

## S5L5

Effettuare una scansione completa su Metasploitable utilizzando Nessus e selezionare 2-4 vulnerabilità critiche o di alto livello per implementare azioni di rimedio.

### Risoluzione:

Una volta eseguita la scansione, si state scelte tre vulnerabilità di livello critico/alto da correggere. Per prima cosa si analizzano le vulnerabilità, poi si implementano le azioni di rimedio; dopo, si esegue nuovamente la scansione per dimostrare l'efficienza delle azioni di rimedio e infine si confrontano i risultati con quelli ottenuti in precedenza.

<input type="checkbox"/>	Sev ▼	CVSS ▼	VPR ▼	Name ▲	Family ▲	Count ▼		
<input type="checkbox"/>	CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1	🕒	✎
<input type="checkbox"/>	CRITICAL	10.0		Unix Operating System Unsupported Version D...	General	1	🕒	✎
<input type="checkbox"/>	CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1	🕒	✎
<input type="checkbox"/>	CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2	🕒	✎
<input type="checkbox"/>	CRITICAL	9.8	9.4	Bash Remote Code Execution (Shellshock)	Gain a shell remotely	1	🕒	✎
<input type="checkbox"/>	CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1	🕒	✎
<input type="checkbox"/>	CRITICAL	9.8	5.1	Weak Debian OpenSSH Keys in ~/.ssh/authoriz...	Gain a shell remotely	1	🕒	✎
<input type="checkbox"/>	MIXED	...	...	📁 99+ Canonical Ubuntu Linux (Multiple Issues)	Ubuntu Local Security Checks	229	🕒	✎
<input type="checkbox"/>	MIXED	...	...	📁 4 Apache Tomcat (Multiple Issues)	Web Servers	4	🕒	✎
<input type="checkbox"/>	CRITICAL	...	...	📁 2 SSL (Multiple Issues)	Gain a shell remotely	3	🕒	✎
<input type="checkbox"/>	MIXED	...	...	📁 3 Apache Log4j (Multiple Issues)	Misc.	3	🕒	✎
<input type="checkbox"/>	HIGH	7.5		NFS Shares World Readable	RPC	1	🕒	✎

## Weak Debian OpenSSH Keys in ~/.ssh/authorized\_keys (CRITICAL)

Questa vulnerabilità indica che ci sono chiavi “OpenSSH Debian” deboli in “~/.ssh/authorized\_keys” e che lo stato è critico. Questo significa che le chiavi SSH sono prevedibili e suscettibili e un utente malintenzionato potrebbe tentare un attacco brute-force contro l'host remoto e accedere utilizzando queste chiavi deboli.

### Soluzione (Suggerita da Nessus)

- Rimuovere tutte le voci incriminate da ~/.ssh/authorized\_keys e generare keys sicure.

In questo modo si eliminano tutte le chiavi deboli, si rafforza il sistema e lo si protegge dagli attacchi di accesso non autorizzato.

#### Solution

Remove all the offending entries from ~/.ssh/authorized\_keys.

#### Output

```
In file /root/.ssh/authorized_keys:
line 1:
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEApmGJFZNl0ibMNALQx7M6sGGoi4KNmj6PVxpb
pG701ShHQldJkcteZZdPFSbW76IUipR0Oh+WBV0x1c6iPL/0zUYFHyFKAzle6/5teoweG1j
r2qOffdomVhvXXvSjGaSFwwOYB8R0QxsOWWTQTYSeBa66X6e777GVkHCDLYgZSo8wWr5JXln
/Tw7XotowHr8FEGvw2zWlkrU3Zo9Bzp0e0ac2U+qUGIzIu/WwgztLZs5/D9IyhtRWocyQPE+
kcP+Jz2mt4y1uA73KqoXfdw5oGUkxdFo9flnu2OwkjOc+Wv8Vw7bwkf+1RgiOMgiJ5cCs4Wo
cyVxsXovcNnbALTp3w== msfadmin@metasploitable

In file /home/msfadmin/.ssh/id_rsa.pub:
line 1:
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEApmGJFZNl0ibMNALQx7M6sGGoi4KNmj6PVxpb
pG701ShHQldJkcteZZdPFSbW76IUipR0Oh+WBV0x1c6iPL/0zUYFHyFKAzle6/5teoweG1j
r2qOffdomVhvXXvSjGaSFwwOYB8R0QxsOWWTQTYSeBa66X6e777GVkHCDLYgZSo8wWr5JXln
/Tw7XotowHr8FEGvw2zWlkrU3Zo9Bzp0e0ac2U+qUGIzIu/WwgztLZs5/D9IyhtRWocyQPE+
kcP+Jz2mt4y1uA73KqoXfdw5oGUkxdFo9flnu2OwkjOc+Wv8Vw7bwkf+1RgiOMgiJ5cCs4Wo
cyVxsXovcNnbALTp3w== msfadmin@metasploitable

In file /home/msfadmin/.ssh/authorized_keys:
line 1:
ssh-dss AAAAB3NzaC1kc3MAAACBANWgcbHvxF2YRX0gTizyoZazzHiU5+63hKFOhzJch8dZ
QpFU5gGkDkZ30rC4jrNqCXNDN50RA4ylcNtO78B/I4+5YCZ39faSiXIOLfi8tOVWtTtg3lku
v3eSV0zuSGeqZPHMtep6iizQA5yoClkCyj8swXH+cPBG5uRPiXYL911rAAAAFQDL+pKRLy6v
y9HCywXWZ/jcPpPHEQAAAIAGt+cN3fDT1RRCYz/VmqfUsqW4jtZ06kvx3L82T2Z1YVeXe792
9JWeu9d3OB+NeE8EopMiWaTzt0WI+OkzxSAGyuTskue4nvGCfxnDr58xa1pZcSO66R5jCSAR
MHU6WBWId3MYzsJNZqTN4uoRa4tIFwM8X99K0UUVmLvNbPByEAAAAIBNfKRDwM/QnEpdRTTs
RBh9rALq6eDlNbu/5gozf4Fv1Dt1Zmq5ZxtXeQtW5BYorILRZ5/Y4pChRa01bxTRSJah0R
Jk5wxAUPZ282N07fzcJyVlBojMvPlbAplpSiecCuLGX7G04Ie8SFzT+wCketP9Vrw0PvtUZU
3DfrVTCytg== user@metasploitable

less...
```

