VULNERABILITY ASSESSMENT

Report di scansione completa sul target Metasploitable
Matteo Tedesco.

Date Prepared: 10/05/2024

Obiettivo

Lo scopo del report è quello di effettuare una scansione completa utilizzando Nessus sul target Metasploitable, identificando e analizzando le vulnerabilità presenti nel sistema al fine di valutarne la sicurezza complessiva e fornire raccomandazioni per migliorare la sua resistenza agli attacchi informatici. Verranno effettuate delle azioni di rimedio e verrà spiegato nel dettaglio come sono state implementate.

Informazioni

Nessus è un potente strumento di scansione delle vulnerabilità progettato per identificare e valutare le debolezze nei sistemi informatici. Utilizzando un vasto database di plugin, Nessus esegue scansioni approfondite per rilevare vulnerabilità di sicurezza, configurazioni non sicure e potenziali punti di accesso per gli attaccanti. Eseguendo Nessus da Kali Linux abbiamo lanciato lo scan utilizzando come target l'indirizzo IP 192.168.50.101 di Metasploitable e dopo la scansione abbiamo ricevuto informazioni su tutte le criticità, il loro livello di rischio e dei consigli su come risolverle.

Primo scan sul Target

192.168.50.101

CRITICAL	HIGH	MEDIUM	LOW	INFO
8	4	17	6	72

Vulnerabilities — Total: 107

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	-	33850	Unix Operating System Unsupported Version 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
HIGH	8.6	-	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42256	NFS Shares World Readable
HIGH	7.5	-	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	-	90509	Samba Badlock Vulnerability

Durante la scansione del sistema con Nessus, sono state individuate diverse vulnerabilità di varia gravità, classificate in base a un sistema di colori per facilitare la comprensione delle azioni correttive.

- **Criticità Critiche (Critical):** Sono state individuate vulnerabilità critiche che rappresentano le minacce più gravi per la sicurezza del sistema. Queste vulnerabilità richiedono un'azione immediata in quanto possono essere sfruttate facilmente dagli attaccanti per compromettere la sicurezza del sistema.
- **Criticità Alte (High):** Le vulnerabilità classificate come alte presentano un rischio significativo per la sicurezza del sistema. Se non affrontate, potrebbero consentire agli attaccanti di ottenere accesso non autorizzato o compromettere l'integrità dei dati.

- **Criticità Medie (Medium):** Sono state individuate vulnerabilità di media gravità che rappresentano un rischio potenziale per la sicurezza del sistema. Sebbene non siano altrettanto gravi delle vulnerabilità critiche o alte, richiedono comunque un'attenzione immediata per garantire la sicurezza complessiva del sistema.
- **Informazioni (Info):** Inoltre, sono state identificate alcune informazioni riguardanti configurazioni non ottimali o dettagli del sistema che, sebbene non rappresentino una minaccia diretta per la sicurezza, possono contribuire a migliorare la postura di sicurezza complessiva del sistema.

