



CyberEagles srl

Sede legale: via volo 1000

00011, Cyberia, <21/6/2024>

Ns. Rif: ORD/2024/00123

Telefono:010/0110010

Email:cybereagles@volo.com

Spett.THETA srl
via scarsa sicurezza 10
00011, Cyberia

Alla c.a. del CISO P.Ranpini

Oggetto: Consulenza per la messa in sicurezza della rete aziendale THETA srl

In seguito ai precedenti contatti, siamo lieti di sottoporVi la nostra proposta economica relativa all'oggetto in questione. I dettagli della proposta sono esposti nei capitoli successivi di questo documento.

Si precisa che la presente offerta annulla e sostituisce tutte le precedenti comunicazioni inerenti.

Cogliamo l'occasione per porgerVi i nostri migliori saluti.

Responsabile commerciale

Sommario

● Architettura implementata del design di rete	4
1. Introduzione al design di rete.....	4
2. Proposta di migrazione a server HTTPS.....	5
3. Creazione di una Zona DMZ con WAF e IPS.....	5
4. Implementazione di Server Interni Dedicati.....	6
5. Componenti da Implementare: WAF, Server, IPS, IDS, UPS.....	7
● Implementazioni servizi di sicurezza.....	7
1. Incident Response: Gestione degli incidenti di sicurezza informatica.....	7
2. Servizi SOC: Monitoraggio e risposta alle minacce di sicurezza.....	9
3. Formazione del Personale: Importanza della formazione.....	9
4. In evidenza.....	10
● Programma in Python per l'enumerazione dei metodi HTTP abilitati su un determinato target.....	12
1. Introduzione al progetto.....	12
2. Descrizione dei metodi HTTP.....	12
3. Sviluppo del programma in Python.....	13
4. Test e analisi.....	14
5. Contromisure e raccomandazioni.....	15
● Programma in Python per la valutazione dei servizi attivi (port scanning).....	15
1. Introduzione al progetto.....	15
2. Funzione del codice.....	16
3. Test e analisi.....	17
4. Conclusioni.....	17
5. Contromisure e raccomandazioni.....	18

● Report degli attacchi Brute Force su phpMyAdmin.....	18
1. Introduzione all'attacco Brute Force.....	18
2. Metodologia utilizzata per l'attacco.....	18
3. Test e analisi.....	19
4. Conclusioni.....	20
5. Contromisure e raccomandazioni.....	20
● Report degli attacchi Brute Force su DVWA	21
1. Introduzione all'attacco brute force su DVWA.....	21
2. Struttura e funzionamento dello script.....	21
3. Test e analisi.....	22
4. Conclusioni.....	24
5. Contromisure e raccomandazioni.....	25
● Report conclusivo dei risultati e contromisure.....	25
1. Analisi delle vulnerabilità riscontrate.....	25
2. Contromisure e raccomandazioni.....	27
3. Costi e servizi.....	30

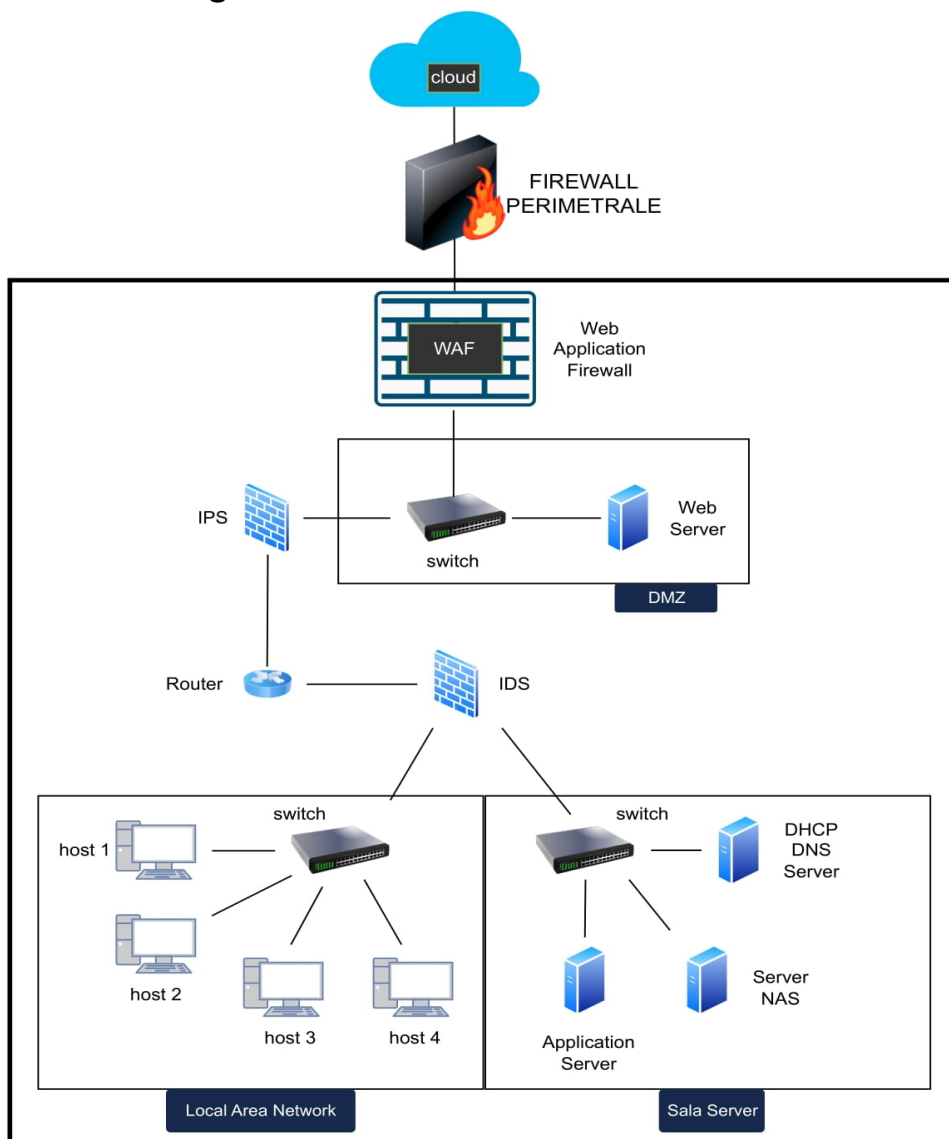
Architettura implementata del design di rete

Introduzione al design di rete

Con il presente documento, la CyberEagles srl fornisce tutte le indicazioni e le specifiche necessarie ai fini della valutazione di rischio riguardanti le infrastrutture critiche della rete aziendale Theta Corporation.

