

### **Phase 3: Identify Vulnerabilities**

#### **1. Tool: Tenable Nessus**

- Description: Nessus is a widely-used vulnerability scanning tool that helps identify security weaknesses in network hosts and applications.
- Usage: Utilize Nessus to perform comprehensive vulnerability scans on target hosts and applications. Configure scan policies to include checks for common vulnerabilities, misconfigurations, and compliance issues. Nessus offers a user-friendly interface and provides detailed reports with prioritized vulnerabilities.

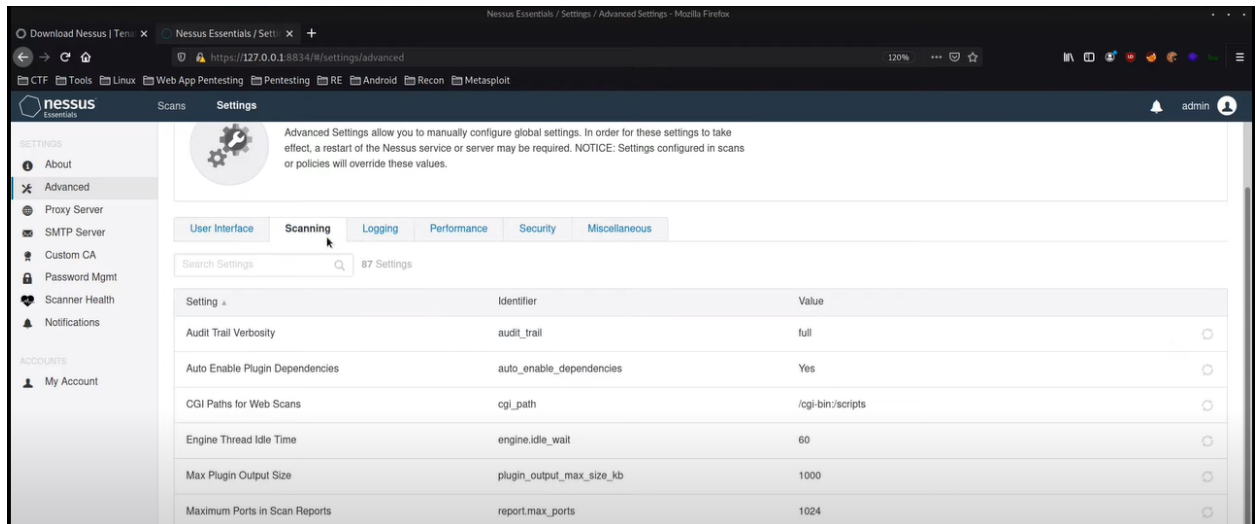
#### ***Pros:***

- Extensive vulnerability coverage with a large vulnerability database.
- User-friendly interface and easy-to-interpret scan reports.
- Provides detailed information on vulnerabilities and suggested remediation steps.

#### ***Cons:***

- Nessus may require a commercial license for full functionality.

- Some advanced features may require additional configuration or expertise to use effectively.



