





Remediation report

Risolvere 4 vulnerabilità critiche delle seguenti:

<input type="checkbox"/>	CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1
<input type="checkbox"/>	CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1
<input type="checkbox"/>	CRITICAL	10.0 *	7.4	UnrealIRCd Backdoor Detection	Backdoors	1
<input type="checkbox"/>	CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1
<input type="checkbox"/>	CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2
<input type="checkbox"/>	CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1
<input type="checkbox"/>	CRITICAL	 SSL (Multiple Issues)	Gain a shell remotely	3
<input type="checkbox"/>	MIXED	 Apache Tomcat (Multiple Issues)	Web Servers	3
<input type="checkbox"/>	HIGH	7.5		NFS Shares World Readable	RPC	1
<input type="checkbox"/>	HIGH	7.5 *	5.9	rlogin Service Detection	Service detection	1
<input type="checkbox"/>	HIGH	7.5 *	5.9	rsh Service Detection	Service detection	1
<input type="checkbox"/>	HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1
<input type="checkbox"/>	MIXED	 SSL (Multiple Issues)	General	28
<input type="checkbox"/>	MIXED	 ISC Bind (Multiple Issues)	DNS	5
<input type="checkbox"/>	MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection	2

N.B causa problema con pfsense ho dovuto ri-effettuare la configurazione del firewall , dunque gli ip variano:

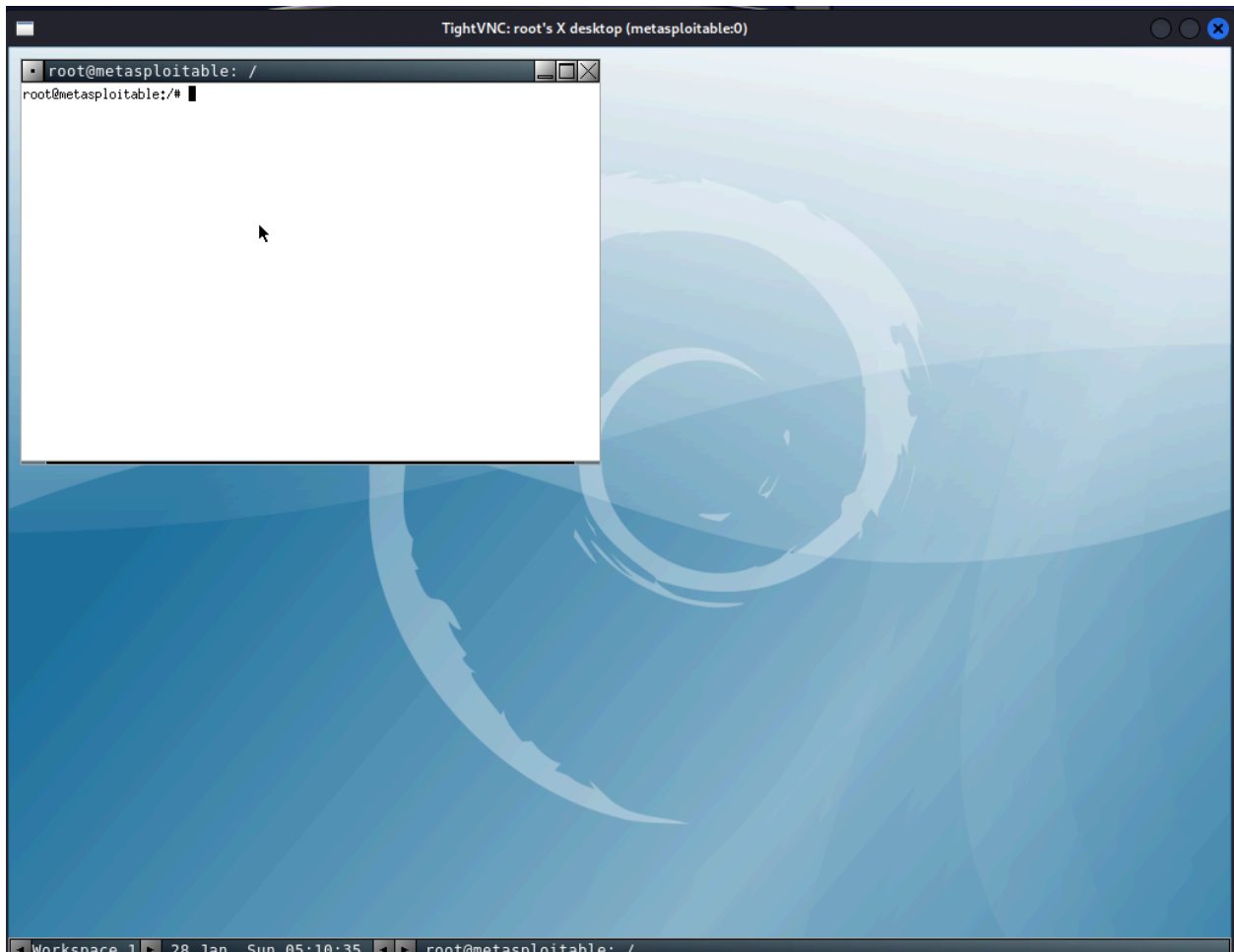
192.169.1.101 prima scansione

192.168.50.100 seconda scansione post riconfigurazione

VNC Pass=password

usando vnc viewer colleghiamoci a meta per verificare il problema ,
useremo la password "password"

```
(toss@upsie)-[~]  
$ vncviewer 192.168.50.100  
Connected to RFB server, using protocol version 3.3  
Performing standard VNC authentication  
Password:
```



andiamo su kali , accediamo come root e cambiamo password

```
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
Sorry, try again.
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password:
```

digitiamo adesso la password attuale
e successivamente inseriamo la nuova password