Il progetto prevede un' analisi della sicurezza della rete aziendale, effettuata in un laboratorio di test al fine di operare le modifiche necessarie al design di rete per risolvere le criticità esistenti ed implementare la sicurezza del sistema stesso.

Modifiche al design di rete



Proposta di migrazione a server HTTPS

Riteniamo che sia fondamentale per il web server dell'azienda Theta passare da un protocollo **HTTP a HTTPS**, in quanto questa transizione offre numerosi vantaggi significativi. HTTPS utilizza la crittografia SSL/TLS per proteggere i dati trasmessi tra il client e il server, garantendo la sicurezza e l'integrità delle informazioni sensibili come password e dati personali. Inoltre, HTTPS verifica l'identità del sito web tramite certificati digitali, **prevenendo attacchi di tipo "man-in-the-middle"** e assicurando agli utenti che stanno comunicando con il sito legittimo.

In conclusione, il protocollo HTTP presenta gravi limitazioni in termini di sicurezza e protezione dei dati rispetto a HTTPS. Nei test condotti nei laboratori, è evidente che HTTP trasmette i dati in chiaro, senza crittografia, rendendoli vulnerabili ad attacchi di intercettazione e manipolazione condotte da terze parti malevole. Questa vulnerabilità espone le informazioni sensibili a rischi significativi di compromissione e violazione della privacy, **sottolineando l'importanza di adottare HTTPS** per garantire una comunicazione sicura e protetta su Internet.

Creazione di una Zona DMZ con WAF e IPS

Proponiamo la creazione di una DMZ (zona demilitarizzata) per ospitare il web server accessibile dalla WAN. La DMZ proteggerà la rete locale dalla rete esterna tramite l'uso di un **WAF** e di un **IPS**.

- **WAF**

Il Web Application Firewall (WAF) protegge le applicazioni nel cloud, on-premise e in ambienti multicloud con controlli avanzati basati su geolocalizzazione, liste di inclusione/esclusione IP, URL e intestazioni HTTP. Blocca il traffico bot maligno con tecniche come JavaScript injection, CAPTCHA, fingerprinting dei dispositivi e analisi dell'interazione umana. Inoltre, utilizza regole OWASP per prevenire attacchi comuni come **SQL injection** e cross-site scripting (XSS), assicurando la sicurezza delle applicazioni web.

- **IPS**

Un IPS (Intrusion Prevention System) è un dispositivo di sicurezza di rete che monitora il traffico di rete per identificare e prevenire attività sospette o dannose. L'IPS analizza i dati in tempo reale, confrontandoli con una base di regole predefinite per rilevare anomalie, vulnerabilità note o comportamenti anomali, e blocca automaticamente le minacce per proteggere le reti e i sistemi da attacchi informatici.

Implementazione di Server Interni Dedicati

Per garantire una maggiore sicurezza e riservatezza dei dati proponiamo di creare una zona server dedicata, come ad esempio un armadio server con al suo interno il web application server un **server NAS**, per creare dei backup e un **server DHCP** e DNS, il quale contribuisce significativamente alla sicurezza e alla gestione efficiente della rete aziendale in quanto semplifica la gestione degli indirizzi IP nella rete interna, assicurando che i dispositivi ottengano configurazioni IP corrette in modo automatizzato. Il **server DNS** gestisce la risoluzione dei nomi per garantire che gli host possano essere raggiunti tramite i nomi di dominio. Consigliamo anche di installare un IDS collegato alla zona server interni alla rete interna e a un modem collegato all'IPS della DMZ. Nella zona server è inoltre consigliato installare un sistema di alimentazione autonoma UPS al fine di preservare intatti i dati di backup del server NAS.

- **IDS**

L'IDS (Intrusion Detection System) è un sistema di sicurezza di rete che monitora il traffico di rete e i sistemi per rilevare attività sospette o violazioni di sicurezza. A differenza di un IPS, un IDS non blocca automaticamente le minacce, ma avvisa gli amministratori di rete quando rileva comportamenti anomali o potenzialmente dannosi, permette quindi di rilevare potenziali intrusioni nei server interni o nella rete interna.

Lista componenti da implementare

- N. 1 WAF Imperva SecureSphere WAF 3500
- N. 2 Server HP ProLiant ML110 Gen10
- N.1 IPS Cisco Firepower 1010
- N.1 IDS AlienVault OSSIM (Open Source Security Information and Event Management)
- N.1 UPS CyberPower CP1000PFCLCD

Implementazione servizi di sicurezza

Incident Response: Gestione degli incidenti di sicurezza informatica

L'incident response è un processo strutturato per identificare e gestire gli incidenti di sicurezza informatica. La risposta comprende diverse fasi, tra cui la preparazione agli incidenti, il rilevamento e l'analisi di un incidente di sicurezza, il contenimento, l'eradicazione e il recupero completo, nonché l'analisi e l'apprendimento post-incidente.

Strutturazione del modello consigliato:

Al fine di ottimizzare le risorse per ottenere una risposta rapida ed efficace, adeguata alle esigenze della azienda THETA, si consiglia di strutturare il team addetto all'incident response (**CSIRT o Computer Security Incident Response Team**) nel seguente modo:

- **Modello Centralizzato interno all'azienda:**

Con questo si intende che un team dedicato interno all'azienda THETA dovrebbe essere istruito al monitoraggio della rete e istruito alle procedure di first response in caso di incidente



- **Con Outsourcing parziale:**

Esternalizzare quindi ad una ditta esterna per il supporto e analisi approfondite dell'incidente.

La Cyber Eagles srl offre un servizio 24/7 di incident response al quale poter fare riferimento, ulteriori informazioni sul servizio possono essere reperite tramite il numero di assistenza 700.123.123 e sul sito <https://cybereagles.com/incidentresponse>

Ruoli e Responsabilità del Team Interno

- **Monitoraggio Continuo:** Sorvegliare i sistemi e rilevare potenziali incidenti di sicurezza.
- **Valutazione Iniziale:** Determinare la gravità e la natura dell'incidente.
- **Mitigazione di Primo Livello:** Prendere misure immediate per contenere l'incidente e prevenire ulteriori danni.
- **Documentazione:** Registrare tutte le attività e le osservazioni durante il troubleshooting iniziale.
- **Comunicazione:** Informare il management e coordinarsi con il team esterno.

Collaborazione con Aziende Esterne

Una volta che il team interno ha gestito l'intervento iniziale, l'azienda esterna può essere coinvolta per:

- **Analisi Forense:** Condurre un'indagine dettagliata per capire come si è verificato l'incidente e determinare l'ampiezza del danno.
- **Mitigazione Avanzata:** Implementare soluzioni di sicurezza avanzate per risolvere completamente l'incidente.
- **Ripristino:** Aiutare nel ripristino dei sistemi compromessi.
- **Miglioramento delle Difese:** Fornire consulenza su come migliorare le difese dell'azienda per prevenire futuri incidenti.

