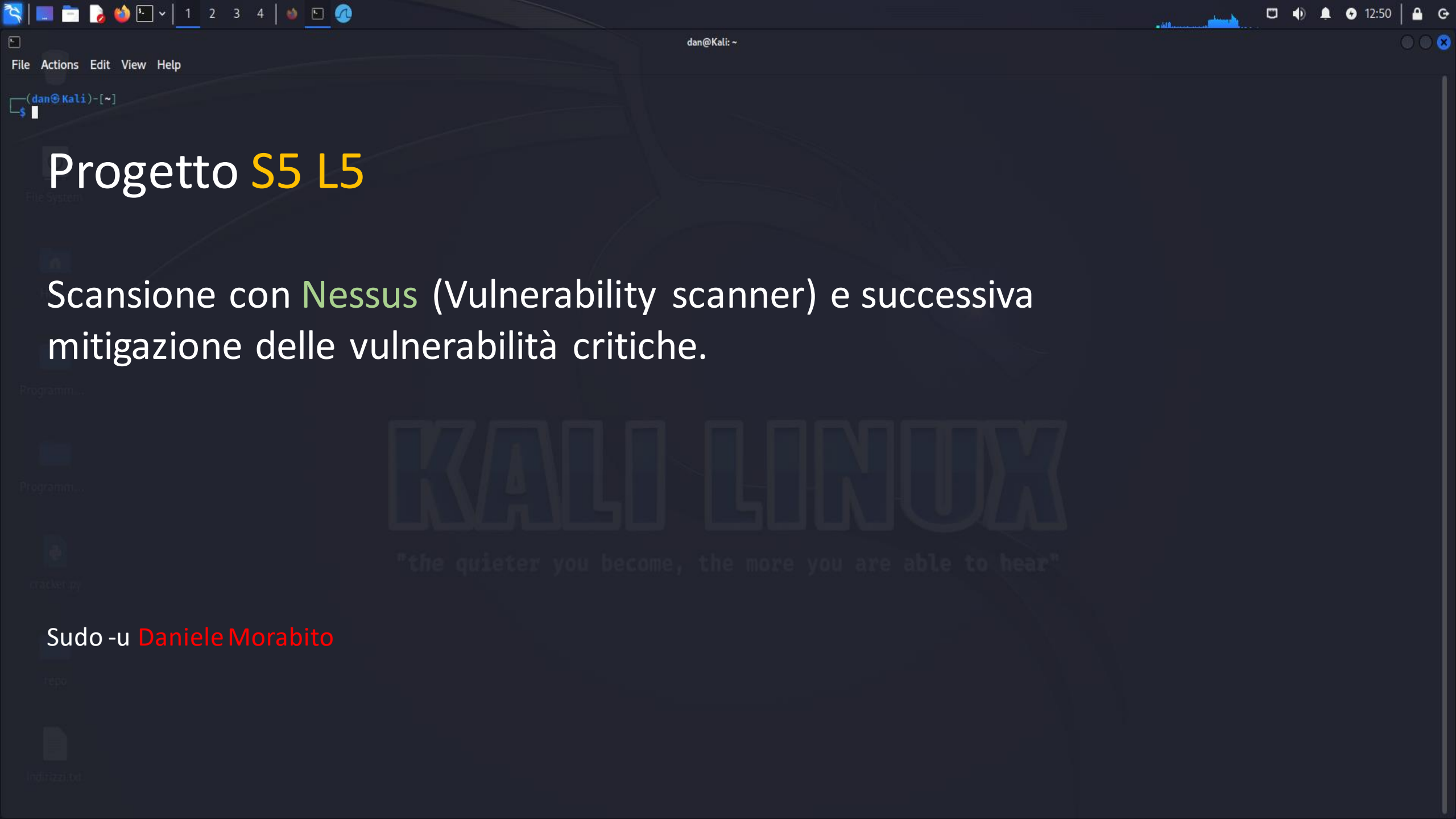
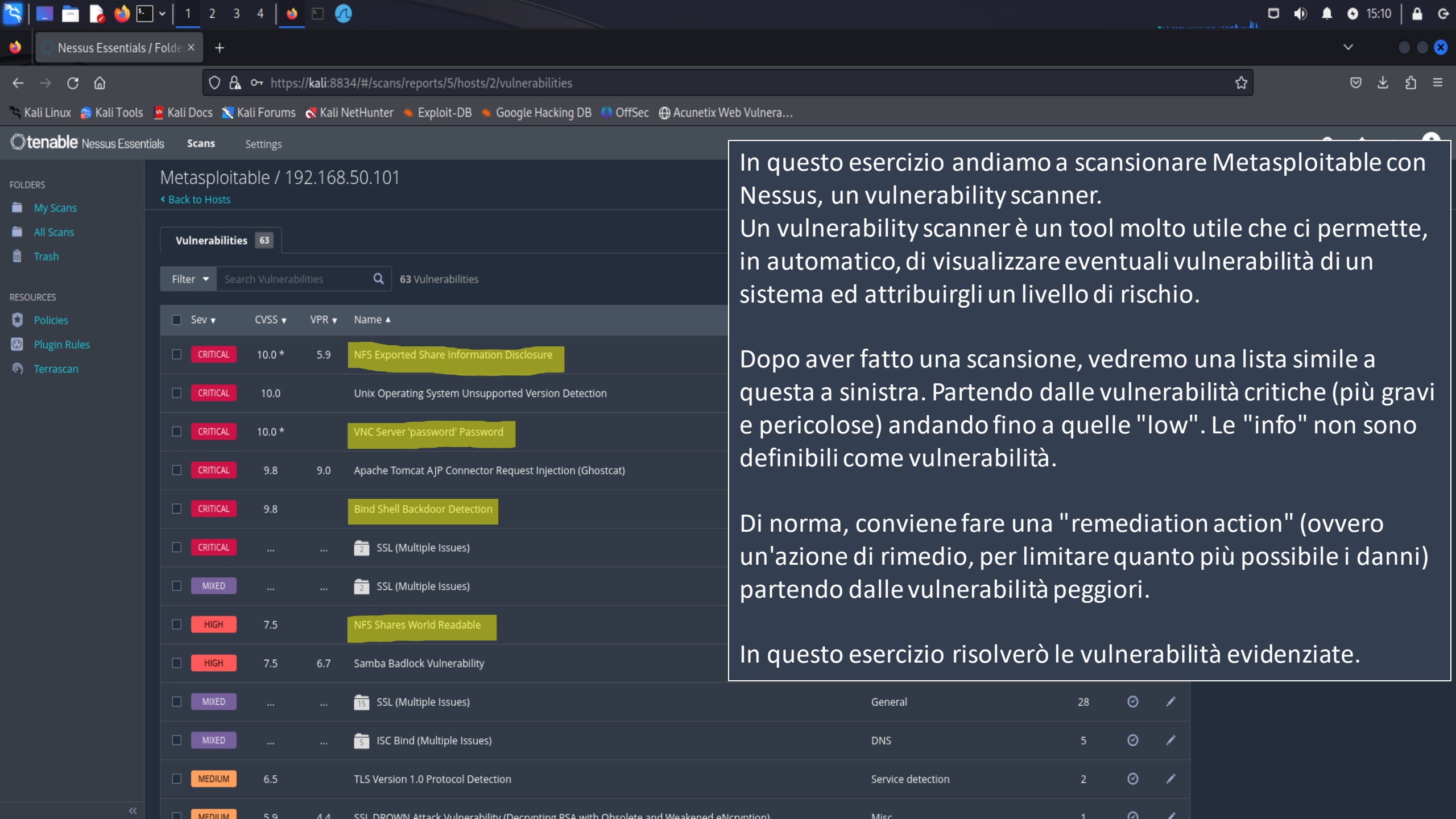

