

Fix di vulnerabilità

Criticità trovate sulla macchina Metasploitable relative alla famiglia "Service Detection"

<input type="checkbox"/>	HIGH	7.5 *	5.9	rlogin Service Det...	Service detection	1		
<input type="checkbox"/>	HIGH	7.5 *	5.9	rsh Service Detec...	Service detection	1		

Queste vulnerabilità permettono ad un attaccante di eseguire controlli da remoto, pertanto sono considerate di livello alto.

Possono essere risolte semplicemente andando a modificare il file di configurazione relativo al servizio inetd (nelle versioni aggiornate di Linux è il processo è chiamato xinetd) e commentando le righe relative al login e all'exec come nello screen:

```
#<off># netbios-ssn      stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sb$
telnet                stream  tcp      nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.te$
#<off># ftp             stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sb$
tftp                  dgram   udp      wait    nobody   /usr/sbin/tcpd  /usr/sbin/in.tf$
#shell                stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rs$
#login                stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rl$
#exec                 stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.re$
xinetd                 stream  tcp      nowait  root    /bin/bash  bash -i
```

Criticità trovata sulla macchina Metasploitable relativa alla famiglia delle “Backdoors”



Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione.

Un utente malintenzionato può utilizzarlo collegandosi alla porta remota e inviando direttamente comandi (Vulnerabilità di livello massimo).

Una possibile soluzione è stata filtrare la porta tramite firewall (in questo caso il fw di Metasploitable iptables):

```
root@metasploitable:~/home/msfadmin# sudo iptables -A INPUT -p tcp --dport 1524 -j DROP
```

È possibile proteggere la porta remota usando altri firewall esterni alla macchina Metasploitable (ad esempio PfSense montato su un'altra macchina).

A seguito di uno scan delle porte, la porta relativa alla criticità (1524) risulta dunque “filtered” e non più “open”

```
Host is up (0.00033s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE      SERVICE
21/tcp    open       ftp
22/tcp    open       ssh
23/tcp    open       telnet
25/tcp    open       smtp
53/tcp    open       domain
80/tcp    open       http
111/tcp   open       rpcbind
139/tcp   open       netbios-ssn
445/tcp   open       microsoft-ds
512/tcp   open       exec
513/tcp   open       login
514/tcp   open       shell
1099/tcp  open       rmiregistry
1524/tcp  filtered  ingreslock
2049/tcp  open       nfs
2121/tcp  open       ccproxy-ftp
3306/tcp  open       mysql
5432/tcp  open       postgresql
5900/tcp  open       vnc
6000/tcp  open       X11
6667/tcp  open       irc
8009/tcp  open       ajp13
8180/tcp  open       unknown
MAC Address: 08:00:27:CA:2B:54 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.40 seconds
```

Criticità trovata sulla macchina Metasploitable relativa al server VNC:



Il server VNC in esecuzione sull'host remoto è protetto con una password debole.

Nessus è riuscito ad accedere utilizzando l'autenticazione VNC e la password "password".

Un attaccante remoto e non autenticato potrebbe sfruttare questa vulnerabilità di livello critico per assumere il controllo del sistema.

Per risolvere questa falla è stato sufficiente modificare la password del server VNC con una più complessa:

```
root@metasploitable:/home/msfadmin# sudo vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
root@metasploitable:/home/msfadmin# _
```

A terminal window with a black background and white text. The prompt is 'root@metasploitable:/home/msfadmin#'. The user enters 'sudo vncpasswd'. The output shows the password file path, prompts for a new password and its verification, a prompt for a view-only password which is answered 'y', and another password prompt and verification. The prompt returns to 'root@metasploitable:/home/msfadmin#'. At the bottom of the terminal, there is a taskbar with various icons and the text 'CTRL (DESTRA)'.

