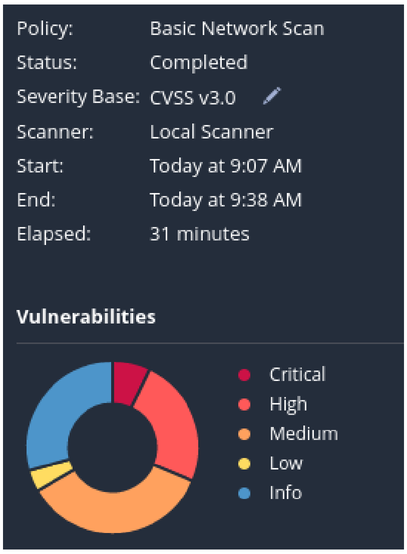
Consegna S5L4

Obiettivi: Effettuare un Vulnerability Assessment con Nessus sulla macchina Metasploitable indicando come target solo le porte comuni.

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 dal Web.

Risoluzione: L’esercizio richiede di effettuare una scansione delle vulnerabilità della macchina virtuale Metasploitable tramite Nessus. Una volta Installato Nessus ho deciso di impostare la modalità di scansione di default. Una volta effettuata la scansione questi sono i risultati:



Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 9:07 AM
End: Today at 9:38 AM
Elapsed: 31 minutes

Vulnerabilities

Da questa panoramica possiamo capire che delle porte analizzate:

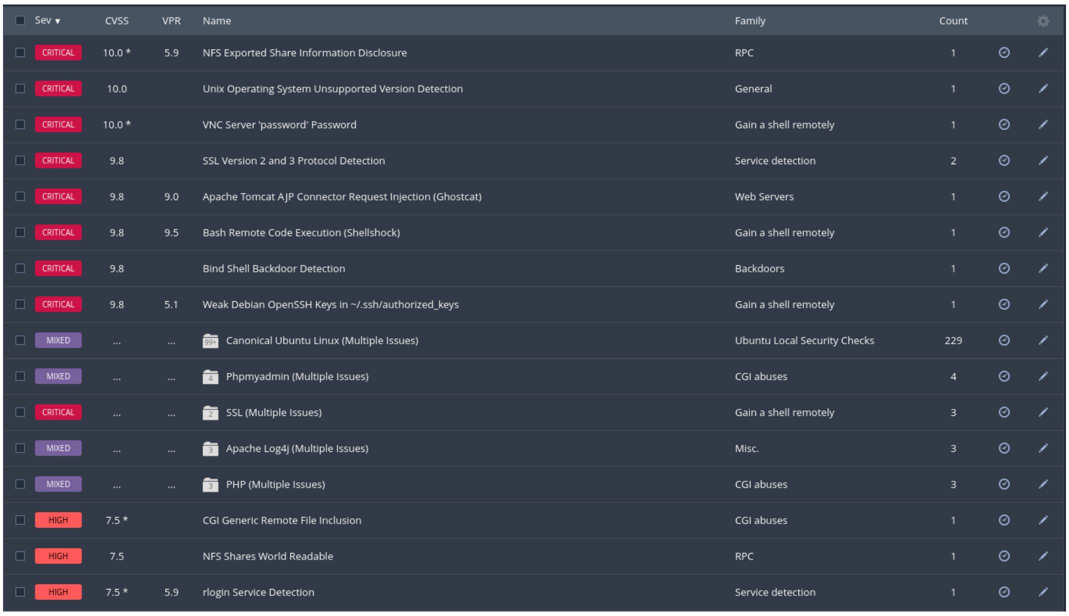
- **33** sono in una condizione di rischio **critica**