Avere un team interno per il primo intervento è una strategia efficace che consente una risposta rapida e mirata agli incidenti di sicurezza, mentre un'azienda esterna può fornire competenze specialistiche e supporto avanzato. Questo approccio integrato migliora la capacità complessiva dell'organizzazione di gestire e mitigare gli incidenti di sicurezza informatica.

Servizi SOC: Monitoraggio e risposta alle minacce di sicurezza

Un **Security Operation Center (SOC)** è un centro operativo dedicato alla sicurezza informatica, essenziale per un'organizzazione che rischia di subire attacchi. Può essere sviluppato internamente, utilizzato come servizio esterno, o adottato in una combinazione di entrambi (ibrido). Quindi, un SOC moderno deve offrire funzionalità specifiche per il rilevamento e la risposta alle minacce, allineate con le priorità aziendali. E' fondamentale avere un modello di SOC flessibile, capace di adattarsi ad ogni tipo di cambiamento. Questo permette all'azienda di modificare il modello operativo secondo le necessità, valutando le risorse finanziarie, umane e tecniche disponibili per implementare e gestire un SOC.

In base alle necessità dell'azienda Theta, emerse durante la nostra consulenza, si raccomanda fortemente di considerare l'outsourcing del servizio SOC presso un azienda specializzata.

La Cyber Eagles srl offre un servizio SOC 24/7 al quale poter fare riferimento, ulteriori informazioni sul servizio possono essere reperite tramite il numero di assistenza 700.123.123 e sul sito <https://cybereagles.com/socservice>

Formazione del Personale: Importanza della formazione

- **simulazioni di attacco** (phishing test, penetration testing, e esercitazioni di emergenza), per valutare la preparazione dei dipendenti.
- **formazione on the job, e-learning** (coinvolgimento e motivazione del personale nei corsi di sicurezza)
- **gestione delle password** (password manager, cambi periodici delle password):
- **riconoscimento delle minacce** (Identificazione di malware, ransomware, attacchi di ingegneria sociale come phishing, smashing, vishing ecc..) anche con nuove tecnologie, ad esempio l' AI e deep fake video)
- **utilizzo sicuro di laptop, smartphone, e altri dispositivi mobili**
- **gestione delle Informazioni** (protezione delle informazioni sensibili)
- **risposta agli Incidenti** (Preparare i dipendenti a rispondere efficacemente a incidenti di sicurezza)



Investire in una **formazione completa e continua** sulla cybersecurity è essenziale per proteggere l'azienda dalle minacce informatiche e per garantire che i dipendenti siano sempre preparati a gestire le sfide legate alla sicurezza. Come consulenti di cybersecurity, sottolineiamo l'importanza cruciale per un'azienda di investire nella formazione del personale in ambito di sicurezza informatica. I dipendenti rappresentano la prima linea di difesa contro le minacce informatiche; senza una conoscenza adeguata e una consapevolezza delle **best practices**, anche le tecnologie di sicurezza più avanzate possono risultare inefficaci. La formazione continua non solo riduce il rischio di incidenti e violazioni, ma promuove una cultura aziendale orientata alla sicurezza.

In evidenza

Simulazioni di attacco:

La simulazione di un attacco informatico è un' emulazione di hacking affidata a personale specializzato. Tali test vengono eseguiti sulla **rete IT delle PMI** per identificare eventuali falle o vulnerabilità nella sicurezza del sistema aziendale. Nel caso in cui una divisione interna all'azienda non sia adeguatamente formata ad eseguire questi controlli è possibile richiedere l'intervento di un'azienda esterna.

Gestione delle password:

Redigere una policy sulla sicurezza delle password che ogni dipendente deve eseguire alla lettera.

Utilizzo di **password manager OBBLIGATORIO** (abbonamento fornito dall'azienda stessa. Quale password manager? 1password o ProtonPass).

Un password manager è una cassaforte digitale che permette di tenere al sicuro le proprie password in maniera crittografata, inoltre le genera per noi (lunghe, complesse e casuali), e non dovremmo ricordarle. Va ricordata solo la password principale per accedere a tale cassaforte, ma anche quella ovviamente deve essere accompagnata da forti criteri.



2FA:

L'autenticazione a due fattori è fondamentale per avere un ulteriore strato di sicurezza dopo l'autenticazione con la password. Si consiglia **Google Authenticator** o **Authy**.

E' assolutamente vietato utilizzare il servizio SMS come secondo fattore di autenticazione. Il protocollo SMS è vulnerabile ad attacchi come il SIM swapping, SIM Jacking, e MITM, motivo per il quale se ne sconsiglia caldamente l'utilizzo.

Utilizzo sicuro di laptop, smartphone, e altri dispositivi mobili:

I laptop aziendali di fascia alta, come i Lenovo ThinkPad, i Dell Latitude e alcuni HP (come gli EliteBook), sono progettati per soddisfare le più rigide policy di sicurezza aziendale. Questi dispositivi, noti per la loro robustezza, offrono numerosi vantaggi pratici e certificazioni di sicurezza avanzate, rendendoli ideali per l'uso in ambienti professionali esigenti. **Esiste inoltre l'esigenza di impostare la crittografia completa del disco (full disk encryption)**, che protegge i dati sensibili da accessi non autorizzati in caso di furto. Su Windows, questa protezione viene implementata tramite BitLocker.

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

1. Introduzione al progetto

L'obiettivo di questo progetto Python è creare un programma che permetta di enumerare i **metodi HTTP abilitati** su un determinato server o endpoint web. Questo strumento sarà particolarmente utile per verificare le configurazioni del server e identificare eventuali metodi HTTP che potrebbero essere disabilitati per ridurre la superficie di attacco.

In sintesi testa le vulnerabilità di un determinato server o endpoint web.

2. Descrizione dei metodi HTTP

I metodi HTTP sono delle operazioni che possono essere eseguite su una risorsa web. In breve, definiscono il modo in cui il client può interagire con quella determinata risorsa. I principali metodi HTTP includono:

- **GET**: Recupera dati da un server.
- **POST**: Invia dati al server per creare o aggiornare una risorsa.
- **PUT**: Sostituisce una risorsa esistente con i dati inviati.
- **DELETE**: Rimuove una risorsa specificata.
- **HEAD**: Simile al metodo GET, ma richiede solo l'intestazione della risposta.
- **OPTIONS**: Richiede al server quali metodi HTTP sono supportati su una risorsa.
- **PATCH**: Applica modifiche parziali a una risorsa.

