

Progetto W5

Scansione vulnerabilità di Metasploitable con Nessus

Traccia

Effettuare una scansione completa sul target Metasploitable.

Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità critiche / high e provate ad implementare delle azioni di rimedio.

N.B. le azioni di rimedio, in questa fase, potrebbero anche essere delle regole firewall ben configurate in modo da limitare eventualmente le esposizioni dei servizi vulnerabili. Vi consigliamo tuttavia di utilizzare magari questo approccio per non più di una vulnerabilità.

Per dimostrare l'efficacia delle azioni di rimedio, eseguite nuovamente la scansione sul target e confrontate i risultati con quelli precedentemente ottenuti.

Dopo aver configurato Nessus, è stata avviata una scansione per individuare le vulnerabilità all'indirizzo di Metasploitable. Il risultato della scansione ha evidenziato numerose criticità, su cui è stato successivamente lavorato per cercare di risolverle.



Risultato scansione iniziale

FIELD

[Back to All Scans](#)

ConfigureAudit TrailLaunchReportExport

Hosts1Vulnerabilities65Remediations2Notes2History1

FilterSearch Vulnerabilities65 Vulnerabilities

<input type="checkbox"/> Sev	CVSS	VPR	Name	Family	Count		
<input type="checkbox"/> CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1	🔄	✎
<input type="checkbox"/> CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1	🔄	✎
<input type="checkbox"/> CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1	🔄	✎
<input type="checkbox"/> CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2	🔄	✎
<input type="checkbox"/> CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1	🔄	✎
<input type="checkbox"/> CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1	🔄	✎
<input type="checkbox"/> CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3	🔄	✎
<input type="checkbox"/> HIGH	7.5		NFS Shares World Readable	RPC	1	🔄	✎
<input type="checkbox"/> HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1	🔄	✎
<input type="checkbox"/> MIXED	SSL (Multiple Issues)	General	28	🔄	✎
<input type="checkbox"/> MIXED	ISC Bind (Multiple Issues)	DNS	5	🔄	✎

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 11:43 AM
End: Today at 12:11 PM
Elapsed: 28 minutes

Vulnerabilities

Critical

High

Medium

Low

Info

Bind Shell Backdoor Detection

Dopo aver ricevuto segnalazioni di una possibile presenza di backdoor sulla porta 1524, è stato necessario intervenire regolando le impostazioni del firewall. Le regole di default sono state configurate per la porta al fine di mitigare il rischio segnalato.

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
```

```
msfadmin@metasploitable:~$ ufw enable
ERROR: You need to be root to run this script
msfadmin@metasploitable:~$ sudo ufw enable
[sudo] password for msfadmin:
Firewall started and enabled on system startup
msfadmin@metasploitable:~$ ufw default allow
ERROR: You need to be root to run this script
msfadmin@metasploitable:~$ sudo ufw default allow
Default policy changed to 'allow'
(be sure to update your rules accordingly)
msfadmin@metasploitable:~$ sudo ufw deny 1524
Rule added
msfadmin@metasploitable:~$ sudo ufw status
Firewall loaded
```

To	Action	From
1524:tcp	DENY	Anywhere
1524:udp	DENY	Anywhere

```
msfadmin@metasploitable:~$ _
```

Una backdoor è un metodo nascosto per accedere in modo non autorizzato a un sistema informatico, consentendo a un attaccante di bypassare le normali procedure di autenticazione e ottenere un accesso segreto e non autorizzato.

VNC Server <password> Password

È stata rilevata una password troppo debole per il server VNC. È stato quindi necessario intervenire per inserire una password più sicura, utilizzando caratteri alfanumerici per garantire maggiore protezione.

```
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 su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# ls -la
.      .bash_history  .gconf        .mysql_history  .rhosts        .sudo_as_admin_successful
..     .distcc        .gconfd       .profile        .ssh           vulnerable
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:/home/msfadmin# _
```

Un server VNC è un software che consente agli utenti di controllare un computer remoto attraverso una connessione di rete. Utilizzando il protocollo VNC (Virtual Network Computing), gli utenti possono visualizzare e interagire con l'interfaccia grafica del computer remoto come se fossero fisicamente presenti di fronte ad esso.

NFS Exported Share Information Disclosure

È stata rilevata una vulnerabilità nell'accesso al NFS. È stato necessario intervenire modificando gli accessi consentiti solo alla macchina Linux, apportando modifiche al file exports per aumentare la sicurezza del sistema.

```
GNU nano 2.0.7      File: 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)
#
192.168.50.101(rw,sync,no_root_squash,no_subtree_check)

^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
CTRL (DESTRA)
```

NFS (Network File System) è un protocollo di rete che consente ai sistemi di memorizzazione di condividere file e risorse su una rete. Consente agli utenti di accedere e montare file e directory remote come se fossero locali sul proprio sistema.

Scansione dopo le modifiche

È evidente che i tre problemi critici individuati sono stati risolti durante l'ultima scansione delle vulnerabilità, migliorando così la sicurezza complessiva del sistema.

<input type="checkbox"/> Sev ▼	CVSS ▼	VPR ▼	Name ▲	Family ▲	Count ▼			Host Details
<input type="checkbox"/> CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1			<div>IP: 192.168.50.101</div> <div>MAC: 08:00:27:CA:E2:7F</div> <div>OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)</div> <div>Start: Today at 2:36 PM</div> <div>End: Today at 3:04 PM</div> <div>Elapsed: 28 minutes</div> <div>KB: Download</div> <div><h3>Vulnerabilities</h3><ul style="list-style-type: none">CriticalHighMediumLowInfo</div>
<input type="checkbox"/> CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2			
<input type="checkbox"/> CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1			
<input type="checkbox"/> CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3			
<input type="checkbox"/> HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1			
<input type="checkbox"/> MIXED	SSL (Multiple Issues)	General	28			
<input type="checkbox"/> MIXED	ISC Bind (Multiple Issues)	DNS	5			
<input type="checkbox"/> MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection	2			
<input type="checkbox"/> MEDIUM	5.9	3.6	SSL Anonymous Cipher Suites Supported	Service detection	1			
<input type="checkbox"/> MEDIUM	5.9	4.4	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1			
<input type="checkbox"/> MEDIUM	5.3	4.0	HTTP TRACE / TRACK Methods Allowed	Web Servers	1			
<input type="checkbox"/> MIXED	SSH (Multiple Issues)	Misc.	6			



Fine della presentazione

Amedeo Natalizi