W12D4 - Pratica

Report sulla valutazione e delle vulnerabilità e remediation su Metasploitable

Introduzione

- **Obiettivo:** Utilizzare Nessus come strumento di scansione delle vulnerabilità sulla macchina Metasploitable
- **Strumenti Utilizzati:** Nessus, la sua documentazione delle vulnerabilità conosciute e materiale trovato su internet.
- **Target:** Metasploitable è una macchina virtuale progettata per essere vulnerabile ed utilizzata come "campo" di addestramento per chi inizia ad imparare la cybersecurity.

Scansione Iniziale e Analisi

Metodologia di Scansione

- La scansione viene fatta con Nessus, uno strumento di scansione delle vulnerabilità conosciute. Viene utilizzato in ambito lavorativo per individuare debolezze nei sistemi informatici e fare report, per poi eventualmente passare all'effettiva messa in sicurezza di essi per prevenire attacchi informatici.
- La scansione fatta è completa e su tutte le porte

Risultati Iniziali

- La scansione di base (la prima fatta sulla macchina prima di fare la remediation) mostra decine di vulnerabilità, le più urgenti (critical) sono 7.
- La scansione sta nella repository (`Scansione di base.pdf`).

192.168.50.101

Vulnerabilities Total: 104

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	-	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0*	-	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	-	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	-	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	-	61708	VNC Server 'password' Password

Remediation delle Vulnerabilità

Vulnerabilità Scelte

- Queste sono le vulnerabilità critiche che sono riuscito a risolvere:
  - **Apache Tomcat A JP Connector Request Injection (Ghostcat):**
    - 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).S
  - **Bind Shell Backdoor Detection:**
    - 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.
  - **NFS Exported Share Information Disclosure:**
    - 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.
  - **VNC Server 'password' Password:**
    - 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.

Azioni di Remediation

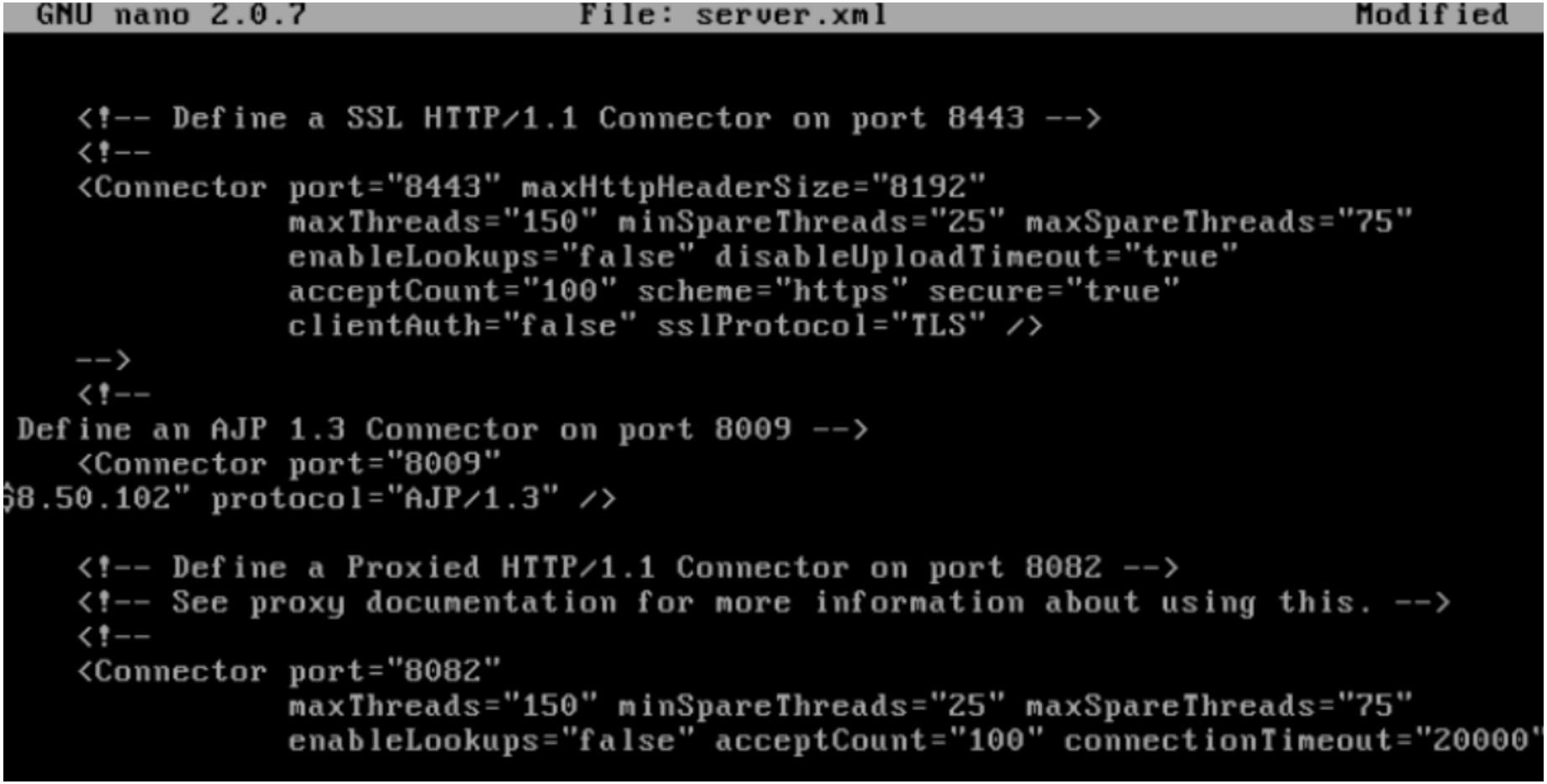
- Di seguito tutti i passaggi fatti per risolvere le vulnerabilità:

Apache Tomcat A JP Connector Request Injection (Ghostcat)

Ho disabilitato il connettore AJP che può essere utilizzato per sfruttare la vulnerabilità Ghostcat.
Per farlo ho commentato la linea nel file server.xml che configura il connettore AJP:

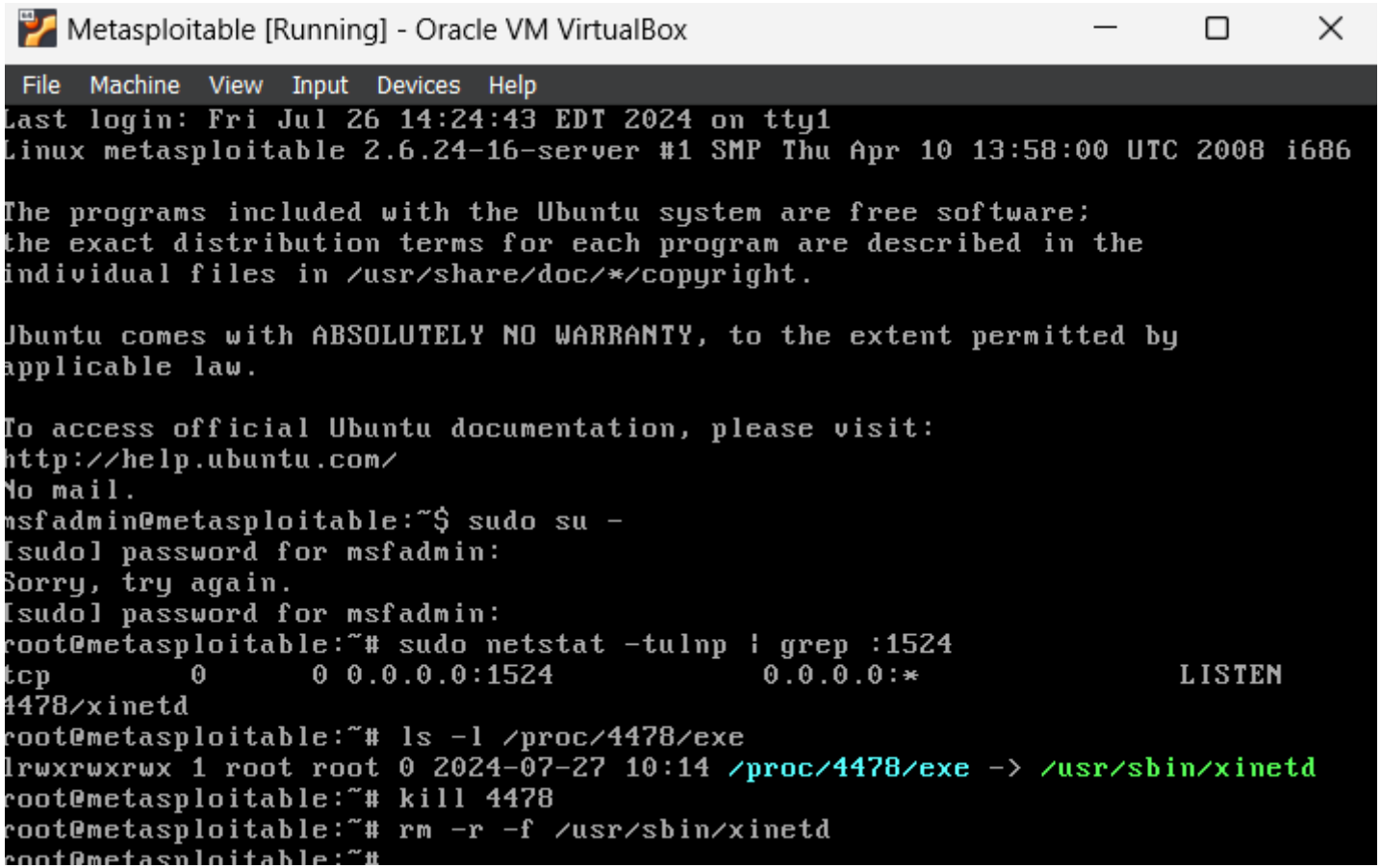
```
msfadmin@metasploitable:~$ cd /etc
msfadmin@metasploitable:/etc$ cd tomcat5.5
msfadmin@metasploitable:/etc/tomcat5.5$ ls
Catalina              context.xml         server-minimal.xml  tomcat-users.xml
catalina.policy       logging.properties  server.xml          web.xml
catalina.properties   policy.d            tomcat5.5
msfadmin@metasploitable:/etc/tomcat5.5$ sudo nano server.xml_
```

```
 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" address="192.168.50.1$

    <!-- 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"

^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
```