Adesso seguiamo il suggerimento di Nessus

>>> Accesso al sistema

```
msfadmin@metasploitable:~$ ssh msfadmin@192.168.1.13
msfadmin@192.168.1.13's password:
```

Eliminammo chiavi deboli comuni:

### 1 “authorized\_keys” DI ROOT

inserendo il comando “sudo nano /root/.ssh/authorized\_keys”

```
GNU nano 2.0.7      File: /root/.ssh/authorized_keys

ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEApmGJFZNl0ibMNALQx7M6sGGoi4KNmj6PVxpbpG70lSh$
```

Eliminiamo quella chiave esistente (poi salva ed esci)

```
kali@kali: ~
File Actions Edit View Help
GNU nano 2.0.7      File: /root/.ssh/authorized_keys      Modified
```

Creazione nuova chiave più sicura

```
msfadmin@metasploitable:~$ ssh-keygen -t rsa -b 4096 -C "META@meta1"
Generating public/private rsa key pair.
Enter file in which to save the key (/home/msfadmin/.ssh/id_rsa):
/home/msfadmin/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/msfadmin/.ssh/id_rsa.
Your public key has been saved in /home/msfadmin/.ssh/id_rsa.pub.
The key fingerprint is:
f8:e9:3c:75:a3:49:aa:e1:82:a4:3d:2e:ec:da:4d:59 META@meta1
```

Inseriamo la nuova chiave al terminale di “authorized\_keys” di root

```
msfadmin@metasploitable:~$ cat /home/msfadmin/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAEAw056aLbqPCKAuZkLHf/engiQRl6wdTx7cgtsL19TPPT0lG1xS6zQusak/u929CiL
9DWLPjvyUg05sY5ExuoS/y5gCZx2BqS0h8beasB1UDrnyb7juM0o8Bp6FFjUE5Nuse2E+r6yWs701wXQuY3HPHlmXr0YtIcooRdO
kXfbJ2r0//FxUaAzUntx4aPoTjLCuCur1/20PHvRxPc1qR25n315tfjmWldbn/sohmJd80macs8x9PZiiCBtzL9y9dyykP0e0lDH
qTHEf7fy8aLmVjtSM0fXdtZM9M6KFICHAmk12v4xXM+jbAoo61l7sg3IwWt fmPWJMMKDWKx0mVz1CBnNZpMD1LWsc09+coUN68dP
lwRfQZ0mF9+zxauDfokjhFDHhNnYKvJtOGZqmnfhbcDcaaSYlCl8DkZi4sCaMGq5JJ3lybNz7cQDWQqGrKpNCLK4Rsa5s0VBGUzb
gSqAopcZPNAuoQAnJnF6Fdj12oIivgtKZDWQ4A03y5+T6s5/aN4W6kx417yCsEzaEFZvKJHUpbr081oja2UKaSbTLTP3ZjJSBYbt
PKXfpU3uL8ugtFqnpzS/mo802vkgmuTEGFclpbVDqfGIh199QnI1PMs1pOE/AxjrvLMqV6WWbEprVl/Z32uOWaKeZ6etnq500MNF
jQUQA5LGWZouYMgDSPs= META@meta1
msfadmin@metasploitable:~$ sudo nano /root/.ssh/authorized_keys

kali@kali: ~
File Actions Edit View Help
GNU nano 2.0.7      File: /root/.ssh/authorized_keys      Modified

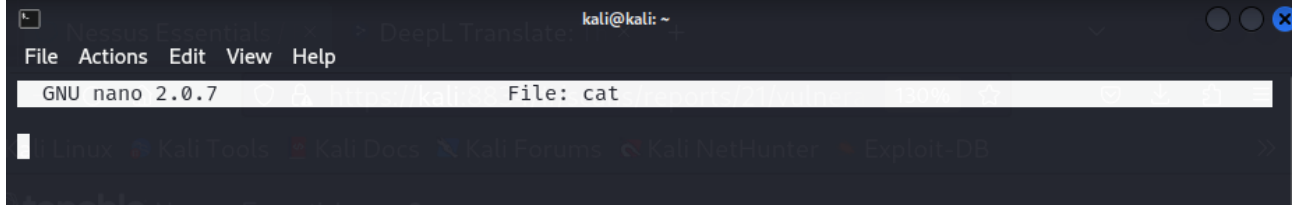
$l99QnI1PMs1pOE/AxjrvLMqV6WWbEprVl/Z32uOWaKeZ6etnq500MNFjQUQA5LGWZouYMgDSPs= META@meta1
```