3. Sviluppo del programma in Python

Questo script Python invia una richiesta HTTP OPTIONS a un host specificato dall'utente per determinare quali metodi HTTP sono supportati. Viene utilizzata la libreria **requests** per effettuare le richieste HTTP.

Funzionamento del Codice

1. Input dell'utente:

- L'utente fornisce l'URL dell'host e il numero di porta.
- In base alla porta fornita (80 per HTTP o 443 per HTTPS), viene costruito l'URL completo. Se la porta non è 80 o 443, il programma chiede di controllare la porta inserita e termina l'esecuzione.

2. Verifica dell'URL:

- Viene stampato l'URL costruito per confermare quale URL sarà verificato.

3. Invio della richiesta HTTP OPTIONS:

- Viene inviata una richiesta HTTP OPTIONS all'URL specificato. Questo metodo è usato per chiedere al server quali metodi HTTP sono supportati.

4. Gestione della risposta:

- Se la risposta ha un codice di stato 200 (OK), il programma controlla se l'intestazione Allow è presente nella risposta.
- Se l'intestazione Allow è presente, stampa i metodi supportati dal server.
- Se l'intestazione Allow non è presente, informa l'utente che l'intestazione non è presente nella risposta.
- Se la risposta ha un codice di stato diverso da 200, stampa il codice di stato della risposta.

5. Gestione degli errori:

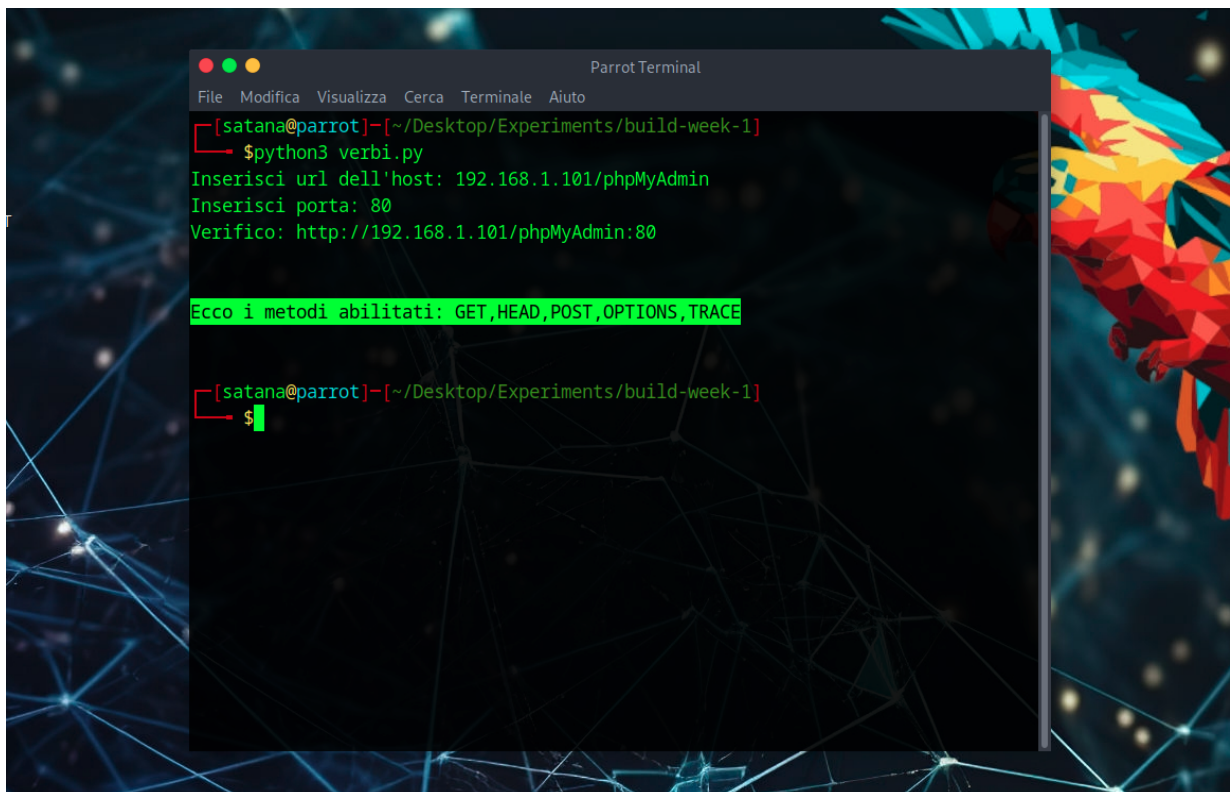
Se si verifica un'eccezione durante l'invio della richiesta, viene catturata e stampata un'appropriata descrizione dell'errore.

Questo programma offre una funzionalità di base per verificare quali **metodi HTTP** sono supportati da un server specificato dall'utente. La **richiesta OPTIONS** è utile per capire le capacità del server e può essere utilizzata come parte di un'analisi più ampia della configurazione e sicurezza di un server web.

Punti di forza

- **Accessibilità:** Permette all'utente di specificare l'host e la porta, offrendo flessibilità.
- **Verifica dei metodi HTTP:** Utilizza il metodo OPTIONS per determinare quali metodi HTTP sono supportati dal server.
- **Gestione delle eccezioni:** Cattura e gestisce eccezioni relative alle richieste HTTP, fornendo feedback utile all'utente.

Test e analisi



```
Parrot Terminal
File Modifica Visualizza Cerca Terminale Aiuto

[satana@parrot]~[~/Desktop/Experiments/build-week-1]
$python3 verbi.py
Inserisci url dell'host: 192.168.1.101/phpMyAdmin
Inserisci porta: 80
Verifico: http://192.168.1.101/phpMyAdmin:80

Ecco i metodi abilitati: GET,HEAD,POST,OPTIONS,TRACE

[satana@parrot]~[~/Desktop/Experiments/build-week-1]
$
```

Come si puo' notare, chiede L'URL e la porta specifica da input, poi parte con la scansione dei verbi attivi e rilascia appunto quali sono.

Contromisure e raccomandazioni

Per mitigare o prevenire attacchi basati sui verbi HTTP, si possono applicare determinate contromisure:

- **Limitazione dei verbi:** Configurare correttamente il server web affinché permetta solo ed unicamente i verbi necessari al corretto utilizzo dell'applicativo. Se ad esempio una pagina web non richiede l'uso di metodi come **PUT** o **DELETE**, è doveroso disabilitarli completamente.
- **Validazione Input:** Ricordarsi di implementare una rigorosa validazione dell'input dal punto di vista sia client che server, per prevenire l'inserimento di dati dannosi o inattesi (vedi progetto bonus SQL injection).
- **Controllo degli accessi:** Garantire l'autorizzazione ai verbi solo ad utenti autorizzati in base al contesto.

