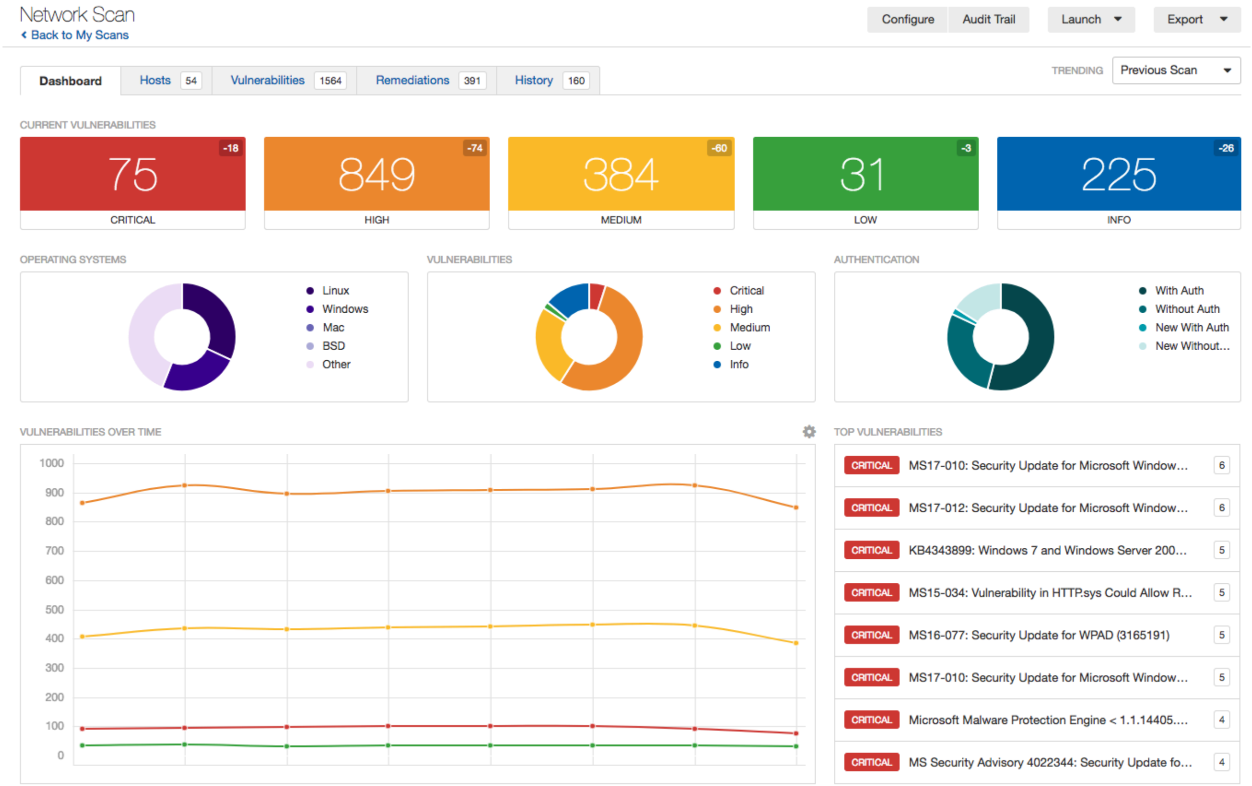
Phase 3: Vulnerability Scanning Tools

The objective of Phase 3 is to identify vulnerabilities within the network, applications, and systems discovered in the earlier phases. This involves scanning for known security flaws and potential misconfigurations that could allow an attacker to gain unauthorized access or exploit sensitive data. For this phase, I've selected five critical tools in Kali Linux for vulnerability assessment: **Tenable Nessus, OpenVAS, Burp Suite, Wapiti, and W3af**. Each tool serves a specific purpose in identifying vulnerabilities, providing insights necessary for risk assessment and mitigation.

