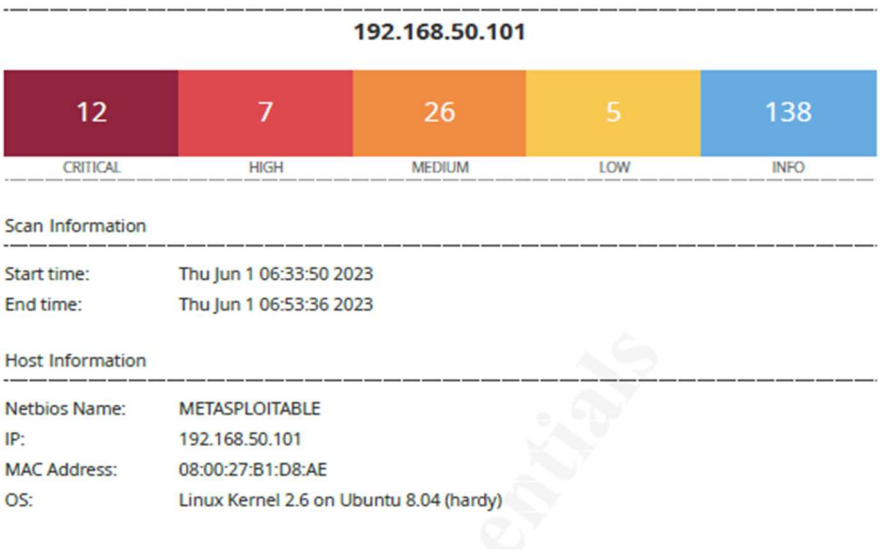
Pierluigi Amorese

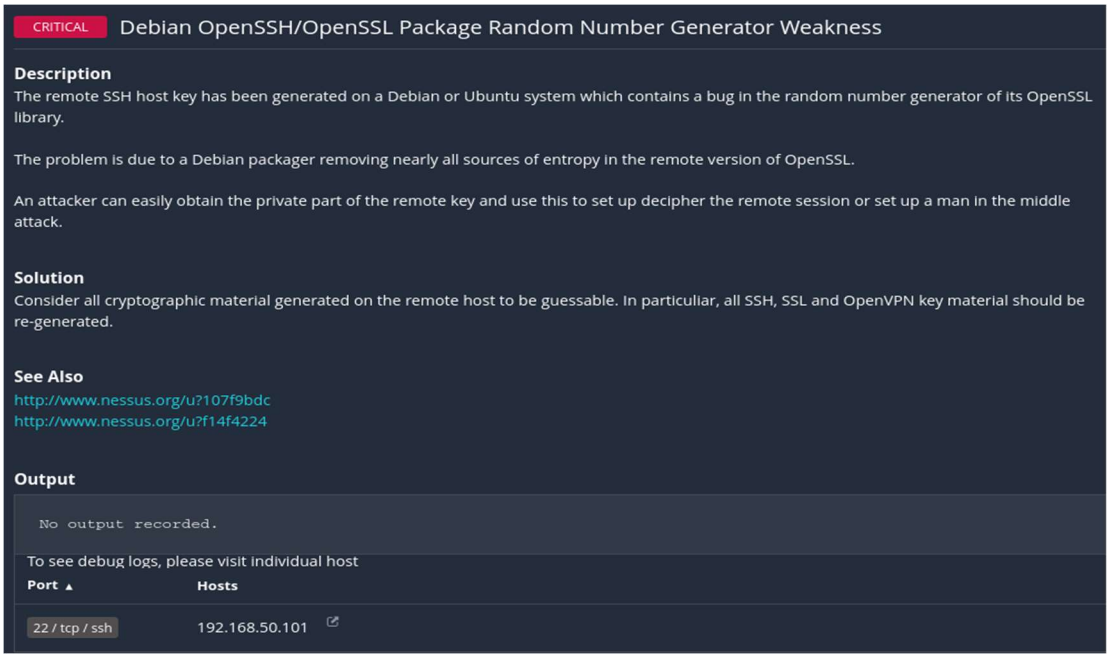
Unit 2: “Remediation actions su Metasploitable 2”

Prima scansione con Nessus:

Con la prima scansione di nessus sono state evidenziate 12 vulnerabilità di livello ***critical.*** In questo report andremo ad analizzare i procedimenti per il risolvimento per alcune di esse.

