**Identify Vulnerabilities**

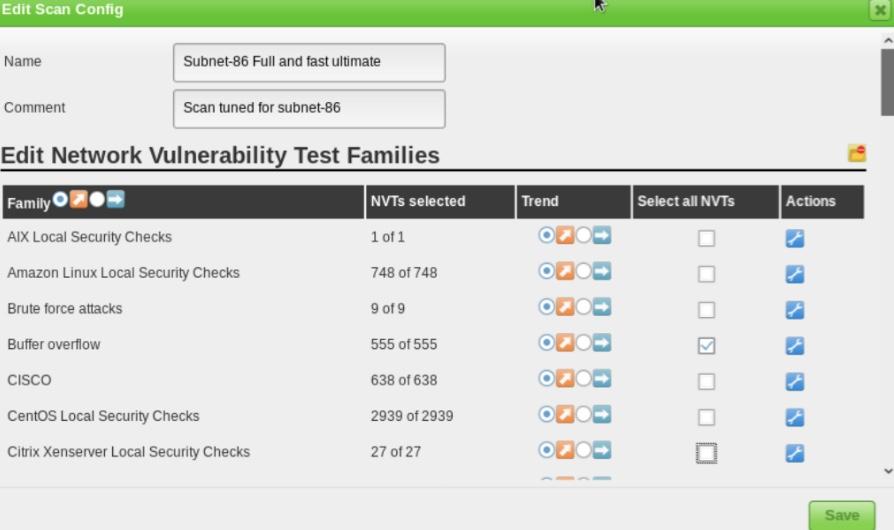
**By: Long Trang**

***Tool 1: OpenVAS***

Description: OpenVAS (Open Vulnerability Assessment System) is a popular open-source vulnerability scanner and management tool used for detecting security vulnerabilities in computer systems and networks. OpenVAS can scan various types of systems, such as web applications, operating systems, and network devices, to identify known security vulnerabilities and weaknesses. OpenVAS uses a combination of active and passive scanning techniques to detect vulnerabilities, including network scanning, service detection, and vulnerability testing. The tool comes with a built-in database of thousands of known vulnerabilities and security issues, which is regularly updated to stay up-to-date with the latest threats.

**How tool will be used:**

1. Perform a network scan to discover all devices on the network.
2. Customize the scan configuration to target specific hosts, servers, and files while excluding the device used by the pentester to avoid any potential false positives.
3. Execute various available scan configurations that differ in speed to minimize the chances of producing inaccurate results, such as full & fast, empty, full & very fast, host discovery, and system discovery scans.
4. Employ the scheduling functionality to conduct regular live scans on a daily basis during different time frames (working hours, after hours, and weekends) in order to identify any unauthorized devices, networks, or IoT devices that may have been connected to the network.





**Pros:**

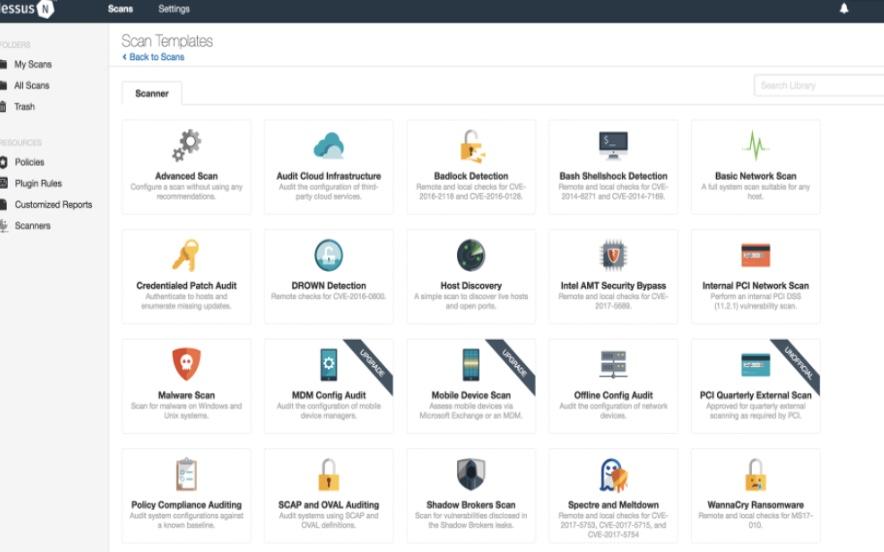
* OpenVAS is an open-source tool, which means that it is free to use, and its source code can be modified and customized according to the user's needs.
* Comprehensive vulnerability database that is constantly updated, making it easier to detect and remediate vulnerabilities.
* Provides detailed reports that can be used to assess the security posture of the organization and prioritize remediation efforts.
* Cons:
* Resource-intensive tool, which means that it can consume a lot of system resources and slow down the performance of the network.
* Can produce false positive results, which can lead to wasted time and effort in investigating and remedying non-existent vulnerabilities.
* Scanning the network with OpenVAS can cause network disruptions or downtime, which can be disruptive to the business operations.

