




Scansione Iniziale con Nessus



Scansione Vulnerabilità

<input type="checkbox"/> Sev ▼	CVSS ▼	VPR ▼	Name ▲	Family ▲	Count ▼	⚙
<input type="checkbox"/> CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1	⊖ ✎
<input type="checkbox"/> CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1	⊖ ✎
<input type="checkbox"/> CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1	⊖ ✎
<input type="checkbox"/> CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2	⊖ ✎
<input type="checkbox"/> CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1	⊖ ✎
<input type="checkbox"/> CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1	⊖ ✎
<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"/> HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1	⊖ ✎
<input type="checkbox"/> MIXED	 SSL (Multiple Issues)	General	28	⊖ ✎
<input type="checkbox"/> MIXED	 ISC Bind (Multiple Issues)	DNS	5	⊖ ✎

Plugin ID: 104743

Come mostrato nella slide precedente sono presenti molteplici vulnerabilità all'interno di Metasploitable, ognuna di esse con il suo indice di rischio.

Per questo esercizio ho deciso di prendere in esame, e risolvere, 4 vulnerabilità:

- NSF Exported Share Information Disclosure

- VNC Server 'password' Password

- Bind Shell Backdoor Detection

- Samba Badlock Vulnerability