

Consegna S5/L5

Scansione completa su Metasploitable

Introduzione

Scansionare con Nessus il target metasploitable, rilevare le criticità e implementare azioni di rimedio per quattro di esse.

Scansione iniziale

Adoperando Nessus abbiamo proceduto con una prima scansione del target Metasploitable, qui uno screen del report in allegato:

192.168.50.101



Vulnerabilities

Total: 104

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	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*	7.4	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	7.4	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	-	61708	VNC Server 'password' Password
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42256	NFS Shares World Readable
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	6.7	90509	Samba Badlock Vulnerability

Scansione delle porte e servizi in ascolto

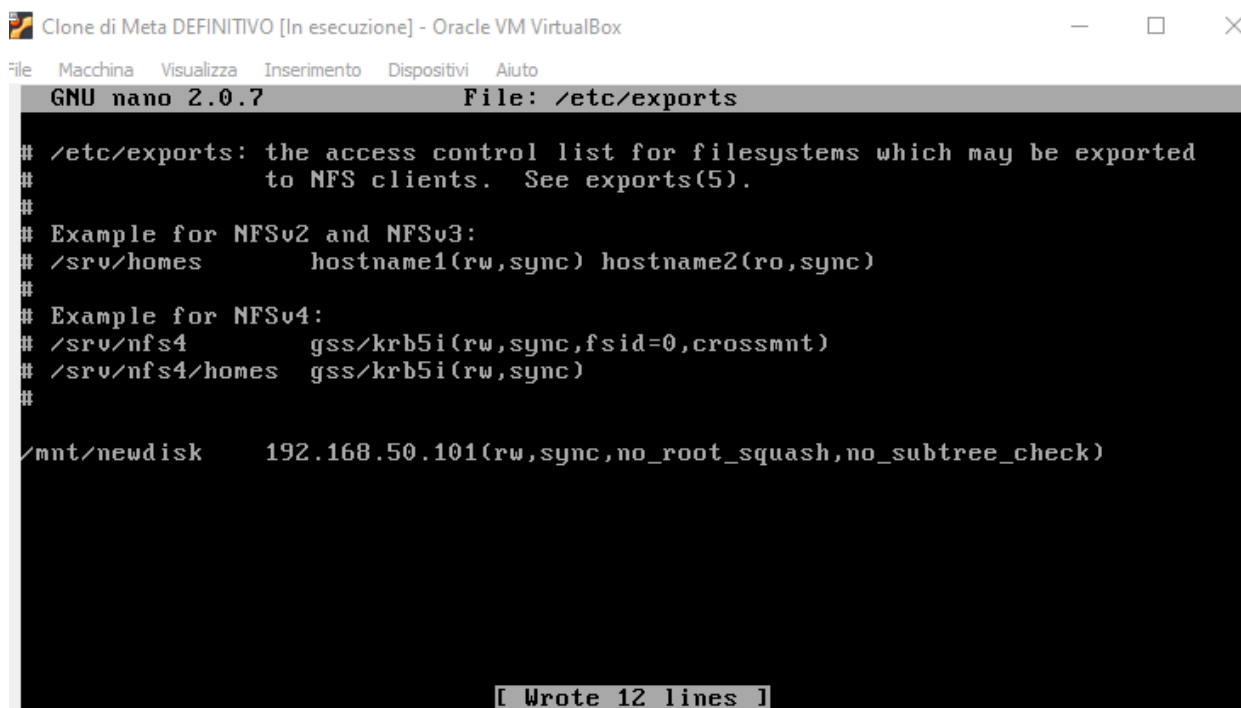
```
(kali@kali)-[~]
$ nmap -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-28 13:02 CET
Nmap scan report for 192.168.50.101
Host is up (0.00059s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE          VERSION
21/tcp    open  ftp              vsftpd 2.3.4
22/tcp    open  ssh              OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet?
25/tcp    open  smtp?
53/tcp    open  domain           ISC BIND 9.4.2
80/tcp    open  http             Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind          2 (RPC #100000)
139/tcp   open  netbios-ssn      Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn      Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec?
513/tcp   open  login?
514/tcp   open  shell?
1099/tcp  open  java-rmi         GNU Classpath grmiregistry
1524/tcp  open  bindshell        Metasploitable root shell
2049/tcp  open  nfs              2-4 (RPC #100003)
2121/tcp  open  ccproxy-ftp?
3306/tcp  open  mysql?
5432/tcp  open  postgresql       PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc              VNC (protocol 3.3)
6000/tcp  open  X11              (access denied)
6667/tcp  open  irc              UnrealIRCd
8009/tcp  open  ajp13            Apache Jserv (Protocol v1.3)
8180/tcp  open  http             Apache Tomcat/Coyote JSP engine 1.1
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 193.11 seconds
```

