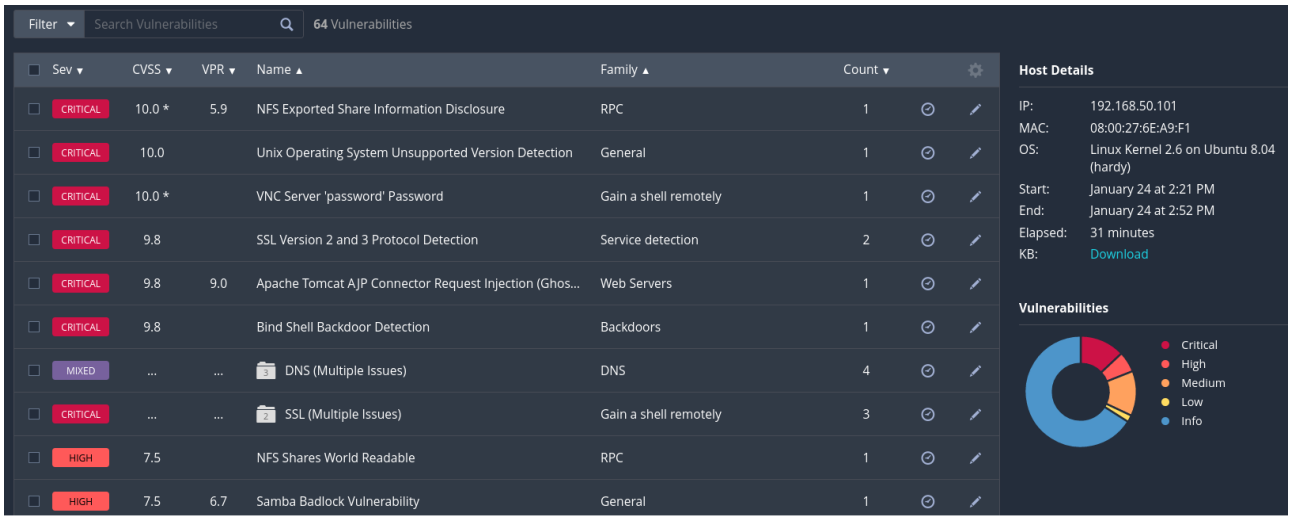
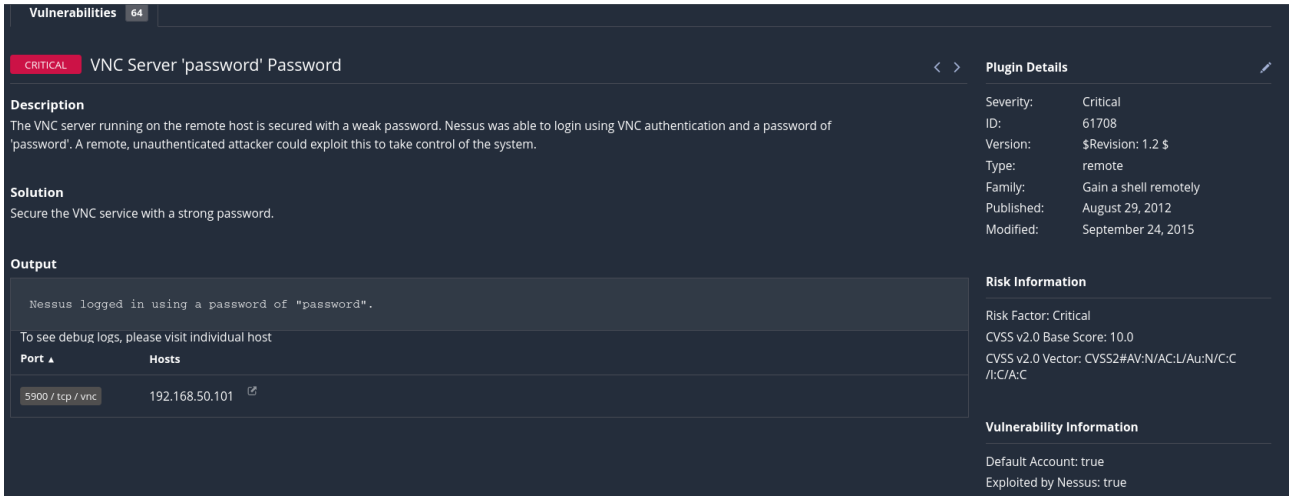
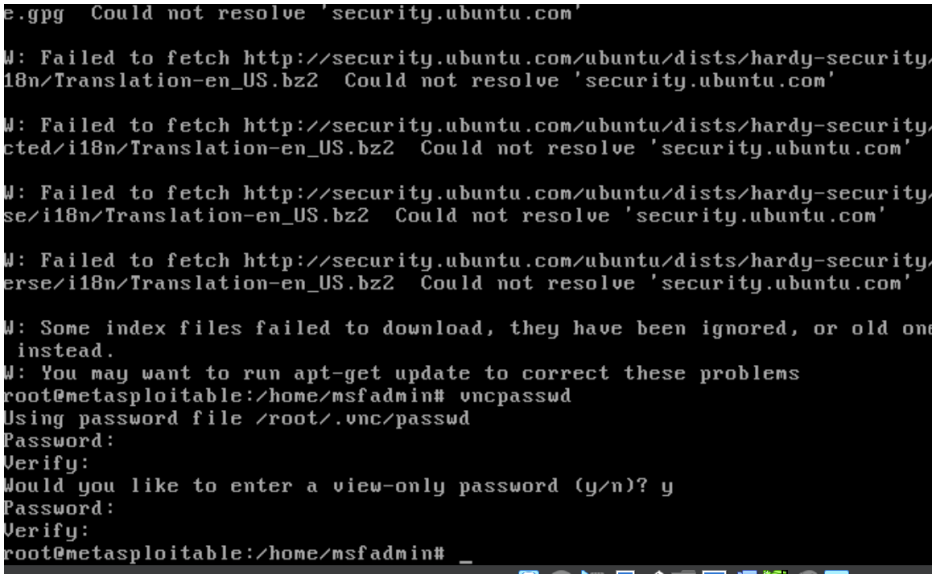
Scansione tramite Nessus e risoluzione vulnerabilità

Ai fini della consegna per il progetto per il Modulo 3 è stata svolta una scansione tramite Nessus sulla macchina target Metasploitable 2 (192.168.32.101), questa ha evidenziato diverse vulnerabilità critiche. Lo scopo dell'esercitazione prevedeva di correggerne 4 o 5.



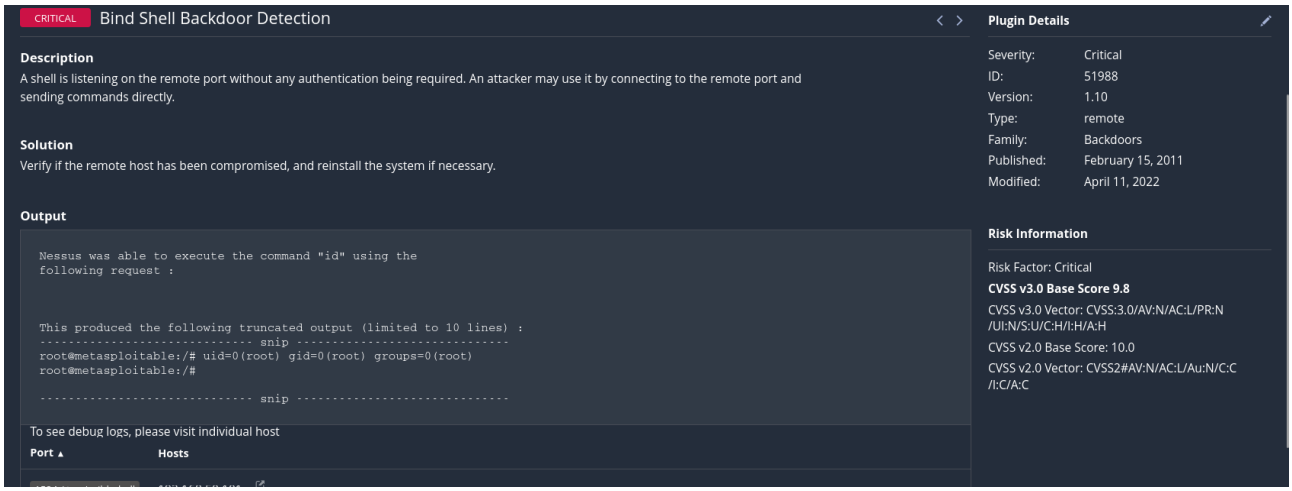

1° Criticità



La prima vulnerabilità ad essere presa in esame è stata la “VNC Server ‘password’ Password”, la soluzione proposta da Nessus richiedeva un cambio di password VNC con una più sicura. Il cambio è stato effettuato direttamente dalla macchina Metasploitable 2: utilizzando i comandi di super amministratore è stato inserito il comando “vncpasswd” per poter cambiare password, la nuova password digitata non risulta visibile sulla shell di metasploit, ma il cambio è avvenuto con successo visto che la successiva scansione con Nessus non ha riportato la vulnerabilità.

