

REMEDIATION META

#1

Bind Shell Backdoor Detection

CRITICAL Nessus Plugin ID 51988

[Information](#) [Dependencies](#) [Dependents](#) [Changelog](#)

Synopsis

The remote host may have been compromised.

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.

Descrizione del problema: una shell è in ascolto sulla remote port senza che sia richiesta alcuna autenticazione, quindi un utente malintenzionato può utilizzarlo collegandosi alla remote port riuscendo anche ad inviare dei comandi.

Soluzione: La soluzione più rapida che ho trovato è stata quella di creare una regola nel firewall di metasploitable che riuscisse a bloccare il servizio TCP e UDP di una specifica porta:

Quindi tramite Nmap ho trovato la porta che gestisce l'errore BindShell 51988:

```

(root@kali)~[/home/kali]
# nmap -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 14:33 EST
Nmap scan report for 192.168.50.101
Host is up (0.00027s latency).
Not shown: 977 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
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:56:BC:C9 (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 66.47 seconds

```

La porta in questione è la **1524**.

Quindi tornando su Metasploitable, creo una regola nel firewall che riesca a disabilitare quella porta specifica:

```

msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# ufw enable
Firewall started and enabled on system startup
root@metasploitable:/home/msfadmin# ufw default allow
Default policy changed to 'allow'
(be sure to update your rules accordingly)
root@metasploitable:/home/msfadmin# ufw deny 1524
Rule added
root@metasploitable:/home/msfadmin# ufw status
Firewall loaded

To Action From
--
1524:tcp DENY Anywhere
1524:udp DENY Anywhere

root@metasploitable:/home/msfadmin#

```

#2

VNC Server 'password' Password

CRITICAL Nessus Plugin ID 61708

Information Dependencies Dependents Changelog

Synopsis

A VNC server running on the remote host is secured with a weak 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.

Descrizione del problema: il server VNC in esecuzione su metasploitable è protetto con una password debole. Nessus è riuscito ad accedere utilizzando l'autenticazione VNC e la password è “password”. Quindi un utente non autorizzato potrebbe riuscire ad introdursi nel sistema prendendone il controllo.

Soluzione: Cambiare la password mettendone una più sicura.

```
root@metasploitable:~# cd /root
root@metasploitable:~# ls -la
.          .config      .gconf       .profile     .ssh
..         Desktop     .gconfd      .purple      .vnc
.bash_history .filezilla  .gstreamer-0.10 reset_logs.sh vnc.log
.bashrc    .fluxbox    .mozilla     .rhosts      .Xauthority
root@metasploitable:~# cd .vnc
root@metasploitable:~/.vnc# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:~/.vnc# reboot
```

#3

NFS Exported Share Information Disclosure

CRITICAL

Nessus Plugin ID 11356

Information

Dependencies

Dependents

Changelog

Synopsis

It is possible to access NFS shares on the remote host.

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.

Descrizione del problema: almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere montata mediante la scansione di metasploitable. Quindi un utente malintenzionato potrebbe essere in grado di sfruttare questo per leggere file sull'host remoto.

Soluzione: Creare una regola in NFS che faccio in modo che solo uno specifico ip (quindi l'host) possa leggere e scrivere al suo interno.

```
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)
#
/mnt/newdisk      192.168.50.101(rw,sync,no_root_squash,no_subtree_check)
```


#4

Samba Badlock Vulnerability

HIGH

Nessus Plugin ID 90509

Information

Dependencies

Dependents

Changelog

Synopsis

An SMB server running on the remote host is affected by the Badlock vulnerability.

Description

The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy)(LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker who is able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services.

Solution

Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.

Descrizione del problema: La mia versione di Samba essendo una versione molto datata ha dei problemi che vengono definiti come Badlock, ciò renderà il traffico tra il client e l'host più facilmente accessibile da un Man-in-the-middle, che potrebbe riuscire a disabilitare grazie ad essi dei servizi di metasploitable che lo renderebbero molto più vulnerabile ad attacchi.

Soluzione: le soluzioni possibili sono due, la prima riguarda l'aggiornare Samba alle ultime versioni disponibili, ma essendo che Meta è una macchina molto vulnerabile usata solo per scopi simulativi, mandando quest'ultima Online potrebbe essere attaccata in qualsiasi momento da alcuni bot che riuscirebbero ad identificare tutte le macchine virtuali basate su Metasploitable che vanno su internet, entrando e riuscendo quindi a creare dei danni seri anche alla macchina originale su cui gira VirtualBox.

La soluzione più rapida ed efficace rimane quindi la creazione di un'altra regola nel Firewall che disabilita il servizio di Samba, rendendo paradossalmente la macchina più sicura.

Sempre tramite Nessus ho trovato le porte da chiudere:

```
(root@kali)-[/home/kali]
# nmap -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 14:33 EST
Nmap scan report for 192.168.50.101
Host is up (0.00027s latency).
Not shown: 977 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
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:56:BC:C9 (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 66.47 seconds
```

Le porte da chiudere sono le seguenti: **139** ; **445** .

```
msfadmin@metasploitable:~$ sudo su
root@metasploitable:/home/msfadmin# ufw deny 445
Rule added
root@metasploitable:/home/msfadmin# ufw status
Firewall loaded

To Action From
--
1524:tcp DENY Anywhere
1524:udp DENY Anywhere
445:tcp DENY Anywhere
445:udp DENY Anywhere
```

```
msfadmin@metasploitable:~$ sudo su
[sudol password for msfadmin:]
root@metasploitable:/home/msfadmin# ufw deny 139
Rule added
root@metasploitable:/home/msfadmin# ufw status
Firewall loaded

To Action From
--
1524:tcp DENY Anywhere
1524:udp DENY Anywhere
445:tcp DENY Anywhere
445:udp DENY Anywhere
139:tcp DENY Anywhere
139:udp DENY Anywhere
```