Criticità n1: NFS Exported Shared Information Disclosure

La vulnerabilità presa in esame su Metasploitable si riferisce a una possibile esposizione non autorizzata di informazioni sensibili tramite condivisioni NFS (Network File System).

Per ovviare a ciò entriamo nel file di testo che regola questo servizio e inseriamo la possibilità di poter comunicare solo con se stesso, in questo modo:



```
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)
#
/mnt/newdisk 192.168.50.101(rw,sync,no_root_squash,no_subtree_check)

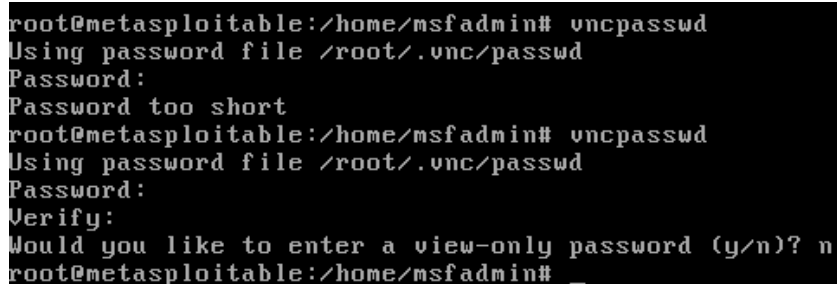
[ Wrote 12 lines ]
```

Criticità n2: VNC Server 'password' Password

Un server VNC (Virtuale Network Computing) è un servizio che permette la visualizzazione e il controllo grafico remoto del desktop del sistema. VNC consente agli utenti di connettersi al server VNC da un'altra macchina e interagire con l'ambiente desktop in modo simile a come farebbero localmente.

Su Metasploitable il server VNC potrebbe essere configurato per fornire un'interfaccia grafica remota su una determinata porta, per questo motivo la password non può essere 'password', che è troppo debole e facilmente indovinabile.

Per questo motivo la cambiamo:



```
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password:
Password too short
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# _
```

Criticità n3: Bind Shell Backdoor Detection

La vulnerabilità “Bind Shell Backdoor Detection” si riferisce alla presenza di una backdoor legata ad una bind shell legata ad un sistema che potrebbe essere utilizzata da un attaccante per ottenere un accesso non autorizzato.

Dalla scansione effettuata ad inizio lavoro abbiamo visto che la porta interessata è la 1524, quindi procediamo ad abilitare il firewall e a chiuderla. Controlliamo poi che sia effettivamente chiusa:

```
msfadmin@metasploitable:~$ sudo su
root@metasploitable:/home/msfadmin# ufw enable
Firewall started and enabled on system startup
root@metasploitable:/home/msfadmin# ufw default allow
Default policy changed to 'allow'
(be sure to update your rules accordingly)
root@metasploitable:/home/msfadmin# ufw deny 1524
Rule added
root@metasploitable:/home/msfadmin# ufw status
Firewall loaded
```

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

Criticità n4: Samba Badlock Vulnerability

La “Samba Badlock” si riferisce a una serie di vulnerabilità di sicurezza scoperte nel protocollo di condivisione di file Samba. Samba è un software open-source che implementa il protocollo SMB/CIFS, consentendo la condivisione di file e la comunicazione tra sistemi Windows e UNIX/Linux.

