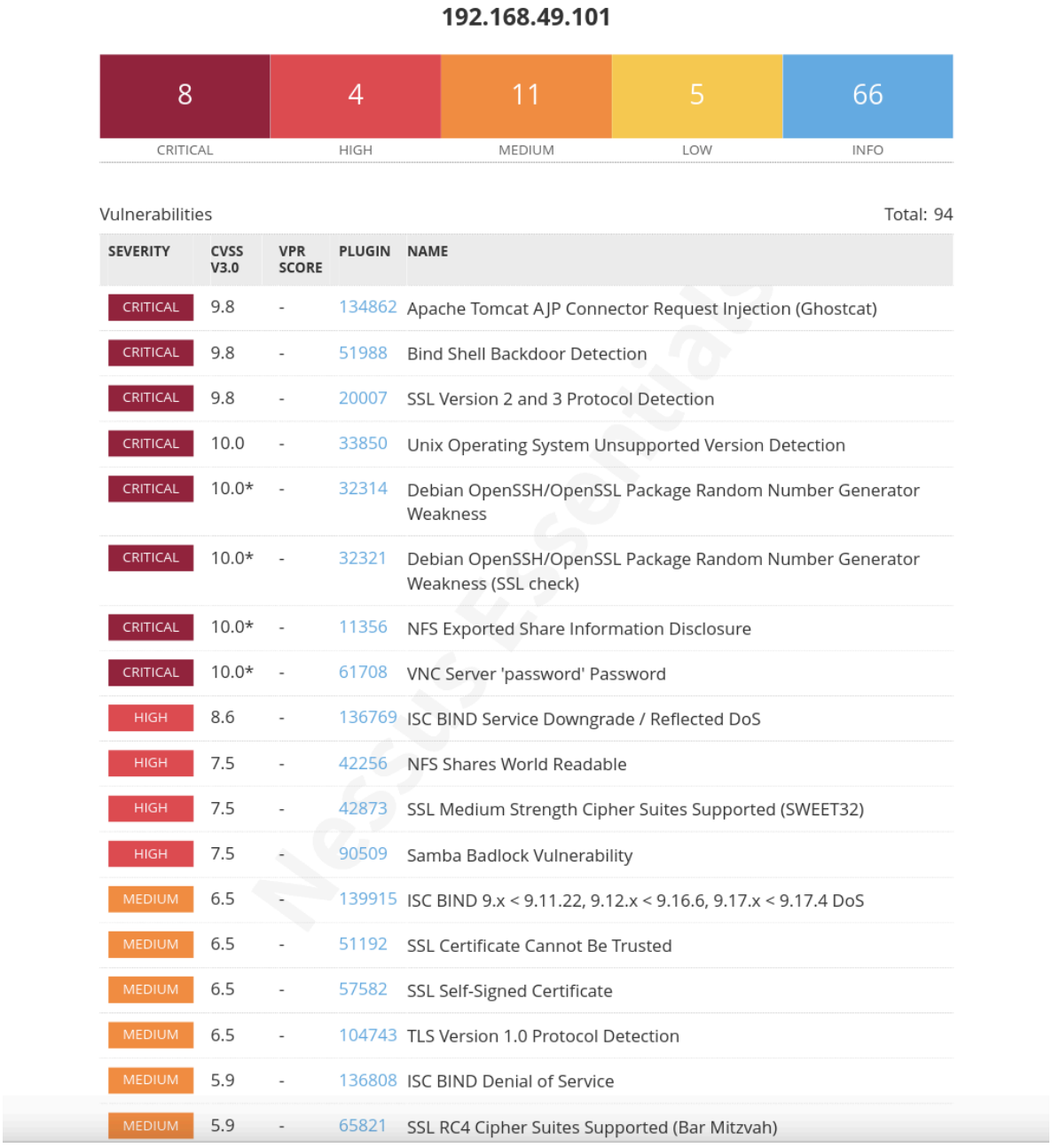
CONSEGNA 22 FEBBRAIO S5L3

La consegna di oggi prevede di effettuare un Vulnerability Assessment con Nessus sulla macchina Metasploitable indicando come target solo le porte comuni. L'obbiettivo è quello di analizzare attentamente il report per ognuna delle vulnerabilità .
Dopo aver effettuato la scansione tramite Nessus, possiamo leggere sul report il numero di vulnerabilità trovate dallo scan, suddivise per grado di gravità. (Fig.1).



