

W12D4_PROGETTO 3_ANALISI DELLE VULNERABILITA' E AZIONI DI RIMEDIO

La protezione delle reti e dei sistemi passa attraverso l'analisi delle vulnerabilità fatta in maniera costante. Durante un PT, nel momento in cui si effettua una scansione completa sul target attraverso l'utilizzo di tool come ad esempio Nessus o Greenbone, si vanno a rilevare tutti i servizi TCP e UDP attivi sulle porte che possono essere aperte o chiuse. Lo scanner effettua una ricerca delle vulnerabilità note per la versione del servizio con l'obiettivo di arrivare ad una Remediation action al termine della fase di exploit, cioè una o più azioni necessarie per andare a sanare i problemi di sicurezza che potrebbero altrimenti essere sfruttati.

L'utilizzo dello scanner di rete Greenbone sul target metasploitable aiuta ad individuare tutta una serie di vulnerabilità note che ne restituisce una fotografia in base alla gravità (CVSS), questo per dare priorità all'azione di rimedio da adottare di conseguenza.

Sul target metaspitable con ip 192.168.50.106 si implementa una scansione delle porte TCP e UDP ovvero i protocolli di trasporto sui quali si trovano porte e servizi.

Avvio del tool Greenbone

```
[kali㉿kali]:~$ sudo gem-check-setup
gem-check-setup 25.04.0
This script is maintained and maintained by Debian and Kali.
Test completeness and readiness of GVM-25.04.0
Step 1: Checking OpenVAS (Scanner) ...
OK: OpenVAS Scanner is present, in version 23.23.1.
OK: OpenVAS Manager is present, in version 22.7.2.
OK: Server CA Certificate is present as /var/lib/gvm/CA/servercert.pem.
Checking permissions of /var/lib/openvas/snmp/
OK: gvm owns all files in /var/lib/openvas/snmp
OK: Redis-OpenVAS is present.
OK: scanner (db_address setting) is configured properly using the redis-server socket: /var/run/redis-openvas/redis-server.sock
OK: the mgmt_server_url is defined in /etc/openvas/openvas.conf
OK: Redis-OpenVAS is active.
OK: NVT collection in /var/lib/openvas/plugins contains 94007 NVTs.
OK: The notus directory /var/lib/notus/products contains 510 NVTs.
Checking that the obsolete redis database has been removed
Could not connect to redis at /var/run/redis-openvas/redis-server.sock: No such file or directory
OK: No old Redis DB
Starting ospd-openvas service
Waiting for ospd-openvas service
OK: ospd-openvas service is active.
OK: ospd-OpenVAS is present, in version 22.9.0.
Step 2: Checking GVM Manager ...
OK: gvm (gvm) is present in version 26.2.1.
Step 3: Checking GVM ...
OK: GVM client certificate is valid and present as /var/lib/gvm/CA/clientcert.pem.
OK: Your GVM certificate infrastructure passed validation.
Step 4: Checking gmd ...
OK: SCAP data found in /var/lib/gm/scap-data.
OK: CERT data found in /var/lib/gm/cert-data.
Step 5: Checking Postgresql DB and user ...
OK: PostgreSQL DB is present.
OK: Postgresql version and default port are OK.
gvmd _ |_ gvm |_ UTF8 |_ libe | en.US.UTF-8 | en.US.UTF-8 | | |
16440 [pg-gvm] [122.6]
At least one user exists.
Step 6: Checking Greenbone Security Assistant (GSA) ...
OK: Greenbone Security Assistant is present in version 24.7.0-git.
Step 7: Checking the GWM services are up and running ...
OK: gwm service is active.
Waiting for gwm service
OK: gwm service is active.
Starting gsd service
Waiting for gsd service
OK: gsd service is active.
Step 8: Checking few other requirements ...
OK: ssh-keygen found, LSC credential generation for GNU/Linux targets is likely to work.
OK: nmsis found, LSC credential package generation for Microsoft Windows targets is likely to work.
OK: xslproc found.
```

Selezione delle porte ed individuazione del target

IP: 192.168.50.106

The screenshot shows the Greenbone Security Assistant web interface. On the left, a sidebar navigation includes 'Dashboards', 'Scans', 'Assets', 'Resilience', 'Security Information', 'Configuration' (selected), 'Targets' (selected), 'Port Lists', 'Credentials', 'Scan Configs', 'Alerts', 'Schedules', 'Report Configs', 'Report Formats', 'Scanners', 'Filters', and 'Tags'. The main content area displays a 'Targets 0 of 0' section with a note: 'No targets available (Applied filter: sort=name first=1 rows=10)'. A modal window titled 'New Target' is centered, containing fields for 'Name' (metasploitable2), 'Comment' (esecuzione di una scansione completa su metà), 'Hosts' (set to 'Manual' with IP 192.168.50.106), 'Exclude Hosts' (set to 'Manual'), 'Allow simultaneous scanning via multiple IPs' (set to 'No'), 'Port List' (set to 'All IANA assigned TCP and UDP'), and 'Alive Test' (set to 'Scan Config Default'). Buttons for 'Cancel' and 'Save' are at the bottom.

