

# Scansione Finale



VULNERABILITY  
FIXED

# Scansione Finale

meta 3

[← Back to My Scans](#)

Configure

Audit Trail

Launch ▼

Report

Export ▼

Hosts 1 Vulnerabilities 55 Remediations 1 Notes 2 History 1

Filter ▼ Search Vulnerabilities 🔍 55 Vulnerabilities

<input type="checkbox"/>	Sev ▼	CVSS ▼	VPR ▼	Name ▲	Family ▲	Count ▼	⚙
<input type="checkbox"/>	CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	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	...	...	📁 SSL (Multiple Issues)	Gain a shell remotely	3	🔄 ✎
<input type="checkbox"/>	MIXED	...	...	📁 SSL (Multiple Issues)	General	24	🔄 ✎
<input type="checkbox"/>	MIXED	...	...	📁 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	3.6	SSL Anonymous Cipher Suites Supported	Service detection	1	🔄 ✎
<input type="checkbox"/>	MEDIUM	5.9	4.4	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1	🔄 ✎
<input type="checkbox"/>	MEDIUM	5.3	4.0	HTTP TRACE / TRACK Methods Allowed	Web Servers	1	🔄 ✎
<input type="checkbox"/>	MIXED	...	...	📁 SSH (Multiple Issues)	Misc.	6	🔄 ✎
<input type="checkbox"/>	MIXED	...	...	📁 TLS (Multiple Issues)	Misc.	2	🔄 ✎

TLS (Multiple Issues)

## Scan Details

Policy: Basic Network Scan  
Status: Completed  
Severity Base: CVSS v3.0 ✎  
Scanner: Local Scanner  
Start: Today at 4:48 PM  
End: Today at 5:17 PM  
Elapsed: 28 minutes

## Vulnerabilities



Dopo aver fixato le 4 vulnerabilità scelte, eseguo nuovamente una scansione con Nessus; il risultato è quello sperato: le 4 vulnerabilità non sono più presenti, questo indica che tutto è andato a buon fine.

Come si può notare però rimangono ancora altre vulnerabilità, molte delle quali sarebbero risolvibili semplicemente aggiornando la macchina Metasploitable

**Grazie**