

REMEDIATION

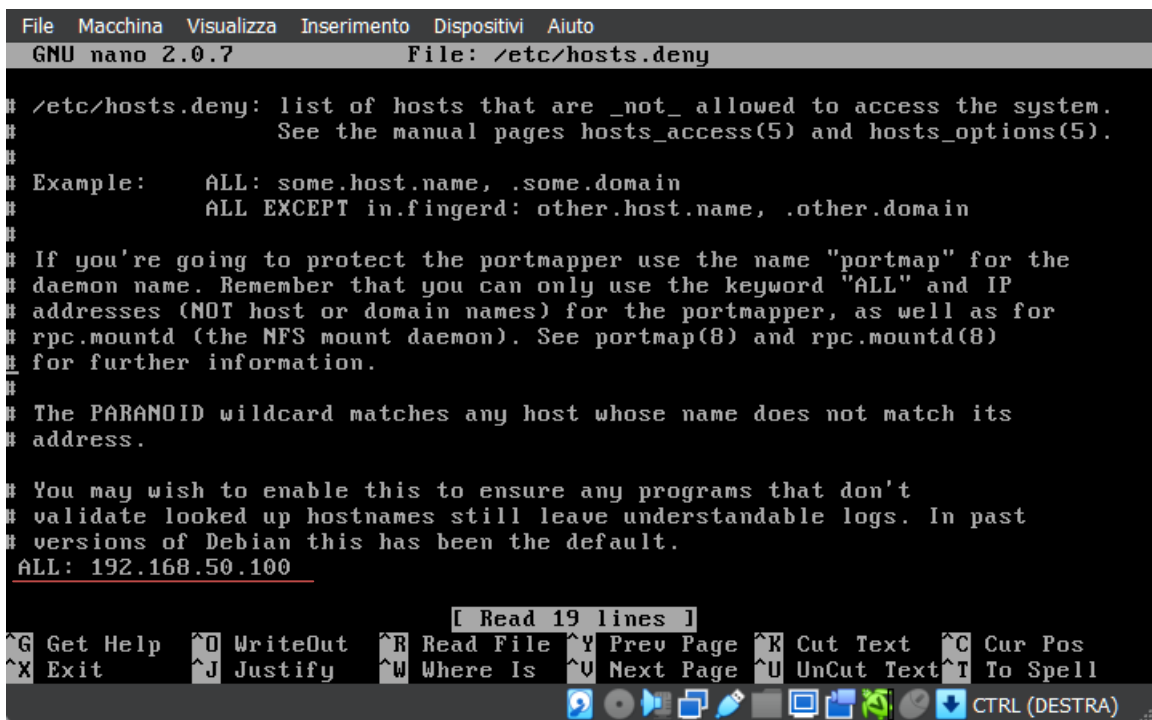
NFS EXPORTED SHARE INFORMATION DISCLOSURE

Descrizione:

Almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione. Un utente malintenzionato potrebbe essere in grado di sfruttare questo per leggere e modificare i file su host remoto.

Soluzione:

Configura NFS sull'host remoto in modo che solo gli host autorizzati possano montare le sue condivisioni remote.



```
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
GNU nano 2.0.7                               File: /etc/hosts.deny

# /etc/hosts.deny: list of hosts that are _not_ allowed to access the system.
#               See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:      ALL: some.host.name, .some.domain
#               ALL EXCEPT in.fingerd: other.host.name, .other.domain
#
# If you're going to protect the portmapper use the name "portmap" for the
# daemon name. Remember that you can only use the keyword "ALL" and IP
# addresses (NOT host or domain names) for the portmapper, as well as for
# rpc.mountd (the NFS mount daemon). See portmap(8) and rpc.mountd(8)
# for further information.
#
# The PARANOID wildcard matches any host whose name does not match its
# address.
#
# You may wish to enable this to ensure any programs that don't
# validate looked up hostnames still leave understandable logs. In past
# versions of Debian this has been the default.
ALL: 192.168.50.100

[ Read 19 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   ^V Next Page  ^U UnCut Text ^T To Spell
CTRL (DESTRA)
```

- Recarsi sul file /etc/hosts.deny con i privilegi di amministratore e modificare la riga **#ALL: PARANOID** con **ALL 192.168.50.100**.
Inserendo l'indirizzo ip, l'utente Kali non potrà accedere ai file di condivisione remota.

