ACTIVITY

PROGETTO S5L5

ha lo scopo di identificare ed assegnare un rischio alle vulnerabilità / configurazioni errate trovate nelle fasi precedenti, e preparare alla fase di exploit.

ACTIVITY

VALUTAZIONE DELLA VULNERABILITÀ

Mettere in communicazione le due macchine (Kali Linux e Metasploitable) mettendoli sulla stessa rete.
Accesso Nessus

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.

Prime 4 vulnerabilità scansionate:

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		Bind Shell Backdoor Detection	Backdoors	1

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 4:16 AM
End:	Today at 4:38 AM
Elapsed:	23 minutes

PRIMA VULNERABILITÀ

1) NFS Exported Share Information Disclosure:

è una vulnerabilità in cui le informazioni condivise tramite NFS sono diffuse in modo non autorizzato. Questo può accadere se la configurazione del sistema NFS non è adeguatamente protetta.

Soluzioni:

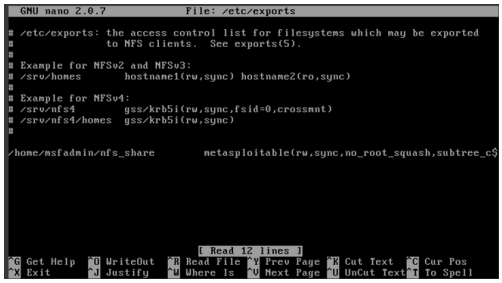
- Impostare i permessi di condivisione in modo che solo gli utenti autorizzati possano accedere ai dati condivisi.
- Limitare l'accesso NFS solo agli host o alle reti autorizzate.
- Mantenere tutti i software di sistema e le implementazioni NFS aggiornate.
- Monitorare e registrare l'accesso NFS per individuare attività sospette o non autorizzate.

Procedura:

- Si apre il terminale;
- Si crea una directory che ti permette di esportare solo i file presenti nella directory. Comando 'mkdir ~/nome directory';
- Si modifica il file exports con il comando 'sudo nano /etc/exports';

ACTIVITY

VALUTAZIONE DELLA VULNERABILITÀ



/home/tuo_utente/nome directory: Il percorso della directory che vuoi condividere.
*: Indica che qualsiasi host ha accesso (assicurati che il tuo sistema sia configurato per accettare connessioni NFS).
rw: Consente la scrittura (puoi personalizzare questa opzione).
sync: Le modifiche vengono sincronizzate subito.
no_root_squash: Consente all'utente root del client di essere l'utente root sul server NFS.
no_subtree_check: Migliora le prestazioni, ma riduce la sicurezza. Puoi considerare di rimuoverlo in un ambiente di produzione.

- Con il comando 'sudo exportfs -a' si aggiornano le configurazioni del NFS;
- Si avvia il servizio con il comando 'sudo /etc/init.d/nfs-kernel-server start';

```
msfadmin@metasploitable:~$ sudo exportfs -a
msfadmin@metasploitable:~$ sudo service nfs-kernel-server start
sudo: service: command not found
msfadmin@metasploitable:~$ sudo rpcbind start
sudo: rpcbind: command not found
msfadmin@metasploitable:~$ sudo service nfs-kernel-server status
sudo: service: command not found
msfadmin@metasploitable:~$ sudo systemct1 nfs-kernel-server start
sudo: systemct1: command not found
msfadmin@metasploitable:~$ sudo systemct1 start nfs-kernel-server
sudo: systemct1: command not found
msfadmin@metasploitable:~$ sudo systemct1 start nfs-kernel-server
sudo: systemct1: command not found
msfadmin@metasploitable:~$ sudo systemct1 start nfs-kernel-server
sudo: systemct1: command not found
msfadmin@metasploitable:~$ sudo /etc/init.d/nfs-kernel-server start
 * Exporting directories for NFS kernel daemon...                [ OK ]
 * Starting NFS kernel daemon                                    [ OK ]
msfadmin@metasploitable:~$ sudo /etc/init.d/nfs-kernel-server status
nfsd running
```

- Infine si avvia la scansione di Nessus per vedere se la vulnerabilità è diminuita.

ACTIVITY

VALUTAZIONE DELLA VULNERABILITÀ

SECONDA VULNERABILITÀ

2) VNC Server 'password' Password:

VNC (Virtual Network Computing) è un sistema di controllo remoto che consente agli utenti di accedere e controllare un computer da un'altra posizione tramite una connessione di rete.