Qui si salva e si esce.

## 2 “authorized\_keys” DI ADMIN

Entriamo al terminale della chiave

```
msfadmin@metasploitable:~$ sudo nano cat /home/msfadmin/.ssh/id_rsa.pub
```

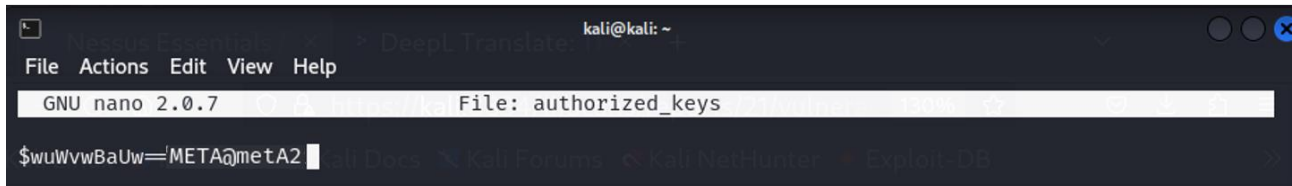


In questo caso è vuoto, quindi dobbiamo generare una nuova chiave e aggiungerla a  
“authorized\_keys” di admin

```
msfadmin@metasploitable:~$ ssh-keygen -t rsa -b 2048 -f ~/.ssh/id_rsa_msadmin_nueva2 -C "META@metA2"
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/msfadmin/.ssh/id_rsa_msadmin_nueva2.
Your public key has been saved in /home/msfadmin/.ssh/id_rsa_msadmin_nueva2.pub.
The key fingerprint is:
79:d2:fd:ea:7d:e6:92:65:ba:88:63:b0:8a:69:0a:10 "META@metA2"
```

Inseriamo la nuova chiave al terminale di “authorized\_keys” di msfadmin

```
msfadmin@metasploitable:~$ cat ~/.ssh/id_rsa_msadmin_nueva2.pub
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAXip2F49pUZ9tKoDU4yhAst1INwnUeaScUrXqT7oXjOR9tdd8hBavzLC7MTDKoaiF
VowvhS0x08fSntoOcdYctM/qLiFS+1lKslGKxBX1U3Uf3oon/nFvsUzQtgvm/LLGVo73V4jo4EnjVtQh3LT3db8p2psZzi/w8FHE
okO5VN5rppoEH2EzsoFwl9uOvkC4QCeJwF7MiK/d0du6kvPdr168wPQswxwvzoU3NYJx4TY/+Z7I8RfLrDmV83CB0tQ2zQrTNjM
M+Pqotovi2u6hv4jIgbt4iA2afL5Xj0QMBBxM0Qwu2krWwp9xmequ1fTg9FSDZ+OJ9AotZUOb+kC5w= "META@metA2"
msfadmin@metasploitable:~$ sudo nano /home/msfadmin/.ssh/authorized_keys
```

