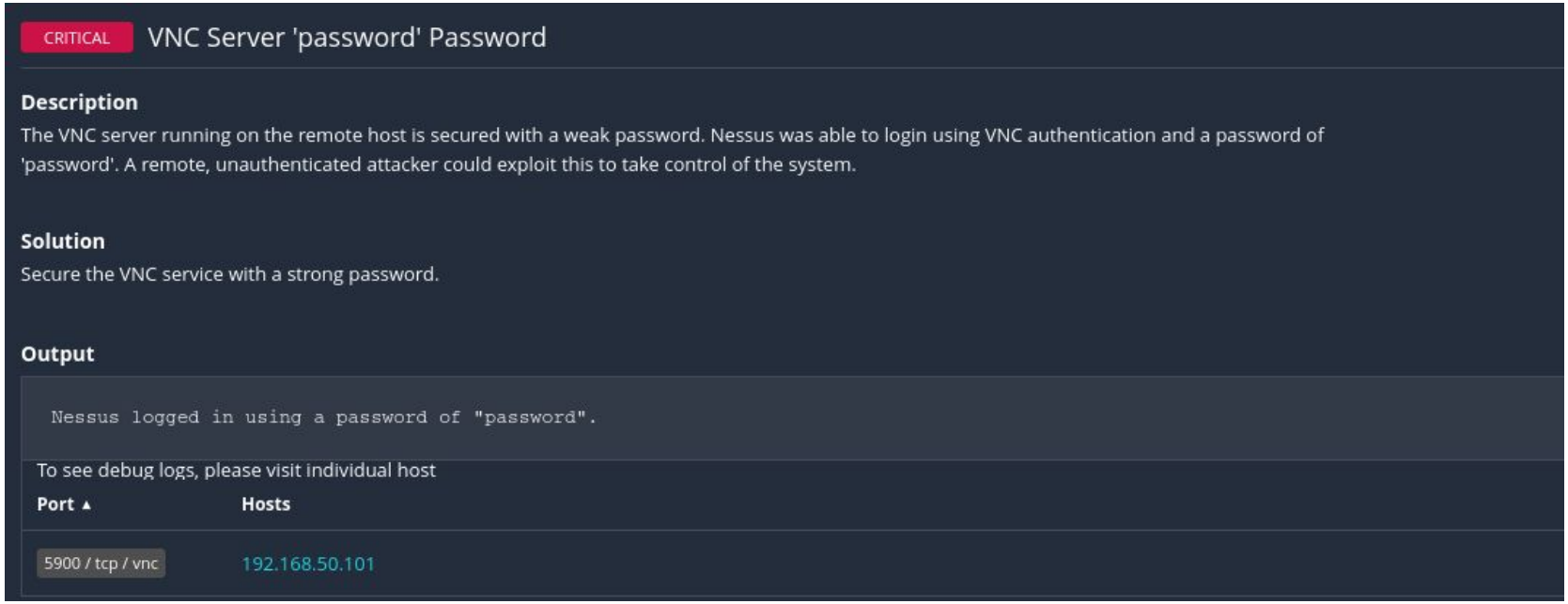
W12D4 - Progetto

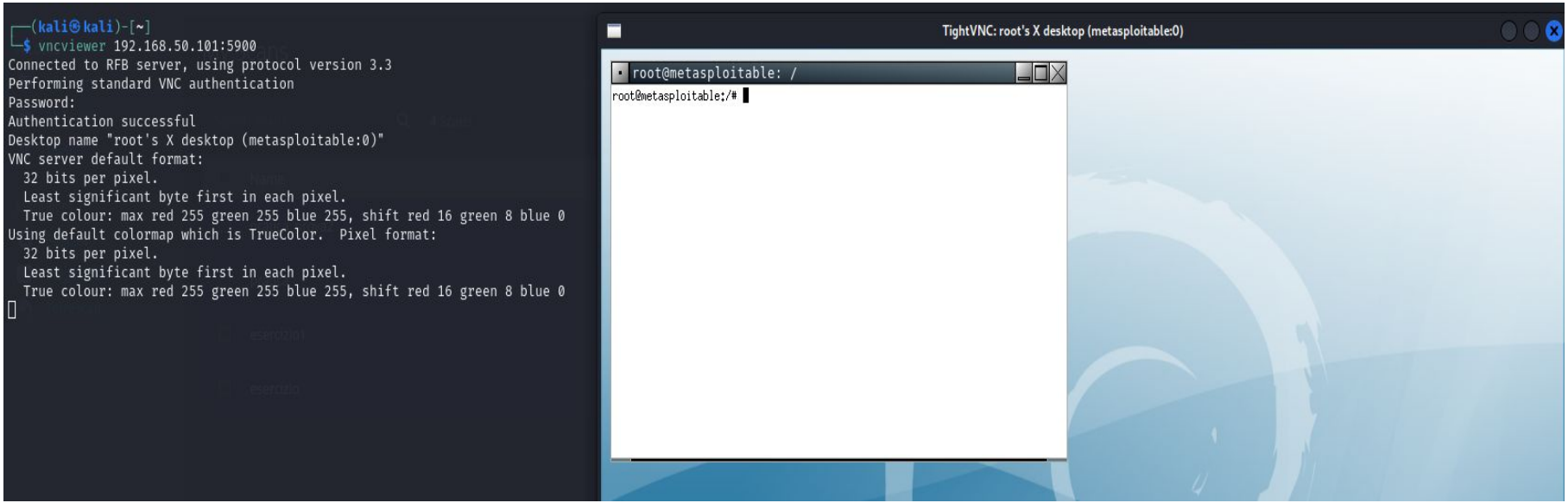
Analisi delle vulnerabilità e azioni di rimedio

Vulnerability: VNC SERVER PASSWORD



Il server VNC, in ascolto sulla porta 5900, ha una password debole facilmente compromettibile.

Vulnerability: VNC SERVER PASSWORD



Da Kali si può avere accesso al Server VNC con privilegi root inserendo