

VULNERABILITY ASSESSTMENT REPORT

NESSUS

KALI LINUX → METASPLOITABLE

INDICE

- 1.MACCHINE VIRTUALI**
- 2.SCANSIONE VULNERABILITA' NESSUS**
- 3.ANALISI VULNERABILITA'**
- 4.REMEDIATION**
- 5.CONCLUSIONI/RACCOMANDAZIONI**

1.MACCHINE VIRTUALI

Oggi siamo qui per eseguire una vulnerability scan tramite Nessus dalla nostra macchina virtuale Kali Linux sulla macchina virtuale Metasploitable.

Entrambe le macchine hanno la scheda di rete in Bridge e comunicano tra di loro facendo la prova di ping.

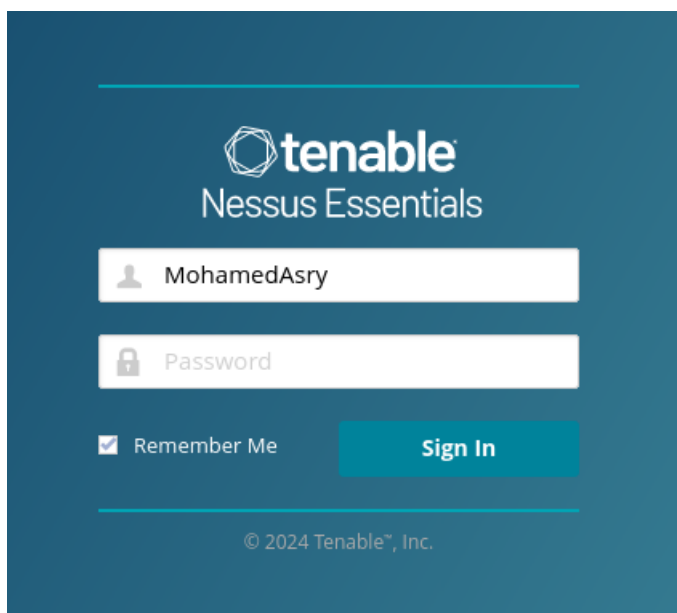
Kali Linux ha accesso alla rete internet.

2.SCANSIONE VULNERABILITA' NESSUS

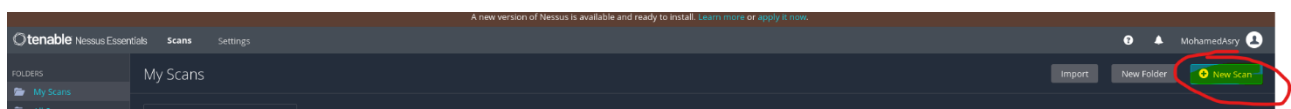
Prima di tutto avviamo Nessus dal terminale di Kali Linux con il seguente comando:

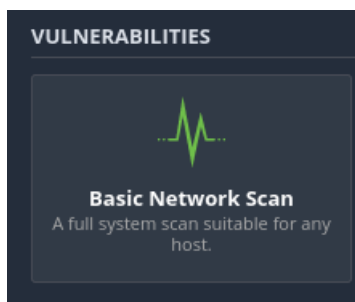
```
(kali@kali)~[~]  
$ sudo systemctl start nessus.service
```

Dopo di che lo scanner sarà attivo sulla pagina <https://kali:8834/> in cui faremo il login e attiveremo il servizio.



Dopo il login possiamo avviare la nostra scansione per individuare le vulnerabilità più critiche presenti sulla nostra VM Metasploitable.





Avviamo una nuova scansione scegliendo la Basic Network Scan inserendo nome, descrizione e come target l'IP della VM Metasploitable che sarebbe 192.168.178.202.

Infine nelle impostazioni, nella sezione discovery, scegliamo Port scan (common ports) per impostare il tipo di scansione.