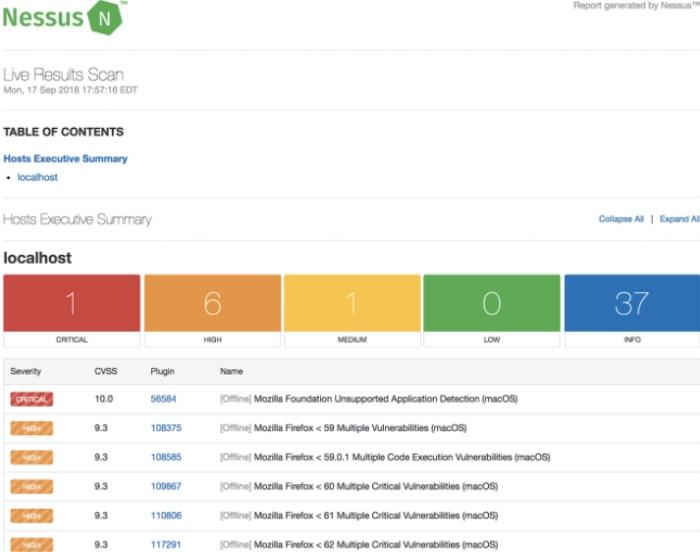
***Tool 2: Nessus***

Description: Nessus is a widely used commercial vulnerability scanner developed by Tenable, Inc. It is designed to help organizations identify and remediate security vulnerabilities in their computer systems and networks. Nessus uses a variety of techniques, including network scanning and credentialed vulnerability scanning, to identify security issues and vulnerabilities. Is known for its extensive vulnerability database, which includes thousands of known vulnerabilities and threats. The tool can be customized to perform specific scans and is often used in compliance audits to ensure that systems meet security standards.

**How tool will be used:**

1. User can configure the scan to selecting the target systems or networks to be scanned, setting the scan type, selecting the plugins to be used, and configuring scan schedules.
2. Launch the scan to start the vulnerability assessment.
3. Performs both active and passive scans to identify vulnerabilities in the network or system.
4. Provides a report of the vulnerabilities identified.
5. Identify vulnerabilities by examining each service on all hosts in comparison to database





**Pros:**

* High accuracy in identifying vulnerabilities, which minimizes false positives and false negatives.
* Customized to meet specific requirements, including the selection of plugins, setting scan schedules, and integrating with other security tools.

**Cons:**

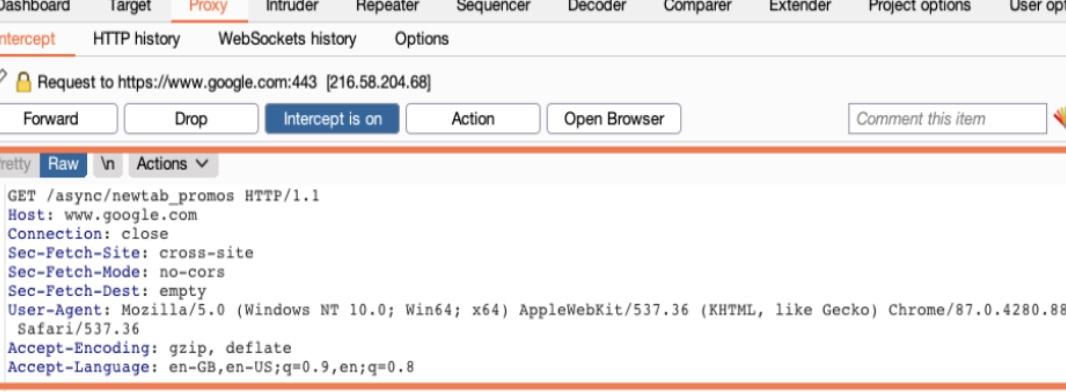
* Commercial tool that requires a license, which can be expensive for small and mid-sized organizations.
* Complex to set up and configure, and it requires some technical expertise to use effectively.

