

REMEDIATION METASPLOITABLE

Come richiesto si è intervenuti con urgenza nel risolvere alcune delle vulnerabilità di livello critical individuate in Metasploitable attraverso la scansione effettuata con Nessus.

VNC Server 'password' Password

CRITICAL VNC Server 'password' Password

Description

The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Solution

Secure the VNC service with a strong password.

La prima vulnerabilità corretta riguarda il server VNC (Virtual Network Computing) nella porta 5900 che permette il controllo di un computer da remoto. Come evidenziato nella figura sopra questo servizio è protetto da una password molto debole ovvero "password" quindi la soluzione è modificarla con una più forte alternando ad esempio caratteri maiuscoli/minuscoli e numeri.

```
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
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
root@metasploitable:/home/msfadmin#
```

Nel dettaglio si procede con privilegi root in Metasploitable (mediante il comando *sudo su*) e si genera una nuova password con il comando *vncpasswd*. Dopo averla riconfermata si risponde con *n* (no) alla richiesta di inserire una password di sola visualizzazione e si riavvia il sistema con il comando *sudo reboot*.

NFS Exported Share Information Disclosure

CRITICAL NFS Exported Share Information Disclosure

Description

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

Solution

Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

Port ▲	Hosts
2049 / udp / rpc-nfs	192.168.50.101

Un'altra criticità riscontrata riguarda invece il NFS (Network File System) un protocollo di rete che consente la condivisione di file tra client diversi. E' attivo sulla porta 2049.

```
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
```

Ciò che si andrà a fare per evitare che utenti non autorizzati possano modificare file su host remoto sarà cambiare i permessi accedendo al file `/etc/exports` (con *nano*) e privilegi root.

```
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)
#
192.168.50.101(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 ^U Next Page ^U UnCut Text ^T To Spell
```

Si sostituisce `*` con l'indirizzo IP di Metasploitable in modo tale che i permessi riportati tra parentesi (lettura-scrittura, permessi root condivisione) vengano affidati solo ad esso.

In alternativa si sarebbe potuto aggiungere una sottorete per dare permessi a client della stessa rete interna.

Bind Shell Backdoor Detection

CRITICAL

Bind Shell Backdoor Detection

Description

A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

Solution

Verify if the remote host has been compromised, and reinstall the system if necessary.

Port ▲	Hosts
1524 / tcp / wild_shell	192.168.50.101

La terza vulnerabilità contrastata fa riferimento al servizio Bindshell sulla porta 1524. E' possibile collegarsi e inviare qualsiasi comando sull'host remoto.

```
(kali@kali)~$ sudo nmap -sV -sT 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-03 04:12 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00015s 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  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
MAC Address: 08:00:27:8F:E3:4F (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 65.63 seconds
```

Facendo un'ulteriore scansione da Kali Linux utilizzando nmap con gli switch -sV e -sT (per avere info su versioni utilizzando una scansione TCP dove viene completato il three-way handshake in modo da avere maggior attendibilità sullo stato delle porte) si nota che la porta 1524 è aperta.

```
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:~# iptables -I INPUT -p tcp -s 192.168.50.100 -
-dport 1524 -j DROP
root@metasploitable:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
DROP      tcp  --  192.168.50.100        anywhere             tcp dpt:ingreslock

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
root@metasploitable:~#
```

Come si può vedere dall'immagine sopra ottenendo anche in questo caso dapprima i privilegi di root si può impostare una regola di firewall in modo tale da impedire con l'action *DROP* il traffico in entrata (*INPUT*) sul protocollo tcp della suddetta porta dall'IP di Kali.

Il firewall utilizzato nel caso specifico è iptables che si trova in genere configurato di default sui sistemi Linux.

Dopo aver confermato con il comando *iptables -L* possiamo verificare la nuova configurazione.

```
(kali@kali)-[~/Desktop]
$ sudo nmap -sV -sT 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-04 06:00 EDT
Nmap scan report for 192.168.50.101
Host is up (0.000086s 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  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
MAC Address: 08:00:27:8F:E3:4F (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 66.68 seconds
```

Infine eseguendo di nuovo la stessa scansione effettuata precedentemente con nmap da Kali si noterà che la porta 1524 sarà filtrata e non si potrà vedere versione ed ulteriori info.