M3 D7

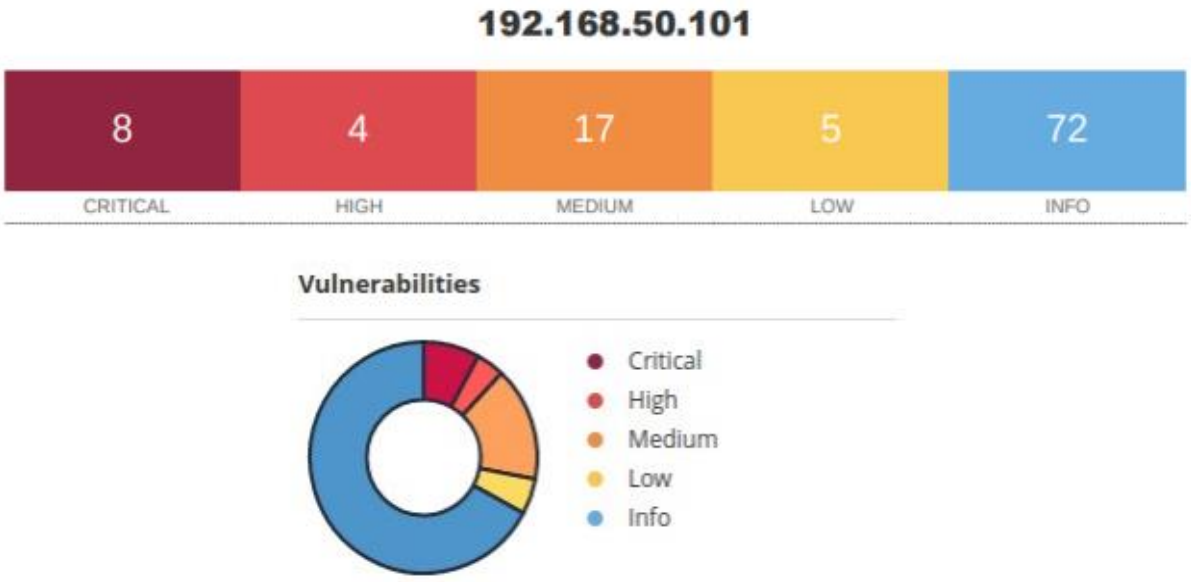
ES 2

ESERCIZIO GIORNO 3 – VULNERABILITY ASSESSMENT

Il report che si presenta è un REPORT PER LA CLASSE DIRIGENZIALE.

Il report in questione, a differenza di un report tecnico, deve avere la caratteristica di essere immediato e poco interpretabile.

Deve far saltare agli occhi la raccolta delle info e vulnerabilità più gravi, indicizzando con grafici la pericolosità delle varie vulnerabilità e le azioni correttive da apportare.
Necessità di pochi dettagli tecnici.



Dalle rosse scuro (gravità elevata) alle azzurre (quasi innocue).

Priorità di risoluzione

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	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*	-	61708	VNC Server 'password' Password

Si consiglia di risolvere in primis le vulnerabilità di grado critico, in quanto sono facilmente identificabili e di conseguenza sfruttabili da utenti malintenzionati. Sfruttando tali falle sarebbe possibile compromettere la quasi totalità della funzionalità del sistema.

Alcune sono facilmente risolvibili, altre invece richiedono interventi sul sistema in quanto ormai datato e non più supportato a livello di security.

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

Successivamente si andrà a risolvere quelle di grado alto, le quali comportano un serio rischio per la riservatezza dei dati.

La risoluzione a questo livello è meno invasiva in quanto si limita, quando possibile, all'aggiornamento dei già servizi utilizzati.

MEDIUM	6.8	5.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
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	5.9	5.1	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)

Le criticità di livello medio espongono il sistema alle stesse criticità delle precedenti ma il loro exploit richiede conoscenze di sistemi più avanzate da parte di un potenziale attaccante.

La loro risoluzione andrà a richiedere un aggiornamento di alcuni servizi mentre per altre sarà necessario la modifica delle configurazioni dei servizi esposti a vulnerabilità. Si fa anche presente la non validità di alcuni certificati che necessitano di essere aggiornati per evitare la compromissione della riservatezza dei vari canali e servizi cifrati.

LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	3.7	4.5	83738	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
LOW	2.6*	2.5	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6*	-	71049	SSH Weak MAC Algorithms Enabled
LOW	2.6*	-	10407	X Server Detection

Le ultime analizzate sono state quelle di basso livello. Sono problemi legati alla crittografia, vanno dunque disabilitati oppure aggiornati, dove possibile.

INFO	N/A	-	39521	Backported Security Patch Detection (WWW)
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	10028	DNS Server BIND version Directive Remote Version Detection
INFO	N/A	-	11002	DNS Server Detection
INFO	N/A	-	72779	DNS Server Version Detection
INFO	N/A	-	35371	DNS Server hostname.bind Map Hostname Disclosure
INFO	N/A	-	132634	Deprecated SSLv2 Connection Attempts
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	10092	FTP Server Detection
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	11156	IRC Daemon Version Detection
INFO	N/A	-	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure

Per completezza abbiamo analizzato anche diverse potenziali vulnerabilità. Se mantenute aggiornate non dovrebbero compromettere la sicurezza; un controllo periodico delle regole di firewall ed una corretta configurazione servizi è più di quanto necessario allo scopo.