

Esercitazione S5L3

In questa esercitazione vediamo nel dettaglio il funzionamento di un vulnerability scanner e l'analisi dei risultati ottenuti da una scansione di una macchina target.

Nessus: spiegazione

Nessus è un software vulnerability scanner in grado di analizzare in modo dettagliato una macchina. La sua forza è quella di fornirci oltre a dei dati oggettivi anche delle informazioni dettagliate sulla macchina target.

Il funzionamento di Nessus consiste nell'inviare dei pacchetti in grado, in base alle risposte, di determinare:

- ping
- porte aperte
- applicazioni
- registri (aggiornamenti)
- servizi attivi sulle porte aperte
- versioni dei servizi.

In più, oltre a queste già importanti funzionalità, è in grado di fare una fase di exploit alla macchina. La fase di exploit consiste nell'attaccare la macchina cercando le vulnerabilità. Nessus è anche in grado di dare un report sulle vulnerabilità trovate classificandole per pericolosità. Ovviamente queste fasi possono richiedere un largo utilizzo della banda, in situazioni nel quale le scansioni debbano essere effettuate per conto di un'azienda è bene tener conto di questa informazione e accordarsi per trovare uno o più giorni utili per effettuare i test.

Nessus: funzionamento

Impostando un IP di destinazione (in questo caso ho utilizzato Metaspitable come target) e eventualmente customizzando la scannerizzazione si può iniziare la scansione. In questo caso ho utilizzato lo scan base.

Nessus: risultati

Finita la scansione ho ottenuto il report dello scan e sono state trovate diverse vulnerabilità:

Metaspitable / 192.168.1.12

Configure Audit Trail Launch Report Export

Vulnerabilities 69

Filter Search Vulnerabilities 69 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count
CRITICAL	10.0 *	7.4	0.6988	UnrealIRCd Backdoor Detection	Backdoors	1
CRITICAL	10.0 *			VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	9.8			Bind Shell Backdoor Detection	Backdoors	1
MIXED	Apache Tomcat (Multiple Issues)	Web Servers	4
CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5	5.9	0.0358	Samba Badlock Vulnerability	General	1
HIGH	7.5 *	5.9	0.015	rlogin Service Detection	Service detection	1
HIGH	7.5 *	5.9	0.015	rsh Service Detection	Service detection	1
HIGH	7.5			NFS Shares World Readable	RPC	1
MIXED	SSL (Multiple Issues)	General	28

Host Details

IP: 192.168.1.12
DNS: PENTOLAPTOP:station
MAC: 08:00:27:E6:BE:7F
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Start: Today at 7:02 AM
End: Today at 7:11 AM
Elapsed: 8 minutes
KB: Download

Vulnerabilities

Legend: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue)

Come si può vedere dall'immagine precedente si ha un elenco di vulnerabilità ordinate per criticità.

Aprendo nel dettaglio una criticità possiamo notare che il software in automatico ci fornisce una descrizione del problema, una soluzione, dei link utili per il dettaglio e la risoluzione del programma, l'output e la porta dove è stata trovata la vulnerabilità.

Metaspitable / Plugin #46882

[Back to Vulnerabilities](#)

Vulnerabilities 69

CRITICAL UnrealIRCd Backdoor Detection

Description
The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.

Solution
Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

See Also
<https://seclists.org/fulldisclosure/2010/jun/277>
<https://seclists.org/fulldisclosure/2010/jun/284>
<http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt>

Output
The remote IRC server is running as :
uid=0 (root) gid=0 (root)
To see debug logs, please visit individual host

Port ▲	Hosts
6667 / tcp / irc	192.168.1.12 🔗

In questo caso ad esempio ci dice che il VNC server è protetto da una password molto semplice e ci consiglia di assicurare il VNC server con una password più sicura.

Metaspitable / Plugin #61708

[Back to Vulnerabilities](#)

Vulnerabilities 69

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	192.168.1.12 🔗

HIGH	Samba Badlock Vulnerability
<h3>Description</h3> <p>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.</p>	
<h3>Solution</h3> <p>Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.</p>	
<h3>See Also</h3> <p>http://badlock.org https://www.samba.org/samba/security/CVE-2016-2118.html</p>	

Description

Solution

See Also

Output

To see debug logs, please visit individual host

In quest'altro caso invece è stata trovata una vulnerabilità sulla porta 445 e corrisponde al protocollo Samba. La criticità trovata in questo caso è una versione obsoleta del protocollo ed è ovviamente vulnerabile. Ci consiglia quindi l'aggiornamento del protocollo Samba.

MEDIUM

Unencrypted Telnet Server

Description

The remote host is running a Telnet server over an unencrypted channel.


Using Telnet over an unencrypted channel is not recommended as logins, passwords, and commands are transferred in cleartext. This allows a remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server.


SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional data streams such as an X11 session.

Solution

Disable the Telnet service and use SSH instead.

Output

```
Nessus collected the following banner from the remote Telnet server :  
----- snip -----  
  
more...  
  
To see debug logs, please visit individual host
```

Port ▲	Hosts
23 / tcp / telnet	192.168.1.12 

Description


Using Telnet over an unencrypted channel is not recommended as logins, passwords, and commands are transferred in cleartext. This allows a remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server.

SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional data streams such as an X11 session.

Solution

Output

To see debug logs, please visit individual host

Port ▲	Hosts
23 / tcp / telnet	192.168.1.12 

Come si può notare le vulnerabilità vengono classificate più o meno critiche, e questo può farlo automaticamente grazie a una sua tabella o a un suo database dove vada a confrontare i risultati ottenuti .