dan@Kali: ~
File Actions Edit View Help
(dan㉿Kali)-[~]
$
Progetto S5 L5
Scansione con Nessus (Vulnerability scanner) e successiva mitigazione delle vulnerabilità critiche.
KALI LINUX
"the quieter you become, the more you are able to hear"
Sudo -u Daniele Morabito



In questo esercizio andiamo a scansionare Metasploitable con Nessus, un vulnerability scanner.
Un vulnerability scanner è un tool molto utile che ci permette, in automatico, di visualizzare eventuali vulnerabilità di un sistema ed attribuirgli un livello di rischio.

Dopo aver fatto una scansione, vedremo una lista simile a questa a sinistra. Partendo dalle vulnerabilità critiche (più gravi e pericolose) andando fino a quelle "low". Le "info" non sono definibili come vulnerabilità.

Di norma, conviene fare una "remediation action" (ovvero un'azione di rimedio, per limitare quanto più possibile i danni) partendo dalle vulnerabilità peggiori.

In questo esercizio risolverò le vulnerabilità evidenziate.

192.168.50.101

8	4	16	6	73
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 107

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	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)
HIGH	7.5	6.7	90509	Samba Badlock Vulnerability
MEDIUM	6.5	3.6	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.9	5.1	136808	ISC BIND Denial of Service

Nessus ci permette, tra l'altro, di generare automaticamente un report delle vulnerabilità, che può essere più o meno dettagliato (in base alle nostre necessità).

