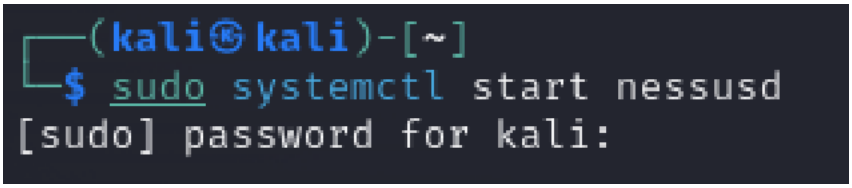
PROGETTO S5-L5

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.



192.168.66.2

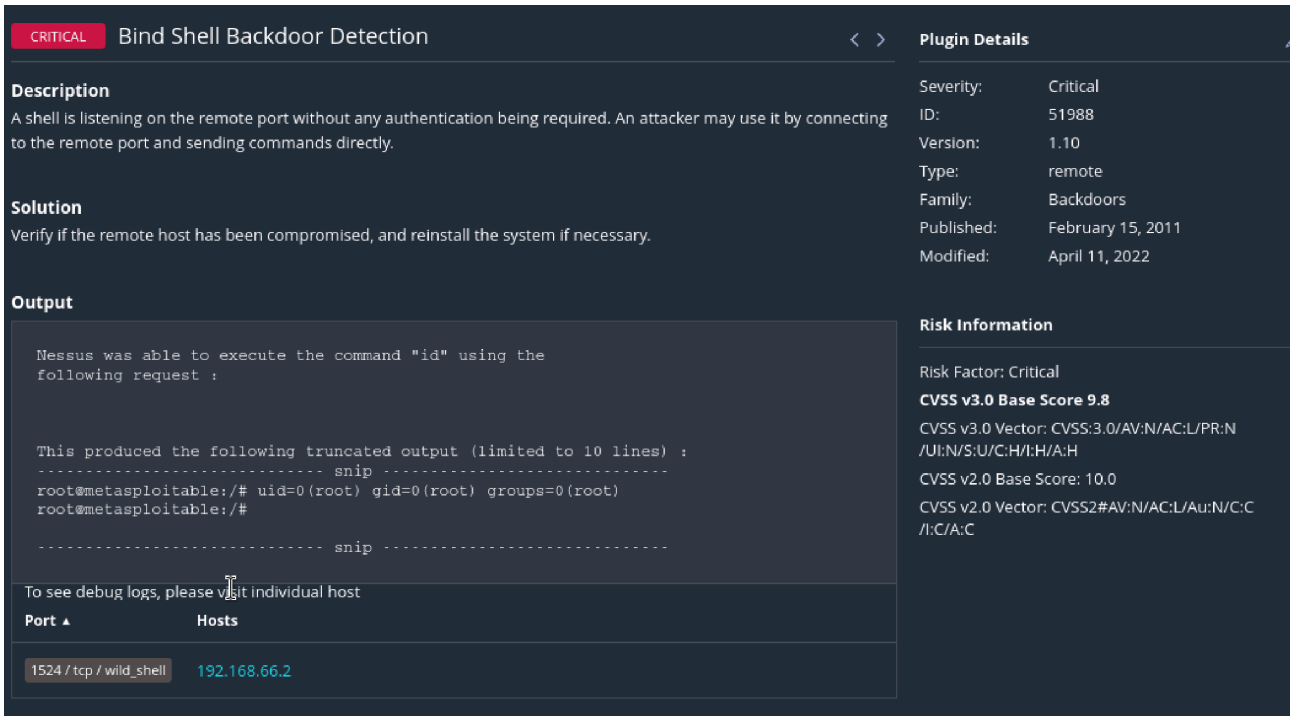
9	4	17	6	73
CRITICAL	HIGH	MEDIUM	LOW	INFO

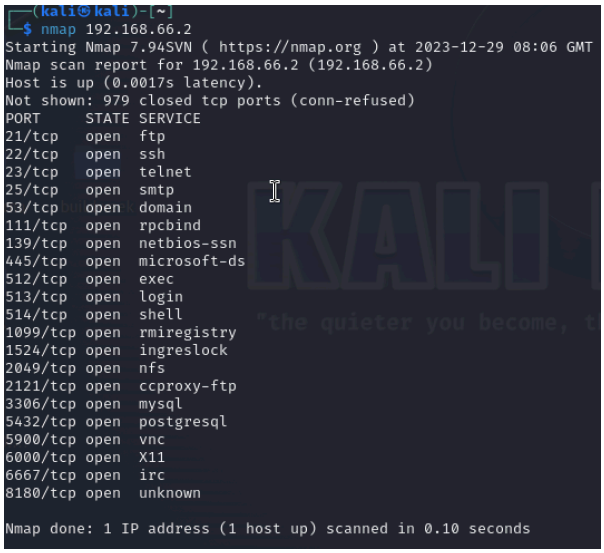
Vulnerabilities — Total: 109

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	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	9.1	6.0	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	7.4	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	7.4	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	-	61708	VNC Server 'password' Password