Soluzioni:

- Password forte: Questa password dovrebbe essere complessa e difficile da indovinare contenente almeno 8 caratteri tra lettere maiuscole e minuscole, alfanumerici e speciali.
- Crittografia: È consigliabile utilizzare una connessione VNC cifrata per proteggere i dati scambiati tra il client e il server.
- Autenticazione a due fattori: Se possibile, utilizzare l'autenticazione a due fattori per il server VNC. Questo aggiunge un ulteriore livello di sicurezza richiedendo un secondo metodo di autenticazione oltre alla password.
- Firewall e filtraggio degli indirizzi IP: Limitare l'accesso al server VNC utilizzando un firewall o il filtraggio degli indirizzi IP.
- Aggiornamenti: Assicurarsi che il software VNC e il sistema operativo siano aggiornati

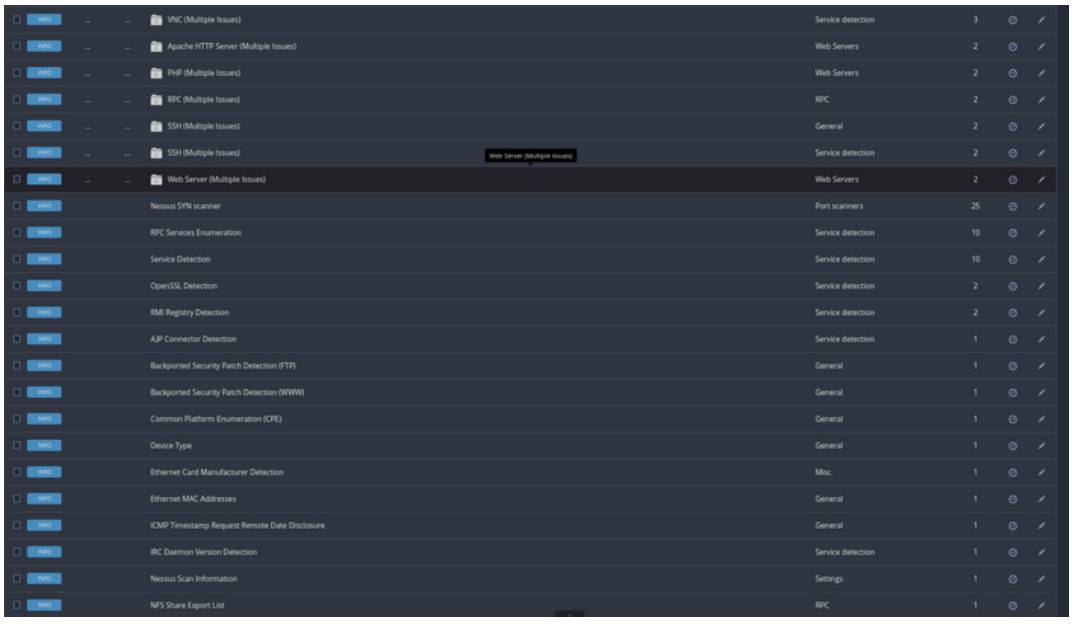
Procedura:

- Aprire il terminale;
- Cambio di privilegi da guest a root con il comando ‘sudo su’;
- Avviare il server di VNC con il comando ‘vncserver’;
- Cambio password con il comando ‘vncpasswd’;
- Infine si fa la scansione per vedere se la vulnerabilità è diminuita.

```
nts/75dpi/,/usr/X11R6/lib/X11/fonts/100dpi/,/usr/share/fonts/X11/misc/,/usr/shar
e/fonts/X11/Type1/,/usr/share/fonts/X11/75dpi/,/usr/share/fonts/X11/100dpi/ -co
/etc/X11/rgb
msfadmin 10776  0.0  0.0   3004   752 tty1     R+   06:21   0:00 grep Xtightvnc
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ cd /home/vncuser
-bash: cd: /home/vncuser: No such file or directory
msfadmin@metasploitable:~$ cd root/home/vncuser
-bash: cd: root/home/vncuser: No such file or directory
msfadmin@metasploitable:~$ cd /root/home/vncuser
-bash: cd: /root/home/vncuser: No such file or directory
msfadmin@metasploitable:~$ cd root
-bash: cd: root: No such file or directory
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# cd /home/vncuser
bash: cd: /home/vncuser: No such file or directory
root@metasploitable:/home/msfadmin# cd /vncuser
bash: cd: /vncuser: No such file or directory
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#
```

