PROGETTO SETTIMANALE VA-PT

Remediation Meta

EPICODE

Giovanni Pisapia

REMEDIATION:

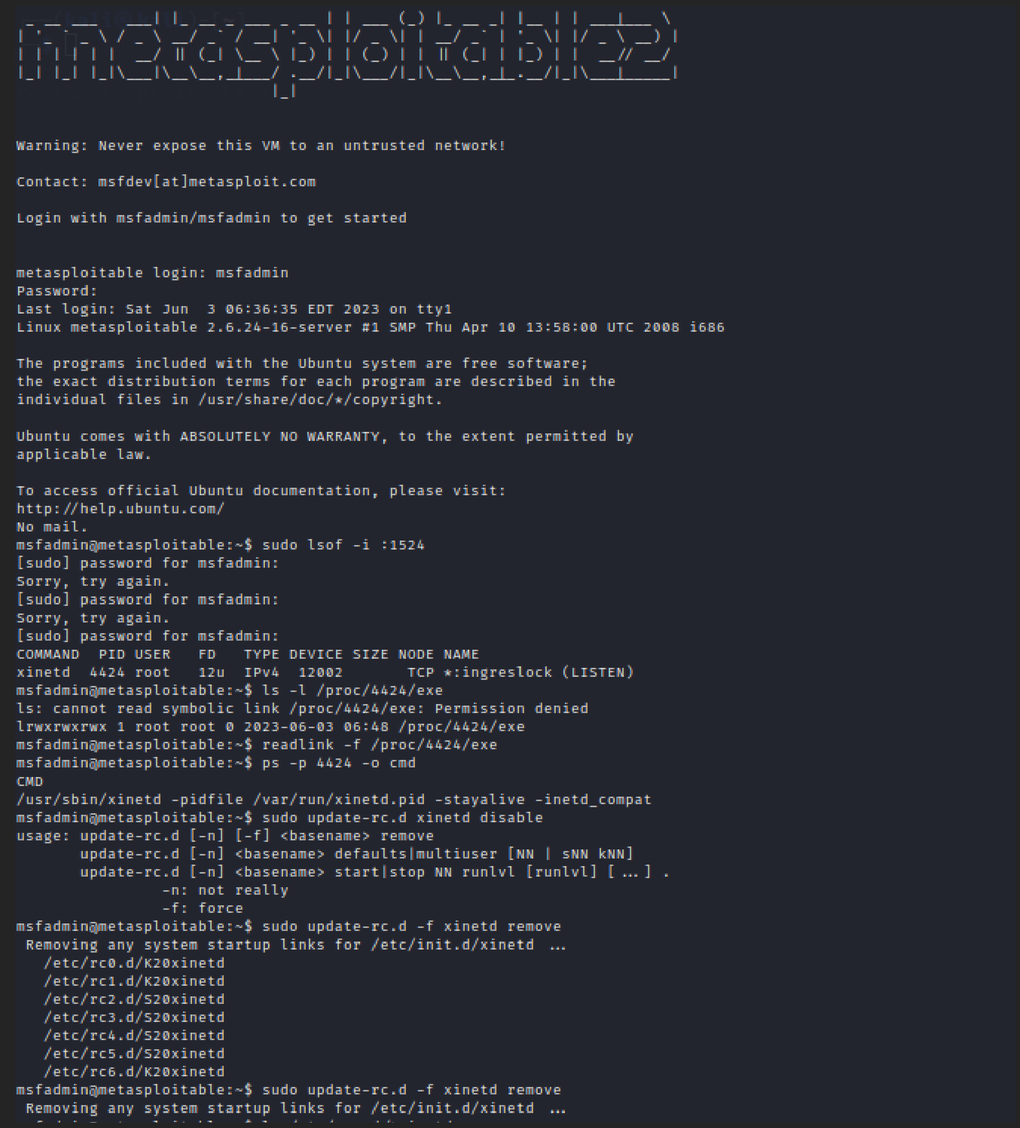
BIND SHELL BACKDOOR DETECTION

La prima vulnerabilità identificata consisteva nella presenza di una shell in ascolto sulla porta remota senza alcuna autenticazione richiesta. Questo avrebbe potuto consentire a un utente malintenzionato di connettersi alla porta remota e inviare comandi direttamente alla macchina.