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42256	NFS Shares World Readable
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)

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





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 protoccollo 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

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)

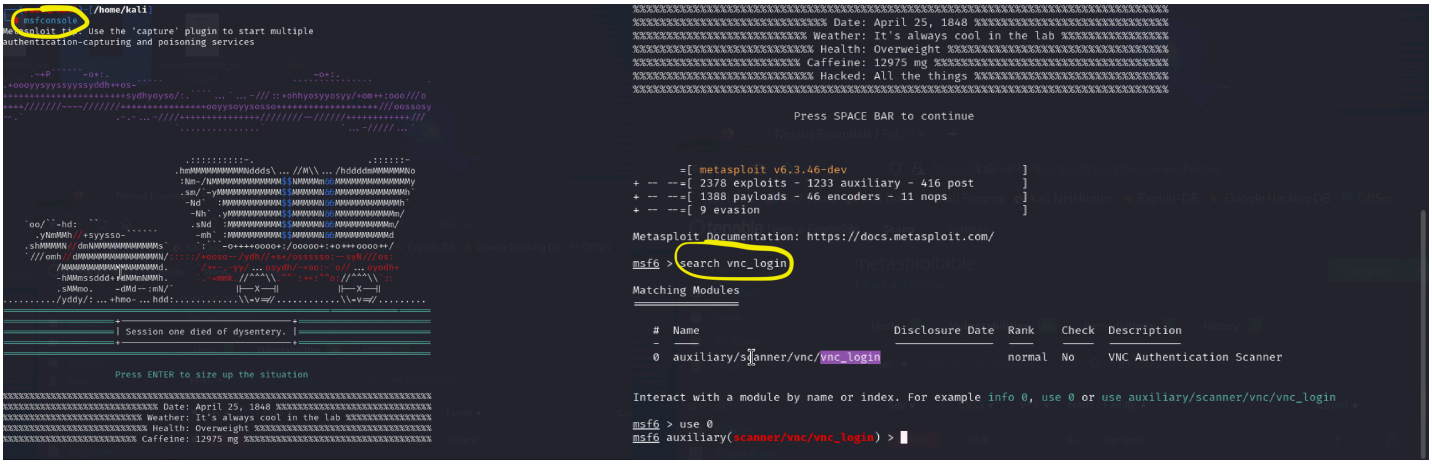
```
Nessus logged in using a password of "password".
```

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.

