

# Scansione Di **Mendolia Valerio**

Thu, 01 Jun 2023 04:29:43 EDT

## Contenuto

### Soluzioni alle vulnerabilità trovate su metasploitable

- 192.168.34.100

## 192.168.34.100

### Informazioni Host

Nome Netbios:	METASPLOITABLE
IP:	192.168.34.100
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

### Vulnerabilità Risolte:

**51988 - Bind Shell Backdoor Detection**

### Sintomi

Shell Remota caricata da terzi.

### Descrizione

Una shell remota chiamata wild\_shell è stata caricata da terzi ed ora è in esecuzione sulla porta 1524. Occorre al più presto poichè consente l'accesso a tutto il sistema senza login quindi andrò bloccare dal firewall questa porta ed effettuare la pulizia del sistema.

### Soluzione

Creazione di una regola personalizzata con pfsense in modo che la porta 1524 venga bloccata e successivamente si potrà pulire il sistema operativo:

Indirizzo Famiglia
IPv4
Seleziona la versione del protocollo Internet a cui si applica questa regola.

Protocollo
TCP
Scegli quale protocollo IP deve rispettare questa regola.

Origine

Origine
☐ Inverti abbinamento
qualsiasi
Origine Address
/

Mostra avanzate
L'intervallo di **porte di origine** per una connessione è in genere casuale e quasi mai uguale alla porta di destinazione. Nella maggior parte dei casi questa impostazione deve rimanere al suo valore predefinito, **qualsiasi** .

Destinazione

Destinazione
☐ Inverti abbinamento
Host singolo o alias
192.168.34.100
/

Intervallo porta di destinazione
(altra)
1524
(altra)
1524
Da Personalizzato A Personalizzato
Specificare la porta o l'intervallo di porte destinazione per questa regola. Il campo "A" può essere lasciato vuoto se si limita a filtrare una singola porta.

Opzioni extra

Ecco qua la regola finale, come si vedrà nel report finale la vulnerabilità verrà patchata:

Regole (trascinare per modificare l'ordine)											
<input type="checkbox"/>	Stati	Protocollo	Origine	Porta	Destinazione	Porta	Gateway	Coda	Planificazione	Descrizione	Azioni
<input checked="" type="checkbox"/>	0 / 2.60 MiB	*	*	*	LAN Address	80	*	*		Regola Anti-Lockout	
<input type="checkbox"/>	0 / 0 B	IPv4 TCP	*	*	192.168.34.100	1524	*	nessuno		Blocco la backdoor	
<input type="checkbox"/>	0 / 1007.50 MiB	IPv4 *	*	*	*	*	*	nessuno			

Aggiungi Aggiungi Elimina Salva Separatore

Ora non resta che ripulire il sistema operativo o reinstallarlo.

## Rischio

Critico

# 11356 - NFS Exported Share Information Disclosure

## Sintomi

È possibile accedere alle condivisioni NFS sull'host remoto.

## Descrizione

Almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione. Un utente malintenzionato potrebbe essere in grado di sfruttare questo per leggere (e possibilmente scrivere) file su host remoto.

## Soluzione

Modifica del file /etc/exports dove vengono contenute le configurazioni per l'NFS

```
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)

[ 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
```

Come si vede nell'immagine ora è settato in modo che tutti i file possono essere letti e modificati nella directory(/) con no\_root\_squash che stabilisce che si possano anche utilizzare i permessi root, quindi va patchato subito.

```
# /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)
#
/               *(noaccess,root_squash)
```

[ Read 12 lines ]

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

Successivamente verranno impostati parametri non permissivi come (No Access) e root\_squash in modo che l'accesso e l'utilizzo di root sia negato a terzi, successivamente si potrà anche solo stabilire una cartella accessibile dal pubblico.

## Rischio

Critico

## 61708 - VNC Server 'password' Password

### Sintomi

Un server VNC in esecuzione sull'host remoto è protetto da una password debole.

### Descrizione

Il server VNC in esecuzione sull'host remoto è protetto da una password debole. Nessus è stato in grado di accedere utilizzando l'autenticazione VNC e una password di "password". Un utente malintenzionato remoto e non autenticato potrebbe sfruttarlo per assumere il controllo del sistema.