VNC SERVER "PASSWORD" PASSWORD

Descrizione:

Il server VNC in esecuzione sull'host remoto è protetto da una password debole. Nessus è stato in grado di accedere, utilizzando l'autenticazione VNC e una password "password". Un utente malintenzionato remoto e non autenticato potrebbe sfruttarlo per assumere il controllo del sistema.

Soluzione:

Proteggi il servizio VNC con una password sicura.

```
Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Sat Jun  3 03:31:35 EDT 2023 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password: _
```

- Con i privilegi di amministratore cambiare password su **vncpasswd**.
- Inserire una password sicura.

BIND SHELL BACKDOOR DETECTION

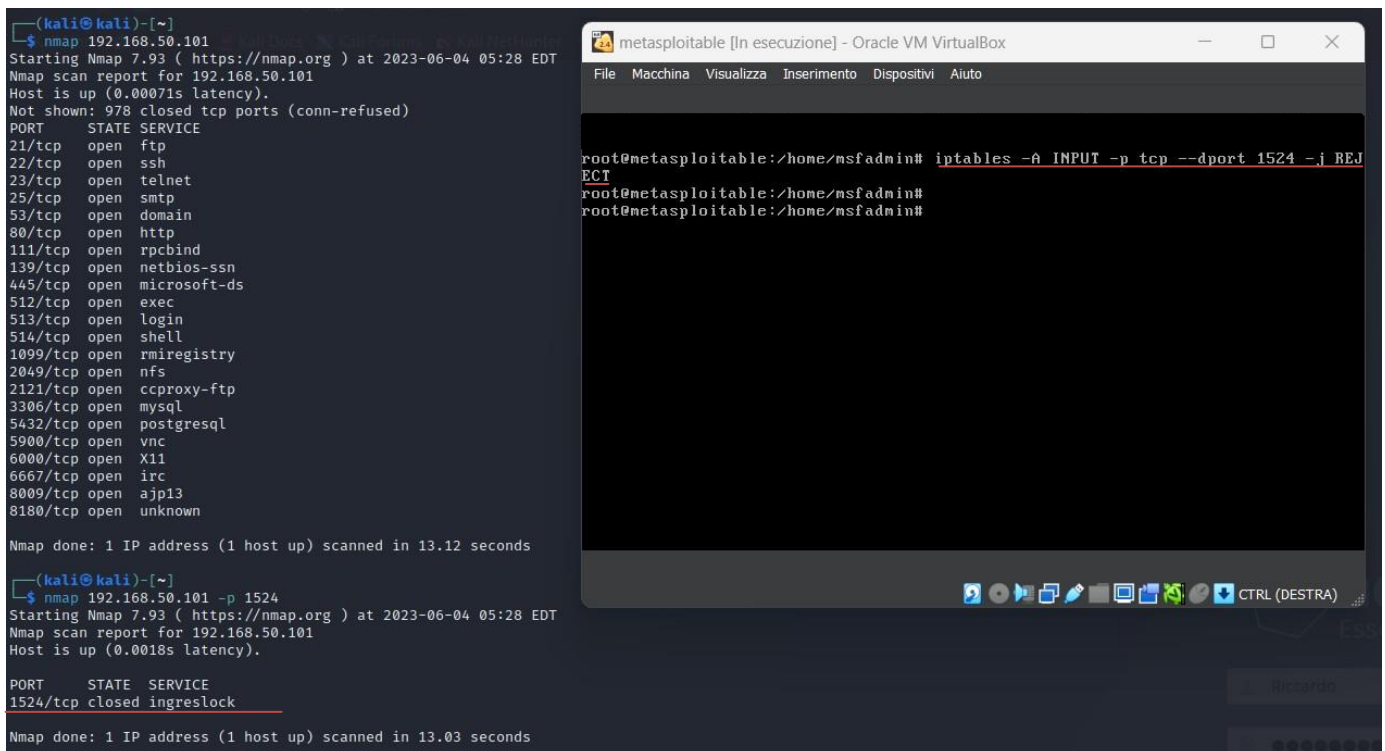
Descrizione:

Una shell è in ascolto sulla porta remota (1524 / tcp / wild_shell) senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può utilizzarlo collegandosi alla porta remota e inviando comandi direttamente.

Soluzione:

Usare iptables, firewall di linux, per bloccare la seguente porta.

Effettuare scansione sulla porta 1524.



