Remediation 1

51988 - Bind Shell Backdoor Detection

Synopsis

The remote host may have been compromised.

Description

A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

Nessun ha trovato la porta TCP 1524 aperta che permette l'accesso diretto alla shell della macchina. Procedo ad inserire una regola REJECT nel firewall alle connessioni in entrata sulla porta 1524.

```
msfadmin@metasploitable:~$ sudo iptables -I INPUT -p tcp --dport 1524 -j REJECT
msfadmin@metasploitable:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
REJECT     tcp  --  anywhere             anywhere            tcp dpt:ingreslock
reject-with icmp-port-unreachable

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Remediation 2

11356 - NFS Exported Share Information Disclosure

Synopsis

It is possible to access NFS shares on the remote host.

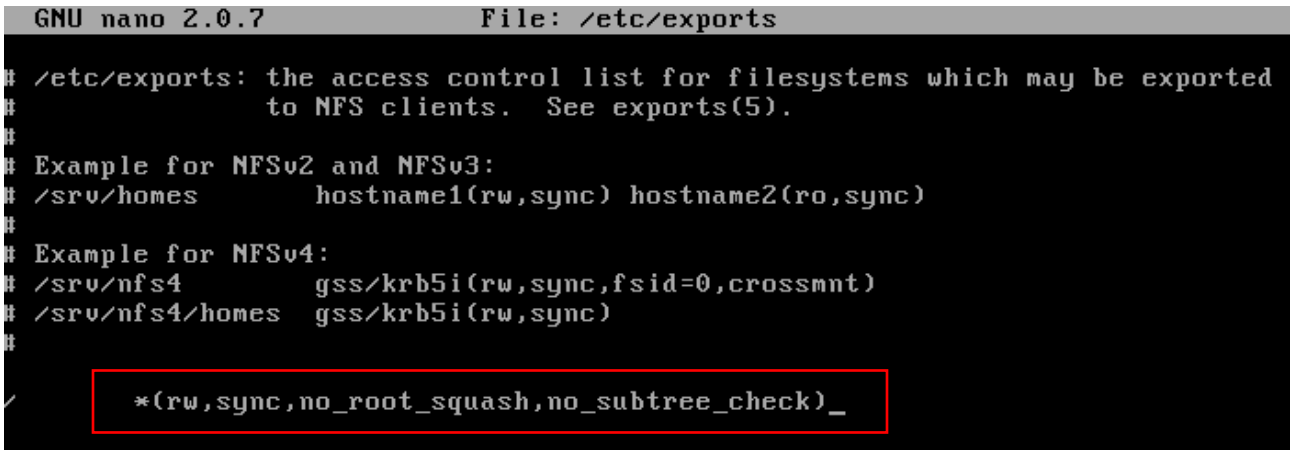
Description

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

Network file sharing è un protocollo che permette la condivisione di directory e file sulla rete tra macchine con differenti sistemi operativi. Verifico con il seguente comando la vulnerabilità segnalata da Nessus. Evinco che la root directory è condivisa e l'attaccante può montarla per visualizzare il contenuto, quindi visualizzare utenti e hash delle password nei file /etc/passwd e /etc/shadow per ottenere gli accessi privilegiati.

```
msfadmin@metasploitable:~$ showmount -e
Export list for metasploitable:
/ *
```

Quindi procedo a cancellare dal file export la riga nel riquadro rosso per non consentire più l'esposizione della directory root ai NFS clients.



Quindi verifico che non sia più presente nelle directory montabili.

Remediation 3

134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat)

Synopsis

There is a vulnerable AJP connector listening on the remote host.

Description

A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).

La vulnerabilità GhostCat consente ad un attaccante non autorizzato di leggere i file dell'applicazione web dal server interessato. L'attaccante potrebbe caricare file con codice malevolo che potrebbe consentire l'esecuzione remota di codice.

Per risolverla procedo ad aprile il file server.xml contenuto nella directory di Tomcat "conf" e commento (con !--) la riga nel riquadro rosso per disabilitare così il servizio AJP connector. La best practice è aggiornare il servizio Tomcat all'ultima versione disponibile, ma questo non mi è stato possibile sulla macchina di test metasploitable.

```
 GNU nano 2.0.7                File: server.xml                      Modified


    <!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
    <!--
    <Connector port="8443" maxHttpHeaderSize="8192"
               maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
               enableLookups="false" disableUploadTimeout="true"
               acceptCount="100" scheme="https" secure="true"
               clientAuth="false" sslProtocol="TLS" />
    -->

    <!-- Define an AJP 1.3 Connector on port 8009 -->
    <!-- Connector port="8009"
               enableLookups="false" redirectPort="8443" protocol="AJP/1.3" />

    <!-- Define a Proxied HTTP/1.1 Connector on port 8082 -->
    <!-- See proxy documentation for more information about using this. -->
    <!--
    <Connector port="8082"
               maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
               enableLookups="false" acceptCount="100" connectionTimeout="20000"
```

Remediation 4

61708 - VNC Server 'password' Password

Synopsis

A VNC server running on the remote host is secured with a weak password.

Description

The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Procedo cambiando la password con una più forte

```
root@metasploitable:/etc/postfix# vncpasswd
Using password file /root/.vnc/passwd
Password:
Warning: password truncated to the length of 8.
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:/etc/postfix#
```