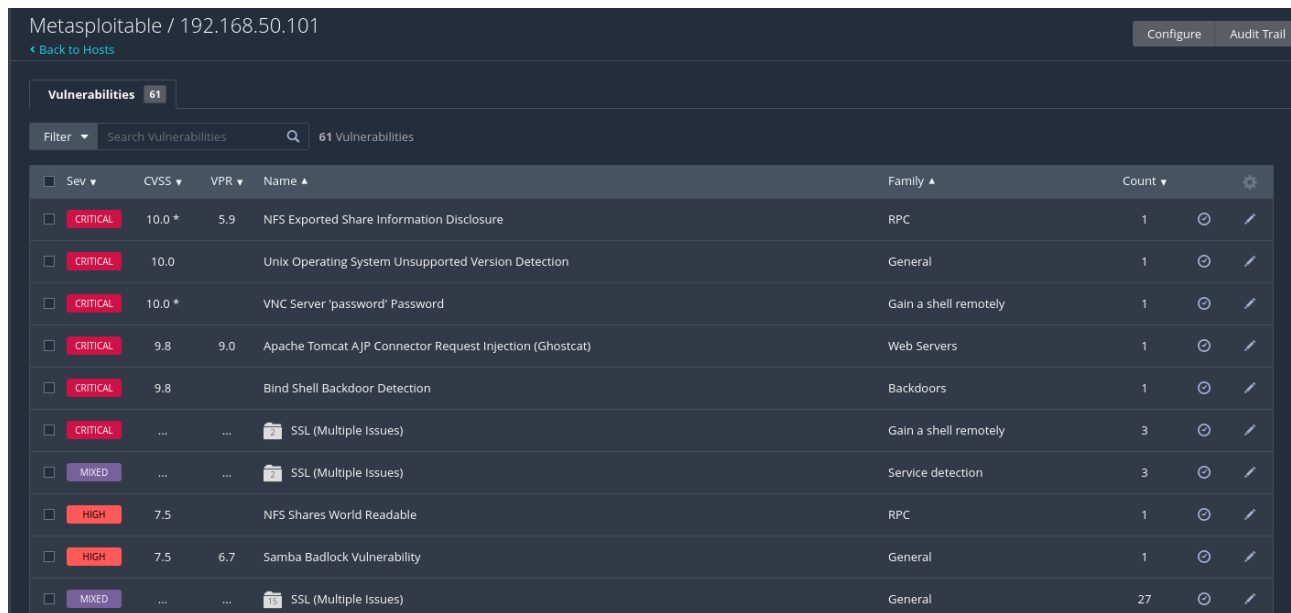


Progetto settimanale (02/06)

Questa settimana ci è stato richiesto di effettuare una scansione completa della vm Metasploitable tramite Nessus, scegliere almeno quattro vulnerabilità riscontrate dal programma e applicare (o teorizzare in caso di molteplici soluzioni) una resolution action in modo da risolvere le vulnerabilità così che Nessus non le riporti in una seconda scansione.

L'immagine seguente è lo screen della prima scansione fatta:



Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1
CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1
CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1
CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3
MIXED	SSL (Multiple Issues)	Service detection	3
HIGH	7.5		NFS Shares World Readable	RPC	1
HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1
MIXED	SSL (Multiple Issues)	General	27

Le vulnerabilità riportate con cui lavoreremo sono le seguenti:

- **VNC server “password” password**
- **NFS exported share information disclosure.**
- **Bind shell backdoor detection**
- **Rexedc service detection** (non presente nella scansione, malgrado abbia provato a incontrarla anche usando la scansione avanzata, ma dalla traccia del progetto possiamo affermare sia presente in ogni caso)

VNC server “password” password

VNC sta per Virtual Network Computing. È un sistema di condivisione dello schermo multiplatforma creato per controllare in remoto un altro computer. Ciò significa che lo schermo, la tastiera e il mouse di un computer possono essere utilizzati a distanza da un utente remoto da un dispositivo secondario come se fossero seduti proprio di fronte ad esso. In questo caso Nessus ci fa sapere che la password del server VNC è

```
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
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
root@metasploitable:/home/msfadmin# _
```

troppo debole, perché lasciata all'impostazione di default "password", ed è riuscito ad effettuare il login confermandola come una vulnerabilità facilmente sfruttabile da un attaccante esterno.

Come si può vedere dall'immagine la vulnerabilità può essere facilmente risolta accedendo ai privilegi di super user tramite il comando "sudo su" e cambiando la password del server VNC tramite il

comando "vncpasswd". C'è da notare che un'altra soluzione possibile sarebbe impostare una regola del firewall che blocchi la porta 5900 che Nessus ci conferma essere la porta che eroga il servizio VNC.

NFS exported share information disclosure.

Network File System (NFS) è un protocollo di rete per la condivisione di file distribuiti. Un file system definisce il modo in cui i dati sotto forma di file vengono archiviati e recuperati dai dispositivi di archiviazione. NFS si distingue in quanto è un protocollo di condivisione file di rete che definisce il modo in cui i file vengono archiviati e recuperati dai dispositivi di archiviazione attraverso le reti.

