

Report Esercizio 09/01/2025

Vulnerability Scanning Nessus Leonardo Catalano

“La traccia di oggi ci chiede di effettuare una scansione di Vulnerabilità sul target VM Metasploitable, utilizzando il programma Nessus, lo scopo è di fare pratica con lo strumento, la configurazione delle scansioni, e di familiarizzare con alcune vulnerabilità note.

Le fasi da effettuare saranno le seguenti:

1. Configurazione della scansione:

Target: Metasploitable

Porte: Solo le porte comuni (es. 21, 22, 23, 25, 80, 110, 139, 443, 445, 3389)

Tipo di Scansione tra:

Basic Network Scan: Configurazione predefinita per una scansione di rete.

Advanced Scan: Configurabile in base alle tue esigenze specifiche.

2. Esecuzione della scansione:

Avvio della scansione configurata su Nessus.

Attendi il completamento della scansione e assicurati che tutte le porte specificate siano state utilizzate.

3. Analisi del Report di Nessus:

Una volta completata la scansione, scarica e analizza il report generato da Nessus.

Per ogni vulnerabilità riportata, si dovrà leggere la descrizione fornita nel report e approfondire con i link suggeriti o altre risorse.”

In sintesi gli obiettivi dell'esercizio sono:

1. Pratica con Nessus:

Imparare a configurare e avviare scansioni con Nessus.

Capire come restringere le scansioni a porte specifiche.

2. Familiarizzazione con le Vulnerabilità:

Conoscere alcune delle vulnerabilità comuni che si possono incontrare.

Imparare a interpretare i risultati dei report di Nessus.

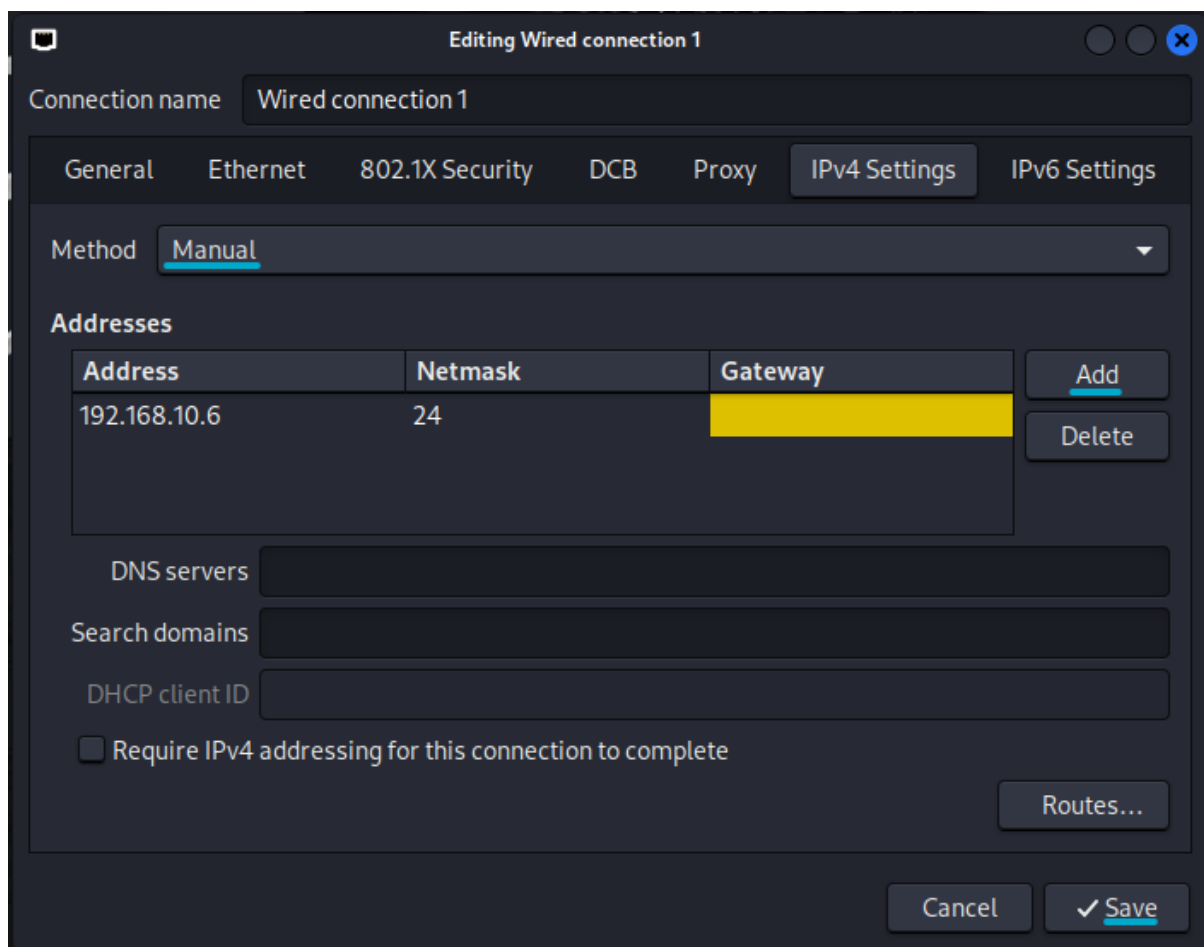
Sviluppare la capacità di approfondire e comprendere le vulnerabilità utilizzando risorse aggiuntive.