Un attaccante potrebbe sfruttare questa vulnerabilità per ottenere informazioni riservate, eseguire attacchi di tipo “Man-in-the-Middle” o modificare i dati nel traffico di rete Samba.

Come prima abbiamo optato per la soluzione più drastica con la chiusura delle porta in ascolto per quel servizio (la 139 e la 445):

```

root@metasploitable:/home/msfadmin# ufw deny 139
Rule added
root@metasploitable:/home/msfadmin# ufw deny 445
Rule added
root@metasploitable:/home/msfadmin# ufw status
Firewall loaded

```

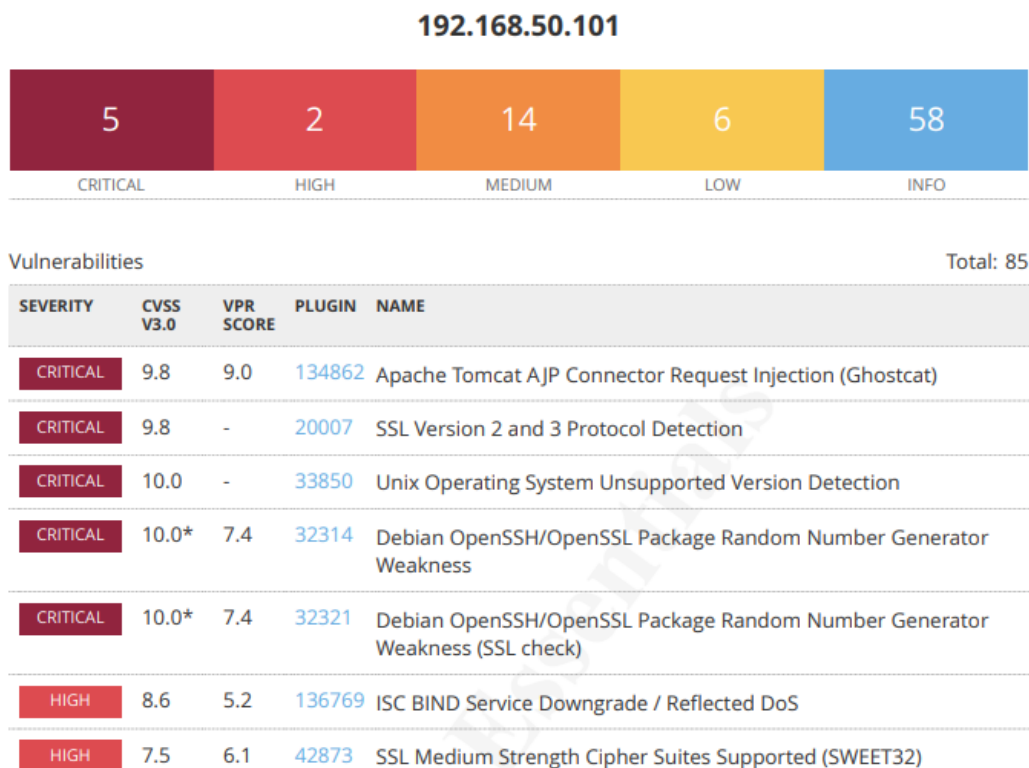
```

To Action From
--
1524:tcp DENY Anywhere
1524:udp DENY Anywhere
139:tcp DENY Anywhere
139:udp DENY Anywhere
445:tcp DENY Anywhere
445:udp DENY Anywhere

```

Scansione finale

Effettuiamo una nuova scansione per accertarci che le nostre azioni di rimedio abbiamo risolto i problemi:



Come possiamo notare le azioni di rimedio hanno avuto effetto.