

Progetto S5/L5

Svolgimento:

- Scansione iniziale dove si vede il grafico con tutte le vulnerabilità e le vulnerabilità da risolvere (ScansioneInizio.pdf).
- Screenshot e spiegazione dei passaggi della remediation (RemediationMeta.pdf)
- Scansione dopo le modifiche che evidenzia la risoluzione dei problemi/vulnerabilità
- (il grafico che mostra tutte le vulnerabilità) ScansioneFine.pdf.
- Nota: i report possono essere lasciati in inglese.

Prendendo in considerazione 4 vulnerabilità del metasploitable :

- Bind Shell Backdoor Detection (critico)
- VNC Server 'password' Password (critico)
- NFS Exported Share Information Disclosure (critico)
- Samba Badlock Vulnerability (alto)

Caso 1)

Bind Shell Backdoor Detection : Una shell è in ascolto sulla porta (1524) remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può utilizzarlo collegandosi alla porta remota e inviando direttamente i comandi.

The screenshot displays the Nessus interface for a vulnerability scan. At the top, a tab labeled 'Vulnerabilities' shows a count of 64. The main section is titled 'Bind Shell Backdoor Detection' with a 'CRITICAL' severity indicator. The 'Description' states: '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.' The 'Solution' advises: 'Verify if the remote host has been compromised, and reinstall the system if necessary.' The 'Output' section shows a log entry: 'Nessus was able to execute the command "id" using the following request :'. Below this, it indicates a truncated output (limited to 10 lines) and shows a sample command prompt: 'root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root) root@metasploitable:/#'. The 'Risk Information' section on the right lists: 'Risk Factor: Critical', 'CVSS v3.0 Base Score 9.8', 'CVSS v3.0 Vector: 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', and 'CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C'. At the bottom, a table shows the port '1524 / tcp / wild_shell' and the host '192.168.32.101'.

Per risolvere questo problema ho aggiunto una regola nel firewall che nega l'accesso alla porta 1524

```

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

To Action From
--
1524:tcp DENY Anywhere
1524:udp DENY Anywhere
msfadmin@metasploitable:~$

```

utilizzando :

- sudo ufw enable** (per entrare nel firewall)
- sudo ufw deny 1524** (per aggiungere la regola)
- sudo ufw status** (per visualizzare la regola che ho aggiunto)

Caso 2)

VNC Server 'password' Password : Il server VNC in esecuzione sull'host remoto è protetto con una password debole. Nessus è riuscito ad accedere utilizzando l'autenticazione VNC e una password "password". Un utente malintenzionato remoto e non autenticato potrebbe sfruttare questa situazione per assumere il controllo del sistema.

Vulnerabilities
64

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.

Output

Nessus logged in using a password of "password".

To see debug logs, please visit individual host

Port ▲	Hosts
5900 / tcp / vnc	192.168.32.101

Plugin Details

Severity: Critical

ID: 61708

Version: \$Revision: 1.2 \$

Type: remote

Family: Gain a shell remotely

Published: August 29, 2012

Modified: September 24, 2015

Risk Information

Risk Factor: Critical

CVSS v2.0 Base Score: 10.0

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Vulnerability Information

Default Account: true

Exploited by Nessus: true

Per risolvere questo problema basta un cambio di password al Server VNC

```
root@metasploitable:~# ls
bin      dev      initrd   lost+found  nohup.out  root    sys      var
boot     etc      initrd.img media        opt        sbin    tmp      vmlinuz
cdrom    home    lib      mnt         proc       srv     usr

root@metasploitable:~# cd root
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# _
```

Si cerca il la cartella **.vnc** , con il comando **ls -a** riuscite a visualizzare anche file nascosti , la cartella l'ho trovata nella directory root .

Una volta entrati nella cartella **.vnc** con il comando **cd .vnc** digitate il codice “vncpasswd” (per cambiare la password) inserite la password da cambiare (questo caso ho utilizzato 123456 come password)

Caso 3)

NFS Exported Share Information Disclosure : Almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione. Un utente malintenzionato potrebbe essere in grado di sfruttare questo per leggere (ed eventualmente scrivere) file su host remoti.

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.

Output

The following NFS shares could be mounted :

+ /
+ Contents of / :
- .
- ..
- bin
- boot
- cdrom
more...