Preconfigurazione macchine virtuali:

Prima di tutto si configurano le VM per farle stare tutte nella stessa rete.
Come indirizzo di rete di riferimento uso il 192.168.10.0 /24.

-Macchina Kali Linux:

Per configurare l'indirizzo ipv4, si aprono le impostazioni della connessione, cliccando con il mouse destro sull'icona dell'ethernet, si va su IPv4 Settings, si cambia il metodo da DHCP a Manuale, si scrive l'indirizzo, si fa Add e si Salva.



Poi si disattiva la scheda di rete e la si riattiva e si va a verificare se l'indirizzo è stato assegnato correttamente aprendo la console e facendo il comando ifconfig o ip a.

```
kali@kali: ~  
File Actions Edit View Help  
Trash  
(kali@kali)-[~]  
$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 08:00:27:ad:25:87 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.10.6/24 brd 192.168.10.255 scope global noprefixroute eth0  
        valid_lft forever preferred_lft forever  
    inet6 fe80::8638:cc35:20dd:4129/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
(kali@kali)-[~]  
$
```

Come si può vedere l'indirizzo è stato configurato correttamente.

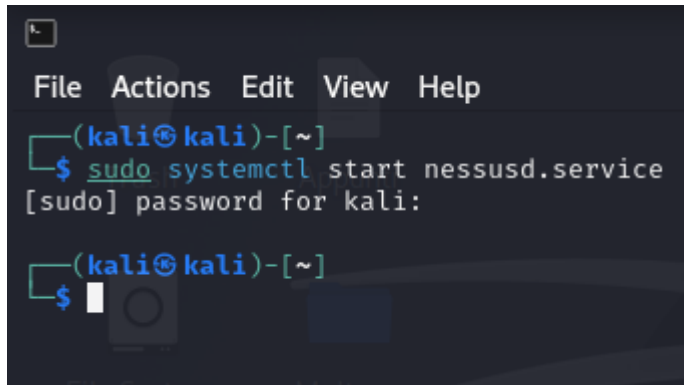
-Macchina Metasploitable:

Per configurare l'indirizzo ipv4 sulla macchina Metasploitable si utilizza il seguente comando: `sudo ifconfig eth0 192.168.10.8/24`

```
Metasploitable_2 [In esecuzione] - Oracle VirtualBox  
File Macchina Visualizza Inserimento Dispositivi Aiuto  
msfadmin@metasploitable:~$ sudo ifconfig eth0 192.168.10.8/24  
msfadmin@metasploitable:~$ msfadmin  
-bash: msfadmin: command not found  
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet  HWaddr 08:00:27:c1:13:61  
          inet addr:192.168.10.8  Bcast:192.168.10.255  Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fec1:1361/64  Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:48 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:101 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:4554 (4.4 KB)  TX bytes:14107 (13.7 KB)  
          Base address:0xd020 Memory:f0200000-f0220000  
  
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1  Mask:255.0.0.0  
          inet6 addr: ::1/128  Scope:Host  
          UP LOOPBACK RUNNING  MTU:16436  Metric:1  
          RX packets:127 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:127 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:36021 (35.1 KB)  TX bytes:36021 (35.1 KB)  
  
msfadmin@metasploitable:~$ _
```

