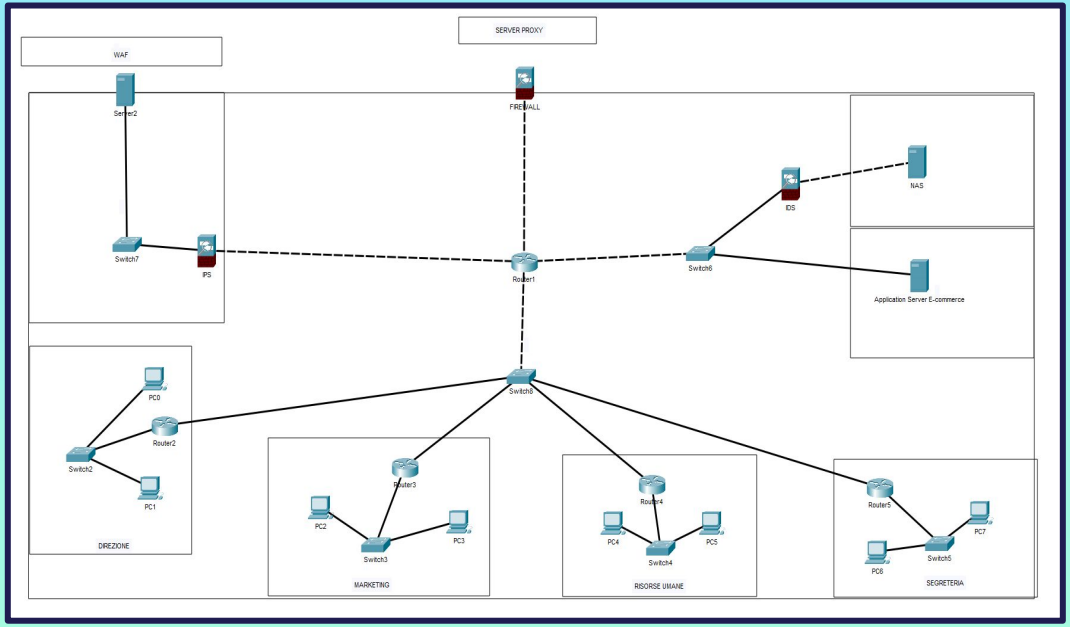
SIMULAZIONE VIOLAZIONE RETE AZIENDALE

Simulazione di un attacco a Theta
A cura di “Squirtle Squad”

LINK AL REPORT

MODELLO DI RETE



Secondo le richieste fatte dal CISO di Theta abbiamo creato un design che aumenta il livello di sicurezza della rete aziendale:

- *Abbiamo inserito un WAF a protezione del Server 2 (il WEB server che espone servizi).*
- *Aggiunto un IPS che incrementa il livello di sicurezza, che si trova al interno di una DMZ.*
- *Un router in ogni VLAN che permette di dividere ogni reparto in una sua SUBNET.*
- *Un Firewall e' un Server Proxy .*
- *Per migliorare la LAN abbiamo aggiunto anche un IDS a proteggere il NAS.*

Codice in python del programma

SCANSIONE DELLE PORTE

Abbiamo eseguito uno scan del range di porte dell'indirizzo IP richiesto.

```
Inserisci l'indirizzo IP del server: 192.168.50.101
Inserisci la porta di partenza della scansione: 1
Inserisci la porta di fine della scansione: 30

Scansione in corso su 192.168.50.101 da porta 1 a 30...

Porte aperte:
Porta 1 (closed): tcpmux
Porta 2 (closed): nbp
Porta 3 (closed): Servizio sconosciuto
Porta 4 (closed): echo
Porta 5 (closed): Servizio sconosciuto
Porta 6 (closed): zip
Porta 7 (closed): echo
Porta 8 (closed): Servizio sconosciuto
Porta 9 (closed): discard
Porta 10 (closed): Servizio sconosciuto
Porta 11 (closed): systat
Porta 12 (closed): Servizio sconosciuto
Porta 13 (closed): daytime
Porta 14 (closed): Servizio sconosciuto
Porta 15 (closed): netstat
Porta 16 (closed): Servizio sconosciuto
Porta 17 (closed): qotd
Porta 18 (closed): Servizio sconosciuto
Porta 19 (closed): chargen
Porta 20 (closed): ftp-data
Porta 21 (open): ftp
Porta 22 (open): ssh
Porta 23 (open): telnet
Porta 24 (closed): Servizio sconosciuto
Porta 25 (open): smtp
Porta 26 (closed): Servizio sconosciuto
Porta 27 (closed): Servizio sconosciuto
Porta 28 (closed): Servizio sconosciuto
Porta 29 (closed): Servizio sconosciuto
Porta 30 (closed): Servizio sconosciuto
```