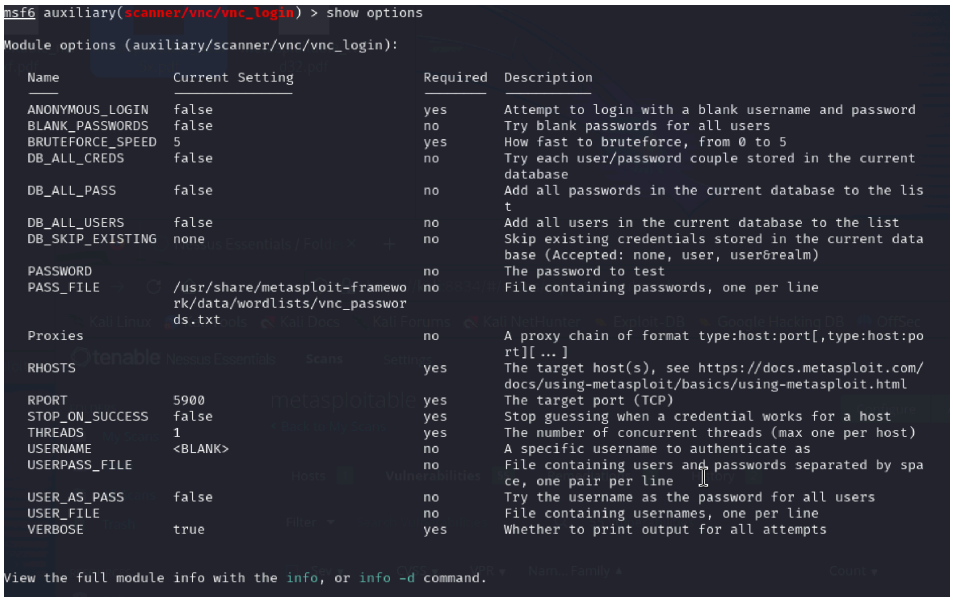
```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.66.2 -p 5900
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-29 03:02 GMT
Nmap scan report for 192.168.66.2 (192.168.66.2)
Host is up (0.0024s latency).

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

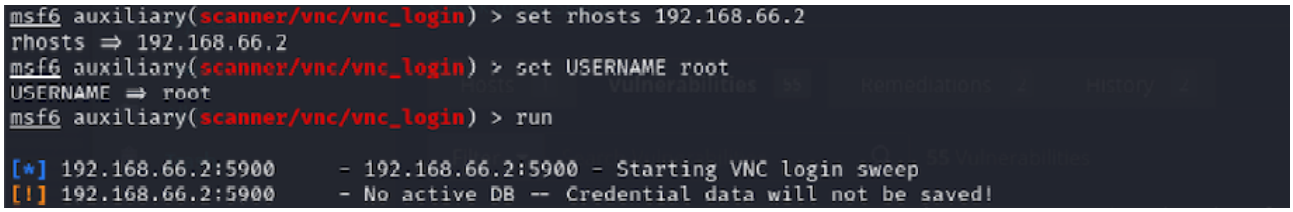
Controllo se la porta presenta vulnerabilità, lancio dapprima il comando msfconsole, ovvero l'interfaccia da riga di comando del metasploit framework utilizzato per l'esecuzione di exploit contro macchine remote, successivamente digito il comando "search vnc-login" per cercare i moduli disponibili relativi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



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.

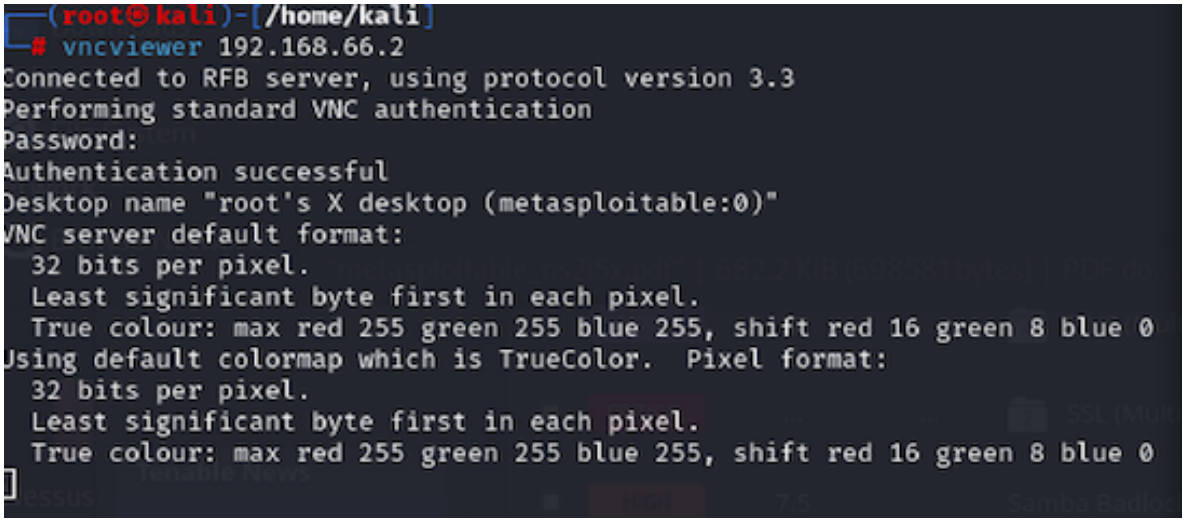


Impostiamo il RHOST(remote host) ovvero l'indirizzo ip del sistema target e un USERNAME.
