

S5_L5

Progetto

23 febbraio 2024

Traccia

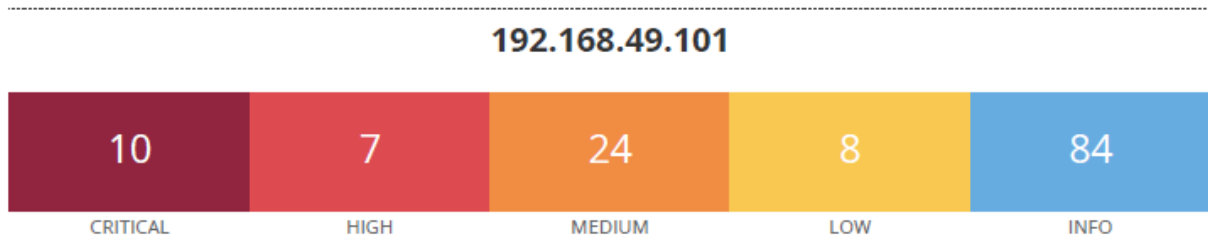
Effettuare una scansione completa sul target Metasploitable. Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità critiche / high e provate ad implementare delle azioni di rimedio.

N.B. le azioni di rimedio, in questa fase, potrebbero anche essere delle regole firewall ben configurate in modo da limitare eventualmente le esposizioni dei servizi vulnerabili. Vi consigliamo tuttavia di utilizzare magari questo approccio per non più di una vulnerabilità.

Per dimostrare l'efficacia delle azioni di rimedio, eseguite nuovamente la scansione sul target e confrontate i risultati con quelli precedentemente ottenuti.

Risultati della scansione

A seguito della scansione effettuata sulla macchina di Metasploit mediante il programma Nessus, quest'ultimo ha generato il report allegato in fondo alla relazione, di seguito riporto i risultati ottenuti



<input type="checkbox"/>	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		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	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1	⊙ ✎
<input type="checkbox"/>	CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2	⊙ ✎
<input type="checkbox"/>	CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1	⊙ ✎
<input type="checkbox"/>	CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3	⊙ ✎
<input type="checkbox"/>	HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1	⊙ ✎
<input type="checkbox"/>	HIGH	7.5		NFS Shares World Readable	RPC	1	⊙ ✎

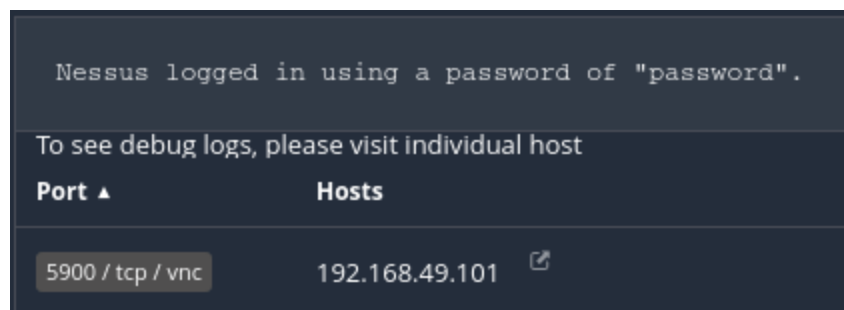
Analisi - Vulnerabilità critiche

61708 - VNC Server 'password' Password

Descrizione: Il server VNC in esecuzione sull'host remoto è protetto con una password debole. Nessus è riuscito ad accedere utilizzando l'autenticazione VNC e una password "password". Un utente malintenzionato remoto e non autenticato potrebbe sfruttarlo per prendere il controllo del sistema.

Soluzione: Proteggi il servizio VNC con una password complessa.


CVSS v2: Fattore di rischio: **Critico** - Punteggio **10**



The screenshot shows a terminal window with the following text:

```
Nessus logged in using a password of "password".
```

Below this, a message says: "To see debug logs, please visit individual host".

Port ▲	Hosts
5900 / tcp / vnc	192.168.49.101 

REMEDIATION ACTION

Andiamo a cambiare la password del server VNC, tramite il terminale di meta. Con il comando **sudo su** otteniamo i privilegi di amministratore, e tramite il comando **vncpasswd** andiamo a cambiare la password "password" con una più sicura, nel nostro caso "MsfAdm1n".

```

File Macchina Visualizza Inserimento Dispositivi Aiuto
msfadmin@metasploitable:~$ sudo su
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n

```

51988 - Bind Shell Backdoor Detection

Descrizione: Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può collegarsi alla porta remota ed inviare comandi direttamente.

