

## **S5I5**

**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.**

## **Vulnerability Assessment**

Effettuiamo un Vulnerability Assessment per verificare le vulnerabilità presenti.

**Un Vulnerability Assessment ,o valutazione delle vulnerabilità, è un processo sistematico per identificare e classificare le vulnerabilità di sicurezza nei sistemi informatici**

La frequenza con cui bisognerebbe eseguire una valutazione della vulnerabilità dipende da diversi fattori, come ad esempio il tipo di sistemi che si possiedono, ed anche la sensibilità dei dati archiviati o il livello di rischio di attacco. In genere, si consiglia di eseguire una valutazione della vulnerabilità almeno una volta all'anno o ogni volta che viene apportata una modifica significativa all'infrastruttura IT.

Alcuni dei vantaggi di una valutazione della vulnerabilità includono:

- Riduce il rischio di attacchi informatici
- Protegge i dati e le informazioni sensibili
- Migliora la postura complessiva della sicurezza informatica
- Aiuta a soddisfare i requisiti di conformità

Per raggiungere il nostro obiettivo utilizzeremo un tool di nome Nessus.

**Nessus è uno strumento che aiuta a trovare punti deboli all'interno di una rete. I punti deboli, chiamati vulnerabilità, possono essere sfruttati da Black Hat hacker per attaccare la tua rete e rubare i tuoi dati.**

//Black Hat Hacker: E' un criminale informatico che viola qualunque rete

Nessus scansiona la rete ed i dispositivi per cercare vulnerabilità. Può scansionare una vasta gamma di sistemi, inclusi server, workstation, dispositivi di rete e applicazioni Web.

Nessus è uno strumento potente e versatile che aiuta a trovare diverse tipologie di vulnerabilità, tra le quali troviamo:

- Difetti di sicurezza nel software, come bug che consentono agli hacker di eseguire codice o accedere a dati sensibili.
- Patch mancanti, che possono lasciare i tuoi sistemi vulnerabili a attacchi noti.
- Configurazioni errate, come porte aperte o password deboli che possono essere sfruttate dagli hacker.
- Malware, come virus, trojan e ransomware.

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	7.4	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	7.4	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	-	61708	VNC Server 'password' Password
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42256	NFS Shares World Readable

Figura 1

Come possiamo notare troviamo un quadro generale che mostra numerose vulnerabilità.

Le vulnerabilità sulla quale andremo a lavorare sono quelle con livelli critici, questo tipo di vulnerabilità potrebbe compromettere i sistemi e l'integrità e la riservatezza dei dati sulla macchina in questione.



Figura 2

## NFS Exported Share Information Disclosure

Tramite questo modulo è possibile accedere alle condivisioni NFS (Network File System) sull' host remoto.

Un Hacker eticamente scorretto potrebbe accedere alla condivisione sfruttando la vulnerabilità per via della configurazione non corretta di NFS, in questo caso, il pirata informatico potrebbe sia leggere che scrivere o modificare i file sulla macchina Hostata in remoto.

La possibilità di lettura permette all'attaccante di avere accesso ad informazioni sensibili.

La possibilità di scrittura permette all'attaccante di introdurre codice malevolo.

La possibilità di modifica permette all'attaccante di compromettere i file presenti sul dispositivo.