Il comando "run" esegue il modulo selezionato con le impostazioni e i parametri specificati.
Notiamo che il login ha avuto successo infatti la password trovata è proprio "password".

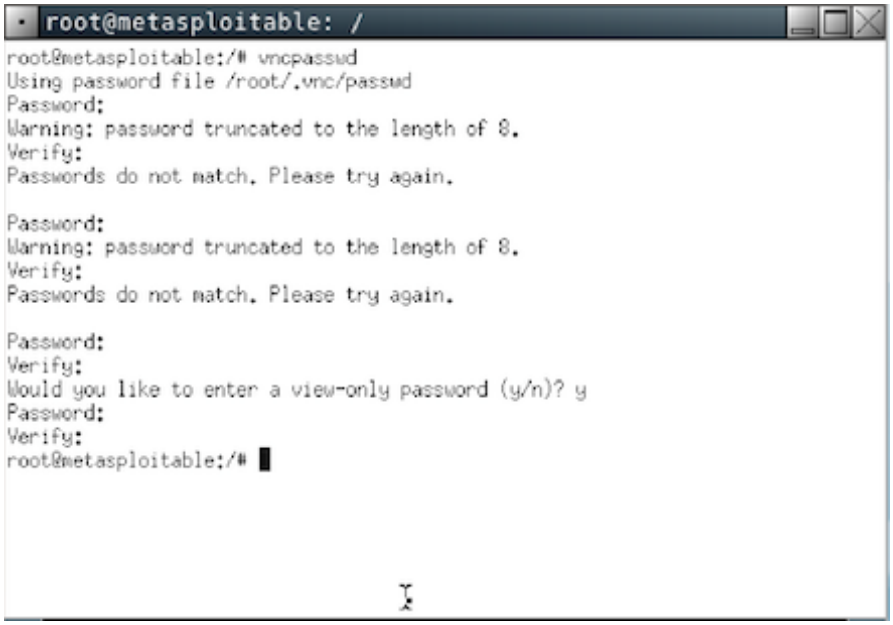


PROGETTO S5-L5

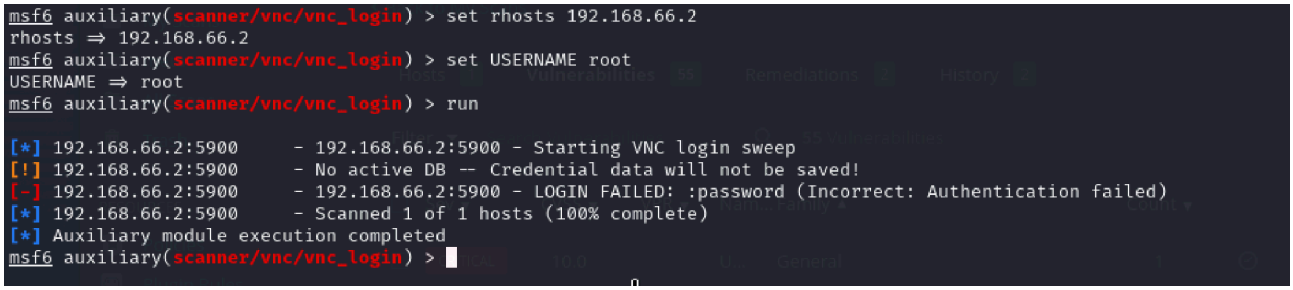
Ora possiamo usare il comando “vncviewer” che ci consentirà di accedere in remoto e interagire con l’ambiente desktop di un server VNC.



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



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



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.