Il protocollo NFS definisce un file system di rete, originariamente sviluppato per la condivisione di file locali tra sistemi Unix e rilasciato da Sun Microsystems nel 1984. La specifica del protocollo NFS è stata pubblicata per la prima volta dalla Internet Engineering Task Force (IETF) come protocollo Internet in RFC 1094 nel 1989.

```
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)
#
#/*              *(rw,sync,root_squash,no_subtree_check)
```

[Wrote 13 lines]

```
^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is   ^U Next Page  ^U UnCut Text ^T To Spell
```

NFS consente agli amministratori di sistema di condividere tutto o parte di un file system su un server di rete per renderlo accessibile agli utenti di computer remoti. I client autorizzati ad accedere al file system condiviso possono montare condivisioni NFS, note anche come file system condivisi. NFS utilizza RPC (Remote Procedure Call) per instradare le richieste tra client e server.

Nessus ci fa presente la vulnerabilità per cui un attaccante esterno potrebbe montare questi

file condivisi tramite NFS e usarli per leggere informazioni sull'host o addirittura riscriverli come root. Come resolution action ho aperto la cartella "/etc/exports" tramite "sudo nano" ed ho modificato la riga finale come commento in modo che non venga letta, questa riga configura i client come root del server e per questo viene la escludiamo, ma faccio notare che per sicurezza ho modificato il "no_root_squash" che

specifica questa dinamica come “root_squash” in caso la riga fosse reintegrata al file; come per la vulnerabilità precedente il problema potrebbe essere risolto sempre tramite un firewall che blocca l’accesso alla porta 2049 che eroga il servizio.

Bind shell backdoor detection / Rexecd service detection

Mi permetto di raggruppare queste due vulnerabilità insieme perché di natura simile e in quanto la remediation action necessaria per correggere entrambe va a toccare la stessa directory come si può vedere dall’immagine:

```
GNU nano 2.0.7      File: /etc/inetd.conf      Modified
#<off># netbios-ssn  stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.telnetd
telnet              stream  tcp      nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.telnetd
#<off># ftp          stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.tftpd
tftp               dgram  udp      wait    nobody  /usr/sbin/tcpd  /usr/sbin/in.tftpd
shell              stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rsh
login              stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rlogin
#exec              stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rexecd
#ingreslock stream tcp nowait root /bin/bash bash -i

[ Read 8 lines ]
^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text    ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page  ^U UnCut Text ^T To Spell
```

Rexecd è progettato per consentire agli utenti di una rete di eseguire comandi in remoto, in questo caso Nessus ci avverte che non provvede un metodo efficace di autenticazione ed è facilmente sfruttabile da un possibile attaccante esterno: entrando nella directory “/etc/inetd.conf/” è possibile modificare come commento la riga “exec” che avvia il servizio come remediation action oppure sempre tramite una regola del firewall bloccare la porta 512 a cui è associata.

Riguardo la vulnerabilità “bind shell backdoor detection” Nessus si rifà a un servizio di backdoor legittimo del sistema che però allo stesso modo è privo di metodi di autenticazione e perciò pronò ad essere sfruttato, Nessus consiglia in caso che l’host sia compromesso a causa di questa vulnerabilità di reinstallare il sistema in modo da resettare possibili accessi indesiderati, essendo questa una simulazione in rete interna ci limiteremo a commentare l’ultima riga (sempre nella directory “/etc/inetd.conf/”) che provvede all’apertura della backdoor oppure basterebbe bloccare l’accesso della porta 1524 con una regola del firewall.

Scansione post-resolution actions

Come possiamo vedere dall'immagine sotto dopo aver applicato le varie remediation actions, effettuando una nuova scansione della vm Metasploitable, Nessus non rileva più le quattro vulnerabilità critiche riscontrate precedentemente.

Metasploitable post / 192.168.50.101

ConfigureAudit Trail

Vulnerabilities57

FilterSearch Vulnerabilities57 Vulnerabilities

<input type="checkbox"/>	Sev ▼	CVSS ▼	VPR ▼	Name ▲	Family ▲	Count ▼	
<input type="checkbox"/>	CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1	⊙ /
<input type="checkbox"/>	CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1	⊙ /
<input type="checkbox"/>	CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3	⊙ /
<input type="checkbox"/>	MIXED	SSL (Multiple Issues)	Service detection	3	⊙ /
<input type="checkbox"/>	HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1	⊙ /
<input type="checkbox"/>	MIXED	SSL (Multiple Issues)	General	27	⊙ /
<input type="checkbox"/>	MIXED	ISC Bind (Multiple Issues)	DNS	5	⊙ /
<input type="checkbox"/>	MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection	2	⊙ /
<input type="checkbox"/>	MEDIUM	5.9	4.4	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1	⊙ /