REPORT DELLE VULNERABILITA' DELL'HOST 192.168.50.101

NUMERAZIONE IN BASE AL LIVELLO DI RISCHIO:

-CRITICO: **8**

-ALTO: **4**

-MEDIO: **16**

-BASSO: **7**

SPIEGAZIONE DELLE VULNERABILITA':

Apache Tomcat A JP Connector Request Injection (Ghostcat)

E' una vulnerabilità del connettore AJP di Apache Tomcat, consente di accedere a qualsiasi file sul server web, inclusi file di configurazione, codice sorgente o altri dati sensibili. Permette anche di eseguire codice arbitrario a seconda della configurazione del server e dei file disponibili.

Bind Shell Backdoor Detection

Una bind shell backdoor è una forma di accesso remoto che permette a un attaccante di eseguire comandi come se fosse fisicamente presente sulla macchina compromessa. Questo tipo di backdoor apre una porta in ascolto sul sistema bersaglio, permettendo all'attaccante di connettersi da remoto e ottenere una shell di comando.

SSL Version 2 and 3 Protocol Detection

SSL (Secure Sockets Layer) versioni 2 e 3 sono protocolli di sicurezza obsoleti che sono stati sostituiti dal più sicuro TLS (Transport Layer Security). SSLv2 e SSLv3 contengono diverse vulnerabilità critiche, come ad esempio la crittografia debole, che possono essere sfruttate da un attacante in vari modi come ad esempio un attacco di tipo ManInTheMiddle.

Unix Operating System Unsupported Version Detection

L'utilizzo di una versione non supportata di un sistema operativo Unix comporta una serie di rischi significativi per la sicurezza e la stabilità del sistema e anche problemi di conformità con le normative.

Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

La debolezza del generatore di numeri casuali nei pacchetti OpenSSH/OpenSSL di Debian è una vulnerabilità critica che è stata scoperta nel 2008. A causa di una modifica errata nel codice sorgente di OpenSSL, il generatore di numeri casuali (RNG) di Debian e delle sue derivate (come Ubuntu) produce numeri casuali prevedibili. Questo difetto si traduce in chiavi crittografiche deboli che possono essere facilmente previste. Questa vulnerabilità può esser sfruttata da un attaccante per leggere e manipolare tutti i dati che passano tra client e server, ottenere un accesso non autorizzato e iniziare una privilege escalation.

NFS Exported Share Information Disclosure

La vulnerabilità di "NFS Exported Share Information Disclosure" si riferisce alla possibilità per un attaccante di accedere a informazioni sensibili o risorse all'interno di un sistema NFS (Network File System) che sono state esplicitamente esportate per l'accesso da parte di client autorizzati. Sfruttando questa vulnerabilità un attaccante potrebbe compiere diverse azioni come:

- Ottenere accesso non autorizzato ai dati

- Raccogliere informazioni sensibili

-Analizzare la struttura dei dati

- Manipolare i dati

- Esecuzione di attacchi di bruteforce

- Ricavare informazioni sulla configurazione di sistema.

VNC Server 'password' Password

La vulnerabilità nota come "VNC Server 'password' Password" si riferisce al rischio associato all'uso di password deboli o predefinite per il login sui server VNC (Virtual Network Computing). Sono tantissimi le azioni che può compiere un attaccante sfruttando questa vulnerabilità tra cui eseguire programmi dannosi e creare una backdoor nel sistema.

ISC BIND Service Downgrade / Reflected DoS

La vulnerabilità di "ISC BIND Service Downgrade / Reflected DoS" si riferisce a un tipo di attacco che può essere sfruttato per compromettere il servizio DNS (Domain Name System) fornito da ISC BIND (Berkeley Internet Name Domain).
Grazie a questa vulnerabilità un attaccante potrebbe effettuare un attacco DoS, effettuare downgrade degli aggiornamenti di sicurezza, manipolare le risposte dei DNS indirizzando gli utenti a risorse malevole.

NFS Shares World Readable

La configurazione di condivisioni NFS (Network File System) come "World Readable" (leggibili da tutti) presenta diversi rischi significativi per la sicurezza, che possono essere sfruttati dagli attaccanti per accedere e compromettere dati sensibili.

SSL Medium Strength Cipher Suites Supported (SWEET32)

La vulnerabilità SSL Medium Strength Cipher Suites Supported, nota anche come SWEET32, è un problema di sicurezza che riguarda l'utilizzo di algoritmi di cifratura deboli all'interno dei protocolli SSL/TLS. Questo rende vulnerabili a diversi attacchi come ad esempio quelli di Decrypting Session Cookies

Samba Badlock Vulnerability

Questa vulnerabilità è stata un problema di sicurezza rilevato nel protocollo Samba, utilizzato per la condivisione di file e la stampa su reti di tipo Unix e Linux. Ecco i principali rischi che porta questa vulnerabilità:

- Esecuzione di codice da remoto
- Accesso a dati non autorizzati
- Attacchi Dos
-Privilege escalation