

Obiettivo: prendere familiarità con nessus

Abbiamo usato lo strumento nessus per individuare le vulnerabilità di metasploitable.

Dal report si possono identificare varie vulnerabilità di sistema tra cui alcune di livello critico.

Abbiamo analizzato le criticità e possibili soluzioni

meta basic scan / 192.168.49.101

Back to Hosts

Configure Audit Trail Launch Reports Export

Vulnerabilities

Filter Search Vulnerabilities 55 Vulnerabilities

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	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1	○	✓
<input type="checkbox"/> CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2	○	✓
<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	6.7	Samba Badlock Vulnerability	General	1	○	✓
<input type="checkbox"/> HIGH	7.5		NFS Shares World Readable	RPC	1	○	✓
<input type="checkbox"/> MEDIUM	—	—	📁 SSL (Multiple Issues)	General	28	○	✓
<input type="checkbox"/> MEDIUM	—	—	📁 ISC Bind (Multiple Issues)	DNS	5	○	✓
<input type="checkbox"/> MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection	2	○	✓
<input type="checkbox"/> MEDIUM	5.9	4.4	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened ebcryption)	Misc.	1	○	✓
<input type="checkbox"/> MEDIUM	5.9	3.6	SSL Anonymous Cipher Suites Supported	Service detection	1	○	✓
<input type="checkbox"/> MEDIUM	—	—	📁 SSH (Multiple Issues)	Misc.	6	○	✓
<input type="checkbox"/> MEDIUM	—	—	📁 SMB (Multiple Issues)	Misc.	2	○	✓
<input type="checkbox"/> MEDIUM	—	—	📁 TLS (Multiple Issues)	Misc.	2	○	✓
<input type="checkbox"/> MEDIUM	—	—	📁 TLS (Multiple Issues)	SMTP problems	2	○	✓
<input type="checkbox"/> LOW	2.6 *		X Server Detection	Service detection	1	○	✓

Host Details

IP: 192.168.49.101
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Start: Today at 7:36 AM
End: Today at 8:02 AM
Elapsed: 25 minutes
KB: [Download](#)

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

Abbiamo utilizzato lo scan di base, indicando di utilizzare solo le porte base e le impostazioni assessment e advanced impostate su default