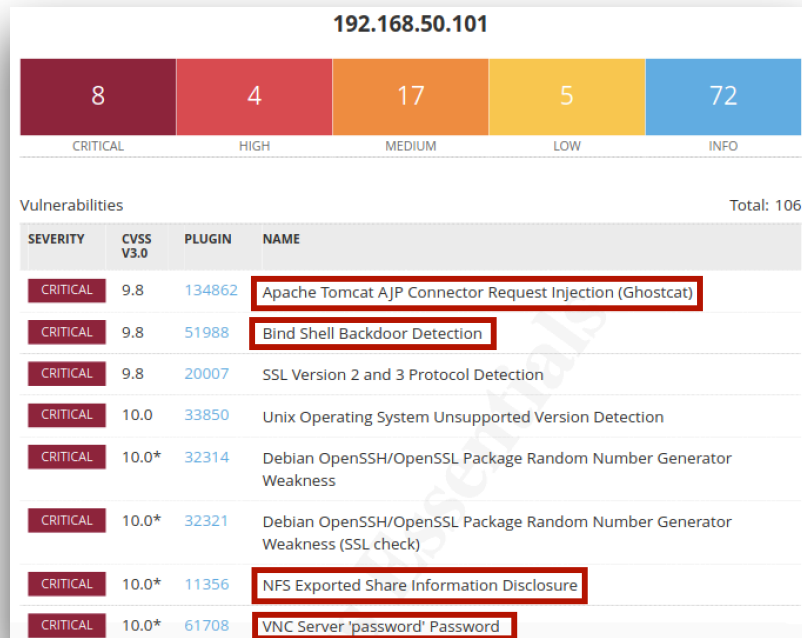


5. Progetto settimanale

SCANSIONE E RISOLUZIONE DELLE VULNERABILITA' SULLA MACCHINA METASPLOITABLE



Evidenziate in rosso possiamo vedere le vulnerabilità scelte per questo esercizio

CRITICAL 9.8 Apache Tomcat AJP Connector Request Injection (Ghostcat)

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

Descrizione

È stata rilevata una vulnerabilità di lettura/inclusione di file in un connettore JP. Potrebbe farlo un utente malintenzionato remoto e non autenticato 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 JavaServer Pages (JSP) dannoso all'interno una varietà di tipi di file e ottenere l'esecuzione di codice remoto (RCE).

CRITICAL 9.8 Bind Shell Backdoor Detection

L'host remoto potrebbe essere stato compromesso.

Descrizione

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 direttamente i comandi.

CRITICAL 10.0* NFS Exported Share Information Disclosure

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 attaccante potrebbe essere in grado di sfruttare questo per leggere (e possibilmente scrivere) file su host remoto.

CRITICAL 10.0* VNC Server 'password' Password

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 riuscito ad accedere utilizzando l'autenticazione VNC e una password di 'password'. Un utente malintenzionato remoto e non autenticato potrebbe sfruttare questo per prendere il controllo del sistema.



REMEDIATION

Apache Tomcat A JP Connector Request Injection (Ghostcat) (porta 8009)

- Dobbiamo disabilitare il protocollo AJP Connector
- Aprire il file di configurazione "server.xml" di Tomcat.
- Una volta trovata la cartella ed aperto il file, troviamo la sezione che si riferisce alla configurazione del protocollo AJP Connector.
- Commentare la linea di codice relativa alla configurazione del protocollo con i caratteri <!-- all'inizio della riga e --> alla fine.
- Così facendo possiamo disabilitare il protocollo AJP Connector e non potrà più essere sfruttato per accedere da remoto a Tomcat.

PRIMA

```
GNU nano 2.0.7      File: server.xml      Modified
      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"
      proxyPort="80" disableUploadTimeout="true" />
-->
```

DOPO

```
GNU nano 2.0.7      File: /usr/share/tomcat5.5/conf/server.xml      Modified
      noCompressionUserAgents="gozilla, traviata"
      compressableMimeType="text/html,text/xml"
-->

<!-- 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"
3" /> -->

<!-- Define a Proxied HTTP/1.1 Connector on port 8082 -->
<!-- See proxy documentation for more information about using this. -->
<!--
```

Bind Shell Backdoor Detection (porta 1524)

- Controlliamo la porta 1524 direttamente da Metasploitable.
- Come possiamo vedere il servizio attivo “ingreslock” è in ascolto.

```
root@metasploitable:~# nmap 192.168.50.101 -p1524

Starting Nmap 4.53 ( http://insecure.org ) at 2023-02-24 08:06 EST
Interesting ports on 192.168.50.101:
PORT      STATE SERVICE
1524/tcp  open  ingreslock

Nmap done: 1 IP address (1 host up) scanned in 13.264 seconds
root@metasploitable:~# netstat -an | grep LISTEN | grep 1524
tcp        0      0 0.0.0.0:1524          0.0.0.0:*            LISTEN
root@metasploitable:~#
```

- Una volta individuato il servizio dobbiamo andare a modificarlo accedendo alla Shell del sistema e commentando la stringa del servizio. Così facendo ad ogni riavvio della macchina, il servizio non sarà più attivo ed impedirà la vulnerabilità.

