

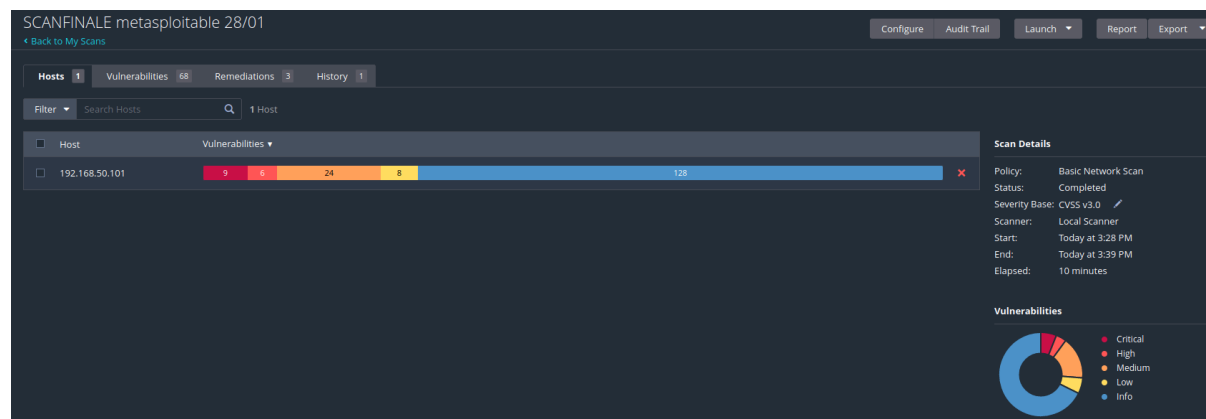
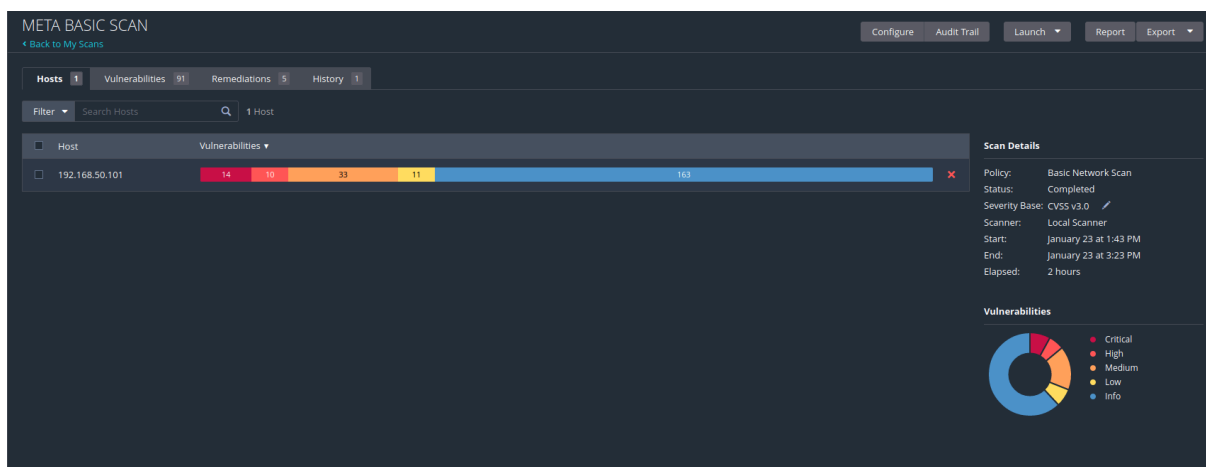
Progetto Modulo 3

Le vulnerabilità corrette sono in totale 4

- 61708 - VNC Server 'password' Password
- 11356 - NFS Exported Share Information Disclosure
- 171340 - Apache Tomcat SEoL (<= 5.5.x)
- 51988 - Bind Shell Backdoor Detection

Rispetto alla prima scansione effettuata da Nessus “META BASIC SCAN” (ScansioneInizio.pdf) nella scansione finale (ScansioneFine.pdf) le vulnerabilità prese in esame, non risultano più presenti e quindi sono state corrette.

Rispetto alla prima scansione, Nessus ha rilevato 5 vulnerabilità in meno ma ne ha aggiunte altre rispetto alla prima scansione fatta con gli stessi parametri.



