REPORT 24.02.2023

Con la prima scansione avanzata tramite il tool NESSUS sono state rilevate diverse vulnerabilità critiche, tra cui:

- NFS EXPORTED SHARE INFORMATION DISCLOSURE
- VNC SERVER 'password' Password
- BIND SHELL BACKDOOR DETECTION
- APACHE TOMCAT AJP CONNECTOR

Vediamo passo passo la risoluzione di queste criticità:

1)NFS EXPORTED SHARE INFORMATION DISCLOSURE

Si tratta di una vulnerabilità forte in quanto permette di condividere file, cartelle, spazio disco fisso o un intero file system tra computer diversi sulla stessa rete. Un server può anche esportare directory locali e un utente potrebbe scaricare/consultare/visualizzare in locale risorse di un server remoto.

RESOLUTION: Occorre stabilire quali IP ADDRESS autorizzare, altrimenti un attaccante potrebbe sfruttare la vulnerabilità ed accedere. In META eseguire i seguenti passaggi:

sudo nano /etc/exports

inserire ip da autorizzare nella riga / * (rw, syn, …..), cambiare volendo anche la modalità di accesso da rw a ro.

2)BIND SHELL BACKDOOR

Nessus ha rilevato una BIND SHELL aperta sulla 1524 aperta come criticità. La chiudiamo impostando una nuova regola firewall con IPTABLES sul traffico in uscita verso quella porta.

3) VNC SERVER

La criticità riguarda il fatto che se qualcuno si collega al servizio di META di server in remoto, può accedervi con una password molto semplice. Per cui o modifichiamo la password oppure procediamo un il blocco della porta su cui vi è il servizio.

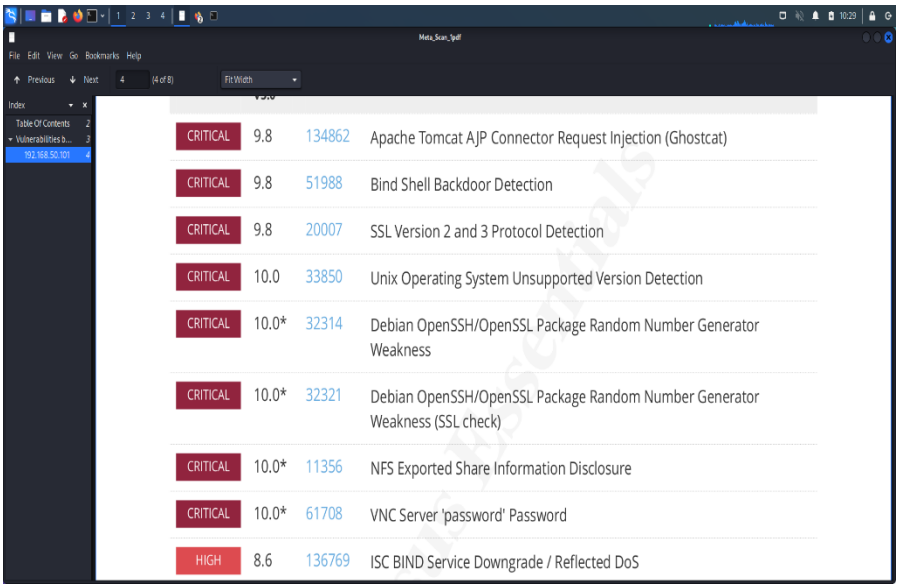
4) APACHE TOMCAT

La risoluzione di questa criticità si effettua accedendo a : nano /etc/tomcat…/server.xml

Andiamo nella sezione di CONNECTOR PORT8909(APJ) e commentiamo con <!--- -->

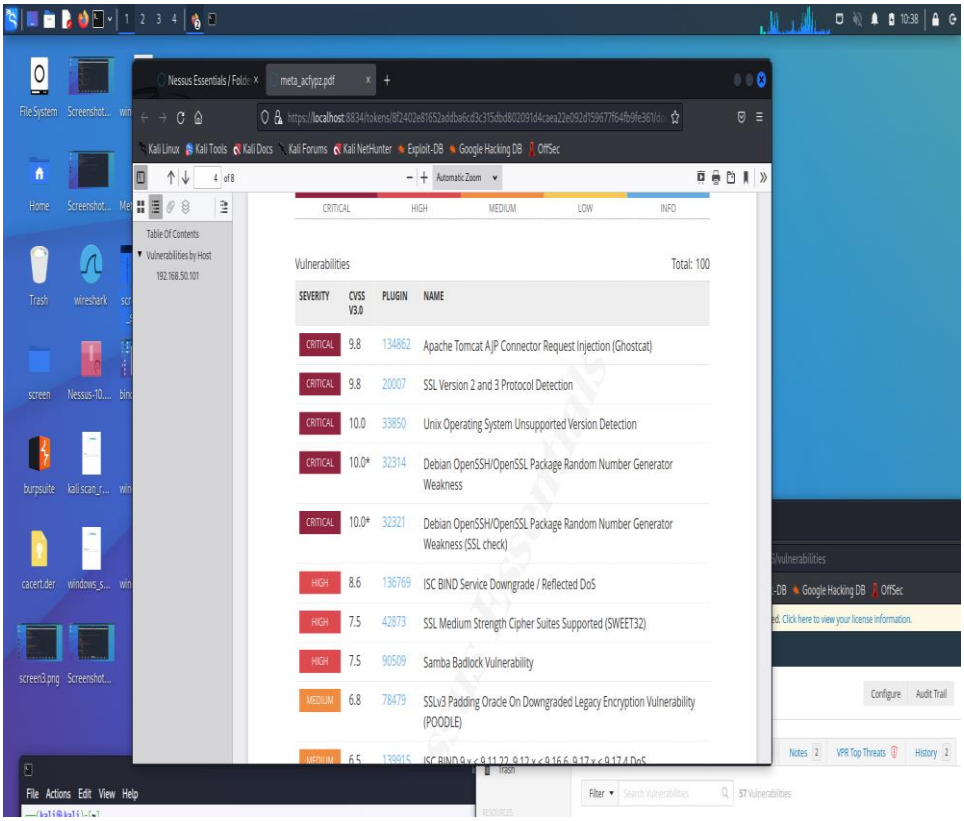
(la criticità risulta ancora in quanto è stata risolta per ultima e la scansione nuova ancora risulta in corso)

PRIMA SCANSIONE



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

REPORT DOPO LA RISOLUZIONE DI ALCUNE CRITICITA’



SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	9.8	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
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)
HIGH	8.6	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	90509	Samba Badlock Vulnerability
MEDIUM	6.8	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)