SBAMPF

Bèccate ‘sta rete de sicurezza

Non può entrare

COSE ANCORA DA FARE/SCRIVERE:

* inserire tutti gli screen mancanti (Federico)
* Promemoria: controllare che i nomi dei programmi corrispondano a quelli degli screen e a quelli consegnati in file .py a parte
* Va controllata la sezione in cui descriviamo il design di rete e motiviamo le scelte;
* Manca la sezione Brute Force PHP
* Manca la sezione Brute Force DVWA
* Manca la sezione sul Brute Force di DVWA (tab) (Alex)
* Le contromisure per ora sono SOLO generiche; occorrerà scrivere quelle specifiche per la Theta e specificare con quale cadenza implementare alcune delle misure di sicurezza (to do list la rotazione delle password)
* Vogliamo inserire un fattore di rischio numerico?

Indice

[Introduzione 1](#_Toc153377087)

[Metodologia 1](#_Toc153377088)

[Design di rete per la messa in sicurezza delle componenti critiche oggetto di analisi 2](#_Toc153377089)

[Programma in Python per la valutazione dei servizi attivi (port scanning); 3](#_Toc153377090)

[Programma in Python per l’enumerazione dei metodi HTTP abilitati su un determinato target 4](#_Toc153377091)

[Report degli attacchi Brute Force sulla pagina phpmyadmin con evidenza della coppia username-password utilizzata per ottenere accesso all’area riservata; 5](#_Toc153377092)

[Report totale che include i risultati trovati e le contromisure da adottare per ridurre eventuali rischi; 7](#_Toc153377093)

[Contromisure da adottare per ridurre eventuali rischi 7](#_Toc153377094)

# Introduzione

L’azienda Theta ci ha ingaggiato per eseguire valutazioni di sicurezza su alcune infrastrutture critiche del loro data center.

Il perimetro delle attività si concentra principalmente su:

Un Web server che espone diversi servizi su internet (e quindi accessibili al pubblico)

Un Application server che espone sulla rete interna un applicativo di e-commerce accessibile dai soli impiegati della compagnia Theta (quindi non accessibile da resti esterne, ovvero internet)

# Metodologia

L’azienda ha chiesto di riprodurre Web Server e Application Server in ambiente di test così da non effettuare test invasivi sull’ambiente di produzione. Per questo, ci siamo avvalsi di Metasploitable per simulare il Web Server di Theta, mentre abbiamo utilizzato la macchina di Kali nel ruolo di attaccante.

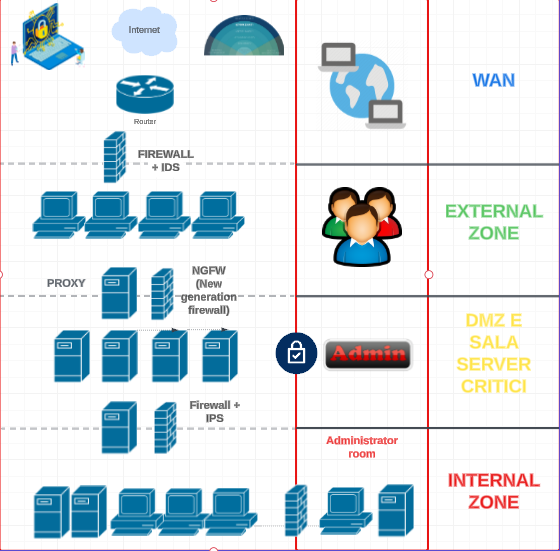
Come da ulteriore richiesta, non abbiamo utilizzato tool già disponibili in Kali, ma abbiamo programmato i tool da zero in linguaggio Python.

