

EPICODE

Progetto Alessandro Moscetti 26/10




New Scan / Basic Network Scan

[← Back to Scan Templates](#)

Settings

Credentials

Plugins 

BASIC

• General

[Schedule](#)

[Notifications](#)

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name

Metasploitable

Description

Folder

My Scans

Targets

192.168.0.101

Upload Targets

[Add File](#)

Save

Cancel

Sono andato ad effettuare un Vulnerability Assessment tramite Nessus sulla macchina Metasploitable.

Utilizzando 'Basic Network Scan' sono andato ad indicare come target solo le porte più comuni.

Di seguito il link del report:

https://github.com/AlessandroMoscetti/Progetto_Epicode_26-10/blob/main/Report-Nessus.pdf

A seguire un breve report delle prime 4 vulnerabilità critiche trovate come richiesto.

CRITICAL

9.8

9.0

[134862](#) Apache Tomcat AJP Connector Request Injection (Ghostcat)

Questa vulnerabilità riguarda il server Apache Tomcat che contiene l'AJP Connector, che è abilitata e sta in ascolto per default sulla porta 8009.

Questa vulnerabilità può essere sfruttata da un malintenzionato per leggere i file di un server vulnerabile in alcuni casi quando il server permette l'upload di file, l'attaccante può arrivare all'accesso remoto.

Come soluzione Nessus ci suggerisce di aggiornare la configurazione AJP per richiedere l'autorizzazione e/o aggiornare il server Tomcat a 7.0.100, 8.5.51, 9.0.31 o successivo.

CRITICAL

9.8

-

51988

Bind Shell Backdoor Detection

Questa vulnerabilità è una backdoor in ascolto sulla porta 1524. Non avendo bisogno di autenticazioni un attaccante può connettersi alla porta e inviare comandi da remoto. Trattandosi di una Bind Shell Backdoor l'attaccante fa partire la connessione verso la porta rendendola una vittima per i firewall a filtraggio dinamico. La soluzione proposta da Nessus è quella di verificare se l'host remoto è stato compromesso e, se necessario, reinstallare il sistema.

CRITICAL

9.8

-

20007

SSL Version 2 and 3 Protocol Detection

Questa vulnerabilità interessa la porta 25 e la 5432.

Il servizio remoto accetta connessioni crittografate utilizzando SSL 2.0 e/o SSL 3.0, versioni affette da difetti crittografici.

Un utente malintenzionato può sfruttare queste falle per condurre attacchi man-in-the-middle o per decrittografare le comunicazioni tra il servizio interessato e i client.

Nessus come soluzione ci consiglia di disattivare SSL 2.0 e 3.0 e utilizzare invece TLS 1.2 (con suite di crittografia approvate) o versioni successive.

CRITICAL

9.1

6.0

33447

Multiple Vendor DNS Query ID Field Prediction Cache Poisoning

Questa vulnerabilità interessa la porta 53 dove il risolutore DNS remoto non utilizza porte casuali quando esegue query su server DNS di terze parti.

Un utente malintenzionato remoto non autenticato può sfruttare questa situazione per avvelenare il server DNS remoto, consentendo all'utente malintenzionato di deviare il traffico legittimo verso siti arbitrari.

Come soluzione Nessus ci suggerisce di contattare il fornitore del Dns server per una patch.

Grazie per l'attenzione.