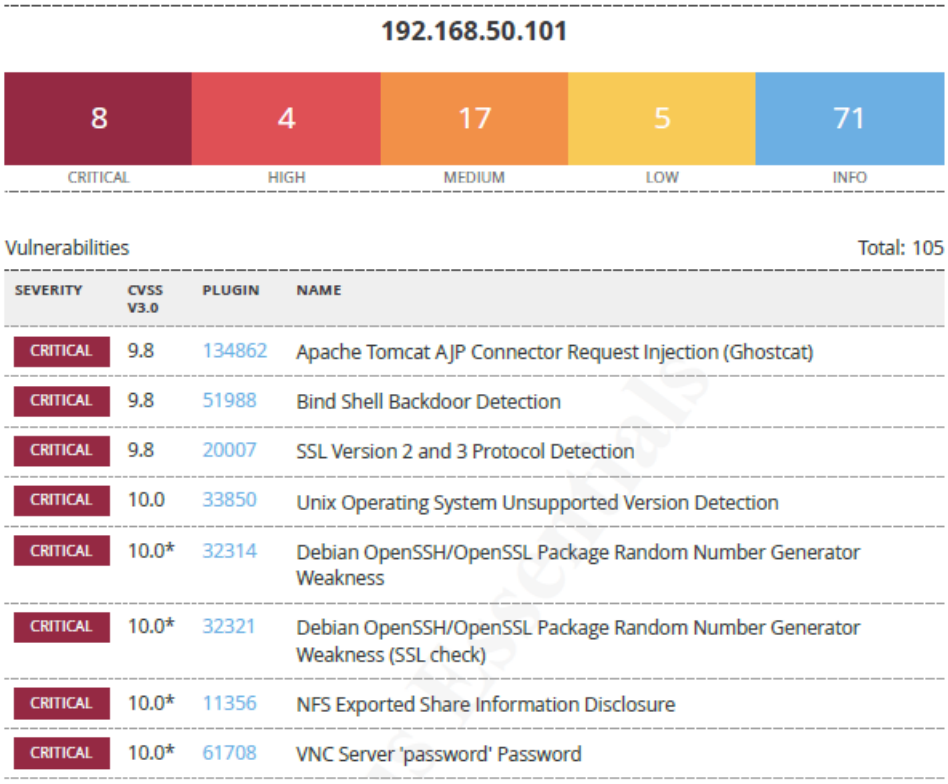
metas

Report generated by Nessus™ Thu, 24 Nov 2022 13:19:11 EST

Vulnerabilities by Host

- 192.168.50.101.....4



192.168.50.101

CRITICAL	HIGH	MEDIUM	LOW	INFO
8	4	17	5	71

Vulnerabilities — Total: 105

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	9.8	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*	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	61708	VNC Server 'password' Password

Tramite Nessus sono state rilevate le seguenti minacce, in questo caso ne sono state prese in esame tre con fattore di rischio critico ed in seguito sono stati attuati dei rimedi ad esse.

Le vulnerabilità sono le seguenti:

51988 - Bind Shell Backdoor Detection

Sinossi

L'host remoto potrebbe essere stato compromesso.

Descrizione

Shell in ascolto sulla porta remota senza che nessuna autenticazione sia richiesta. Un utente malintenzionato potrebbe usarla collegandosi alla porta remota e inviando comandi diretti.

FATTORE DI RISCHIO: CRITICO

Soluzione

Verificare eventuali compromissioni dell'host remote e reinstallare il sistema se necessario.

Informazioni Plugin

Effettuato: 2011/02/15, Modificato: 2022/04/11

Plugin Output

tcp/1524/wild_shell

```
Nessus ha potuto eseguire il comando "id" usando la seguente richiesta :
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root) root@metasploitable


) :
 snip root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root) root@metasploitable:/#
— — — — — — — — — — — —         — — — — — — — — — — — —
 snip


— — — — — — — — — — — —         — — — — — — — — — — — —
```

11356 - NFS Exported Share Information Disclosure

Sinossi

Possibile accedere alle condivisioni NFS sull’host remote.

Descrizione

Almeno una delle condivisioni NFS esportate dal server remote potrebbe essere montata dall’host di scansione. Un utente malintenzionato potrebbe sfruttare questa falla per leggere (e possibilmente scrivere) file su host remoto.