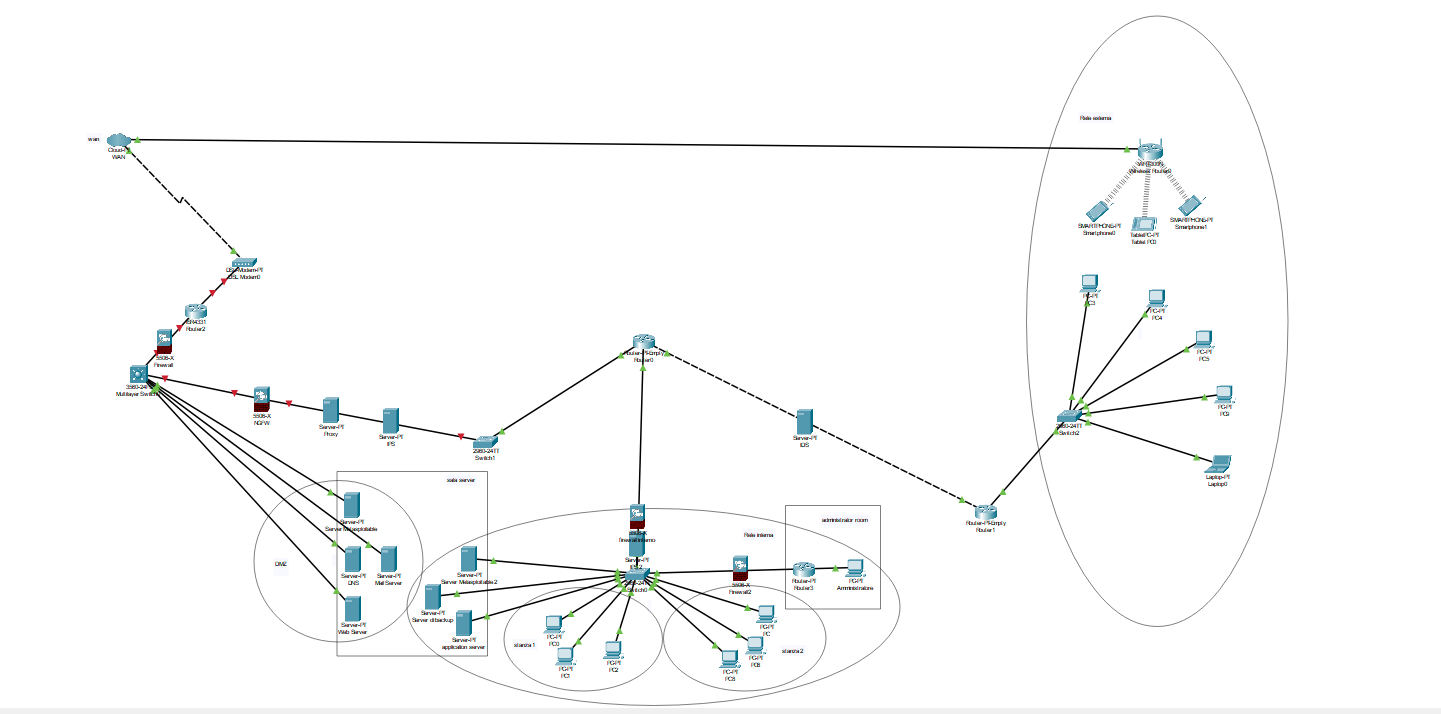
Il CISO ha stabilito i seguenti task da portare a termine:

1. Design di rete per la messa in sicurezza delle componenti critiche oggetto di analisi;
2. Programma in Python per l’enumerazione dei metodi HTTP abilitati su un determinato target
3. Programma in Python per la valutazione dei servizi attivi (port scanning);
4. Report degli attacchi Brute Force sulla pagina phpmyadmin con evidenza della coppia username-password utilizzata per ottenere accesso all’area riservata;
5. Report degli attacchi Brute Force sulla DVWA per ogni livello di Sicurezza (low, medium, high);
6. Report totale che include i risultati trovati e le contromisure da adottare per ridurre eventuali rischi;

Nelle sezioni di seguito vedremo lo svolgimento di ciascun task.

## Design di rete per la messa in sicurezza delle componenti critiche oggetto di analisi





Il CISO della compagnia Theta ci ha richiesto di proporre un modello (design) di rete per mettere in sicurezza le due componenti critiche dell’azienda (Web Server e Application Server), includendo nell’analisi i dispositivi di sicurezza che potrebbero servire per aumentare la protezione della rete.

Il nostro design di rete prevede tre zone principali: una DMZ (zona demilitarizzata), una rete interna e una rete esterna. Occorrerà inoltre predisporre due aree fisiche all’interno dell’azienda: la Sala Server, che include i server della DMZ e quelli della rete interna, e la Administrator room, che include il rooter e il PC dell’Amministratore, anch’essi collegati alla linea interna.

DMZ (Zona Demilitarizzata):

La DMZ serve a ospitare servizi accessibili dall'esterno, come server web o servizi di posta elettronica, in modo che siano isolati dalla rete interna per motivi di sicurezza.

Nel nostro caso la DMZ contiene il Server Metasploitable, il DNS e il Web Server.

Rete Interna:

La rete interna è la parte della rete aziendale che contiene risorse e servizi critici per l'organizzazione. Nel nostro caso ospita un Server Metasploitable 2 di backup, un altro Server di backup e l’Application Server. Ospita inoltre il PC dell’Amministratore con relativo router e 6 PC per i dipendenti.