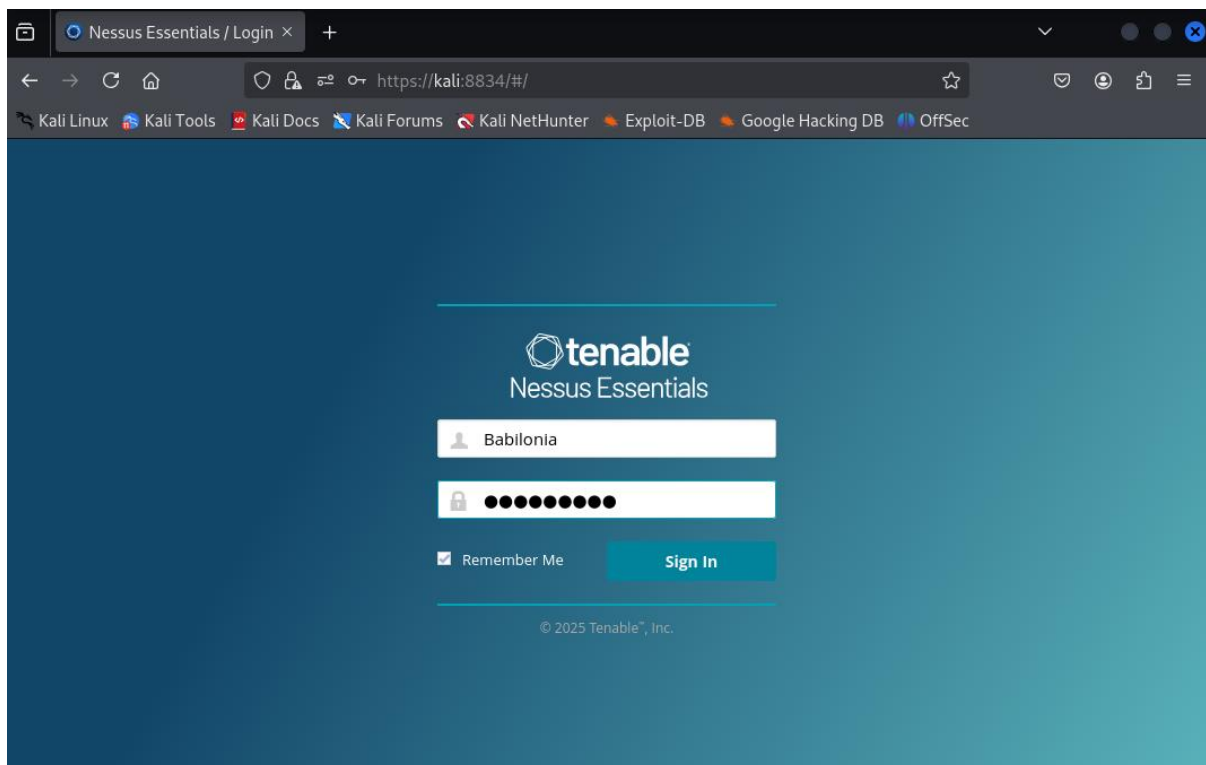
-Avvio del servizio Nessus:

Per prima cosa bisogna avviare il servizio Nessus, per fare ciò si utilizza il seguente comando : `sudo systemctl start nessusd.service`.

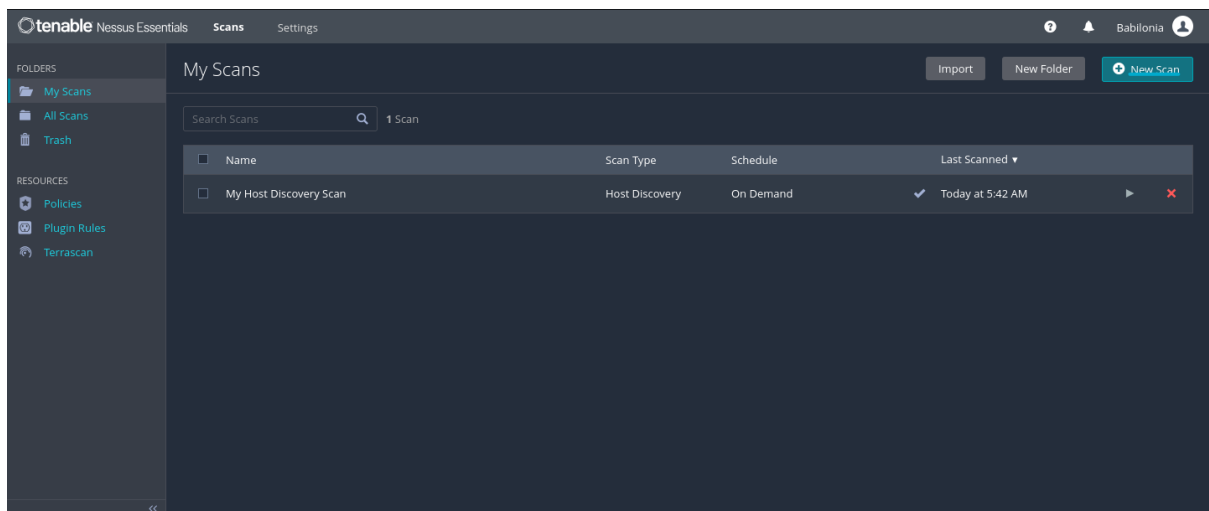


```
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo systemctl start nessusd.service
[sudo] password for kali:
(kali㉿kali)-[~]
$
```