Soluzione

Configurare NFS sull’host remote in modo che solo host autorizzati possano modificare le condivisioni remote.

Fattore di rischio : Critico

Informazioni Plugin

Eseguito: 2003/03/12, Modificato: 2018/09/17

Plugin Output

udp/2049/rpc-nfs

```
The following NFS shares could be mounted :

+ /
  + Contents of / :
    - dev
    - etc
    - home
    - initrd
    - initrd.img
    - lib
    - lost+found
    - media
    - mnt
    - nohup.out
    - opt
    - proc
    - root
    - sbin
    - srv
    - sys
    - tmp
    - usr
    - var
    - vmlinuz
```

61708 - VNC Server 'password' Password

Sinossi

Un server VNC server attivo sull'host remoto utilizza una password debole.

Descrizione

Un server VNC attivo sull'host remoto utilizza una password debole. Nessus è stato in grado di fare log in usando come autenticazione VNC la password "password". Un utente malintenzionato e non autorizzato potrebbe usare questa falla per prendere controllo del sistema.

Soluzione

Assicurare il servizio VNC con una password meno identificabile.

Rischio

Critico

CVSS v2.0 Base Score

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

Informazioni Plugin

Effettuato: 2012/08/29, Modificato: 2015/09/24

Plugin Output

```
Nessus può loggarsi usando come password  "password".
```

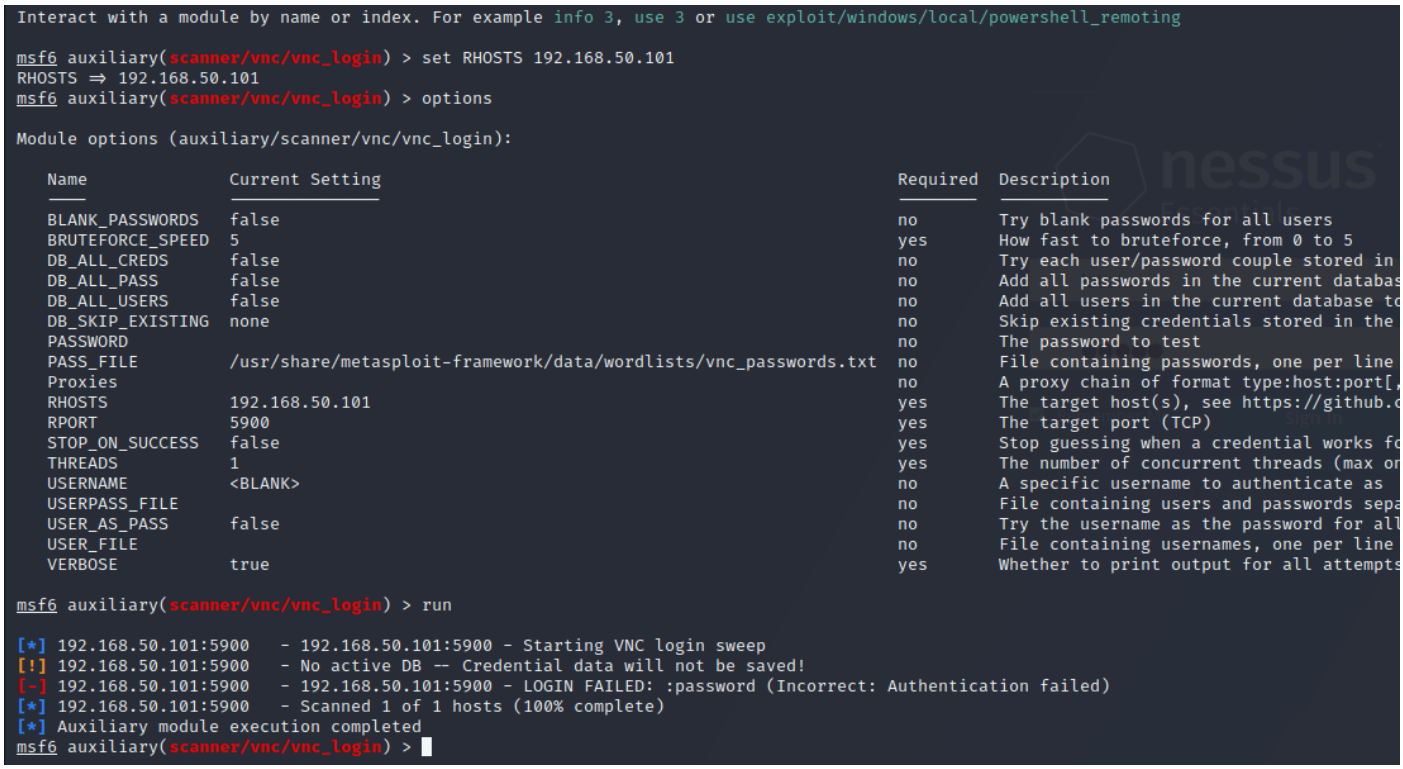
tcp/5009/vnc

Dopo averle attentamente analizzate è stato possibile effettuare delle remediation action per risolverle:

61708 - VNC Server 'password' Password

Per risolvere questa criticità tramite directory VNC, sarà sufficiente cambiare la password (vncpasswd) in una più sicura per evitare accessi da parte di utenti non autorizzati.

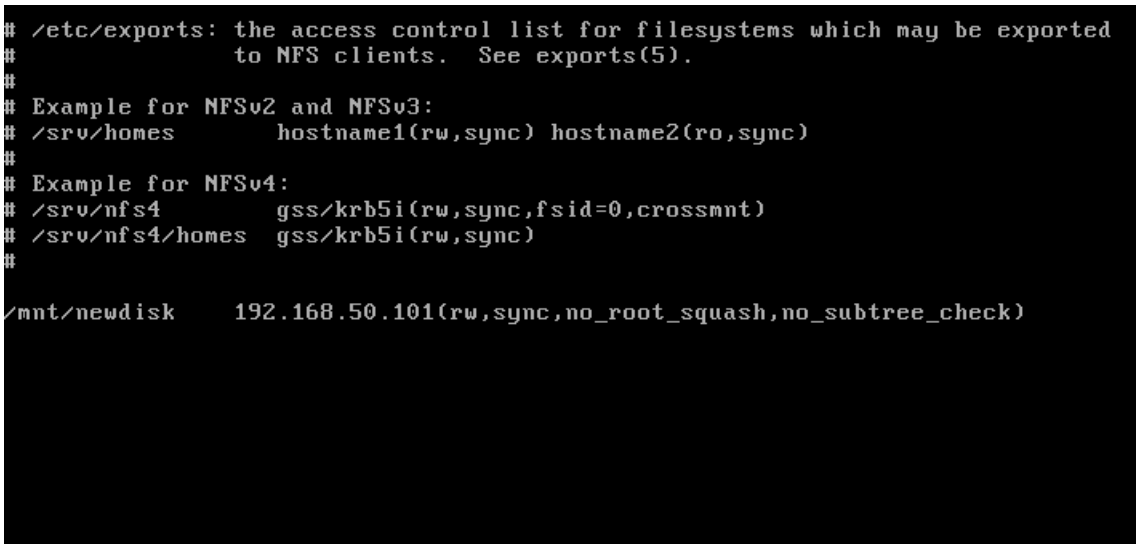
Andremo poi a controllare l’accessibilità adesso resa più sicura tramite Metasploit msfconsole, che ci restituirà il seguente risultato