10. 61708 - VNC Server 'password' Password

Severity: **CRITICAL**

CVSS v3.0 Base Score **10.0**

Descrizione e Danno

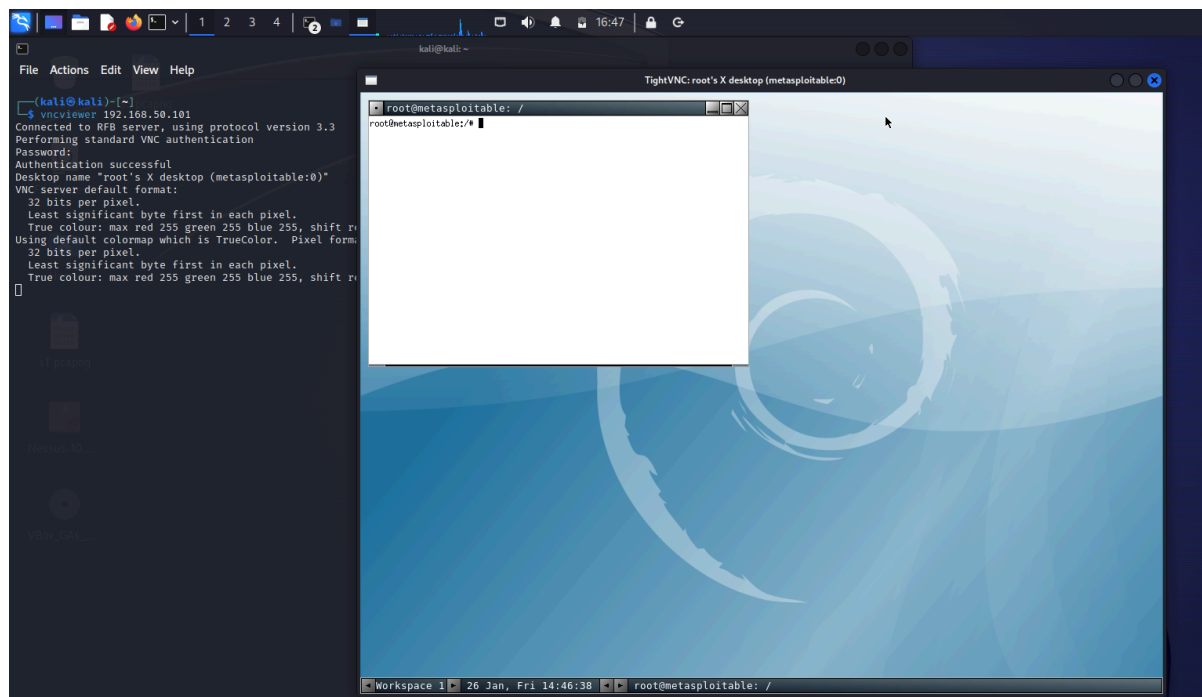
Il server VNC in esecuzione sull'host remoto è protetto da una password poco sicura. un Malintenzionato potrebbe prendere il controllo del sistema.

Contromisure

Mettere in sicurezza il servizio VNC con una password più forte e se possibile, un autenticazione a più fattori.

Implementazione azione di rimedio

Da Terminale Kali lancio il comando **"vncviewer"** per avviare il client VNC e connettermi al server VNC remoto. Inserisco la password **"password"** per testare la vulnerabilità.



Per comodità torno su meta e lancio il comando **"sudo su"** per ottenere accesso da superutente (root) e lancio il comando **"vncpasswd"** per cambiare la password.

```

You will require a password to access your desktops.
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
xauth: creating new authority file /home/msfadmin/.Xauthority

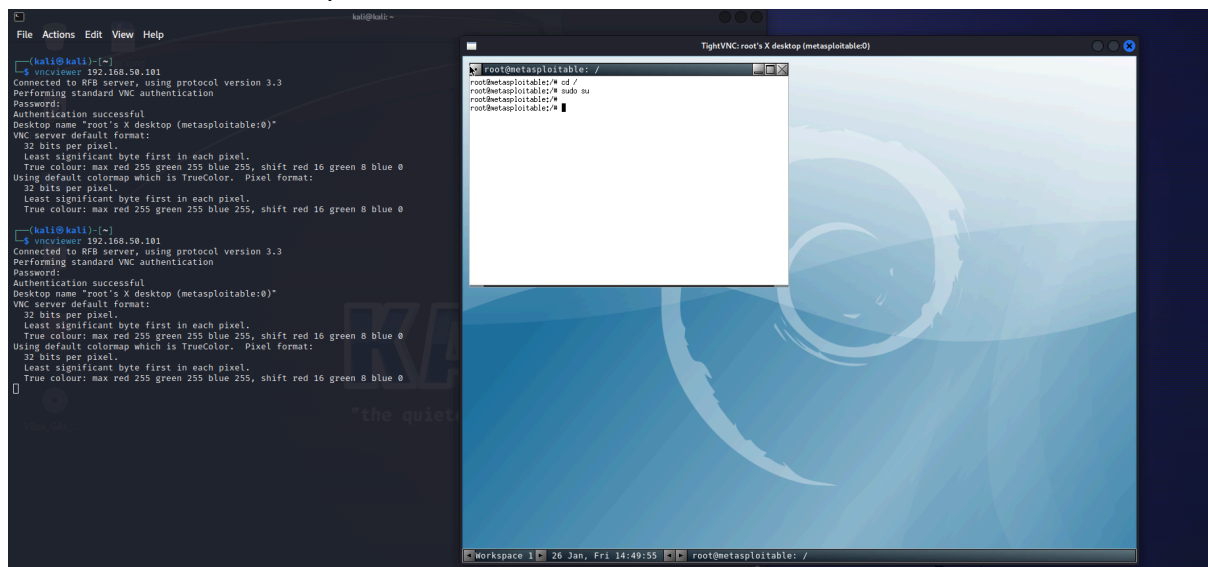
New 'X' desktop is metasploitable:1

Creating default startup script /home/msfadmin/.vnc/xstartup
Starting applications specified in /home/msfadmin/.vnc/xstartup
Log file is /home/msfadmin/.vnc/metasploitable:1.log

msfadmin@metasploitable:/root$ cd /
msfadmin@metasploitable:/root$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/root# 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)? y
Password:
Verify:
root@metasploitable:/root#

