Vulnerability Analysis

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 analyze live network responses.
    - Proactively identifies vulnerabilities.
2. **Passive Assessment:**
    - Uses packet sniffing to discover vulnerabilities and open ports.
    - Observes network traffic without active engagement.
3. **External Assessment:**
    - Identifies vulnerabilities from an external perspective.
    - Focuses on potential external exploits.
4. **Internal Assessment:**
    - Discovers vulnerabilities through internal network scanning.
    - Assesses risks from within the organizational environment.

Vulnerability Classification

Categorizes vulnerabilities based on attributes like impact, severity, and exploitation methods. Common systems aid in understanding and prioritizing mitigation.

1. **CVSS (Common Vulnerability Scoring System):**
   - Numerical score system (0.0 to 10.0) ranking vulnerabilities by severity.
2. **CWE (Common Weakness Enumeration):**
   - Community list categorizing software and hardware weaknesses leading to vulnerabilities.
3. **OWASP Top Ten:**
   - Lists critical web app vulnerabilities by prevalence and impact.
4. **NVD (National Vulnerability Database) Categories:**
   - Maintained by NIST, categorizes vulnerabilities by attributes, using unique CVE identifiers.
5. **Exploitability Categories:**
   - Rates vulnerabilities by exploit difficulty: Low, Medium, High.
6. **Impact Categories:**
   - Categorizes vulnerabilities by potential impact: Low, Moderate, High.
7. **Industry-Specific Categories:**
   - Tailored systems for specific industries (e.g., HIPAA, PCI DSS) based on regulatory requirements and risk

Vulnerability Scoring – CVSS:

- **Common Vulnerability Scoring System (CVSS):**
  - Captures key characteristics of a vulnerability.
  - Produces a numerical severity score.
- **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.
- Provides descriptions of cybersecurity vulnerabilities.

Websites:

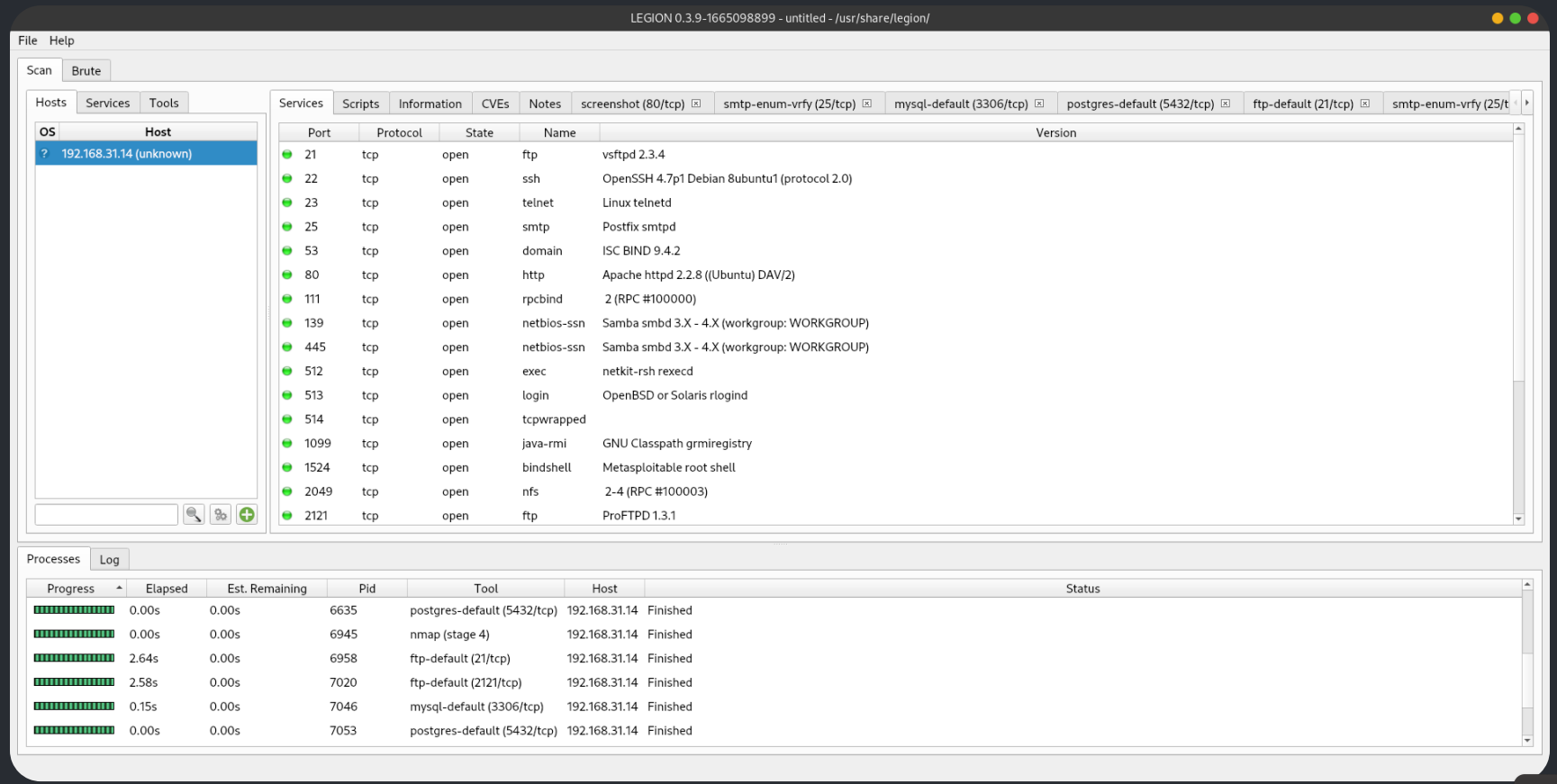
1. **CVE - MITRE**
   - Identifies, defines, and catalogs disclosed cybersecurity vulnerabilities.
2. **Exploit Database**
   - OffSec's archive with exploits, shellcode, 0days, vulnerability reports, and more.
3. **National Vulnerability Database (NVD)**
   - U.S. government repository for standards-based vulnerability data.
   - Enables automation of vulnerability management and security compliance.

Vulnerability Assessment Tools:

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.



AutoPWN Suite

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

Installation

sudo pip install

```
autopwn-suite
```

Usage Automatic mode

```
autopwn-suite -y
```