Esercitazione W12D1 Pratica 2

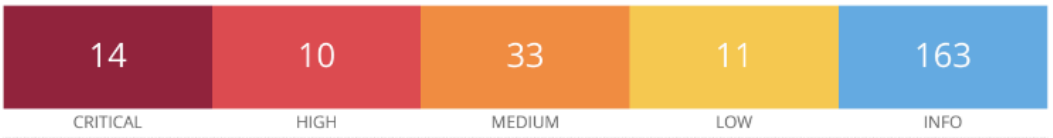
Ilaria Pedrelli

Report Vulnerabilità

Nel documento ho presentato le principali vulnerabilità riscontrate dopo una scansione basica con NESSUS sulla macchina target metasploitable. In particolare, ho riportato le vulnerabilità con rischio critico e le vulnerabilità a rischio alto che ritenevo di maggior importanza.

A. Presentazione grafica delle vulnerabilità rilevate

192.168.50.101



Scan Information

Start time: Tue Jan 23 13:43:17 2024
End time: Tue Jan 23 15:23:27 2024

Vulnerabilities Total: 153

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	8.9	70728	Apache PHP-CGI Remote Code Execution
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.8	5.9	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)
CRITICAL	9.1	6.0	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
CRITICAL	10.0	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	7.4	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	7.4	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	7.4	46882	UnrealIRCd Backdoor Detection
CRITICAL	10.0*	-	61708	VNC Server 'password' Password

B. Risultati

1. 70728 - Apache PHP-CGI Remote Code Execution

Severity: **HIGH**
CVSS v3.0 Base Score **9.8**

1.1 Descrizione e Danno

La vulnerabilità riguarda l'installazione di PHP o del Web Server remoto che contiene una falla. Un possibile attaccante potrebbe manipolare la stringa di Query per introdurre comandi malevoli che il server PHP-CGI eseguirebbe senza adeguati controlli.

Un attacco di questo tipo potrebbe portare a gravi conseguenze come l'esecuzione di codice sul server, la divulgazione del codice sorgente PHP sino al crash del sistema.

1.2 Contromisure

Upgrade della versione PHP a 5.%.4.3 o successive

2. 171340 - Apache Tomcat SEoL (<= 5.5.x)

Severity: **CRITICAL**
CVSS v3.0 Base Score **10.0**

2.1 Descrizione e Danno

La seguente versione di Apache Tomcat è inferiore alla versione 5.5.x. questa versione non è più supportata o mantenuta dal fornitore e questo implica che non verranno più rilasciati nuovi patch di sicurezza.

In assenza di aggiornamenti di sicurezza, il software potrebbe contenere o sviluppare vulnerabilità nel tempo.

2.3 Contromisure

Fare un Upgrade di Apache Tomcat che sia mantenuta attivamente e aggiornata con i patch più recenti.

3. 51988 - Bind Shell Backdoor Detection

Severity: **CRITICAL**
CVSS v3.0 Base Score **9.8**

3.1 Descrizione e Danno

Questa vulnerabilità indica che c'è una shell in ascolto su una porta remota senza che venga richiesta autenticazione. Ciò significa che un possibile attaccante potrebbe connettersi a questa porta e inviare comandi senza doversi autenticare e ottenere il controllo del sistema.

3.2 Contromisure

Verificare se l'host è compromesso e reinstallare il sistema se necessario. Implementare misure di sicurezza come l'autenticazione per limitare l'accesso non autorizzato.

4. 32314 - 32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL, SSL check)

Severity: **CRITICAL**
CVSS v3.0 Base Score **10.0**

4.1 Descrizione e Danno

Vulnerabilità che riguarda le chiavi SSH, SSL (CERTIFICATO x.509) generata su un sistema Debian Ubuntu che contiene un difetto nel generatore di numeri casuali della libreria Open SSL.
Un pacchetto Debian ha rimosso tutte le fonti di entropia nella versione remota Open SSL.
Questo bug nella generazione casuale di numeri rende la chiave vulnerabile. Un attaccante potrebbe ottenere la parte privata della chiave remota e utilizzarla per impostare la cifratura o eseguire un attacco "man-in-the-middle".

4.2 Contromisure

Aggiornare la versione OpenSSL e rigenerare le chiavi SSH, SSL e il materiale Openvpn dovrà essere rigenerato.