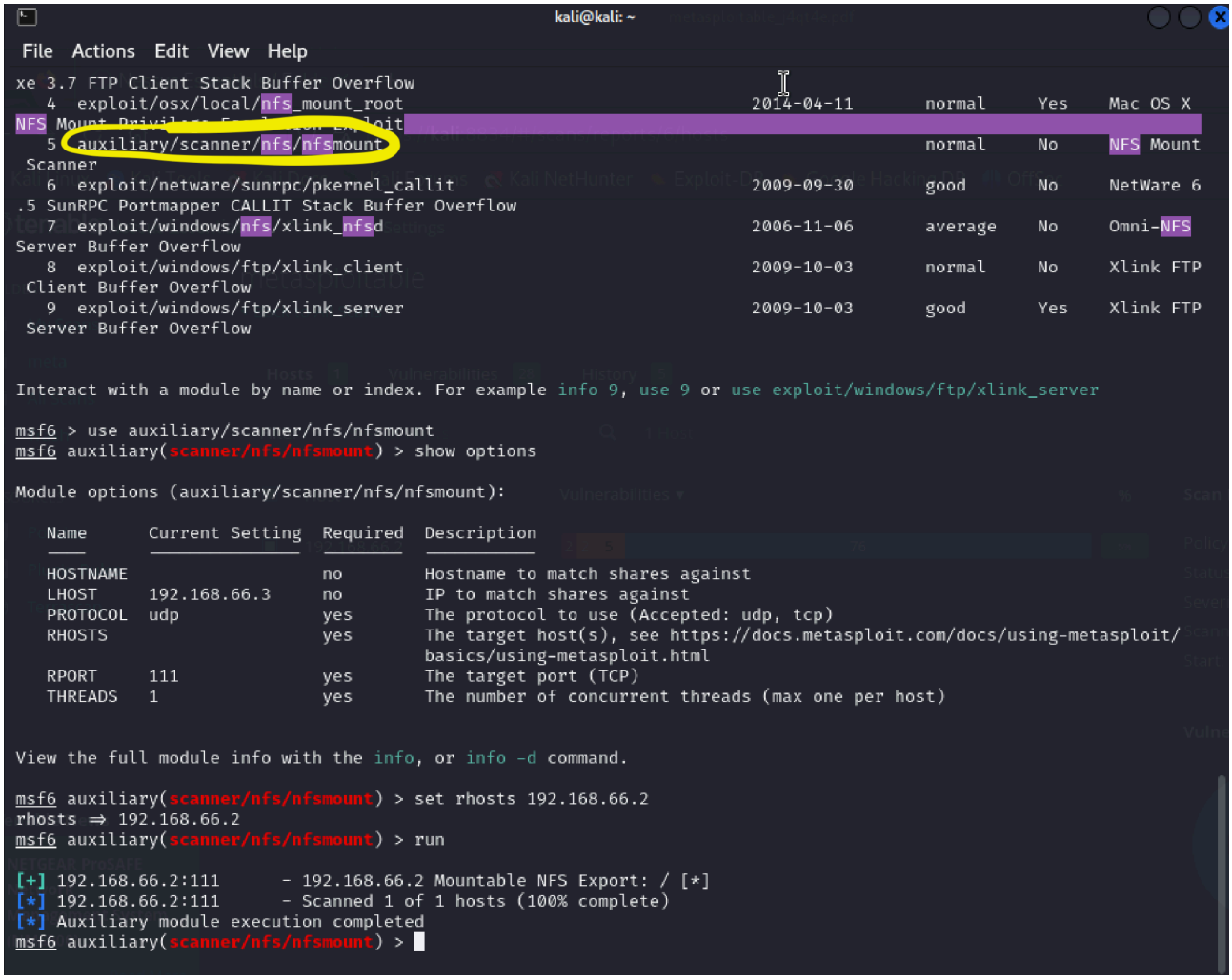
```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.66.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-29 09:09 GMT
Nmap scan report for 192.168.66.2 (192.168.66.2)
Host is up (0.00097s latency).