```

Da kali verifico il cambio password accedendo nuovamente al servizio.



11356 - NFS Exported Share Information Disclosure

Severity: **CRITICAL**

CVSS v3.0 Base Score **10.0**

Descrizione e Danno

Una delle condivisione NFS esportate da un servizio remoto potrebbe essere montata senza autenticazione. Un attaccante potrebbe sfruttare questa vulnerabilità per accedere e

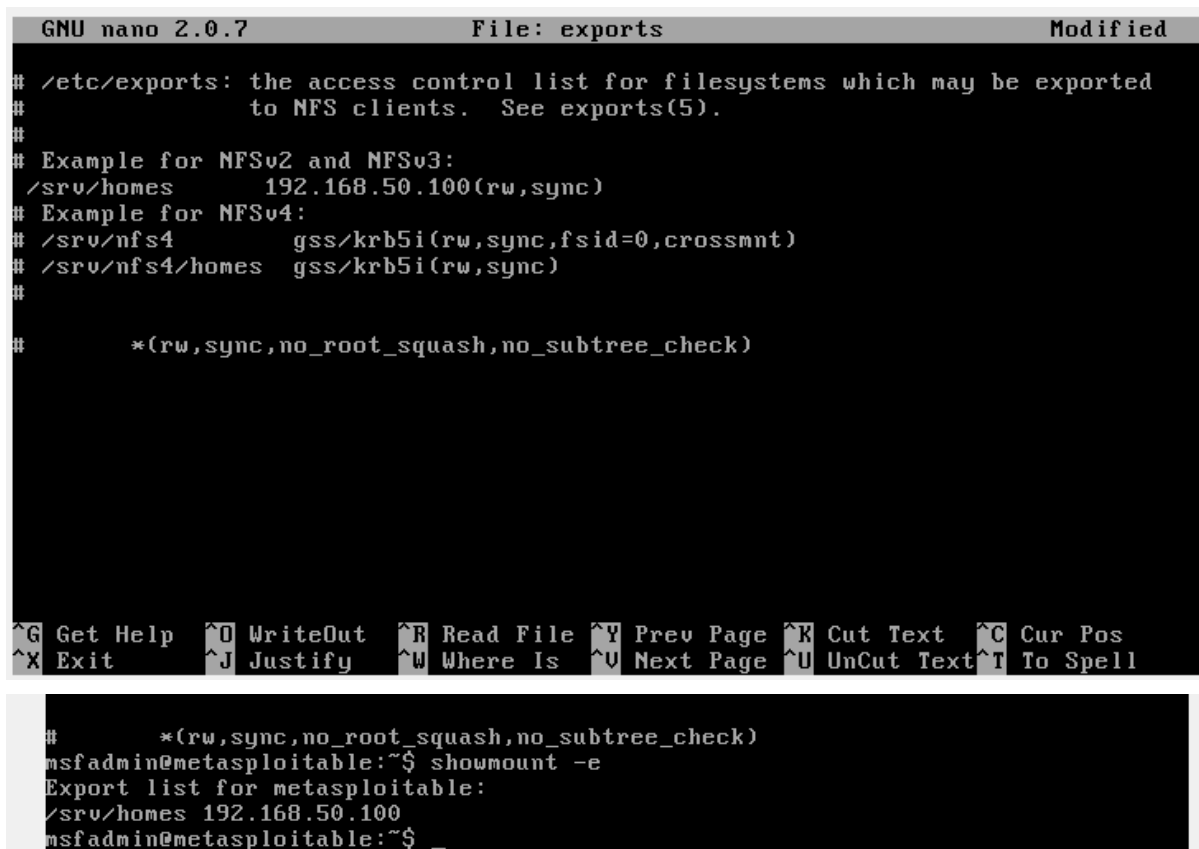
manipolare file o risorse remote ottenendo il permesso di lettura e scrittura senza la necessità di autenticarsi. In pratica, permette all'attaccante di eseguire operazioni di scrittura e lettura non autorizzate su risorse condivise NFS.