Codice in python
del programma

SCANSIONE DEI METODI

```
Inserisci un IP: 192.168.50.101
Inserisci la porta da scansionare: 80

Scansione sulla porta 80:
GET: Metodo presente
POST: Metodo presente
PUT: Metodo presente
DELETE: Metodo presente
PATCH: Metodo presente
OPTIONS: Metodo presente

Vuoi scansionare un'altra porta? (Si/No):
```

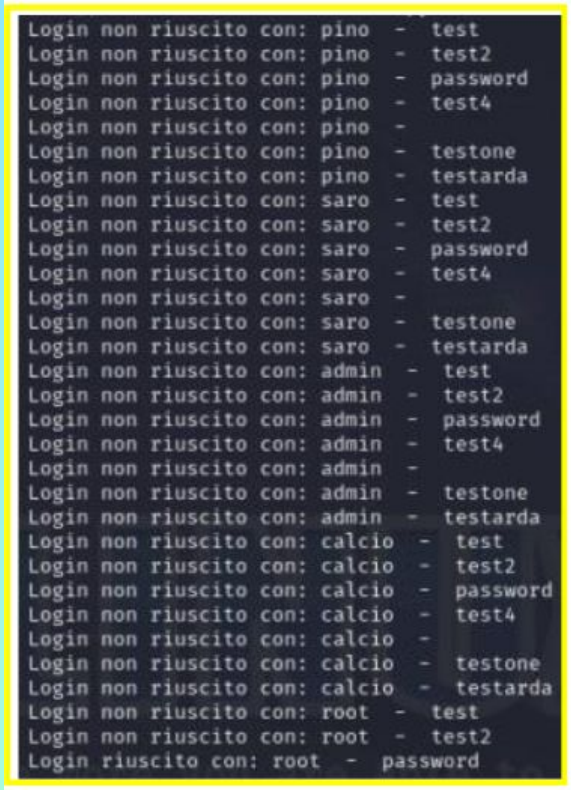
Scansione dei metodi HTTP abilitati sulla porta 80 del Web Server.

Codice in python
Del programma

BRUTEFORCE WEB SERVER

Come richiesto dal CISO abbiamo eseguito una simulazione di attacco bruteforce.
In allegato troverete un report con annesse criticità e consigli per migliorare la sicurezza del login.

Link Report



Codice in python del programma

BRUTEFORCE E-COMMERCE SERVER

Successivamente ,sempre sotto richiesta del CISO, abbiamo eseguito una simulazione di attacco bruteforce all'application server.
Anche in questo caso vi alleghiamo il link al report con i vari consigli e criticità.

Link Report

```
└─$ python BruteforceDVWA.py
Login riuscito come admin con password: password
Login non riuscito con: pino  -  test
Login non riuscito con: pino  -  test2
Login non riuscito con: pino  -  password
Login non riuscito con: pino  -  test4
Login non riuscito con: pino  -
Login non riuscito con: pino  -  testone
Login non riuscito con: pino  -  testarda
Login non riuscito con: saro  -  test
Login non riuscito con: saro  -  test2
Login non riuscito con: saro  -  password
Login non riuscito con: saro  -  test4
Login non riuscito con: saro  -
Login non riuscito con: saro  -  testone
Login non riuscito con: saro  -  testarda
Login non riuscito con: admin  -  test
Login non riuscito con: admin  -  test2
Login riuscito con: admin  -  password
```

GRAZIE!

Crediti:

- *Kristiano Kamenica*
- *Marco D'Antoni*
- *Gerardo Carrabs*
- *Georges Fotsing*
- *Samuel Capoti*
- *Gabriel Goldy*
- *Prince Dylan Colletta Ehichioya*
- *Sergio Bodron*