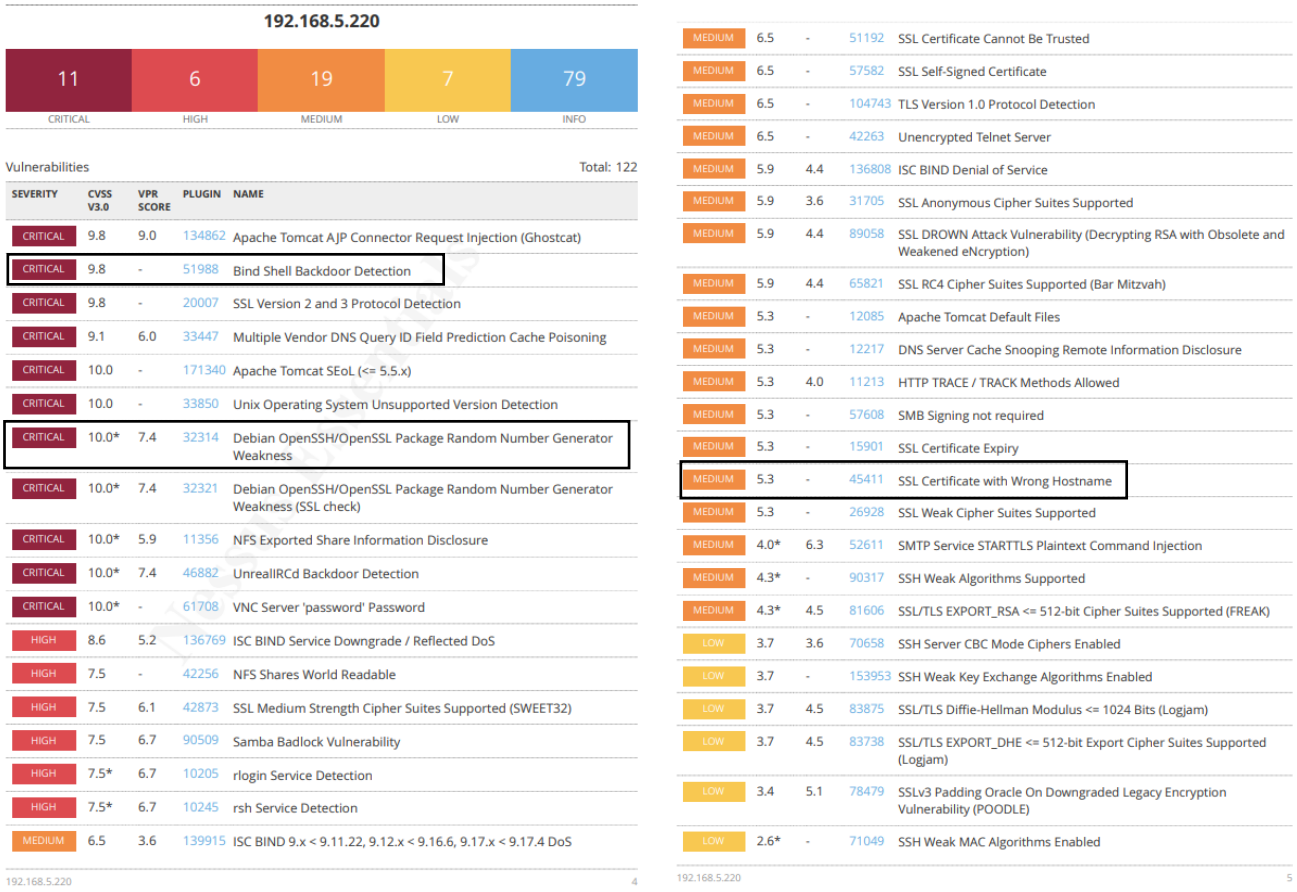
[CONSEGNA SETTIMANA 5 LEZIONE 4]

Vulnerability assessment

La fase successiva nel processo di pentesting viene chiamata *vulnerability assessment*, ovvero la ricerca di possibili vulnerabilità all'interno del target che potrebbero essere exploitate da individui malintezionati.

Di seguito sono elencate le vulnerabilità riscontrate sulla macchina metasploitable.



192.168.5.220

CRITICAL	HIGH	MEDIUM	LOW	INFO
11	6	19	7	79

Vulnerabilities — Total: 122

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.1	6.0	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
CRITICAL	10.0	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	7.4	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	7.4	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	6.7	90509	Samba Badlock Vulnerability
HIGH	7.5*	6.7	10205	rlogin Service Detection
HIGH	7.5*	6.7	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

192.168.5.220 4

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	4.4	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	-	12085	Apache Tomcat Default Files
MEDIUM	5.3	-	12217	DNS Server Cache Snooping Remote Information Disclosure
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

192.168.5.220 5

Di queste vulnerabilità ne prenderemo in esame 3, due di importanza critica e una media.

VULNERABILITA' #1

Bind Shell Backdoor Detection

SPIEGAZIONE *: La macchina metasploitable è in ascolto su una porta, a cui è possibile connettersi.Questa vulnerabilità risulta ad importanza critica in quanto connettendosi a tale porta tramite netcat è possibile avere il controllo sulla macchina.*

POSSIBILE SOLUZIONE*: Chiudere la porta associata o aggiornare il sistema e ripetere la scansione.*

VULNERABILITA' #2

Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

SPIEGAZIONE *: Nel 2008 il sistema operativo Debian risultò avere una falla nel sistema di generazione di numeri casuali, questo ha portato le chiavi di criptazione SSH e SSL ad essere facilmente prevedibili.*

POSSIBILE SOLUZIONE*: Aggiornare il sistema, rigenerare le chiavi SSH e SSL e ripetere la scansione.*

VULNERABILITA' #3

SSL Certificate With Wrong Hostname

SPIEGAZIONE *: Questa vulnerabilità avviene solitamente quando c'è un errore durante la generazione del certificato SSL, in particolare il CN (commonName) assegnato è per una macchina differente.*

POSSIBILE SOLUZIONE*: Generare o comprare un nuovo certificato SSL per la macchina e ripetere la scansione.*