la password corretta. Dato che la password settata è debole, può essere facilmente compromessa con un attacco brute force.

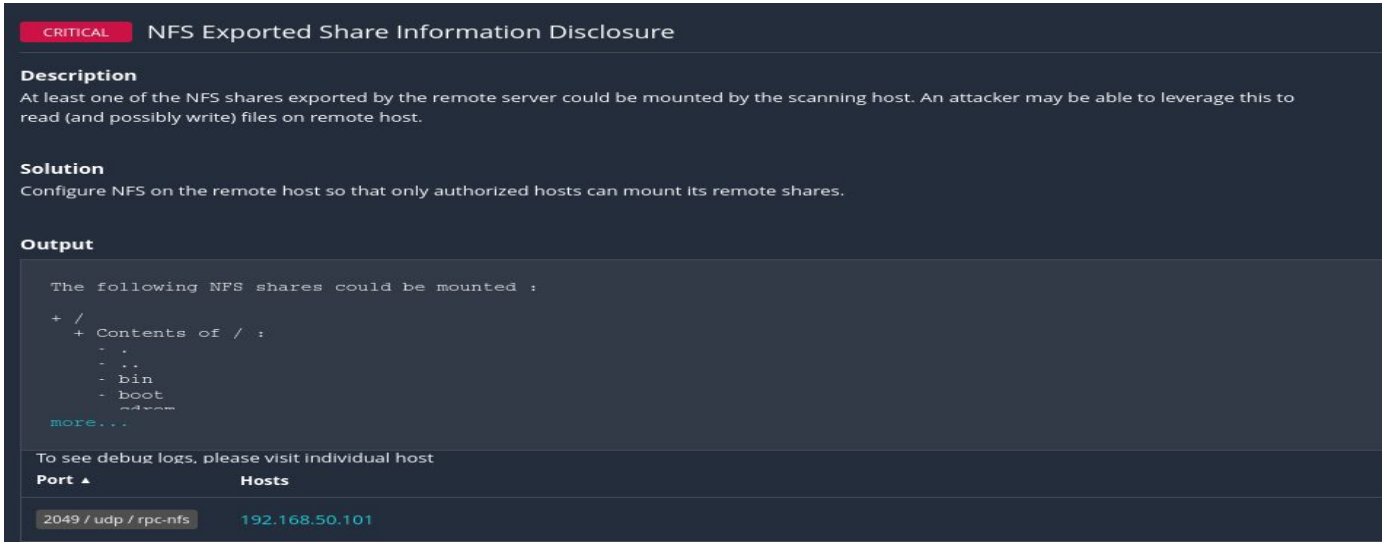
Remediation: VNC SERVER PASSWORD

```
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
```

```
┌──(kali㉿kali)-[~]
└─$ vncviewer 192.168.50.101:5900
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication failure
```

