# Vulnerability Analysis Module-5

by Durgesh Thakare

# Vulnerability Analysis

Vulnerability Analysis, often part of the scanning phase, is the process of examining, discovering, and identifying security measures and weaknesses in systems and applications. It aims to assess the potential vulnerabilities that could be exploited by malicious actors.

# Types of Vulnerability Assessment

1. **Active Assessment**: Actively sends requests to the live network and examines the responses.
2. **Passive Assessment**: Involves packet sniffing to discover vulnerabilities, running services, open ports, and other information.
3. **External Assessment**: Focuses on finding vulnerabilities from an external perspective to exploit them from the outside.
4. **Internal Assessment**: Involves discovering vulnerabilities by scanning the internal network and infrastructure.

**Other Types of Vulnerability Assessment include:**

**Application Assessment**

Focused on identifying vulnerabilities within specific applications.

**Host-based Assessment**

Concentrates on individual systems or hosts.

**Network-Based Assessment**

Evaluates vulnerabilities across the network.

**Wireless Network Assessment**

Targets wireless networks and devices for potential weaknesses.

# Vulnerability Classification

Vulnerability classification categorizes vulnerabilities based on various attributes, including their impact, severity, and how they are exploited. Common vulnerability classification systems help security professionals understand and prioritize vulnerabilities for mitigation. Here are some common vulnerability classifications:

1. **CVSS (Common Vulnerability Scoring System)**:
    - CVSS is a widely used system for rating and ranking vulnerabilities based on their impact and severity. It provides a numerical score to represent the risk level of a vulnerability.
    - CVSS metrics include Base, Temporal, and Environmental scores, which assess the exploitability, impact, and context of a vulnerability.
    - The scores range from 0.0 (no impact) to 10.0 (maximum impact), and vulnerabilities are typically classified into severity levels: None, Low, Medium, High, and Critical.
2. **CWE (Common Weakness Enumeration)**:
    - CWE is a community-developed list of software and hardware weaknesses that can lead to security vulnerabilities.
    - CWE categorizes vulnerabilities based on the types of weaknesses and their associated risk.
    - It provides a reference guide for identifying and addressing specific security issues within software and hardware.
3. **OWASP Top Ten**:
    - The OWASP (Open Web Application Security Project) Top Ten is a list of the most critical web application security vulnerabilities.
    - It classifies vulnerabilities commonly found in web applications, such as injection attacks, broken authentication, and security misconfigurations.
    - These vulnerabilities are ranked based on their prevalence and impact.
4. **NVD (National Vulnerability Database) Categories**:
    - NVD, maintained by NIST (National Institute of Standards and Technology), categorizes vulnerabilities based on various attributes, including product type, vendor, and impact.
    - Vulnerabilities are assigned unique CVE (Common Vulnerabilities and Exposures) identifiers and are linked to specific products and versions.
5. **Exploitability Categories**:
    - Vulnerabilities can be categorized based on how easily they can be exploited. Categories may include:
        - Low Exploitability: Difficult to exploit and requires special conditions.
        - Medium Exploitability: Requires some effort or specific conditions.
        - High Exploitability: Easily exploitable with little effort.
6. **Impact Categories**:
    - Vulnerabilities can also be categorized based on their potential impact on systems or data. Categories may include:
        - Low Impact: Minimal or no impact on the system or data.
        - Moderate Impact: Some impact that can be mitigated.
        - High Impact: Significant impact, potentially leading to data loss or system compromise.
7. **Industry-Specific Categories**:
    - Some industries, such as healthcare (HIPAA) or finance (PCI DSS), have specific vulnerability classification systems tailored to their regulatory requirements and risks.