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

Introduzione al progetto

L'obiettivo del programma in **Python** per la valutazione dei servizi attivi (port scanning) è quello di eseguire una scansione delle porte su un determinato host o range di indirizzi IP. Il programma utilizzerà **socket e connessioni di rete** per verificare la disponibilità dei servizi su ciascuna porta, determinando se una porta è aperta, chiusa o filtrata. Il risultato della scansione verrà presentato all'utente, indicando quali porte sono aperte e quindi potenzialmente accessibili per servizi o attività di rete. Questo strumento è utile per la valutazione della sicurezza di un sistema o per la configurazione della rete, identificando potenziali vulnerabilità o configurazioni errate di firewall o router.

Funzionamento del Codice

1. Input dell'utente:

- L'utente fornisce l'indirizzo IP da scansionare e un intervallo di porte (ad esempio, 0-1024)

2. Preparazione per la scansione:

- Due liste vuote vengono inizializzate per tenere traccia delle porte chiuse (**porte_chiuse**) e delle porte filtrate (**porte_filtrate**).
- L'intervallo delle porte viene suddiviso in porte basse (**low_port**) e alte (**high_port**).

3. Scansione delle porte:

Se la connessione ha **successo (stato == 0)**, viene inviata una **richiesta HTTP (HEAD / HTTP/1.0\r\n\r\n)** e si cerca di ricevere una risposta.

La risposta viene analizzata tramite la funzione "**identifica_servizio**" per determinare il servizio in esecuzione sulla porta.

Se la connessione fallisce con **codice 111**, la porta viene aggiunta alla lista delle porte chiuse. Altrimenti, viene considerata filtrata.

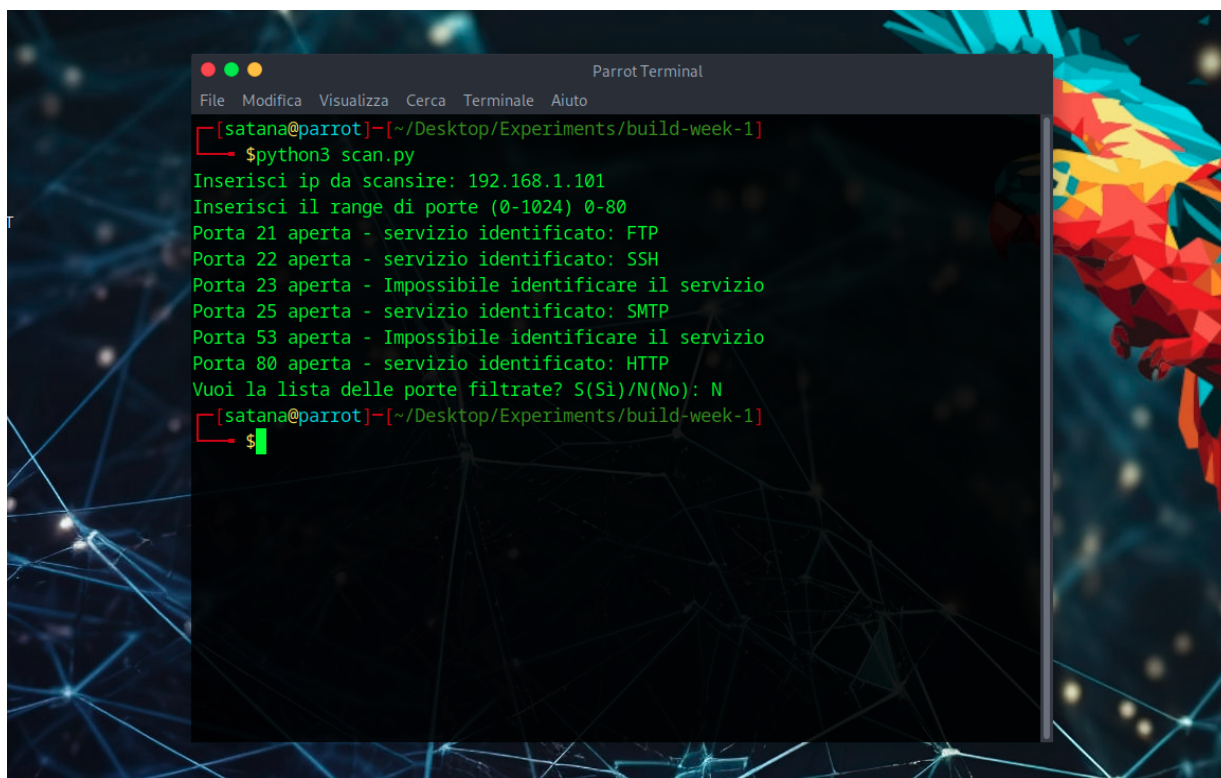
4. Visualizzazione dei risultati:

- Dopo la scansione, l'utente può scegliere se visualizzare la lista delle porte filtrate.

5. Identificazione del servizio:

- La funzione `identifica_servizio` utilizza espressioni regolari per identificare il servizio in base alla risposta ricevuta. Cerca parole chiave come **SSH, HTTP, SMTP, FTP, IMAP, POP3, Telnet e DNS** nella risposta del server. Si potrebbe implementare un sistema più complesso per l'identificazione dello specifico servizio (vedi nmap), ma ciò richiederebbe ovviamente un'analisi dettagliata di ogni protocollo supportato e del metodo di comunicazione associato.

Test e analisi



```
[satana@parrot]~/Desktop/Experiments/build-week-1
$python3 scan.py
Inserisci ip da scansire: 192.168.1.101
Inserisci il range di porte (0-1024) 0-80
Porta 21 aperta - servizio identificato: FTP
Porta 22 aperta - servizio identificato: SSH
Porta 23 aperta - Impossibile identificare il servizio
Porta 25 aperta - servizio identificato: SMTP
Porta 53 aperta - Impossibile identificare il servizio
Porta 80 aperta - servizio identificato: HTTP
Vuoi la lista delle porte filtrate? S(Si)/N(No): N
[satana@parrot]~/Desktop/Experiments/build-week-1
$
```

Dal test possiamo notare che chiede in input l'ip e il range delle porte da scansionare, scansiona le porte e rilascia le porte aperte; inoltre permette all'user di scegliere se mostrare le porte filtrate.

Conclusioni

Il codice implementa una scansione delle porte basata su socket che permette di identificare porte aperte, chiuse e filtrate su un **indirizzo IP** specificato dall'utente. Inoltre, tenta di identificare il servizio in esecuzione sulla porta aperta inviando una **richiesta HTTP** e analizzando la risposta.