Cambiando la password con una più complessa, sarà più difficile sfruttare l'exploit.

Vulnerability: NFS EXPORTED SHARE INFORMATION DISCLOSURE



Utenti possono effettuare operazioni sensibili sul NFS, come scrivere file o aggiungere cartelle locali sulla macchina target, senza necessità di autenticazione.

Remediation: NFS EXPORTED SHARE INFORMATION DISCLOSURE

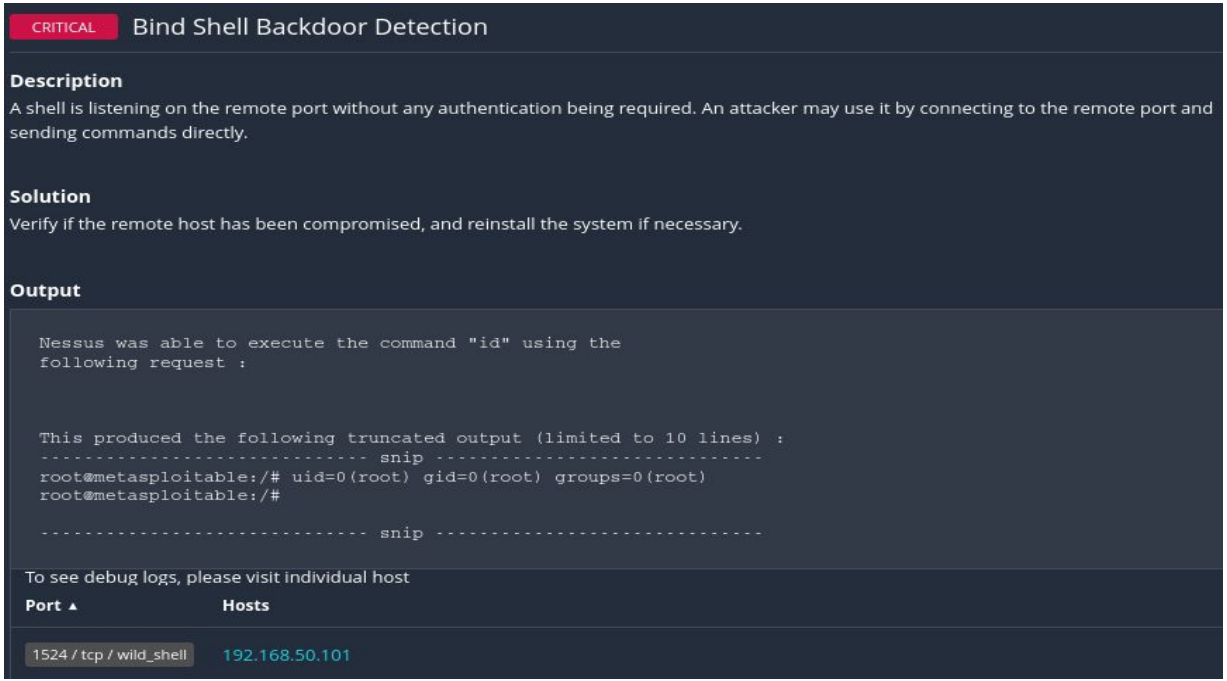
```
# /etc/exports: the access control list for filesystems which may be exported
#               to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes       hostname1(rw,sync) hostname2(ro,sync)
#
# Example for NFSv4:
# /srv/nfs4        gss/krb5i(rw,sync,fsid=0,crossmnt)
# /srv/nfs4/homes  gss/krb5i(rw,sync)
#


/       *192.168.50.100(rw,sync,root_squash,no_subtree_check)
#/      *(rw,sync,no_root_squash,no_subtree_check)
```

```
root@metasploitable:/home/msfadmin# iptables -A INPUT -p tcp -s 192.168.50.100 -
-dport 2049 -m state --state NEW,ESTABLISHED,RELATED -j DROP
root@metasploitable:/home/msfadmin# iptables -A OUTPUT -p tcp -s 192.168.50.100
--dport 2049 -m state --state NEW,ESTABLISHED,RELATED -j DROP
root@metasploitable:/home/msfadmin# iptables -A OUTPUT -p udp -s 192.168.50.100
--dport 2049 -m state --state NEW,ESTABLISHED,RELATED -j DROP
root@metasploitable:/home/msfadmin# iptables -A INPUT -p udp -s 192.168.50.100 -
-dport 2049 -m state --state NEW,ESTABLISHED,RELATED -j DROP
root@metasploitable:/home/msfadmin# _
```

