Remediation Critical Vulnerabilities

192.168.50.101

7	4	17	5	70
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 103

SEVERITY	CVSS V3.0	PLUGIN	NAME
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*	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	61708	VNC Server 'password' Password

- Bind Shell Backdoor Detection

```
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
  status                     show firewall status
  version                    display version information

root@metasploitable:/home/msfadmin# ufw enable 1524
Firewall started and enabled on system startup
root@metasploitable:/home/msfadmin# ufw

Usage: ufw COMMAND

Commands:
  enable                     Enables the firewall
  disable                    Disables the firewall
  default ARG                set default policy to ALLOW or DENY
  logging ARG                set logging to ON or OFF
  allow|deny RULE            allow or deny RULE
  delete allow|deny RULE     delete the allow/deny RULE
  status                     show firewall status
  version                    display version information

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

Per risolvere la prima criticità, entrando con i permessi di Root, ci siamo affidati al comando **UFW (Uncomplicated Firewall)** , un sistema semplificato per la gestione del Firewall, dove siamo andati ad eseguire prima " **ufw default allow "** consentendo il traffico in entrata e di seguito **" ufw deny 1524 "** bloccando così la vulnerabilità riscontrata

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -T5 -sV -p1524 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-25 07:05 EST
Nmap scan report for 192.168.50.101
Host is up (0.0071s latency).

PORT     STATE    SERVICE    VERSION
1524/tcp filtered ingreslock
MAC Address: 08:00:27:ED:A5:B7 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.88 seconds
```

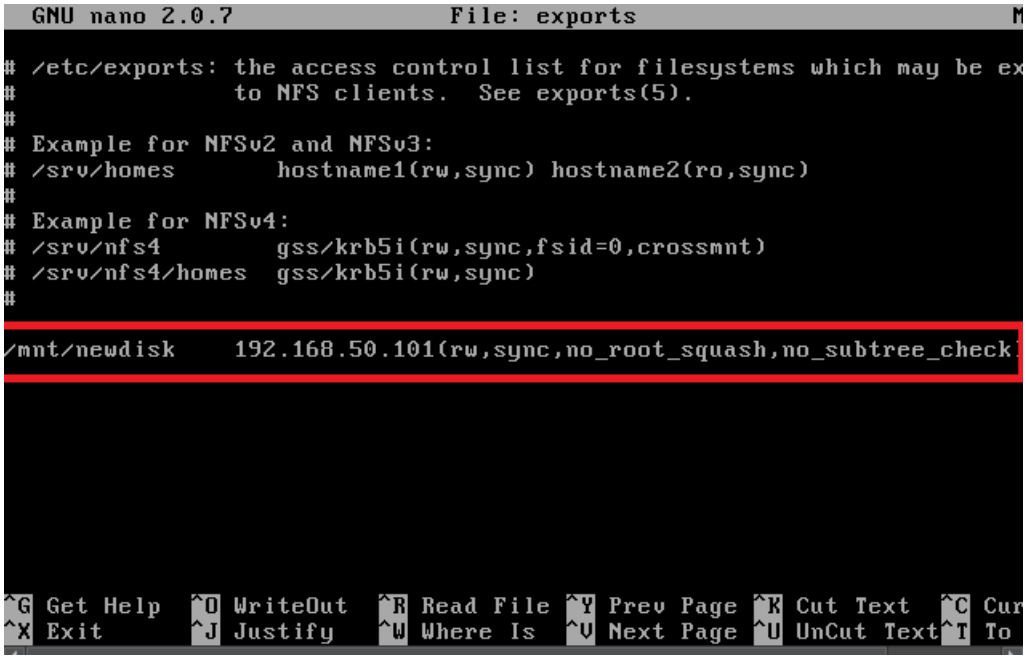
- **1524/tct filtered**

- NFS Exported Share Information Disclosure

Sempre con i permessi di Root attivi, ci spostiamo nella cartella dal **root - etc/nano exports**

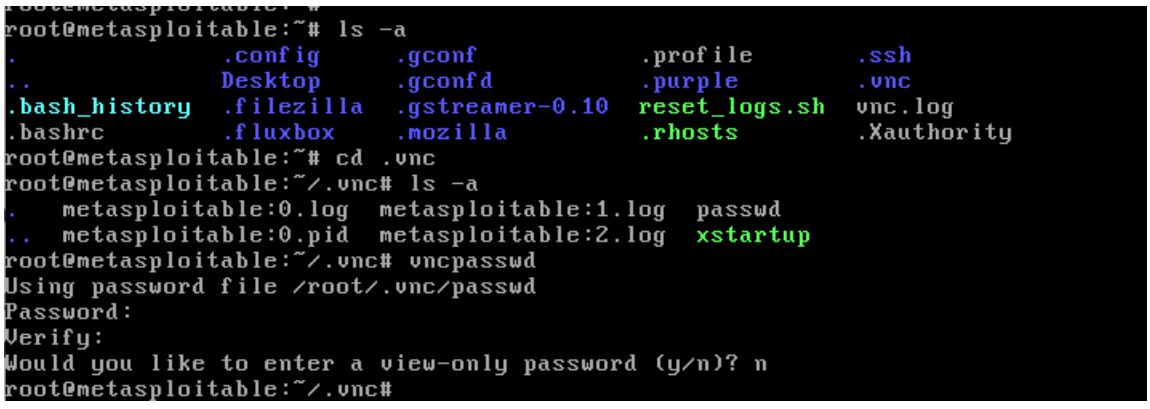
```
root@metasploitable:/etc# nano exports
```

Entrati nel file **exports** andremo ad inserire il comando **/mnt/newdisk** e di conseguenza l'ip di Metasploitable. Così facendo, avremmo configurato in maniera corretta NFS. Riparando la vulnerabilità riscontrata



- VNC Server "password" password

Per questa soluzione, senza mai uscire dai permessi di Root, ci sposteremo nella directory **.vnc** per avviare il comando di conseguenza il comando **vcnpasswd** , questo farà in modo di chiederci una nuova password risolvendo la criticità trovata



- Conclusione

Vulnerabilities Total: 89

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	9.8	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
HIGH	8.6	136769	ISC BIND Service Downgrade / Reflected DoS

Con una nuova scansione si possono notare le criticità risolte.