1. Tenable Nessus

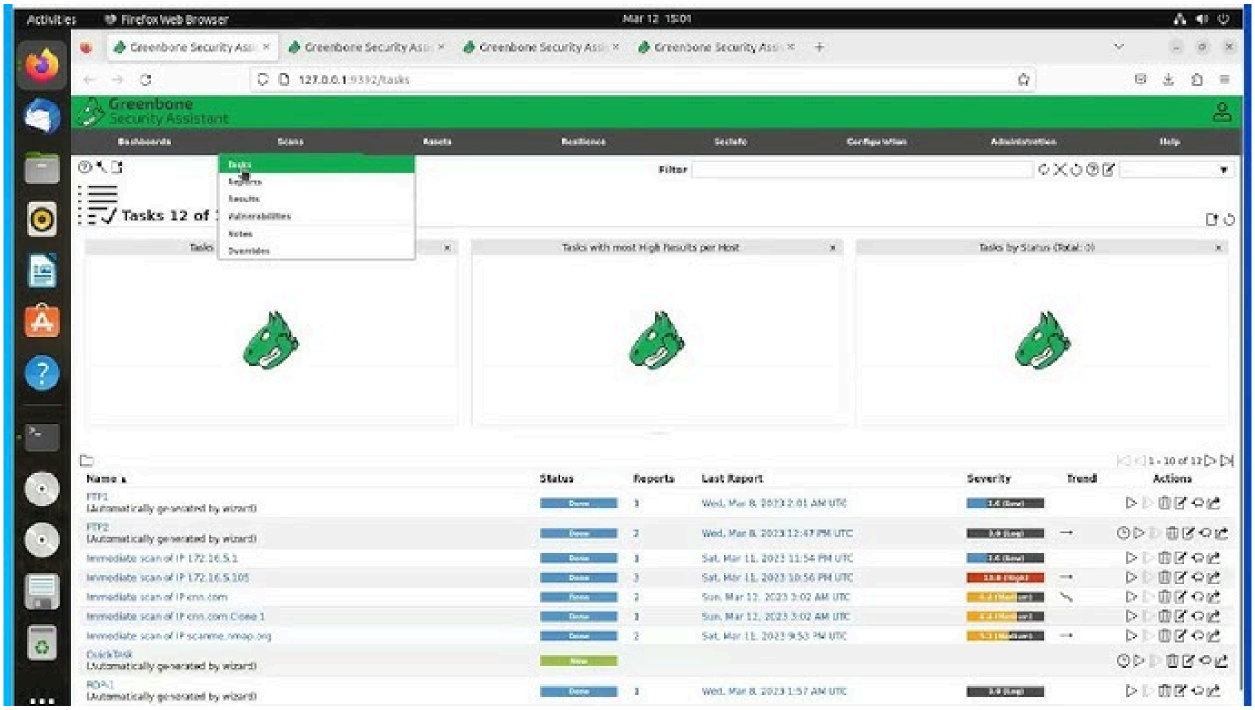
- **Purpose**: Nessus is a comprehensive vulnerability scanner that assesses systems and services for known vulnerabilities, misconfigurations, and weaknesses. It includes a vast plugin library that is regularly updated, making it highly effective for identifying current security issues.
- **Usage**:
    - **Basic Scan Setup**: Create a new scan profile, select the type (e.g., Basic Network Scan), configure the target IP range, and choose any specific plugins if needed.
    - **Configuration Options**: Configure scan settings to target specific ports, enable/disable plugins, and define scan policies for thorough or fast scans. Choose the "High Security" profile for deeper analysis.
    - **Sample Command**: The Nessus interface is primarily GUI-based, allowing the user to customize scans without command-line input.
- **Pros**:
    - Comprehensive vulnerability coverage with a large plugin library.
    - User-friendly interface for easy setup and reporting.
- **Cons**:
    - Requires a license for full access to plugins, which can be costly.
    - Resource-intensive and may slow down performance during scans.



CRITICAL	MS17-010: Security Update for Microsoft Window...	6
CRITICAL	MS17-012: Security Update for Microsoft Window...	6
CRITICAL	KB4343899: Windows 7 and Windows Server 200...	5
CRITICAL	MS15-034: Vulnerability in HTTP.sys Could Allow R...	5
CRITICAL	MS16-077: Security Update for WPAD (3165191)	5
CRITICAL	MS17-010: Security Update for Microsoft Window...	5
CRITICAL	Microsoft Malware Protection Engine < 1.1.14405....	4
CRITICAL	MS Security Advisory 4022344: Security Update fo...	4