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

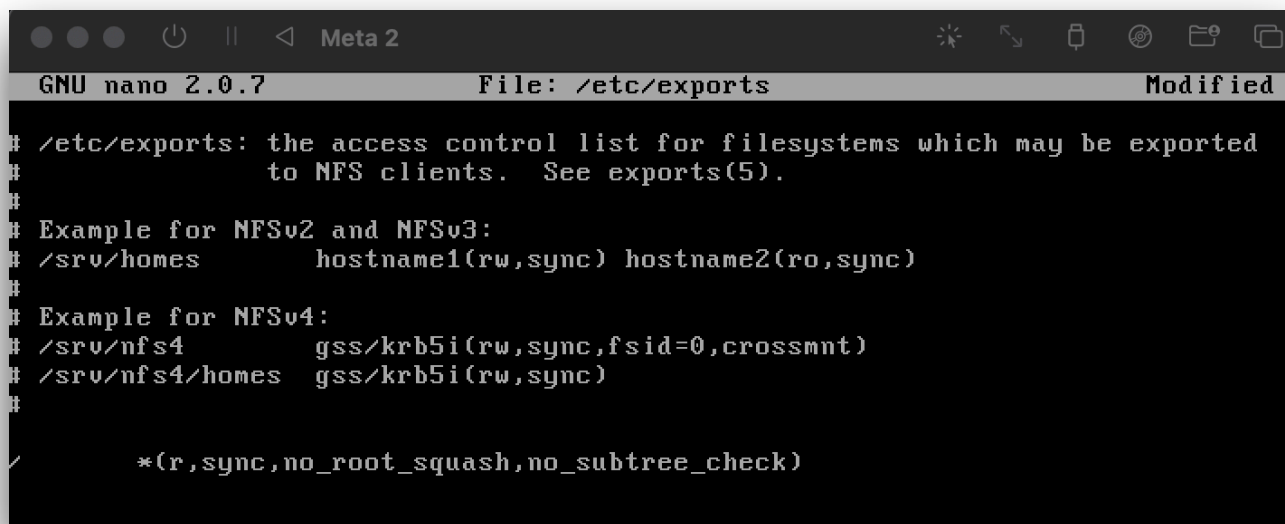
#<off># netbios-ssn    stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.tftpd
telnet               stream  tcp     nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.telnetd
#<off># ftp            stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.ftpd
tftp                 dgram   udp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

(Commento dell'ultima riga corrispondente al servizio)

NFS Exported Share Information Disclosure (porta 2049)

- Essendo NFS un protocollo per condivisione di file e directory tra computer in una rete, è una condivisione esposta a rischi.

-Per questo motivo modifichiamo i permessi degli altri utenti di avere accesso alla scrittura del file.



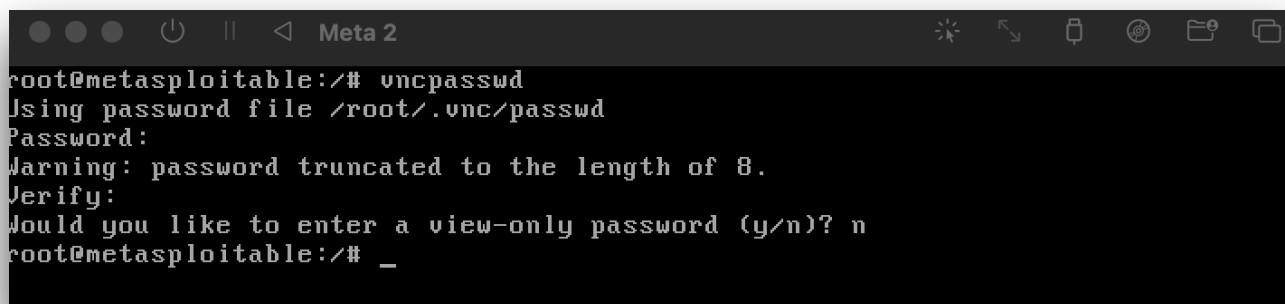
```
GNU nano 2.0.7      File: /etc/exports      Modified
# /etc/exports: the access control list for filesystems which may be exported
#                  to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes       hostname1(rw,sync) hostname2(ro,sync)
#
# Example for NFSv4:
# /srv/nfs4        gss/krb5i(rw,sync,fsid=0,crossmnt)
# /srv/nfs4/homes  gss/krb5i(rw,sync)
#
/*(r,sync,no_root_squash,no_subtree_check)
```

(In precedenza nell'ultima riga c'era la possibilità anche di scrivere il file con *rw,sync, no..)

