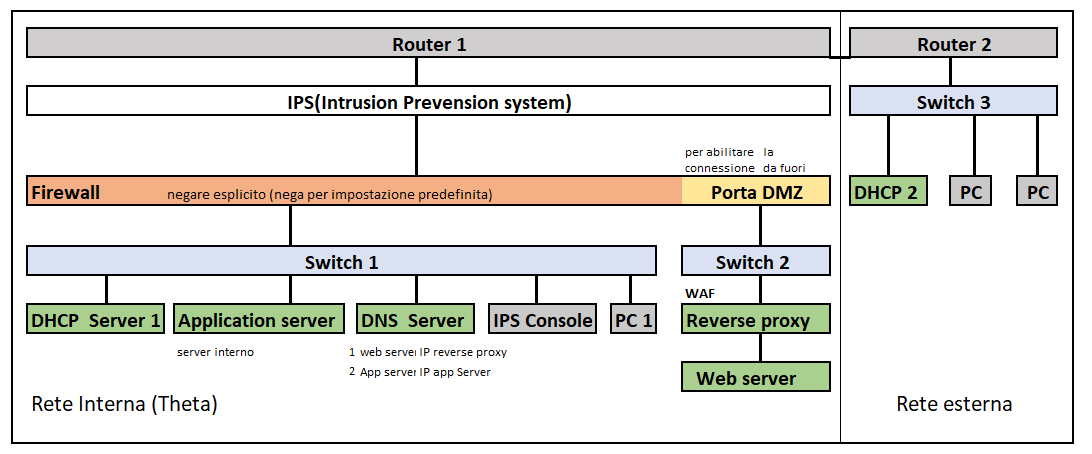
Report Totale

Valutazione di Sicurezza

Theta Company

1. **Modello Di Rete**

**Modello Block Diagram**

Per migliorare il design della rete, abbiamo aggiunto alcune funzionalità come mostrato nella figura sopra:

1. **IPS (Sistema di prevenzione delle intrusioni)**

Un sistema di prevenzione delle intrusioni (IPS) è uno strumento di sicurezza della rete (che può essere un dispositivo hardware o un software) che monitora continuamente una rete per rilevare attività dannose e intraprende azioni per prevenirle, inclusi segnalazione, blocco o eliminazione, quando si verifica.

1. **Firewall con DMZ**

Il firewall con la funzione di negazione esplicita per impedire qualsiasi richiesta di connessione dall'esterno dell'azienda, una porta DMZ (area) dove abbiamo collegato il server WEB, le DMZ consentono le connessioni dall'esterno.

1. **Reverse Proxy Server (proxy inverso)**

Viene utilizzato per coprire il server originale poiché la richiesta di connessione dall'esterno andrà direttamente al server proxy inverso, abbiamo anche installato il WAF (WEB Application Firewall) che è responsabile del filtraggio dei pacchetti dannosi http e https.

1. **VLAN (Virtual lan)**

La Vlan e la segmentazione della rete per salvaguardare nodi aziendali dal rischio di infezioni

Modello Packet Tracer

Graphical user interface

Description automatically generated

Con il rettangolo grande arancio abbiamo delimitato la zona aziendale

Con il rettangolo celeste abbiamo delimitato la zona DMZ

Con il rettangolo verde abbiamo delimitato la zona firewall

Con il rettangolo bianco abbiamo rappresentato la rete pubblica

Abbiamo messo il (IPS) tramite il router e il firewall per prevenire tutta la rete dalla connessione malevoli.

1. **Web server**
2. **Port scan:**

**Esecuzione del programma**

Text

Description automatically generated

Innanzitutto, abbiamo creato un programma per testare le porte aperte nel server, come mostrato in figura. Abbiamo riscontrato che le porte aperte sono molte rispetto a quelle che servono per l’utilizzo del server; quindi, consigliamo di chiudere le porte non necessarie.