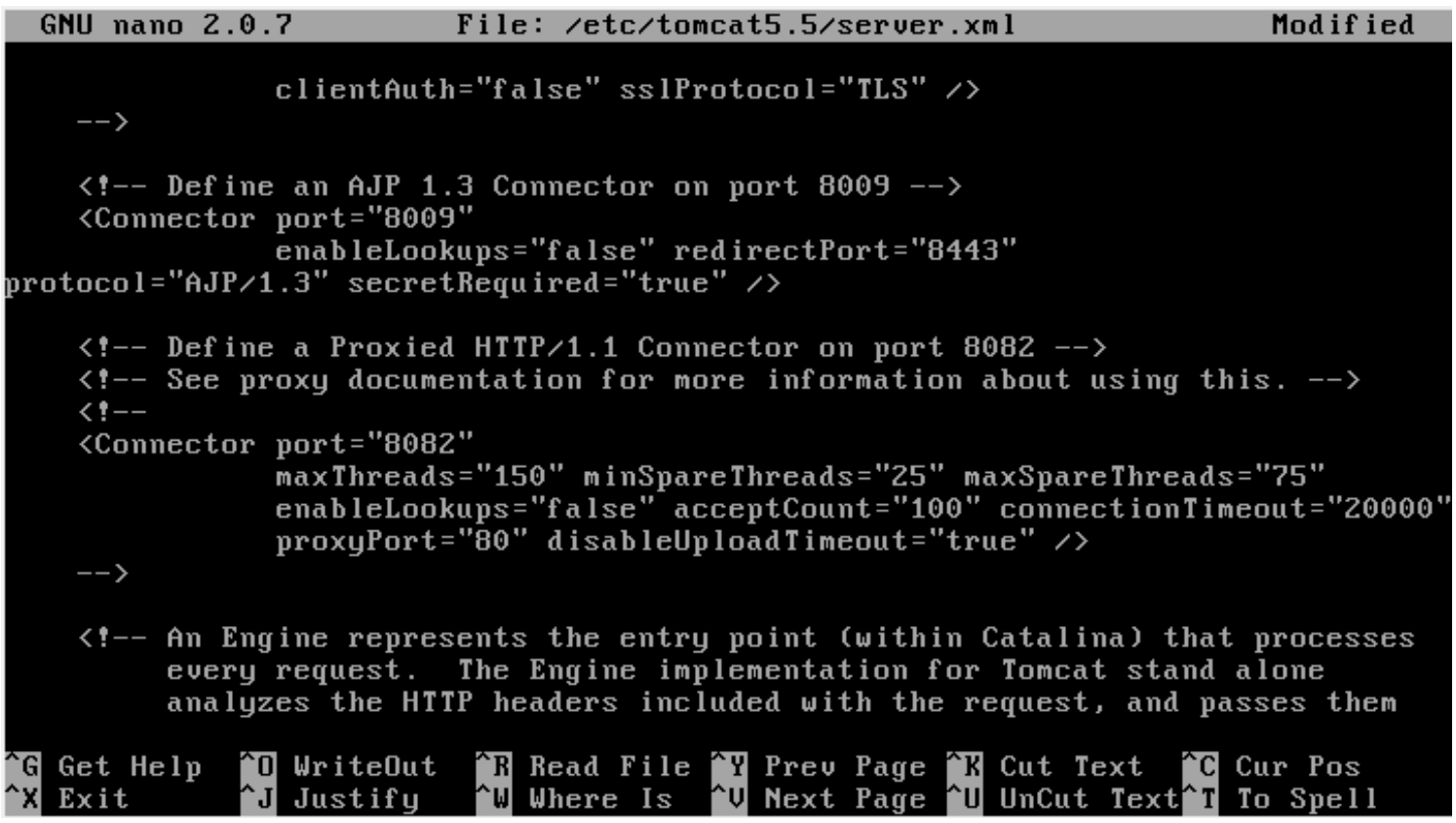
Azioni di rimedio

Apache Tomcat AJP Connector Request Injection (Ghostcat)

Questa riguarda una vulnerabilità di lettura di file nel connettore AJP (Apache JServ Protocol) su un server Tomcat. Un attaccante remoto e non autenticato potrebbe sfruttare questa vulnerabilità per leggere file dell'applicazione web da un server vulnerabile. In casi in cui il server vulnerabile consenta il caricamento di file, un attaccante potrebbe caricare codice JavaServer Pages (JSP) maligno all'interno di una varietà di tipi di file e ottenere l'esecuzione remota del codice (RCE).

Per la risoluzione è stato possibile aggiornare la configurazione AJP (Apache JServ Protocol) per richiedere l'autorizzazione su Metasploitable.
E’ stato individuato il file di configurazione

1. **E’ stato individuato il file di configurazione di Tomcat che gestisce il connettore AJP chiamato server.xml nella cartella di configurazione Tomcat**
2. **Il file di configuazione server.xml di Tomcat è stato aperto tramite editor di testo**
3. **E’ stata cercata la sezione del file relativa alla configurazione del connettore AJP**
4. **E’ stata aggiunta la configurazione di autorizzazione modificando la configurazione del connettore. E’ bastato aggiungere l’attributo ‘’secretRequired=true” per richiedere l’autorizzazione.**
5. Il risultato è <Connector port="8009" protocol="AJP/1.3" redirectPort="8443" secretRequired="true" />



Vnc server password ‘’password’’

VNC sta per "Virtual Network Computing". È un sistema software che consente di controllare e interagire con un computer remoto tramite una connessione di rete. In sostanza, VNC consente di visualizzare il desktop di un computer remoto e di interagire con esso come se ci si trovasse fisicamente di fronte a esso. VNC è utilizzato per una vasta gamma di scopi, tra cui l'assistenza remota, l'amministrazione di sistemi, la condivisione del desktop e molto altro ancora. È una tecnologia utile per consentire l'accesso e il controllo di computer remoti in modo efficiente e flessibile.
Questa vulnerabilità riguarda l'utilizzo di una password debole per il server VNC (Virtual Network Computing) in esecuzione sul server remoto. Utilizzare una password debole rende il sistema vulnerabile agli attacchi di forza bruta, consentendo a un attaccante remoto e non autenticato di prendere il controllo del sistema. **Per risolvere questa vulnerabilità, la soluzione proposta è quella di proteggere il**

servizio VNC con una password forte.

Modifica della password: Accedendo al server VNC è stata cambiata la password utilizzata per l'autenticazione. E' importante scegliere una password **complessa** e **robusta** che includa una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali.