### Soluzione

Proteggi il servizio VNC con una password sicura. Innanzitutto vado a cambiare la password a VNC dell'utente msfadmin con il comando '**sudo vncpasswd**':

```
metasploitable login: [B
Password:

Login incorrect
metasploitable login: msfadmin
Password:
Last login: Sat May 27 22:27:15 EDT 2023 on pts/1
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 vncpasswd
lsudol password for msfadmin:
Using password file /home/msfadmin/.vnc/passwd
Password: _
```

Successivamente mi accorgo di aver cambiato la password di vnc solo per l'utente msfadmin, ma un altro utente possiede la password per vnc cioè il root. Quindi vado ad eliminare la sua configurazione in modo da utilizzare solo l'utente msfadmin:(Elimino passwd nella cartella di root)

```
root@metasploitable:/# ls
bin boot cdrom dev etc home initrd initrd.img lib lost+found media mnt nohup.out opt proc root sbin srv sys tmp usr var vmlinuz
root@metasploitable:/# cd root
root@metasploitable:~# ls
Desktop reset_logs.sh vnc.log
root@metasploitable:~# ls -la
total 76
drwxr-xr-x 13 root root 4096 2023-05-27 23:45 .
drwxr-xr-x 21 root root 4096 2012-05-20 14:36 ..
lrwxrwxrwx 1 root root 9 2012-05-14 00:26 .bash_history -> /dev/null
-rw-r--r-- 1 root root 2227 2007-10-20 07:51 .bashrc
drwx----- 3 root root 4096 2012-05-20 15:08 .config
drwxr-xr-x 2 root root 4096 2012-05-20 15:08 Desktop
drwx----- 2 root root 4096 2012-05-20 15:13 .filezilla
drwxr-xr-x 5 root root 4096 2023-05-27 23:45 .fluxbox
drwx----- 2 root root 4096 2012-05-20 15:38 .gconf
drwx----- 2 root root 4096 2012-05-20 15:40 .gconfd
drwxr-xr-x 2 root root 4096 2012-05-20 15:09 .gststreamer-0.10
drwx----- 4 root root 4096 2012-05-20 15:07 .mozilla
-rw-r--r-- 1 root root 141 2007-10-20 07:51 .profile
drwx----- 5 root root 4096 2012-05-20 15:11 .purple
-rwx----- 1 root root 401 2012-05-20 15:55 reset_logs.sh
-rwx----- 1 root root 4 2012-05-20 14:25 .rhosts
drwxr-xr-x 2 root root 4096 2012-05-20 14:21 .ssh
drwx----- 2 root root 4096 2023-05-27 23:57 .vnc
-rw-r--r-- 1 root root 138 2023-05-27 23:45 vnc.log
-rw----- 1 root root 324 2023-05-27 23:45 .Xauthority
root@metasploitable:~# cd .vnc
root@metasploitable:~/.vnc# ls
metasploitable:0.log metasploitable:0.pid metasploitable:1.log metasploitable:2.log passwd xstartup
root@metasploitable:~/.vnc# rm passwd
root@metasploitable:~/.vnc# ls
metasploitable:0.log metasploitable:0.pid metasploitable:1.log metasploitable:2.log xstartup
root@metasploitable:~/.vnc# reboot
```

Mi accorgo che la vulnerabilità è sparita poichè sto utilizzando solo il mio account e la mia password

## Rischio

Critico

### 10203 - rexec Service Detection

## Sintomi

Il servizio rexecd è in esecuzione sull'host remoto

## Descrizione

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 potrebbe essere abusato da un attacco per scansionare host di terze parti.

## Soluzione

Commenta la riga 'exec' in /etc/inetd.conf e riavvia il processo inetd:

```
GNU nano 2.0.7      File: /etc/inetd.conf      Modified

#<off># netbios-ssn      stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/
telnet                  stream  tcp      nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.tel
#<off># ftp              stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/
tftp                   dgram  udp      wait    nobody   /usr/sbin/tcpd  /usr/sbin/in.tft
shell                  stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rsh
login                  stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rsh
#<off>#exec              stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/
ingreslock stream tcp nowait root /bin/bash bash -i
```

Successivamente riavviando il sistema la vulnerabilità è sparita.

