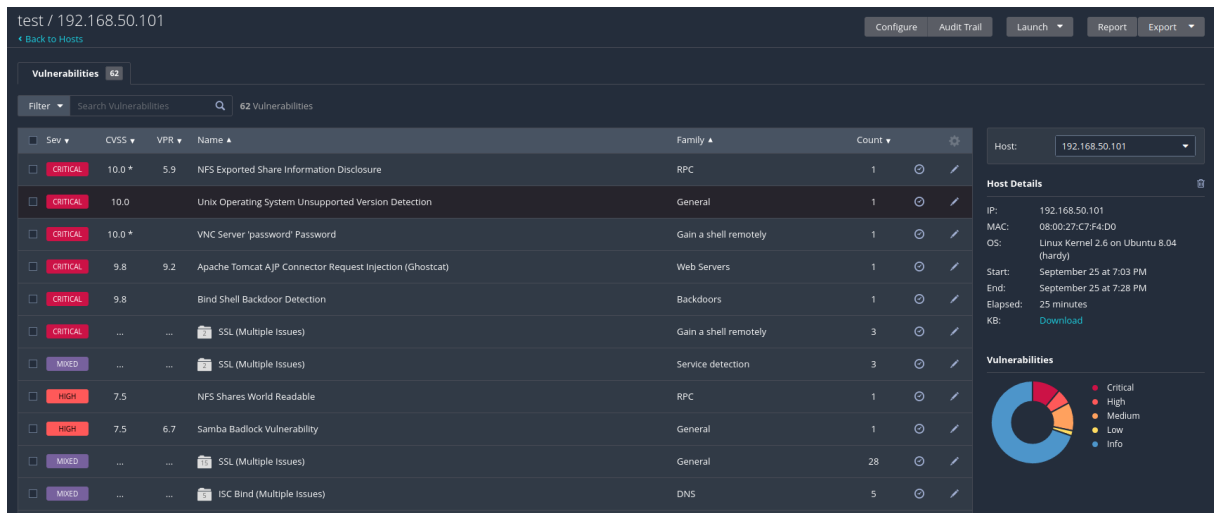


# D8. PT – Attacchi alle Web APP (1)

## Prima scansione con Nessus



Nell'immagine sopra riportata possiamo vedere la scansione effettuata con Nessus dalla macchina Linux(attaccante) alla macchina Metasploitable(vittima). Tra le vulnerabilità richieste dalla traccia dell'esercizio possiamo vedere **NFS Exported Share Information Disclosure**, **VNC Server 'password' Password** e **Bind Shell Backdoor Detenction**. Non è stata invece trovata la vulnerabilità **rexecd Service Detenction**.

## Fase di remediation

La vulnerabilità **NFS Exported Share Information Disclosure** può essere sfruttata da un'attaccante per poter leggere e scrivere file grazie al file system condiviso. Per fixare questa vulnerabilità ho modificato i permessi di lettura e scrittura limitando i permessi solo agli host appartenenti alla rete della macchina Metasploitable.

```
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)
# 192.168.50.0/24(rw, sync)
```

La vulnerabilità **VNC Server 'password' Password** riguarda la password di accesso al server e dove Nessus indica che è troppo debole e che quindi va cambiata. Per motivi puramente pratici e didattici ho scelto una password facile e non sicura ovvero "Vale123!".

```
root@metasploitable:/# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
root@metasploitable:/# _
```

Per quanto riguarda la **Bind Shell Backdoor Detention** ho provveduto ad impostare una regola di firewall impedendo alla macchina metasploitable di ricevere pacchetti TCP sulla porta 1524.

Firewall / Rules / LAN

The changes have been applied successfully. The firewall rules are now reloading in the background.  
[Monitor the filter reload progress.](#)

Floating WAN **LAN**

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 2/1.29 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✗ 0/0 B	IPv4 TCP	*	*	192.168.50.101/24	1524	*	none		blocking kali	
<input type="checkbox"/>	✓ 0/515 B	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	✓ 0/0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add Add Delete Toggle Copy Save Separator

Invece per quanto riguarda la vulnerabilità **rexecd Service Detention** che non è stata trovata ho provveduto comunque ad entrare nel file `inetd.conf` ed ho commentato la linea `exec` per evitare l'esecuzione di comandi da utenti non autenticati.