5. 33447 - Multiple Vendor DNS Query ID Field Prediction Cache Poisoning

Severity: **HIGH**

CVSS v3.0 Base Score **9.1**

5.1 Descrizione e Danno

Il resolver DNS remoto non utilizza una porta casuale quando effettua richiesta ai serve DNS di terze parti. La mancanza di casualità nella selezione delle porte facilita agli attacanti la manipolazione delle risposte DNS con il rischio di redirezionare il traffico verso destinazioni dannose. Questo può portare ad attacchi di tipo DNS spoofing.

5.2 Contromisure

Uso di porte casuali per le richieste DNS e contattare il fornitore di servizio per aggiornare i patch.

6. 11356 - NFS Exported Share Information Disclosure

Severity: **CRITICAL**

CVSS v3.0 Base Score **10.0**

6.1 Descrizione e Danno

Una delle condivisione NFS esportate da un servizio remoto potrebbe essere montata senza autenticazione. Un attaccante potrebbe sfruttare questa vulnerabilità per accedere e manipolare file o risorse remote ottenendo il permesso di lettura e scrittura senza la necessità di autenticarsi. In pratica, permette all'attaccante di eseguire operazioni di scrittura e lettura non autorizzate su risorse condivise NFS.

6.2 Contromisure

Configurare correttamente l’autenticazione e l’autorizzazione per limitare l’accesso non autorizzato alle risorse NFS.

7. 20007 - SSL Version 2 and 3 Protocol Detection

Severity: **CRITICAL**

CVSS v3.0 Base Score **9.8**

7.1 Descrizione e Danno

Il servizio remoto utilizza connessioni crittografate utilizzando SSL 2.0 e/o SSL 3.0. Queste versioni di SSL sono affetto da diversi difetti crittografici. Un utente malintenzionato può sfruttare queste falle per condurre attacchi man-in-the-middle o per decrittografare le comunicazioni tra il servizio e il client. Inoltre, anche se SSL e TLS dispongano di mezzi per supportare la versione più alta supportata dal protocollo, alcuni browser lo implementano in modo non sicuro aumentando il rischio di attacchi POODLE.

7.2 Contromisure

Disabilitare completamente questi protocolli (non più accettati dal NIST come sicuri). Utilizzare invece TLS 1.2 e versioni successive.

8. 33850 - Unix Operating System Unsupported Version Detection

Severity: **CRITICAL**

CVSS v3.0 Base Score **10.0**

8.1 Descrizione e Danno

Il Sistema operativo Unix in esecuzione sull'host remoto non è più supportato e quindi, potrebbe essere esposto a vulnerabilità.

8.2 Contromisure

Fare l'upgrade della versione Unix attualmente supportata.

9. 46882 - UnrealIRCd Backdoor Detection

Severity: **CRITICAL**

CVSS v3.0 Base Score **10.0**

9.1 Descrizione e Danno

Il server IRC remoto è una versione di UnrealIRCd con una backdoor che consente a un utente malintenzionato di eseguire codice arbitrario sull'host interessato.

9.2 Contromisure

Scaricare nuovamente il software, verificarlo utilizzando i checksum MD5/SHA1 pubblicati e reinstallarlo.

10. 61708 - VNC Server 'password' Password

Severity: **CRITICAL**
CVSS v3.0 Base Score **10.0**

10.1 Descrizione e Danno

Il server VNC in esecuzione sull'host remoto è protetto da una password poco sicura. un Malintenzionato potrebbe prendere il controllo del sistema.

10.2 Contromisure

Mettere in sicurezza il servizio VNC con una password più forte e se possibile, un autenticazione a più fattori.

11. 125855 - phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)

Severity: **HIGH**
CVSS v3.0 Base Score **9.8**

11.1 Descrizione e Danno

Questo report di vulnerabilità indica che l'applicazione phpMyAdmin sul server web remoto ha una versione precedente alla 4.8.6 ed è affetta da una vulnerabilità di iniezione SQL (SQLi) nella funzione di designer. Un attaccante non autenticato potrebbe sfruttare questa vulnerabilità per iniettare o manipolare le query SQL nel database di backend, con il rischio di divulgare o manipolare dati arbitrari.

11.2 Contromisure

Aggiornare phpMyAdmin a una versione uguale o successiva alla 4.8.6