2. OpenVAS (Open Vulnerability Assessment System)

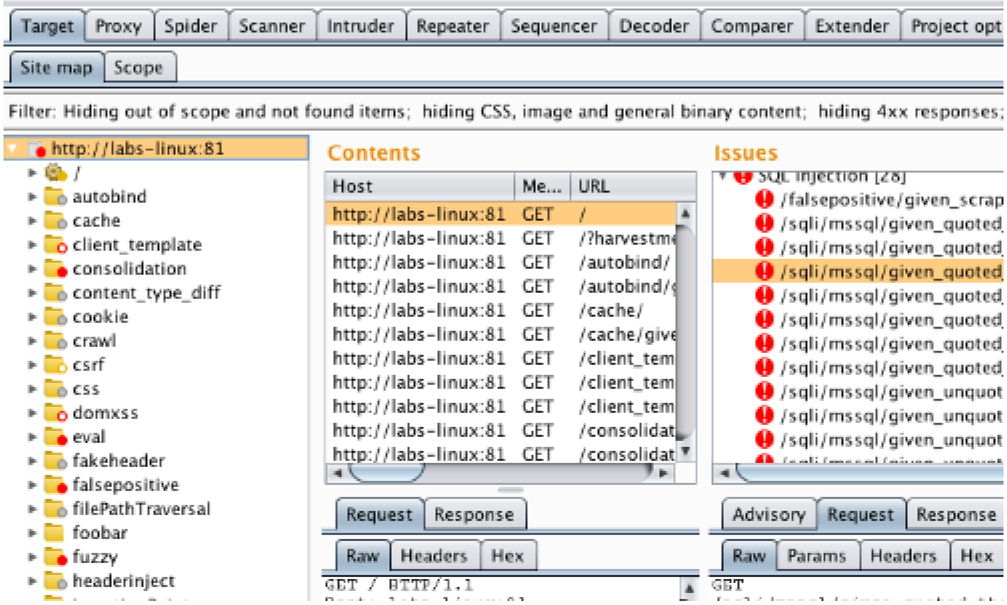
- **Purpose**: OpenVAS is an open-source vulnerability scanner designed for network-level assessments. It checks for a wide range of vulnerabilities across various operating systems and applications and generates detailed reports with risk ratings.
- **Usage**:
  - **Basic Scan Setup**: In the OpenVAS interface, create a new task, specify the IP range, and select desired scan configurations, such as the “Full and Fast” scan profile for a comprehensive analysis.
  - **Configuration Options**: Configure options for timing, sensitivity, and custom vulnerability checks to reduce false positives or target specific systems.
  - **Commands**: OpenVAS setup and task management are managed through its graphical interface; customization of scan tasks is also GUI-based.
- **Pros**:
  - Free to use with a robust set of vulnerability checks.
  - Detailed reporting with risk levels and recommendations.
- **Cons**:
  - Heavy on system resources, particularly when performing extensive scans.
  - The initial setup can be complex and time-consuming.



Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
FTP1 (Automatically generated by wizard)	Done	1	Wed, Mar 8, 2023 2:01 AM UTC	2.6 (Low)		
FTP2 (Automatically generated by wizard)	Done	2	Wed, Mar 8, 2023 12:47 PM UTC	0.0 (Log)	→	
Immediate scan of IP 172.16.5.1	Done	1	Sat, Mar 11, 2023 11:54 PM UTC	2.6 (Low)		
Immediate scan of IP 172.16.5.105	Done	3	Sat, Mar 11, 2023 10:56 PM UTC	10.0 (High)	→	
Immediate scan of IP cnn.com	Done	2	Sun, Mar 12, 2023 3:02 AM UTC	6.4 (Medium)	↘	
Immediate scan of IP cnn.com Clone 1	Done	1	Sun, Mar 12, 2023 3:02 AM UTC	6.4 (Medium)		
Immediate scan of IP scanme.nmap.org	Done	2	Sat, Mar 11, 2023 9:53 PM UTC	5.3 (Medium)	→	
QuickTask (Automatically generated by wizard)	New					
RDP1 (Automatically generated by wizard)	Done	1	Wed, Mar 8, 2023 1:57 AM UTC	0.0 (Log)		

3. Burp Suite

- **Purpose**: Burp Suite is a web application security scanner primarily used for detecting vulnerabilities such as SQL injection, cross-site scripting (XSS), and other web application security flaws.
- **Usage**:
  - **Proxy Setup**: Burp Suite's proxy captures HTTP/S traffic, allowing for manual testing and modification of requests.
  - **Scanner Configuration**: Select the "Active Scan" option to automate testing for common vulnerabilities across target web applications. Configure scan depth, insertion points, and sensitivity levels.
  - **Sample Configuration**: Set Burp's scope to include specific URLs for targeted testing, minimizing unnecessary scans.
- **Pros**:
  - Powerful for web application testing with extensive vulnerability checks.
  - Highly configurable for both manual and automated testing.
- **Cons**:
  - The full version requires a license for advanced scanning and vulnerability detection features.
  - Resource-intensive, especially during extensive web scans.