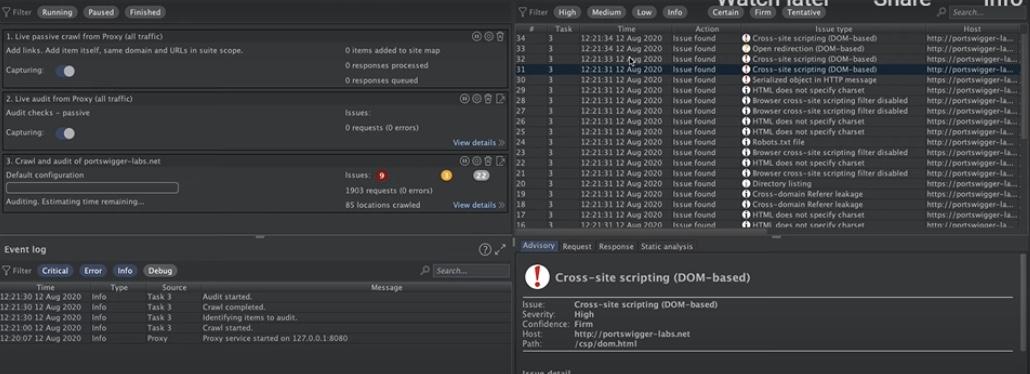
***Tool 3: Burp Suite***

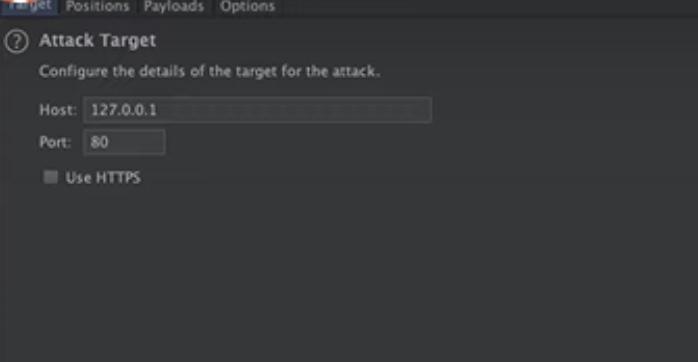
Description: Burp Suite is a comprehensive platform for performing web application security testing. It is developed by PortSwigger and consists of a variety of tools designed to help security professionals test and identify vulnerabilities in web applications. Burp Suite includes features such as a web application scanner, a proxy server, a web vulnerability scanner, and a variety of other tools that can help identify and exploit web application vulnerabilities.