## 2. Tool: OpenVAS

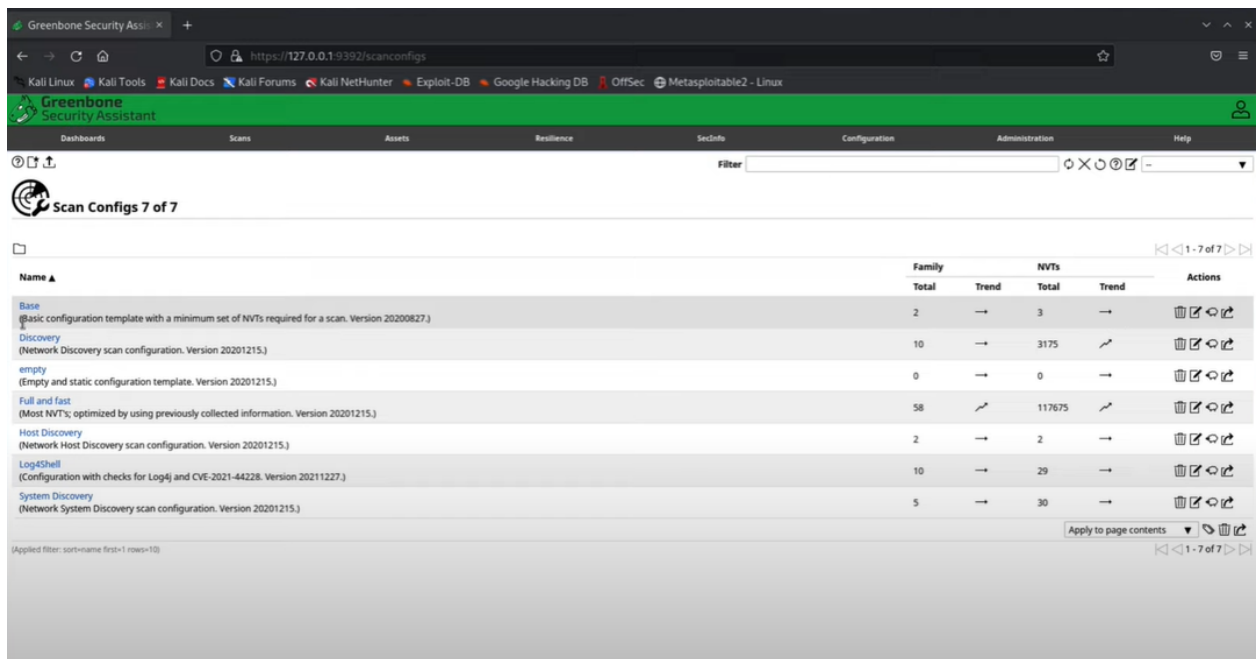
- Description: OpenVAS (Open Vulnerability Assessment System) is an open-source vulnerability scanner that provides similar capabilities to Nessus.
- Usage: Utilize OpenVAS to perform vulnerability scans, identify weaknesses, and generate comprehensive reports. Configure scan policies to target specific technologies, platforms, or compliance requirements.

### Pros:

- Open-source and freely available, making it accessible for various scenarios.
- Comprehensive vulnerability checks with regular updates to the vulnerability database.
- Provides detailed reports with actionable recommendations.

### Cons:

- OpenVAS may require additional setup and configuration compared to commercial alternatives.
- User interface and report generation may not be as polished as commercial tools.



| Name   | Family |       | NVTs   |       | Actions |
|--|--------|-------|--------|-------|---------|
|  | Total  | Trend | Total  | Trend |         |
| Base<br>(Basic configuration template with a minimum set of NVTs required for a scan. Version 20200827.) | 2      | →     | 3      | →     | 🗑️🔍🔗🔗   |
| Discovery<br>(Network Discovery scan configuration. Version 20201215.)                                   | 10     | →     | 3175   | ↗     | 🗑️🔍🔗🔗   |
| empty<br>(Empty and static configuration template. Version 20201215.)                                    | 0      | →     | 0      | →     | 🗑️🔍🔗🔗   |
| Full and fast<br>(Most NVTs; optimized by using previously collected information. Version 20201215.)     | 58     | ↗     | 117675 | ↗     | 🗑️🔍🔗🔗   |
| Host Discovery<br>(Network Host Discovery scan configuration. Version 20201215.)                         | 2      | →     | 2      | →     | 🗑️🔍🔗🔗   |
| Log4Shell<br>(Configuration with checks for Log4j and CVE-2021-44228. Version 20211227.)                 | 10     | →     | 29     | →     | 🗑️🔍🔗🔗   |
| System Discovery<br>(Network System Discovery scan configuration. Version 20201215.)                     | 5      | →     | 30     | →     | 🗑️🔍🔗🔗   |

