

Settimana 5 - Esercizio 5

Alessio Golfetto 12/01/2023

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.

Vulnerabilità 1

VNC Server “password” Password

Un server VNC (Virtual Network Computing) è un software che consente la condivisione del desktop di un computer o di un server tramite la rete. VNC è un protocollo che permette a un utente di controllare un sistema remotamente visualizzando il desktop e interagendo con esso attraverso un altro host.

Questa vulnerabilità rilevata tramite Nessus ci informa che la password utilizzata a protezione del server VCN è “password”. Trattandosi di una password molto facile da individuare espone il server ad un altissimo rischio di un eventuale attacco da parte di terzi non autorizzati.

Filter ▼ password ✕ 1 of 79 Vulnerabilities

☐ Sev ▼

CVSS ▼

VPR ▼

Na... Family ▲

Count ▼

☐

CRITICAL

10.0 *

VNC Gain a shell remotely

Results per page 50 ▼ << < Showing: 1 to 1 of 1 > >>

Scan Details

Policy:

Basic Network Scan

Status:

Completed

Severity Base:

CVSS v3.0

Scanner:

Local Scanner

Start:

January 11 at 12:14 PM

End:

January 11 at 12:22 PM

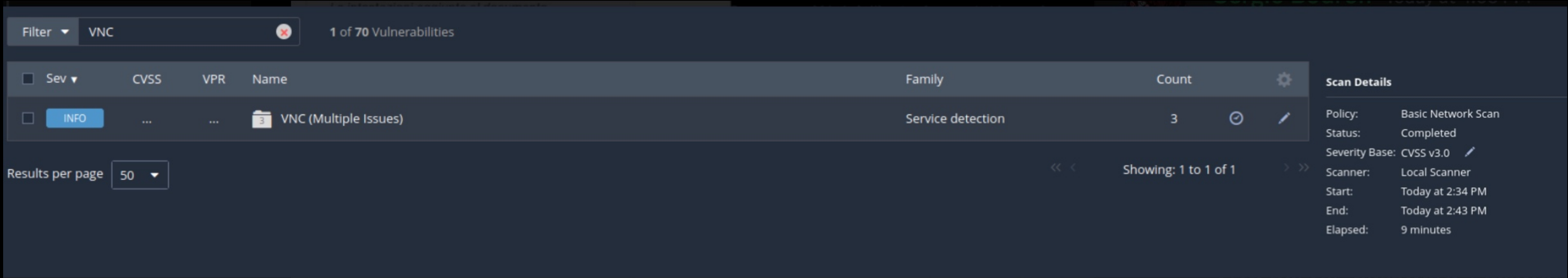
Elapsed:

9 minutes

Risoluzione problematica 1

Utilizzando su Metasploitable il comando ***vncpasswd*** sono andato a sostituire la vecchia password vulnerabile con una nuova alfanumerica più sicura. Ora risulterà più complicato per un eventuale hacker individuare la password per entrare nel server VNC.

```
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#
```



Vulnerabilità 2

NFS Exported share information disclosure

Network file system (NFS) è un protocollo utilizzato solitamente per condividere file o directory da un sistema Unix/Linux su una rete.

La vulnerabilità NFS Exported share information disclosure si ha quando le informazioni sulle condivisioni effettuate possono essere intercettate da host non autorizzati, i quali potrebbero potenzialmente leggere o anche scrivere file sul server remoto.

Filter

3 of 79 Vulnerabilities

<input type="checkbox"/>	Sev ▼	CVSS ▼	VPR ▼	Na... Far	Plugin ID: 11356	Count ▼	⚙
<input type="checkbox"/>	CRITICAL	10.0 *	5.9	NFS IRPC		1	🕒 ✎
<input type="checkbox"/>	HIGH	7.5		NFS IRPC		1	🕒 ✎
<input type="checkbox"/>	INFO			NFS IRPC		1	🕒 ✎

Results per page

<< < Showing: 1 to 3 of 3 > >>

Scan Details

Policy: Basic Network Scan

Status: Completed

Severity Base: CVSS v3.0 ✎

Scanner: Local Scanner

Start: January 11 at 12:14 PM

End: January 11 at 12:22 PM

Elapsed: 9 minutes

Risoluzione vulnerabilità 2

Da Metasploitable ho inserito il comando ***sudo nano etc/exports*** e sono andato ad eliminare l'ultima riga che autorizzava chiunque ad avere accesso al server. Con l'operazione svolta nessuno altro host , me escluso, avrà accesso al server.

