

## PRATICA S5 – L5

### VULNERABILITY ASSESSMENT, REMEDIATION ACTION E NUOVA VULNERABILITY ASSESSMENT PER VERIFICA MITIGAZIONE DELLE VULNERABILITA' RISCONTRATE SU METASPLOITABLE.

#### 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.

#### Svolgimento:

- Scansione iniziale dove si vede il grafico con tutte le vulnerabilità e le vulnerabilità da risolvere (ScansioneInizio.pdf ).
- Screenshot e spiegazione dei passaggi della remediation (RemediationMeta.pdf )
- Scansione dopo le modifiche che evidenzia la risoluzione dei problemi/vulnerabilità
- (il grafico che mostra tutte le vulnerabilità) ScansioneFine.pdf.

### 1) Scansione iniziale di Metasploitable

Dalla lista di vulnerabilità riscontrate, tramite Nessus, relativamente a Meta ho scelto quattro vulnerabilità a cui porre rimedio:

CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	-	61708	VNC Server 'password' Password
HIGH	7.5	6.7	90509	Samba Badlock Vulnerability

## 2) Remediation Action

### 2.1) Bind Shell Backdoor Detection

La vulnerabilità in questo caso consiste nel fatto che una shell è in ascolto sulla porta remota 1524 senza richiedere alcuna autenticazione, il che potrebbe consentire ad un attaccante di connettersi alla porta e inviare comandi direttamente al sistema, compromettendo la macchina Meta.

- Per rimediare sono intervenuta sul Firewall Di Meta (ufw).

In primo luogo, con privilegi di amministratore, ho abilitato il Firewall su Meta attraverso il comando **'ufw enable'**.

In secondo luogo, ho impostato la policy di default (predefinita) del firewall su allow (consenti) tramite il comando **'ufw default allow'**.

Con il comando **'ufw deny 1524'**, ho aggiunto una regola al firewall per negare la connessione e il traffico di rete sulla porta 1524, impedendo di fatto alla backdoor di funzionare.

Infine ho controllato lo stato corrente del Firewall, che è attivo e settato con le regole configurate, tramite il comando **'ufw status'**.

metasploit [In esecuzione] - Oracle VM VirtualBox  
File Macchina Visualizza Inserimento Dispositivi Aiuto

```
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:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# ufw enable
Firewall started and enabled on system startup
root@metasploitable:/home/msfadmin# ufw default allow
Default policy changed to 'allow'
(be sure to update your rules accordingly)
root@metasploitable:/home/msfadmin# ufw deny 1524
Rule added
root@metasploitable:/home/msfadmin# ufw status
Firewall loaded

To Action From
--
1524:tcp DENY Anywhere
1524:udp DENY Anywhere
root@metasploitable:/home/msfadmin#
```

## 2.2) NFS Exported Share Information Disclosure

La vulnerabilità consiste nella possibilità di accedere alle condivisioni NFS (Network File System) sull' host remoto.

In particolare, almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere oggetto di accesso non autorizzato da parte dell'host che sta effettuando la scansione.

L'esportazione di NFS permette ad altri sistemi di accedere (montare) alle directory condivise sull' host remoto Metasploitable.

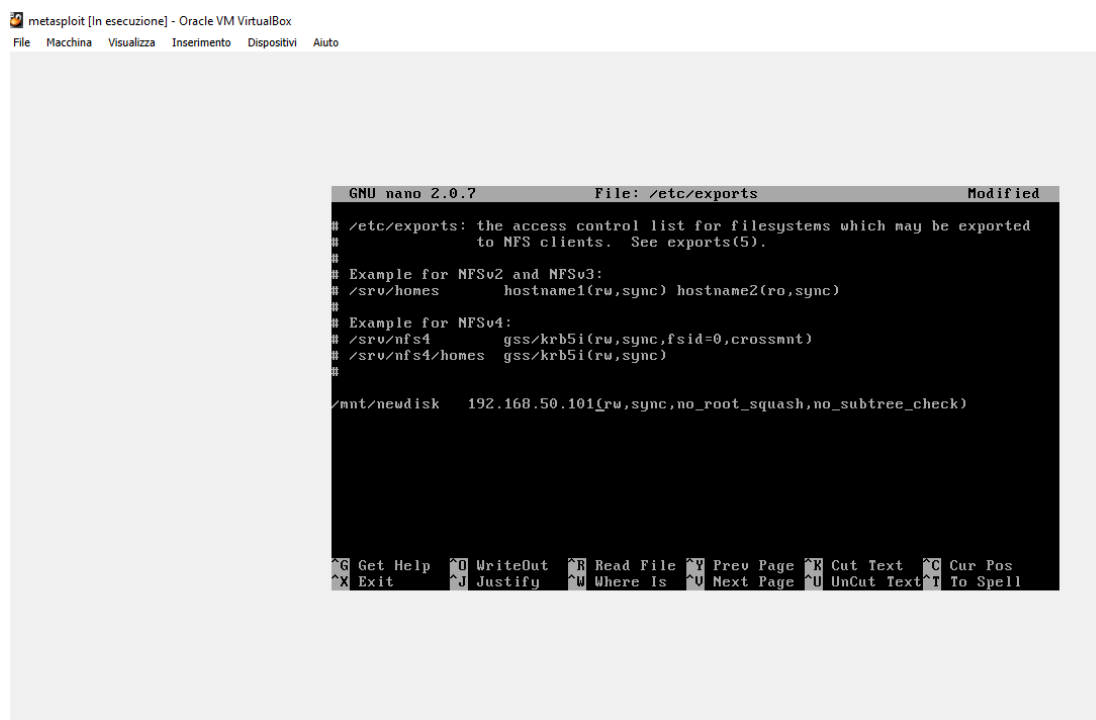
Qualora un attaccante riuscisse ad accedere alle condivisioni, per via della configurazione non corretta di NFS, potrebbe non solo leggere ma anche scrivere e modificare i file sull'host remoto (Meta).