Questo a fianco è un esempio di report semplificato. E' il report prima di applicare le azioni di rimedio.

```
  GNU nano 2.0.7                File: /etc/hosts.allow

# /etc/hosts.allow: list of hosts that are allowed to access the system.
#                   See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:    ALL: LOCAL @some_netgroup
#             ALL: .foobar.edu EXCEPT terminalserver.foobar.edu
#
# If you're going to protect the portmapper use the name "portmap" for the
# daemon name. Remember that you can only use the keyword "ALL" and IP
# addresses (NOT host or domain names) for the portmapper, as well as for
# rpc.mountd (the NFS mount daemon). See portmap(8) and rpc.mountd(8)
# for further information.
#

                              [ Read 14 lines ]
^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
```

```
  GNU nano 2.0.7                File: /etc/hosts.deny

# /etc/hosts.deny: list of hosts that are _not_ allowed to access the system.
#                  See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:    ALL: some.host.name, .some.domain
#             ALL EXCEPT in.fingerd: other.host.name, .other.domain
#
# If you're going to protect the portmapper use the name "portmap" for the
# daemon name. Remember that you can only use the keyword "ALL" and IP
# addresses (NOT host or domain names) for the portmapper, as well as for
# rpc.mountd (the NFS mount daemon). See portmap(8) and rpc.mountd(8)
# for further information.
#
# The PARANOID wildcard matches any host whose name does not match its
# address.

# You may wish to enable this to ensure any programs that don't
# validate looked up hostnames still leave understandable logs. In past
# versions of Debian this has been the default.
ALL: ALL

                              [ Read 19 lines ]
^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
```

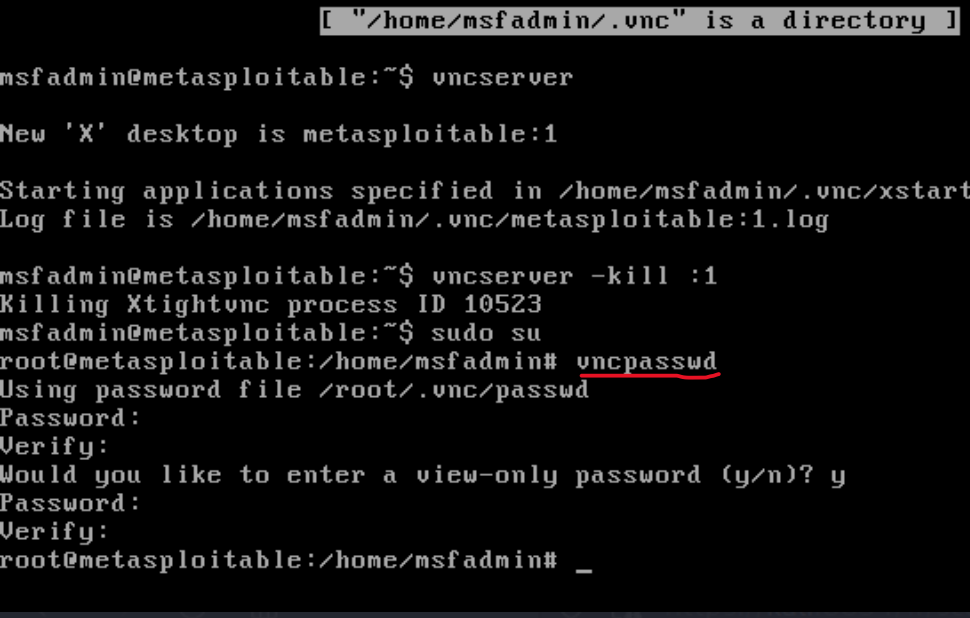
Per prima cosa, andremo a risolvere il problema del NFS (Network File System).
Il Network File System è un "protocollo" per il quale si possono condividere determinate cartelle da remoto, come se fossero disponibili in locale.