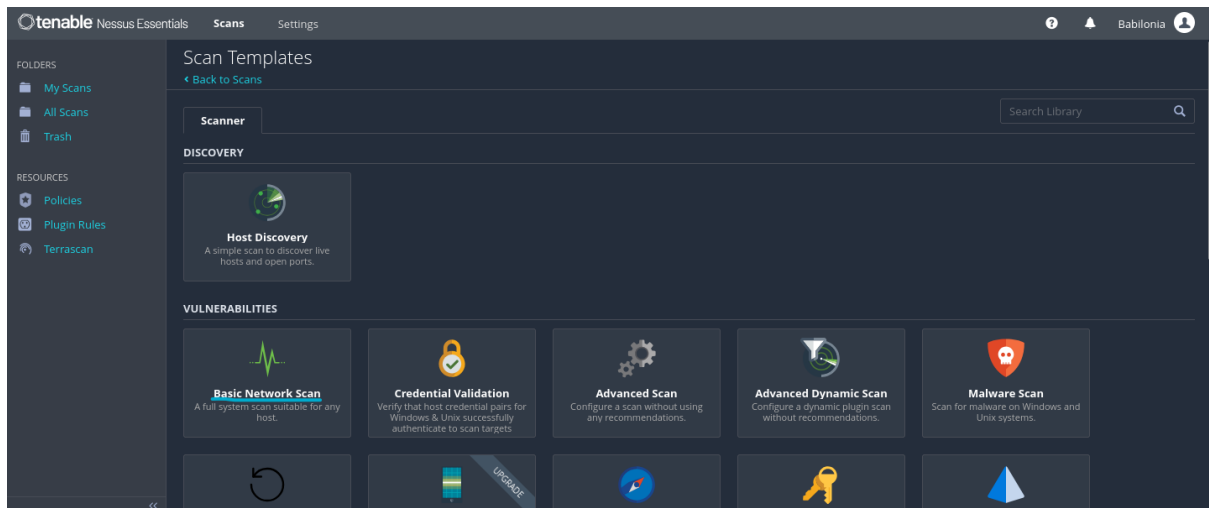
Per accedere al servizio abbiamo 2 modi: o ci connettiamo tramite la porta 8834, oppure tramite l'indirizzo ip di localhost 127.0.0.1, (nel mio caso uso la porta 8834).



Successivamente si andrà a creare una nuova scansione cliccando l'icona in alto a destra specifica :

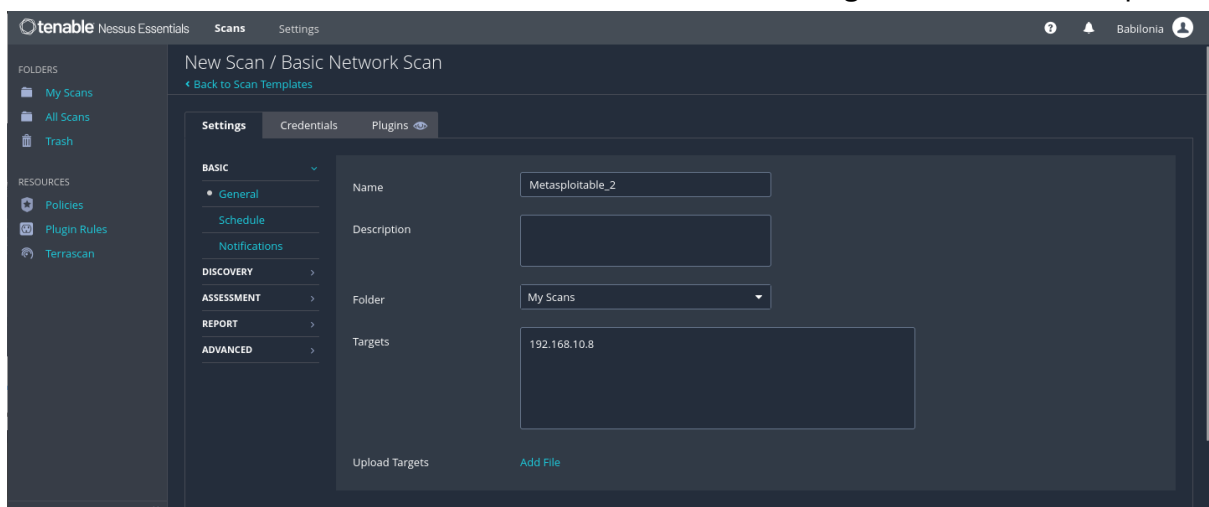


Poi si va a scegliere il tipo di scansione che si vuole effettuare e per mia scelta userò la scansione di base “Basic Network Scan”.



E si cominciano ad inserire le informazioni richieste per lo scan del target:

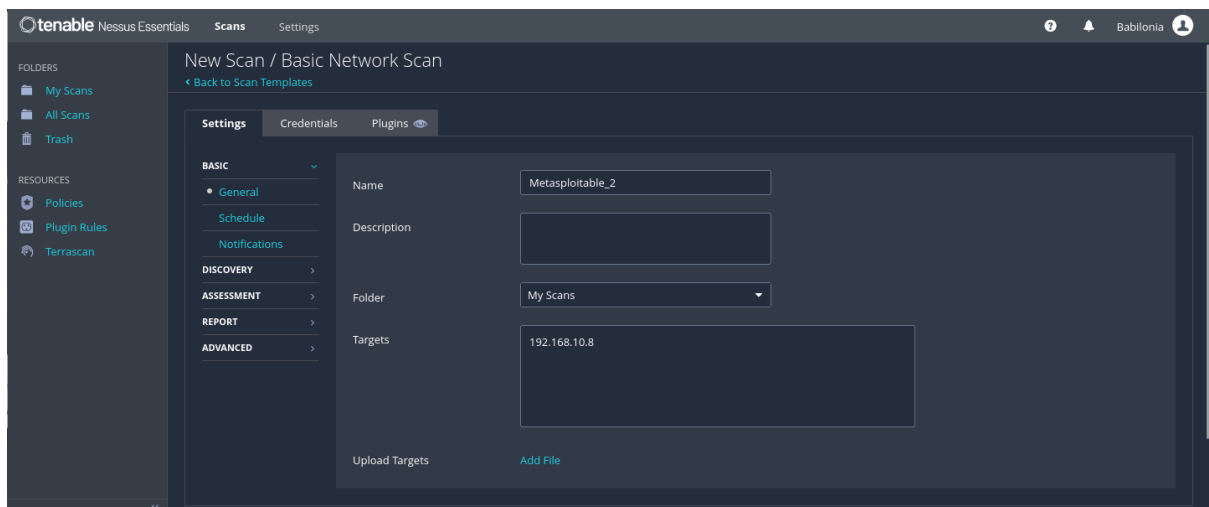
Nella sezione General indichiamo il nome della macchina target e il suo indirizzo ipv4