192.168.49.101

8	4	11	5	66
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 94

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	-	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*	-	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	-	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	-	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	-	61708	VNC Server 'password' Password
HIGH	8.6	-	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42256	NFS Shares World Readable
HIGH	7.5	-	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	-	90509	Samba Badlock Vulnerability
MEDIUM	6.5	-	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	-	136808	ISC BIND Denial of Service
MEDIUM	5.9	-	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Fig.1

Ho approfondito la prima criticità, che ha un CVSS di 9.8 e codice plugin 134862, dove è presente un connettore AJP vulnerabile in ascolto su remoto. Il connettore AJP è un componente connector che comunica con un connettore web tramite il protocollo AJP.

Quando si utilizza questo protocollo, è necessario prestare attenzione alle connessioni in entrata. Tomcat tratta le connessioni AJP con maggiore “fiducia” rispetto, ad esempio, ad una connessione HTTP. Se tali connessioni sono disponibili un malintenzionato potrebbe approfittarne. Infatti prima che la vulnerabilità fosse nota, l’attaccante poteva baypassare i controlli di sicurezza basati sull’IP del client, oppure poteva bypassare l’autenticazione dell’utente se Tomcat era configurato in modo da fidarsi dei dati di autenticazione forniti dal riverse proxy. Più precisamente, il meccanismo di attacco consisteva nella restituzione di file arbitrati da qualsiasi punto dell’applicazione web, anche sotto la directory WEB-IF e META-INF, e l’elaborazione di qualsiasi file nell’applicazione web come JSP. Inoltre se l’applicazione web consentiva il caricamento di file e li archiviava all’interno dell’applicazione web, insieme alla capacità di elaborare un file come JSP, rendeva possibile l’esecuzione del codice da remoto. Come vediamo in Fig.2, la soluzione proposta è quella di aggiornare la configurazione AJP per richiedere l’autorizzazione, e di aggiornare il server Tomcat,

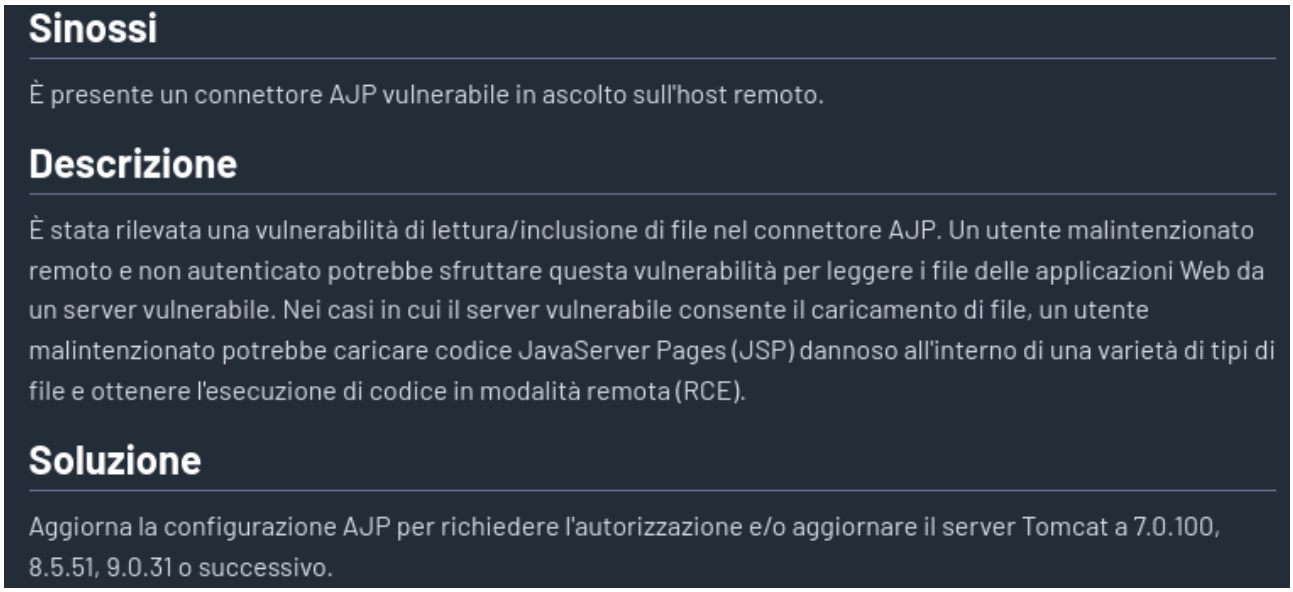


Fig.2