



Report generated by Nessus™

METASPLOITABLE 2 remediation (remediation meta)

Thu, 01 Jun 2023 12:49:11 CEST

Dobbiamo andare a risolvere le criticità rilevate durante il vulnerability assessment, quindi andiamo ad esaminare caso per caso e procediamo con le remediation possibili per ovviare al problema. Cercheremo di porre una politica di remediation su un minimo di 2 a un massimo di 4 vulnerabilità tra quelle critiche.

Vulnerabilities by Host

192.168.50.101



CRITICAL HIGH MEDIUM LOW INFO

Scan Information

Start time: Thu Jun 1 12:22:51 2023

End time: Thu Jun 1 12:49:11 2023

Host Information

Netbios Name: METASPLOITABLE

IP: 192.168.50.101

MAC Address: 08:00:27:D8:79:E5

OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Vulnerabilities

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

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Plugin Information

Published: 2011/02/15, Modified: 2022/04/11

Plugin Output

Questa vulnerabilità riguarda una backdoor aperta sulla porta 1524: un servizio di shell senza autenticazione è in ascolto sulla porta 1524. Un malintenzionato può connettersi a questo servizio e usarlo per inviare codice malevolo.

La soluzione in questo caso consiste nel chiudere la porta compromessa. Per farlo andiamo a inserire una regola ad hoc sul firewall iptables di metasploitable. Il comando da inserire è `<sudo iptables -I INPUT -p tcp --dport 1524 -j DROP>`.

```
msfadmin@metasploitable:/$ sudo iptables -I INPUT -p tcp --dport 1524 -j DROP
```

La regola blocca le connessioni in entrata con protocollo tcp sulla porta 1524.

tcp/1524/wild_shell

Nessus was able to execute the command "id" using the following request :

```
This produced the following truncated output (limited to 10 lines) :
----- snip -----
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#
----- snip -----
```

11356 - NFS Exported Share Information Disclosure

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.

Risk Factor

Critical

VPR Score

5.9

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

CVE [CVE-1999-0170](#)

CVE [CVE-1999-0211](#)

CVE [CVE-1999-0554](#)

Exploitable With

Metasploit (true)

Plugin Information

Published: 2003/03/12, Modified: 2018/09/17

Plugin Output

La NFS exported disclosure è una vulnerabilità che riguarda il network file system dell'host remoto. Normalmente nei file di configurazione di questo servizio l'accesso è permesso a qualsiasi connessione, ma un hacker potrebbe avvalersi di questa porta per leggere e modificare i dati all'interno della macchina. Dunque cambiamo il file di configurazione "hosts.deny" dalla cartella di sistema "/etc" e blocchiamo l'accesso a tutti i client:

```
GNU nano 2.0.7      File: hosts.deny      Modified
# 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: PARANOID
ALL:ALL_

^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

[ Read 12 lines ]
CTRL (DESTRA)
```

Successivamente andiamo a editare la controparte "hosts.allow" per cancellare la riga "ALL:ALL".

```
GNU nano 2.0.7      File: hosts.allow

# /etc/hosts.allow: list of hosts that are allowed to access the system.
#                  See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:        ALL: LOCAL @some_netgroup
#                  ALL: .foobar.edu EXCEPT terminalserver.foobar.edu
#
# 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.
#
_

[ 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  ^V Next Page  ^U UnCut Text ^T To Spell

CTRL (DESTRA)
```

In questo modo si negano tutte le connessioni nfs all'host e non si permette nulla.

udp/2049/rpc-nfs

The following NFS shares could be mounted :

```
+ /
+ Contents of / :
- .
- ..
- bin
- boot
- cdrom
- dev
- etc
- home
- initrd
- initrd.img
- lib
- lost+found
- media
- mnt
- nohup.out
- opt
- proc
- root
- sbin
- srv
- sys
- tmp
- usr
- var
- vmlinuz
```

33850 - Unix Operating System Unsupported Version Detection

Synopsis

The operating system running on the remote host is no longer supported.

Description

According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

Solution

Upgrade to a version of the Unix operating system that is currently supported.

Risk Factor

Critical

CVSS v3.0 Base Score

10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

XREF IAVA:0001-A-0502

XREF IAVA:0001-A-0648

Plugin Information

Published: 2008/08/08, Modified: 2023/05/18

Plugin Output

La soprastante vulnerabilità è la più banale: il sistema è obsoleto e necessita un aggiornamento. Le vecchie versioni degli os e in generale dei software dopo diversi anni perdono il supporto della casa madre, lasciando spesso scoperte delle falle che invece sarebbero risolte facendo un update o un upgrade. Nel nostro caso metasploitable ci serve così com'è, dunque non possiamo aggiornarlo. Se fossimo in una situazione reale, questo scenario sarebbe l'esempio perfetto di risk acceptance.

tcp/0

Ubuntu 8.04 support ended on 2011-05-12 (Desktop) / 2013-05-09 (Server).
Upgrade to Ubuntu 21.04 / LTS 20.04 / LTS 18.04.