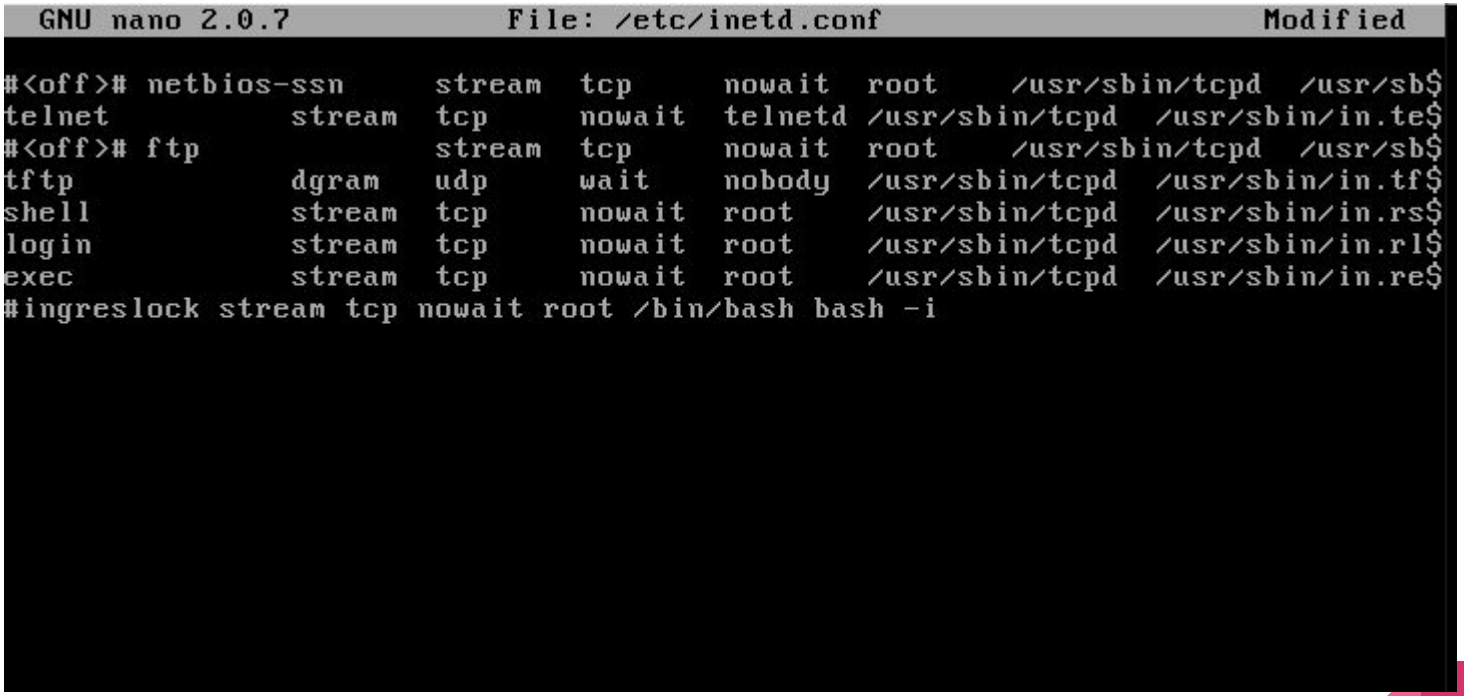
Si può rimediare modificando il file di exports per bloccare l'indirizzo ip 192.168.50.100 di Kali Linux o configurando una regola firewall con ip tables.