Alcuni consigli:

1. Chiudere la porta 23 Telnet perché si usa per fare connessione da remoto ma non in maniera criptata. E consigliato usare la porta 22 (ssh) perché criptata
2. Usare HTTPS su porta 443 invece di usare l’HTTP sulla porta 80, perché, con HTTPS la connessione sarà più sicura

**Codice Port scan:**

A screenshot of a computer

Description automatically generated

1- **Import**:

Dove va ad importare le librerie socket, platform, os preconfigurate a linux per poter usare le sue funzioni

2- **target, portrange**:

Sono variabili che salvano l’inserimento dell’utente di IP e numero della porta tramite funzione **input**

3- **lowport, highport**:

Sono variabili per chiamare la funzione preconfigurata **split ()**

4- **Ciclo for**:

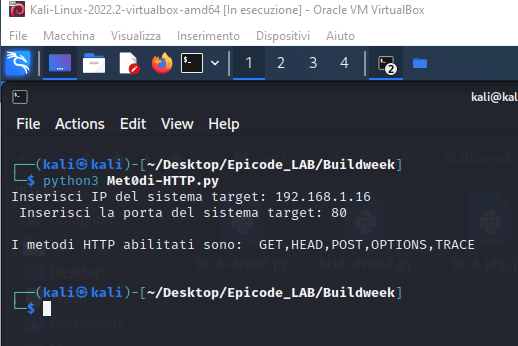
Per scansionare il range di porte date dall’utente

5- **Controllo if**:

Se la porta e aperta il programma indica il numero della porta e il nome del servizio.

1. **Application server**
2. **I metodi di http**

**Esecuzione del programma**



Abbiamo creato un programma per dimostrare i metodi abilitati http nella pagina phpMyAdmin del vostro server web e come mostrato nella figura abbiamo riscontrato che i metodi abilitati sono

• GET:

Il metodo GET richiede una rappresentazione della risorsa specificata. Le richieste che utilizzano GET dovrebbero solo recuperare i dati.

• HEAD:

Il metodo HEAD richiede una risposta identica a una richiesta GET, ma senza il corpo della risposta.

• POST:

Il metodo POST invia un'entità alla risorsa specificata, causando spesso una modifica dello stato o effetti collaterali sul server.

• OPTIONS:

Il metodo OPTIONS descrive le opzioni di comunicazione per la risorsa di destinazione.

• Trace:

Il metodo TRACE esegue un test di loopback del messaggio lungo il percorso della risorsa di destinazione.

**Codice metodi http**

A screenshot of a computer

Description automatically generated

Il programma e composta da 4 parti come si è mostrato nella figura

1. **Import**:

Dove va ad importare la libreria http.client preconfigurata a linux per poter usare le sue funzioni

1. **Host, port**:

Sono variabili che salvano l’inserimento dell’utente di IP e numero della porta tramite funzione **input**

1. **Controllo** **if**:

Controlla se l’inserimento dell’utente e = 80

1. **Ciclo try**:

Permette di intercettare gli errori nell’esecuzione di istruzioni tramite la funzione **except**

1. **Brute force-dvwa**

Text

Description automatically generatedC**odice brute-force**

Il programma e composta da 4 parti come si è mostrato nella figura

1. **import**:

Dove va ad importare le librerie http.client e urllib.parse preconfigurata a linux per poter usare le sue funzioni

1. **username\_file, password\_file**:

Sono variabili che aprono il file nel percorso scritto nella funzione **open**.

1. **user\_list, password\_list:**

Sono variabili che leggono il contenuto del file tramite la funzione **readlines ()**

1. **Target, url:**

Sono variabili che salvano l’inserimento dell’utente di IP e url da attaccare

1. **Doppio for**:

Per selezionare l’user dalla lista di username e provare tutte password nella lista finche trova quelli esatti

1. **Controllo if**:

per controllare il contenuto di location in header.

**Esecuzione del programma**

Text

Description automatically generated

Il programma come mostrato in figura ha subito trovato le credenziali di accesso essendo molto comuni. Abbiamo provato a immaginare che un dipendente dell’azienda scrivesse una password leggermente più complessa, ma riconducibili ai sui dati anagrafici (federico91)

Text

Description automatically generatedRiscontrando che un possibile attacco

di brute force può intercettare una

password che abbia solo caratteri e

numeri

Text

Description automatically generatedMettendo una password

Complessa (feDerico@91)

Abbiamo riscontrato che il

Sistema non individua la

password di ingresso

Considerazioni per i dipendenti

1. Non usare nomi e date di nascita relativi al vostro nucleo famigliare.
2. Non usare parole presenti nei dizionari perché possibile utilizzare tali dizionari in formato elettronico.
3. Non scrivere e non memorizzare la password sulle utenze utilizzate.
4. Non salvare la password sul browser come mostrato in figura:

A screenshot of a computer

Description automatically generated

1. E buona norma cambiare la password ogni 2-3 mesi.
2. Utilizzare caratteri speciali per rafforza la sicurezza della password.
3. Utilizzare la password di minimo di 10 caratteri.

Queste sono le norme oltre alla sicurezza perimetrale aziendale