Punti di forza

- **Interattività:** Richiede input dall'utente per l'indirizzo IP e l'intervallo delle porte.
- **Dettagli sui risultati:** Fornisce informazioni dettagliate su porte aperte e i servizi rilevati, e permette all'utente di vedere la lista delle porte filtrate.
- **Timeout configurabile:** Usa un timeout per evitare blocchi prolungati su una singola porta.

Contromisure e raccomandazioni

Per mettere in sicurezza il tuo sistema contro le scansioni delle porte e altre minacce, concentra gli sforzi su queste misure chiave:

1. **Firewall:** Configura per bloccare traffico non autorizzato.
 2. **IDS/IPS:** Implementa sistemi di rilevamento e prevenzione delle intrusioni.
 3. **Segmentazione della rete:** Isola le parti critiche della rete.
 4. **Servizi minimi:** Disabilita servizi e porte non necessari.
 5. **Honeypot:** Un sistema trappola che simuli un servizio appositamente vulnerabile su specifiche porte. Questo potrebbe attirare dei malintenzionati e di conseguenza fornire informazioni su intenzioni, tecniche ed eventuali obiettivi.
 6. **Aggiornamenti regolari:** Mantieni software e sistemi operativi aggiornati.
- Queste misure essenziali rafforzano significativamente la sicurezza della tua rete.

Report degli attacchi Brute Force su phpMyAdmin

Introduzione all' attacco Brute Force (attacco dizionario) su phpMyAdmin

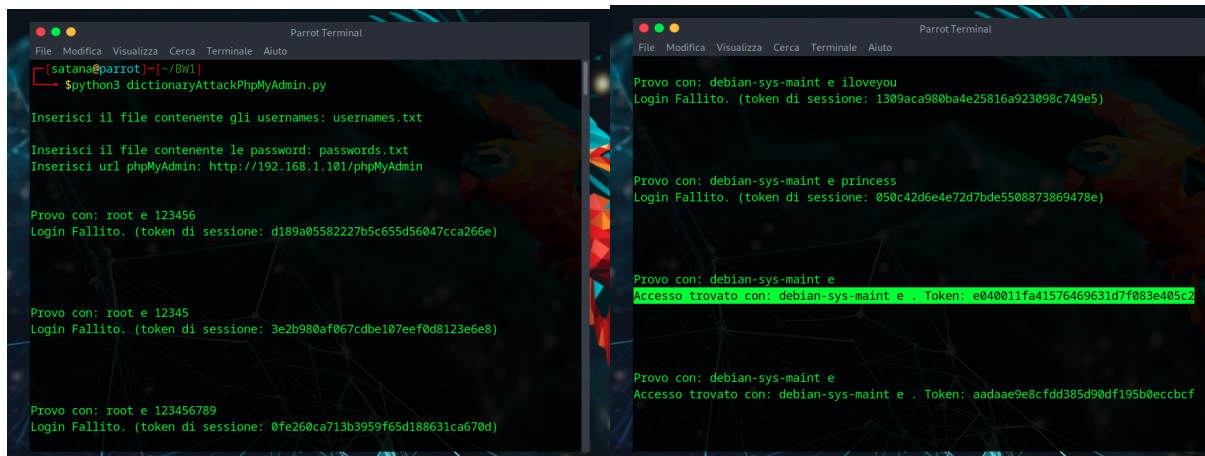
Un attacco brute force è una tecnica di hacking utilizzata per ottenere accesso a un account provando sistematicamente tutte le combinazioni possibili di username e password fino a trovare quella corretta. Questo tipo di attacco è particolarmente efficace contro account con password deboli o non complesse. Gli attacchi brute force possono essere automatizzati e accelerati utilizzando script che testano rapidamente molte combinazioni.

Metodologia utilizzata per l'attacco

Per questo attacco brute force, utilizziamo un programma Python che tenta di effettuare il login alla pagina di phpMyAdmin. Il programma utilizza i seguenti passi:

1. Inizializzazione della sessione **HTTP**.
2. Richiesta **GET** alla pagina di login per ottenere il **token CSRF**.
3. Lettura dei file contenenti gli username e le password.
4. Tentativi di login utilizzando tutte le combinazioni di username e password.
5. Verifica del successo del login.

Test e analisi



```
[satana@parrot]~/BW1
$python3 dictionaryAttackPhpMyAdmin.py

Inserisci il file contenente gli usernames: usernames.txt
Inserisci il file contenente le password: passwords.txt
Inserisci url phpMyAdmin: http://192.168.1.101/phpMyAdmin

Provo con: root e 123456
Login Fallito. (token di sessione: d189a05582227b5c655d56047cca266e)

Provo con: root e 12345
Login Fallito. (token di sessione: 3e2b980af067cdbc107eef0d8123e6e8)

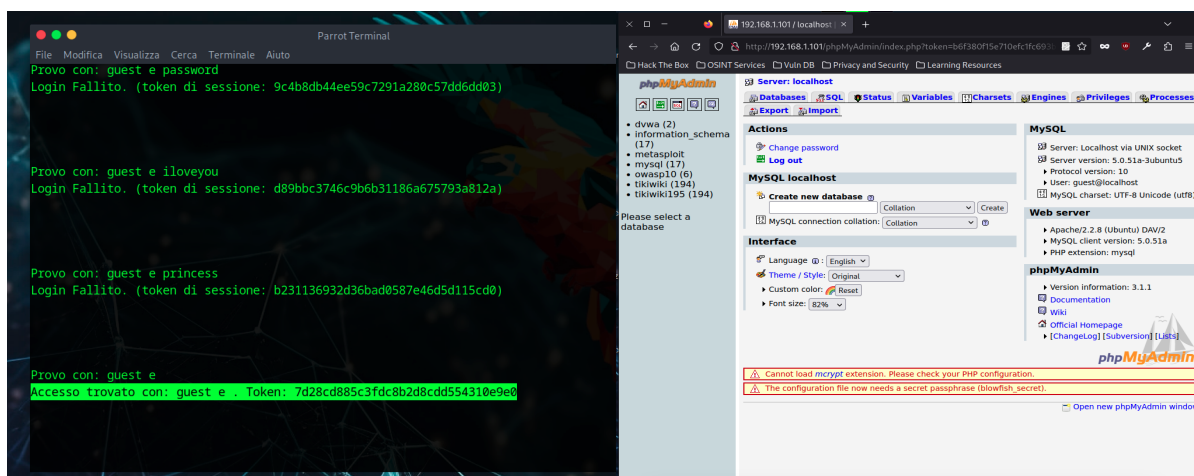
Provo con: root e 123456789
Login Fallito. (token di sessione: 0fe260ca713b3959f65d188631ca670d)

Provo con: debian-sys-maint e iloveyou
Login Fallito. (token di sessione: 1309aca980ba4e25816a923098c749e5)

Provo con: debian-sys-maint e princess
Login Fallito. (token di sessione: 050c42d6e472d7bde5508873869478e)

Provo con: debian-sys-maint e
Accesso trovato con: debian-sys-maint e . Token: e040011fa41576469631d7f083e405c2

Provo con: debian-sys-maint e
Accesso trovato con: debian-sys-maint e . Token: aadaae9e8cfd8d90df195b0eccbcf
```



```
Provo con: guest e password
Login Fallito. (token di sessione: 9c4b8db44ee59c7291a280c57dd6dd03)

Provo con: guest e iloveyou
Login Fallito. (token di sessione: d89bbc3746c9b6b31186a675793a812a)

Provo con: guest e princess
Login Fallito. (token di sessione: b231136932d36bad0587e46d5d115cd0)

Provo con: guest e
Accesso trovato con: guest e . Token: 7d28cd885c3fdc8b2d8dd54310e9e0
```