VNC Server 'password' Password (porta 5900)

- Essendo il VNC Server un software di accesso remoto da un pc all'altro, in questo caso la vulnerabilità la troviamo nella richiesta della password che è troppo semplice

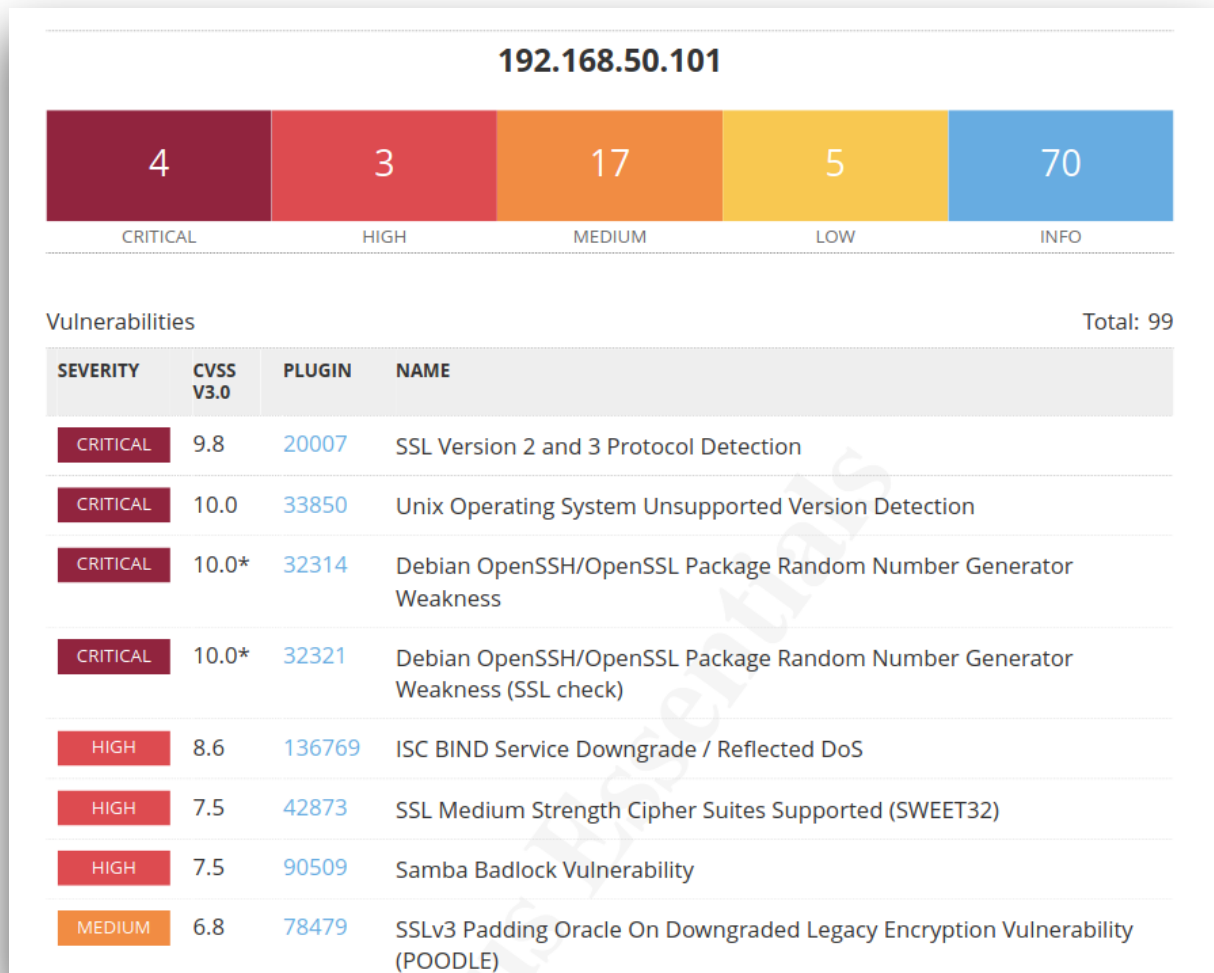
-Per evitare questo problema abbiamo dovuto modificare la password troppo semplice già presente e sostituirla con una più complicata. In modo da impedire l'accesso ai non autorizzati.



```
root@metasploitable:/# 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:/# _
```



SCANSIONE DOPO LE MODIFICHE CHE EVIDENZIA LA RISOLUZIONE DELLE VULNERABILITA'



Come possiamo vedere nella scansione effettuata dopo la risoluzione dei problemi, non troviamo più la presenza delle vulnerabilità precedenti.