The screenshot shows two windows. The left window is a Kali Linux terminal with the following output:

```
(kali@kali)-[~]
$ nmap 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-04 05:28 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00071s latency).
Not shown: 978 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 13.12 seconds

(kali@kali)-[~]
$ nmap 192.168.50.101 -p 1524
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-04 05:28 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0018s latency).
PORT      STATE SERVICE
1524/tcp  closed ingreslock

Nmap done: 1 IP address (1 host up) scanned in 13.03 seconds
```

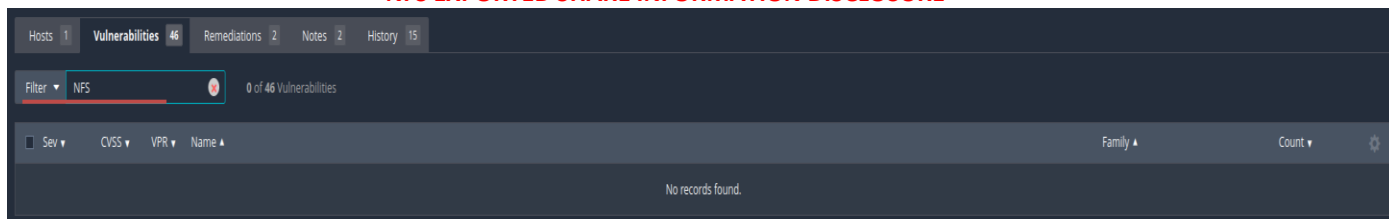
The right window is a Metasploitable VM titled "metasploitable [In esecuzione] - Oracle VM VirtualBox". It shows the command `iptables -A INPUT -p tcp --dport 1524 -j REJECT` being executed in a terminal, followed by two prompts for the root user.

- Eseguire il comando : **"iptables -A INPUT -p tcp --dport 1524 -j REJECT"**
- I seguenti comandi rifiuteranno i pacchetti sulla porta 1254.
- Come si può vedere nella figura precedente, effettuando una scansione con nmap, con il comando: **"nmap 192.168.50.101 -p 1524"** la porta risulta chiusa.

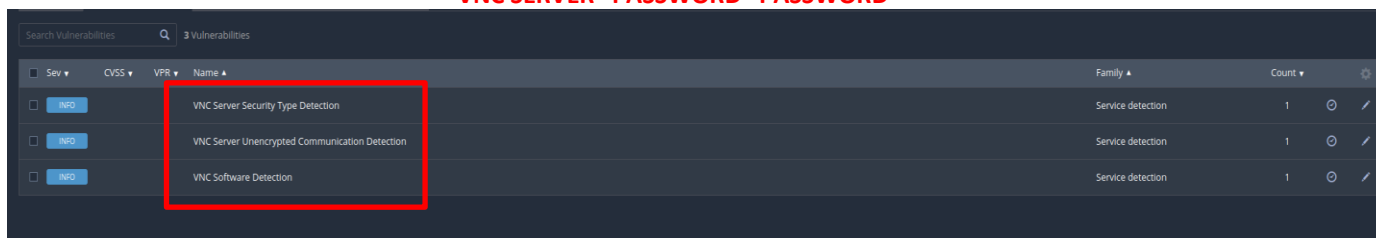
CONCLUSIONE

Dopo aver eseguito la remediation si può procedere con una nuova scansione su Nessus e verificare l'andamento delle vulnerabilità.

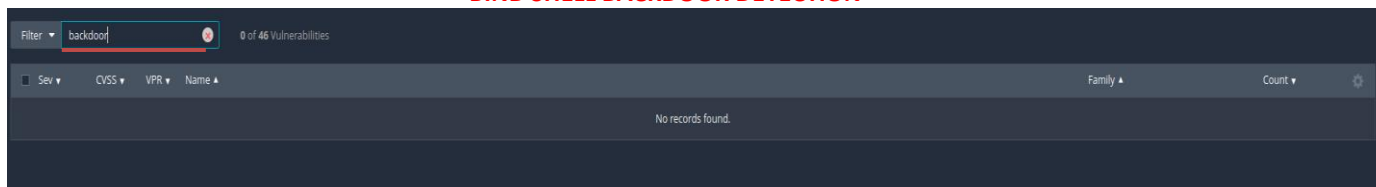
NFS EXPORTED SHARE INFORMATION DISCLOSURE



VNC SERVER "PASSWORD" PASSWORD



BIND SHELL BACKDOOR DETECTION



Come si può vedere nelle foto le vulnerabilità non sono state trovate da Nessus.