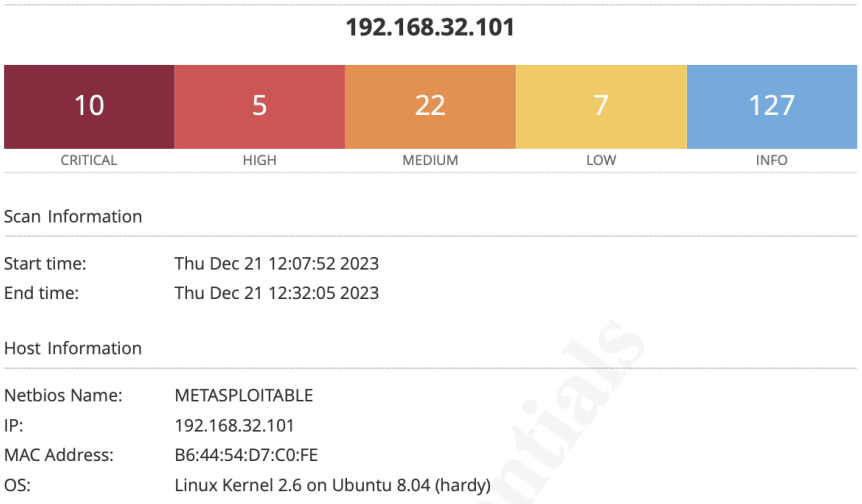
NESSUS:
Scan VM Metasploitable

Con Nessus facciamo una scansione sulla nostra macchina metasplitable2 con IP: 192.168.32.101.

Il risultato è un documento che racchiude una serie diversa di vulnerabilità:



Andiamo ad analizzare le vulnerabilità critical:

134862 - Apache Tomcat AJP Connector Request Injection(Gostcat)

Un utente malevolo potrebbe attraverso un server vulnerabile a leggere i file delle web application. Si potrebbe anche caricare JSP malevoli da remoto.
Ultimo update aggiornamento ad Apache Tomcat 9.0.31, 8.5.51 o 7.0.100 o successivo per aggirare il problema.

51988 - Bind Shell Backdoor Detection

Una Backdoor con possibilità di connettersi da remoto e mandare direttamente comandi dalla porta.
Controllare se il server è compromesso, in caso reinstallare il sistema.

32314 - Debian OpenSSH/OpenSSL Packege Random Number Generetor Weakness

CVE-2008-0166
Genera chiavi private per la decriptazione di OpenSSL(software per la crittografia e comunicazioni sicure). Facile Svolgere Brute Force contro le chiavi crittografiche.
La vulnerabilità è presente fino alla versione 0.9.8.g-9 e solo per Debian.
Soluzione: rigenerare nuove chiavi con diversi software, aggiornare OpenSSL a versioni più recenti.

11356 - NFS Export Share Information Disclosure

Gli aggressori remoti possono montare un file system NFS in Ultrix o OSF, anche se viene negato di accesso.

33850 - Unix Operationf System Unsupported Detection

Vulnerabilità in quanto il sistema non può più essere implementato con nuove patches.
Soluzione: passare alla versione Unix supportata.

61708 - VCN Server ‘password’ Password

La password non è assolutamente efficace, Nessus è riuscito facilmente a trovare la password per il VCN server.
Soluzione: mettere in sicuro il server VCN (per il controllo da remoto della macchina meta) con password più solide.