Filter: Hiding out of scope and not found items; hiding CSS, image and general binary content; hiding 4xx responses;

- http://labs-linux:81
  - /
  - autobind
  - cache
  - client_template
  - consolidation
  - content_type_diff
  - cookie
  - crawl
  - csrf
  - css
  - domxss
  - eval
  - fakeheader
  - falsepositive
  - filePathTraversal
  - foobar
  - fuzzy
  - headerinject

Host	Me...	URL
http://labs-linux:81	GET	/
http://labs-linux:81	GET	/?harvestme
http://labs-linux:81	GET	/autobind/
http://labs-linux:81	GET	/autobind/
http://labs-linux:81	GET	/cache/
http://labs-linux:81	GET	/cache/give
http://labs-linux:81	GET	/client_tem
http://labs-linux:81	GET	/client_tem
http://labs-linux:81	GET	/client_tem
http://labs-linux:81	GET	/consolidat
http://labs-linux:81	GET	/consolidat

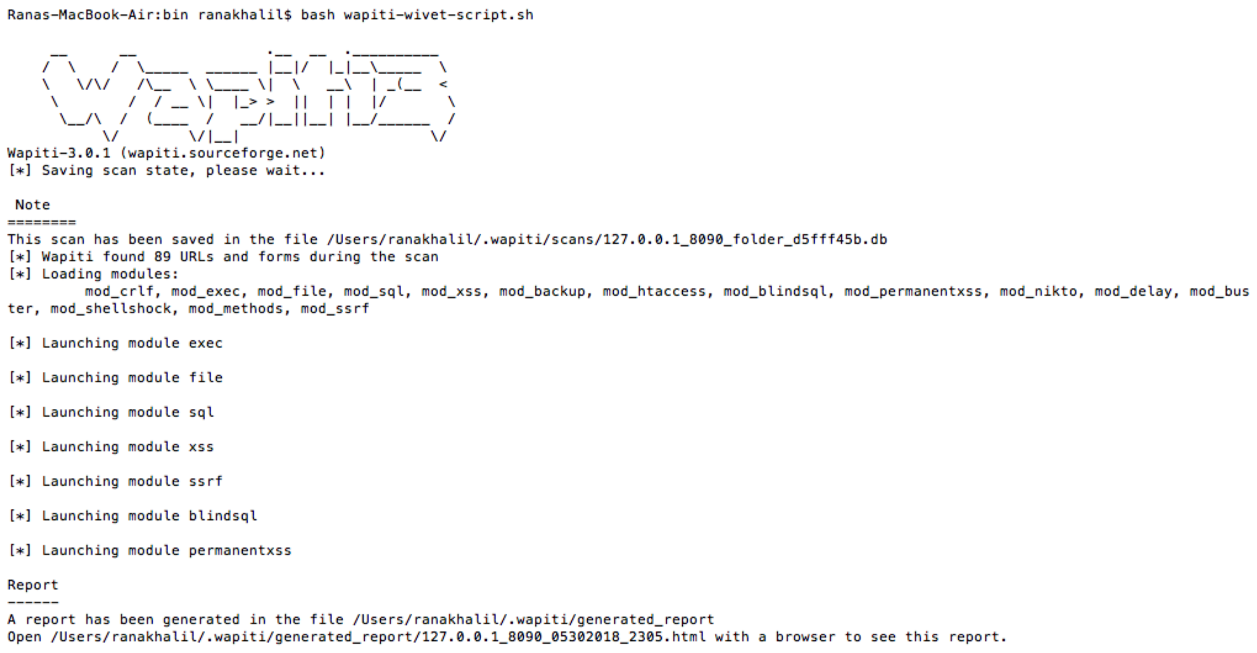
- SQL injection [28]
  - /falsepositive/given_scrap
  - /sqli/mssql/given_quoted
  - /sqli/mssql/given_quoted
  - /sqli/mssql/given_quoted
  - /sqli/mssql/given_quoted
  - /sqli/mssql/given_quoted
  - /sqli/mssql/given_quoted
  - /sqli/mssql/given_quoted
  - /sqli/mssql/given_unquot
  - /sqli/mssql/given_unquot
  - /sqli/mssql/given_unquot

```
GET / HTTP/1.1
```

```
GET
```