### 3. Tool: Burp Suite

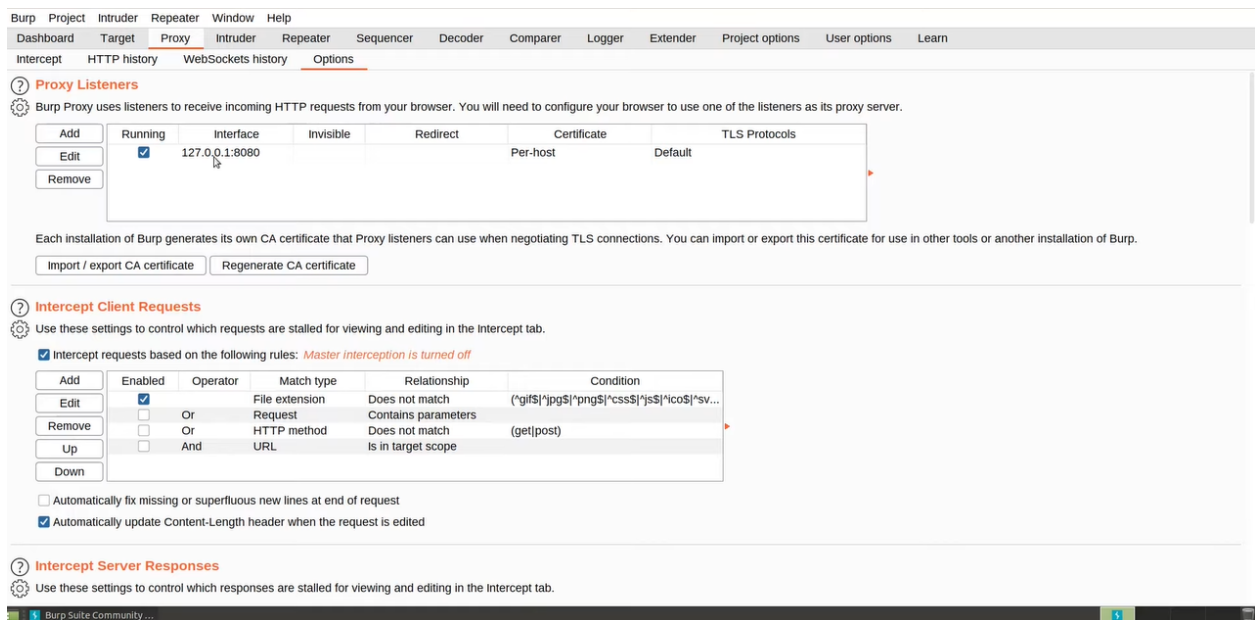
- Description: Burp Suite is a popular web application security testing tool that combines vulnerability scanning, web proxy, and other testing capabilities.
- Usage: Utilize Burp Suite's scanning modules (such as Burp Scanner) to identify vulnerabilities in web applications, including common issues like SQL injection, cross-site scripting (XSS), and insecure direct object references (IDOR). Configure scan settings to fit the target application and testing requirements.

**Pros:**

- Specialized for web application security testing.
- Offers advanced scanning features, such as active and passive vulnerability detection.
- Provides detailed reports and allows for manual verification and exploitation of vulnerabilities.

### Cons:

- Burp Suite is focused on web application security and may not cover vulnerabilities in other areas, such as network infrastructure or endpoints.
- Some advanced features may require expertise to utilize effectively.



## 4. OpenVAS NVT Feed

- Description: OpenVAS Network Vulnerability Tests (NVT) Feed is a collection of vulnerability checks used by OpenVAS to identify security weaknesses.

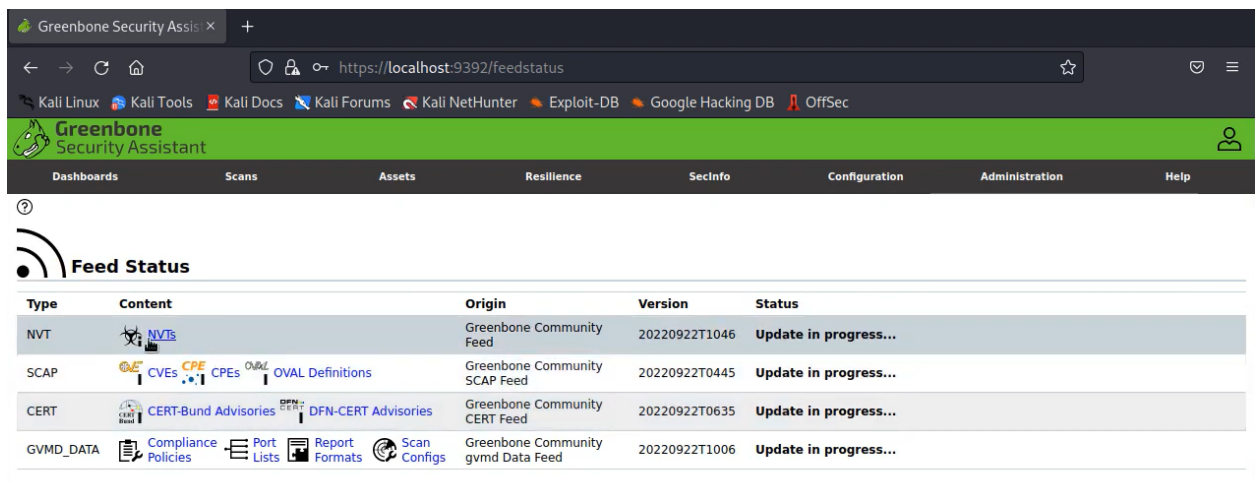
- Usage: Ensure the NVT Feed is regularly updated to incorporate the latest vulnerability checks. Configure OpenVAS to utilize the NVT Feed during scans to identify vulnerabilities specific to target technologies, platforms, or compliance requirements.