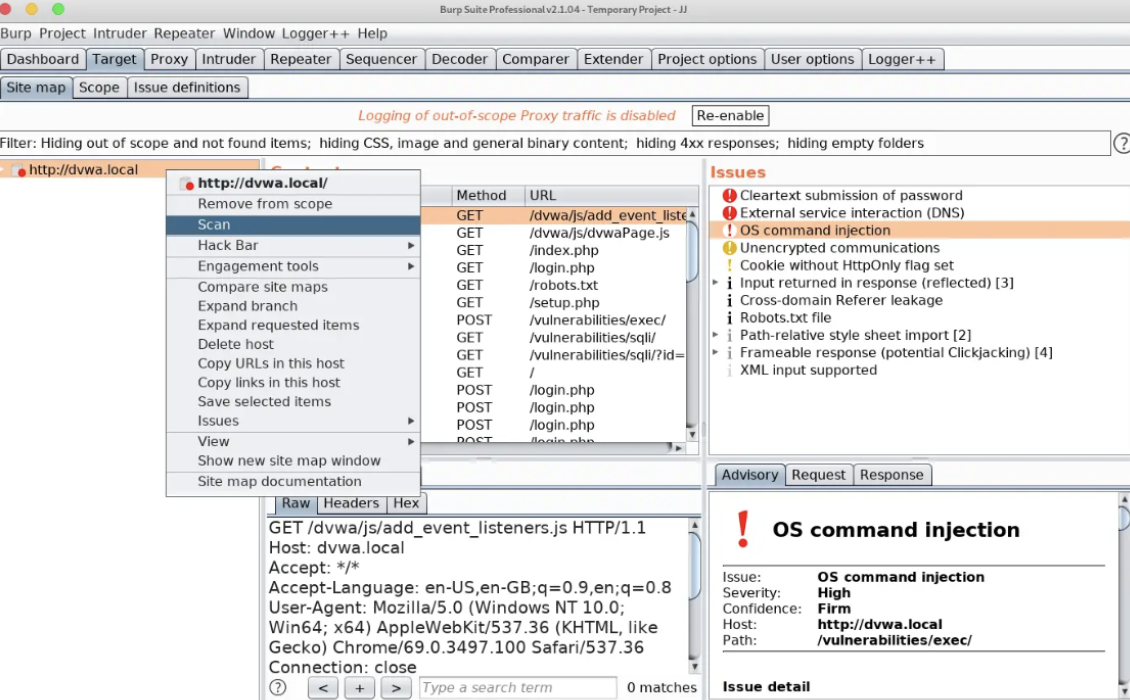
**How tool will be used:**

1. Intercepting HTTP requests and responses without modifying them. The tool can then analyze the data to identify potential vulnerabilities.
2. Active Scanning: This technique involves sending malicious payloads to the application in order to identify vulnerabilities. Burp Suite includes a scanner that can automate this process.
3. Spidering: This technique involves crawling the target website to identify all its pages and the relationships between them. This can help identify hidden pages and potential vulnerabilities.
4. Fuzzing: This technique involves sending large amounts of random data to the application in order to identify vulnerabilities.









**Pros:**

1. Provides a wide range of tools that can be used for different types of web application security testing, including scanning, crawling, and manual testing.
2. User-friendly interface that makes it easy to use, even for beginners.
3. Tool is regularly updated with new features and bug fixes, and it has an active user community and support team.

**Cons:**

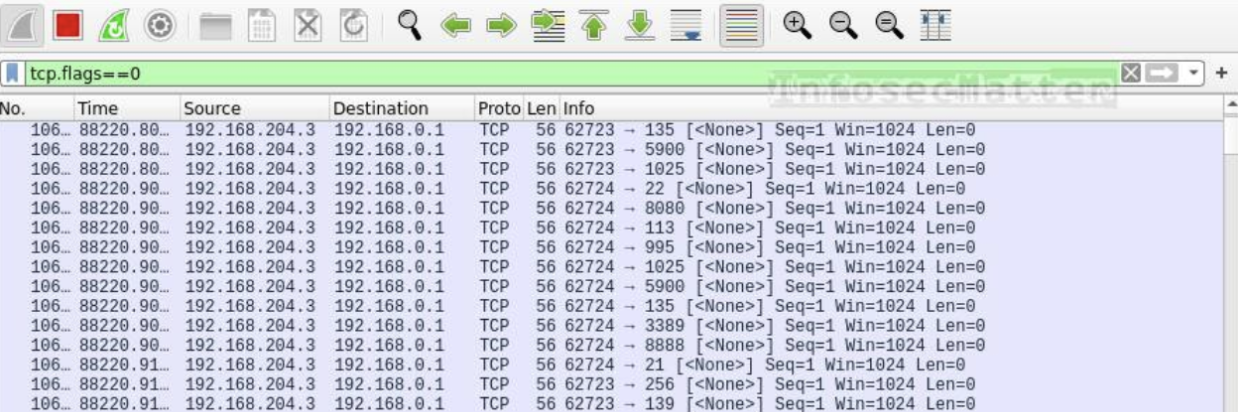
* Expensive as its pricing may not be affordable for small or independent security testing teams.
* Running scans and other tests with Burp Suite can be resource-intensive, requiring a powerful machine or server to run efficiently.