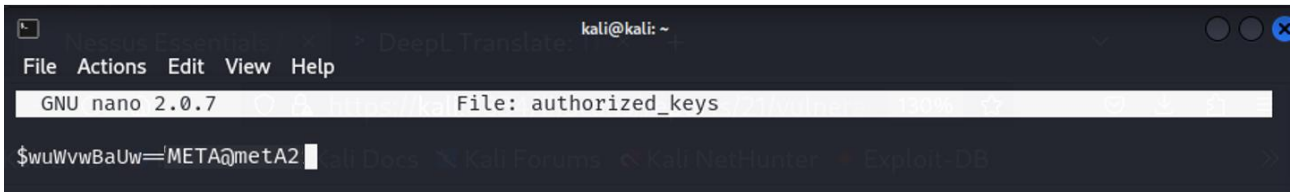


```
$wuWvwBaUw="META@metA2"
```

Qui si salva e si esce

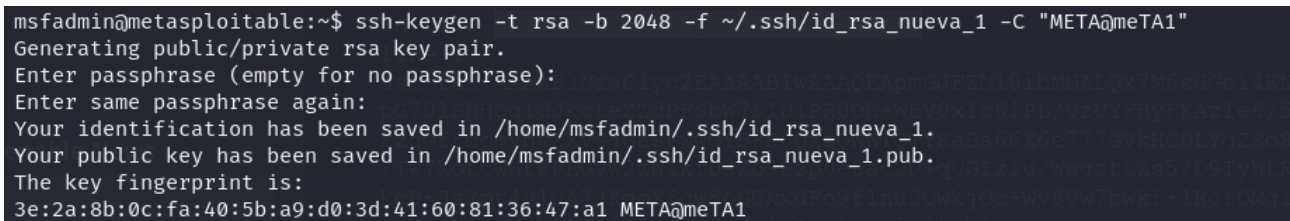
### 3 “id\_rsa.pub” DI MSFADMIN

Entriamo al terminale della chiave



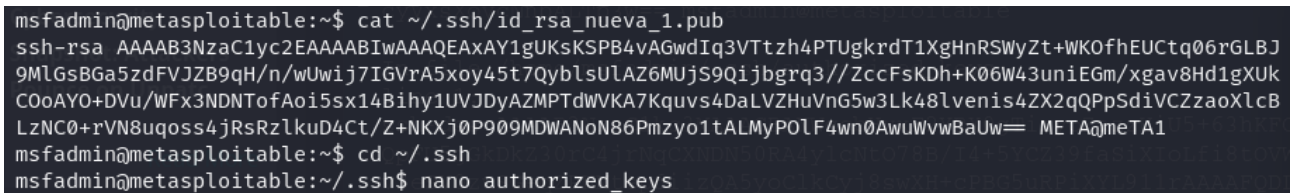
```
kali@kali: ~  
File Actions Edit View Help  
GNU nano 2.0.7 File: authorized_keys  
$WuWvwBaUw==META@metA2
```

In questo caso troviamo solo la chiave creata precedentemente e dobbiamo generare un'altra per “id\_rsa.pub”:

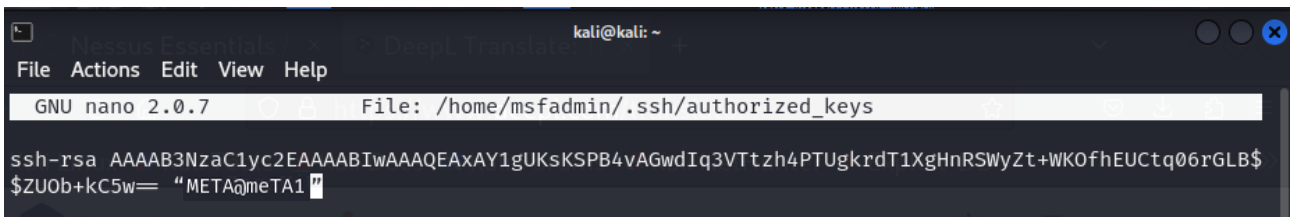


```
msfadmin@metasploitable:~$ ssh-keygen -t rsa -b 2048 -f ~/.ssh/id_rsa_nueva_1 -C "META@meTA1"  
Generating public/private rsa key pair.  
Enter passphrase (empty for no passphrase):  
Enter same passphrase again:  
Your identification has been saved in /home/msfadmin/.ssh/id_rsa_nueva_1.  
Your public key has been saved in /home/msfadmin/.ssh/id_rsa_nueva_1.pub.  
The key fingerprint is:  
3e:2a:8b:0c:fa:40:5b:a9:d0:3d:41:60:81:36:47:a1 META@meTA1
```