Inizialmente, ho considerato di risolvere la vulnerabilità utilizzando IP tables per configurare un firewall. Tuttavia, ho riscontrato che dopo il riavvio della macchina la configurazione del firewall andava persa. Quindi ho optato per un approccio più aggressivo eliminando direttamente la vulnerabilità.

Ho eseguito il comando "sudo lsof -i :1524" per individuare il processo xinetd che stava ascoltando sulla porta 1524. Successivamente, ho utilizzato il comando "sudo update-rc.d -f xinetd remove" per rimuovere i link di avvio del servizio xinetd dai runlevel specificati. Infine, ho verificato che i link di avvio associati a xinetd fossero stati correttamente rimossi utilizzando il comando "ls /etc/rc*.d/*xinetd".

In poche parole, abbiamo identificato il processo demone xinetd che utilizzava la porta 1524 e abbiamo rimosso la sua configurazione di avvio automatico. Ciò impedisce al servizio xinetd di avviarsi automaticamente al riavvio del sistema. Inoltre, abbiamo verificato che i link di avvio associati a xinetd siano stati rimossi correttamente.La procedura è stata eseguita utilizzando la macchina Kali Linux per una maggiore praticità. Ho utilizzato il comando "telnet 192.168.51.103", in cui l'indirizzo IP corrisponde alla macchina Metasploitable. Questo comando mi ha consentito di connettermi alla macchina Metasploitable tramite il protocollo Telnet.



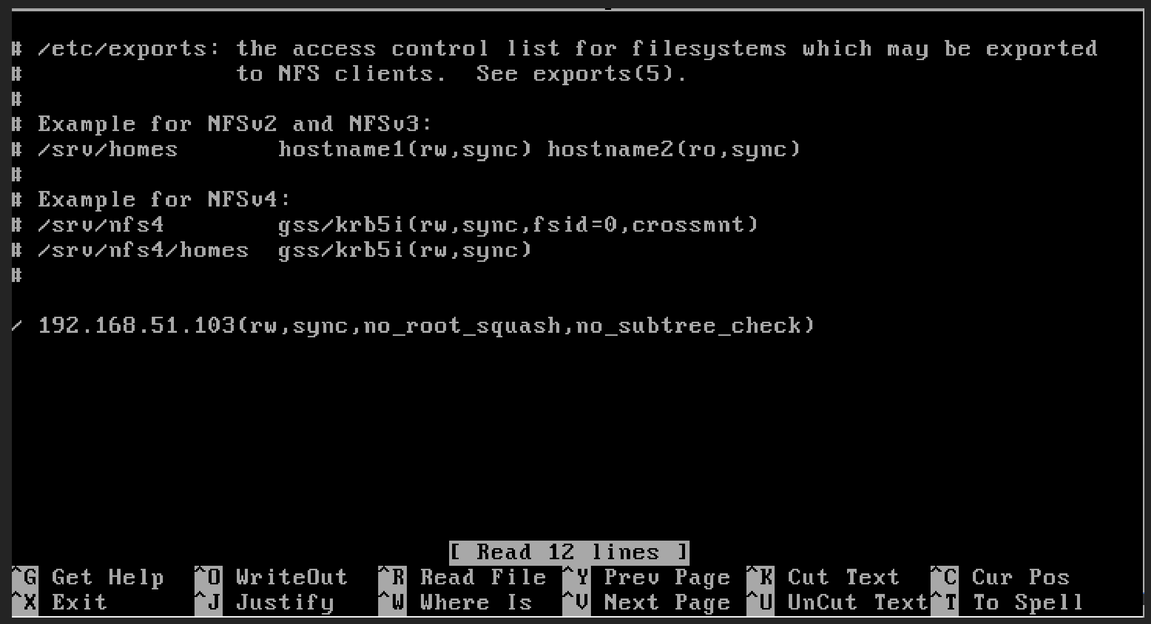
```
 _                                  _       _ _        _     _
| |_ ___ _ __ ___  _ __ ___   ___ | |_ ___| (_) ___  | |__ | | ___
| __/ _ \ '_ ` _ \| '_ ` _ \ / _ \| __/ _ \ | |/ _ \ | '_ \| |/ _ \
| ||  __/ | | | | | | | | | | (_) | ||  __/ | |  __/ | |_) | |  __/
 \__\___|_| |_| |_|_| |_| |_|\___/ \__\___|_|_|\___| |_.__/|_|\___|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Sat Jun  3 06:36:35 EDT 2023 on tty1
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 lsof -i :1524
[sudo] password for msfadmin:
Sorry, try again.
[sudo] password for msfadmin:
Sorry, try again.
[sudo] password for msfadmin:
COMMAND  PID USER   FD   TYPE DEVICE SIZE NODE NAME
xinetd  4424 root   12u  IPv4  12002       TCP *:ingreslock (LISTEN)
msfadmin@metasploitable:~$ ls -l /proc/4424/exe
ls: cannot read symbolic link /proc/4424/exe: Permission denied
lrwxrwxrwx 1 root root 0 2023-06-03 06:48 /proc/4424/exe
msfadmin@metasploitable:~$ readlink -f /proc/4424/exe
msfadmin@metasploitable:~$ ps -p 4424 -o cmd
CMD
/usr/sbin/xinetd -pidfile /var/run/xinetd.pid -stayalive -inetd_compat
msfadmin@metasploitable:~$ sudo update-rc.d xinetd disable
usage: update-rc.d [-n] [-f] <basename> remove
       update-rc.d [-n] <basename> defaults|multiuser [NN | sNN kNN]
       update-rc.d [-n] <basename> start|stop NN runlvl [runlvl] [ ... ] .
                -n: not really
                -f: force
msfadmin@metasploitable:~$ sudo update-rc.d -f xinetd remove
 Removing any system startup links for /etc/init.d/xinetd  ...
   /etc/rc0.d/K20xinetd
   /etc/rc1.d/K20xinetd
   /etc/rc2.d/S20xinetd
   /etc/rc3.d/S20xinetd
   /etc/rc4.d/S20xinetd
   /etc/rc5.d/S20xinetd
   /etc/rc6.d/K20xinetd
msfadmin@metasploitable:~$ sudo update-rc.d -f xinetd remove
 Removing any system startup links for /etc/init.d/xinetd  ...
```

