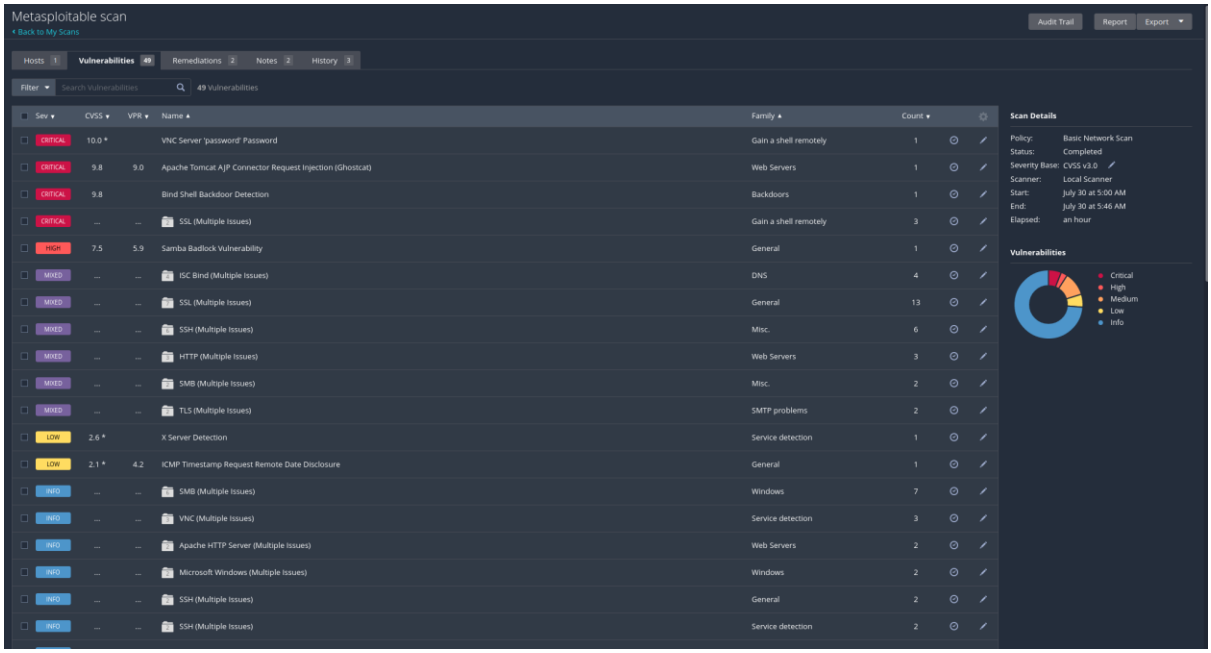
Isabelle Adjetey

Remediation



Vulnerabilità 1

61708 - VNC Server 'password' Password

Synopsis

A VNC server running on the remote host is secured with a weak 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.

Risk Factor

Critical

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Plugin Information

Published: 2012/08/29, Modified: 2015/09/24

Plugin Output

tcp/5900/vnc

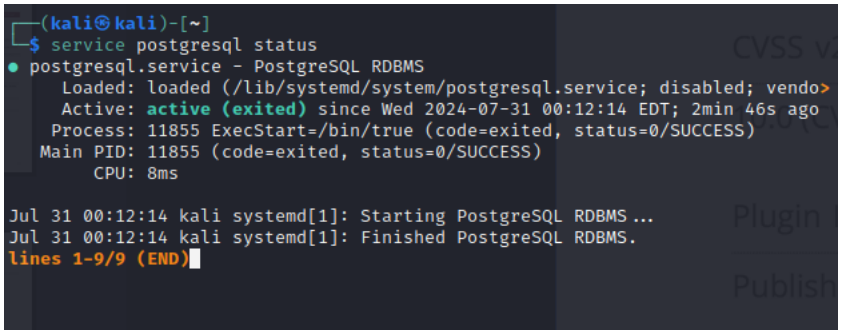
```
Nessus logged in using a password of "password".
```

Si tratta di password non adeguata per il server VNC(Virtual network computing), unservizio che consente l'accesso e il controllo remoto di un computer. Servirà semplicemente configurare una password più efficace.

Utilizziamo il comando vncpasswd sotto le vesti root.

```
root@metasploitable:/home/msfadmin# 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# exit
exit
```

Una volta fatto, testiamo che la vulnerabilità sia stata corretta. Kali linux ha già installato nel Metaploit Framework, msfconsole.



Prima di accedere alla tipologia di exploit che ci interessa, attiviamo il database postgresql.

Da msfconsole msfconsole, cerchiamo il modulo vnc_client.

Confermiamo lanostra scelta con use auxiliary/scanner/vnc/vnc_login. Inseriamo le indicazioni per l'attacco: L'indirizzo da attaccare e la metodologia STOP_ON_SUCCESS = true.

Passiamo da vncviewer e cerchiamo di visualizzare il desktop di un computer remoto. In questo caso, la password 'password' non ha effetto.

Vulnerabilità 2

51988 - Bind Shell Backdoor Detection

Synopsis

The remote host may have been compromised.

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.

Solution

Verify if the remote host has been compromised, and reinstall the system if necessary.

Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Plugin Information

Published: 2011/02/15, Modified: 2022/04/11

Plugin Output

tcp/1524/wild_shell

All'interno de metasploitable sembra esserci una shell che apre una porta vulnerabile verso l'esterno. In base a ciò che ci ha detto Nessus, sappiamo che questo servizio è aperto sulla porta tcp 1524. Rintracciamo il file con fuser.

Il PID del prpcesso è 4502. Con sudo readlink abbiamo il percorso al programma stesso.

Lo eliminiamo

```
msfadmin@metasploitable:~$ sudo readlink -f /proc/4502/exe
/usr/sbin/xinetd
msfadmin@metasploitable:~$ cd usr/sbin
-bash: cd: usr/sbin: No such file or directory
msfadmin@metasploitable:~$ cd /usr/sbin
msfadmin@metasploitable:/usr/sbin$ file xinetd
xinetd: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), for GNU/Linux
2.6.8, dynamically linked (uses shared libs), stripped
msfadmin@metasploitable:/usr/sbin$ sudo rm xinetd
msfadmin@metasploitable:/usr/sbin$
```

Riavviamo Metaploitable e controlliamo se la porta tcp 1524 è ancora in funzione. Dalla scansione nmap stealth vediamo che la backdoor non viene visualizzata.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.50.101
Starting Nmap 7.92 ( https://nmap.org ) at 2024-07-31 01:15 EDT
Nmap scan report for 192.168.50.101
Host is up (0.034s latency).
Not shown: 983 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
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
1099/tcp open  rmiregistry
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: 08:00:27:32:AC:1B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 15.25 seconds

┌──(kali㉿kali)-[~]
└─$
```

Grafico Scanzione finale