EPICODE

EPICODE-CS0124
Build Week - 1
TEAM 1

Report Finale

EPICODE

Compagnia Theta:
Vulnerability Assessment

La compagnia Theta, con lo scopo di valutare la sicurezza del proprio sistema informativo, ha richiesto i servizi del nostro Team al fine di effettuare un vulnerability assessment

EPICODE

La nostra proposta

Il nostro team propone i seguenti test per il raggiungimento dell'obiettivo:

- Port Scan
- Method Scan
- Attacco Brute Force
- Progetto per un nuovo design di rete

EPICODE

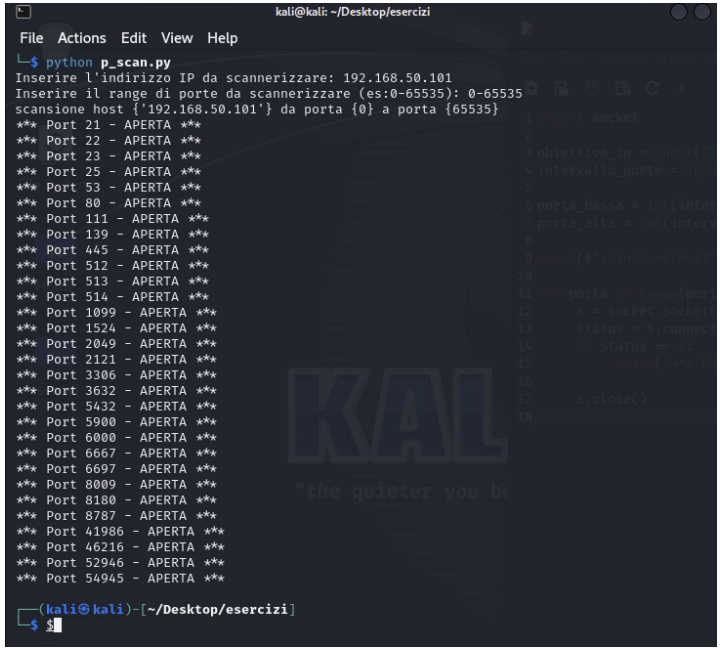
Port Scan e Method Scan

Risultati emersi **port scan**:

- di fianco sono elencate le porte aperte
- non tutte sono state identificate come necessarie

Risultati emersi **method scan**:

- tutti i metodi sono abilitati



EPICODE

Attacco Brute Force

Target dell’attacco:

- pagina di login DVWA
- pagina di test DVWA brute force
- pagina di login phpMyAdmin

EPICODE

Attacco Brute Force DVWA

Tools utilizzati:

- WireShark
- Python
- Kali Linux

Risultati emersi:

- nessuna vulnerabilità evidente
- errore umano e di gestione credenziali
- semplicità di accesso

EPICODE

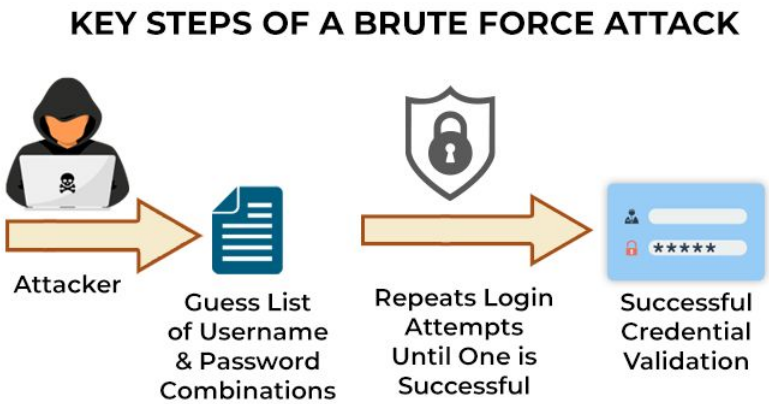
Attacco phpMyAdmin

Tools utilizzati:

- WireShark
- Python
- Kali Linux

Risultati emersi:

- nessuna vulnerabilità evidente
- errore umano e di gestione credenziali
- semplicità di accesso



EPICODE

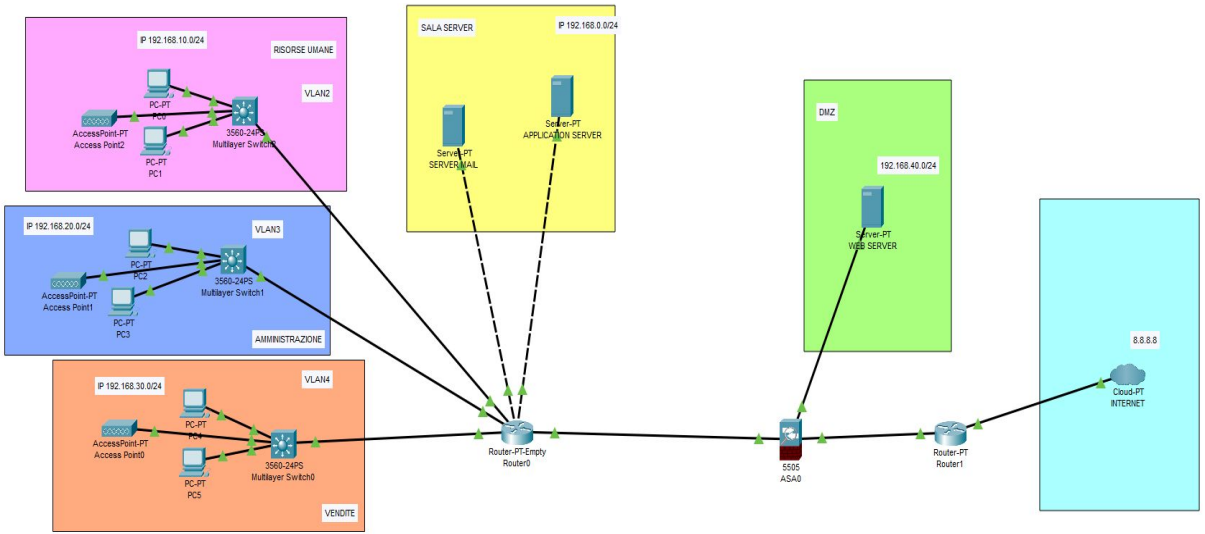
Azioni di mitigazione

- Firewall perimetrale
- **Formazione del personale**
- **Password policies**
- **Blocco temporaneo accesso**
- Aggiornamento software
- Antivirus aziendale
- **MFA (Multi factor authentication)**
- VPN e tunnel SSH
- Chiusura porte non necessarie
- Vulnerability assessment periodici
- Certificato SSL

EPICODE

Nuovo design della rete

- DMZ per server pubblici
- Rete Interna
- Firewall perimetrale
- VLAN indipendenti per i vari reparti



Grazie per l’attenzione
Team 1

“La maggior minaccia per una rete è l’essere umano”