

Report di Scansione di Vulnerabilità

Data della scansione: 27/10/2023

Sistema Scansionato: Metasploitable – 192.168.1.80

Riepilogo delle principali vulnerabilità critiche

Sev ▼	CVSS ▼	VPR ▼	Name ▲	Family ▲
<input type="checkbox"/> CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC
<input type="checkbox"/> CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General
<input type="checkbox"/> CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely
<input type="checkbox"/> CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors

1. NFS Exported Share Information Disclosure

- Descrizione: almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione. Un aggressore potrebbe sfruttare questa situazione per leggere (e, eventualmente,

2. Bind Shell Backdoor Detection

- Descrizione: è presente una shell in ascolto sulla porta remota senza richiedere alcuna autenticazione. Un aggressore potrebbe utilizzarla collegandosi alla porta remota e inviando comandi direttamente.

3. VNC Server 'password' Password

- Descrizione: il server VNC in esecuzione sull' host remoto è protetto da una password debole. Nessus è stato in grado di effettuare l'accesso utilizzando l'autenticazione VNC e una password 'password'. Un aggressore remoto e non autenticato potrebbe sfruttare questa situazione per prendere il controllo del sistema."

Azioni necessarie

- NFS Exported Share Information Disclosure

Per mitigare questa vulnerabilità, è consigliabile prendere le seguenti misure:

- Configurare l'accesso NFS in modo appropriato: assicurarsi che solo gli host autorizzati possano accedere alle condivisioni NFS. Modificare il file di configurazione NFS (/etc/exports) per specificare gli host o le reti consentiti e le relative autorizzazioni.
- Utilizzare l'autenticazione: Configura l'autenticazione basata su chiavi o nome utente/password per le condivisioni NFS, in modo da richiedere l'autenticazione dell'utente prima di concedere l'accesso.
- Monitoraggio e registrazione: Configura un sistema di monitoraggio e registrazione per rilevare eventuali tentativi di accesso non autorizzati alle condivisioni NFS. In questo modo, sarai in grado di rilevare e rispondere prontamente agli accessi non autorizzati.
- Mantenere il software NFS aggiornato: Assicurati di utilizzare una versione aggiornata del software NFS, in modo da beneficiare delle correzioni di sicurezza più recenti.
- Limitare l'accesso alle sole condivisioni necessarie: Configura il server NFS in modo da esportare solo le condivisioni necessarie per le operazioni quotidiane e disabilita o rimuovi quelle non necessarie.
- Implementando queste misure, è possibile ridurre il rischio di divulgazione delle informazioni sulle condivisioni NFS esportate e proteggere meglio il sistema da potenziali attacchi.

In questo caso abbiamo modificato il file di configurazione in modo da autorizzare l'accesso ai files ai soli ip specificati.

```
GNU nano 2.0.7      File: /etc/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)
#
192.168.1.80(rw,sync,no_root_squash,no_subtree_check)
192.168.1.60(ro,sync,no_root_squash,no_subtree_check)
```

- **Bind Shell Backdoor Detection**

Identificazione della backdoor: lo scanner Nessus ha individuato la porta 1524 / tcp / wild\_shell.

Per proteggerci dall'eventuale utilizzo di questa porta, siamo andati a modificare le impostazioni del firewall nativo dell'host, andando a inserire una regola DENY per la suddetta porta.

```
msfadmin@metasploitable:~$ sudo ufw status
Firewall loaded

To Action From
--
1524:tcp DENY Anywhere
1524:udp DENY Anywhere

msfadmin@metasploitable:~$
```

- **VNC Server 'password' Password**

Un semplice rimedio è la modifica della password VNC da "password" a una password robusta e complessa. La password dovrebbe contenere una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali e avere una lunghezza sufficiente.




```
msfadmin@metasploitable:~$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
msfadmin@metasploitable:~$ _
```

Abbiamo subito testato la nuova password effettuando l'accesso al server dalla macchina Kali:

```
(giacomo@kali)-[~]
$ vncviewer 192.168.1.80
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
```

### Nuova scansione delle principali vulnerabilità critiche

Eseguendo una nuova scansione possiamo osservare che le vulnerabilità critiche individuate sono state risolte.

<input type="checkbox"/>	Sev ▼	CVSS	VPR	Name	Family
<input type="checkbox"/>	CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General
<input type="checkbox"/>	MIXED	...	...	 Apache Tomcat (Multiple Issues)	Web Servers
<input type="checkbox"/>	CRITICAL	...	...	 SSL (Multiple Issues)	Gain a shell remotely
<input type="checkbox"/>	MIXED	...	...	 SSL (Multiple Issues)	Service detection
<input type="checkbox"/>	HIGH	7.5 *	6.7	rlogin Service Detection	Service detection