REMEDIATION:

NFS EXPORTED SHARE INFORMATION DISCLOSURE

Questa vulnerabilità potrebbe consentire all'attaccante di accedere in modo non autorizzato alle condivisioni NFS esportate dal server remoto, consentendo loro di leggere (e potenzialmente modificare) i file sull'host remoto.
La prima cosa che ho fatto è comprendere che il file /etc/exports è il file di configurazione principale per il servizio NFS e determina quali file system sono esportati e quali host possono accedervi. Modificando correttamente questo file. Quindi per mitigare questa vulnerabilità ho esguito i seguenti passaggi :

1. Apro il file /etc/exports utilizzando l'editor di testo nano. Eseguo il comando seguente nel terminale: sudo nano /etc/exports
2. Trovo la riga nel file che inizia con / *(rw,sync,no_root_squash,no_subtree_check). Questa riga indica che l'intero file system radice ("/") è esportato e accessibile a tutti gli host.
3. Modifico la riga in modo che specifichi gli host autorizzati che possono accedere alla condivisione NFS. Modifico la riga come segue: / 192.168.51.103 (rw,sync,no_root_squash,no_subtree_check)
4. Salvo le modifiche e chiudo l'editor di testo. Utilizzo la combinazione di tasti Ctrl + X per uscire da nano e confermo di salvare le modifiche.
5. Riavvio macchina Meta in questo modo abbiamo mitigato la seguente vulnerabilità ,in più con questa procedura ne abbiamo eliminata una altra hight che aveva il nome NFS Shares World Readable come si evince dal report metafine.pdf



REMEDIATION:

VNC SERVER 'PASSWORD' PASSWORD

Questa vulnerabilità potrebbe consentire a un utente malintenzionato remoto e non autenticato di ottenere il controllo del sistema, a causa della debole protezione della password del server VNC in esecuzione sull'host remoto. Durante il test, Nessus è riuscito ad accedere al server utilizzando l'autenticazione VNC e la password predefinita "password". È fondamentale correggere questa situazione per prevenire possibili attacchi e garantire la sicurezza del sistema.

