Progetto S5-L4

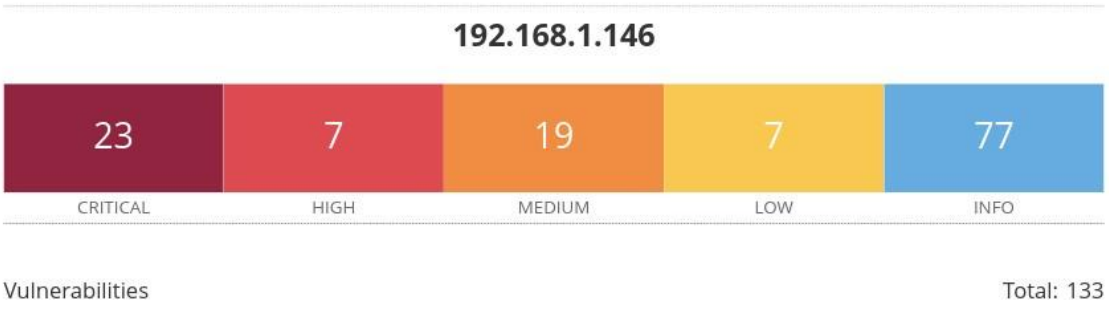
Studente: Simone Mininni

Obiettivo: Fase di scansione della rete o di un sistema con l'ausilio di un vulnerability scanner alla ricerca di vulnerabilità conosciute.

Software utilizzato per la scansione è Nessus, mentre il target della scansione è la macchina Metasploitable.

Nessus è stato settato su ambiente Linux, e poi è stata eseguita una basic network scan sulle porte più comuni sul target.

Analizziamo i risultati prodotti dalla scansione che poi saranno utili per la fase di exploit del pentesting.




Possiamo notare che sono state trovate 133 vulnerabilità di cui 23 critiche, 7 high, 19 medium, 7 low e il resto info(non dovrebbero presentare un problema, anche se ci potrebbero essere dei falsi negativi)

Sicuramente i risultati critici meritano la priorità assoluta e sono quelli che analizzeremo ai fini del progetto.

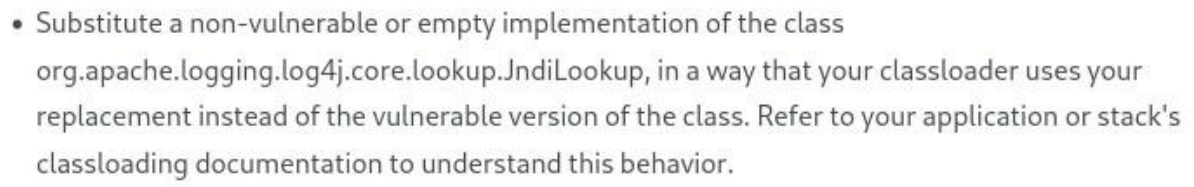
Vulnerabilità critica: Log4j


Si tratta di una vulnerabilità che interessa la java logging library log4j(version 2).

Interessa tutti gli utilizzatori di Apache Struts( framework java per la programmazione di web application).

Abbiamo un attacco di tipo LDAP(code) injection che va a manipolare i parametri di input passati a una funzione di logging → il problema è determinato dal fatto che gli input non sono ripuliti e quindi si immette una query che costringe il server a fare una request malevola che porta infine l'attaccante a eseguire un codice arbitrario nel server target.

Soluzione al problema è quella di aggiornare ad Apache log4j versione 2.15.0 o successive.
Se non è possibile aggiornare:




Fonte: https://www.lunasec.io/docs/blog/log4j-zero-day/

Vulnerabilità critica: versione sistema operativo


Unix operating system non più supportato, trovata una versione ubuntu 8.04.
Bisognerebbe aggiornare a Ubuntu 23.04 / LTS 22.04 / LTS 20.04

Vulnerabilità critica: Vnc server password


Vnc server , applicazioni che permettono il controllo da remoto di una macchina.Trovata vulnerabilità della password troppo debole, un attaccante potrebbe facilmente prendere il controllo della macchina.

Vulnerabilità critica: NFS


NFS ( Network File Sharing) è un protocollo che permette di condividere file system( directories e files) sulla rete.
In questo caso vi è una criticità importante poichè un malintenzionato(client linux)  potrebbe montare il file system e ispezionare tranquillamente directories file e magari anche manipolarli.

Bisogna quindi impostare NFS in modo che possa essere accessibile solo da client autorizzati.