Rete Esterna:

La rete esterna rappresenta l'area al di fuori della rete aziendale.

Dispositivi di sicurezza:

**Fra il Modem e la rete interna**, consigliamo il posizionamento in quest’ordine di:

Un firewall perimetrale

Un proxy

Un IPS

Il **firewall perimetrale** è la prima linea di difesa tra la rete interna e Internet. Controlla e filtra il traffico in ingresso e in uscita sulla base di regole di sicurezza predefinite.

Il **proxy** funge da intermediario tra i dispositivi interni della rete e Internet, consentendo un controllo più granulare sull'accesso a risorse web.

L’**IPS** monitora il traffico di rete per rilevare e prevenire intrusioni o attacchi informatici, protegge la rete da attacchi dannosi, come tentativi di intrusioni, malware o exploit, interviene attivamente per bloccare o mitigare tali minacce.

Abbiamo aggiunto l’ulteriore protezione di un firewall alla rete interna e collocato invece un **IDS** fra la

Rete interna e la Rete esterna, tale dispositivo permetterà di monitorare il traffico di rete, rilevare attività sospette in entrata o in uscita. L’IDS non interverrà attivamente ma si limiterà a segnalare le potenziali minacce agli amministratori di sistema.

## Programma in Python per la valutazione dei servizi attivi (port scanning);

Un **portscanning** è fondamentale per sondare un range di porte su una macchina per determinare quali di esse sono in ascolto e quali servizi sono attivi. Questo può essere utile sia per garantire che solo i servizi necessari siano attivi, sia per rilevare quelle vulnerabilità che potrebbero essere sfruttate per lanciare attacchi mirati.

Qui l’esempio del portscanning utilizzato per andare a scansionare le porte aperte sul server 192.168.32.101.

A screenshot of a computer screen

Description automatically generated

Si devono inserire manualmente IP del server che vogliamo scansionare e successivamente il range di porte da controllare. Una volta forniti i dati, il programma manderà a schermo le informazioni inserite ed inizierà a scansionare le porte aperte ed il servizio disponibile per ogni porta.

Nello specifico, partendo da linea di codice numero 16 leggiamo: per tutte le porte nel range interessato tentiamo una connessione IPv4 TCP; se le porte sono aperte ,*(status == 0)*, il programma manderà a schermo le informazioni di:

*A computer screen shot of a program

Description automatically generated*

Possiamo notare che in questo esempio abbiamo voluto scansionare tutte le porte aperte, dalla 1 all 1024, per andare ad individuare in un secondo momento le vulnerabilità del server. Il programma non ci rivela le porte chiuse, che non ci interessano, mentre delle porte aperte, grazie alla linea di codice numero 20, possiamo sapere anche il tipo di servizio disponibile.

Ai fini di questo report andiamo ad osservare la porta 80; la porta è aperta e il suo servizio è HTTP.

Quest’ultima informazione è particolarmente interessante ai fini della sicurezza, perchè alcune porte potrebbero essere vulnerabili ad attacchi potenzialmente rischiosi:

* port 21:se il servizio FTP (File Transfer Protocol) è aperto e non è configurato in modo sicuro, potrebbe essere sfruttato per accessi non autorizzati e trasmissione di dati sensibili.
* port 23: telnet è un protocollo di comunicazione non crittografato, e se la porta Telnet è aperta senza cifratura, le credenziali e i dati possono essere esposti.
* port 25: Se il servizio di posta (SMTP - Simple Mail Transfer Protocol) è aperto in modo non sicuro, potrebbe essere utilizzato per inviare spam o sfruttato per attacchi di phishing.

## Programma in Python per l’enumerazione dei metodi HTTP abilitati su un determinato target

Conoscere i **metodi HTTP** attivi su una porta consente agli amministratori di sistema di identificare i servizi web in esecuzione su un server. Questo è utile per la gestione e la manutenzione della rete. Se un server supporta metodi obsoleti o non sicuri, è necessario prendere provvedimenti per mitigare i rischi associati. Se vengono utilizzati metodi noti per essere vulnerabili, gli amministratori possono adottare misure preventive o correttive.

Vi è inoltre un aspetto di efficientamento non direttamente legato alla sicurezza informatica ma comunque importante a livello di sistema: conoscere i metodi HTTP attivi può aiutare nell'ottimizzazione e nella gestione del traffico di rete. Ad esempio, potrebbe essere necessario indirizzare o filtrare specifici metodi per migliorare le prestazioni.