1. **Abilitare il blocco degli indirizzi IP**: Se possibile, è importante configurare il server VNC per limitare l'accesso solo da determinati indirizzi IP autorizzati. Questo può essere fatto tramite la configurazione del firewall o delle regole di accesso del server VNC.
2. **E' importante fornire formazione agli utenti sulle pratiche di sicurezza delle password e sulla loro importanza**
3. **Mantenere aggiornato il software del server VNC per proteggere il sistema da vulnerabilità note**

   in questo caso è stata utilizzata una password di 8 caratteri composta da maiuscole, minuscole numeri e lettere.

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 1524 -j DROP
[sudo] password for msfadmin:
msfadmin@metasploitable:~$ sudo iptables-save
# Generated by iptables-save v1.3.8 on Sun May 12 08:29:14 2024
*filter
:INPUT ACCEPT [157:32439]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [173:33702]
-A INPUT -p tcp -m tcp --dport 1524 -j DROP
COMMIT
# Completed on Sun May 12 08:29:14 2024
msfadmin@metasploitable:~$
```

NSF SHARE INFORMATION DISCLOSURE

Durante lo scan del sistema Metasploitable utilizzando Nessus, è stata individuata una configurazione non sicura delle impostazioni NFS. NFS (Network File System) supporta la condivisione di file e cartelle tra sistemi Linux/Unix, consentendo il "montaggio" di una share remota localmente. Tuttavia, la configurazione attuale su Metasploitable consente a tutti di accedere a tutte le share condivisibili. Questo può comportare rischi di sicurezza significativi, inclusi accessi non autorizzati ai file e potenziali violazioni della privacy e della sicurezza dei dati.

La configurazione non sicura di NFS su Metasploitable può comportare diversi rischi per la sicurezza del sistema:

- **Accesso non autorizzato ai file**: Consentendo l'accesso a tutte le share condivisibili da parte di qualsiasi host sulla rete, un attaccante potrebbe accedere e manipolare i file sensibili sul sistema Metasploitable.
- **Violazione della privacy e della sicurezza dei dati**: Se i file sensibili o riservati vengono esposti tramite NFS, potrebbe verificarsi una violazione della privacy e della sicurezza dei dati.
- **Rischi di esecuzione di codice malevolo**: Un attaccante potrebbe sfruttare l'accesso alle share condivisibili per eseguire codice malevolo sul sistema Metasploitable, compromettendo ulteriormente la sua sicurezza.

```
  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
```

L’attuale configurazione di metasploitable consentiva a tutti di accedere a tutte le share condivisibili. Tra le possibili soluzioni è stato scelto di limitare l'accesso alle cartelle condivisibili e contemporaneamente restrignere le macchine che possono accedere tramite la modifica dei file di configurazione.

I percorsi di configurazione sono stati raggiunti con il comando sudo nano **/etc/exports**
e sudo nano **/etc/hosts.allow**

```
  GNU nano 2.0.7                File: /etc/hosts.allow                      Modified

# /etc/hosts.allow: list of hosts that are allowed to access the system.
#                   See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:    ALL: LOCAL @some_netgroup
#             ALL: .foobar.edu EXCEPT terminalserver.foobar.edu
#
# If you're going to protect the portmapper use the name "portmap" for the
# daemon name. Remember that you can only use the keyword "ALL" and IP
# addresses (NOT host or domain names) for the portmapper, as well as for
# rpc.mountd (the NFS mount daemon). See portmap(8) and rpc.mountd(8)
# for further information.
#

ALL:192.168.50.101_

^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
```

Bind Shell Backdoor

Durante l'analisi del sistema Metasploitable, è stata individuata la presenza di una **backdoor attiva** sulla porta 1524. Questa backdoor rappresentava un serio rischio per la sicurezza del sistema, in quanto consentiva a potenziali attaccanti di ottenere accesso non autorizzato al sistema e di eseguire azioni dannose.

Tramite il comando nc 192.168.50.101 1524 (indirizzo Ip e porta) ci si è resi conto dell’effettiva comunicazione tramite la porta 1524.