phpMyAdmin

Server: localhost

MySQL

Server: Localhost via UNIX socket

Server version: 5.0.51a-3ubuntu5

Protocol version: 10

User: guest@localhost

MySQL charset: UTF-8 Unicode (utf8)

Web server

Apache/2.2.8 (Ubuntu) DAV/2

MySQL client version: 5.0.51a

PHP extension: mysql

phpMyAdmin

Version information: 3.1.1

Documentation

Wiki

Official Homepage

ChangeLog (Subversion) [RSS]

Cannot load mcrypt extension. Please check your PHP configuration.

The configuration file now needs a secret passphrase (blowfish, secret).

Open new phpMyAdmin window

Abbiamo effettuato alcuni test in un ambiente isolato (<http://192.168.1.101/phpMyAdmin/>), al fine di testare l'efficacia del nostro script. Le prime informazioni che ci richiede lo script per poter eseguire correttamente l'attacco dizionario, sono sicuramente i due file contenenti liste di username e password, inoltre ci chiede l'URL sul quale risponde l'applicativo in questione. Fornite le corrette informazioni, comincia l'attacco individuando il token e testando ogni singola username e password contenuta nei due file specificati. Alla fine, trova le corrispondenze ed effettivamente, come attestato dal quarto screenshot, riusciamo ad accedere al pannello di phpmyadmin. Da qui in poi siamo in grado di visionare ogni database e ogni singola tabella al suo interno.

Conclusioni

Il **brute force su PHP** è un attacco in cui un aggressore tenta di accedere a un sistema web-based scritto in PHP provando un gran numero di combinazioni di nomi utente e password fino a trovare quelle corrette. Questo tipo di attacco sfrutta script automatizzati per effettuare migliaia o milioni di tentativi di accesso in un breve periodo. Se il sistema non implementa misure di sicurezza adeguate come il blocco degli account dopo ripetuti tentativi falliti o l'uso di CAPTCHA, può essere vulnerabile a questo tipo di attacco.

Contromisure e raccomandazioni

Per proteggersi dagli attacchi brute force, si raccomandano le seguenti contromisure:

- Utilizzare password complesse e uniche per ogni account.
- Implementare meccanismi di blocco dell'account dopo un certo numero di tentativi falliti.
- Utilizzare **CAPTCHA** per impedire tentativi automatizzati.
- Abilitare l'autenticazione a due fattori (**2FA**).
- Monitorare i tentativi di login e reagire agli accessi sospetti.

Report degli attacchi Brute Force su DVWA

Introduzione all'attacco Brute force su DVWA

Lo script presentato è scritto in Python e utilizza la libreria requests per effettuare tentativi di login su un sito vulnerabile, configurato tramite **Damn Vulnerable Web Application (DVWA)**. Lo scopo principale dello script è dimostrare un attacco di forza bruta per accedere al sistema utilizzando un elenco di username e password.

Struttura e Funzionamento dello Script

1. Importazione delle Librerie:

- **os:** Per operazioni sui file di sistema.
- **requests:** Per fare richieste HTTP.
- **colorama:** Per colorare l'output sulla console.

2. Configurazione e Verifica dei File di Input:

- Lo script richiede i nomi dei file contenenti gli username e le password da utilizzare nei tentativi di login.
- Verifica l'esistenza dei file e, in caso di mancato riscontro, segnala un errore e termina l'esecuzione.

3. Lettura delle Liste di Username e Password:

- Gli username e le password vengono letti dai file e memorizzati in liste.

4. Configurazione dell'Indirizzo IP e dell'URL di Login:

- L'indirizzo IP del server DVWA viene fissato a 192.168.1.101.
- Viene definito l'URL per la pagina di login di DVWA.

5. Tentativi di Login:

- Lo script avvia una sessione HTTP.
- Utilizza una combinazione di username e password per effettuare i tentativi di login.
- Verifica il successo del login controllando la presenza della stringa "Login failed" nella risposta.
- In caso di successo, interrompe i tentativi e segnala il successo.

6. Cambio del Livello di Sicurezza:

- Lo script consente all'utente di scegliere un livello di sicurezza per DVWA (low, medium, high).
- Effettua una richiesta POST per cambiare il livello di sicurezza.

7. Attacco di Forza Bruta:

- Dopo aver cambiato il livello di sicurezza, lo script tenta un attacco di forza bruta sulla pagina delle vulnerabilità specifica.

- Controlla se il login ha successo analizzando la risposta del server.



Scopo del Codice

Il codice è progettato per:

1. Automatizzare il processo di tentativi di login su una pagina di **login di DVWA**.
2. Dimostrare come un attacco brute force può essere implementato e condotto su una pagina di login web vulnerabile.
3. Evidenziare l'importanza della sicurezza delle credenziali e della protezione contro gli attacchi brute force.

Test e analisi

Durante la recente valutazione della sicurezza del sistema di autenticazione della THETA srl, utilizzando la Damn Vulnerable Web Application (DVWA), sono emerse diverse vulnerabilità agli attacchi di brute force attraverso i tre livelli di difficoltà: Base, Medio e Alto.

