

SCAN CON NESSUS

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1
CRITICAL	10.0 *	7.4	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	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1
CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1
MIXED	DNS (Multiple Issues)	DNS	5
CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5		NFS Shares World Readable	RPC	1
HIGH	7.5 *	6.7	rlogin Service Detection	Service detection	1
HIGH	7.5 *	6.7	rsh Service Detection	Service detection	1
HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1
MIXED	SSL (Multiple Issues)	General	28

1 VULNERABILITA'

Vulnerabilities 71

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	192.168.178.63

Il messaggio indica che il server VNC su un computer remoto ha una password molto debole e Nessus è riuscito ad accedere usando la password 'password'. Questa situazione è pericolosa perché significa che chiunque, da remoto e senza autenticazione, potrebbe sfruttare questa debolezza per prendere il controllo completo del computer.

SOLUZIONE: cambiare la password con una piu forte oppure controllare l'accesso,ovvero impostare il server in modo tale che solo alcuni pc possono accedere.

2 VULNERABILITA'

gerardo / Plugin #51988 Configure Audit Tr

[Back to Vulnerabilities](#)

Vulnerabilities 71

CRITICAL Bind Shell Backdoor Detection < >

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.

Output

```
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 -----
```

To see debug logs, please visit individual host

Port ▲	Hosts
1524 / tcp / wild_shell	192.168.178.63 🔗

Su una porta (1524) remota del sistema, c'è una shell in ascolto senza richiedere alcuna autenticazione. Questo significa che chiunque, senza dover fornire alcuna credenziale, potrebbe connettersi a questa porta e inviare comandi direttamente al sistema.

SOLUZIONE: chiudere la porta in questione oppure impostare un sistema di autenticazione su questa porta in modo da limitarne l'accesso

3 VULNERABILITA'

Vulnerabilities71

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	192.168.178.63

Sul computer remoto è attivo un servizio Telnet su un canale non crittografato(porta 23). L'utilizzo di Telnet su un canale non crittografato non è consigliato perché le informazioni di accesso: password e comandi vengono trasferite in chiaro. Questo significa che un attaccante remoto, posizionato nel mezzo della comunicazione (man-in-the-middle), potrebbe intercettare una sessione Telnet per ottenere credenziali o altre informazioni sensibili e anche modificare il traffico tra il client e il server.

SOLUZIONE: utilizzare un servizio SSH poichè protegge le credenziali da intercettazioni