- Per rimediare, sempre con privilegi di amministratore (sudo su), sono andata a configurare le regole di accesso NFS nel file /etc/exports, con il comando nano /etc/exports.

In questo file è possibile specificare gli host che sono autorizzati ad accedere alle diverse condivisioni NFS.

In particolare, ho aggiunto alla fine **/mnt/newdisk 192.168.50.101:** In questo modo ho aggiunto una nuova configurazione di esportazione NFS per la directory '/mnt/newdisk/' con l'indirizzo IP di Meta.

Quindi, ho autorizzato esclusivamente Meta ad accedere alla condivisione NFS, mitigando la vulnerabilità precedente, che consentiva l'accesso di qualunque host (cosa che visivamente si poteva vedere dalla presenza di un asterisco prima della parentesi che definisce le opzioni della condivisione).



```
metasploit [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

GNU nano 2.0.7      File: /etc/exports      Modified
# /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)
#
/mnt/newdisk 192.168.50.101(rw,sync,no_root_squash,no_subtree_check)

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

### 2.3) VNC Server 'password' Password

La vulnerabilità riscontrata riguarda la sicurezza di un server VNC (Virtual Network Computing) in esecuzione sull'host remoto Meta.

In particolare, il server VNC è configurato e protetto da una password debole.

Infatti, Nessus è stato in grado di accedere al Server utilizzando l'autenticazione con una password impostata su 'password'.

Tramite una password così facile da indovinare, un malintenzionato potrebbe ottenere l'accesso non autorizzato al sistema attraverso il server VNC.

- Per rimediare sono andati, sempre con privilegi amministrativi, ad eseguire il comando **'vncpasswd'**, che è specifico per cambiare la password del server VNC.

Dopo aver inserito la nuova password e averla verificata, ho detto di no all'impostazione di una password di sola lettura.

metasploit [In esecuzione] - Oracle VM VirtualBox  
File Macchina Visualizza Inserimento Dispositivi Aiuto

```
# 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)
#
/mnt/newdisk 192.168.50.101(rw, sync, no_root_squash, no_subtree_check)

[ Wrote 12 lines ]

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

## 2.4) Samba Badlock Vulnerability

La vulnerabilità riguarda un server Samba, utilizzato su sistemi Linux e Unix, che consente la condivisione di file e risorse su una rete, implementando i protocolli SMB (Server Message Block) e CIFS (Common Internet File System) per facilitare la condivisione di file tra computer. In particolare, il server Samba, in esecuzione sull'host remoto Meta, è influenzato da una vulnerabilità nota come Badlock.

Questa vulnerabilità riguarda due protocolli specifici per la gestione dell'autenticazione su una rete: SAM (Security Account Manager) e LSAD (Local Security Authority Domain Policy).

La Badlock è presente in Samba a causa di una negoziazione impropria del livello di autenticazione su canali di Remote Procedure Call (RPC), ovvero a causa di una sorte di errore nella fase di negoziazione della sicurezza tra un client e un server che utilizzano i protocolli SAM e LSAD.

Ciò consentirebbe ad un attaccante, in posizione di Man-in-the-middle (cioè di intermediario che intercetta il traffico tra client e server), di forzare una riduzione della sicurezza dell'autenticazione durante la comunicazione fra i due.

La conseguenza sarebbe la possibilità per l'aggressore di eseguire operazioni non autorizzate sul server Samba, tra cui visualizzare o modificare informazioni sensibili presenti nel database Active Directory (AD) (parte cruciale di molti sistemi di autenticazione e gestione degli utenti) e disabilitare servizi importanti, compromettendo così l'integrità e la disponibilità del sistema.

- Per rimediare alla vulnerabilità sono andati ad intervenire nuovamente sul firewall di Meta (ufw) inserendo due nuove regole ('**ufw deny 139**' e '**ufw deny 445**') che negano la comunicazione ed il traffico sulle porte 139 e 445, sulle quali sono in ascolto i servizi Netbios e SMB associati a Samba.

Disabilitando in tal modo i servizi, si riducono le opportunità per un attaccante di sfruttare vulnerabilità legate a Samba o ad altri servizi SMB.

metasploit [In esecuzione] - Oracle VM VirtualBox  
File Macchina Visualizza Inserimento Dispositivi Aiuto

```
root@metasploitable:~/home/msfadmin# ufw deny 139
Rule added
root@metasploitable:~/home/msfadmin# ufw deny 445
Rule added
root@metasploitable:~/home/msfadmin#
```

### 3) Scansione finale di Metasploitable

Sono andata ad effettuare una nuova scansione tramite Nessus su Metasploitable, per verificare la mitigazione delle vulnerabilità dopo aver posto in essere Remediation action. Qui riporto la parte di report nel quale si può vedere che non vengono più elencate le vulnerabilità sanate.

N.B. In allegato sono presenti sia la ScansioneIniziale.pdf che la Scansionefine.pdf.

