PEN. TEST DI FINE MESE, M3 CHRISTIAN BRENCI.

In questo report vedremo la risoluzione di alcune anomalie scansionate usando Nessus. Abbiamo un architetture server-client rispettivamente kali linux e metsplaitable 2.0 usufruendo di un ambiente virtuale (Virtual box).

Prenderemo singolarmente ogni anomalia, la analizzeremo graficamente e contestualizzeremo ogni passaggio.

VNC Server 'password' Password

```
root@metasploitable:/home/msfadmin# passwd
Enter new UNIX password:
Retype new UNIX password:
No password supplied
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@metasploitable:/home/msfadmin#
```

Questa anomalia era piuttosto semplice da risolvere, il problema era il seguente "Il server VNC in esecuzione sull'host remoto è protetto con una password debole". Il nostro programma ha rilevato che nel server precedentemente nominato, la password che richiedeva l'accesso era proprio "password" un malintenzionato potrebbe entrare in un batter d'occhio. Ho risolto per prima cosa richiedendo i permessi di root, subito dopo dando il comando "passwd" mi veniva chiesto di immettere la password attuale e dopo di metterne una nuova password più complessa e completa di caratteri speciali e numeri. Successivamente ridando la scansione l'anomalia era risolta.

NFS Exported Share Information Disclosure

```
/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)

/media/nfs 192.168.51.1/24(rw,sync,no_subtree_check)
```

Questa anomalia diceva "delle condivisioni NFS esportate dal server remoto potrebbe essere installata dall'host di scansione. Un utente malintenzionato potrebbe essere in grado di sfruttare questo per leggere (ed eventualmente scrivere) file sull'host



remoto." La soluzione a quest'ultima era limitare i permessi per la visualizzazione del contenuto solo a se stessi (metasploitable) specificandolo e immettendolo manualmente. Per esemplificare la lettura vi spiegherò a step.

- Step 1) modificheremo il file di configurazione /etc/exports. Qui posiamo configurare quali directory condividi e chi può accedervi. Possiamo anche impostare autorizzazioni specifiche per le condivisioni per limitare ulteriormente l'accesso. (foto1)
- Scriviamo il seguente comando /media/nfs (ip macchina)(eventuali specifiche) questo ci servirà per indicare e limitare l'accesso per la visualizzazione dei file NFC solo al nostro client. (foto 1)

```
root@metasploitable:/media/nfs# exportfs -arv
exporting 192.168.51.1/24:/media/nfs
root@metasploitable:/media/nfs# _
```

 Una volta impostato tutto nel modo desiderato, salviamo ed esciamo dal file.
 Quindi, eseguiamo il comando exportfs per caricare la nuova configurazione delle esportazioni. La nostra condivisione è ora accessibile dalle macchine client che abbiamo configurato (metasploit) nel nostro file /etc/exports.

```
mount -t nfs4 192.168.51.100:/media/nfs/media/
mount.nfs4: access denied by server while mounting 192.168.51.100:/media/nfs
```

Infine sulla nostra macchina server abbiamo provato a "montare" o
visualizzare il contenuto del file su una cartella da noi creata /media, l'accesso
ci è stato proibito risolvendo così l'anomalia e confermandoci la risoluzione
usando nessus.