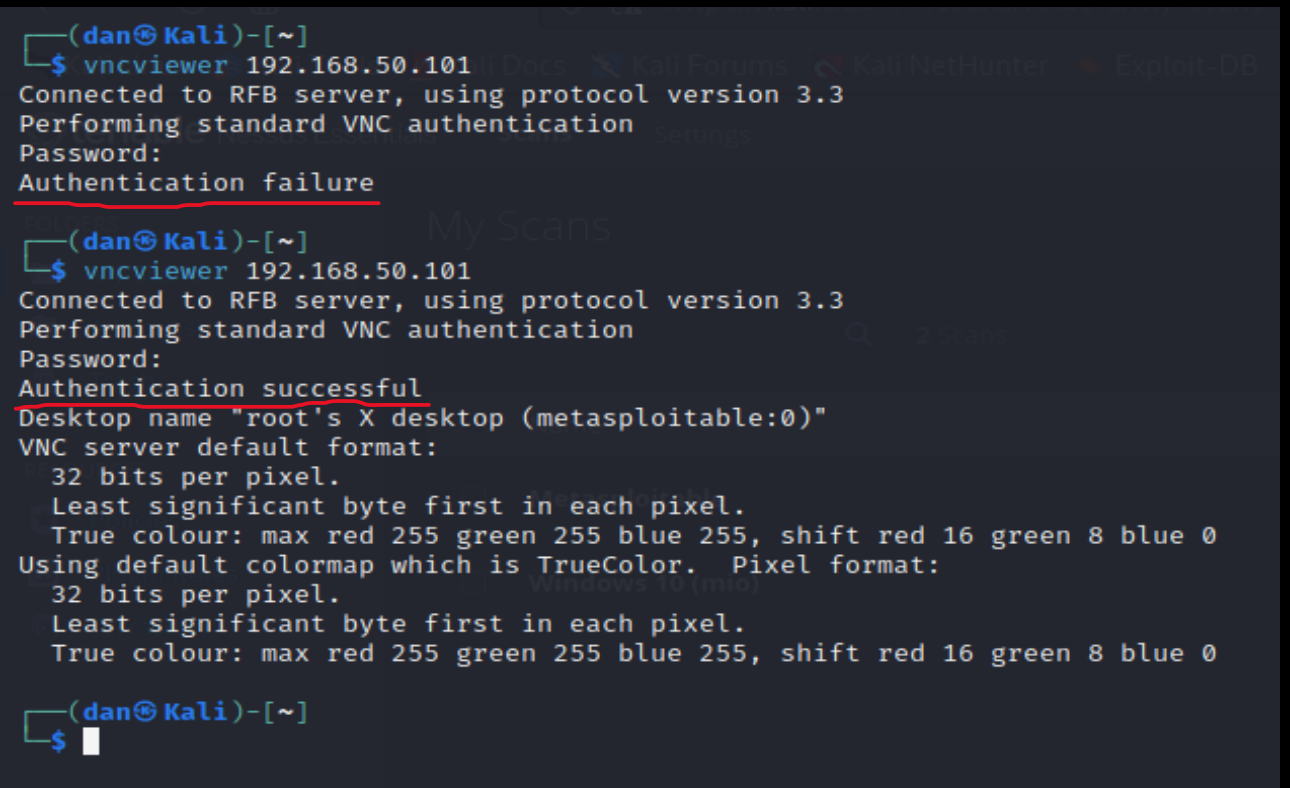
In questo caso, tutto ciò non è regolato correttamente, chiunque, compresi malintenzionati, potrebbero accedervi.

Per risolvere abbiamo a disposizione due file di testo modificabili che ci permettono di gestire l'accesso al NFS.

Il primo, è "hosts.allow", è praticamente una whitelist, ovvero una lista che permette agli utenti definiti in quest'ultima, di ottenere l'accesso.
Il secondo file è "hosts.deny", una blacklist, ovvero una lista che blocca l'accesso agli utenti che sono scritti in quest'ultima.

In questo caso "hosts.allow" ha la priorità su ciò che è scritto su "hosts.deny".
Ho negato l'accesso a qualsiasi host (come si può notare dalla lista in basso su "ALL: ALL"), ma in alternativa potremmo aggiungere un'eccezione dalla lista in alto, la whitelist.





Il secondo problema con cui abbiamo a che fare è il server VNC (Virtual Network Computing).
Il server VNC ci permette di controllare da remoto un determinato dispositivo (un po' come programmi tipo Teamviewer oppure Anydesk, ma più spartano).

Secondo quanto risultato dall'analisi con Nessus, la password per accedere da remoto è veramente basilare, infatti è riuscito ad accedervi semplicemente con "password".

Per cambiarla, ho usato su Metasploitable il comando "vncpasswd" con i privilegi di root, ed ho impostato una password più complessa.

Nell'immagine sotto ho fatto dei test per confermare che tutto funzionasse correttamente. Nella prima parte ho provato a scrivere "password", l'autenticazione non è andata a buon fine (proprio come mi aspettavo).
Nella seconda parte, scrivendo la password che ho scelto, l'autenticazione va a buon fine e ci connette al dispositivo in questione.

