REPORT VULNERABILITA' METASPLOITABLE
GIULIA FIACCHI

Data la scansione completa del target Metasploitable, sono state rilevate molteplici vulnerabilità critiche/high e si è cercata una soluzione a questi problemi.
In particolare ci si è soffermati su:

1. NFS Exported Share Information Disclosure
2. VNC Server 'password' Password
3. rexecd Service Detection
4. rlogin Service Detection
5. Bind Shell backdoor Detection

1. NFS Exported Share Information Disclosure

E' una vulnerabilità di sicurezza che si verifica quando le informazioni sui file condivisi tramite NFS vengono esposte in modo inappropriato.
L'NFS è un file system che consente a computer client di utilizzare la rete per accedere a directory condivise da server remoti come fossero disponibili in locale.
Questa esposizione può avvenire a causa di configurazioni errate, come permessi di accesso mal configurati, mancanza di restrizioni adeguate sui client che possono accedere alla condivisione, o versioni obsolete del software NFS che contengono bug di sicurezza.

Usando il comando sudo nmap sS -p- 192.168.50.101, possiamo vedere tutte le porte aperte sulla macchina Metasploitable e si è notato che la porta 2049/tcp nfs è aperta, quindi significa che il servizio NFS è attivo e sta accettando connessioni TCP su quella porta.
Ancora nella ricerca delle porte si è notata anche un'altra criticità, la porta 111/tcp è aperta e data la ricerca effettuata sulla funzionalità di ogni porta, si è evinto che è atta al servizio rpcbind utilizzato dai programmi che fanno uso della chiamata di procedura remota e perciò è sempre in ascolto in attesa che un client faccia la richiesta.

SOLUZIONI:

- Configurare correttamente i permessi di accesso, assicurandosi che solo i client autorizzati possano accedere alle condivisioni NFS
- Implementare misure di sicurezza aggiuntive come l'uso di firewall per limitare l'accesso alle porte NFS

Con il comando *sudo /etc/exports* per modificare la directory del NFS, questo file definisce quali directory saranno condivise tramite NFS e i permessi di accesso per i client

→/var/nfs 192.168.1.0/24(rw,sync,no_subtree_check)

Poi fatto questo si va a modificare l'iptables andando a dare accesso a alle porte 2049 e 111 solo all'IP 192.168.50.102 sia per TCP che per UDP.

```
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
3632/tcp open  distccd
5432/tcp open  postgres
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
```

```
 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,no_root_squash,no_subtree_check)
```

```
 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)
#

/var/nfs 192.168.50.102/24(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
```

```
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

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 iptables -L INPUT --line-numbers
[sudo] password for msfadmin:
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp -s 192.168.50.102 --dpo
rt 2049 -j ACCEPT
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p udp -s 192.168.50.102 --dpo
rt 2049 -j ACCEPT
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp -s 192.168.50.102 --dpo
rt 111 -j ACCEPT
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p udp -s 192.168.50.102 --dpo
rt 111 -j ACCEPT
msfadmin@metasploitable:~$ _
```

2. VNC Server 'password' Password

   VNC è un sistema software che consente di controllare un computer da remoto tramite una connessione di rete, visualizzando il desktop e permettendo l'interazione con il sistema come se ci si trovasse fisicamente davanti al computer

In questo contesto, 'password' indica il parametro o l'opzione all'interno della configurazione del server VNC che consente di specificare la password per l'accesso remoto, Nessus la individua come critica perché si tratta di una password molto debole.

SOLUZIONE:

- impostare una password che sia forte ed unica per proteggere l'accesso non autorizzato

E' necessario per prima cosa diventare root con *sudo su*

Con il comando *vncpasswd* in Metasploitable è possibile impostare una nuova password più sicura

```
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
```

3. rexecd Service Detection

Si riferisce alla capacità di identificare e rilevare la presenza di un servizio di rexec (remote execution) su una macchina o su una rete. Il servizio rexec consente a un utente di eseguire comandi su una macchina remota senza autenticazione, o con autenticazione basata solo sull'indirizzo IP.

SOLUZIONI:

- entrare nella directory *inetd.conf* e commentare la riga exec

Con il comando *sudo nano /etc/inetd.conf* entrare nella directory e commentare la riga exec aggiungendo all'inizio *#.*