- **96** sono in una condizione di rischio **alta**

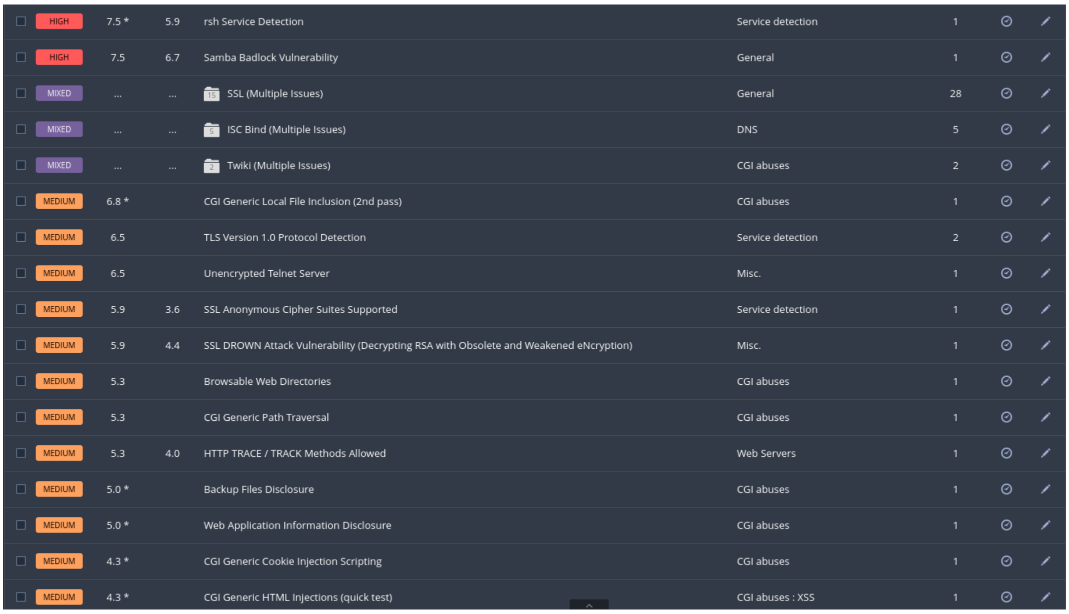
- **149** sono in una condizione di rischio **media**

- **18** sono in una condizione di rischio **bassa**

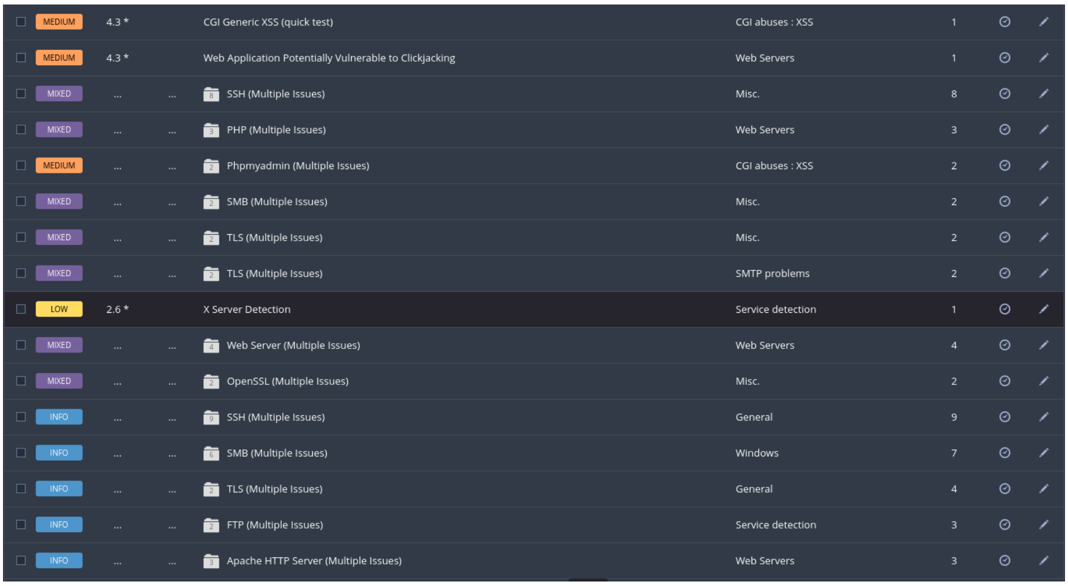
Oltre alla lista delle porte scansionate vengono riportati degli esempi di consigli su come risolvere alcune problematiche legate alla sicurezza tramite dei link resi disponibili da Nessus:



