W12D1 - Pratica (2)

Target : 192.168.50.106 (metasploitable)

-Vulnerabilità critiche:

- 134862 - Apache Tomcat A JP Connector Request Injection

Questa vulnerabilità permette ad un utente malintenzionato di leggere i dati nel server vulnerabile, in mancanza di autorizzazione. In caso il server permetta di caricare file al suo interno l'utente malintenzionato potrebbe iniettare del codice malevolo.

Per abbattere la vulnerabilità è necessario aggiornare il server AJP in modo che richieda l'autorizzazione all'accesso ed aggiornare il server TomCat all'ultima versione disponibile.

- 51988 - Bind Shell Backdoor Detection

Vi è la possibilità che l'host sia stato compromesso, in quanto è presente una shell in ascolto sulla porta e questo comporta che un utente malintenzionato possa lanciare comandi senza autorizzazione.

Per risolvere questa vulnerabilità è necessario reinstallare il sistema.

- 61708 - VNC Server 'password' Password

Il server VNC ha una password debole, nonchè 'password'.

Un utente malintenzionato potrebbe accedere con facilità e prendere il controllo della macchina senza permesso.

Per risolvere questa vulnerabilità è necessario aggiornare la password con una più complessa.

-Vulnerabilità alte:

- 42256 -NFS Shares World Readable

Questa vulnerabilità condivide parole sensibili leggibili da tutti gli utenti. Il server NFS può essere raggiungibile da chiunque perchè non ha una regola che ne limiti l'accesso a deteterminati host o ip.

Per risolvere questa vulnerabilità è necessario applicare delle restrizioni per limitare l'accesso a indirizzi ip e utenti verificati e sicuri.

-Vulnerabilità medie:

- 11213 - HTTP TRACE

Le funzioni di debug sono abilitate sul server, ovvero trace/track che consentono il debug.

E' consigliato disabilitare questi metodi.