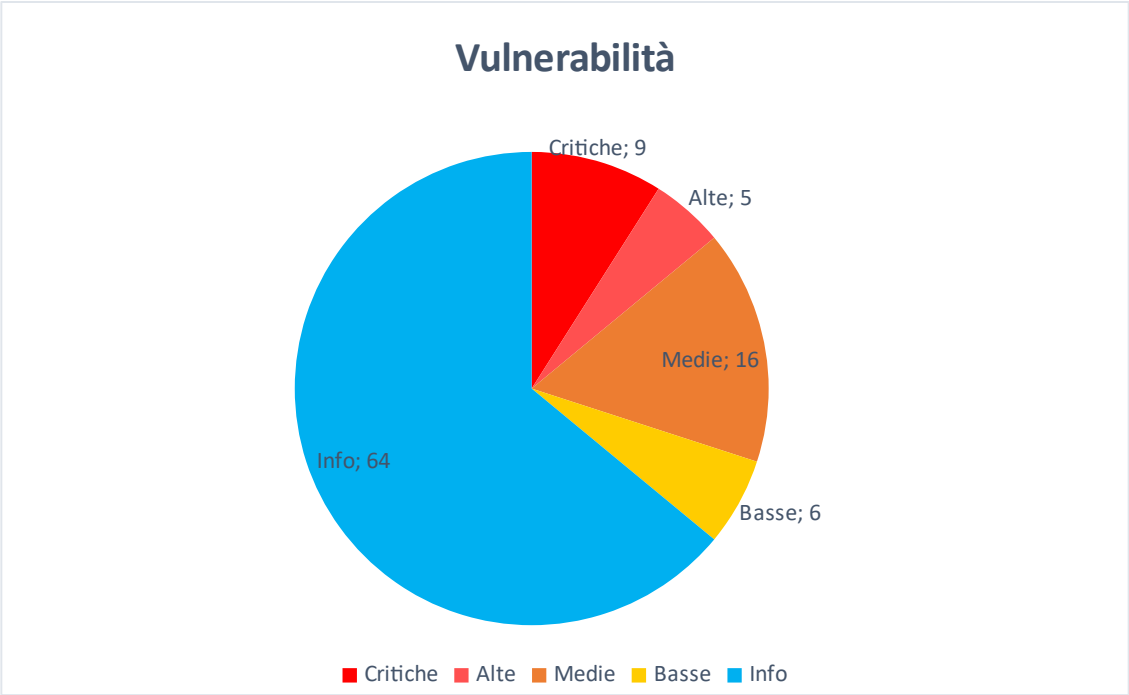


Scansione Inizio

Hosts		Vulnerabilities		Remediations		Notes		History	
Filter		Search Vulnerabilities		68 Vulnerabilities					
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		Bind Shell Backdoor Detection	Backdoors	1				
MIXED	Apache Tomcat (Multiple Issues)	Web Servers	4				
CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3				
MIXED	SSL (Multiple Issues)	Service detection	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				
MIXED	ISC Bind (Multiple Issues)	DNS	5				
MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection	2				
MEDIUM	6.5		Unencrypted Telnet Server	Misc.	1				
MEDIUM	5.9	4.4	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1				
MIXED	SSH (Multiple Issues)	Misc.	6				



NFS Export Share Information Disclosure

The screenshot shows a Nessus vulnerability report for 'NFS Exported Share Information Disclosure'. The report is categorized as 'CRITICAL'. The description states: '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.' The solution suggests: 'Configure NFS on the remote host so that only authorized hosts can mount its remote shares.' The output section shows a terminal-like view of the command 'df -h' and its output, indicating that the root filesystem is mounted on '/'. Below the output, there is a table with the following data:

Port	Hosts
2049 / udp / rpc-nfs	192.168.30.100

NFS = Network File System è un protocollo di sistema, che consente ai clienti di accedere a file e directory su una rete, questo vuol dire che sono accessibili da remoto. Se gli NFS non sono protetti correttamente c'è la possibilità che terze parti possano accedere a queste informazioni; modificandole o eventualmente divulgarle.

VNC Server 'password' Password

The screenshot shows a Nessus vulnerability report for 'VNC Server 'password' Password'. The report is categorized as 'CRITICAL'. The description states: '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.' The solution suggests: 'Secure the VNC service with a strong password.' The output section shows a terminal-like view of the command 'vncviewer 192.168.30.100:5900' and its output, indicating that the VNC server is running on port 5900. Below the output, there is a table with the following data:

Port	Hosts
5900 / tcp / vnc	192.168.30.100

VNC= Virtual Network Computing è un protocollo che consente a un utente di controllare un computer da remoto. Nessus consiglia di cambiare la password attuale con una più complessa.

Bind Shell Backdoor Detection

Hosts1

Vulnerabilities56

Notes1

History13

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

192.168.30.100

Una Shell è in ascolto su una porta (la 1524) remota senza autenticazione. Questa può essere utilizzata da un attaccante che può collegarsi e inviare comandi da remoto.

Rexecd Service Detection

rexecd Service Detection

CRITICAL

Nessus Plugin ID 10203

Information

Dependencies

Dependents

Changelog

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.

Il servizio Rexecd è progettato per consentire agli utenti di una rete di eseguire comandi in remoto su un sistema. Tuttavia, è importante notare che Rexecd non fornisce un mezzo di autenticazione adeguato, il che significa che potrebbe essere abusato da un attaccante per eseguire comandi non autorizzati su un sistema di terze parti o per effettuare scansioni indesiderate su altre macchine.