Contromisure

Configurare correttamente l'autenticazione e l'autorizzazione per limitare l'accesso non autorizzato alle risorse NFS.

Implementazione azione di rimedio

Da Metasploitable lancio il comando `showmount -e` per visualizzare le info sugli exports NFS e risultava essere configurato con una wildcard (*) e con tutti i permessi. Ho usato il comando **"`sudo nano /etc/exports`"** per aprire l'editor di testo del file dove è presente la configurazione degli exports NFS e commento la stringa `*(rw,sync,no_root_squash,no_subtree_check)` e aggiungo `/srv/home 192.168.50.100(rw,sync)` per dare limitare l'autorizzazione alla sola macchina kali con permessi di lettura-scrittura. Verifico poi nuovamente con il comando `showmount -e`.



```
GNU nano 2.0.7      File: 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      192.168.50.100(rw,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)

^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

#
#      *(rw,sync,no_root_squash,no_subtree_check)
msfadmin@metasploitable:~$ showmount -e
Export list for metasploitable:
/srv/homes 192.168.50.100
msfadmin@metasploitable:~$ _
```

51988 - Bind Shell Backdoor Detection

Severity: **CRITICAL**

CVSS v3.0 Base Score **9.8**

Descrizione e Danno

Questa vulnerabilità indica che c'è una shell in ascolto su una porta remota senza che venga richiesta autenticazione. Ciò significa che un possibile attaccante potrebbe connettersi a questa porta e inviare comandi senza doversi autenticare e ottenere il controllo del sistema.

Contromisure

Verificare se l'host è compromesso e reinstallare il sistema se necessario. Implementare misure di sicurezza come l'autenticazione per limitare l'accesso non autorizzato.

Implementazione azione di rimedio

Con la scansione Nmap posso notare che la vulnerabilità si trova sulla porta 1524 e con il comando netcat confermo la vulnerabilità (la connessione con la porta va a buon fine):

```
File Actions Edit View Help
(kali@kali)-[~]
└─$ nc 192.168.50.101 1524
root@metasploitable:/#
```

Con una ricerca Online trovo informazioni sulla porta e sui servizi attivi cioè ingreslock e dove si trova il suo file di configurazione inetd.conf.

https://pt.wikipedia.org/wiki/Lista_de_portas_dos_protocolos_TCP_e_UDP

In root apro l'editor di testo del file **etc/inetd.conf** e trovo il servizio ingreslock e lo commento per renderlo inattivo. Provo nuovamente ad accedere alla porta con netcat 192.18.50.101 1524 e ho come risultato connessione rifiutata.

```
GNU nano 2.0.7 File: /etc/inetd.conf Modified
#<off># netbios-ssn    stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.telnetd
#<off># ftp           stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.tftpd
#<off># shell         stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rshd
#<off># login         stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rlogind
#<off># exec          stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rexecd
#ingreslock stream tcp nowait root /bin/bash bash -i

File Actions Edit View Help
(kali@kali)-[~]
└─$ nc 192.168.50.101 1524
(UNKNOWN) [192.168.50.101] 1524 (ingreslock) : Connection refused
(kali@kali)-[~]
```

171340 - Apache Tomcat SEoL (<= 5.5.x)

Severity: **CRITICAL**

CVSS v3.0 Base Score **10.0**

Descrizione e Danno

La seguente versione di Apache Tomcat è inferiore alla versione 5.5.x. questa versione non è più supportata o mantenuta dal fornitore e questo implica che non verranno più rilasciati nuovi patch di sicurezza.

In assenza di aggiornamenti di sicurezza, il software potrebbe contenere o sviluppare vulnerabilità nel tempo.

Contromisure

Fare un Upgrade di Apache Tomcat che sia mantenuta attivamente e aggiornata con i patch più recenti.

Implementazione azione di rimedio

In questo caso, è stata applicata la remediation più veloce cioè è stata impostata una regola Firewall con Iptables.

Dopo essermi accertata su quale porta fosse attivo il servizio (8180), ho applicato la regola firewall **“sudo iptables -I INPUT -p tcp --dport 8180 -j DROP”** da macchina Meta così da rigettare il traffico in entrata sulla porta 8180.

```
msfadmin@metasploitable:~$ nmap -sV 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-28 13:39 EST
Nmap scan report for 192.168.50.101 (192.168.50.101)
Host is up (0.024s latency).
Not shown: 978 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        netkit-rsh rexecd
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.09 seconds

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ sudo iptables -I INPUT -p tcp --dport 8180 -j DROP
[sudo] password for msfadmin:
msfadmin@metasploitable:~$ sudo reboot
```