□	Sev ▾	CVSS	VPR	Name	Family	Count
□	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	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1
□	CRITICAL	9.8	9.5	Bash Remote Code Execution (Shellshock)	Gain a shell remotely	1
□	CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1
□	CRITICAL	9.8	5.1	Weak Debian OpenSSH Keys in ~/.ssh/authorized_keys	Gain a shell remotely	1
□	MIXED	...	...	Canonical Ubuntu Linux (Multiple Issues)	Ubuntu Local Security Checks	229
□	MIXED	...	...	Phpmyadmin (Multiple Issues)	CGI abuses	4
□	CRITICAL	...	...	SSL (Multiple Issues)	Gain a shell remotely	3
□	MIXED	...	...	Apache Log4j (Multiple Issues)	Misc.	3
□	MIXED	...	...	PHP (Multiple Issues)	CGI abuses	3
□	HIGH	7.5 *		CGI Generic Remote File Inclusion	CGI abuses	1
□	HIGH	7.5		NFS Shares World Readable	RPC	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	6.7	Samba Badlock Vulnerability	General	1
□	MIXED	...	...	SSL (Multiple Issues)	General	28
□	MIXED	...	...	ISC Bind (Multiple Issues)	DNS	5
□	MIXED	...	...	Twiki (Multiple Issues)	CGI abuses	2
□	MEDIUM	6.8 *		CGI Generic Local File Inclusion (2nd pass)	CGI abuses	1
□	MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection	2
□	MEDIUM	6.5		Unencrypted Telnet Server	Misc.	1
□	MEDIUM	5.9	3.6	SSL Anonymous Cipher Suites Supported	Service detection	1
□	MEDIUM	5.9	4.4	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1
□	MEDIUM	5.3		Browsable Web Directories	CGI abuses	1
□	MEDIUM	5.3		CGI Generic Path Traversal	CGI abuses	1
□	MEDIUM	5.3	4.0	HTTP TRACE / TRACK Methods Allowed	Web Servers	1
□	MEDIUM	5.0 *		Backup Files Disclosure	CGI abuses	1
□	MEDIUM	5.0 *		Web Application Information Disclosure	CGI abuses	1
□	MEDIUM	4.3 *		CGI Generic Cookie Injection Scripting	CGI abuses	1
□	MEDIUM	4.3 *		CGI Generic HTML Injections (quick test)	CGI abuses : XSS	1



□	MEDIUM	4.3 *		CGI Generic XSS (quick test)	CGI abuses : XSS	1
□	MEDIUM	4.3 *		Web Application Potentially Vulnerable to Clickjacking	Web Servers	1
□	MIXED	...	...	SSH (Multiple Issues)	Misc.	8
□	MIXED	...	...	PHP (Multiple Issues)	Web Servers	3
□	MEDIUM	...	...	Phpmyadmin (Multiple Issues)	CGI abuses : XSS	2
□	MIXED	...	...	SMB (Multiple Issues)	Misc.	2
□	MIXED	...	...	TLS (Multiple Issues)	Misc.	2
□	MIXED	...	...	TLS (Multiple Issues)	SMTP problems	2
□	LOW	2.6 *		X Server Detection	Service detection	1
□	MIXED	...	...	Web Server (Multiple Issues)	Web Servers	4
□	MIXED	...	...	OpenSSL (Multiple Issues)	Misc.	2
□	INFO	...	...	SSH (Multiple Issues)	General	9
□	INFO	...	...	SMB (Multiple Issues)	Windows	7
□	INFO	...	...	TLS (Multiple Issues)	General	4
□	INFO	...	...	FTP (Multiple Issues)	Service detection	3
□	INFO	...	...	Apache HTTP Server (Multiple Issues)	Web Servers	3

http://seclists.org/oss-sec/2014/q3/650
http://www.nessus.org/u?dacf7829
https://www.invisiblethreat.ca/post/shellshock/

https://www.schneier.com/academic/paperfiles/paper-ssl.pdf
http://www.nessus.org/u?b06c7e95
http://www.nessus.org/u?247c4540
https://www.openssl.org/~bodo/ssl-poodle.pdf
http://www.nessus.org/u?5d15ba70
https://www.imperialviolet.org/2014/10/14/poodle.html
https://tools.ietf.org/html/rfc7507
https://tools.ietf.org/html/rfc7568

http://badlock.org
https://www.samba.org/samba/security/CVE-2016-2118.html

https://en.wikipedia.org/wiki/Remote_File_Inclusion
http://projects.webappsec.org/w/page/13246955/Remote%20File%20Inclusion

https://en.wikipedia.org/wiki/Remote_File_Inclusion