--S5L4--
Oggi abbiamo scaricato e installato Nessus;
Dopo la configurazione del programma abbiamo eseguito,come richiesto dall'esercizio,la scansione basic network scan su metasploitable e abbiamo rilevato diverse vulnerabilita' sia lievi che critiche.
Tra quelle critiche possiamo notare che ci sono 2 backdoor e l'utilizzo di una password molto debole per accedere alla M.v.
Tra le eventuali soluzioni dovremmo per cominciare parlare con il responsabile dell'amministrazione interna e successivamente procedere con le modifiche al fine di evitare possibili attacchi da parte dell'esterno.

scan meta

‹ Back to My Scans

Configure | Audit Trail | Launch | Report | Export

Hosts 1 | Vulnerabilities 71 | Remediations 3 | History 1

Filter | Search Hosts | 1 Host

Host	Vulnerabilities
192.168.49.101	12 7 24 8 133

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 2:35 PM
End:	Today at 2:54 PM
Elapsed:	19 minutes

Vulnerabilities

Vulnerabilities 71

Filter | Search Vulnerabilities | 71 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *	7.4	UnrealIRCd Backdoor Detection	Backdoors	1
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 *		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	6.7	Samba Badlock Vulnerability	General	1
HIGH	7.5 *	5.9	rlogin Service Detection	Service detection	1
HIGH	7.5 *	5.9	rsh Service Detection	Service detection	1
HIGH	7.5		NFS Shares World Readable	RPC	1

Plugin ID: 42256

Host Details

IP:	192.168.49.101
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Start:	Today at 8:35 AM
End:	Today at 8:54 AM
Elapsed:	19 minutes
KB:	Download

Vulnerabilities