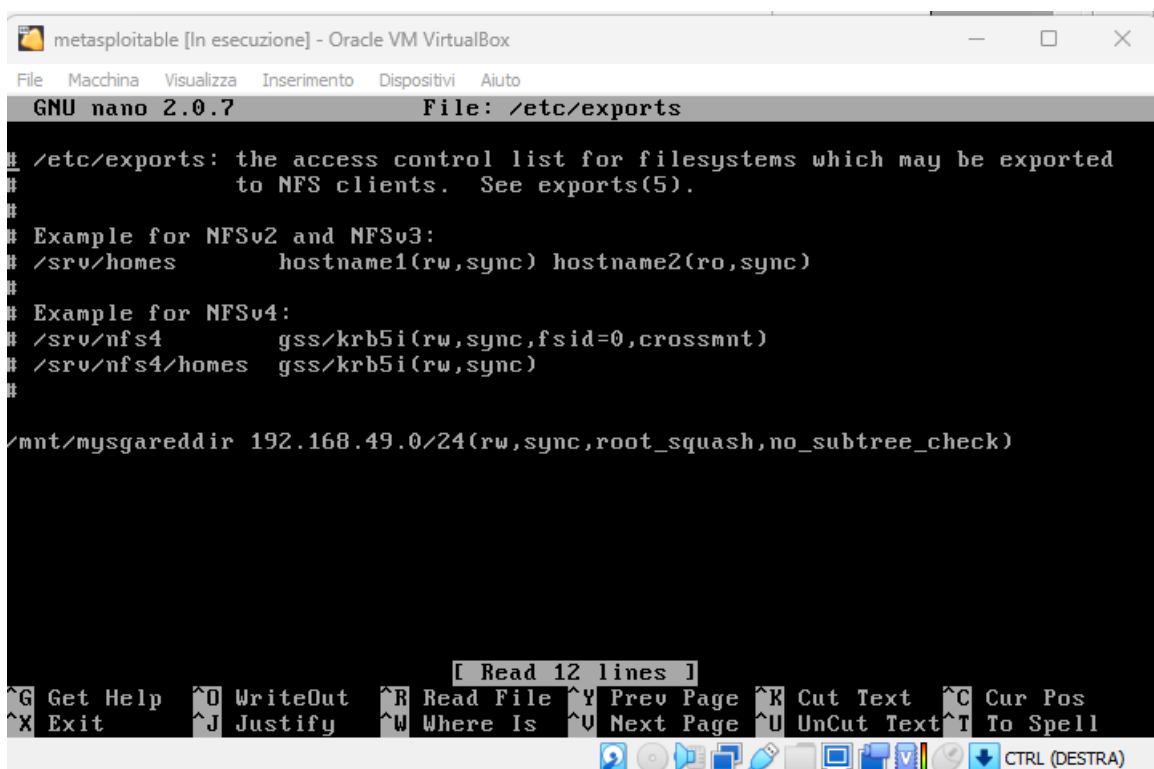
Criticità trovata sulla macchina Metasploitable relativa alle cartelle condivise:



Almeno una delle cartelle NFS esportate dal server remoto potrebbe essere montata dall'host di scansione.

Un attaccante potrebbe essere in grado di sfruttare questo per leggere (ed eventualmente scrivere) file sull'host remoto.

In questo caso si è risolta la vulnerabilità di livello critico configurando NFS sull'host remoto (/etc/exports) in modo tale che solo gli host autorizzati possano montare le sue condivisioni remote (nello specifico è stato ristretto l'accesso solo agli utenti del nostro network).



```
metasploitable [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
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/mysgareddir 192.168.49.0/24(rw,sync,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
CTRL (DESTRA)
```

In seguito all'applicazione dei fix sopracitati, ripetendo uno scan approfondito con Nessus, le 5 criticità risultano tutte risolte con successo:

Sev	CVSS	VPR	Name	Family	Count	
<input type="checkbox"/> CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1	
<input type="checkbox"/> MEDIUM	Apache Tomcat (Multiple Issues)	Web Servers	4	
<input type="checkbox"/> MEDIUM	Phpmyadmin (Multiple Issues)	CGI abuses	4	
<input type="checkbox"/> CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3	
<input type="checkbox"/> MEDIUM	PHP (Multiple Issues)	CGI abuses	3	
<input type="checkbox"/> HIGH	8.3		CGI Generic SQL Injection (blind)	CGI abuses	1	
<input type="checkbox"/> HIGH	7.5 *		CGI Generic Command Execution	CGI abuses	1	
<input type="checkbox"/> HIGH	7.5 *		CGI Generic Remote File Inclusion	CGI abuses	1	
<input type="checkbox"/> HIGH	7.5	5.9	Samba Badlock Vulnerability	General	1	
<input type="checkbox"/> MEDIUM	ISC Bind (Multiple Issues)	DNS	5	
<input type="checkbox"/> MEDIUM	Twiki (Multiple Issues)	CGI abuses	2	
<input type="checkbox"/> MEDIUM	6.8 *		CGI Generic Local File Inclusion (2nd pass)	CGI abuses	1	