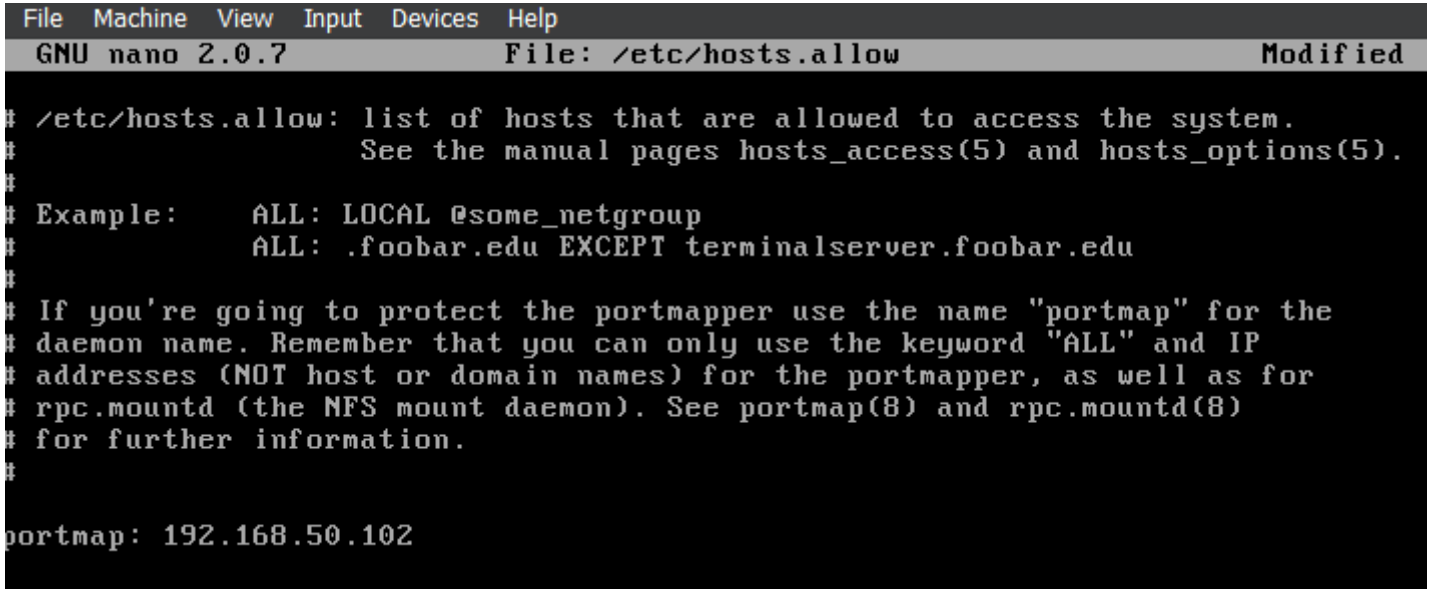
Bind Shell Backdoor Detection

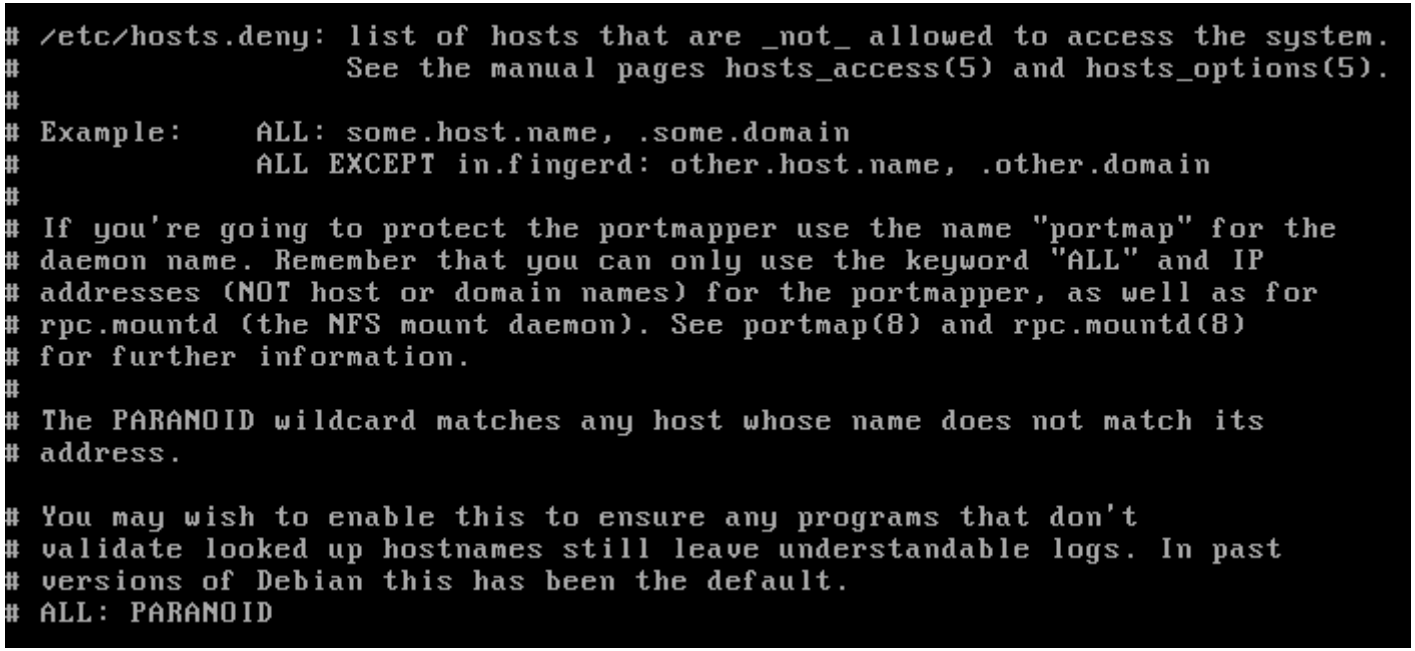
Dopo aver individuato il processo della backdoor l'ho eliminato e sono risalito allo script che avvia la backdoor rimuovendola definitivamente:



NFS Exported Share Information Disclosure

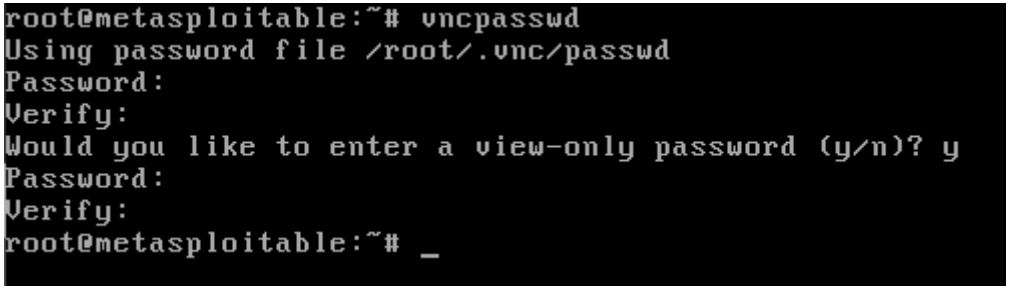
Modifico i file /etc/hosts.allow e /etc/hosts.deny per controllare l'accesso ai servizi NFS:





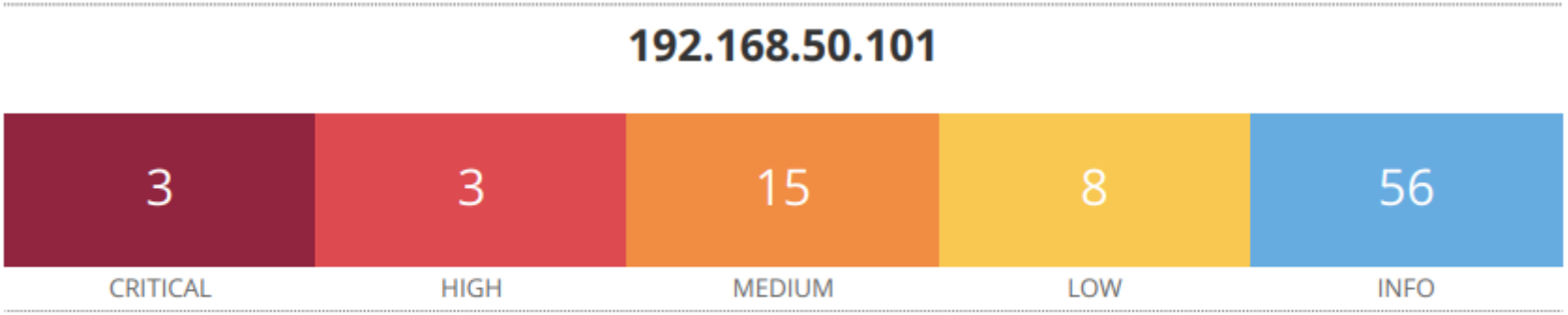
VNC Server 'password' Password

Ho cambiato la password in una più sicura:



Scansione Post-Remediation

ecco come appare la lista delle vulneranilità critiche dopo aver eseguito l'azione di remediation:



Vulnerabilities Total: 85

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0*	5.1	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	5.1	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

Risultati Post-Remediation

la riduzione delle vulnerabilità ha ridotto superficie di attacco e migliorato la sicurezza della macchina.
Nella repository è allegata la scansione finale (`Scansione finale.pdf`).

Conclusione

Dopo aver rimediato ad alcune delle vulnerabilità più critiche, bisogna continuare con le altre residue e manutenere costantemente la macchina.
Nel caso di una macchina reale, conviene sempre aggiornarla e fare scansioni periodiche.