2° Criticità




La seconda vulnerabilità risolta è stata la “Bind Shell Backdoor Detection”, Nessus ha rilevato una Backdoor nella shell di Metasploit tramite la porta 1524. Prima di cominciare a risolvere questa criticità è stata eseguita una scansione “nmap -sV 192.168.32.101” evidenziando come la porta 1524 fosse aperta e sfruttabile per eventuali attacchi. Preso atto della situazione è stato lanciato il comando netcat “nc 192.168.32.101 1524” così facendo è stato possibile “sfruttare” la backdoor come root@metasploitable, da qui è stato lanciato il comando “netstat -an | grep 192.168.32.101” per vedere quali utenti fossero in ascolto con determinate porte ed è stata evidenziata una connessione fra Metasploitable e la macchina Kali. Per poter interrompere questa connessione è stata utilizzata la regola firewall “iptables -A INPUT -p tcp –dport 1524 -j DROP”, un successivo lancio di “nmap -sV 192.168.32.101” ha evidenziato la porta 1524 con la dicitura “filtered” chiudendo la connessione fra le due macchine. Una successiva scansione Nessus non ha presentato la criticità “Bind Shell Backdoor Detection”, risultando così essere stata risolta correttamente.

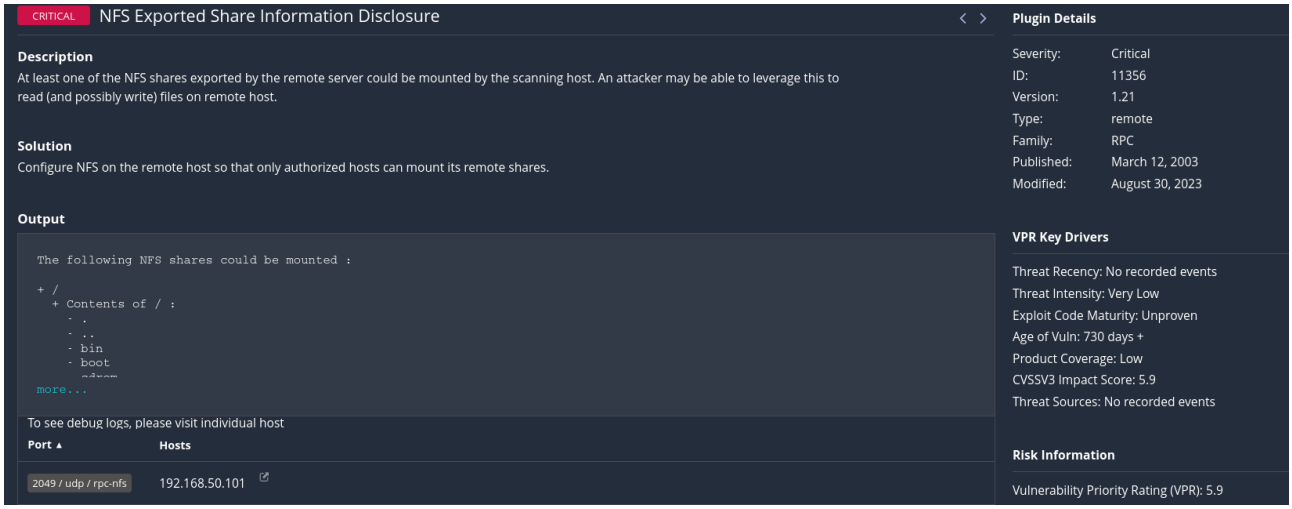
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.32.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-27 11:54 EST
Nmap scan report for 192.168.32.101
Host is up (0.021s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ccproxy-ftp?