Inseriamo la nuova chiave al terminale di “id\_rsa.pub” di msfadmin



```
msfadmin@metasploitable:~$ cat ~/.ssh/id_rsa_nueva_1.pub  
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAXAY1gUKsKSPB4vAGwdIq3VTtz4PTUgkrdT1XgHnRSWyZt+WKOfhEUCtq06rGLBJ  
9MlGsBGa5zdFVJZB9QH/n/wUwij7IGVrA5xoy45t7QyblsULAZ6MUjs9Qijbgrq3//ZccFsKDh+K06W43uniEGm/xgav8Hd1gXUk  
COoAYO+DVu/WFx3NDNTofAoi5sx14Bihy1UVJDyAZMPTdWVKA7Kquvs4DaLVZHuVnG5w3Lk48lvenis4ZX2qQPpSdiVCZzaoXlCB  
LzNC0+rVN8uqoss4jRsRzlkud4Ct/Z+NKXj0P909MDWANoN86Pmzyo1tALMyPOLF4wn0AwuWvwBaUw== META@meTA1  
msfadmin@metasploitable:~$ cd ~/.ssh  
msfadmin@metasploitable:~/.ssh$ nano authorized_keys
```



```
kali@kali: ~  
File Actions Edit View Help  
GNU nano 2.0.7 File: /home/msfadmin/.ssh/authorized_keys  
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAXAY1gUKsKSPB4vAGwdIq3VTtz4PTUgkrdT1XgHnRSWyZt+WKOfhEUCtq06rGLB$  
$ZUOb+kC5w== "META@meTA1"
```

Qui si salva e si esce

ORA POSSIAMO VEDERE LE 3 CHIAVI MODIFICATE

authorized\_keys de root

```
msfadmin@metasploitable:~$ cat /root/.ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQBAQCw56aLbqPCXKauZkLHf/eng iQRl6wdTx7cgtsL19TPPT0
lG1xS6zQusak/u929CiL9DWLP jvyUg05sY5ExuoS/y5gCZx2BqS0h8beasB1UDrnyb7 juM0o8Bp6FF jU
E5Nuse2E+r6yWs701wXQuY3HPHlmXr0YtIcooRd0kXfbJ2r0//FxUaAzUntx4aPoTj1CuCuR1/20PHuR
xPc1qR25n315tf jmWldbn/sohmJd80macs8x9PZiiCBtzL9y9dykP0e0lDHgTHEf7fy8a1MvJtSM0fX
dt2M9M6KFICHAmki2v4xXM+jbAoo6117sg3lwWtfmPWJMMKDWKx0mVz1CBnNZpMD1LWsc09+coUN68dP
lwRfQZ0mF9+zxauDfOkjhFDHhNnYKvJtOGZqmmfhbcDcaasYICl8DkZi4sCaMGq5JJ3lybNz7cQDWQqG
rKpNCLK4Rsa5s0VBGUzbGsqAopc2PNAuoQAnJnF6Fdj12oliugtK2DWQ4A03y5+T6s5/aN4W6kx417yC
sEzaEFZvKJHUpbr081o ja2UKaSbT1TP3Z jJSBYbtPKXfpU3uL8ugtFqnzps/mo802vkgmuTEGfc1pbVD
qfG1h199QmI1Pms1pOE/AxjrvLMqV6WWbEpvR1/232uOWaKe26etnq500MNF jQUQA5LGWZouYMgDSPs=
META@meta1
```