## Rischio

Critico

## 134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat)

### Sintomi

C'è un connettore AJP vulnerabile in ascolto sull'host remoto.

### Descrizione

È stata rilevata una vulnerabilità di lettura/inclusione di file nel connettore AJP. Un utente malintenzionato remoto e non autenticato potrebbe sfruttare questa vulnerabilità per leggere i file dell'applicazione Web da un server vulnerabile. Nei casi in cui il server vulnerabile consente il caricamento di file, un utente malintenzionato potrebbe caricare codice JSP (JavaServer Pages) dannoso all'interno di una varietà di tipi di file e ottenere l'esecuzione di codice remoto (RCE).

### Soluzione

Aggiorna la configurazione AJP per richiedere l'autorizzazione, vado a modificare il file server.xml di tomcat 5.5:

```
Last login: Sun May 28 02:11:59 2023 from 192.168.33.100
msfadmin@metasploitable:~$ cd /etc/tomcat*
msfadmin@metasploitable:/etc/tomcat5.5$ ls
Catalina          logging.properties  server.xml.save      web.xml
catalina.policy    policy.d             server.xml.save.1
catalina.properties  server-minimal.xml  tomcat5.5
context.xml        server.xml            tomcat-users.xml
msfadmin@metasploitable:/etc/tomcat5.5$ sudo nano server.xml
msfadmin@metasploitable:/etc/tomcat5.5$ reboot
reboot: Need to be root
msfadmin@metasploitable:/etc/tomcat5.5$ sudo nano server.xml
msfadmin@metasploitable:/etc/tomcat5.5$
```

Successivamente modifico il parametro nello screen aggiungendo 'secretRequired="true"'

```
-->
  clientAuth="false" sslProtocol="TLS" />

<!-- Define an AJP 1.3 Connector on port 8009 -->
<Connector port="8009"
  enableLookups="false" redirectPort="8443" protocol="org.apache.coyote.ajp.AjpProtocol" secretRequired="true" />

<!-- Define a Proxyied HTTP/1.1 Connector on port 8082 -->
<!-- See proxy documentation for more information about using this, -->
<!--
  <Connector port="8082" proxy="http://192.168.33.100:8080" />
-->
```

In questo modo quando un utente cercherà di accedere alla pagina di tomcat apparirà un login prima di entrare nell'area riservata. Successivamente si possono cambiare username e password da un altro file di configurazione.

Rischio

Critico

90509 - Samba Badlock Vulnerability -

Sintomi



Un server SMB in esecuzione sull'host remoto è interessato dalla vulnerabilità Badlock.

Descrizione

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 (SAM) e nella Local Security Authority (Domain Policy) (LSAD ) a causa di una negoziazione errata del livello di autenticazione sui canali RPC (Remote Procedure Call). Un attaccante man-in-the-middle in grado di intercettare il traffico tra un client e un server che ospita un database SAM può sfruttare questa falla per forzare un downgrade del livello di autenticazione, che consente l'esecuzione di chiamate di rete Samba arbitrarie nel contesto dell'utente intercettato, come la visualizzazione o la modifica di dati sensibili sulla sicurezza nel database di Active Directory (AD) o la disabilitazione di servizi critici.

Soluzione

Blocca samba alla porta 445 e la porta 139 consentendole solo ad alcuni indirizzi ip fidati.

<input type="checkbox"/>	✖	0 / 432 B	IPv4 TCP	*	*	192.168.34.100	139 (NetBIOS-SSN)	*	nessuno	Blocco netbios	
<input type="checkbox"/>	✖	0 / 432 B	IPv4 TCP/UDP	*	*	192.168.34.100	445 (MS DS)	*	nessuno	Blocco smb	

Dopo aver impostato la regola inserire gli indirizzi ip che possono accedere a samba.

Rischio

Alto