EPICODE

Andrea Rocca
CSPT0323

# Cybersecurity Analyst

**Week 12** - W12D4

# M3: Progetto

## Esercizio

Mediante l'utilizzo di **Nessus**, effettuare una scansione completa sul target Metasploitable.

Scegliere da un minimo di 2 fino ad un massimo di 4 **vulnerabilità critiche** e provare ad implementare delle **azioni di rimedio**.

Per dimostrare l'efficacia delle azioni di rimedio, eseguire nuovamente la scansione sul target e **confrontare i risultati con quelli precedentemente ottenuti**.

Andrea Rocca
CSPT0323

# INTRODUZIONE

Il presente report documenta i risultati di un **test di vulnerabilità** eseguito su macchina virtuale **Metasploitable**.

L'obiettivo primario di questo test è valutare la sicurezza del sistema, identificando potenziali vulnerabilità e rischi che potrebbero essere **sfruttati da attacchi malevoli**, fornendo una panoramica chiara dello stato attuale della sicurezza della macchina e **mettendo in evidenza le vulnerabilità critiche che richiedono attenzione immediata**.

# SCAN

**Inizio:** 25/01/2024 12:56:31
**Fine:** 25/01/2024 14:13:03

# HOST

**Netbios Name:** METASPLOITABLE
**IP:** 192.168.40.100
**OS:** Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

# RIEPILOGO VULNERABILITÀ

| 10 | 8 | 30 | 8 |
|---|---|---|---|
| CRITICHE | ALTE | MEDIE | BASSE |

# PANORAMICA VULNERABILITÀ CRITICHE

| LIVELLO | CVSS* | NOME |
|---|---|---|
| CRITICA | 10.0 | NFS Exported Share Information Disclosure |
| CRITICA | 10.0 | Unix Operating System Unsupported Version Detection |
| CRITICA | 10.0 | VNC Server 'password' Password |
| CRITICA | 10.0 | Debian OpenSSH/OpenSSL Package Random Number Generator Weakness |
| CRITICA | 10.0 | Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check) |
| CRITICA | 9.8 | SSL Version 2 and 3 Protocol Detection |
| CRITICA | 9.8 | Apache Tomcat AJP Connector Request Injection (Ghostcat) |
| CRITICA | 9.8 | Apache PHP-CGI Remote Code Execution |
| CRITICA | 9.8 | Bind Shell Backdoor Detection |
| CRITICA | 9.8 | Unix Operating System Unsupported phpMyAdmin prior to 4.8.6 |

* **Common Vulnerability Scoring System** (CVSS) è uno standard che assegna un punteggio numerico alle vulnerabilità informatiche per misurarne la gravità. Il punteggio, su una scala da 0 a 10, aiuta a valutare l'impatto della vulnerabilità considerando vari fattori come la facilità di sfruttamento, l'accesso remoto, l'impatto sulla riservatezza, l'integrità e la disponibilità dei dati.