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.32.101 1524
root@metasploitable:/# netsta -an | grep 192.168.32.101
bash: netsta: command not found
root@metasploitable:/# netstat -an | grep 192.168.32.101
tcp        0      0 192.168.32.101:53       0.0.0.0:*               LISTEN
tcp        0      0 192.168.32.101:1524     192.168.50.100:35304    ESTABLISHED
tcp       85      0 192.168.32.101:6667     192.168.50.100:47998    ESTABLISHED
udp        0      0 192.168.32.101:137      0.0.0.0:*
udp        0      0 192.168.32.101:138      0.0.0.0:*
udp        0      0 192.168.32.101:53       0.0.0.0:*
udp        0      0 192.168.32.101:36606    192.168.1.254:53        ESTABLISHED
root@metasploitable:/# iptables -P INPUT 1524 DROP
Try `iptables -h' or 'iptables --help' for more information.
Bad argument `DROP'
root@metasploitable:/# iptables -A INPUT -p tcp --dport 1524 -j DROP
root@metasploitable:/# netstat -an | grep 192.168.32.101
```

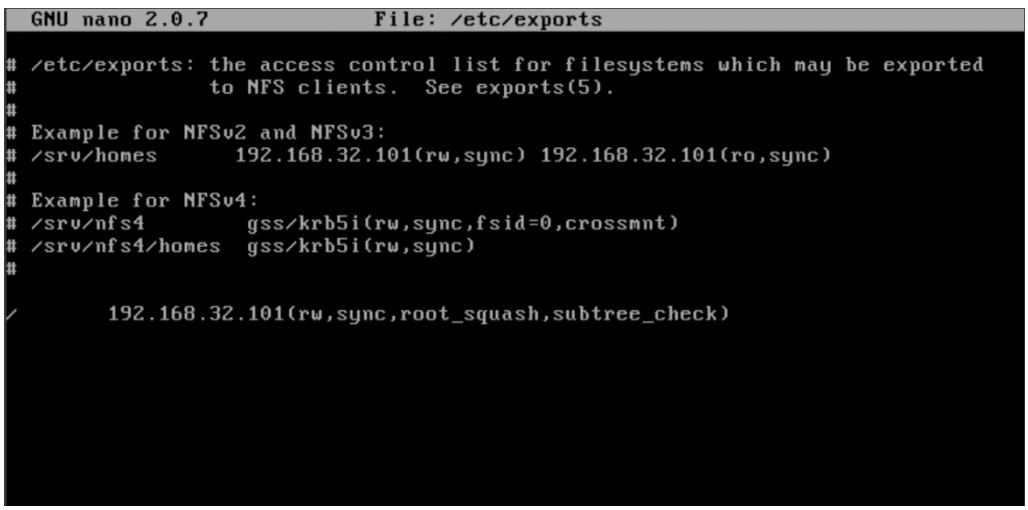
```
Nmap scan report for 192.168.32.101
Host is up (0.021s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE    SERVICE     VERSION
21/tcp   open     ftp         vsftpd 2.3.4
22/tcp   open     ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open     telnet      Linux telnetd
25/tcp   open     smtp        Postfix smtpd
53/tcp   open     domain      ISC BIND 9.4.2
80/tcp   open     http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open     rpcbind     2 (RPC #100000)
139/tcp  open     netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open     netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open     exec        netkit-rsh rexecd
513/tcp  open     login?