Not shown: 978 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   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
```

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

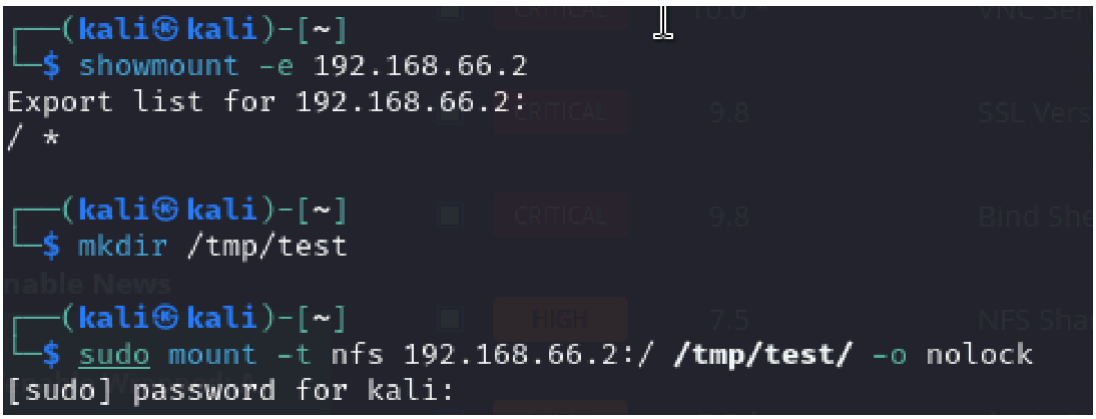
```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Use the edit command to open the currently active module
in your editor

       =[ metasploit v6.3.46-dev                          ]
+ -- --=[ 2378 exploits - 1233 auxiliary - 416 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search nfs
```

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.



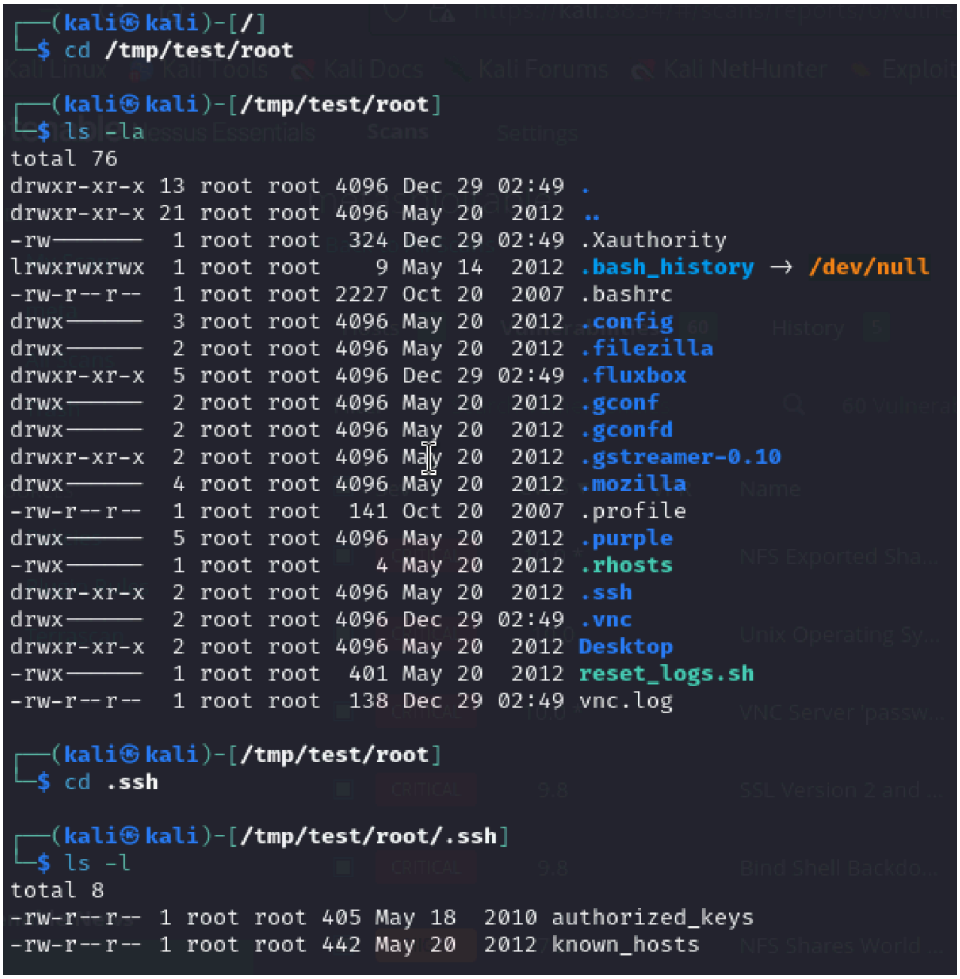
Il passo successivo sarà capire quali privilegi abbiamo sulla directory condivisa.