4. Wapiti

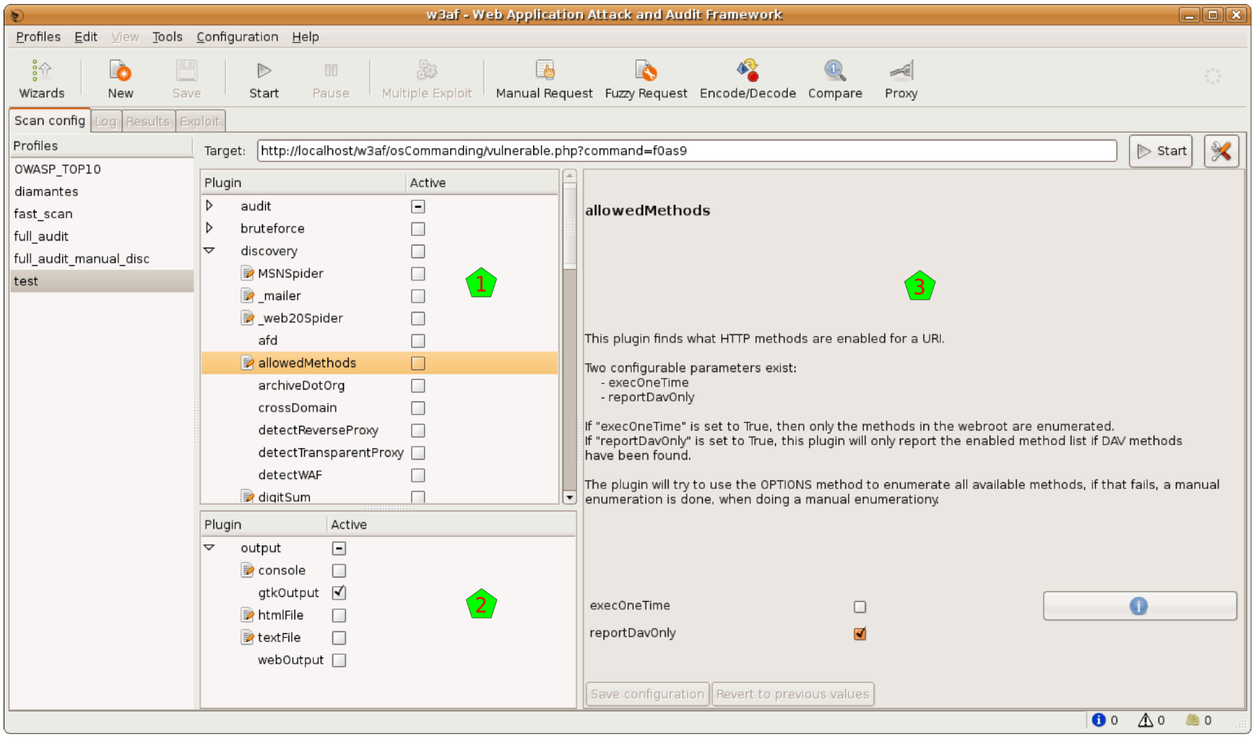
- **Purpose**: Wapiti is an open-source web application vulnerability scanner focused on detecting SQL injections, XSS, file inclusion vulnerabilities, and more. It performs scans by analyzing HTTP requests and responses for web applications.
- **Usage**:
  - **Basic Scan Command**: `wapiti -u <target_url>` — Initiates a scan against the target web application.
  - **Configuration Options**: Use command-line options to customize scan depth, timeout values, and which modules to enable or disable (e.g., enable SQL injection and XSS checks).
  - **Commands**: `wapiti -u <target_url> -m “sqli,xss”` to scan only for SQL injection and XSS vulnerabilities.
- **Pros**:
  - Fast and efficient for web vulnerability scanning.
  - Lightweight and easy to set up without additional configuration requirements.
- **Cons**:
  - Limited to web applications, and lacks the depth of more comprehensive tools like Burp Suite.
  - No GUI, which can be challenging for users unfamiliar with command-line tools.



```
Ranas-MacBook-Air:bin ranakhalil$ bash wapiti-wivet-script.sh

     __      __               .__  __  .__________
    /  \    /  \_____  ______ |__|/  |_|__\_____  \
    \   \/\/   /\__  \ \____ \|  \   __\  | _(__  <
     \        /  / __ \|  |_> >  ||  | |  |/       \
      \__/\  /  (____  /   __/|__||__| |__/______  /
           \/        \/|__|                      \/
Wapiti-3.0.1 (wapiti.sourceforge.net)
[*] Saving scan state, please wait...

 Note
========
This scan has been saved in the file /Users/ranakhalil/.wapiti/scans/127.0.0.1_8090_folder_d5fff45b.db
[*] Wapiti found 89 URLs and forms during the scan
[*] Loading modules:
         mod_crlf, mod_exec, mod_file, mod_sql, mod_xss, mod_backup, mod_htaccess, mod_blindsql, mod_permanentxss, mod_nikto, mod_delay, mod_bus
ter, mod_shellshock, mod_methods, mod_ssrf

[*] Launching module exec

[*] Launching module file

[*] Launching module sql

[*] Launching module xss

[*] Launching module ssrf

[*] Launching module blindsql

[*] Launching module permanentxss

Report
------
A report has been generated in the file /Users/ranakhalil/.wapiti/generated_report
Open /Users/ranakhalil/.wapiti/generated_report/127.0.0.1_8090_05302018_2305.html with a browser to see this report.
```