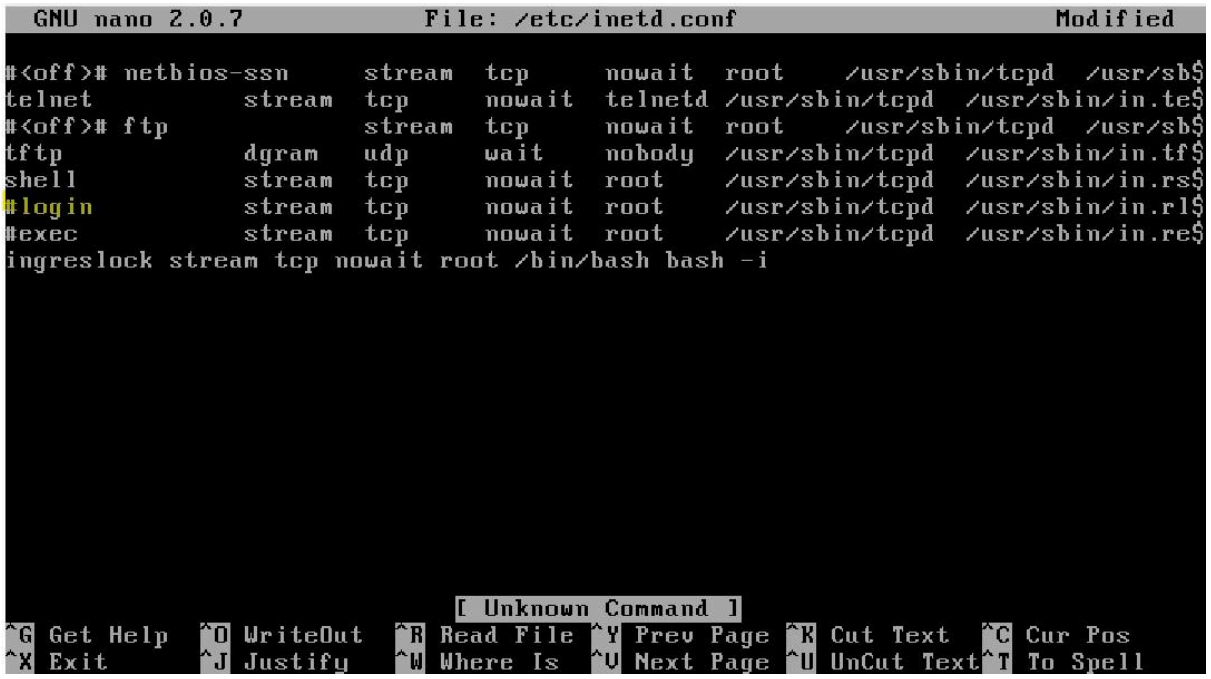
4. rlogin Service Detection

Questo servizio è vulnerabile poiché i dati vengono passati tra il client e il server rlogin in chiaro. Un utente malintenzionato man-in-the-middle può sfruttare questa situazione per sniffare login e password. Inoltre, potrebbe consentire accessi scarsamente autenticati senza password. Se l'host è vulnerabile all'ipotesi del numero di sequenza TCP (da qualsiasi rete) o allo spoofing IP (incluso il dirottamento ARP su una rete locale), potrebbe essere possibile ignorare l'autenticazione.

SOLUZIONE:

- entrare nella directory *inetd.conf* e commentare la riga exec

Con il comando *sudo nano /etc/inetd.conf* entrare nella directory e commentare la riga login aggiungendo all'inizio *#*.



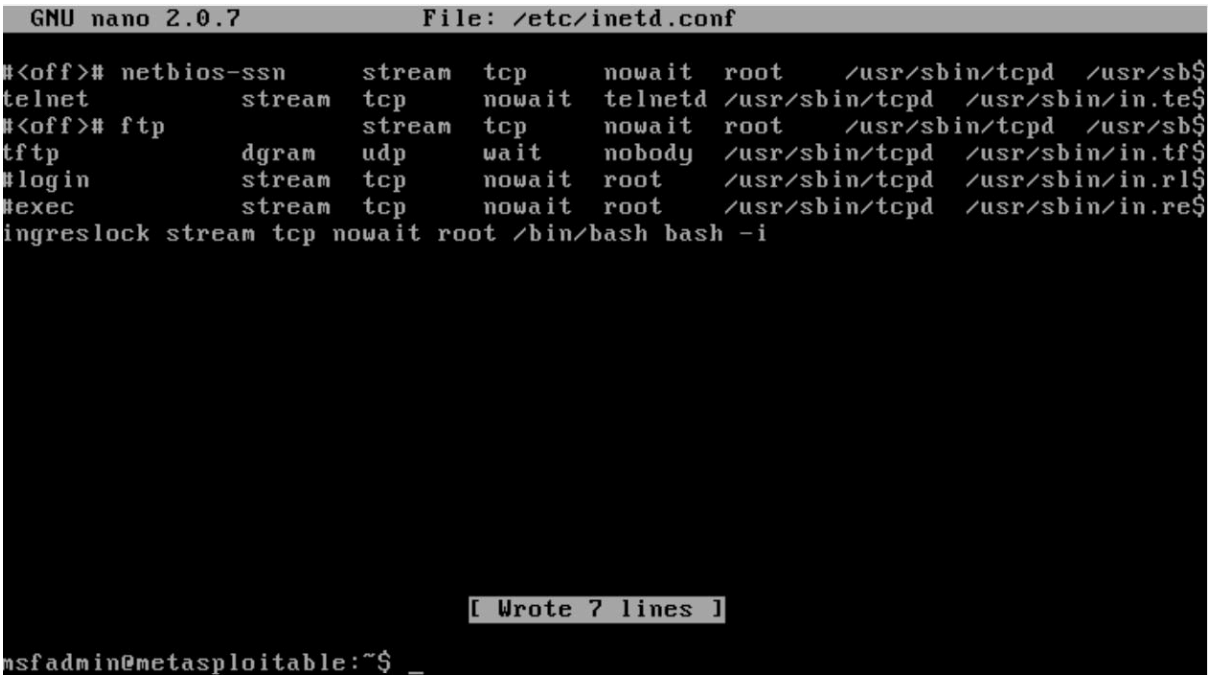
5.Bind Shell backdoor Detection

Il termine "Bind Shell Backdoor Detection" si riferisce alla rilevazione di backdoor di tipo bind shell su un sistema. Una bind shell è un tipo di backdoor in cui un programma malevolo apre una porta su un computer compromesso e "ascolta" le connessioni in entrata. Un attaccante può quindi connettersi a questa porta e ottenere il controllo della macchina.

SOLUZIONE:

Da Kali inserisci *sudo netstat -tulnp | grep 1524* che troverà la porta in ascolto che è la 4426 che andremo a chiudere con *sudo kill -9 4426*.

Poi su Metasploitable *sudo nano /etc/inetd.conf* e qui eliminare la riga Shell stream.



E' stato infine effettuata una nuova scansione su Nessus e i risultati sono consultabili nel "Documento 2"