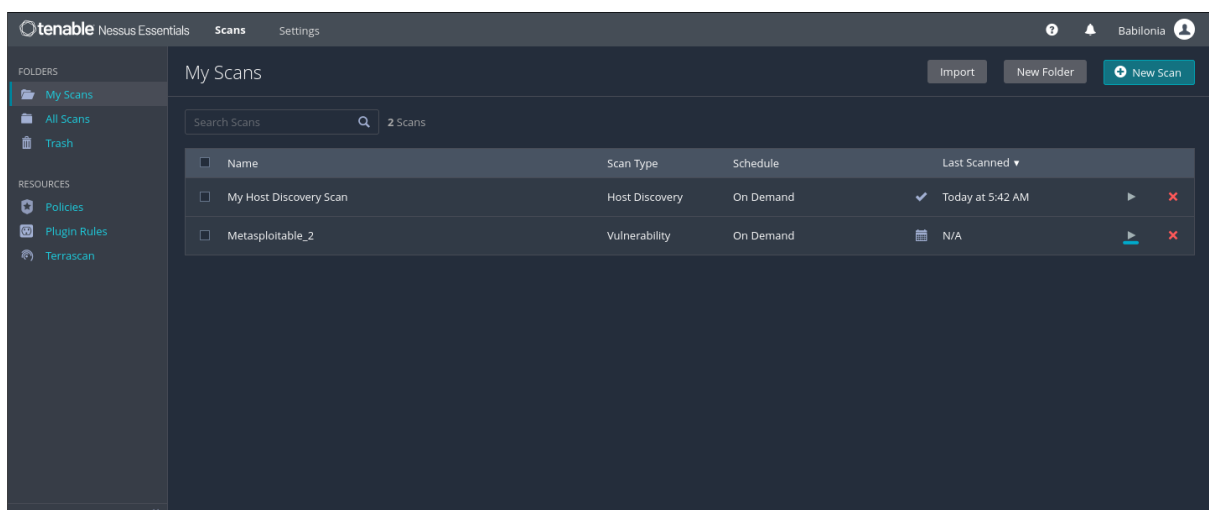
Nella sezione Discovery indichiamo il tipo di Port scan, tra common quindi le porte comuni per Nessus, tutte le porte o Custom dove gli andiamo a inserire noi nello

specifico le porte che deve scansionare.

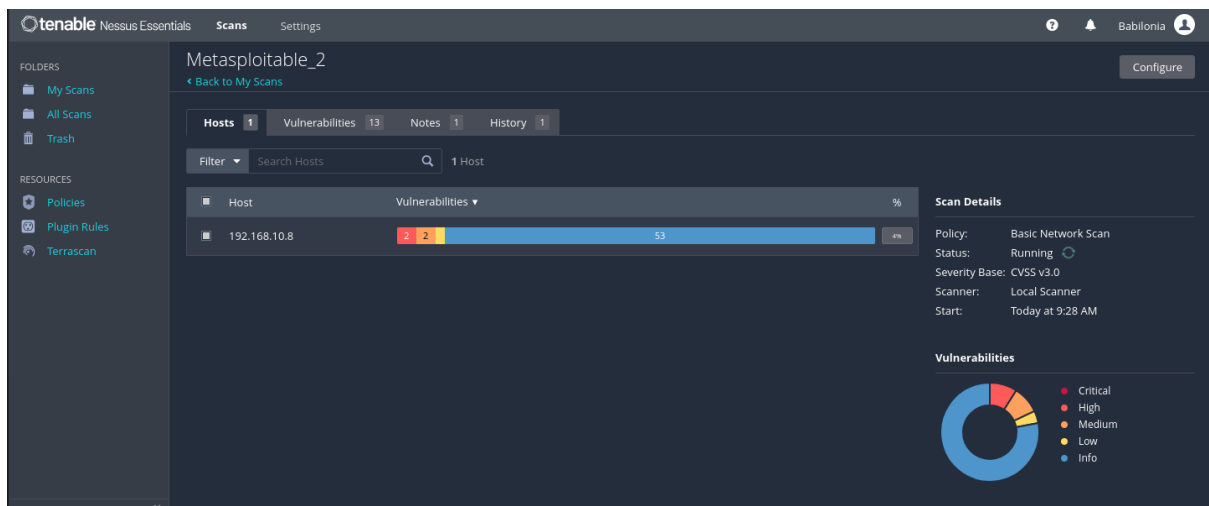
In questo caso utilizzeremo l'opzione Port scan (common ports):