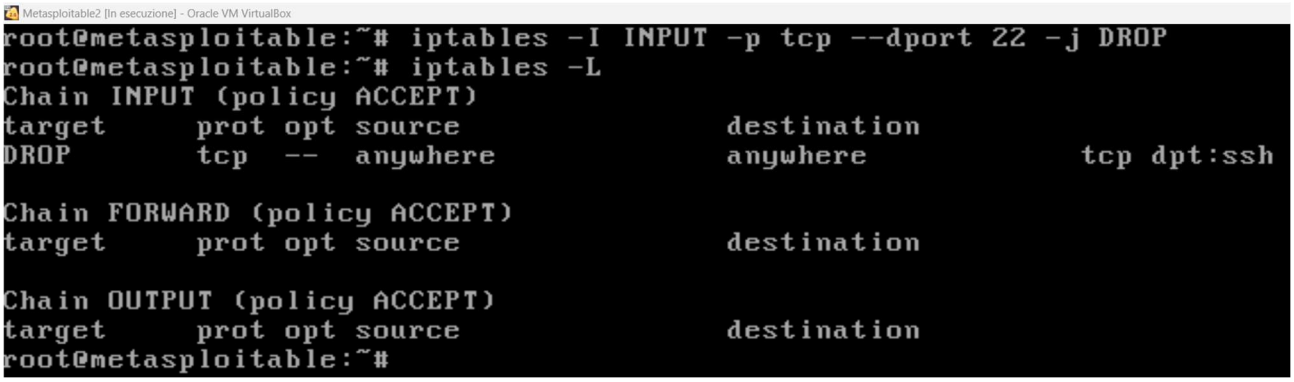


1. La prima vulnerabilità risolta **è Debian OpenSSH/OpenSSL Package Random Number Generator Weakness**.

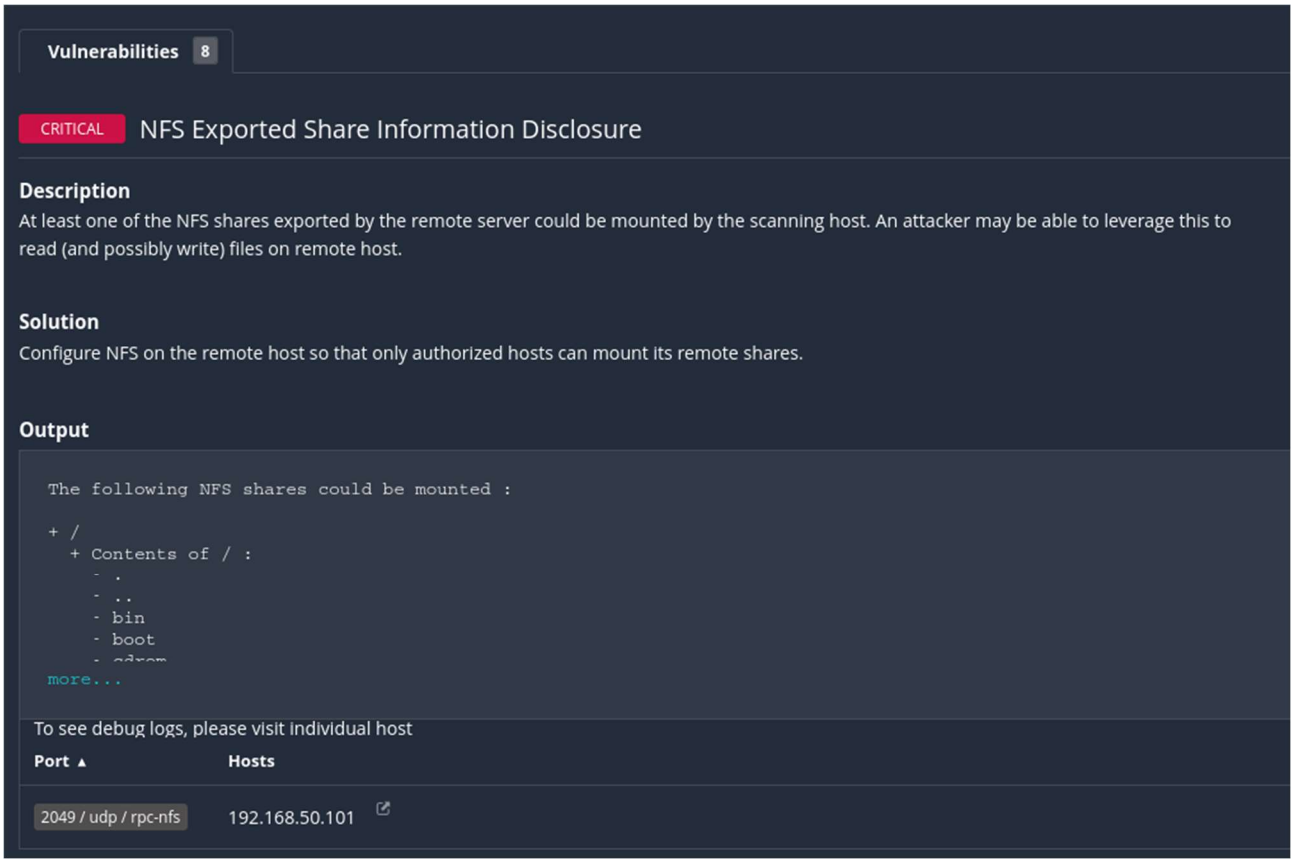


Per questo caso utilizzeremo una regola del firewall. Grazie alla scansione possiamo notare che il processo in questione si trova sulla porta 22 aperta. Per questo dalla macchina Metasploitable 2, con privilegi da superuser (comando *sudo* o come nel mio caso *sudo su*), creiamo la seguente regola per rigettare il traffico in entrata sulla suddetta porta:

iptables -I INPUT -p tcp –dport 22 DROP

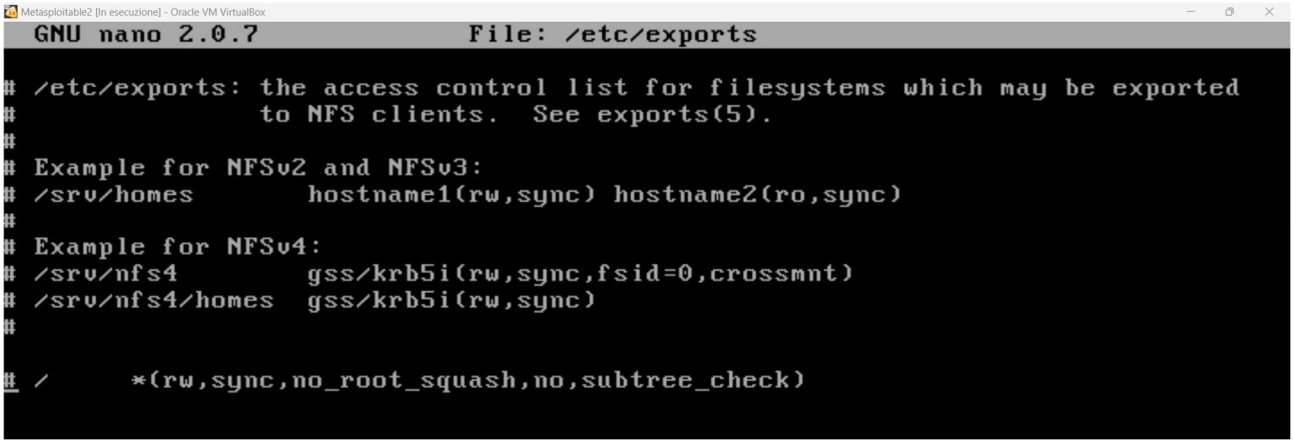


2. Risolveremo adesso la vulnerabilità **NFS Exported** Share Information Disclosure.

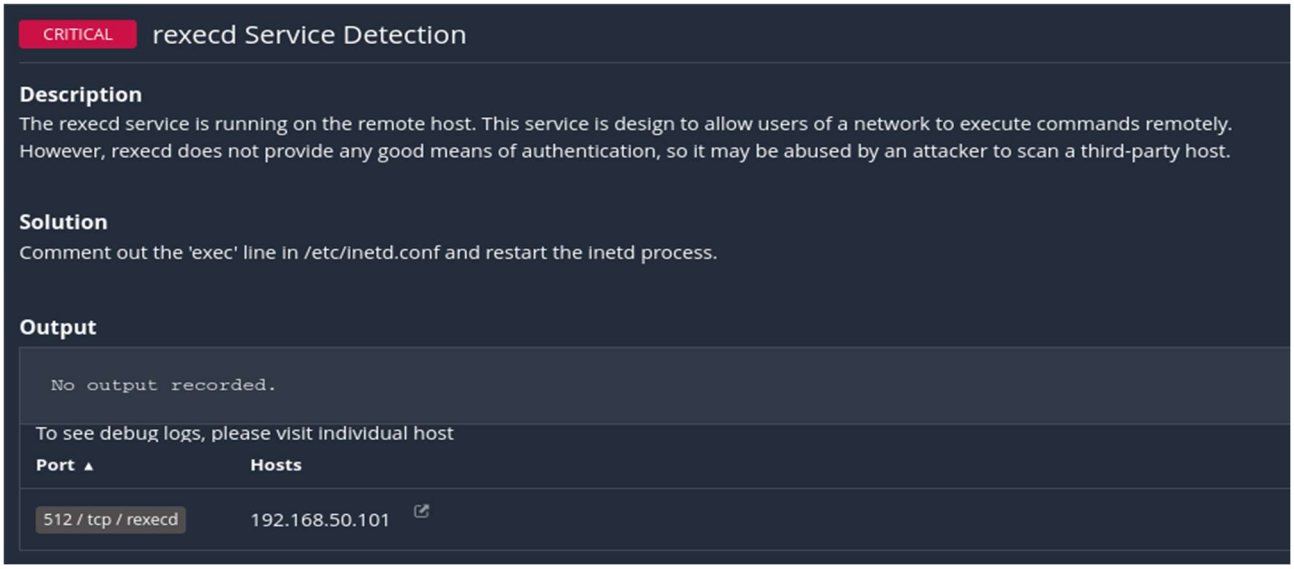


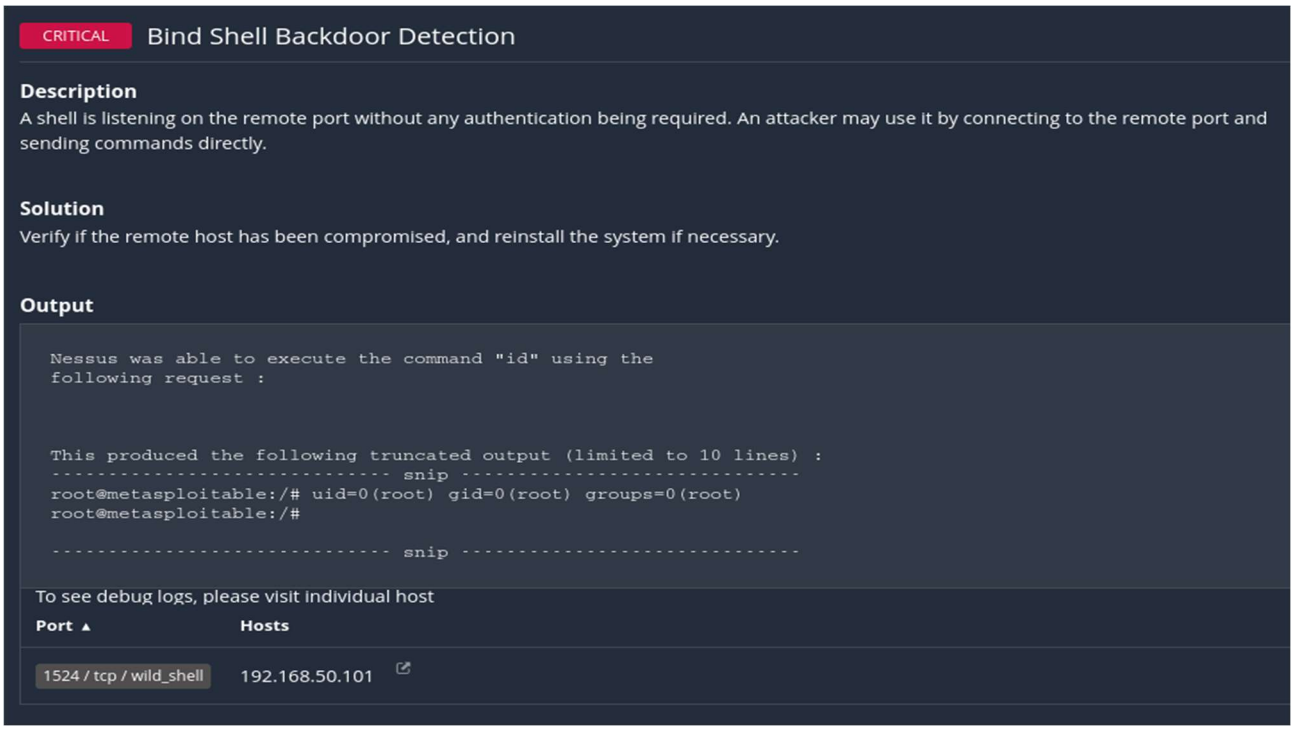
La solution ci suggerisce di configurare la macchina in modo che solo gli host autorizzati possano accedere da remoto tramite la porta 2049 al servizio nfs, che permette di accedere alle NFS directory (che nel nostro caso sono quelle riportate nel campo Output nell’immagine) e volendo anche di leggere e scrivere dati.

Procediamo quindi modificando il file exports presente nella directory /etc commentando semplicemente l'ultima riga del file, che contiene la regola per la condivisione della cartella (e del suo contenuto).