Primi risultati della scansione

-host

The screenshot shows the 'Hosts' dashboard. The sidebar navigation is identical to the previous screen. The main area features three visualizations: 'Hosts by Severity Class (Total: 1)' (a pie chart with one segment labeled 'Low'), 'Hosts Topology' (a small network diagram), and 'Hosts by Modification Time (Total: 1)' (a line chart showing activity from Mon 15 to Wed 17). Below these is a table with columns: Name, Hostname, IP Address, OS, Severity, Modified, and Actions. One row is present: 192.168.50.106, 192.168.50.106, 2.3 (Low), Tue, Dec 16, 2025 7:56 PM Coordinated Universal Time. Buttons for 'Apply to page contents' and 'Print' are at the bottom right.

Sistema operativo

The screenshot shows the Greenbone Security Assistant web interface. The left sidebar is a navigation menu with the following items:

- Dashboard
- Scans
- Assets
- Hosts
- Operating Systems** (selected)
- TLS Certificates
- Resilience
- Security Information
- Configuration
- Administration
- Help

The main content area is titled "Operating Systems 1 of 1". It contains three visualizations:

- Operating Systems by Severity Class (Total: 1)**: A pie chart showing 1 item in the "Low" category.
- Most Vulnerable Operating Systems**: A bar chart showing one entry: "cpe:/o:linux:kernel" with a severity score of 2.1 (Low).
- Operating Systems by CVSS (Total: 1)**: A bar chart showing one entry: "cpe:/o:linux:kernel" with a CVSS score of 2.1.

Below these charts is a table listing the operating system details:

Name ↑↓	Title ↑↓	Severity			Hosts		Actions	
		Latest ↓	Highest ↑↓	Average ↑↓	All ↑↓	Best OS ↑↓	Modified ↑↓	
cpe:/o:linux:kernel		2.1 (Low)	2.1 (Low)	2.1 (Low)	1	1	Tue, Dec 16, 2025 7:56 PM Coordinated Universal Time	Edit Delete

At the bottom of the page, there is a note: "(Applied filter: sort-reverse=latest_severity first=1 rows=10)" and copyright information: "Copyright © 2009-2025 by Greenbone AG, www.greenbone.net".

The screenshot displays two main sections of the Greenbone Security Assistant web interface:

- Port List: All IANA assigned TCP** (Left Side):
 - Information:** Port Ranges (842), User Tags (0), Permissions (2).
 - Comment:** Version 20200827.
 - Port Count:** 5836
 - TCP Port Count:** 5836
 - UDP Port Count:** 0
 - Targets using this Port List:**
 - Target for new full scan - 2025-12-22 17:39:53
 - Target for new full scan - 2025-12-22 17:38:23
 - Target for FULL SCAN META - 2025-12-22 17:24:32
- Report: Coordinated Universal Time** (Right Side):
 - Mon, Dec 22, 2025 6:08 PM**
 - Report ID:** 3402906-4064-4ca8-a146-66a18dfb18e7ab=1
 - Created Time:** Mon, Dec 22, 2025 6:08 PM Coordinated Universal Time
 - Modified Time:** Mon, Dec 22, 2025 6:48 PM Coordinated Universal Time
 - Owner:** admin
 - Filter:** []
 - Results:** 1 of 601
 - Columns:** Vulnerability (severity), Hosts (IP), Ports (of 20), Applications (17 of 17), Operating Systems (1 of 1), CVEs (1 of 1), Closed CVEs (0 of 0), TLS Certificates (1 of 1), Error Messages (1 of 1), User Tags (0).
 - Row:** ICMP Timestamp Reply Information Disclosure, IP: 192.168.50.106, Severity: 2.1 (Low), QoD: 80 %, Host IP: 192.168.50.106, Name: general/icmp, Location: general/icmp, EPSS Score: N/A, Percentile: N/A, Created: Mon, Dec 22, 2025 6:41 PM Coordinated Universal Time.