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
Sorry, try again.
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# sudo nano 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)
```



Vulnerabilities80

Filternfs1 of 80 Vulnerabilities

Sev

CVSS

VPR

Na... Family

Count

INFO

NFS :RPC

1

results per page50Showing: 1 to 1 of 1

Host Details

IP:192.168.64.8

MAC:1A:44:A4:FE:11:BB

OS:Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Start:Today at 1:35 PM

End:Today at 1:43 PM

Elapsed:8 minutes

KB:Download

Vulnerabilities

Vulnerabilità 3

Bind shell backdoor detection

Una backdoor è un tipo di accesso segreto o nascosto a un sistema informatico. Questo accesso consente a un hacker di controllare il sistema senza essere rilevato e senza autorizzazione del proprietario. La backdoor può essere utilizzata per eseguire comandi, raccogliere informazioni, modificare configurazioni o svolgere altre attività malevole.

Con una backdoor spesso si intende la creazione di un punto di accesso segreto che bypassa le normali procedure di autenticazione. Può essere incorporata nel codice di un'applicazione, nascosta in un file eseguibile o implementata come un servizio di sistema.

Filter

Search Vulnerabilities

62 Vulnerabilities

<input type="checkbox"/> Sev	CVSS	VPR	Name	Family	Count	
<input type="checkbox"/> CRITICAL	10.0		Unix Operating System Unsupp...	General	1	
<input type="checkbox"/> CRITICAL	9.8		SSL Version 2 and 3 Protocol De...	Service detection	2	
<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	9.8		Apache Tomcat AJP Connector ...	Web Servers	1	

Scan Details

Policy:

Basic Network Scan

Status:

Completed

Severity Base:

CVSS v3.0

Scanner:

Local Scanner

Start:

Today at 1:33 PM

End:

Today at 2:01 PM

Elapsed:

28 minutes

Vulnerabilities

Risoluzione vulnerabilità 3

Grazie al software Nessus ero a conoscenza che la backdoor si trovasse sulla porta 1524 del nostro sistema.

Utilizzando su Metasploitable il comando ***Isotf -i :1524*** sono riuscito a risalire al pid del processo in corso su quella porta (nel mio caso 4437). Successivamente con il comando ***kill 4437*** sono andato a chiudere la porta sulla quale era stata rilevata la backdoor. Come ulteriore conferma ho eseguito anche uno scan sull’ip di meta con Nmap per verificare che la porta fosse realmente chiusa.

```

$ nmap -sV 192.168.64.8
Starting Nmap 7.92 ( https://nmap.org ) at 2024-01-12 14:30 CET
Nmap scan report for 192.168.64.8
Host is up (0.0030s latency).
Not shown: 983 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
22/tcp    open  ssh            OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
25/tcp    open  smtp           Postfix smtpd
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)
1099/tcp  open  java-rmi       GNU Classpath grmiregistry
2049/tcp  open  nfs            2-4 (RPC #100003)
2121/tcp  open  ftp            ProFTPD 1.3.1
3306/tcp  open  mysql          MySQL 5.0.51a-3ubuntu5
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: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Linux, Unix; CPE: cpe:/o:li
nux: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 11.80 seconds
```

Filter

bind backdoor

0 of 73 Vulnerabilities

☐

Sev

CVSS

VPR

Na... Family

Count

No records found.

Results per page

50

<< <

Showing 0 to 0 of 0 entries

> >>

Scan Details

Policy:

Basic Network Scan

Status:

Completed

Severity Base:

CVSS v3.0

Scanner:

Local Scanner

Start:

Today at 2:34 PM

End:

Today at 2:43 PM

Elapsed:

9 minutes

Fine