Per ottenere informazioni sui metodi abilitati sulla nostra porta target abbiamo elaborato un secondo programma “NOME\_PROGRAMMA.PY”:

—------- INSERIRE SCREEN CODICE—---------

L’obiettivo di questo script Python è effettuare una richiesta HTTP di tipo OPTIONS a un server di destinazione specifico e visualizzare i metodi HTTP consentiti dal server.

Il programma inizia richiedendo all’utente di inserire l’indirizzo IP del server di destinazione (nel nostro caso quello di Metasploitable) e, se necessario, la porta. Se questa non viene specificata viene utilizzato il valore di default 80 (che è la porta genericamente associata ai servizi HTTP).

Successivamente, il programma tenta di stabilire una connessione al server utilizzando la classe ‘HTTPConnection’ del modulo ‘http.client’. Una volta stabilita la connessione, viene inviata una richiesta HTTP di tipo OPTIONS al server, specificando il percorso della richiesta (nel nostro caso http://192.168.XX.YYY/phpMyAdmin/phpMyAdmin.html).

Dopo aver ricevuto la risposta dal server, il programma estrae i metodi consentiti dalla risposta, analizzando il campo dell’intestazione ‘Allow’. Questi metodi vengono quindi stampati a schermo uno per uno.

Infine, il programma chiude la connessione al server.

In caso di connessione rifiutata (ad esempio, se il server non è in ascolto sulla porta specificata), gestisce un’eccezione ‘ConnectionRefusedError’ e stampa un messaggio d’errore.

—-----EVENTUALE SCREEN DI CONNESSIONE NON RIUSCITA—----

Lanciando il programma, abbiamo rilevato che sulla porta 80 di Metasploitable sono attivi i seguenti metodi: GET, HEAD, POST, OPTIONS, TRACE:

A screenshot of a computer screen

Description automatically generated

Elenchiamo brevemente alcune vulnerabilità associate a ciascun metodo:

GET:

I parametri della richiesta GET sono inclusi nell'URL, quindi possono essere memorizzati nei log del server web o nei log intermediari, esponendo potenzialmente informazioni sensibili come token di sessione.

HEAD:

E’ simile a GET, ma restituisce solo le intestazioni della risposta senza il corpo. Valgono le medesime considerazioni sulla raccolta di informazioni sensibili.

POST:

Injection di parametri: I dati del corpo della richiesta POST possono essere soggetti ad attacchi di injection (ad esempio, SQL injection o XSS) se non vengono trattati correttamente dal lato server.

Cross-Site Request Forgery (CSRF): Le richieste POST possono essere soggette a attacchi CSRF se non vengono adottate misure di sicurezza adeguate, come l'uso di token CSRF.

OPTIONS:

La richiesta OPTIONS può restituire informazioni sulla configurazione del server, rivelando dettagli potenzialmente sensibili.

TRACE:

Il metodo TRACE può essere sfruttato per eseguire attacchi di Cross-Site Tracing, in cui un malintenzionato può ottenere informazioni sulle intestazioni della richiesta inviata da un client. TRACE è spesso disabilitato per motivi di sicurezza.

Come già detto, l'utilizzo dei metodi HTTP dovrebbe essere limitato solo a quelli necessari per l'applicazione.

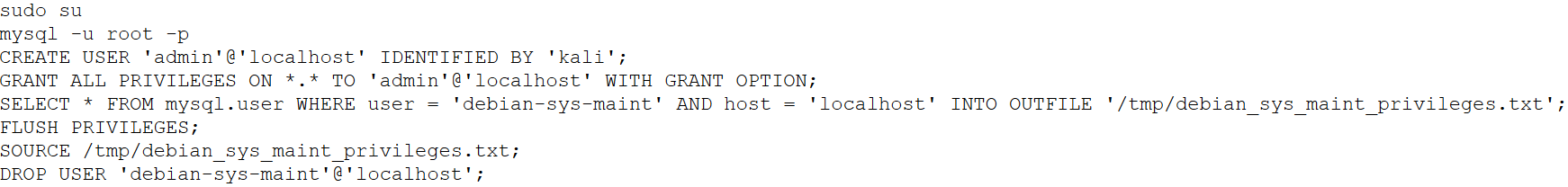
## Report degli attacchi Brute Force sulla pagina phpmyadmin con evidenza della coppia username-password utilizzata per ottenere accesso all’area riservata;

L’attacco **brute force** è una tecnica utilizzata in ambito di cybersecurity per ottenere accesso non autorizzato a un sistema o a un account. In questo tipo di attacco, l'attaccante cerca di indovinare la password di un account provando una serie di possibili combinazioni, spesso sfruttando un "dizionario" contenente parole comuni, frasi, o combinazioni di caratteri. L'esecuzione di attacchi controllati aiuta a valutare quanto un sistema sia esposto a rischi di sicurezza e quale potrebbe essere l'impatto di un attacco reale.

