Progetto settimana 5

Traccia: Effettuare una scansione completa sul target Metasploitable. Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità critiche / high e provate ad implementare delle azioni di rimedio. N.B. le azioni di rimedio, in questa fase, potrebbero anche essere delle regole firewall ben configurate in modo da limitare eventualmente le esposizioni dei servizi vulnerabili. Vi consigliamo tuttavia di utilizzare magari questo approccio per non più di una vulnerabilità. Per dimostrare l'efficacia delle azioni di rimedio, eseguite nuovamente la scansione sul target e confrontate i risultati con quelli precedentemente ottenuti.

Vulnerabilità 1:

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

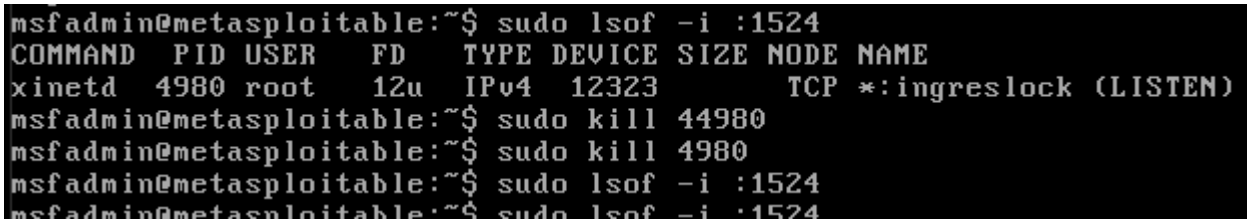
tcp/1524/wild_shell

```
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 ------------------------------
```

192.168.50.103 7

Da questo report si vede che nessus ha rilevato una backdoor sulla porta 1524, essa consente l'accesso non autorizzato al sistema creando una shell in ascolto sulla porta 1524.
La gravità è considerata critica perché avere una tale backdoor significa che un attaccante potrebbe potenzialmente connettersi alla porta da remoto ed eseguire comandi ottenendo un accesso non autorizzato al sistema.

Soluzione:



Ho individuato un servizio sospetto in ascolto sulla porta 1524 del sistema Metasploitable. Utilizzando comandi come `lsof`, ho identificato il processo associato a quella porta e l'ho interrotto usando `kill`. Successivamente, ho verificato che non ci fossero più connessioni attive su quella porta e ho eseguito controlli aggiuntivi per assicurarmi che il sistema fosse libero da altre anomalie o backdoor.

Vulnerabilità 2:

32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Synopsis

The remote SSH host keys are weak.

Description

The remote SSH host key 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 set up decipher the remote session or set up a man in the middle attack.

See Also

http://www.nessus.org/u?107f9bdc

http://www.nessus.org/u?f14f4224

Solution

Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

Risk Factor

Critical

VPR Score

7.4

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

8.3 (CVSS2#E:F/RL:OF/RC:C)

References

BID	29179
CVE	CVE-2008-0166
XREF	CWE:310

Exploitable With

Core Impact (true)

Plugin Information

Published: 2008/05/14, Modified: 2018/11/15

Plugin Output

tcp/22/ssh

Questo report invece indica un problema di sicurezza legato alla generazioni di chiavi SSH, questo rischio è classificato come critico perché compromette l'integrità dei sistemi che utilizzano le chiavi ssh generate su questo sistema, potrebbe portare a un'intercettazione delle sessioni o attacchi di tipo "man in the middle".

Soluzione:

```
sudo ssh-keygen -A
```

```
sudo /etc/init.d/ssh stop
sudo /etc/init.d/ssh start
```

In questo modo sono state rigenerate tutte le chiavi crittografiche presenti nel sistema

```
msfadmin@metasploitable:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/msfadmin/.ssh/id_rsa):
/home/msfadmin/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/msfadmin/.ssh/id_rsa.
Your public key has been saved in /home/msfadmin/.ssh/id_rsa.pub.
The key fingerprint is:
10:eb:93:19:48:99:1a:23:ec:81:63:fa:2e:42:5b:5b msfadmin@metasploitable
msfadmin@metasploitable:~$
```

Vulnerabilità 3:

42256 - NFS Shares World Readable

Synopsis

The remote NFS server exports world-readable shares.