Soluzione: Verifica se l'host remoto è stato compromesso e, se necessario, reinstallare il sistema.

CVSS v3: Fattore di rischio: **Critico** - Punteggio **9.8**

```

Output

Nessus was able to execute the command "id" using the
following request :

This produced the following truncated output (limited to 10 lines) :
----- snip -----
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#
----- snip -----

To see debug logs, please visit individual host

```

Port ▲	Hosts
1524 / tcp / wild_shell	192.168.49.101 🔗

REMEDIATION ACTION

Questa criticità indica la presenza di una backdoor in ascolto sulla porta 1524. Per risolvere tale problematica possiamo adottare due soluzioni:

- A. Chiudere la porta
- B. Applicare delle regole firewall che blocchino il traffico verso la porta

SOLUZIONE A - CHIUSURA DELLA PORTA

Dal terminale di meta verifichiamo lo stato della porta tramite il comando `netstat` ed i parametri `-tulnp` (`-t` tcp; `-u` udp; `-l` listening solo le porte in ascolto; `-p` program mostra il nome del programma che la sta utilizzando; `-n` numeric).

L'output sarà una lista di tutte le porte in ascolto, lo andiamo a filtrare tramite il comando `grep` "port_id". Ci verrà restituito lo stato della porta ed il processo che la sta utilizzando

```
root@metasploitable:~# sudo netstat -tulnp | grep 1524
tcp        0      0 0.0.0.0:1524        0.0.0.0:*          LISTEN
4500/xinetd
```

Tramite il comando `sudo kill "numero_processo"`, terminiamo il processo individuato.

```
root@metasploitable:~# sudo kill 4500
```

Verifichiamo la chiusura della porta tramite il portale di kali ed il comando `netstat`.

```
(kali㉿kali)-[~]
$ sudo nmap -sS -p 1524 192.168.49.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 06:31 EST
Nmap scan report for 192.168.49.101
Host is up (0.00075s latency).

PORT      STATE SERVICE
1524/tcp  closed ingreslock

Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds
```

SOLUZIONE B - CREAZIONE REGOLA FIREWALL

Creiamo una regola firewall che blocchi le connessioni provenienti da qualunque indirizzo verso la porta di Meta

<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP	*	*	192.168.49.101	1524	*	none
--------------------------	-------------------------------------	-------	----------	---	---	----------------	------	---	------

Effettuando un test con nmap possiamo verificare l'efficacia di tale policy.

```
(kali@kali)-[~]
$ sudo nmap -sS -p 1524 192.168.49.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 09:02 EST
Nmap scan report for 192.168.49.101
Host is up (0.00061s latency).

PORT      STATE      SERVICE
1524/tcp  filtered  ingreslock

Nmap done: 1 IP address (1 host up) scanned in 0.60 seconds
```

11356 - NFS Exported Share Information Disclosure

Descrizione: Almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere controllate da un host in scansione. L'attaccante potrebbe essere in grado di sfruttare questa vulnerabilità per leggere (ed eventualmente scrivere) file sull'host remoto.

L'NFS è un file system che consente a computer client di utilizzare la rete per accedere a directory condivise da server remoti come fossero disponibili in locale.

Soluzione: Configurare NFS sull'host remoto in modo che solo gli host autorizzati possano montare le sue condivisioni remote.

CVSS v2: Fattore di rischio: **Critico** - Punteggio **10**

REMEDIATION ACTION

Dal terminale di Meta andiamo a modificare il file di configurazione, nello specifico modifichiamo il file exports, dove andiamo a modificare i permessi di scrittura e lettura che (come in figura" erano abilitati per tutti gli utenti

```
GNU nano 2.0.7      File: exports
# /etc/exports: the access control list for filesystems which may be exported
#               to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes      hostname1(rw,sync) hostname2(ro,sync)
#
# Example for NFSv4:
# /srv/nfs4       gss/krb5i(rw,sync,fsid=0,crossmnt)
# /srv/nfs4/homes gss/krb5i(rw,sync)
#
#
# *(rw,sync,no_root_squash,no_subtree_check)
```

134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat)

Descrizione: È stata rilevata una vulnerabilità di lettura/inclusione di file nel connettore AJP. Un utente malintenzionato remoto e non autenticato potrebbe sfruttare questa vulnerabilità per leggere file di applicazioni web da un server vulnerabile. Nei casi in cui il server vulnerabile consenta il caricamento di file, un utente malintenzionato potrebbe caricare al suo interno codice dannoso JavaServer Pages (JSP) codice con una varietà di tipi di file e ottenere l'esecuzione di codice remoto (RCE).