3. e 4. In questo punto risolveremo insieme 2 vulnerabilità allo stesso momento, parliamo **di Bind Shell Backdoor Detection** e di **Rexecd Service Detection**.





Bind Shell Backdoor Detection è un servizio sulla porta 1524 che permette di accedere al sistema da remoto in incognito e senza necessità di autenticazione.

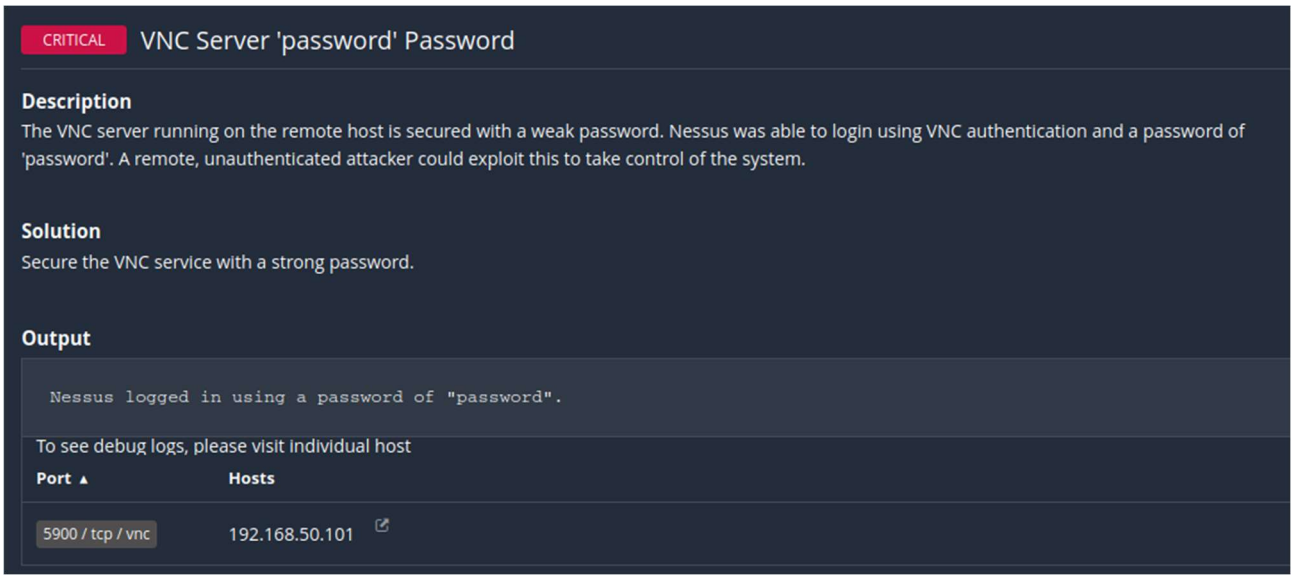
Rexecd Service Detection sulla porta 512 è un servizio che permette agli utenti di una rete di eseguire comandi da remoto.

Procediamo a rimuovere entrambe le vulnerabilità aprendo il file *inetd.conf* presente nella directory /etc e commentiamo la riga “exec” per quanto riguarda il servizio Rexecd e la riga “ingreslock” per la beckdoor.

```
  GNU nano 2.0.7            File: /etc/inetd.conf

#<off># netbios-ssn     stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sb$
telnet          stream  tcp     nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.te$
#<off># ftp             stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sb$
tftp            dgram   udp     wait    nobody  /usr/sbin/tcpd  /usr/sbin/in.tf$
shell           stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rs$
login           stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rl$
#exec            stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.re$
#ingreslock stream tcp nowait root /bin/bash bash -i
```

5. L’ultima vulnerabilità risolta è **VNC Server 'password' Password**



Questo servizio permette di controllare un altro dispositivo da remoto per visualizzarne il contenuto. In questo caso la password per accedere a tale servizio sulla nostra macchina è troppo debole; infatti, Nessus ci avvisa dicendoci che è riuscito ad accedere usando la password: “password”.

Dovremo quindi semplicemente cambiare la password, ne potremo inserire una con massimo 8 caratteri di lunghezza, se proveremo a inserirne una più lunga ci verrà automaticamente troncata.

```
root@metasploitable:/# vncpasswd
Using password file /root/.vnc/passwd
Password:
Warning: password truncated to the length of 8.
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:/# _
```

Terminate le remediation actions abbiamo ridotto significativamente le vulnerabilità del sistema. Come possiamo vedere dalla scansione finale siamo scesi a 5 di levello critical rispetto ai 12 della scansione iniziale.