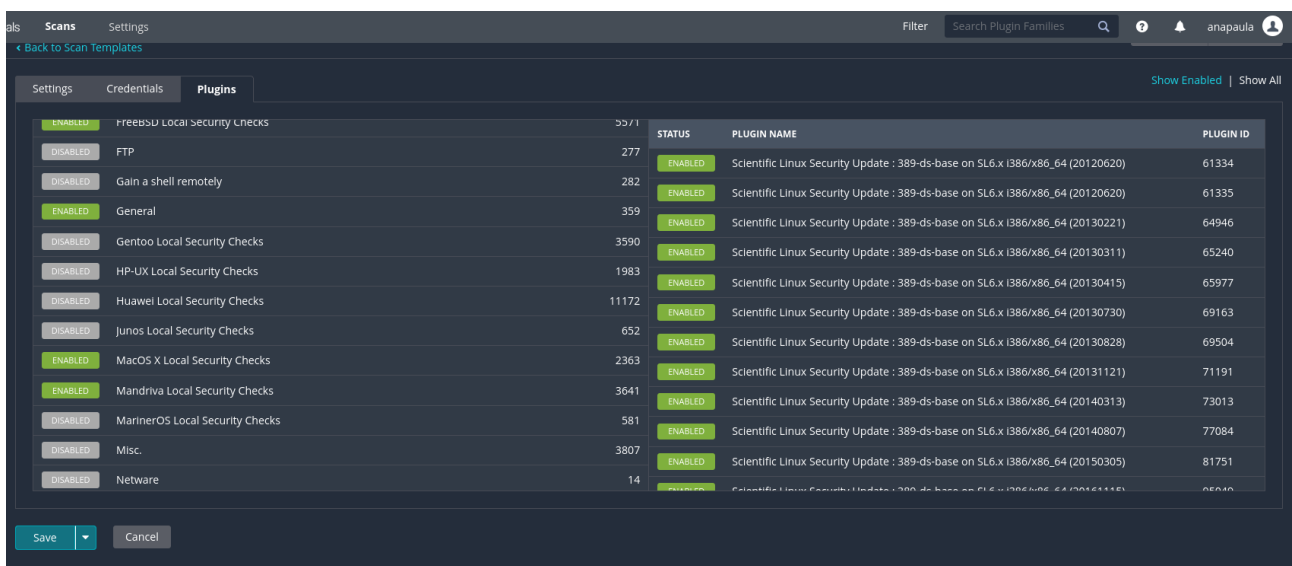
id\_rsa.pub de msfadmin

```
msfadmin@metasploitable:~$ cat /home/msfadmin/.ssh/id_rsa_msadmin_nueva2.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQBAQCw56aLbqPCXKauZkLHf/eng iQRl6wdTx7cgtsL19TPPT0
lG1xS6zQusak/u929CiL9DWLP jvyUg05sY5ExuoS/y5gCZx2BqS0h8beasB1UDrnyb7 juM0o8Bp6FF jU
E5Nuse2E+r6yWs701wXQuY3HPHlmXr0YtIcooRd0kXfbJ2r0//FxUaAzUntx4aPoTj1CuCuR1/20PHuR
xPc1qR25n315tf jmWldbn/sohmJd80macs8x9PZiiCBtzL9y9dykP0e0lDHgTHEf7fy8a1MvJtSM0fX
dt2M9M6KFICHAmki2v4xXM+jbAoo6117sg3lwWtfmPWJMMKDWKx0mVz1CBnNZpMD1LWsc09+coUN68dP
lwRfQZ0mF9+zxauDfOkjhFDHhNnYKvJtOGZqmmfhbcDcaasYICl8DkZi4sCaMGq5JJ3lybNz7cQDWQqG
rKpNCLK4Rsa5s0VBGUzbGsqAopc2PNAuoQAnJnF6Fdj12oliugtK2DWQ4A03y5+T6s5/aN4W6kx417yC
sEzaEFZvKJHUpbr081o ja2UKaSbT1TP3Z jJSBYbtPKXfpU3uL8ugtFqnzps/mo802vkgmuTEGfc1pbVD
qfG1h199QmI1Pms1pOE/AxjrvLMqV6WWbEpvR1/232uOWaKe26etnq500MNF jQUQA5LGWZouYMgDSPs=
META@meta2
```

authorized\_keys de msfadmin

```
msfadmin@metasploitable:~$ cat /home/msfadmin/.ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQBAQCw56aLbqPCXKauZkLHf/eng iQRl6wdTx7cgtsL19TPPT0
lG1xS6zQusak/u929CiL9DWLP jvyUg05sY5ExuoS/y5gCZx2BqS0h8beasB1UDrnyb7 juM0o8Bp6FF jU
E5Nuse2E+r6yWs701wXQuY3HPHlmXr0YtIcooRd0kXfbJ2r0//FxUaAzUntx4aPoTj1CuCuR1/20PHuR
xPc1qR25n315tf jmWldbn/sohmJd80macs8x9PZiiCBtzL9y9dykP0e0lDHgTHEf7fy8a1MvJtSM0fX
dt2M9M6KFICHAmki2v4xXM+jbAoo6117sg3lwWtfmPWJMMKDWKx0mVz1CBnNZpMD1LWsc09+coUN68dP
lwRfQZ0mF9+zxauDfOkjhFDHhNnYKvJtOGZqmmfhbcDcaasYICl8DkZi4sCaMGq5JJ3lybNz7cQDWQqG
rKpNCLK4Rsa5s0VBGUzbGsqAopc2PNAuoQAnJnF6Fdj12oliugtK2DWQ4A03y5+T6s5/aN4W6kx417yC
sEzaEFZvKJHUpbr081o ja2UKaSbT1TP3Z jJSBYbtPKXfpU3uL8ugtFqnzps/mo802vkgmuTEGfc1pbVD
qfG1h199QmI1Pms1pOE/AxjrvLMqV6WWbEpvR1/232uOWaKe26etnq500MNF jQUQA5LGWZouYMgDSPs=
META@meta1
```

PER VERIFICARE CHE SIA ANDATO A BUON FINE POSSIAMO PROVARE A RIFARE LA  
SCANSIONE SU NESSUS



Qui ho filtrato i plugings, attivando solo quelli che hanno relazione con SSH per risparmiare  
tempo