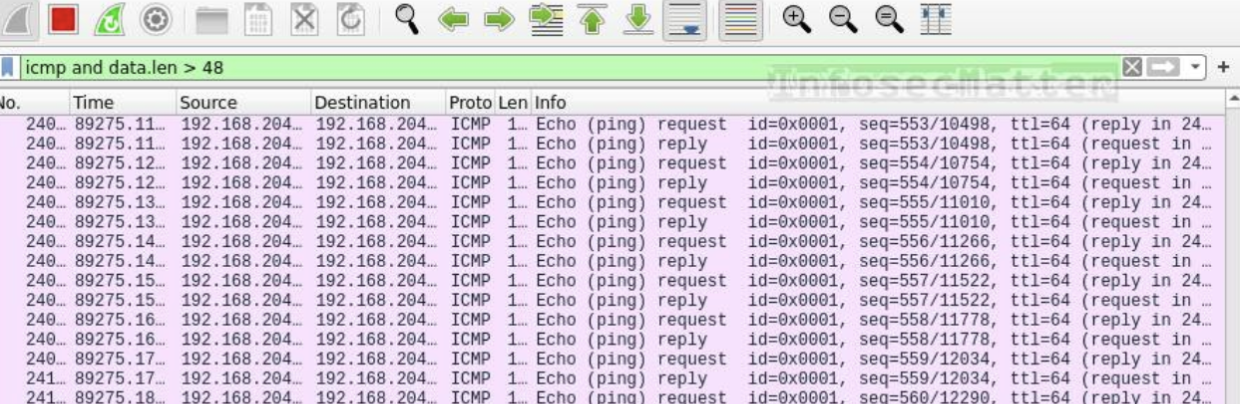
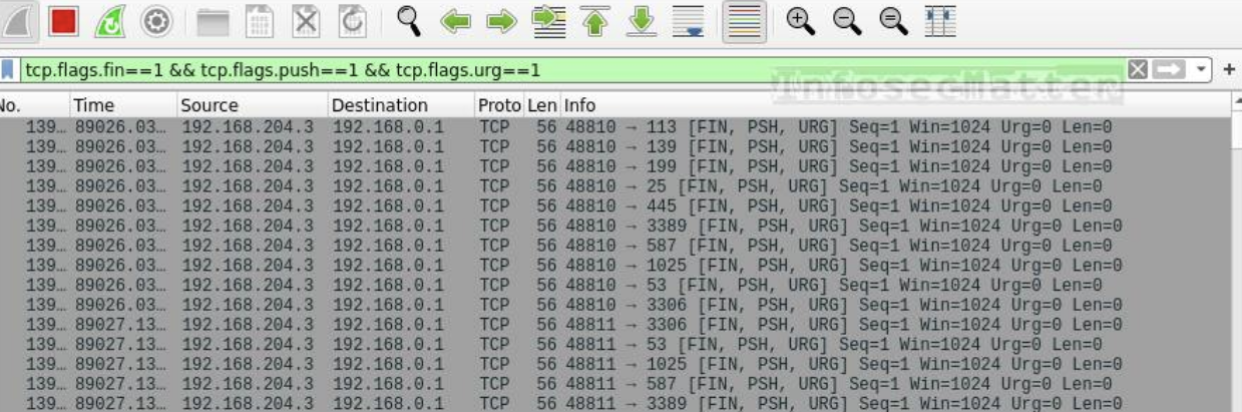
***Tool 4: Wireshark***

Description: Wireshark is a highly utilized network protocol analyzer that is widely regarded as the preeminent tool in the security practitioner's arsenal. Its extensive usage spans various sectors such as government agencies, enterprises, and educational institutions. Wireshark enables microscopic level inspection of networks by capturing online issues and conducting offline analyses. Additionally, it is compatible with several platforms including Linux, macOS, Windows, and Solaris.

**How tool will be used:**

1. Analyze network protocols to detect any anomalies, unexpected behavior or patterns in network traffic that may indicate the presence of vulnerabilities.
2. Inspect individual packets to identify any potential vulnerabilities that may exist within the packet structure or payload.
3. Attempts to exploit known vulnerabilities by analyzing network traffic for patterns that match known exploits or attack techniques.





**Pros:**

* Tailored configurations to identify particular vulnerabilities.
* Free use since its open-source.
* It is possible to utilize pcap files derived from previous network traffic scans for inspection purposes, and it is not mandatory for them to originate from a live scan.

**Cons:**

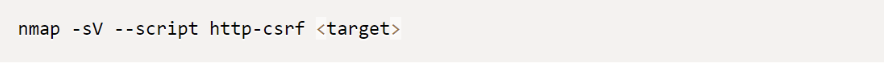
* It does not offer remedial actions.
* Comprehending potential implications requires a thorough comprehension of packet data and protocols.

