

### Traccia:


Esercizio Traccia Effettuare un Vulnerability Assessment con Nessus sulla macchina Metasploitable indicando come target solo le porte comuni (potete scegliere come scansione il «basic network scan», o l'advanced e poi configurarlo) A valle del completamento della scansione, analizzate attentamente il report per ognuna delle vulnerabilità riportate, approfondendo qualora necessario con i link all'interno dei report e/o con contenuto da Web.

### Ambiente:

- Kali Linux VM 192.168.1.100 Bridged
- Metasploitable VM 192.168.1.101 Bridged

### Svolgimento:

#### Scan Details

Policy: Basic Network Scan  
Status: Completed  
Severity Base: CVSS v3.0   
Scanner: Local Scanner  
Start: Today at 5:45 AM  
End: Today at 6:12 AM  
Elapsed: 27 minutes

#### Vulnerabilities



<input type="checkbox"/> Host	Vulnerabilities ▼
<input type="checkbox"/> 192.168.1.101	<div><div>Critical: 9</div><div>High: 4</div><div>Medium: 21</div><div>Low: 8</div><div>Info: 102</div></div>

## Report:

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	<a href="#">134862</a>	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	<a href="#">51988</a>	Bind Shell Backdoor Detection
CRITICAL	9.8	-	<a href="#">20007</a>	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	-	<a href="#">33850</a>	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	5.1	<a href="#">32314</a>	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	5.1	<a href="#">32321</a>	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	-	<a href="#">61708</a>	VNC Server 'password' Password
HIGH	8.6	5.2	<a href="#">136769</a>	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	5.1	<a href="#">42873</a>	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	5.9	<a href="#">90509</a>	Samba Badlock Vulnerability
MEDIUM	6.5	3.6	<a href="#">139915</a>	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	-	<a href="#">51192</a>	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	<a href="#">57582</a>	SSL Self-Signed Certificate
MEDIUM	6.5	-	<a href="#">104743</a>	TLS Version 1.0 Protocol Detection

MEDIUM	5.9	4.4	<a href="#">136808</a>	ISC BIND Denial of Service
MEDIUM	5.9	4.4	<a href="#">31705</a>	SSL Anonymous Cipher Suites Supported
MEDIUM	5.9	4.4	<a href="#">89058</a>	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
MEDIUM	5.9	4.4	<a href="#">65821</a>	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	-	<a href="#">57608</a>	SMB Signing not required
MEDIUM	5.3	-	<a href="#">15901</a>	SSL Certificate Expiry
MEDIUM	5.3	-	<a href="#">45411</a>	SSL Certificate with Wrong Hostname
MEDIUM	5.3	-	<a href="#">26928</a>	SSL Weak Cipher Suites Supported
MEDIUM	4.0*	6.3	<a href="#">52611</a>	SMTP Service STARTTLS Plaintext Command Injection
MEDIUM	4.3*	-	<a href="#">90317</a>	SSH Weak Algorithms Supported
MEDIUM	4.3*	3.7	<a href="#">81606</a>	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
LOW	3.7	3.6	<a href="#">70658</a>	SSH Server CBC Mode Ciphers Enabled
LOW	3.7	-	<a href="#">153953</a>	SSH Weak Key Exchange Algorithms Enabled
LOW	3.7	3.9	<a href="#">83738</a>	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
LOW	3.4	5.1	<a href="#">78479</a>	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
LOW	2.1*	4.2	<a href="#">10114</a>	ICMP Timestamp Request Remote Date Disclosure
LOW	2.6*	-	<a href="#">71049</a>	SSH Weak MAC Algorithms Enabled
LOW	2.6*	-	<a href="#">10407</a>	X Server Detection
INFO	N/A	-	<a href="#">10223</a>	RPC portmapper Service Detection

**Description and solution:**