



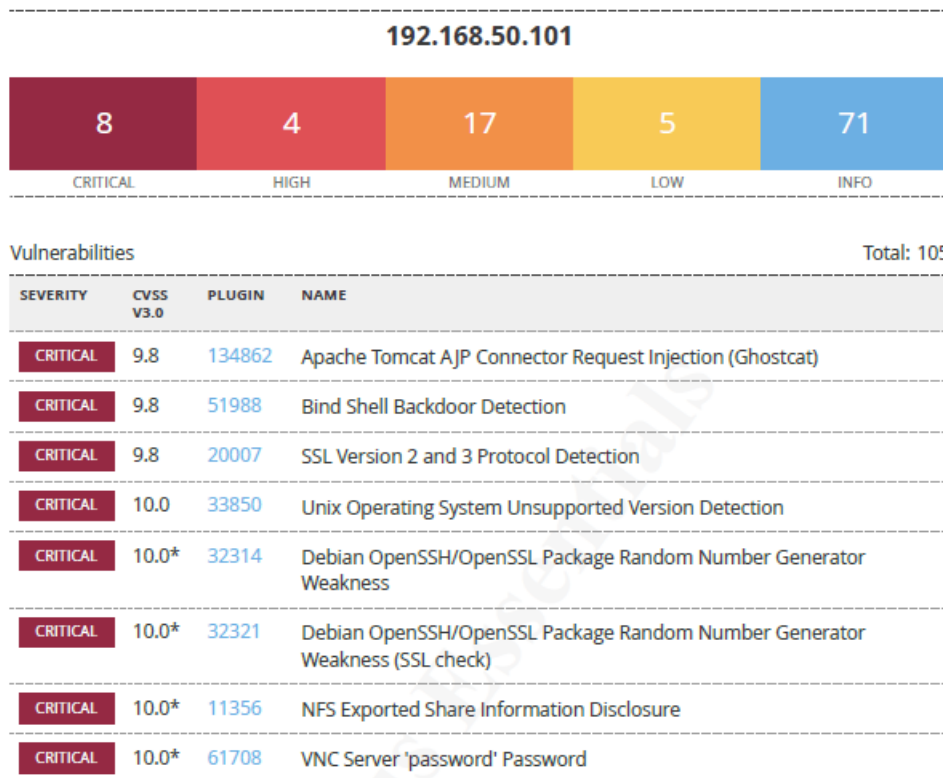
## metas

Report generated by Nessus™

Thu, 24 Nov 2022 13:19:11 EST

### Vulnerabilities by Host

- 192.168.50.101 .....4



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

## 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.

```
/mnt/newdisk 192.168.50.101(rw, sync, no_root_squash, no_subtree_check)
```

[ Wrote 15 lines ]

```
root@metasploitable:~# ls -la
.          .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 -la
.  metasploitable:0.log  metasploitable:1.log  passwd
.. metasploitable:0.pid  metasploitable:2.log  xstartup
root@metasploitable:~/vnc# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? _
```

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

```
Interact with a module by name or index. For example info 3, use 3 or use exploit/windows/local/powershell_remoting

msf6 auxiliary(scanner/vnc/vnc_login) > set RHOSTS 192.168.50.101
RHOSTS => 192.168.50.101
msf6 auxiliary(scanner/vnc/vnc_login) > options

Module options (auxiliary/scanner/vnc/vnc_login):
```

| Name             | Current Setting  | Required | Description  |
|------------------|--|----------|--|
| BLANK_PASSWORDS  | false  | no       | Try blank passwords for all users  |
| BRUTEFORCE_SPEED | 5  | yes      | How fast to bruteforce, from 0 to 5  |
| DB_ALL_CREDS     | false  | no       | Try each user/password couple stored in the current database                             |
| DB_ALL_PASS      | false  | no       | Add all passwords in the current database to the list                                    |
| DB_ALL_USERS     | false  | no       | Add all users in the current database to the list  |
| DB_SKIP_EXISTING | none   | no       | Skip existing credentials stored in the current database                                 |
| PASSWORD         |  | no       | The password to test   |
| PASS_FILE        | /usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt | no       | File containing passwords, one per line  |
| Proxies          |  | no       | A proxy chain of format type:host:port[,type:host:port][...]                             |
| RHOSTS           | 192.168.50.101   | yes      | The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-RHOSTS |
| RPORT            | 5900   | yes      | The target port (TCP)  |
| STOP_ON_SUCCESS  | false  | yes      | Stop guessing when a credential works for a host   |
| THREADS          | 1  | yes      | The number of concurrent threads (max one between 1 and 16)                              |
| USERNAME         | <BLANK>  | no       | A specific username to authenticate as   |
| USERPASS_FILE    |  | no       | File containing users and passwords separated by a colon                                 |
| USER_AS_PASS     | false  | no       | Try the username as the password for all   |
| USER_FILE        |  | no       | File containing usernames, one per line  |
| VERBOSE          | true   | yes      | Whether to print output for all attempts   |

```
msf6 auxiliary(scanner/vnc/vnc_login) > run

[*] 192.168.50.101:5900 - 192.168.50.101:5900 - Starting VNC login sweep
[!] 192.168.50.101:5900 - No active DB -- Credential data will not be saved!
[-] 192.168.50.101:5900 - 192.168.50.101:5900 - LOGIN FAILED: :password (Incorrect: Authentication failed)
[*] 192.168.50.101:5900 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) >
```

## 11356 - NFS Exported Share Information Disclosure

Questa vulnerabilità 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.

```
# /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/newdisk        192.168.50.101(rw,sync,no_root_squash,no_subtree_check)
```

## 51988 - Bind Shell Backdoor Detection

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

```
root@metasploitable:~/vnc# cd
root@metasploitable:~# ufw

Usage: ufw COMMAND

Commands:
  enable                Enables the firewall
  disable               Disables the firewall
  default ARG           set default policy to ALLOW or DENY
  logging ARG           set logging to ON or OFF
  allow|deny RULE       allow or deny RULE
  delete allow|deny RULE delete the allow/deny RULE
  status               show firewall status
  version               display version information

root@metasploitable:~# ufw default allow
Default policy changed to 'allow'
(be sure to update your rules accordingly)
root@metasploitable:~# ufw deny 1524
Rules updated
root@metasploitable:~# _
```

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  0.0.101
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
```

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.