```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.50.101 1524
root@metasploitable:/# id
uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/# whoami
root
root@metasploitable:/#
```

Per la risoluzione del problema ci si è adoperati per la chiusura della porta dal terminale di Metasploitable tramite il comando: iptables -A INPUT -p tcp --dport 1524 -j DROP.
Nello screen sottostante abbiamo la conferma di chiusura della comunicazione.

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 1524 -j DROP
[sudo] password for msfadmin:
msfadmin@metasploitable:~$ sudo iptables-save
# Generated by iptables-save v1.3.8 on Sun May 12 08:29:14 2024
*filter
:INPUT ACCEPT [157:32439]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [173:33702]
-A INPUT -p tcp -m tcp --dport 1524 -j DROP
COMMIT
# Completed on Sun May 12 08:29:14 2024
msfadmin@metasploitable:~$
```

Da questo momento, dal terminale di kali linux non sarà più possibile entrare in comunicazione.

```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.50.101 1524
(UNKNOWN) [192.168.50.101] 1524 (ingreslock) : Connection timed out
```

RISULTATI FINALI ED ANALISI DEL RISCHIO

Durante l'attività di testing condotta sul sistema , sono state identificate e corrette diverse vulnerabilità che potrebbero potenzialmente esporre a rischi significativi per la sicurezza delle informazioni. Di seguito riportiamo un'analisi dettagliata dei rischi identificati, delle azioni correttive adottate e delle raccomandazioni per la gestione del rischio residuo.

Azioni Correttive

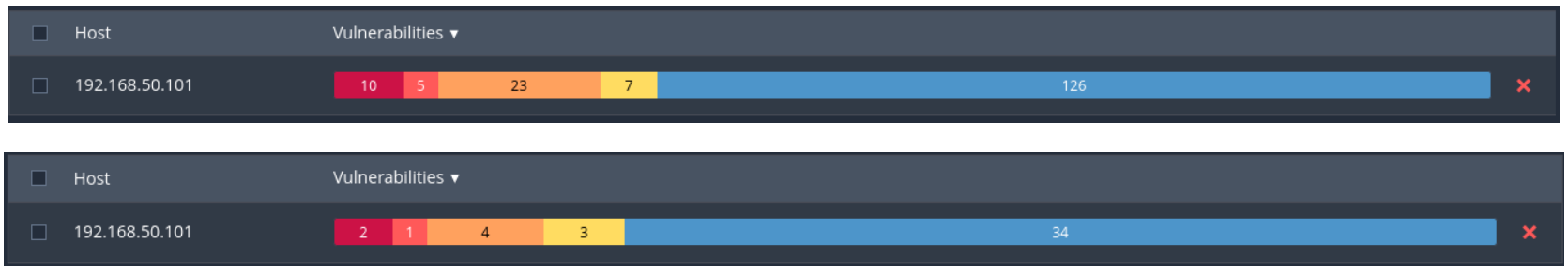
Sono state svolte diverse azioni correttive, qui vengono riportate alcune di queste:

1. **Configurazione del Servizio NFS**: Le condivisioni NFS sono state rese più sicure attraverso la restrizione degli accessi e l'implementazione di regole firewall per limitare l'esposizione dei servizi vulnerabili.
2. **Rimozione della Backdoor**: La backdoor attiva sulla porta 1524 è stata identificata e rimossa, impedendo ulteriori accessi non autorizzati al sistema.
3. **Potenziamento della Sicurezza del Servizio VNC**: La password del servizio VNC è stata cambiata e resa più sicura, riducendo così il rischio di accessi non autorizzati.
4. **Aggiornamento della Configurazione del Servizio AJP**: La configurazione del servizio AJP è stata aggiornata per richiedere l'autenticazione e per ridurre le vulnerabilità di lettura dei file e di esecuzione remota di codice.

Dopo l'implementazione delle azioni correttive, è essenziale gestire il **rischio residuo** per garantire la sicurezza continua del sistema.
Se il rischio residuo rimane significativo, possono essere effettuati **ulteriori test** e miglioramenti per ridurre ulteriormente il rischio. Se il rischio residuo è accettabile e basso, il management può decidere di accettarlo.

E' importante da considerare che gli **aggiornamenti software** sono fondamentali per garantire la sicurezza e il corretto funzionamento dei sistemi informatici. Ogni software, inclusi sistemi operativi, applicazioni e librerie, è soggetto a costanti miglioramenti e correzioni di bug da parte dei produttori. Questi aggiornamenti non solo introducono nuove funzionalità e miglioramenti delle prestazioni, ma soprattutto correggono vulnerabilità di sicurezza che potrebbero essere sfruttate dagli hacker per compromettere il sistema.

Nei grafici sottostanti forniti da Nessus è possibile verificare le differenze nel rischio e i miglioramenti relativi alla macchina target.



192.168.50.101

2	1	4	3	27
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 37

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	-	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
HIGH	8.6	-	136769	ISC BIND Service Downgrade / Reflected DoS
MEDIUM	6.5	-	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	5.9	-	136808	ISC BIND Denial of Service
MEDIUM	2.1*	-	10114	ICMP Timestamp Request Remote Date Disclosure
MEDIUM	4.3*	-	90317	SSH Weak Algorithms Supported
LOW	3.7	-	70658	SSH Server CBC Mode Ciphers Enabled
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	2.6*	-	71049	SSH Weak MAC Algorithms Enabled

Matteo Tedesco, Epicode school.

10/05/2024