Il resto delle impostazioni ho lasciato a Default, si salvano le impostazioni e si fa partire la Scansione:

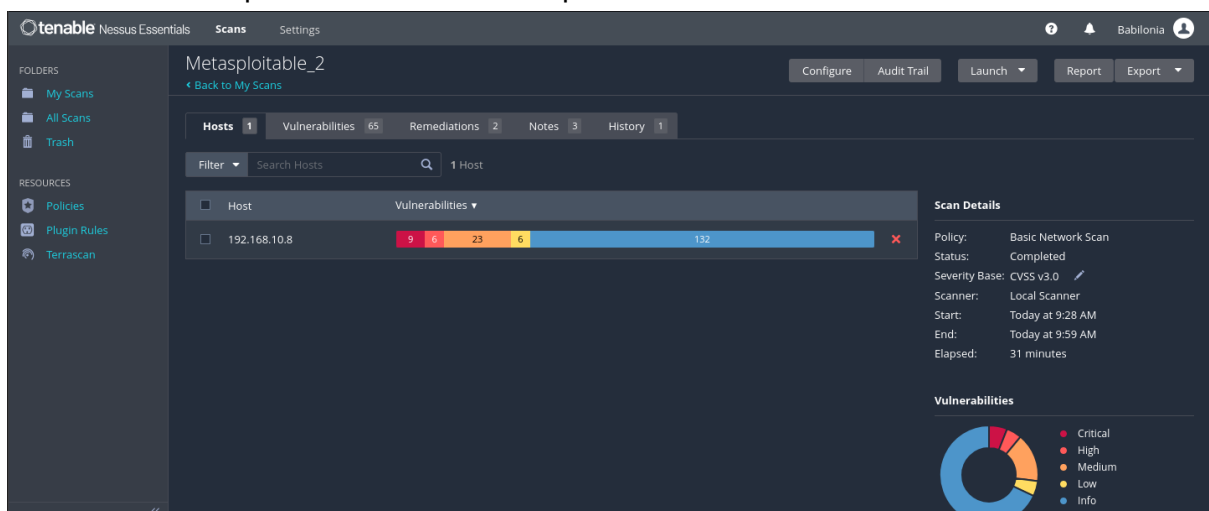


Se si clicca sul nome della scansione ci compariranno i dettagli della scansione delle vulnerabilità trovate e lo stato a % della scansione:



La scansione richiederà del tempo prima di essere completata del tutto.

A scansione completata la situazione è questa:



Metasploitable_2

← Back to My Scans

Configure Audit Trail Launch Report Export

Hosts 1 Vulnerabilities 65 Remediations 2 Notes 3 History 1

Filter Search Vulnerabilities

Severity	CVSS	VPR	EPSS	Name	Family	Count	Details
Critical	10.0	*		Win Server 'password' Password	Gain a shell remotely	1	✓
Critical	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2	✓
Critical	9.8			Bind Shell Backdoor Detection	Backdoors	1	✓
Info	—	—	—	Apache Tomcat (Multiple Issues)	Web Servers	4	✓
Critical	—	—	—	SSL (Multiple Issues)	Gain a shell remotely	3	✓
High	7.5	7.4	0.015	Hugin Service Detection	Service detection	1	✓
High	7.5	5.9	0.0489	Samba Badlock Vulnerability	General	1	✓
High	7.5			NFS Shares World Readable	RPC	1	✓
Info	—	—	—	SSL (Multiple Issues)	General	28	✓
Info	—	—	—	OC Bind (Multiple Issues)	DNS	5	✓
Medium	6.5			TLS Version 1.0 Protocol Detection	Service detection	2	✓
Medium	6.5			Unencrypted Telnet Server	Misc.	1	✓
Medium	5.9	4.4	0.003	SSL Anonymous Cipher Suites Supported	Service detection	1	✓
Medium	5.9	3.6	0.035	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened efcryption)	Misc.	1	✓
Info	—	—	—	HTTP (Multiple Issues)	Web Servers	5	✓
Info	—	—	—	DMB (Multiple Issues)	Misc.	2	✓
Info	—	—	—	TLS (Multiple Issues)	Misc.	2	✓
Info	—	—	—	TLS (Multiple Issues)	SMTP problems	2	✓
Low	3.7	4.5	0.9689	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Misc.	1	✓
Low	2.6	*		X Server Detection	Service detection	1	✓

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 9:28 AM
End: Today at 9:59 AM
Elapsed: 31 minutes

Vulnerabilities

Donut Chart: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue)

Ci sono diverse Vulnerabilità critiche o cmq di alto livello.

da linea di comando comincio la procedura per eseguire la scansione da Kali al target.

