

Phase 3: Identify Vulnerabilities

Nessus

Usage: Nessus is a cross-platform vulnerability scanner from Tenable, Inc. that is able to scan many types of systems, including web applications, Internet-facing attack surfaces, and more.

Config & Settings:

Setting up a new scan:

The screenshot shows the Nessus web interface for creating a new scan. The 'Name' field is set to 'Network Scan', the 'Description' is 'Testing Basic Network Scan', the 'Folder' is 'My Scans', and the 'Targets' field contains the IP address '172.25.10.171'. The 'Save' button is highlighted with a red box.

Example of vulnerabilities found:

The screenshot shows the Nessus web interface displaying the results of a scan on the host 172.25.10.171. The table lists 10 vulnerabilities found, including 'Novonyx Web Server Multiple Sample Application Files Present' (Medium severity) and several 'Backported Security Patch Detection' (Info severity). A donut chart on the right shows the distribution of severity levels: 1 Medium and 9 Info.

Severity	Plugin Name	Plugin Family	Count
MEDIUM	Novonyx Web Server Multiple Sample Application Files Present	Netware	1
INFO	netstat portscanner (SSH)	Port scanners	2
INFO	Remote listeners enumeration (Linux / ADX)	Service detection	2
INFO	Service Detection	Service detection	2
INFO	Apache Banner Linux Distribution Disclosure	Web Servers	1
INFO	Authenticated Check : OS Name and Installed Package Enumeration	Settings	1
INFO	Backported Security Patch Detection (SSH)	General	1
INFO	Backported Security Patch Detection (WWW)	General	1
INFO	BIOS version (SSH)	General	1
INFO	Common Platform Enumeration (CPE)	General	1

Host Details

IP: 172.25.10.171
DNS: ubuntu-15
MAC: 00:50:56:a9:70:2c
OS: Linux Kernel 4.2.0-34-generic on Ubuntu 15.10
Start: Today at 7:11 PM
End: Today at 7:16 PM
Elapsed: 5 minutes
KB: Download

Vulnerabilities

Donut chart showing severity distribution: 1 Medium (yellow), 9 Info (blue).

Click on one vulnerability to see more details:

The screenshot shows the Nessus interface with a network scan in progress. The main section displays a vulnerability titled "Novonyx Web Server Multiple Sample Application Files Present" with a medium severity. The description states that a default installation of Novell NetWare 5.x includes numerous web server files that could reveal system information. The solution suggests removing these files if not required. The output section lists various files found on the server, including /netbasic/webinfo.bas, /log/sevse.nlm?sys:/novonyx/suiteapot/docs/sevse/misc/allfield.js, and others. The right sidebar provides plugin details (Severity: Medium, ID: 12049, Version: \$Revision: 1.17 \$, Type: remote, Family: Netware, Published: 2004/02/07, Modified: 2011/03/17) and risk information (Risk Factor: Medium, CVSS Base Score: 5.0, CVSS Vector: CVSS2#AVN/ACL/AuN/C:P/RN/A/N, CVSS Temporal Vector: CVSS2#EF/RLU/RC:ND, CVSS Temporal Score: 4.8). The vulnerability information section indicates that exploits are available and the vulnerability was published on 2002/05/30.

Pros	Cons
cross-platform	expensive license
live results	proprietary software
easy to use and understand results	free version is very limited and slow

OpenVAS

Usage: OpenVAS is a software framework containing multiple services and tools for vulnerability scanning and management.

Config & Settings:

Add credentials:

The screenshot shows the "New Credential" form in OpenVAS. The form includes fields for Name (Linux-default), Comment (Linux machines username and password), Type (Username + Password), Allow insecure use (No), Auto-generate (No), Username (root), and Password (masked). A "Create" button is located at the bottom right. Orange arrows point to each of these fields.

Configure target:

New Target

Name

localhost

Comment

Manual

127.0.0.1

From file

Browse...

No file selected.

From host assets (0 hosts)

Exclude Hosts

Reverse Lookup Only

Yes

No

Reverse Lookup Unify

Yes

No

Port List

All IANA assigned TCP an...