Soluzione: Aggiornare la configurazione AJP per richiedere l'autorizzazione e/o aggiornare il server Tomcat alla versione 7.0.100, 8.5.51, 9.0.31 o successiva.

CVSS v3: Fattore di rischio: **Critico** - Punteggio **9.4**

REMEDIATION ACTION

Questa criticità indica la presenza di una vulnerabilità sulla porta utilizzata dal servizio. Per risolvere tale problematica possiamo adottare due soluzioni:

- A. Chiudere la porta (come visto sopra)
- B. Applicare delle regole firewall che blocchino il traffico verso la porta

Per aggiornare Apache all'ultima versione vanno eseguite le seguenti operazioni dal terminale di Meta:

1. Verificare la versione di apache

```
root@metasploitable:/etc#  
root@metasploitable:/etc# sudo apache2 -v  
Server version: Apache/2.2.8 (Ubuntu)  
Server built:   Mar  9 2010 20:45:36
```

2. Aggiungere il repository di apache

```
root@metasploitable:/etc# sudo add-apt-repository ppa>ondrej&apache2  
sudo: add-apt-repository: command not found  
[1] 364  
apache2: bad user name ${APACHE_RUN_USER}  
[1]+  Exit 1                  sudo add-apt-repository ppa > ondrej
```

3. Scaricare gli aggiornamenti: `sudo apt update`
4. Installare gli aggiornamenti: `sudo apt upgrade`
5. Verificare la nuova versione di apache: `sudo apache2 -v`

Valutazioni finali

In base all'analisi condotta sulla sicurezza informatica del sistema, si presentano di seguito le valutazioni finali insieme alle raccomandazioni per migliorare la robustezza complessiva della sicurezza:

Sommario delle Vulnerabilità:

Sono state identificate diverse vulnerabilità, suddivise in quattro categorie principali: critiche, elevate, moderate e basse. Le vulnerabilità critiche rappresentano un rischio significativo per la sicurezza del sistema e richiedono azioni immediate

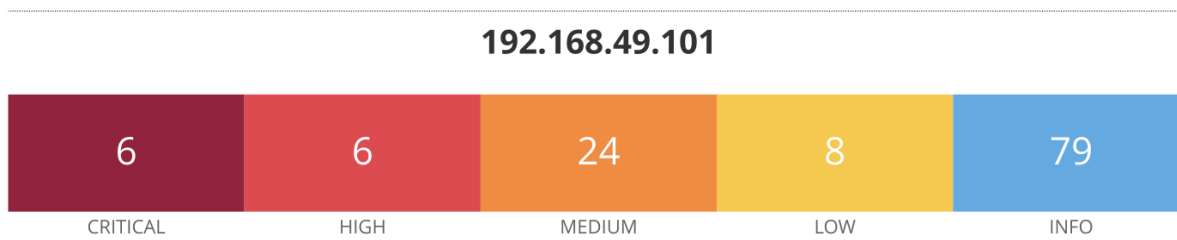
Valutazione del Rischio:

Il rischio associato alle vulnerabilità è stato valutato considerando l'impatto sulla riservatezza, integrità e disponibilità dei dati.

Le vulnerabilità critiche presentavano un rischio elevato, mentre quelle di livello moderato richiedono attenzione per prevenire l'aggravamento.

Conclusione

L'implementazione delle remediation action fornite ha contribuito in modo significativo a rafforzare la sicurezza del sistema, riducendo il rischio di violazioni e proteggendo l'integrità delle informazioni. La scansione effettuata in seguito mostra l'effettivo miglioramento della sicurezza.



Scan post remediation Action / 192.168.49.101 Configure Audit Tra

[Back to Hosts](#)

Vulnerabilities 70

Filter 70 Vulnerabilities

<input type="checkbox"/>	Sev ▼	CVSS ▼	VPR ▼	Name ▲	Family ▲	Count ▼	
<input type="checkbox"/>	CRITICAL	10.0		Unix Operating System Unsupported Version De...	General	1	
<input type="checkbox"/>	CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2	
<input type="checkbox"/>	MIXED	Phpmyadmin (Multiple Issues)	CGI abuses	4	
<input type="checkbox"/>	CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3	
<input type="checkbox"/>	MIXED	PHP (Multiple Issues)	CGI abuses	3	
<input type="checkbox"/>	HIGH	7.5	5.9	Samba Badlock Vulnerability	General	1	
<input type="checkbox"/>	MIXED	SSL (Multiple Issues)	General	28	