5. W3af (Web Application Attack and Audit Framework)

- **Purpose**: W3af is an open-source web application vulnerability scanner and exploit tool. It focuses on detecting vulnerabilities in web applications and offers options for manual testing and automated vulnerability scanning.
- **Usage**:
  - **Basic Scan Setup**: Set the target URL, configure the type of scan (e.g., full audit), and select specific modules to enable, such as SQL injection or XSS testing.
  - **Configuration Options**: Customize scan profiles to focus on particular vulnerabilities. For example, use the “injections” module to detect SQL, XSS, and OS command injection vulnerabilities.
  - **Commands**: `w3af_console` opens the W3af interface for configuring and running scans interactively.
- **Pros**:
  - Extensive plugin library allows for targeted web application vulnerability scanning.
  - Open-source and customizable with support for both automated and manual testing.
- **Cons**:
  - Interface can be slow and occasionally buggy during extensive scans.
  - Limited reporting options compared to tools like Burp Suite.



Target: http://localhost/w3af/osCommanding/vulnerable.php?command=f0as9

Plugin	Active
▷ audit	⊟
▷ bruteforce	□
▽ discovery	□
MSNSpider	□
_mailer	□
_web20Spider	□
afd	□
allowedMethods	□
archiveDotOrg	□
crossDomain	□
detectReverseProxy	□
detectTransparentProxy	□
detectWAF	□
digitSum	□

Plugin	Active
▽ output	⊟
console	□
gtkOutput	☑
htmlFile	□
textFile	□
webOutput	□

allowedMethods

This plugin finds what HTTP methods are enabled for a URI.

Two configurable parameters exist:
- execOneTime
- reportDavOnly

If "execOneTime" is set to True, then only the methods in the webroot are enumerated.
If "reportDavOnly" is set to True, this plugin will only report the enabled method list if DAV methods have been found.

The plugin will try to use the OPTIONS method to enumerate all available methods, if that fails, a manual enumeration is done, when doing a manual enumerationy.

execOneTime □
reportDavOnly ☑

Summary

Each of these tools provides distinct advantages in vulnerability scanning, allowing for a well-rounded assessment of Artemis's network and application security:

1. **Nessus** and **OpenVAS** deliver comprehensive network-level scans for identifying host vulnerabilities.
2. **Burp Suite** focuses on web application security, detecting common web vulnerabilities.
3. **Wapiti** and **W3af** serve as supplementary web application scanners, providing additional insights and validation for web-related vulnerabilities.

Challenges and Limitations

- **Resource Intensity**: Nessus, OpenVAS, and Burp Suite are resource-intensive, which can slow down the system or trigger detection in monitored environments.
- **Scope-Specific Tools**: Tools like Burp Suite, Wapiti, and W3af are limited to web applications, meaning they do not provide insights on network-level vulnerabilities outside web servers.
- **Configuration Complexity**: OpenVAS and W3af require significant configuration time to perform optimally, which may not be suitable for short testing windows.

By combining these tools, we can ensure a thorough vulnerability assessment, uncovering potential weaknesses in both network services and web applications.