For more information, see : <https://wiki.ubuntu.com/Releases>

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

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

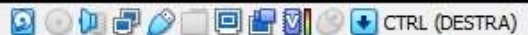
Plugin Information

Published: 2012/08/29, Modified: 2015/09/24

Plugin Output

Un altro scenario piuttosto banale e molto diffuso è quello delle password deboli o di default: macchine, sistemi, servizi e programmi lasciati con le credenziali stabilite dal produttore o cambiate con delle alternative troppo semplici, che possono essere facilmente indovinate dagli hacker. La soluzione è altrettanto banale: andiamo a cambiare la password del servizio vnc, utilizzando i privilegi di root con "sudo su", e poi andando ad eseguire il comando "vncpasswd":

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



Andiamo anche ad inserire una password view-only, come ulteriore misura di sicurezza.

tcp/5900/vnc

Nessus logged in using a password of "password".

10203 - rexecd Service Detection

Synopsis

The rexecd service is running on the remote host.

Description

The rexecd service is running on the remote host. This service is design to allow users of a network to execute commands remotely.

However, rexecd does not provide any good means of authentication, so it may be abused by an attacker to scan a third-party host.

Solution

Comment out the 'exec' line in /etc/inetd.conf and restart the inetd process.

Risk Factor

Critical

VPR Score

6.7

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

CVE [CVE-1999-0618](#)

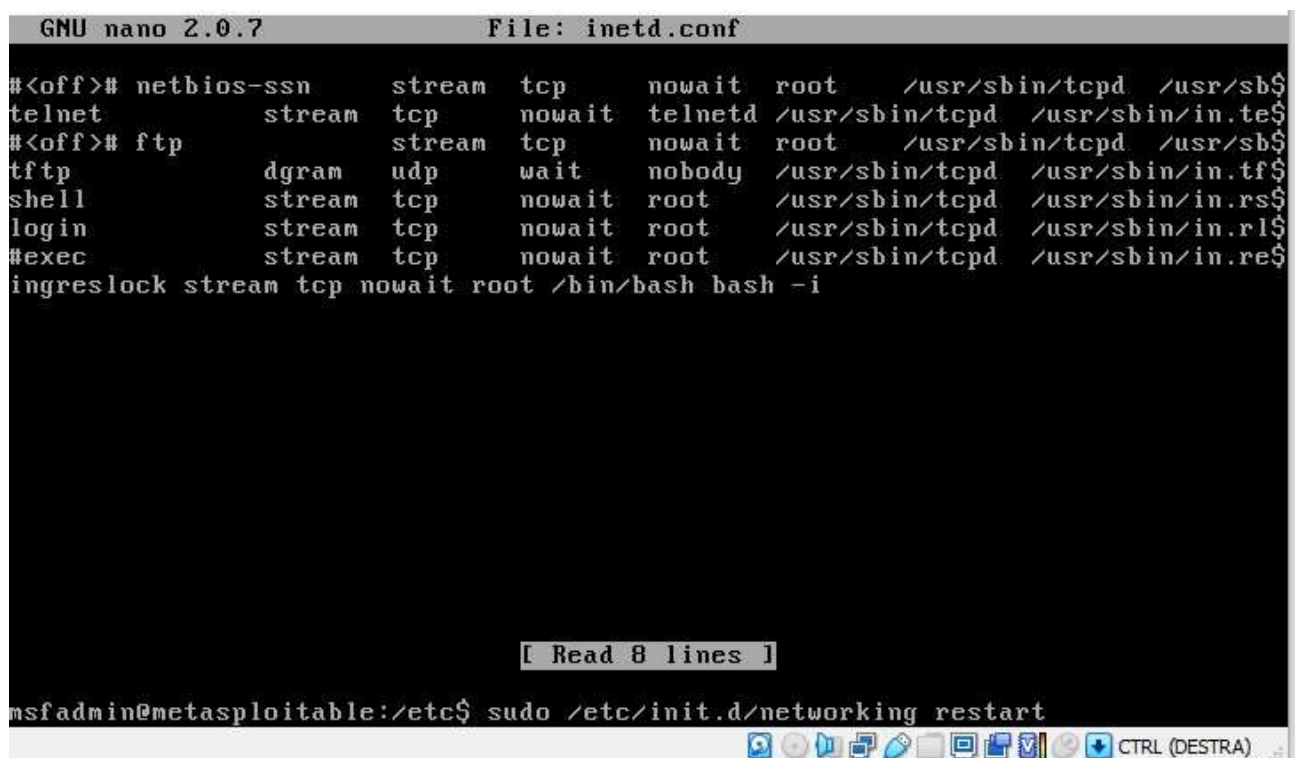
Plugin Information

Published: 1999/08/31, Modified: 2018/08/13

Plugin Output

Per l'ultima vulnerabilità, similmente ad altre, è attivo un servizio che permetterebbe ad utenti nella rete di eseguire comandi da remoto. Non avendo dei metodi efficaci di autenticazione, potrebbe essere violato il sistema.

La soluzione è modificare il file di configurazione "inetd.conf" dentro la directory /etc e poi riavviare la connessione.



```
GNU nano 2.0.7 File: 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

[ Read 8 lines ]

msfadmin@metasploitable:/etc$ sudo /etc/init.d/networking restart
```

tcp/512/rexecd

CONCLUSIONE

Dovremmo essere riusciti a risolvere 4 vulnerabilità critiche, mentre per una abbiamo adottato una politica di risk acceptance. Effettuando una nuova scansione con nessus, verificheremo che la riuscita dell'operazione.