514/tcp  open     shell       Netkit rshd
1099/tcp open     java-rmi    GNU Classpath grmiregistry
1524/tcp filtered ingreslock
2049/tcp open     nfs         2-4 (RPC #100003)
2121/tcp open     ccproxy-ftp?
3306/tcp open     mysql?
5432/tcp open     postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open     vnc         VNC (protocol 3.3)
6000/tcp open     X11         (access denied)
6667/tcp open     irc         UnrealIRCd
8009/tcp open     ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open     unknown
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 186.92 seconds
```

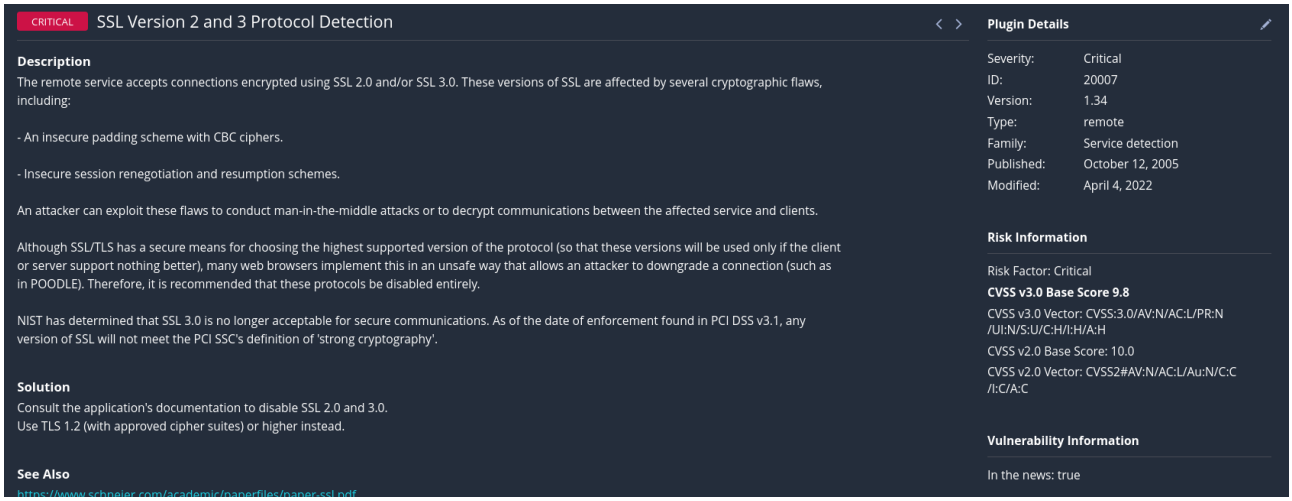
3°Criticità




La terza criticità affrontata risulta essere la “NFS Exported Share Information Disclosure”. Questa vulnerabilità è stata risolta direttamente dalla macchina metasploit entrando e modificando il file /etc/exports dopo aver usato il comando da amministratore “sudo nano /etc/exports”. Dopo essere entrati nel file sono state modificate le voci “hostname 1” e “hostname 2” sostituite con l’IP di Metasploit. È stata effettuata una scansione Nessus per vedere se questa fosse stata risolta, ma dopo essere stata rilevata nuovamente si è proceduto con il sostituire “*” con l’IP Metasploit e sono stati rimossi le voci “no_” fra parentesi. Una successiva scansione Nessus non ha più rilevato la criticità lasciando intendere che fosse stata risolta.

## 4° Criticità




La quarta vulnerabilità critica identificata riguarda la “SSL Version 2 and 3 Protocol Detection”, la corretta risoluzione è stata effettuata dal browser Mozilla Firefox direttamente dalla macchina Kali. Nella barra di ricerca è stato inserito il testo “about:config”, accettato il rischio è stato inserito “tls” nella nuova barra di ricerca della pagina e modificato il valore da “3” a “0” della voce “security.tls.version.min”. Una nuova scansione non ha rilevato la criticità, risultando così risolta.