Base64, Hex, GZIP, etc. *Smart Decode* option allows for automated decoding.
  6. Burp Sequencer analyses token randomness for security strength.
  7. Burp Comparer compares differences between HTTP requests or responses.

- **OWASP**
  The Open Worldwide Application Security Project is a community producing articles, methodologies, tools etc. for ethical hacking and cybersecurity, especially for IoT, system software and web security.

- **OWASP ZAP**
  A penetration testing tool developed by OWASP Foundation to detect vulnerabilities in web apps.

  Features:

  1. Provides active or passive scans. Passive scans scan HTTP requests and responses to find vulnerabilities but cannot change any requests. Active scans can send requests to test edge case behavior and find hidden vulnerabilities effectively.

2. Supports various authentication formats, configured before running a scan.
3. Monitors WebSockets to find and exploit full-duplex vulnerabilities.
4. The OWASP ZAP Fuzzer sends large volumes of unexpected data to the server to ensure secure and robust behavior.

- ## Ettercap

  A comprehensive network security tool focused on man-in-the-middle (MITM) attacks.

  Features:

1. Supports active and passive network sniffing on LANs.
2. Capable of intercepting, modifying, and injecting packets in real-time.
3. Includes features like ARP poisoning to redirect traffic through the attacker's machine.
4. Provides protocol analysis and filtering for various network protocols.
5. Offers both command-line and graphical user interfaces for flexibility.
6. Works on multiple platforms including Linux and Windows.

- ## Hydra

Hydra is an open source password cracking tool used for login bypasses.

Features:

1. Can perform parallelized login attempts to speed up cracking using multiple Hydra heads.
2. Allows use of custom wordlists and username lists for targeted dictionary attacks.
3. Supports both online and offline password gaming.
4. Highly configurable with options to adjust timing and retries. .

- ## Mosquitto

  An open-source MQTT (Message Queuing Telemetry Transport) broker used for lightweight messaging.

  Features:

1. Designed for efficient communication between IoT (Internet of Things) apps via TLS.
2. Enables publish/subscribe messaging pattern for real-time data exchange.
3. Lightweight and optimized for low-bandwidth, high-latency networks.
4. Provides features like authentication, authorization, and TLS encryption for secure communication.
5. Easy to install and configure, making it popular in IoT projects and testing environments.

- **Nmap**

  Nmap, i.e. Network Mapper, is a software used to discover hosts and services on a network by sending requests.

  Features:

  1. Performs scans to identify all services and hosts connected to a network, along with ping scans and port scans for identifying exposed ports.
  2. TCP/IP Stack fingerprinting to determine hardware and OS details of network devices.
  3. Scriptable using Nmap Scripting Engine(NSE), allowing for custom scripts to find vulnerabilities.
  4. Additional features including DNS name reversal, MAC address lookups, etc.

- **Netcat**

A simple utility for reading and writing to network connections using TCP or UDP.

Features:

1. Can act as a port scanner, proxy, or chat server.
2. Useful for banner grabbing and transferring files.
3. Supports listening mode to create backdoors or shells.
4. Simple command-line tool, widely available.

- **SQLMap**

  An open-source penetration testing tool that automates the process of detecting SQL Injection vulnerabilities.

  Features:

1. Supports various database management systems (MySQL, Postgres, MSSQL, Oracle, etc.).
2. Automated detection of injectable parameters.
3. Offers techniques for data extraction, database fingerprinting, and takeover.
4. Supports bypassing WAFs and filters.

- **SQLNinja**
  Another SQL Injection exploitation tool specifically designed to exploit vulnerabilities on Microsoft SQL Server.

  Features:
  1. Automates exploitation and post-exploitation assessment on MSSQL.
  2. Supports techniques like OS command execution and file uploads.
  3. Performs data extraction, system admin password cracking, etc.
  4. Focuses on MSSQL-specific attack vectors.
  5. Integrates with other tools like Metasploit.

- **MSFVenom**

This Payload generator is a part of the Metasploit framework and is used to create custom payloads for penetration testing.

Features:

1. Combines payload generation and encoding.
2. Supports various platforms (Windows, Linux, macOS, Android).
3. Can generate payloads in multiple formats including executables, scripts, etc.
4. Can encode payloads to evade antivirus detection.

- **Microsoft threat modeling tool**

This is a free tool designed by microsoft to help developers identify and mitigate security threats during software design.

Features:

1. Uses the STRIDE threat model, which includes:

    - **Spoofing:** An attacker pretending to be another party to gain unauthorized access to a resource.
    - **Tampering:** Unauthorized modification of confidential information or code.
    - **Repudiation:** User denying an action committed by them.
    - **Information Disclosure:** Exposing sensitive information to unauthorized users.
    - **Denial of Service:** Preventing legitimate users from accessing a service.
    - **Elevation of Privilege:** Gaining higher access rights than allowed.
2. Provides templates and automated threat identification.
3. Integrates with development workflows and helps create visual threat models.

- ## PyCharm Community Edition

PyCharm Community is a free, open-source Integrated Development Environment (IDE) for Python development.

Key features:

- Code editor with syntax highlighting, automated code completion, and refactoring tools.
- Integrated debugger and interpreter to run Python code.
- Support for version control systems like Git.
- Lightweight and contains extensive documentation along with a large community.

Aditya Chopra

CCE – B

230953156

IS Lab (B1)