# Vulnerability Scoring Systems

**Common Vulnerability Scoring System**

**mmon Vulnerability Scoring System (CVSS)**:

- Provides a way to capture the principal characteristics of a vulnerability and produces a numerical score reflecting its severity.
- Security Rating:
  - None (0.0)
  - Low (0.1 - 3.9)
  - Medium (4.0 - 6.9)
  - High (7.0 - 8.9)
  - Critical (9.0 - 10.0)

# Common Vulnerabilities and Exposures (CVE)

- Maintains a list of known vulnerabilities, each identified by a unique number, along with descriptions of cybersecurity vulnerabilities.
- Websites:

cve.mitre.org

**CVE - CVE**

The mission of the CVE® Program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities.

www.exploit-db.com

**OffSec's Exploit Database Archive**

The Exploit Database - Exploits, Shellcode, 0days, Remote Exploits, Local Exploits, Web Apps, Vulnerability Reports, Security Articles, Tutorials and more.

# National Vulnerability Database (NVD)

- A U.S. government repository of standards-based vulnerability management data, enabling automation of vulnerability management, security measurement, and compliance.
- Website:

nvd.nist.gov

**NVD - Home**

CVE-2020-19189 - Buffer Overflow vulnerability in postprocess_terminfo function in tinfo/parse_entry.c:997 in ncurses 6.1 allows remote attackers to cause a denial of service via crafted command. Published: August 22, 2023;...

# Vulnerability Assessment Tools

Several tools are available for conducting vulnerability assessments, including:

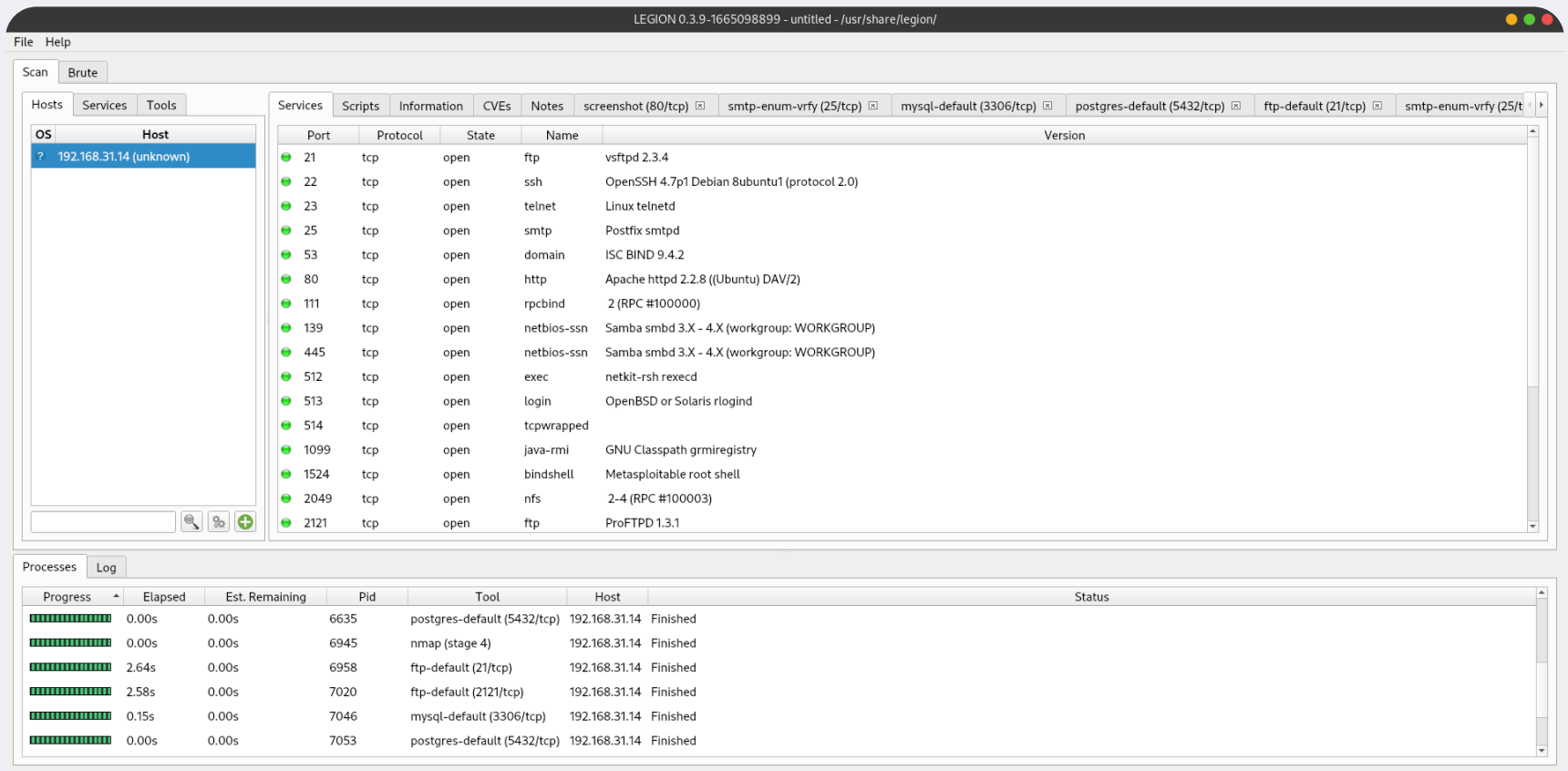
1. **Nessus**
2. **OpenVAS**
3. **Nexpose**
4. **Retina**
5. **GFI LanGuard**
6. **Qualys FreeScan**
7. **Acunetix**
8. **Nikto (Web Vulnerability Scanner)**
9. **NMap**
10. **Legion (Graphical Web Vulnerability Scanner)**