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

[ Read 12 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
```

Figura 3

## Azioni di rimedio

Eseguiamo il comando “sudo” che sta per “Super User do”, cioè “Il super Utente fa” (Sta ad indicare l’amministratore, così facendo il comando che daremo successivamente sarà eseguito come amministratore.

Utilizzo il comando “nano /etc/exports”; su questo documento ho la possibilità di modificare le istruzioni che la macchina eseguirà.

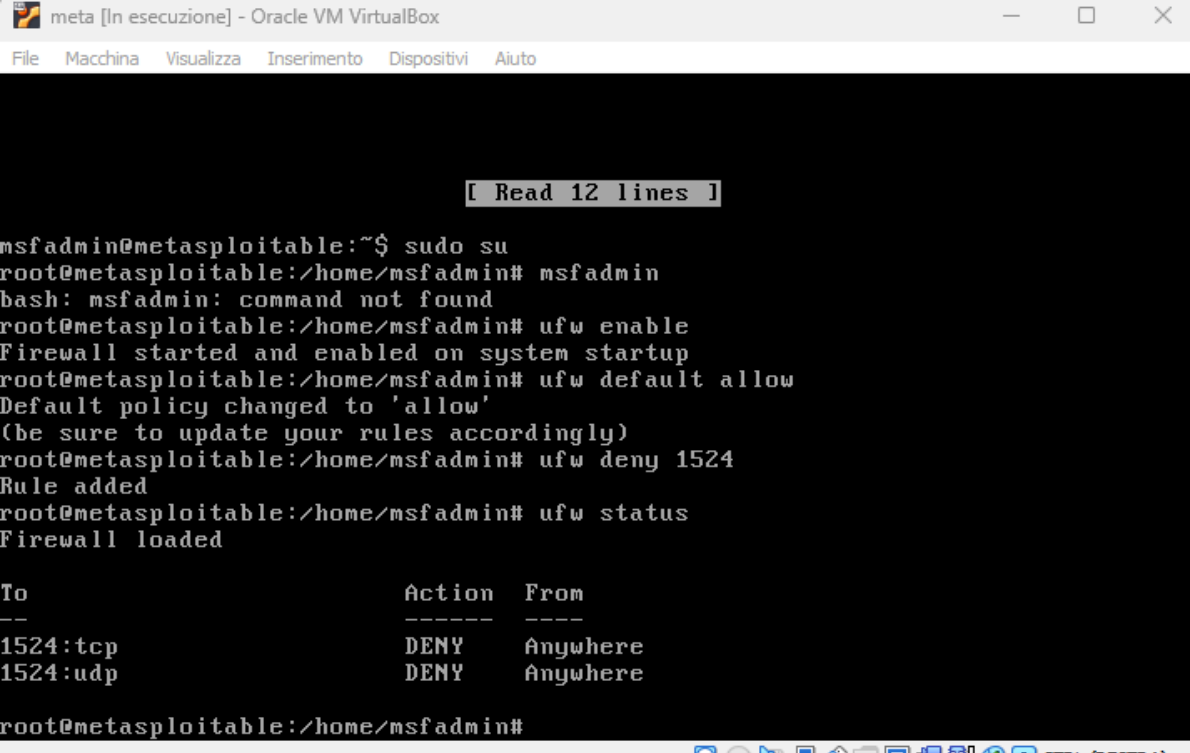
In questo file è possibile specificare gli host che sono autorizzati ad accedere alle diverse condivisioni NFS.

Come si può notare dalla Figura 3 Abbiamo aggiunto l’IP di Meta nella seguente configurazione, così facendo: /mnt/newdisk 192.168.50.101

Grazie alla nuova configurazione soltanto Meta potrà accedere alla condivisione NFS e nessun altro dispositivo.

Abbiamo così diminuito le problematiche relative a questo aspetto che consentiva prima l’accesso anche a dispositivi esterni non autorizzati

## Bind Shell Backdoor Detection



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

[ Read 12 lines ]

msfadmin@metasploitable:~$ sudo su
root@metasploitable:/home/msfadmin# msfadmin
bash: msfadmin: command not found
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#
```

Figura 4

La Figura 4 si riferisce all'attivazione del Firewall, utilissima difesa contro le vulnerabilità dei computer.