Iniziamo con la creazione di una nuova directory localmente nella direcotry “tmp”.



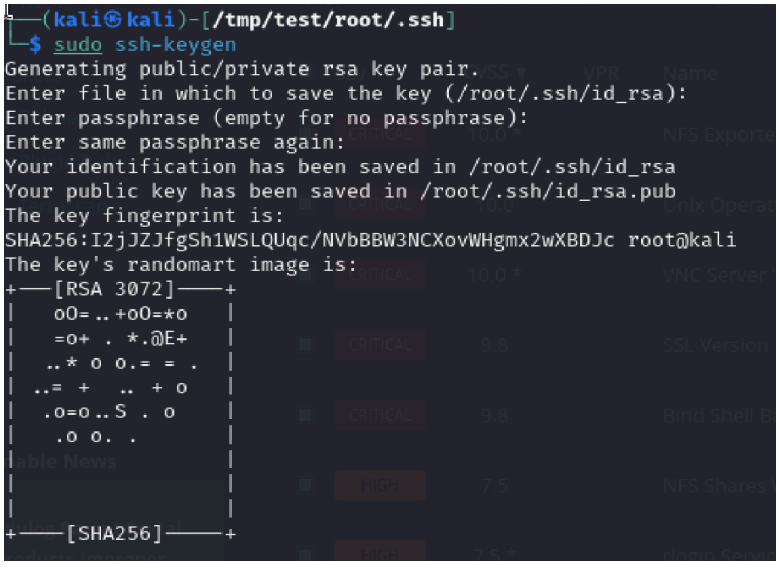
Il comando “Mount” con l’opzione “nolock” è utilizzato per montare un file System NFS senza utilizzare il locking dei file(meccanismo che previene conflitti quando più client tentano di accedere allo stesso file contemporaneamente).

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.



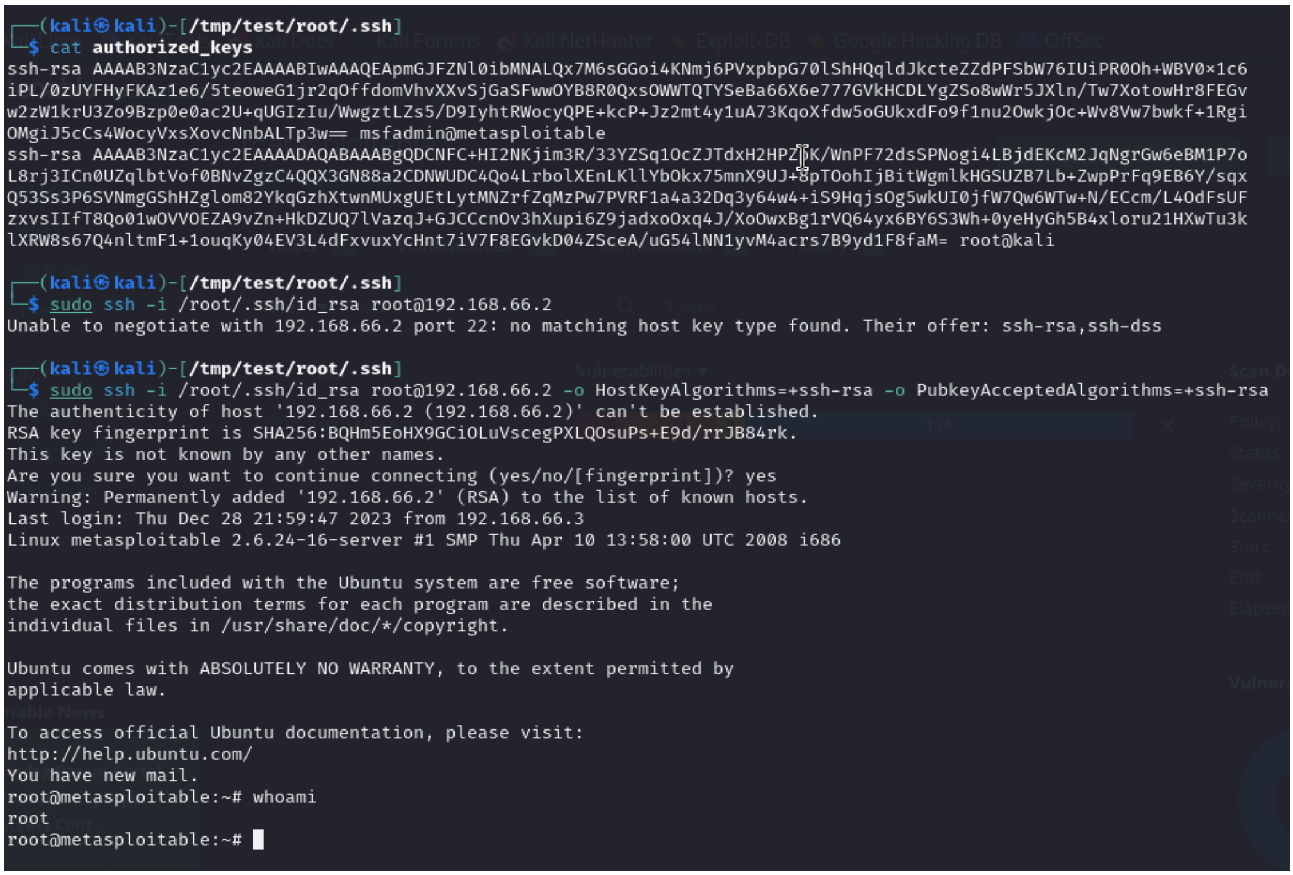
"ssh-keygen" è un comando utilizzato per gestire e convertire le chiavi di autenticazione per il protocollo SSH. Crea una coppia di chiavi, una pubblica e una privata, nella directory /root/.ssh/ id_rsa. La chiave pubblica può essere