Per mitigare questa vulnerabilità, ho seguito i seguenti passaggi:

1. Ho aperto il terminale da Meta ed eseguito il comando "vncpasswd". Dopo aver effettuato alcune ricerche, ho scoperto che questo comando viene utilizzato per cambiare la password dei server VNC.
2. Mi è stato richiesto di inserire una nuova password per il VNC Server. Ho scelto una nuova password desiderata, tenendo presente l'importanza di utilizzare una password sicura e complessa. Tuttavia, è importante notare che la lunghezza massima della password era limitata a 8 caratteri nel mio caso. In generale, per gli standard attuali di sicurezza, si consiglia di utilizzare password di almeno 12 caratteri.
3. Successivamente, mi è stato chiesto di reinserire la nuova password per conferma. Ho digitato nuovamente la password e ho premuto Invio.
4. La password del VNC Server è stata modificata con successo.

```
etasploitable login: msfadmin
assword:
ast login: Sat Jun  3 11:21:04 EDT 2023 on tty1
inux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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

buntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
pplicable law.

o access official Ubuntu documentation, please visit:
ttp://help.ubuntu.com/
o mail.
sfadmin@metasploitable:~$ vncpasswd
sing password file /home/msfadmin/.vnc/passwd
assword:
erify:
ould you like to enter a view-only password (y/n)? n
```

REMEDIATION:

REXECD SERVICE DETECTION

Per l'ultima vulnerabilità, ho utilizzato un metodo di scansione diverso poiché Nessus non rilevava la vulnerabilità. Quindi ho utilizzato Nmap e ho effettivamente constatato che la porta 512 era aperta. Dopo una scansione più approfondita, ho confermato che il servizio era in esecuzione. È una buona pratica utilizzare più strumenti per evitare falsi positivi o falsi negativi.

Per mitigare questa vulnerabilità, ho seguito i seguenti passaggi:

1. Ho eseguito una scansione con Nmap su tutte le porte per individuare se la porta con la potenziale vulnerabilità era aperta. Ho utilizzato il comando "nmap -p 1-65535 192.168.51.103" per scansionare tutte le porte dell'host.
2. Una volta individuata la porta 512 come potenzialmente vulnerabile, ho effettuato una scansione più approfondita specificamente su quella porta utilizzando il comando "nmap -p 512 -A 192.168.51.103". Questa scansione mi ha confermato che il servizio era attivo sulla porta 512.
3. Successivamente, ho creato una regola nel firewall iptables per mitigare questa vulnerabilità. Ho utilizzato il comando "sudo iptables -A INPUT -p tcp --dport 512 -j DROP" per bloccare il traffico in ingresso sulla porta 512.
4. Infine, ho effettuato una prova utilizzando il comando "nc 192.168.51.103" per verificare se la porta era ancora in ascolto. Dopo aver applicato la regola di iptables, la porta non rispondeva più alle connessioni.

```
└─$ nmap -p 512 -A 192.168.51.103
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-04 05:48 EDT
Nmap scan report for 192.168.51.103
Host is up (0.00040s latency).

PORT    STATE SERVICE VERSION
512/tcp open  exec    netkit-rsh rexecd
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.41 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ ssh -oHostKeyAlgorithms=ssh-rsa,ssh-dss msfadmin@192.168.51.103
msfadmin@192.168.51.103's password:
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.
Last login: Sun Jun  4 06:19:14 2023 from 192.168.51.100
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 512 -j DROP
msfadmin@metasploitable:~$
```

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-04 06:23 EDT
Nmap scan report for 192.168.51.103
Host is up (0.00044s latency).

PORT    STATE    SERVICE VERSION
512/tcp filtered exec

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 13.52 seconds

┌──(kali㉿kali)-[~]
└─$
```