

Scansione e risoluzione criticità

Utilizzando Nessus individuare criticità e risolverle.

Prima criticità: Credenziali deboli

CRITICAL VNC Server 'password' Password

Description
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.

Solution
Secure the VNC service with a strong password.

```
root@metasploitable:/etc#  
root@metasploitable:/etc# cd /  
root@metasploitable:/# ls  
bin      dev      initrd   lib      mnt      proc     sbin     tmp      vmlinuz  
boot     etc      initrd.img lost+found nohup.out ^R       srv      usr  
cdrom    home    %J@FC   media    opt       root     sys      var  
root@metasploitable:/# cd root  
root@metasploitable:~# ls  
Desktop  reset_logs.sh vnc.log  
root@metasploitable:~# ls -a  
.          .config      .gconf       .profile     .ssh  
..         Desktop      .gconfd      .purple     .vnc  
.bash_history .filezilla   .gstreamer-0.10 reset_logs.sh vnc.log  
.bashrc     .fluxbox     .mozilla     .rhosts     .Xauthority  
root@metasploitable:~# cd .vnc  
root@metasploitable:~/vnc# ls  
metasploitable:0.log  metasploitable:1.log  passwd  
metasploitable:0.pid  metasploitable:2.log  xstartup  
root@metasploitable:~/vnc# _
```

Nessus in questo caso è stato in grado di rilevare che la nostra password è debole, riuscendo a decifrarla. Per ovviare a questa vulnerabilità ci basterà andare a modificare la password, utilizzandone una più robusta. Questo primo passo ci aiuterà a rendere la nostra macchina più sicura.

Per andare a modificare la password, tramite terminale di meta, dobbiamo andare a modificare il documento nella quale sono descritte le credenziali di accesso.

Il percorso che dobbiamo fare è partire dal root, muoverci nella cartella root, poi digitiamo il comando “*ls -a*” per visualizzare i file e le directory nascoste, poi a questo punto andiamo su *.vnc*, e all’interno della directory avviamo il comando “*vncpasswd*”, il terminale ci chiederà di inserire le nuove credenziali e di verificarne la correttezza, una volta fatto ciò, confermiamo e la nostra password sarà modificata.

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

Seconda Criticità: Backdoors

CRITICAL UnrealIRCd Backdoor Detection < >

Description
The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.

1524 / tcp / wild_shell

CRITICAL Bind Shell Backdoor Detection < >

Description
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.

6667 / tcp / irc

La seconda criticità che rileviamo è la presenza di due backdoor differenti, aperte e accessibili a tutti. Una backdoor come sappiamo è una porta di accesso, che non richiede autorizzazioni, bypassando il sistema di autenticazione. Nessus ci informa anche del numero della porta aperta, sulle quali andremo a lavorare, per rendere più sicuro il nostro ambiente di rete.

Per regolamentare l'accesso alle nostre porte, ci sono almeno due soluzioni: chiuderla, o applicare delle regole specifiche sul firewall.

Chiusura delle porte

```
msfadmin@metasploitable:/$ sudo netstat -tulnp | grep 1524
[sudo] password for msfadmin:
tcp        0      0 0.0.0.0:1524        0.0.0.0:*          LISTEN
4415/xinetd
msfadmin@metasploitable:/$ sudo kill 4415
msfadmin@metasploitable:/$ _
```

```
root@metasploitable:/# netstat -tulnp | grep 6667
tcp        0      0 0.0.0.0:6667        0.0.0.0:*          LISTEN
4792/unrealircd
root@metasploitable:/# sudo kill 4792
root@metasploitable:/# _
```

Per chiudere le porte apriamo il terminale di meta e andiamo a digitare:

*“sudo netstat -tulnp | grep *numero_porta*”*

Questo comando viene utilizzato per visualizzare le informazioni sulle connessioni di rete e i servizi in ascolto sulla porta selezionata. L'output sarà una lista di informazioni sulle connessioni di rete e i servizi in ascolto sulla porta 1524 o 6667, se ce ne sono. In questo caso vediamo che ci sono dei servizi attivi sulle porte. Con il comando successivo, andiamo a interrompere i servizi attivi su quelle porte, chiudendo appunto le porte stesse. In basso vediamo la scansione effettuata con nmap, che ci mostra lo stato delle porte.

```
(fox@kali)-[~/Desktop]
$ nmap -sV 192.168.1.16 -p 1524
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-27 13:43 BST
Nmap scan report for kali.station (192.168.1.16)
Host is up (0.00052s latency).

PORT      STATE SERVICE VERSION
1524/tcp  closed ingreslock

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

```
(fox@kali)-[~/Desktop]
$ nmap -sV 192.168.1.16 -p 6667
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-27 13:48 BST
Nmap scan report for kali.station (192.168.1.16)
Host is up (0.0011s latency).

PORT      STATE SERVICE VERSION
6667/tcp  closed irc

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds

(fox@kali)-[~/Desktop]
$
```


Configurazione del servizio NFS

CRITICAL NFS Exported Share Information Disclosure

Description
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.

Solution
Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

L'errore "NFS Exported share information disclosure" in Nessus indica che il tool di scansione ha rilevato un problema o una potenziale vulnerabilità relativa alle condivisioni NFS (Network File System) su un sistema. NFS è un protocollo utilizzato per condividere file e risorse su una rete, e la scansione potrebbe aver rilevato problemi legati a come le condivisioni NFS sono configurate o protette. Quindi sta a noi andare a modificare i file di configurazione per stabilirne i parametri.

Per andare a modificare le configurazioni andiamo a modificare il file "export" che si trova all'interno della cartella "/etc" in questo caso apriamo l'editor di testo e andiamo a modificare il parametro che regola l'accessibilità agli host. In altre parole, prima era una condivisione pubblica aperta a tutti gli host nella rete, ma una volta modificata come nella figura sotto, solamente l'IP selezionato avrà l'accesso al servizio.

```
# /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)
#
#                192.168.1.3(rw,sync,no_root_squash,no_subtree_check)
# /nfs/share 192.168.1.26(rw)
```

Come possiamo evincere da questi screen, e con i report in allegato, siamo riusciti a ridurre il numero di criticità.

Vulnerabilities69

Filter

Search Vulnerabilities

69 Vulnerabilities

<input type="checkbox"/> Sev	CVSS	VPR	Name	Family	Count	
<input type="checkbox"/> CRITICAL	10.0 *	5.9	NFS Exported Sha	Plugin ID: 33850	1	
<input type="checkbox"/> CRITICAL	10.0		Unix Operating Sy...	General	1	
<input type="checkbox"/> CRITICAL	10.0 *		VNC Server 'passw...	Gain a shell remotely	1	
<input type="checkbox"/> CRITICAL	9.8		Bind Shell Backdo...	Backdoors	1	

Vulnerabilities57

Filter

Search Vulnerabilities

57 Vulnerabilities

<input type="checkbox"/> Sev	CVSS	VPR	Name	Family	Count	
<input type="checkbox"/> CRITICAL	10.0		Unix Operating Sy...	General	1	
<input type="checkbox"/> CRITICAL	9.8	9.0	Apache Tomcat AJ...	Web Servers	1	
<input type="checkbox"/> CRITICAL	SSL (Multiple ...	Gain a shell remotely	3	

Fin.

Vincenzo Colletta 27/10/2023