Avviamo la scansione ed una volta completata le vulnerabilità rilevate sono le seguenti:

Vulnerabilities 67								
Filter	Search Vulnerabilities						67 Vulnerabilities	
Sev	CVSS	VPR	Name	Family	Count			
<input type="checkbox"/> CRITICAL	10.0	5.9	NFS Exported Share Information Disclosure	RPC	1			
<input type="checkbox"/> CRITICAL	10.0		SSL Version 2 and 3 Protocol Detection	Service detection	2			
<input type="checkbox"/> CRITICAL	10.0		Bind Shell Backdoor Detection	Backdoors	1			
<input type="checkbox"/> CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1			
<input type="checkbox"/> CRITICAL	10.0		VNC Server 'password' Password	Gain a shell remotely	1			
<input type="checkbox"/> CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3			
<input type="checkbox"/> HIGH	7.5	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1			
<input type="checkbox"/> HIGH	7.5	5.9	rlogin Service Detection	Service detection	1			
<input type="checkbox"/> MEDIUM	6.8	5.9	Samba Badlock Vulnerability	General	1			
<input type="checkbox"/> MEDIUM	6.1		TLS Version 1.0 Protocol Detection	Service detection	2			
<input type="checkbox"/> MEDIUM	5.8		Unencrypted Telnet Server	Misc.	1			

Host Details
IP: 192.168.178.202
MAC: 08:00:27:F9:69:C2
OS: Linux Kernel 2.6 on Ubuntu 8 (hardy)
Start: Today at 1:53 PM
End: Today at 2:03 PM
Elapsed: 10 minutes
KB: [Download](#)

Vulnerabilities

3.ANALISI VULNERABILITA'

Le vulnerabilità critiche che analizzeremo e a cui rimedieremo sono le seguenti:

-SSL Version 2 and 3 Protocol detection


-VNC Server “password” Password

La prima vulnerabilità è dovuta al fatto che i protocolli di comunicazione utilizzati, SSL 2.0 e/o SSL 3.0, siano ormai obsoleti e con molte lacune di sicurezza che potrebbero essere facilmente “exploitate” da un’eventuale hacker attaccante per eseguire un attacco “man-in-the-middle” o per decriptare il contenuto delle comunicazioni tra service e client.

La seconda vulnerabilità invece è dovuta al fatto che la password del server VNC sia troppo “debole” e di conseguenza facilmente “exploitabile” da malintenzionati per avere accesso e controllo del server.

4.REMEDIATION

1) Per risolvere la prima vulnerabilità riguardante i protocolli di comunicazione crittografati bisogna disattivare quei due vecchi protocolli obsoleti e lasciare attivo il protocollo di comunicazione TLS che è una versione più recente e che risolve alcune vulnerabilità di sicurezza dei precedenti protocolli di comunicazione.



```
GNU nano 2.0.7 File: /etc/apache2/mods-available/ssl.conf
SSLProtocol all -SSLv2 -SSLv3

[ Wrote 2 lines ]
msfadmin@metasploitable:~$
```

Eseguiamo il comando sul terminale di Metasploitable con i permessi di root (**sudo nano** /etc/apache2/mods-available/ssl.conf.) e modifichiamo la cartella dei protocolli SSL con la dicitura nell’immagine soprastante. Salviamo le modifiche, usciamo dalla cartella(ctrl o + ctrl x) e riavviamo la macchina con il comando sudo reboot.

Ora i protocolli obsoleti sono stati disabilitati e le comunicazioni crittografate tra client e server saranno eseguite con il protocollo TLS (Transport Layer Security) abilitato che è più sicuro.

2) La seconda vulnerabilità è quella che riguarda la password del server VNC che possiamo risolvere semplicemente cambiando la password con la seguente procedura:

```
metasploitable login: msfadmin
Password:
Last login: Wed May 15 07:18:20 EDT 2024 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
Password:
Warning: password truncated to the length of 8.
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Warning: password truncated to the length of 8.
Verify:
msfadmin@metasploitable:~$ vncpasswd
```

Dal terminale di Metasploitable eseguiamo il comando “vncpasswd”, inseriamo la nuova password più “forte” e sicura (8+ caratteri alfanumerici, lettere maiuscole e minuscole, caratteri speciali) una volta e la reinseriamo di nuovo per verificare che sia stata digitata correttamente. Anche in questo caso riavviamo la VM con il comando “sudo reboot” per far sì che salvi le modifiche e inseriamo la nuova password per verificare l’efficacia della nostra modifica.

5.CONCLUSIONI/RACCOMANDAZIONI

Le vulnerabilità individuate non sono poche e le azioni di rimedio per tutte sono di vario tipo. Per le vulnerabilità analizzate in questo report le mie raccomandazioni sarebbero di tenere sempre d’occhio i protocolli di comunicazione crittografati e aggiornarli quando possibile con l’ultima versione disponibile e di modificare la password del server VNC con cadenza bimestrale o trimestrale con una password sempre complessa e mai simile alla precedente.