Per generare il Report si clicca in alto a destra sull'icona Report e si sceglie il formato di esso:

Generate Report

Report Format: ☐ HTML ☒ PDF ☐ CSV

Select a Report Template:

SYSTEM

- Complete List of Vulnerabilities by Host
- Detailed Vulnerabilities By Host**
- Detailed Vulnerabilities By Plugin
- Vulnerability Operations

Template Description:
This report presents detailed vulnerabilities by host.

Filters Applied:
None

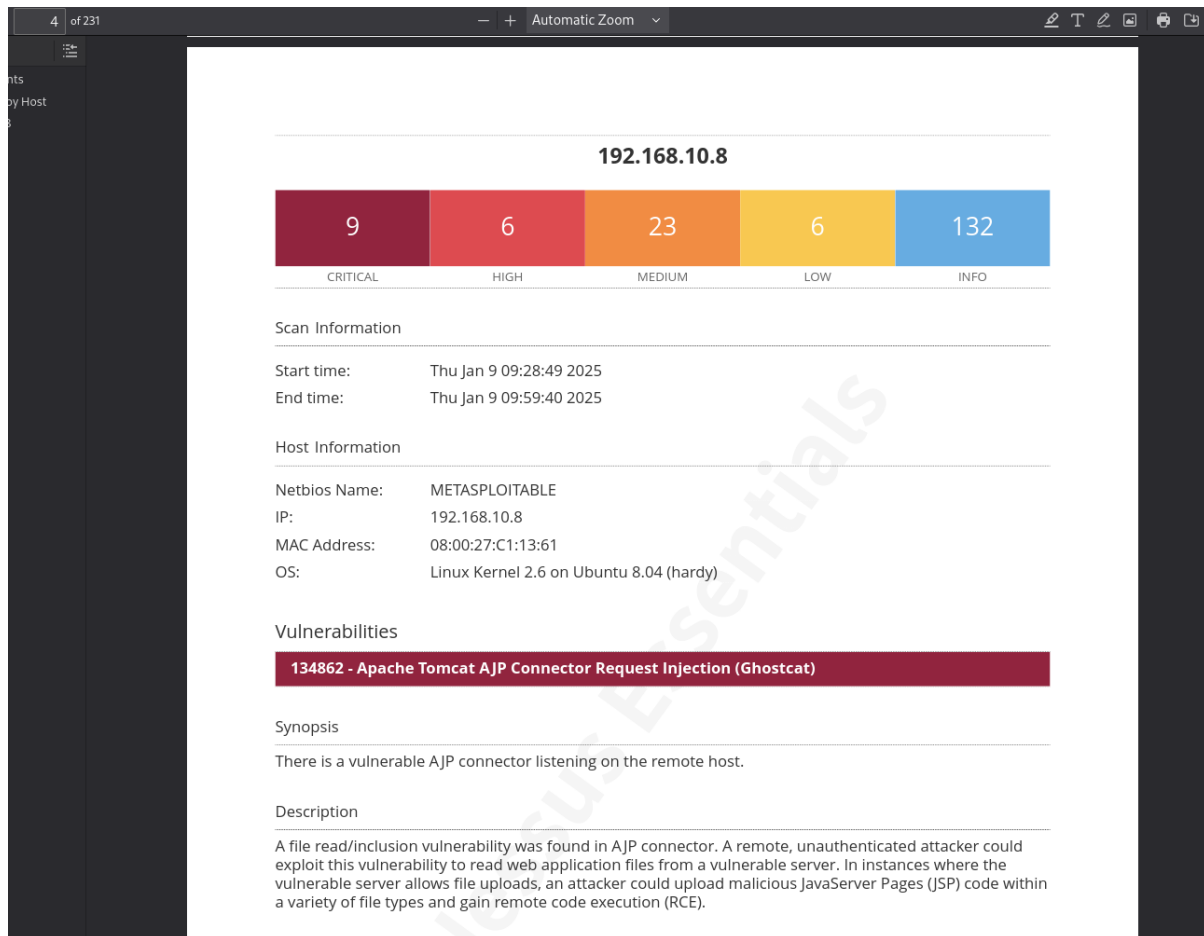
Formatting Options:
☒ Include page breaks between vulnerability results

In questo caso scelgo la linea Dettagliata perché così mi verrà fuori un report più completo.

A generazione del report dettagliato sono uscite 231 pagine dove si vanno ad analizzare le singole vulnerabilità partendo da quelle critiche segnate in rosso scuro a quelle inferiori fino a quelle di info al colore azzurro.