Alive Test

Scan Config Default

Credentials for authenticated checks

SSH

Linux-default

on port

22

SMB

--

ESXi

--

SNMP

--

Create

Configure scan:

Name	Families		NVTs		Actions
	Total	Trend	Total	Trend	
Discovery (Network Discovery scan configuration.)	20		2748		
empty (Empty and static configuration template.)	0		0		
Full and fast (Most NVT's; optimized by using previously collected information.)	62		50175		
Full and fast ultimate (Most NVT's including those that can stop services/hosts; optimized by using previously collected information.)	62		50175		
Full and very deep (Most NVT's; don't trust previously collected information; slow.)	62		50175		
Full and very deep ultimate (Most NVT's including those that can stop services/hosts; don't trust previously collected information; slow.)	62		50175		
Host Discovery (Network Host Discovery scan configuration.)	2		2		
System Discovery (Network System Discovery scan configuration.)	6		29		

1 - 8 of 8

Apply to page contents

Configure task:

New Task

Name

unnamed

Comment

Scan Targets

localhost

Alerts

Schedule

--

☒ Once

Add results to Assets

☒ yes ☐ no

Apply Overrides

☒ yes ☐ no

Min QoD

70

%

Alterable Task

☒ yes ☐ no

Auto Delete Reports

☒ Do not automatically delete reports

☐ Automatically delete oldest reports but always keep newest

5

reports

Scanner

OpenVAS Default

Scan Config

Full and fast

Network Source Interface

ens33

Order for target hosts

Sequential

Maximum concurrently executed NVTs per host

4

Maximum concurrently scanned hosts

20

Create

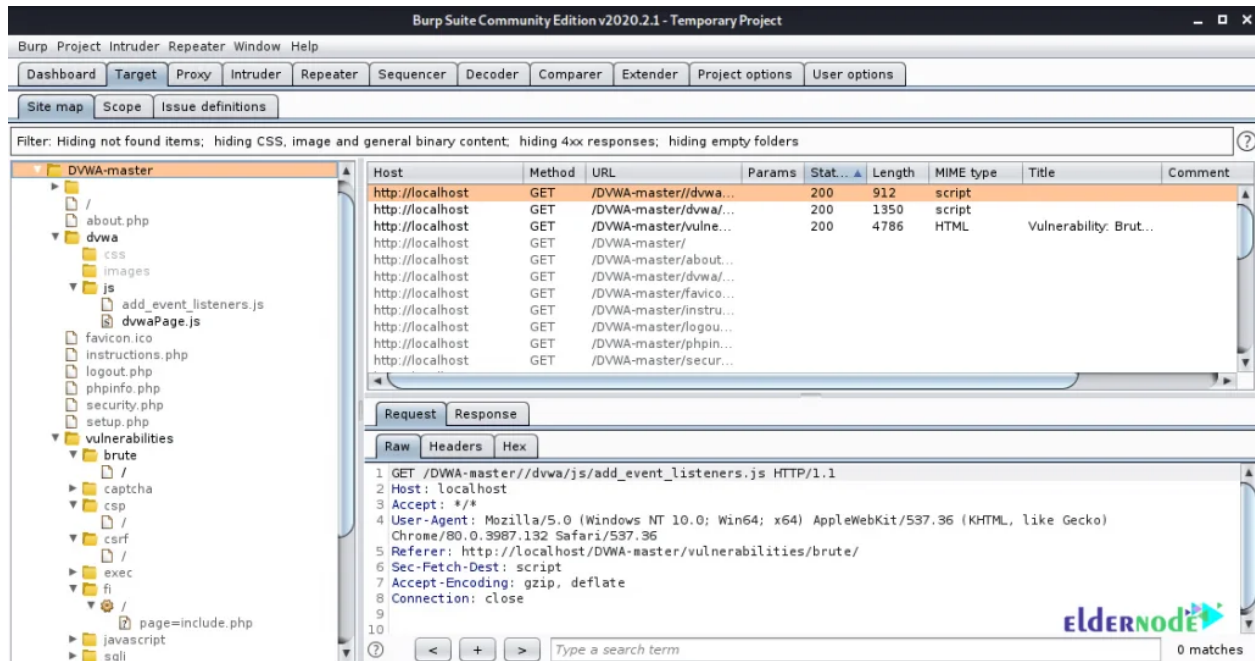
Pros	Cons
FOSS	GUI can be difficult to use/navigate
cross-platform	can be misconfigured
GUI available	sometimes results in false negatives

Burp Suite

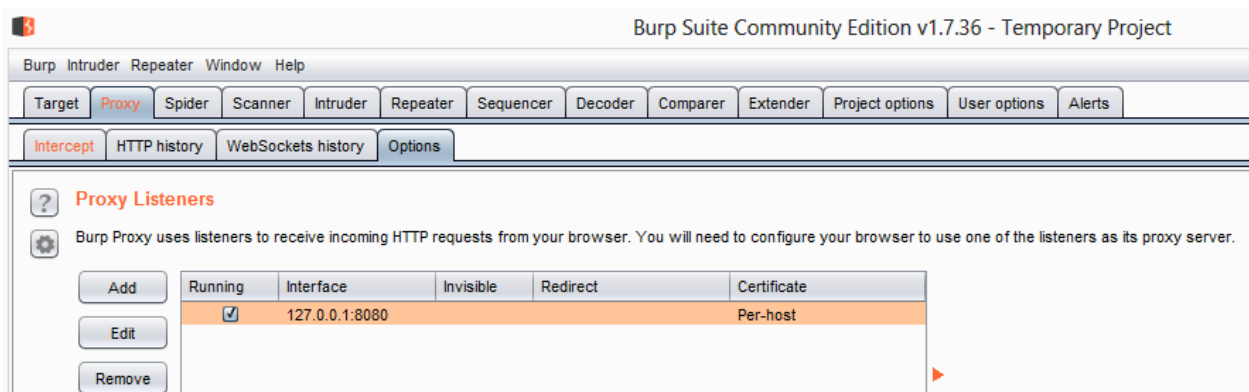
Usage: Burp Suite is a software security tool suite for pentesting web applications.