### Pros:

- Regularly updated with new vulnerability checks.
- Covers a wide range of technologies and platforms.
- Enhances the effectiveness of OpenVAS vulnerability scans.

### Cons:

- Dependency on the availability and regular updates of the NVT Feed.
- May require additional configuration for customized vulnerability checks.



| Type      | Content  | Origin                            | Version       | Status                |
|-----------|--|-----------------------------------|---------------|-----------------------|
| NVT       |  <a href="#">NVTs</a>   | Greenbone Community Feed          | 20220922T1046 | Update in progress... |
| SCAP      |  <a href="#">CVEs</a> <a href="#">CPE</a> <a href="#">CPEs</a> <a href="#">OVAL</a> <a href="#">OVAL Definitions</a>        | Greenbone Community SCAP Feed     | 20220922T0445 | Update in progress... |
| CERT      |  <a href="#">CERT-Bund Advisories</a> <a href="#">DFN-CERT Advisories</a>   | Greenbone Community CERT Feed     | 20220922T0635 | Update in progress... |
| GVMd_DATA |  <a href="#">Compliance Policies</a> <a href="#">Port Lists</a> <a href="#">Report Formats</a> <a href="#">Scan Configs</a> | Greenbone Community gvm Data Feed | 20220922T1006 | Update in progress... |

## 5. Tool: Nikto

- Description: Nikto is a web server scanning tool that specializes in identifying common web server vulnerabilities and misconfigurations.

- Usage: Utilize Nikto to scan web servers for known vulnerabilities, insecure configurations, and potential issues such as outdated software versions, default pages, or open directories.

### **Pros:**

- Specifically designed for web server vulnerability scanning.
- Provides a comprehensive scan of web servers and their configurations.
- Covers a wide range of common web vulnerabilities and misconfigurations.

### **Cons:**

- Limited to web server scanning and may not cover vulnerabilities in other areas.
- Requires additional manual verification for potential false positives and further analysis.

```

L$ nikto -H

Options:
  -ask+           Whether to ask about submitting updates
                   yes   Ask about each (default)
                   no    Don't ask, don't send
                   auto  Don't ask, just send
  -check6         Check if IPv6 is working (connects to ipv6.google.com or value set in nikto.conf)
  -Cgidirs+       Scan these CGI dirs: "none", "all", or values like "/cgi/ /cgi-a/"
  -config+        Use this config file
  -Display+       Turn on/off display outputs:
                   1     Show redirects
                   2     Show cookies received
                   3     Show all 200/OK responses
                   4     Show URLs which require authentication
                   D     Debug output
                   E     Display all HTTP errors
                   P     Print progress to STDOUT
                   S     Scrub output of IPs and hostnames
                   V     Verbose output
  -dbcheck        Check database and other key files for syntax errors
  -evasion+       Encoding technique:
                   1     Random URI encoding (non-UTF8)
                   2     Directory self-reference (../)
                   3     Premature URL ending
                   4     Prepend long random string
                   5     Fake parameter
                   6     TAB as request spacer
                   7     Change the case of the URL
                   8     Use Windows directory separator (\)

```