

EPICODE-CS0124
Build Week - 1
TEAM 1

Report Finale

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



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

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

```
File Actions Edit View Help
└─$ python p_scan.py
Inserire l'indirizzo IP da scannerizzare: 192.168.50.101
Inserire il range di porte da scannerizzare (es:0-65535): 0-65535
scansione host {'192.168.50.101'} da porta {0} a porta {65535}
** Port 21 - APERTA **
** Port 22 - APERTA **
** Port 23 - APERTA **
** Port 25 - APERTA **
** Port 53 - APERTA **
** Port 80 - APERTA **
** Port 111 - APERTA **
** Port 139 - APERTA **
** Port 445 - APERTA **
** Port 512 - APERTA **
** Port 513 - APERTA **
** Port 514 - APERTA **
** Port 1099 - APERTA **
** Port 1524 - APERTA **
** Port 2049 - APERTA **
** Port 2121 - APERTA **
** Port 3306 - APERTA **
** Port 3632 - APERTA **
** Port 5432 - APERTA **
** Port 5900 - APERTA **
** Port 6000 - APERTA **
** Port 6667 - APERTA **
** Port 6697 - APERTA **
** Port 8009 - APERTA **
** Port 8180 - APERTA **
** Port 8787 - APERTA **
** Port 41986 - APERTA **
** Port 46216 - APERTA **
** Port 52946 - APERTA **
** Port 54945 - APERTA **

1 s = socket
2
3 obiettivo_ip = ip
4 intervallo_porte = range(
5
6 porta_bassa + 1, porta_alta + 1)
7 porta_alta + 1)
8
9 s.connect(obiettivo_ip)
10
11 porta = 0
12 s = socket.socket
13 status = s.connect
14 status == 0
15 status == 0
16
17 s.close()
18
```

Attacco Brute Force



Target dell'attacco:

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

Attacco Brute Force DVWA

Tools utilizzati:

- WireShark
- Python
- Kali Linux

Risultati emersi:

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



Attacco phpMyAdmin

Tools utilizzati:

- WireShark
- Python
- Kali Linux

Risultati emersi:

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

KEY STEPS OF A BRUTE FORCE ATTACK



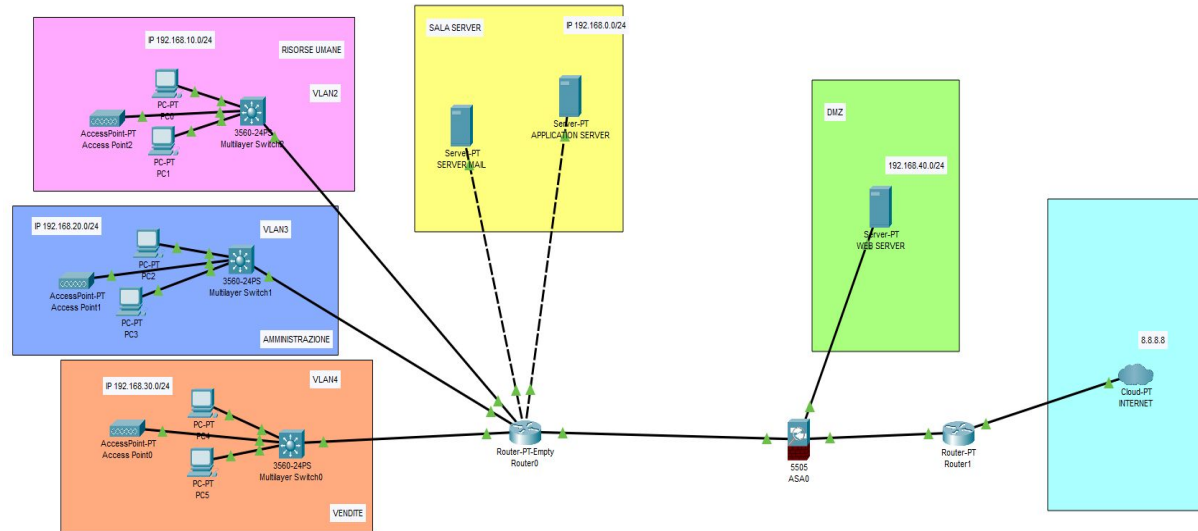
Azioni di mitigazione



- 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

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 ”