VNC →

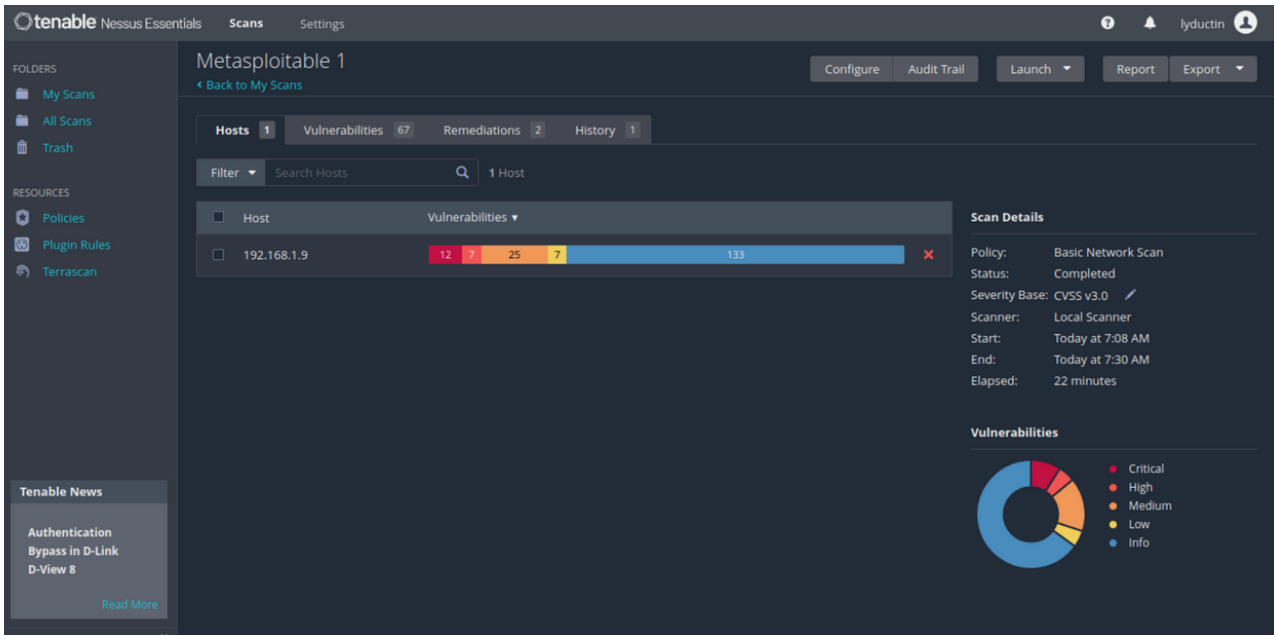
NFS →

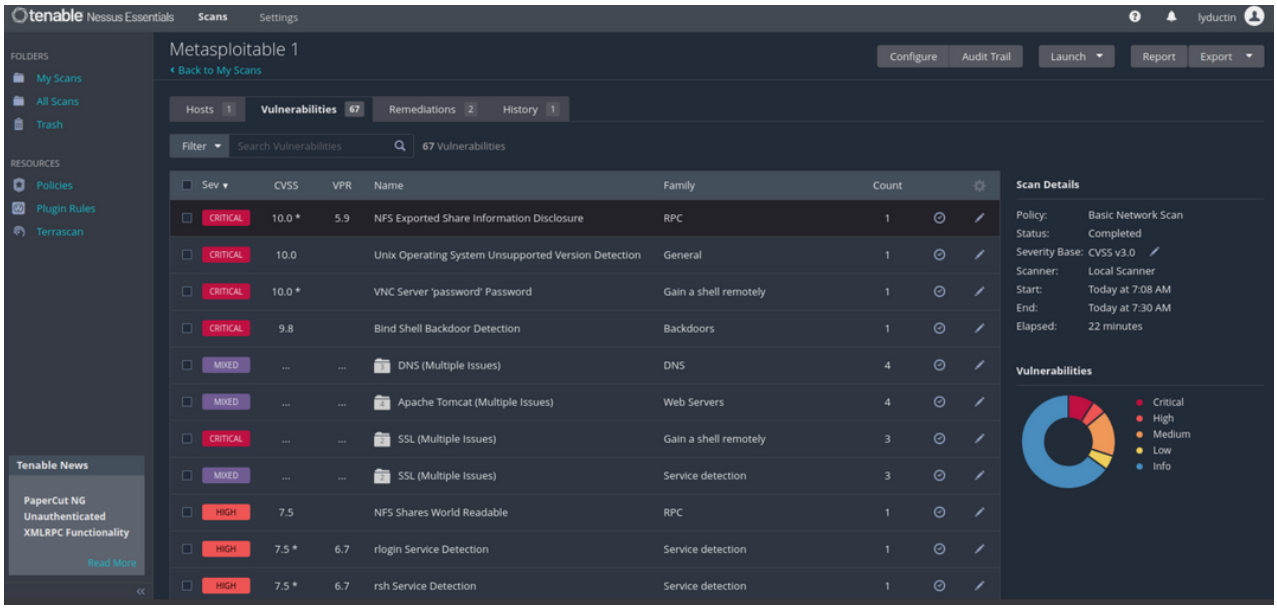


ACTIVITY

VALUTAZIONE DELLA VULNERABILITÀ

SCANSIONE





ACTIVITY

VALUTAZIONE DELLA VULNERABILITÀ

SCANSIONE FINALE