Description

The remote NFS server is exporting one or more shares without restricting access (based on hostname, IP, or IP range).

See Also

http://www.tldp.org/HOWTO/NFS-HOWTO/security.html

Solution

Place the appropriate restrictions on all NFS shares.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2009/10/26, Modified: 2020/05/05

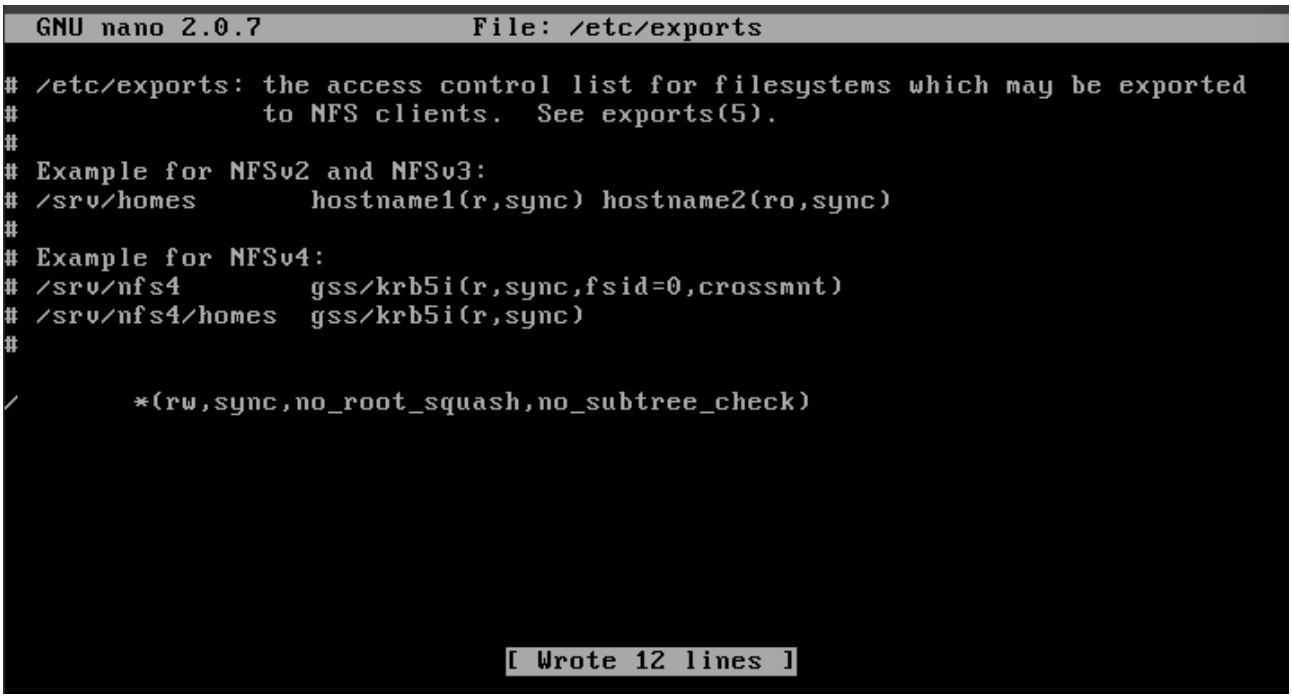
Plugin Output

tcp/2049/rpc-nfs

```
The following shares have no access restrictions :

  / *
```

Questo report indica che il server NFS sta esportando condivisioni senza restrizioni di accesso, il che significa che qualsiasi host o utente può accedere liberamente a queste condivisioni.

Soluzione:



Prima di tutto sono state localizzate le zone non protette e dopo di che sono stati cambiati i permessi ai file in modo da non permettere la scrittura, volendo si potrebbe anche togliere la lettura.

Vulnerabilità 4:

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

tcp/5900/vnc

```
Nessus logged in using a password of "password".
```

Banalmente bisogna cambiare la password per il server VNC

```
msfadmin@metasploitable:~$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
Password:
Password too short
msfadmin@metasploitable:~$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
Password:
Warning: password truncated to the length of 8.
Verify:
Passwords do not match. Please try again.

Password:
Warning: password truncated to the length of 8.
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
msfadmin@metasploitable:~$
```