Name	Schedule	Last Scanned
scansione solo ssh	On Demand	Today at 8:13 AM

Una volta finito possiamo vedere che non c'è più la vulnerabilità

scansione solo ssh

Configure

Audit Trail

Launch

Report

Export

Back to metasploitable2

Hosts 1

Vulnerabilities 17

History 1

Filter

Search Vulnerabilities

17 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count	
HIGH	7.5	5.9	Samba Badlock Vulnerability	General	1	
MIXED	...	...	SSL (Multiple Issues)	General	28	
LOW	2.1 *	4.2	ICMP Timestamp Request Remote Date Disclosure	General	1	
INFO	...	...	TLS (Multiple Issues)	General	4	
INFO	...	...	SSH (Multiple Issues)	General	2	
INFO			Nessus SYN scanner	Port scanners	25	
INFO			Backported Security Patch Detection (FTP)	General	1	
INFO			Backported Security Patch Detection (WWW)	General	1	
INFO			Common Platform Enumeration (CPE)	General	1	
INFO			Device Type	General	1	Modify

Scan Details

Policy: Advanced Scan

Status: Completed

Severity Base: CVSS v3.0


Scanner: Local Scanner

Start: Today at 8:13 AM

End: Today at 8:23 AM

Elapsed: 10 minutes

Vulnerabilities



Critical

High

Medium

Low

Info



## NFS Shares World Readable (High)

Questa vulnerabilità indica che un server NFS remoto sta esportando una o più condivisioni senza limitare l'accesso (in base a hostname, IP o intervallo IP). Ciò significa che le risorse non hanno restrizioni e qualsiasi macchina può accedervi.

Soluzione (suggerita da Nessus)

- Impostare le restrizioni e limitare l'accesso alle condivisioni NFS solo alle macchine autorizzate.

**HIGH** NFS Shares World Readable < >

**Description**  
The remote NFS server is exporting one or more shares without restricting access (based on hostname, IP, or IP range).

**Solution**  
Place the appropriate restrictions on all NFS shares.

**See Also**  
<http://www.tldp.org/HOWTO/NFS-HOWTO/security.html>

**Output**  
The following shares have no access restrictions :  
/ \*

To see debug logs, please visit individual host

Port ▼	Hosts
2049 / tcp / rpc-nfs	192.168.1.13

Adessi seguiamo il suggerimento di Nessus



## Accesso a Metasploitable tramite Kali

```
(kali@kali)-[~]
└─$ ssh -o HostKeyAlgorithms=+ssh-rsa,ssh-dss msfadmin@192.168.1.13
msfadmin@192.168.1.13's password:
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/
No mail.
Last login: Wed May 15 08:11:23 2024
msfadmin@metasploitable:~$
```

## Verifichiamo le exports attuali per vedere le risorse condivise

```
msfadmin@metasploitable:~$ cat /etc/exports
# /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)
#
#
#                *(rw,sync,no_root_squash,no_subtree_check)
msfadmin@metasploitable:~$
```

## Ora dobbiamo editare il file per restringere l'accesso

```
kali@kali: ~
File Actions Edit View Help
GNU nano 2.0.7 File: /etc/exports Modified

# /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)
#
#
#                *(rw,sync,no_root_squash,no_subtree_check)
/home 192.168.1.0/24(rw,sync,no_root_squash,no_subtree_check)
^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is   ^V Next Page  ^U UnCut Text ^T To Spell
```

In questo caso ho permesso l'accesso solo alla rete 192.168.1.0/24. Ora dobbiamo riavviare il server NFS

```
msfadmin@metasploitable:~$ sudo /etc/init.d/nfs-kernel-server restart
* Stopping NFS kernel daemon
... done.
* Unexporting directories for NFS kernel daemon...
... done.
* Exporting directories for NFS kernel daemon...
... done.
* Starting NFS kernel daemon
... done.
msfadmin@metasploitable:~$
```