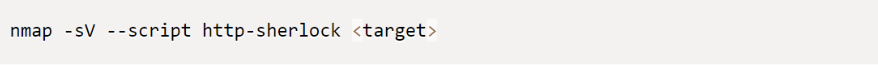
***Tool 5: Nmap Vulnerability Scripts***

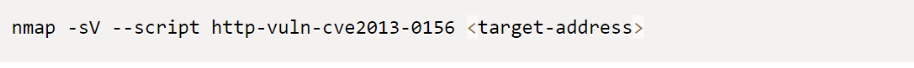
**Description:** Nmap Vulnerability Scripts is a feature in the Nmap network exploration and security auditing tool that contains a collection of scripts designed to identify potential vulnerabilities in target systems. These scripts utilize various techniques to detect security weaknesses, such as testing for known software flaws, checking default configurations, and attempting to exploit known vulnerabilities. Nmap Vulnerability Scripts can be highly effective in identifying potential security issues in a target system and can be used as part of a comprehensive vulnerability assessment or penetration testing.

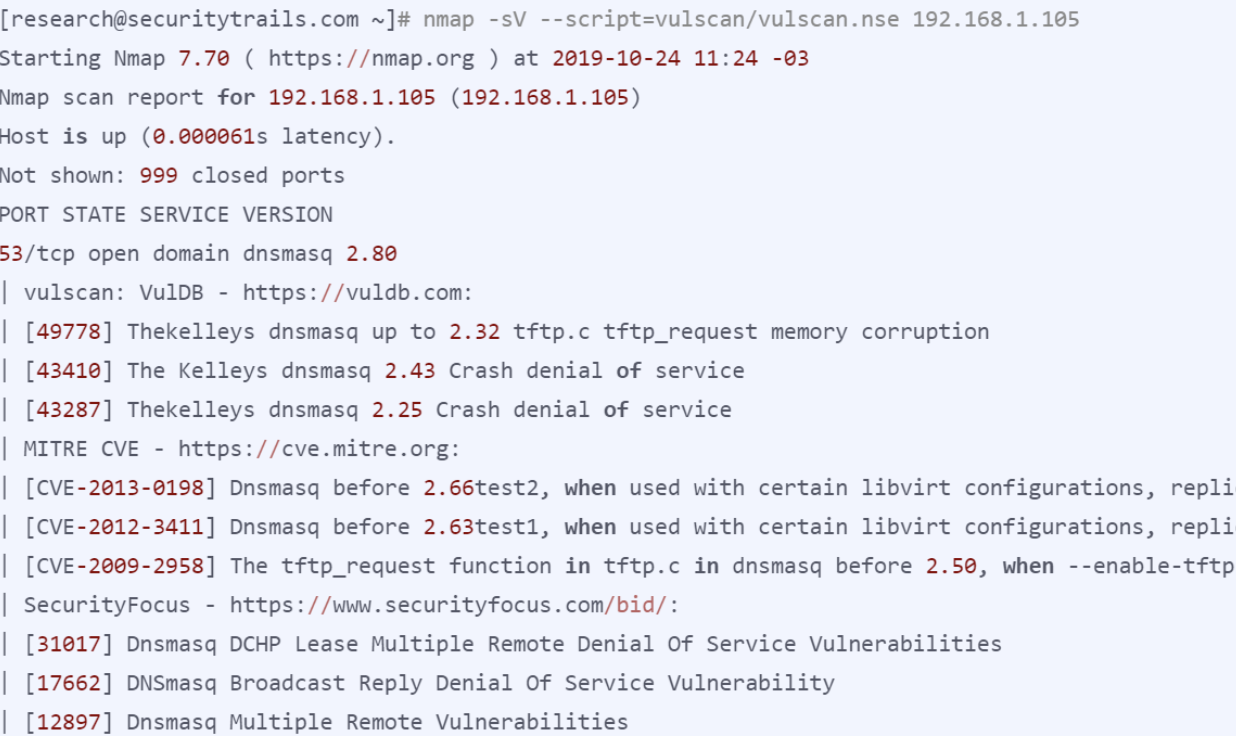
**How tool will be used:**

1. Detect services running on target systems and test them for known vulnerabilities.
2. Banner grabbing: Extract information from service banners, such as version numbers, and compare them against known vulnerabilities.
3. Attempt to exploit known vulnerabilities in target systems to test their resilience to attacks.
4. Fingerprinting: Used to gather information about the target system's operating system, applications, and network topology to identify potential vulnerabilities.









**Pros:**

* The configuration of scans is uncomplicated and readily accessible on the internet.
* Free source to utilize.
* CVE references are included in the output scans

**Cons:**

* Potentially contains lots of false positives.
* It does not provide as comprehensive a database of CVE vulnerabilities as compared to Nessus or OpenVAS.