Nel caso in oggetto, ci è stato richiesto di effettuare un attacco Brute Force dizionario per effettuare il login su PhpMyAdmin.

Come prima cosa, ci spostiamo su Metasploitable e andiamo a settare la macchina creando un utente “admin” cui associamo la password “kali”.

Lo facciamo utilizzando i seguenti comandi:



Che implementiamo naturalmente su Metasploitable:

A screenshot of a computer screen

Description automatically generated

Ora ci spostiamo su Kali. Per eseguire il Brute Force scriviamo un terzo programma in Python.

Questo programma si avvale delle liste di username e password più comuni già presenti su Kali e tramite due cicli for, l’uno nidificato nell’altro, prova tutte le combinazioni finché il codice di risposta del sito non risulta essere 200. A quel punto stampa “Successo !!” per comunicarci qual è la coppia corretta di credenziali per entrare e interrompe l’esecuzione.

A screenshot of a computer

Description automatically generated

Poiché conosciamo già username e password corretti avendoli creati noi, per ottimizzare il processo modifichiamo la lista username spostando “admin” in cima e inseriamo invece nella lista password “kali”, anche qui in cima alla lista.

Pochi secondi dopo il lancio del Brute Force, il programma ci comunica di aver trovato la coppia corretta, come da screen di seguito:

A screenshot of a computer

Description automatically generated

## Report totale che include i risultati trovati e le contromisure da adottare per ridurre eventuali rischi;

### Contromisure da adottare per ridurre eventuali rischi

Politiche di sicurezza: Definire e attuare politiche di sicurezza chiare e ben definite per proteggere le risorse aziendali. Queste politiche dovrebbero coprire l'accesso autorizzato, la gestione delle password, l'uso sicuro dei dispositivi, e altro ancora.

Formazione degli Utenti: Fornire formazione sulla sicurezza informatica ai dipendenti per aumentare la consapevolezza sui rischi e insegnare pratiche di sicurezza come la creazione di password robuste e la gestione delle e-mail.

Gestione delle Password: Implementare politiche robuste per la gestione delle password, inclusa la richiesta di password complesse, la rotazione periodica delle password e l'autenticazione a due fattori (2FA) quando possibile.

Aggiornamenti e Patch: Mantenere tutti i sistemi operativi, applicazioni e software di sicurezza aggiornati con le ultime patch e aggiornamenti di sicurezza per mitigare vulnerabilità note.

Protezione Antivirus e Antimalware: Installare e mantenere aggiornati programmi antivirus e antimalware su tutti i dispositivi per rilevare e prevenire attacchi malware.

Firewall: Configurare e mantenere firewall per proteggere la rete aziendale da accessi non autorizzati e attacchi provenienti dall'esterno.

Controllo degli Accessi: Implementare un sistema di controllo degli accessi che limiti l'accesso alle risorse aziendali solo a coloro che ne hanno bisogno per svolgere le proprie mansioni.

Backup Regolari: Effettuare regolarmente il backup dei dati aziendali critici e assicurarsi che i backup siano archiviati in modo sicuro. In caso di attacco ransomware o perdita di dati, sarà possibile ripristinare le informazioni.

Monitoraggio della Sicurezza: Implementare strumenti di monitoraggio della sicurezza per rilevare e rispondere tempestivamente agli incidenti di sicurezza. Questo può includere il monitoraggio degli accessi, la rilevazione delle minacce e l'analisi dei log.

Politiche di Utilizzo dei Dispositivi Mobili: Se i dipendenti utilizzano dispositivi mobili aziendali o personali, implementare politiche chiare sulla sicurezza dei dispositivi mobili, inclusa la crittografia dei dati e il controllo remoto.

Consapevolezza della Privacy: Rispettare le normative sulla privacy dei dati, come il GDPR, e garantire che le pratiche aziendali siano conformi a tali normative.

Test di Sicurezza e Audit: Condurre regolarmente test di sicurezza e audit per identificare e correggere potenziali vulnerabilità prima che possano essere sfruttate da attaccanti.

Queste sono solo alcune delle pratiche di sicurezza di base che le aziende possono adottare. La sicurezza informatica è un processo continuo che richiede una vigilanza costante e l'adattamento alle nuove minacce. Le raccomandazioni specifiche possono variare in base alle esigenze e al contesto specifico di ciascuna azienda.