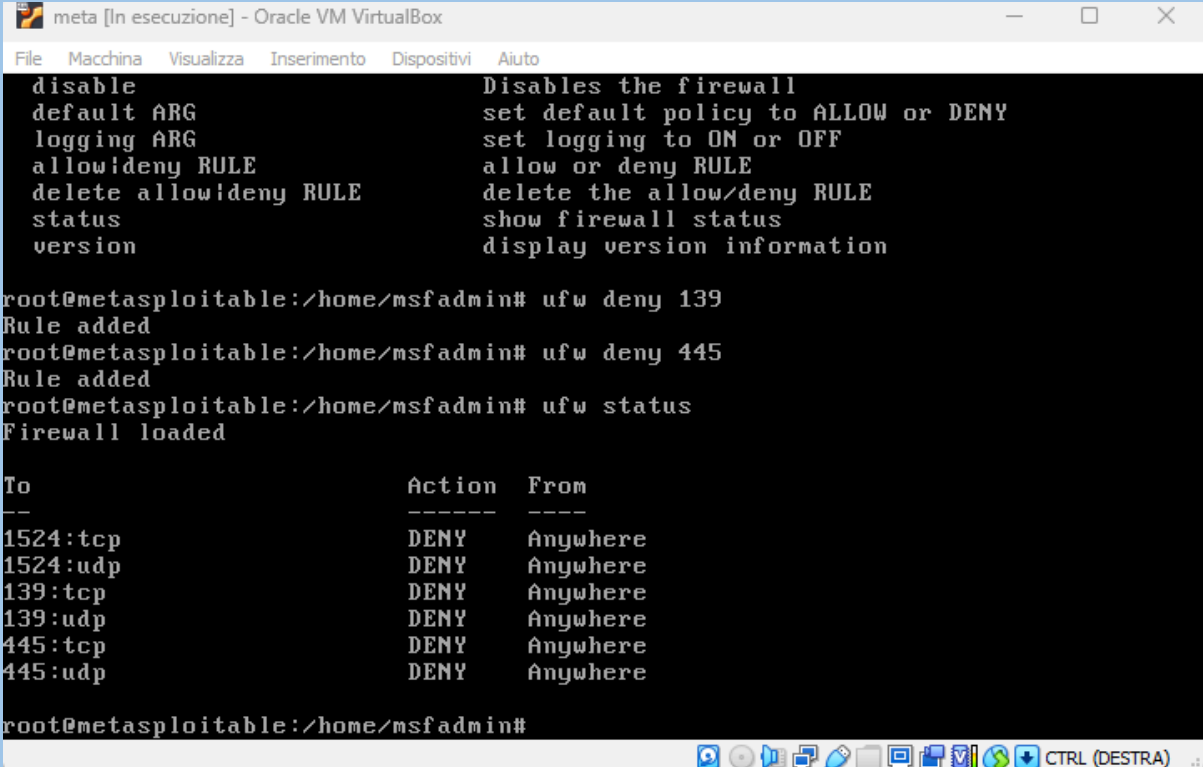
Ho eseguito l'accesso come amministratore utilizzando nuovamente il comando "sudo su", Meta ci chiede di inserire la password per assicurarsi che l'accesso venga realmente effettuato dall'amministratore.

Ho utilizzato il comando "ufw enable" per abilitare il Firewall di meta.

In secondo luogo, ho impostato la policy di default del nostro firewall su allow (consenti) utilizzando il comando "ufw default allow".

Ho aggiunto una regola al firewall per negare la connessione e il traffico di rete sulla porta 1524, utilizzando il comando “ufw deny 1524”, così facendo impediamo di fatto ad una potenziale backdoor di funzionare.

Ho utilizzato poi il comando “ufw status” per assicurarmi che la mia configurazione fosse salvata e caricata.



The screenshot shows a terminal window titled "meta [In esecuzione] - Oracle VM VirtualBox". The terminal displays the ufw firewall help text, followed by commands to deny traffic on ports 139 and 445, and then the ufw status command. The status output shows a table of rules denying traffic on ports 1524, 139, and 445 for both TCP and UDP.

```
disable          Disables the firewall
default ARG      set default policy to ALLOW or DENY
logging ARG      set logging to ON or OFF
allow|deny RULE  allow or deny RULE
delete allow|deny RULE delete the allow/deny RULE
status           show firewall status
version          display version information

root@metasploitable:/home/msfadmin# ufw deny 139
Rule added
root@metasploitable:/home/msfadmin# ufw deny 445
Rule added
root@metasploitable:/home/msfadmin# ufw status
Firewall loaded

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

root@metasploitable:/home/msfadmin#
```

Figura 5

Questa vulnerabilità consiste in una shell che si tiene in ascolto sulla porta 1524 senza richiedere autenticazioni.

Potenzialmente un Black Hat Hacker potrebbe avere motivo di attaccare il nostro sistema, Con questa vulnerabilità il nostro attaccante potrà scegliere di connettersi alla porta e inviare comandi direttamente al sistema, che ne risulterebbe dunque compromesso.