Andrò ad analizzare in questo caso soltanto alcune vulnerabilità critiche:

1) Vulnerabilità Critica Apache- Tomcat AJP Connector Request Injection (Ghostcat):



The screenshot displays the Nessus interface for a scan of host 192.168.10.8. At the top, a summary bar shows the distribution of vulnerability severity levels: 9 Critical, 6 High, 23 Medium, 6 Low, and 132 Info. Below this, the 'Scan Information' section indicates the scan was performed on Thursday, January 9, 2025, from 09:28:49 to 09:59:40. The 'Host Information' section identifies the host as 'METASPLOITABLE' with IP 192.168.10.8, MAC address 08:00:27:C1:13:61, and OS 'Linux Kernel 2.6 on Ubuntu 8.04 (hardy)'. The 'Vulnerabilities' section highlights a single Critical vulnerability: '134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat)'. The 'Synopsis' states: 'There is a vulnerable AJP connector listening on the remote host.' The 'Description' provides details: 'A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).'

Solution

Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.

Risk Factor

High

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

References

CVE	CVE-2020-1745
CVE	CVE-2020-1938
XREF	CISA-KNOWN-EXPLOITED:2022/03/17
XREF	CEA-ID:CEA-2020-0021

Nessus in generale ci dà un recap grafico con il numero di Vulnerabilità da quelle più critiche a quelle meno critiche, la durata della scansione con la fascia oraria d'esecuzione, i dettagli del nome, l'indirizzo ip e il sistema operativo della macchina target.

Per poi cominciare a specificare le Vulnerabilità singole una alla volta.

Come esempio per la prima possiamo vedere che è una Vulnerabilità critica, come Sinossi ci dice che è presente un connettore AJP in ascolto sull'host remoto.

Ciò significa che è stata rilevata una vulnerabilità di lettura/inclusione nel connettore AJP, e un utente malintenzionato da remoto non autenticato potrebbe sfruttare questa vulnerabilità, per leggere file di applicazioni web da un server vulnerabile, e nel caso in cui i server vulnerabili dovessero consentire il caricamento di file, un utente malintenzionato potrebbe caricare un suo codice interno dannoso di tipo JavaServer Pages (JSP), composto da varie variabili e tipi di file e ottenere l'esecuzione del suo codice da remoto (RCE).

Come soluzione Nessus ci dice di fare l'update della configurazione AJP, per richiedere l'autorizzazione e/o aggiornare il server Tomcat ad una versione più recente.

Nessus ci fornisce l'indice di fattore del rischio, che in questo caso è alto, il CVSS 9.8 indica lo score della vulnerabilità e infine nelle References possiamo notare che questa vulnerabilità è stata rilevata nel 2020.

2) Vulnerabilità Critica Apache Tomcat SEoL (<= 5.5x):

171340 - Apache Tomcat SEoL (<= 5.5.x)

Synopsis

An unsupported version of Apache Tomcat is installed on the remote host.

Description

According to its version, Apache Tomcat is less than or equal to 5.5.x. It is, therefore, no longer maintained by its vendor or provider.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

See Also

<https://tomcat.apache.org/tomcat-55-eol.html>

Solution

Upgrade to a version of Apache Tomcat that is currently supported.

Risk Factor

Critical

CVSS v3.0 Base Score

10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Plugin Information

Published: 2023/02/10, Modified: 2024/05/06

Plugin Output

tcp/8180/www

```
URL : http://192.168.10.8:8180/
Installed version : 5.5
Security End of Life : September 30, 2012
Time since Security End of Life (Est.) : >= 12 years
```

Sinassi:

Una versione ormai non più supportata di Apache Tomcat è installata nella macchina.

Descrizione:

Secondo la versione, Apache Tomcat è inferiore o uguale a 5.5, pertanto ormai non è più mantenuta aggiornata dal produttore.

La mancanza di supporto e aggiornamento implica che il fornitore non rilascerà più nessuna patch di sicurezza per quel tipo di prodotto/versione, quindi ormai questa versione potrebbe contenere vulnerabilità di sicurezza.

Soluzione:

Effettuare l'Upgrade ad una versione Apache Tomcat che è attualmente supportata e aggiornata.

Fattore rischio:

Critico

CVSS 10.0 Base Score

Inoltre abbiamo anche l'informazione a che anno è aggiornata la configurazione di sicurezza di questo Apache Tomcat e risale al 2012.

3) Bind Shell Backdoor Detection:

51988 - Bind Shell Backdoor Detection
Synopsis
The remote host may have been compromised.
Description
A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.
Solution
Verify if the remote host has been compromised, and reinstall the system if necessary.
Risk Factor
Critical
CVSS v3.0 Base Score
9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
CVSS v2.0 Base Score
10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)
Plugin Information
Published: 2011/02/15, Modified: 2022/04/11

Sinassi:

L'host remoto può essere stato compromesso.

Descrizione:

Una Shell è in ascolto sulla porta remota, senza che ci sia alcuna richiesta d'autenticazione.

Un utente malintenzionato può usarla per collegarsi alla porta remota e inviare comandi direttamente da lì.

Soluzione:

Verificare se l'host remoto è stato compromesso e, se necessario, reinstallare da 0 il sistema.

Fattore rischio:

Critico

CVSS 9.8 Base Score