Bind Shell Backdoor Detection

```
TYPE DEVICE SIZE NODE NAME
COMMAND PID USER
                    FD
xinetd
        4453 root
                     12u
                          IPv4
                                12080
                                             TCP *: ingreslock (LISTEN)
        4766 root
                          IPv4
                                             TCP 192.168.2.100:ingreslock->192.168
                     \theta u
                                12648
bash
.1.100:45822 (CLOSE_WAIT)
                                             TCP 192.168.2.100:ingreslock->192.168
bash
        4766 root
                     1u
                          IPv4
                                12648
.1.100:45822 (CLOSE_WAIT)
                                             TCP 192.168.2.100:ingreslock->192.168
        4766 root
                          IPv4
                                12648
bash
                     2u
.1.100:45822 (CLOSE_WAIT)
                                            TCP 192.168.2.100:ingreslock->192.168
        4766 root 255u
                          IPv4
                                12648
bash
             (CLOSE_WAIT)
.1.100:45822
        4779 root
                          IPv4
                                12648
                                            TCP 192.168.2.100:ingreslock->192.168
                     θп
nano
.1.100:45822 (CLOSE WAIT)
                                            TCP 192.168.2.100:ingreslock->192.168
                                12648
nano
        4779 root
                      1u
                          IPv4
.1.100:45822 (CLOSE_WAIT)
                                            TCP 192.168.2.100:ingreslock->192.168
nano
        4779 root
                     2u
                          IPv4
                                12648
.1.100:45822 (CLOSE_WAIT)
                                            TCP 192.168.2.100:ingreslock->192.168
        4872 root
                     0u
                          IPv4
                                12861
bash
.1.100:51460 (ESTABLISHED)
        4872 root
                                            TCP 192.168.2.100:ingreslock->192.168
bash
                      1u
                          IPv4
                                12861
.1.100:51460 (ESTABLISHED)
                                             TCP 192.168.2.100:ingreslock->192.168
                                12861
bash
        4872 root
                     2u
                          IPv4
.1.100:51460 (ESTABLISHED)
                                             TCP 192.168.2.100:ingreslock->192.168
        4872 root 255u
                          IPv4
                                12861
.1.100:51460 (ESTABLISHED)
root@metasploitable:/home/msfadmin#
```

Quest'anomalia diceva "Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può usarlo da collegandosi alla porta remota e inviando comandi direttamente." la risoluzione di questa anomalia è piuttosto semplice quanto complessa in quanto non avendo le competenze specifiche per la la sua risoluzione mi ha richiesto una ricerca più approfondita. Ho iniziato individuando il nome del demone associato alla porta che nessus ci ha trovato eseguendo la scansione (1524), il nome del demone è "xinetd" il "superdemone", inoltre in ci ha dato anche il nome della backdoor su quale il demone adopera "ingresslock".

```
root@metasploitable:/home/msfadmin# nc 192.168.51.100 1524
root@metasploitable:/# whoami
root
root@metasploitable:/# netstat -an | grep 192.168.51.100
                  0 192.168.51.100:53
                                              0.0.0.0:*
                                                                       LISTEN
tcp
                  0 192.168.51.100:1524
                                              192.168.51.100:48169
                                                                       ESTABLISHED
tcp
           0
                  34 192.168.51.100:48169
                                              192.168.51.100:1524
                                                                       ESTABLISHED
tcp
           0
                  0 192.168.51.100:137
                                              0.0.0.0:*
udp
           0
                    192.168.51.100:138
                  0
                                              0.0.0.0:*
udp
           0
                    192.168.51.100:53
                                             0.0.0.0:*
```

Successivamente documentandomi ho trovato il nome del file da modificare per la risoluzione dell'anomalia. Eseguo quindi il comando /etc/inetd.conf.



```
#<off># netbios-ssn
                                                                        /usr/sb$
                        stream
                                tcp
                                        nowait
                                                root
                                                        /usr/sbin/tcpd
telnet
                stream
                                nowait
                                        telnetd /usr/sbin/tcpd /usr/sbin/in.te$
                        tcp
#<off># ftp
                                                        /usr/sbin/tcpd /usr/sb$
                        stream
                                tcp
                                        nowait root
tftp
                                        nobody /usr/sbin/tcpd /usr/sbin/in.tf$
                                wait
                dgram
                        udp
shell
                        tcp
                                nowait
                                                                /usr/sbin/in.rs$
                stream
                                        root
                                                /usr/sbin/tcpd
login
                stream
                                nowait
                                        root
                                                /usr/sbin/tcpd
                                                                /usr/sbin/in.rl$
                        tcp
                                nowait
                                        root
                                                /usr/sbin/tcpd
                                                                 /usr/sbin/in.re$
exec
                stream
                        tcp
ngreslock stream top nowait root /bin/bash bash -i
```

Ci verrà presentata questa schermata, per risolvere l'anomalia basterà eliminare l'ultima stringa "ingresslock stream tcp..." ecc..

```
oot@metasploitable:/home/msfadmin# nc 192.168.51.100 1524
(UNKNOWN) [192.168.51.100] 1524 (ingreslock) : Connection refused
root@metasploitable:/home/msfadmin#
```