condivisa liberamente, in questo caso il tipo di chiave utilizzato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



PROGETTO S5-L5

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

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 procedure saremo in grado di accedere al server come root.

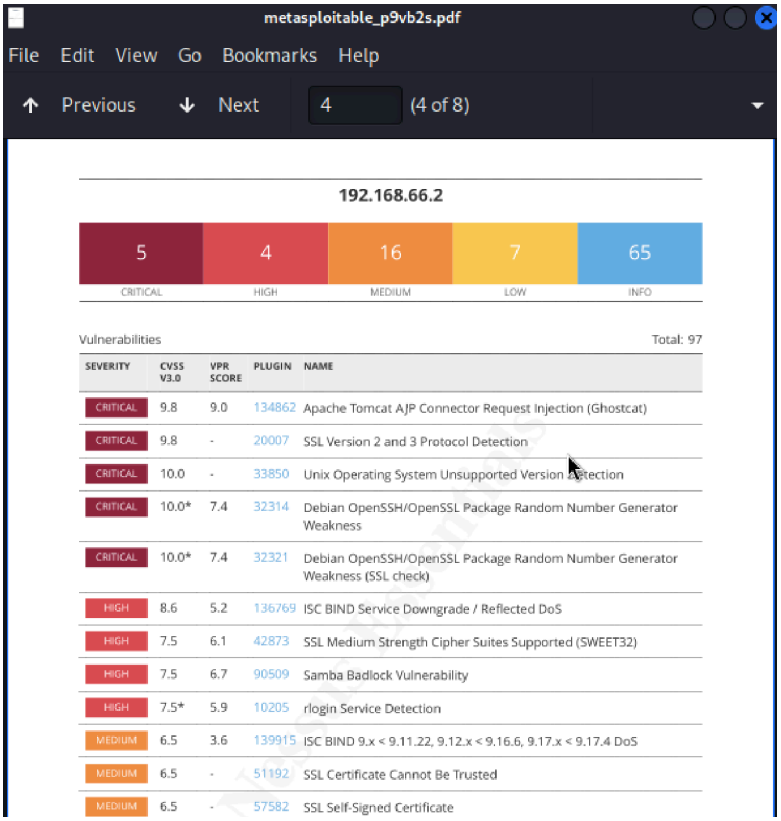


Per evitare che tutto ciò si verifichi è necessario modificare la configurazione del server NFS. Su metasploitable nella directory /etc modifichiamo il file “exports” attraverso il comando “sudo nano exports”. Una volta aperto il file di testo modificheremo la configurazione come segue.

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.