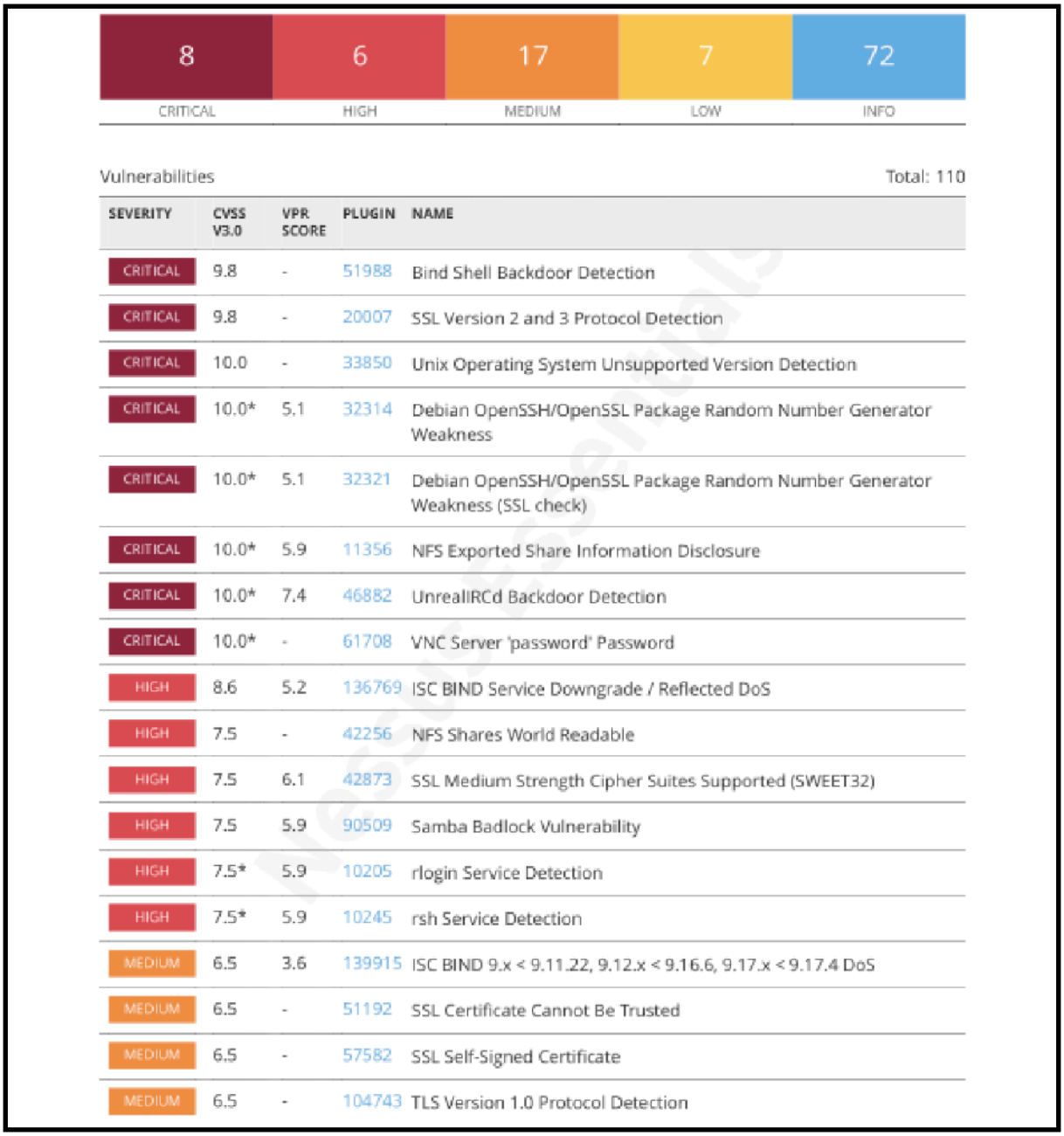
M3_W12D1(2)

Analisi delle vulnerabilità rilevate sulla macchina target Metasploitable.

Il Vulnerabilty Assessment effettuato sull'indirizzo IP 192.168.50.100 appartenente alla macchina Metasploitable ha evidenziato significative vulnerabilità sull'host. Di seguito la lista completa degli exploit:

10 Critical Vulnerabilities
7 High Vulnerabilities
23 Medium Vulnerabilities
8 Low Vulnerabilities
72 Info System



8	6	17	7	72
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 110

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	5.1	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	5.1	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	7.4	46882	UnrealIRCd Backdoor Detection
CRITICAL	10.0*	-	61708	VNC Server 'password' Password
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42256	NFS Shares World Readable
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	5.9	90509	Samba Badlock Vulnerability
HIGH	7.5*	5.9	10205	rlogin Service Detection
HIGH	7.5*	5.9	10245	rsh Service Detection
MEDIUM	6.5	3.6	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection

MEDIUM	6.5	-	42263	Unencrypted Telnet Server
MEDIUM	5.9	4.4	136808	ISC BIND Denial of Service
MEDIUM	5.9	3.6	31705	SSL Anonymous Cipher Suites Supported
MEDIUM	5.9	4.4	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
MEDIUM	5.9	3.6	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	4.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	-	57608	SMB Signing not required
MEDIUM	5.3	-	15901	SSL Certificate Expiry
MEDIUM	5.3	-	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.3	-	26928	SSL Weak Cipher Suites Supported
MEDIUM	4.0*	6.3	52611	SMTP Service STARTTLS Plaintext Command Injection
MEDIUM	4.3*	-	90317	SSH Weak Algorithms Supported
MEDIUM	4.3*	4.5	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
LOW	3.7	3.6	70658	SSH Server CBC Mode Ciphers Enabled
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	3.7	4.5	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
LOW	3.7	4.5	83738	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
LOW	3.4	5.1	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
LOW	2.6*	-	71049	SSH Weak MAC Algorithms Enabled
LOW	2.6*	-	10407	X Server Detection

Sulla base del grafico sotto riportato agiremo sugli exploit segnalati da Nessus per agire in maniera tempestiva su tutti gli exploit che presentano uno score CVSS impattante sul livello di criticità.

Vulnerabilities		
Level	**CVSS**	**Remediation Action**
20007 - SSL Version 2 and 3 Protocol Detection	10,0	Disabilitare SSL 2.0 - 3.0 ed Abilitare TLS 1.2
32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	10,0	Tutto il materiale crittografato SSH, SSL e OpenVPN dovrà essere crittografato
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	7,5	Configurare diversamente le applicazioni che utilizzano Chiare
90509 - Samba Badlock Vulnerability	7,5	Aggiornare Samba alla versione 4.2.11 o successiva
11213 - HTTP TRACE / TRACK Methods Allowed	5,3	Disabilita i metodi HTTP TRACE e TRACK
12085 - Apache Tomcat Default Files	5,3	Segui le istruzioni Tomcat o OWASP per modificare la pagina default di errore