11356 - NFS Exported Share Information Disclosure

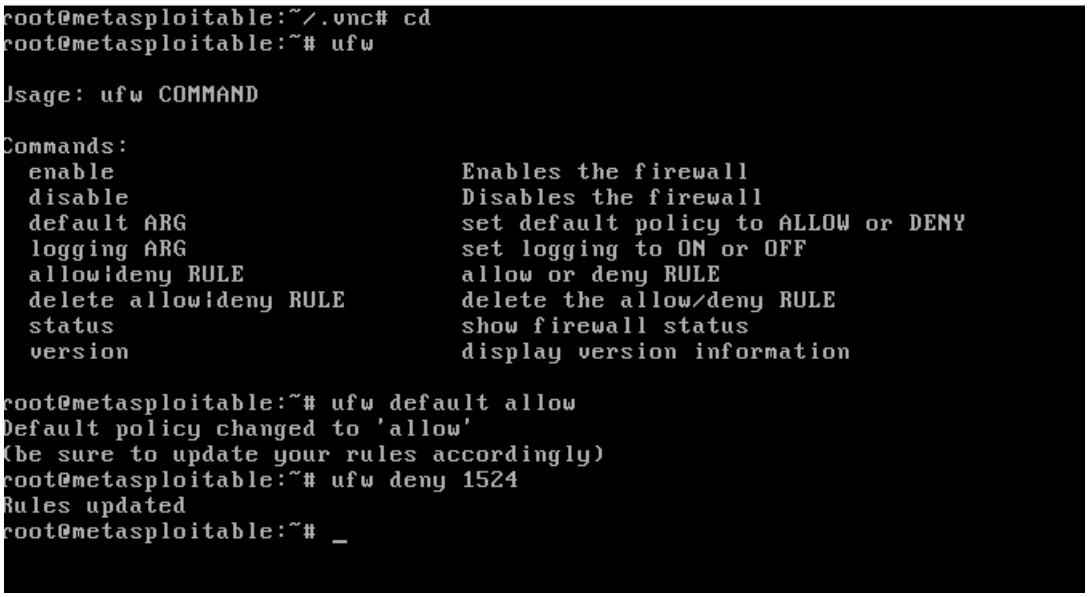
Questa vulnerabilià esponeva al rischio che anche in modalità remota i file condivisi risultassero accessibili anche da remoto come se fossero disponibili in ambito locale.

Per risolvere la criticità è stato ritenuto necessario configurare il server NFS per far sì che la lettura sia autorizzata con i privilegi necessari, esportando i file di sistema esplicitamente per i soli utenti che ne possono avere accesso, nella propria partizione.



51988 - Bind Shell Backdoor Detection

Per risolvere questa vulnerabilità infine è risultato sufficiente abilitare un firewall sulla porta specifica:



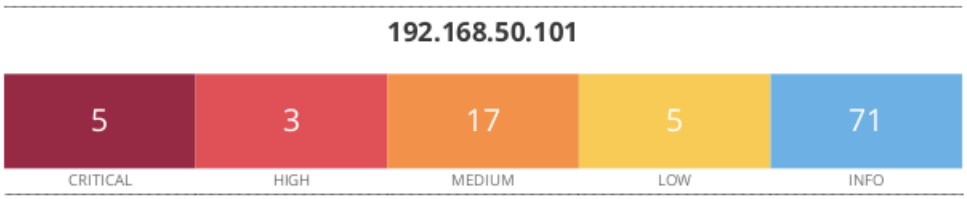
Utilizzando un Uncomplicated firewall, ci assicuriamo l'impostazione di una nuova regola chiudendo la porta 1524.Dopo aver impostato la nuova rules (n.d. qui risulta "updated" anziché "added" poiché ho ripetuto l'operazione per lo screen)

Andremo a controllarne l'effettivo stato tramite un port scanning specifico per la porta in questione.

Come possiamo notare la porta è passata da uno stato 'Open' ad uno 'Filtered' assicurandoci quindi che l'operazione è avvenuta con successo.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -T5 -sV -p1524 192.168.50.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-25 08:29 EST
Nmap scan report for 192.168.50.101
Host is up (0.00047s latency).

PORT     STATE SERVICE   VERSION
1524/tcp open  bindshell Metasploitable root shell
MAC Address: 08:00:27:C6:DE:4F (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.55 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -T5 -sV -p1524 192.168.50.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-25 08:38 EST
Nmap scan report for 192.168.50.101
Host is up (0.00055s latency).

PORT     STATE    SERVICE    VERSION
1524/tcp filtered ingreslock
MAC Address: 08:00:27:C6:DE:4F (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.77 seconds

┌──(root㉿kali)-[/home/kali]
└─#
```

A fine delle remediation actions andremo quindi a ripetere un vulnerabilità scan tramite Nessus, che ci restituirà un grafico con le criticità risolte non presenti.



Vulnerabilities — Total: 101

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	9.8	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
HIGH	8.6	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	90509	Samba Badlock Vulnerability