La vulnerabilità dovrebbe così esser risolta.

```
root@metasploitable:/home/msfadmin# ufw deny 1524
Rule added
root@metasploitable:/home/msfadmin# ufw default ALLOW
Default policy changed to 'allow'
(be sure to update your rules accordingly)
root@metasploitable:/home/msfadmin# ufw status
Firewall loaded

To                         Action  From
--                         ------  ----
1524:tcp                   DENY    Anywhere
1524:udp                   DENY    Anywhere

root@metasploitable:/home/msfadmin#
```

```
┌──(dan㉿Kali)-[~]
└─$ nmap -sV -p 1524 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-27 14:59 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00024s latency).

PORT     STATE SERVICE   VERSION
1524/tcp open  bindshell Metasploitable root shell

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.17 seconds
```

Pre-Firewall

```
┌──(dan㉿Kali)-[~]
└─$ nmap -sV -p 1524 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-27 14:36 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00026s latency).

PORT     STATE    SERVICE VERSION
1524/tcp filtered ingreslock

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.37 seconds
```

Post-Firewall

Per risolvere la terza ed ultima vulnerabilità critica (ovvero la Backdoor), ho utilizzato UFW (Uncomplicated FireWall), un firewall piuttosto basilare, ma efficace, integrato nei sistemi Linux.

Così facendo ho impostato due regole, un ALLOW di default (onde evitare di bloccare tutte le connessioni) ed un DENY alla porta 1524, ovvero la porta che era stata utilizzata per la backdoor.

La backdoor è molto pericolosa, poiché permetterebbe ad un malintenzionato di ottenere l'accesso al dispositivo senza dover rifare i vari passaggi del Penetration Test.

Sopra si può vedere la seguenza di comandi usati per settare il firewall.
Le due immagini di Kali, al centro e in basso, ci fanno notare la differenza della porta 1524 con la scansione di Nmap.

Nessus Essentials / Folde

https://kali:8834/#/scans/reports/5/vulnerabilities

Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec | Acunetix Web Vulnera...

tenable Nessus Essentials | Scans | Settings | Sk3L7

FOLDERS
- My Scans 1
- All Scans
- Trash

RESOURCES
- Policies
- Plugin Rules
- Terrascan

Metasploitable

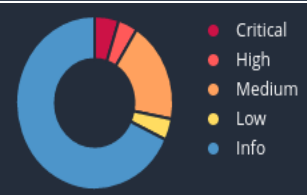
‹ Back to My Scans

Configure | Audit Trail | Launch | Report | Export

Hosts 1 | **Vulnerabilities 45** | Remediations 2 | Notes 2 | History 11

Filter | Search Vulnerabilities | 45 Vulnerabilities

Sev	CVSS	VPR	Name			
CRITICAL	10.0 *	7.4	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL c			
CRITICAL	10.0		Unix Operating System Unsupported Version Detection			
CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)			
MIXED	...	...	2 SSL (Multiple Issues)			
HIGH	7.5	6.7	Samba Badlock Vulnerability			
MIXED	...	...	15 SSL (Multiple Issues)	General	28	
MIXED	...	...	5 ISC Bind (Multiple Issues)	DNS	5	
MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection	2	
MEDIUM	5.9	4.4	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1	
MIXED	...	...	3 HTTP (Multiple Issues)	Web Servers	3	
MIXED	...	...	2 SMB (Multiple Issues)	Misc.	2	
MIXED	...	...	2 TLS (Multiple Issues)	Misc.	2	



Con quest'ultimo scan possiamo già notare che le vulnerabilità evidenziate nella seconda pagina, sono state risolte.

Per sicurezza, creerò un report finale da paragonare con quello mostrato all'inizio.
(Entrambi i report possono essere visualizzati in qualsiasi momento dalla mia repository su GitHub)

Ecco i due report messi a confronto. A sinistra il primo, a destra quello dopo aver preso la remediation action.

192.168.50.101

8	4	16	6	73
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 107

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	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)
HIGH	7.5	6.7	90509	Samba Badlock Vulnerability
MEDIUM	6.5	3.6	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.9	5.1	136808	ISC BIND Denial of Service

192.168.50.101

4	3	15	3	54
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 79

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	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*	7.4	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	6.7	90509	Samba Badlock Vulnerability
MEDIUM	6.5	3.6	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.9	5.1	136808	ISC BIND Denial of Service
MEDIUM	5.9	3.6	31705	SSL Anonymous Cipher Suites Supported
MEDIUM	5.9	4.4	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
MEDIUM	5.9	4.4	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)