Infine usando netcat e provando a connettersi alla porta 1524 notiamo il messaggio "connection refused" cio' implica che non c'è connessione alla porta, indi per cui il processo e la backdoor associata sono stati disabilitati, eliminando la backdoor e l'anomalia. Confermiamo sempre alla fine con uno scan di nessus.

```
Rexecd server detection
  GNU nano 2.0.7
                               File: inetd.conf
                                                                         Modified
#<off># netbios-ssn
                         stream
                                 tcp
                                          nowait root
                                                          /usr/sbin/tcpd
telnet
                stream
                                 nowait
                                          telnetd /usr/sbin/tcpd /usr/sbin/in.te$
                         tcp
#<off># ftp
                                          nowait root /usr/sbin/tcpd /usr/sb$
                         stream
                                 tcp
tftp
                                 wait
                                         nobody
                                                 /usr/sbin/tcpd /usr/sbin/in.tf$
                dgram
                         udp
shell
                                                  /usr/sbin/tcpd /usr/sbin/in.rs$
/usr/sbin/tcpd /usr/sbin/in.rl$
                stream
                                 nowait
                         tcp
                                         ront
                stream
                         tcp
                                 nowait
                                         root
                                         nowait root /usr/sbin/tcpd /usr/sb$
#<off>#exec
                         stream
                                 ten
#<off>#ingreslock stream tcp nowait root /bin/bash bash -i
 msfadmin@metasploitable:/etc/xinetd.d$ ls
 chargen daytime discard echo ingreslock
                                                      rexecd time
                                                                       usftpd
 msfadmin@metasploitable:/etc/xinetd.d$
  GNU nano 2.0.7
                                File: rexecd
service rexecd
disable = yes
               Visualizza
      Macchina
                         Inserimento
                                    Dispositivi
msfadmin@metasploitable:~$ sudo lsof -i :512
msfadmin@metasploitable:~$ _
```

Questa anomalia non era presente nel report di nessus, ma noi sapevamo della sua presenza e abbiamo deciso di eliminarla lo stesso. L'anomalia consiste in "Il servizio rexecd è in esecuzione sull'host remoto. Questo servizio è progettato per consentire agli utenti di una rete di eseguire comandi in remoto. Tuttavia, rexecd non fornisce alcun buon mezzo di autenticazione, quindi un utente malintenzionato potrebbe abusarne per scansionare un host di terze parti." La risoluzione di questa anomalia è stata facile e veloce.

Abbiamo aperto il file /etc/inetd.conf, abbiamo commentato l'ultima stringa, un po' come nella risoluzione della della vulnerabilità della backdoor. Riavviando la macchina il problema era ancora presnte, così documentandoci, ho trovato la soluzione, abbiamo aperto il file rexecd e l'abbiamo disabilitato come vedere nella terza figura dall'alto. Dopo, facendo un controllo sulla porta, (ultimo screen) notiamo che non ci ritorna nessuna risposta, questo indica che il servizio è stato disabilitato e nessus ce lo conferma. Infondo trovare anomalie anche quando non ci vengono segnalate fa parte dei nostri test.

Samba Badlock Vulnerability

```
root@metasploitable:/home/msfadmin# apt-get remove samba
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
    samba-common
Use 'apt-get autoremove' to remove them.
The following packages will be REMOVED:
    samba
O upgraded, O newly installed, 1 to remove and 138 not upgraded.
After this operation, 6590kB disk space will be freed.
Do you want to continue [Y/n]? y
(Reading database ... 37634 files and directories currently installed.)
Removing samba ...
Stopping Samba daemons: nmbd smbd.
root@metasploitable:/home/msfadmin#_
```

Questa vulnerabilità non era classificata come critica ma noi per completezza l'abbiamo risolta lo stesso. La vulnerabilità consisteva in "La versione di Samba, un server CIFS/SMB per Linux e Unix, in esecuzione sull'host remoto è affetta da un difetto, noto come Badlock, presente nel Security Account Manager." Per risolvere è bastato usare il comando in alto nella foto, così facendo ho rimosso tutti i pacchetti di Samba e Samba stesso, eliminando l'anomalia.