To see debug logs, please visit individual host

Port ▲	Hosts
2049 / udp / rpc-nfs	192.168.32.101 🔗

Plugin Details

Severity: Critical

ID: 11356

Version: 1.21

Type: remote

Family: RPC

Published: March 12, 2003

Modified: August 30, 2023

VPR Key Drivers

Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: Unproven
Age of Vuln: 730 days +
Product Coverage: Low
CVSSv3 Impact Score: 5.9
Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 5.9
Risk Factor: Critical
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Per risolvere questo problema serve aggiungere un regola al file exports entrando con il comando `-sudo nano /etc/exports`

```
GNU nano 2.0.7      File: 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 192.168.32.101(rw,sync,no_root_squash,no_subtree_check)

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

una volta entrati si aggiunge ip della macchina di metasploitable (192.168.32.101) salivate e uscite facendo **“ctrl + x”** poi digitando **“y”**.

Caso 3)

Samba Badlock Vulnerability : La versione di Samba, un server CIFS/SMB per Linux e Unix, in esecuzione sull'host remoto è affetta da un difetto, noto come Badlock, presente nel Security Account Manager (SAM) e nella Local Security Authority (Domain Policy) (LSAD) a causa di una negoziazione impropria del livello di autenticazione sui canali RPC (Remote Procedure Call). Un utente malintenzionato man-in-the-middle in grado di intercettare il traffico tra un client e un server che ospita un database SAM può sfruttare questa falla per forzare un downgrade del livello di autenticazione, che consente l'esecuzione di chiamate di rete Samba arbitrarie nel contesto dell'utente intercettato, come visualizzare o modificare dati sensibili di sicurezza nel database di Active Directory (AD) o disabilitare servizi critici.

Vulnerabilities
64

HIGH
Samba 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.

See Also

<http://badlock.org>
<https://www.samba.org/samba/security/CVE-2016-2118.html>

Output

```
Nessus detected that the Samba Badlock patch has not been applied.
```

To see debug logs, please visit individual host

Port ▲	Hosts
445 / tcp / cifs	192.168.32.101

Plugin Details

Severity: High
ID: 90509
Version: 1.8
Type: remote
Family: General
Published: April 13, 2016
Modified: November 20, 2019

VPR Key Drivers

Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: Unproven
Age of Vuln: 730 days +
Product Coverage: Medium
CVSSV3 Impact Score: 5.9
Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 6.7
Risk Factor: Medium
CVSS v3.0 Base Score 7.5

Ci sono due metodi per risolvere questo problema :

- 1) mettere la macchina online e aggiornarlo
- 2) chiudere le porte e quindi chiudere il servizio

Ho utilizzato il secondo metodo per non far connettere la macchina online

```
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

Ho aggiunto due regole al firewall - **ufw deny 445** e - **ufw deny 139** per chiudere le porte del servizio Samba

<input type="checkbox"/>	CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1	🔄	✎
<input type="checkbox"/>	CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2	🔄	✎
<input type="checkbox"/>	CRITICAL	📁 SSL (Multiple Issues)	Gain a shell remotely	3	🔄	✎
<input type="checkbox"/>	HIGH	7.5		NFS Shares World Readable	RPC	1	🔄	✎
<input type="checkbox"/>	MIXED	📁 SSL (Multiple Issues)	General	24	🔄	✎
<input type="checkbox"/>	MIXED	📁 ISC Bind (Multiple Issues)	DNS	5	🔄	✎
<input type="checkbox"/>	MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection	2	🔄	✎
<input type="checkbox"/>	MEDIUM	5.9	3.6	SSL Anonymous Cipher Suites Supported	Service detection	1	🔄	✎
<input type="checkbox"/>	MEDIUM	5.9	4.4	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1	🔄	✎
<input type="checkbox"/>	MEDIUM	5.3	4.0	HTTP TRACE / TRACK Methods Allowed	Web Servers	1	🔄	✎
<input type="checkbox"/>	MIXED	📁 SSH (Multiple Issues)	Misc.	6	🔄	✎
<input type="checkbox"/>	MIXED	📁 TLS (Multiple Issues)	Misc.	2	🔄	✎
<input type="checkbox"/>	MIXED	📁 TLS (Multiple Issues)	SMTP problems	2	🔄	✎

Dopo lo scan finale si può notare che gli 4 punti vulnerabili lo abbiamo risolto .