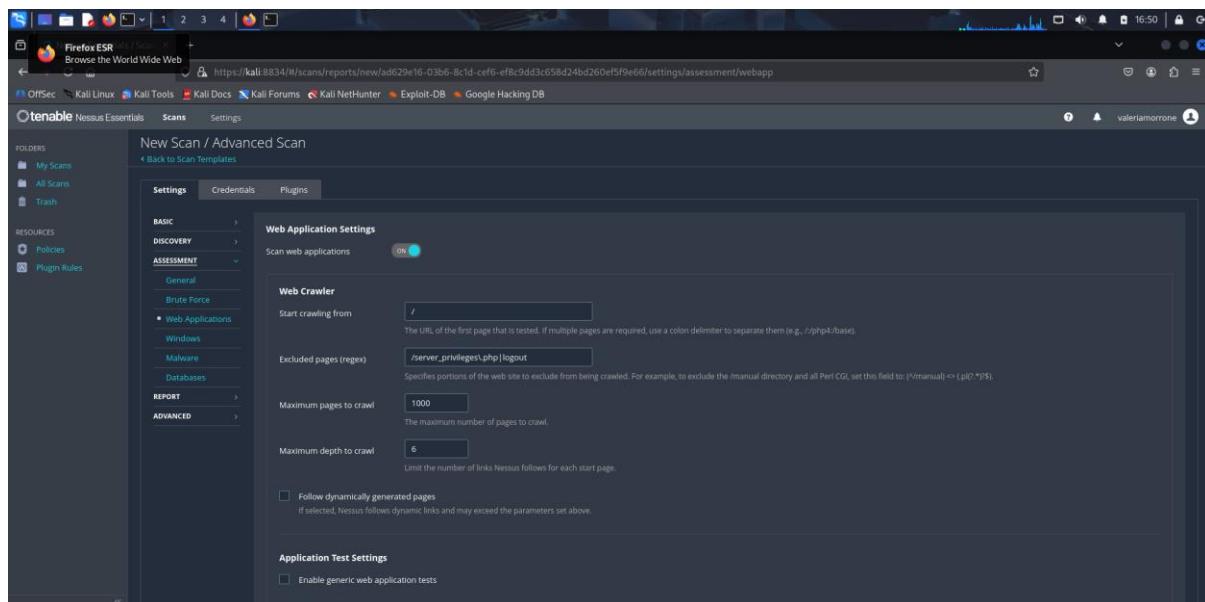
Sulla sezione report è possibile individuare e controllare quelle che sono le informazioni riguardanti la scansione.

/

Sono state effettuate varie scansioni ma non sono state trovate vulnerabilità sul target.

(è stato effettuato un tentativo anche con l'utilizzo dello scanner di rete Nessus ma non è andato a buon fine in quanto il programma consente un numero limitato di scansioni, per tale motivo l'attività è stata effettuata con il tool Greenbox.)

Segue immagine rappresentativa dei passaggi



The screenshot shows the 'New Scan / Advanced Scan' configuration interface. On the left, a sidebar lists 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules). The main panel is titled 'Malware Settings' under the 'Settings' tab. It includes sections for 'Scan for malware' (with an 'On' toggle), 'Hash and Allowlist Files' (with an 'Add File' button for Netstat IP Threat List), 'Provide your own list of known bad MD5/SHA1/SHA256 hashes' (with an 'Add File' button), and 'Hosts file allowlist' (with an 'Add File' button for system hosts files). A note at the bottom states: 'Nessus checks system hosts files for signs of a compromise (e.g., Plugin ID 23910 titled Compromised Windows System (hosts File Check)). This option allows you to upload a file containing a list of IPs and hostnames to be ignored by Nessus during a scan. Include one IP and one hostname (formatted identically to your hosts file on the target) per line in a regular text file.'

The screenshot shows the 'New Scan / Advanced Scan' configuration interface. The sidebar is identical to the previous screenshot. The main panel is titled 'General Settings' under the 'Discovery' tab. It includes a section for 'Collect Identity Data from Active Directory' (with a checked checkbox) and a note: 'Checking this box will enable collection of identity information from Active Directory using Domain User credentials.' At the bottom of the panel are 'Save' and 'Cancel' buttons.

Da una prima scansione effettuata le vulnerabilità sulla macchina risultano essere 54 che sono poi scese successivamente a 14.

NOTE FINALI:

Implementate le azioni di rimedio per le vulnerabilità scelte e con livello di gravità più elevato, si effettua l'esecuzione di una seconda scansione della rete che deve restituire un risultato diverso da quello della precedente.

Una volta avuta quindi una panoramica delle porte e dei servizi attivi è importante ridurre al minimo i tentativi di attacco.

Fine progetto 22/12/2025