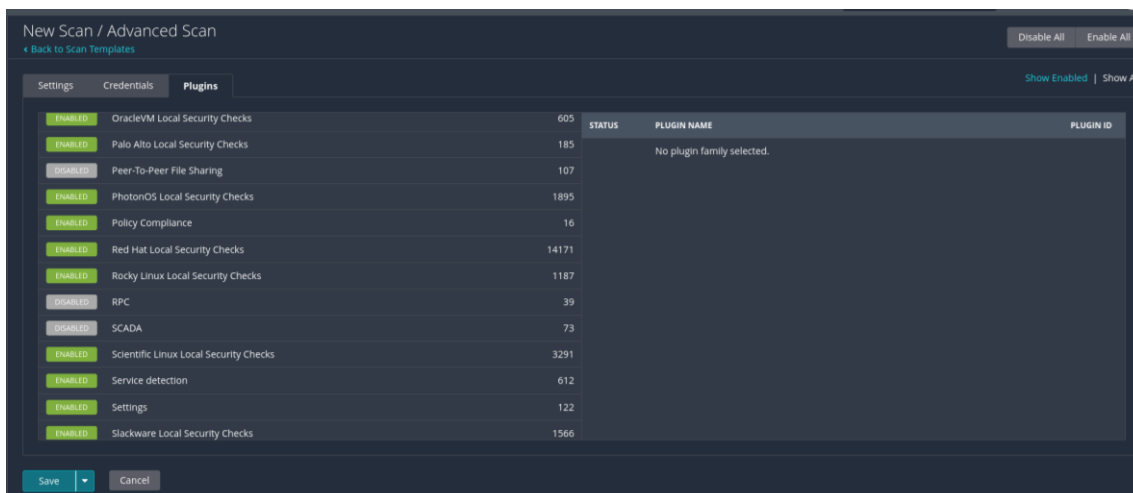
Ci assicuriamo che si siano aggiornate le modifiche:

```
msfadmin@metasploitable:~$ sudo exportfs -v
/home                                192.168.1.0/24(rw,wdelay,no_root_squash,no_subtree_check)
```

Ora per verificare il rimedio di questa vulnerabilità facciamo l'accesso dalla macchina Kali che è nella stessa rete

```
(kali@kali)-[~]
$ sudo mount -t nfs 192.168.1.13:/home /mnt
[sudo] password for kali:
Created symlink /run/systemd/system/remote-fs.target.wants/rpc-statd.service → /usr/lib/systemd/system/rpc-statd.service.
```

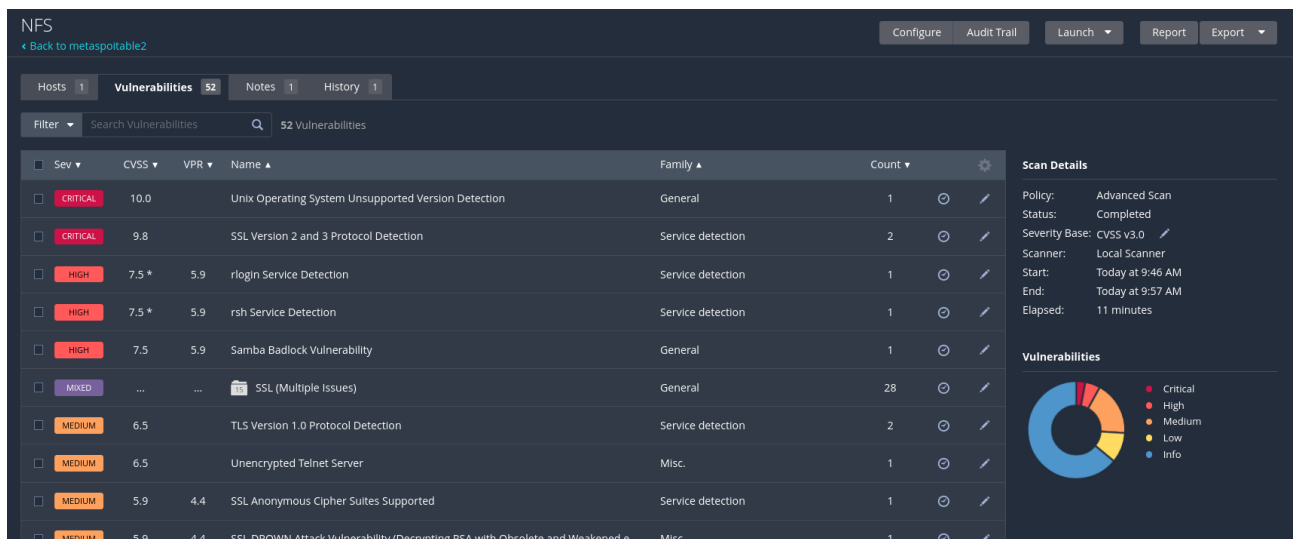
ora possiamo provare a rifare la scansione su Nessus



Qui ho filtrato i plugings, attivando solo quelli che hanno relazione con NFS per risparmiare tempo



Una volta finito possiamo vedere che non c'è più la vulnerabilità



Dopo questa analisi possiamo concludere che le vulnerabilità scelte (Weak Debian OpenSSH Keys in ~/.ssh/authorized\_keys e NFS Shares World Readable) sono state corrette, grazie al programma Nessus è possibile individuarle e risolverle. È consigliabile effettuare un monitoraggio costante per individuare future vulnerabilità e mantenere un ambiente sicuro e privo di rischi.