Config & Settings:

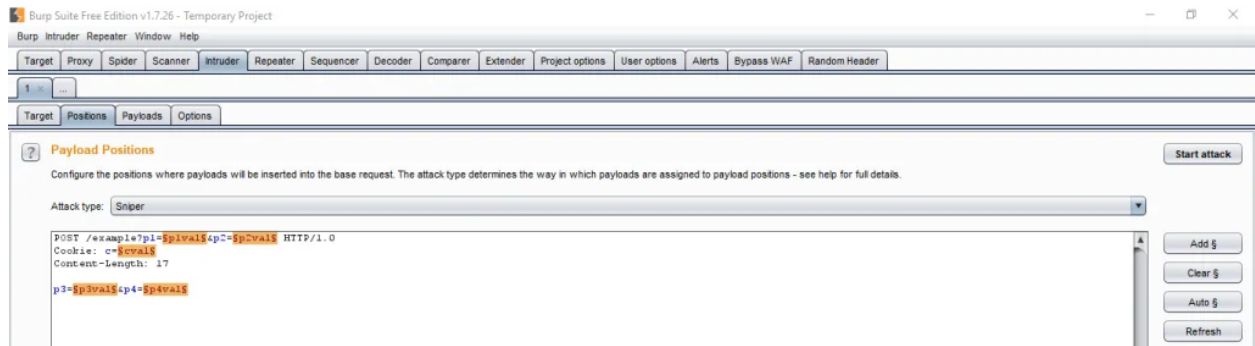
Target view:



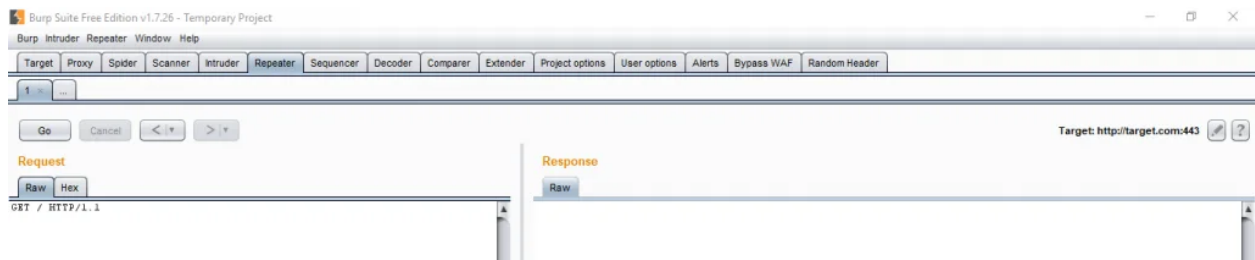
Proxy:



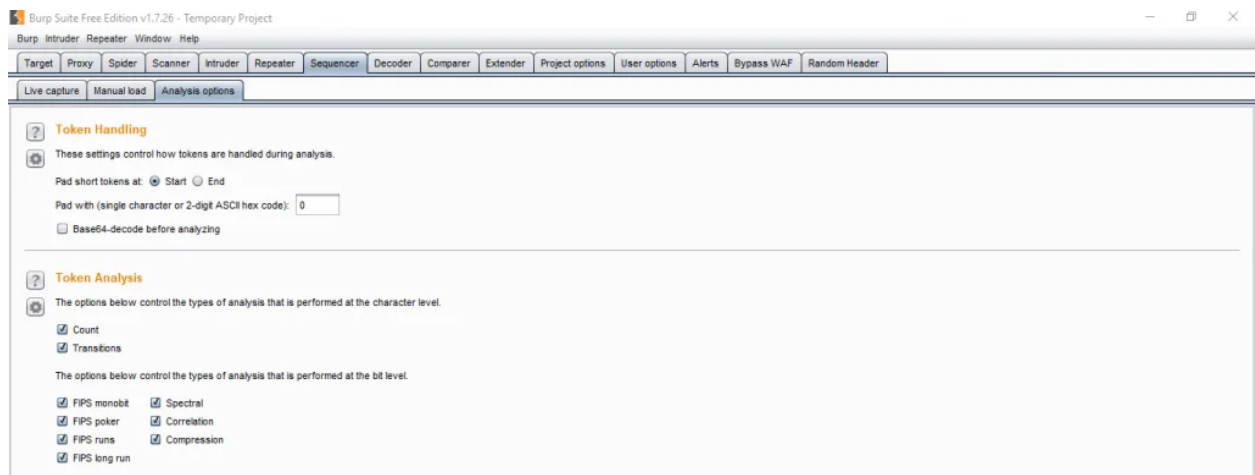
Intruder:



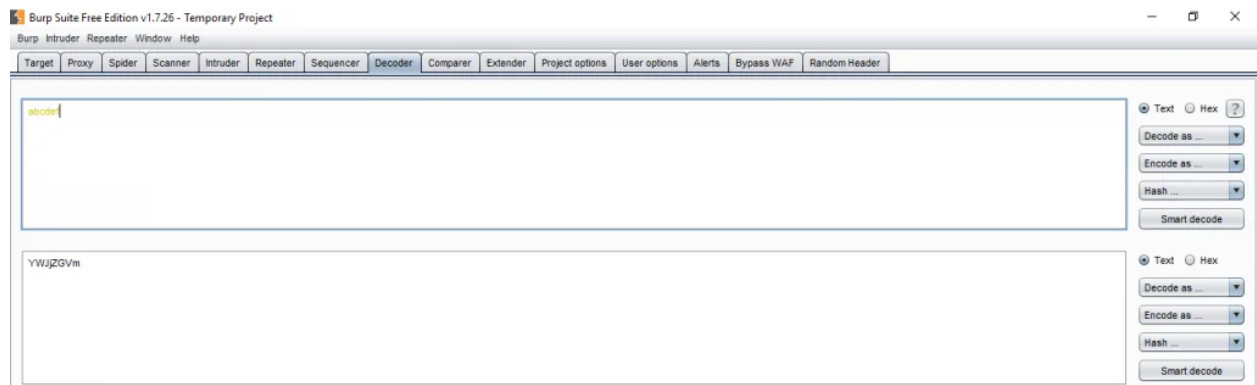
Repeater:



Sequencer:



Decoder:



Pros	Cons
cross-platform	can be overwhelming
GUI	free version has limited features
comprehensive toolkit	can be overwhelming to use

Nikto

Usage: Nikto is a command-line vulnerability scanner for scanning web servers.

Config & Settings:

Scan scanme.nmap.org on port 80:

```
nikto -h scanme.nmap.org
```

(append -ssl or -p 80 if site uses https)

Scan scanme.nmap.org and output results to text file:

```
nikto -h scanme.nmap.org -o output.txt
```

Pros	Cons
FOSS	uses some non-FOSS resources
CLI	no GUI
many plugins available	by default, very noisy

Wapiti

Usage: Wapiti performs black-box security scans of web applications by crawling the sites to find injection points.

Config & Settings:

```
root@kali:~# wapiti -h
```

Wapiti-3.0.4 (wapiti.sourceforge.io)

[*] Be careful! New moon tonight.

```
usage: wapiti [-h] [-u URL] [--scope {page,folder,domain,url,punk}]
              [-m MODULES_LIST] [--list-modules] [--update] [-l LEVEL]
              [-p PROXY_URL] [--tor] [-a CREDENTIALS]
              [--auth-type {basic,digest,kerberos,ntlm,post}] [-c COOKIE_FILE]
              [--skip-crawl] [--resume-crawl] [--flush-attacks]
              [--flush-session] [--store-session PATH] [--store-config PATH]
              [-s URL] [-x URL] [-r PARAMETER] [--skip PARAMETER] [-d DEPTH]
              [--max-links-per-page MAX] [--max-files-per-dir MAX]
              [--max-scan-time SECONDS] [--max-attack-time SECONDS]
              [--max-parameters MAX] [-S FORCE] [-t SECONDS] [-H HEADER]
              [-A AGENT] [--verify-ssl {0,1}] [--color] [-v LEVEL] [-f FORMAT]
              [-o OUPUT_PATH] [--external-endpoint EXTERNAL_ENDPOINT_URL]
              [--internal-endpoint INTERNAL_ENDPOINT_URL]
              [--endpoint ENDPOINT_URL] [--no-bugreport] [--version]
```

Wapiti-3.0.4: Web application vulnerability scanner

Basic usage form:

```
wapiti -u <target> <options>
```

Pros	Cons
CLI	no GUI
FOSS	running on Windows requires WSL
tests for many different injection attacks	ongoing project that may have bugs