Vulnerability: BIND SHELL BACKDOOR DETECTION



Una backdoor è in ascolto sulla porta 1524. Un attaccante potrebbe connettersi ad essa e inviare comandi alla macchina target.

Remediation: BIND SHELL BACKDOOR DETECTION



Si può rimediare modificando il file di configurazione al path /etc/inetd.conf e commentando la riga che riguarda la Ingreslock Backdoor.

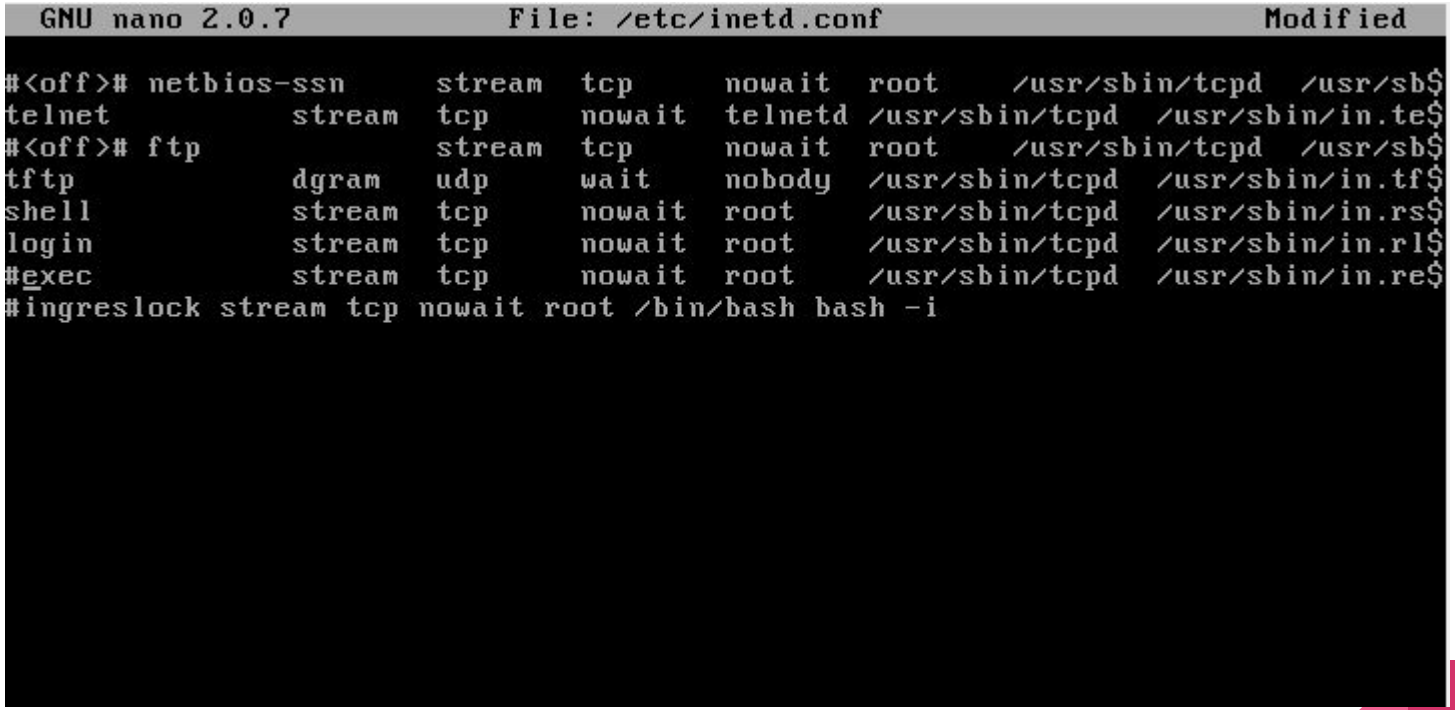
Vulnerability: rexecd service detection

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-28 15:06 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.50.101
Host is up (0.00075s latency).
Not shown: 978 closed tcp ports (reset)
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  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
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:D0:01:23 (Oracle VirtualBox virtual NIC)
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 53.79 seconds
```

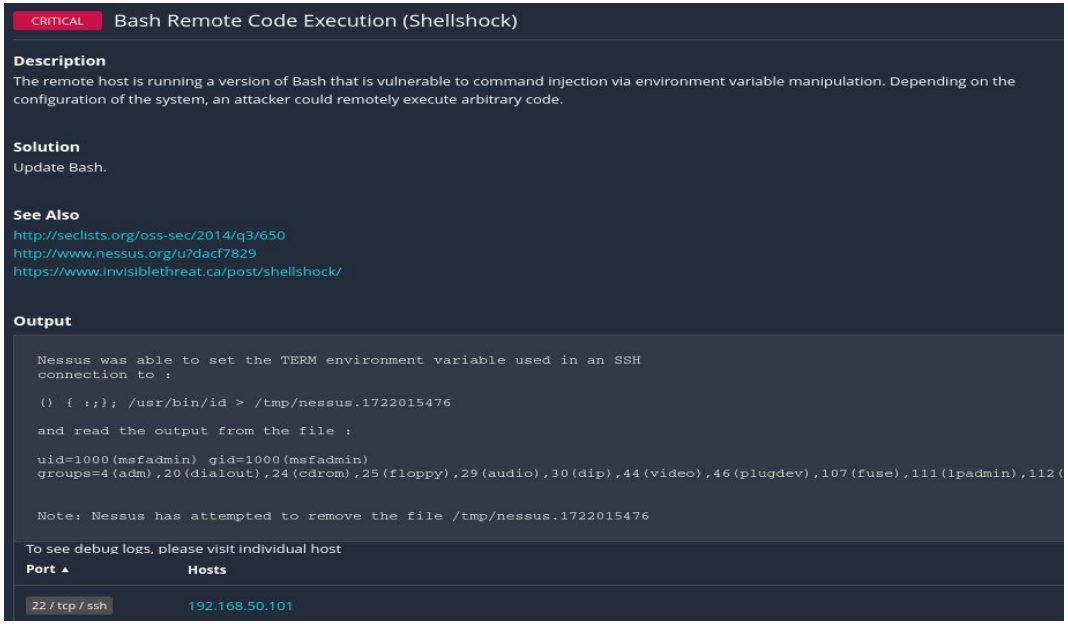
Il servizio rexecd permette agli utenti su una rete di eseguire comandi da remoto. Un attaccante potrebbe scansionare host di terze parti senza necessità di autenticazione.

Remediation: rexecd service detection



Si può rimediare modificando il file di configurazione al path /etc/inetd.conf e commentando la riga che riguarda la 'exec'.

Vulnerability: Bash Remote Code Execution (Shellshock)



La versione di Bash presente su Metasploitable è vulnerabile ai command injections.

Remediation: Bash Remote Code Execution (Shellshock)

```
root@metasploitable:/home/msfadmin/bash-4.4# bash --version
GNU bash, version 4.4.0(1)-release (i686-pc-linux-gnu)
Copyright (C) 2016 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
```

Come suggerito nella soluzione di Nessus, si può fare un upgrade della Bash con il comando wget http://ftp.gnu.org/gnu/bash/bash-4.4.tar.gz. Dopo aver estratto il file e aver sostituito la nuova versione alla vecchia, la bash sarà aggiornata alla versione 4.4 che non presenta questa vulnerabilità.