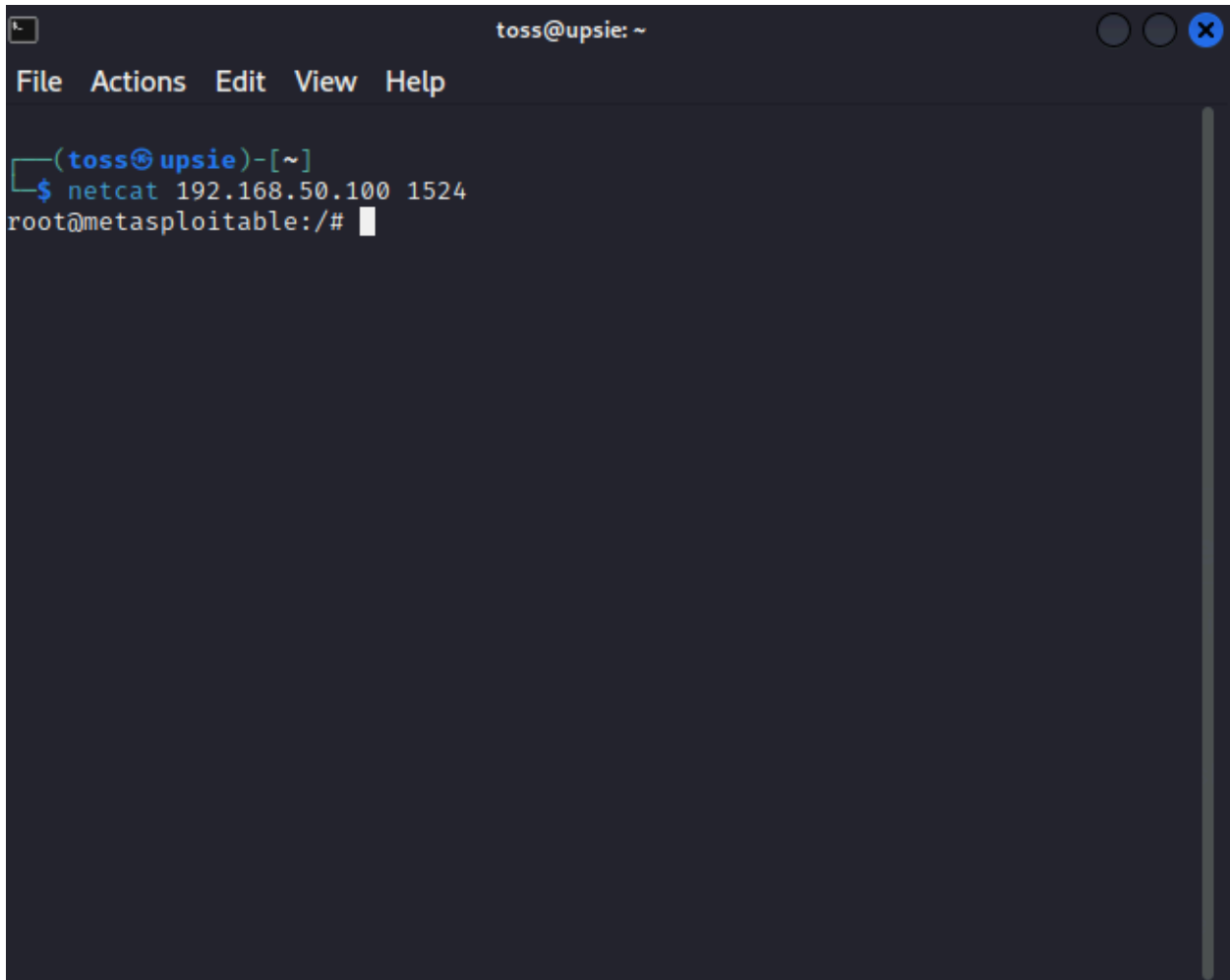
Bind shell

Effettuiamo una scansione con nmap

```
(toss@upsie)-[~]
$ nmap 192.168.50.100 -sV
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-28 11:27 CET
Nmap scan report for 192.168.50.100
Host is up (0.00031s 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        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
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  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 11.48 seconds
```

proviamo a collegarci alla porta 1524 di meta



```
toss@upsie: ~  
File Actions Edit View Help  
(toss@upsie)-[~]  
$ netcat 192.168.50.100 1524  
root@metasploitable:/#
```

cercando online sembrerebbe che sulla porta 1524 sia presente la backdoor ingresslock. Le possibilità dunque sono due. Utilizzare un firewall oppure eliminare la backdoor seguendo quanto consigliato online. Dunque andiamo sul file inetd.conf e modifichiamolo

```
msfadmin@metasploitable:~$ sudo nano /etc/inetd.conf
```

commentiamo l'ultima riga dov'è presente ingreslock

```
GNU nano 2.0.7      File: /etc/inetd.conf      Modified
#<off># netbios-ssn  stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.td$
telnet             stream  tcp    nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.tel$
#<off># ftp          stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.ft$
tftp               dgram  udp    wait    nobody   /usr/sbin/tcpd  /usr/sbin/in.tft$
shell              stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rsh$
login              stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rlog$
exec               stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rex$
#ingreslock stream tcp nowait root /bin/bash bash -i
```

salviamo il file e effettuiamo il reboot della macchina

Non sarà più possibile ricollegarsi

```
(toss@upsie)-[~]
$ netcat 192.168.50.100 1524
(UNKNOWN) [192.168.50.100] 1524 (ingreslock) : Connection refused
```

NFS Exported share Information Disclosure

```
GNU nano 2.0.7      File: /etc/exports

# /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)

[ Read 12 lines ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^U Next Page ^U UnCut Text ^T To Spell
```

inseriamo l'ip della sottorete così da poter accedere al servizio da qualunque macchina appartenente a questa sottorete





```
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.*

Save modified buffer (ANSWERING "No" WILL DESTROY CHANGES) ?
Y Yes
N No      ^C Cancel
```

successivamente salviamo e effettuiamo il reboot

Unrealicd backdoor

ho provato a coprire questa backdoor con la regola

<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP	*	*	192.168.50.100	8180	*	none	   
--------------------------	-------------------------------------	-------	----------	---	---	----------------	------	---	------	---

effettivamente la vulnerabilità sembra essersi risolta , ma purtroppo comunque permare l'errore sul report

—