# Legion

Legion is a powerful open-source tool for conducting comprehensive and efficient security assessments of web applications. It is designed to assist cybersecurity professionals, penetration testers, and ethical hackers in identifying vulnerabilities and potential security issues within web applications. Here's some key information about Legion:

**Key Features of Legion:**

1. **Comprehensive Scanning:** Legion provides a wide range of features for scanning and assessing web applications. It can identify common web vulnerabilities, misconfigurations, and other security issues.
2. **User-Friendly Interface:** Legion offers a user-friendly graphical user interface (GUI), making it accessible to both experienced and less experienced security professionals.
3. **Active and Passive Scanning:** It supports both active scanning (where it interacts with the target web application) and passive scanning (where it observes and analyzes network traffic and interactions without direct interaction).
4. **Customization:** Users can customize the tool's settings and configurations to suit their specific assessment needs. This allows for fine-tuning scans to focus on specific vulnerabilities or areas of concern.
5. **Scanning Profiles:** Legion provides predefined scanning profiles, making it easier to select the appropriate configuration for different types of web applications.
6. **Report Generation:** It generates detailed and well-structured reports that highlight vulnerabilities, severity, and recommended remediation steps. These reports are often useful for communication with stakeholders.
7. **Integration:** Legion can be integrated with other tools and frameworks, offering flexibility and interoperability for the user.
8. **Web Proxy:** It can function as a web proxy, allowing users to intercept, inspect, and manipulate HTTP requests and responses.
9. **Authentication Support:** It can handle various forms of authentication, including session management and handling cookies.
10. **Extensibility:** Legion can be extended with plugins, making it adaptable to specific assessment needs.



# AutoPWN Suite

**AutoPWN Suite is a project for scanning vulnerabilities and exploiting systems automatically.**

## Features

- Fully automatic
- Detect network IP range without any user input.
- Vulnerability detection based on version.
- Web app vulnerability testing. (LFI, XSS, SQLI)
- Web app dirbusting.
- Get information about the vulnerability right from your terminal.
- Automatically download exploit related with vulnerability.
- Noise mode for creating a noise on the network.
- Evasion mode for being sneaky.
- Automatically decide which scan types to use based on privilege.
- Easy to read output.
- Specify your arguments using a config file.
- Send scan results via webhook or email.
- Works on Windows, MacOS and Linux.

## Installation

```
sudo pip install autopwn-suite
```

## Usage

Automatic mode

```
autopwn-suite -y
```