Livello Base: Il sistema di autenticazione al livello "Low" è risultato estremamente vulnerabile. Non sono presenti meccanismi di protezione, permettendo tentativi illimitati di accesso senza alcun blocco temporaneo o CAPTCHA. Questa configurazione facilita notevolmente l'accesso non autorizzato tramite attacchi di brute force.

```
(kali@kali)-[~/Desktop]
$ python3 brutedvwa.py
Inserisci il nome del file dell'username: username.txt
Inserisci il nome del file delle password: password.txt
Inizio dei tentativi di login all'indirizzo: http://192.168.50.101/dvwa/login.php
Tentativo con: adminn - Password
Tentativo con: adminn - Passord
Tentativo con: adminn - pasweord
Tentativo con: adminn - paertsod
Tentativo con: adminn - password
Tentativo con: Admin - Password
Tentativo con: Admin - Passord
Tentativo con: Admin - pasweord
Tentativo con: Admin - paertsod
Tentativo con: Admin - password
Login riuscito con le credenziali: Admin - password
Scegli il livello di sicurezza (low, medium, high): low
Livello di sicurezza cambiato con successo
Prova di login all'URL: http://192.168.50.101/dvwa/vulnerabilities/brute/
Tentativo di login con: adminn - Password
Tentativo di login con: adminn - Passord
Tentativo di login con: adminn - pasweord
Tentativo di login con: adminn - paertsod
Tentativo di login con: adminn - password
Tentativo di login con: Admin - Password
Tentativo di login con: Admin - Passord
Tentativo di login con: Admin - pasweord
Tentativo di login con: Admin - paertsod
Tentativo di login con: Admin - password
Login riuscito con username: Admin e password: password
```

Livello Medio: Al livello "Medium", sono stati implementati controlli di sicurezza basici. Il sistema inserisce un tempo di ritardo statico di x secondi tra un tentativo di accesso e un altro. Questo riduce, ma non elimina, il rischio di attacchi di brute force. Tuttavia, un attaccante persistente potrebbe ancora compromettere l'account con sforzi prolungati.

```
(kali@kali)-[~/Desktop]
$ python3 brutedvwa.py
Inserisci il nome del file dell'username: username.txt
Inserisci il nome del file delle password: password.txt
Inizio dei tentativi di login all'indirizzo: http://192.168.50.101/dvwa/login.php
Tentativo con: adminn - Password
Tentativo con: adminn - Passord
Tentativo con: adminn - pasweord
Tentativo con: adminn - paertsod
Tentativo con: adminn - password
Tentativo con: Admin - Password
Tentativo con: Admin - Passord
Tentativo con: Admin - pasweord
Tentativo con: Admin - paertsod
Tentativo con: Admin - password
Login riuscito con le credenziali: Admin - password
Scegli il livello di sicurezza (low, medium, high): medium
Livello di sicurezza cambiato con successo
Prova di login all'URL: http://192.168.50.101/dvwa/vulnerabilities/brute/
Tentativo di login con: adminn - Password
Tentativo di login con: adminn - Passord
Tentativo di login con: adminn - pasweord
Tentativo di login con: adminn - paertsod
Tentativo di login con: adminn - password
Tentativo di login con: Admin - Password
Tentativo di login con: Admin - Passord
Tentativo di login con: Admin - pasweord
Tentativo di login con: Admin - paertsod
Tentativo di login con: Admin - password
Login riuscito con username: Admin e password: password
```


Livello Alto: Al livello "High", la sicurezza è significativamente migliorata. Sono stati adottati meccanismi come CAPTCHA e limiti rigidi sui tentativi di accesso. Ha all'interno un Token anti CSRF che bisogna individuare ad ogni tentativo; inoltre rilascia un ritardo ad ogni tentativo fallito di login CASUALE. Queste misure rendono gli attacchi di brute force molto più complessi e dispendiosi in termini di tempo.

```
(kali@kali)-[~/Desktop]
$ python3 brutedvwa.py
Inserisci il nome del file dell'username: username.txt
Inserisci il nome del file delle password: password.txt
Inizio dei tentativi di login all'indirizzo: http://192.168.50.101/dvwa/login.php
Tentativo con: adminn - Password
Tentativo con: adminn - Passord
Tentativo con: adminn - pasweord
Tentativo con: adminn - paertsod
Tentativo con: adminn - password
Tentativo con: Admin - Password
Tentativo con: Admin - Passord
Tentativo con: Admin - pasweord
Tentativo con: Admin - paertsod
Tentativo con: Admin - password
Login riuscito con le credenziali: Admin - password
Scegli il livello di sicurezza (low, medium, high): high
Livello di sicurezza cambiato con successo
Prova di login all'URL: http://192.168.50.101/dvwa/vulnerabilities/brute/
Tentativo di login con: adminn - Password
Tentativo di login con: adminn - Passord
Tentativo di login con: adminn - pasweord
Tentativo di login con: adminn - paertsod
Tentativo di login con: adminn - password
Tentativo di login con: Admin - Password
Tentativo di login con: Admin - Passord
Tentativo di login con: Admin - pasweord
Tentativo di login con: Admin - paertsod
Tentativo di login con: Admin - password
Login riuscito con username: Admin e password: password
```

Conclusioni

DVWA (Damn Vulnerable Web Application) è un'applicazione web vulnerabile creata per testare le abilità di penetration testing. Un attacco brute force su DVWA tenta di accedere a un account utilizzando un gran numero di combinazioni di nomi utente e password fino a trovare quelle corrette. Gli attaccanti possono usare strumenti automatizzati per effettuare questi tentativi rapidamente. DVWA include livelli di sicurezza variabili, permettendo agli utenti di sperimentare diverse difese contro gli attacchi brute force, come il blocco dell'account o l'uso di CAPTCHA per prevenire accessi non autorizzati.

Contromisure e raccomandazioni

Per proteggersi dagli attacchi brute force su applicazioni come DVWA, si raccomandano le seguenti misure di sicurezza:

1. **Utilizzare password complesse:** Assicurarsi che le password siano lunghe, complesse e uniche per ogni account.
2. **Implementare il blocco degli account:** Bloccare gli account dopo un certo numero di tentativi di login falliti per impedire tentativi sistematici.
3. **Utilizzare CAPTCHA:** Implementare CAPTCHA nelle pagine di login per prevenire tentativi automatizzati.
4. **Abilitare l'autenticazione a due fattori (2FA):** Aggiungere un secondo livello di autenticazione per aumentare la sicurezza.
5. **Monitorare i tentativi di login:** Registrare e monitorare i tentativi di login sospetti e reagire prontamente a possibili attacchi.
6. **Aggiornare e configurare correttamente i sistemi di autenticazione:** Assicurarsi che il software di autenticazione sia aggiornato e configurato secondo le best practice di sicurezza.
7. **Utilizzare strumenti di sicurezza:** Implementare strumenti di sicurezza e auditing per rilevare e prevenire attacchi brute force.

Queste misure aiutano a mitigare i rischi associati agli attacchi brute force e a proteggere le applicazioni web e i dati degli utenti.

Report conclusivo dei risultati e contromisure

Analisi delle vulnerabilità riscontrate

1. **Durante l'analisi del sistema,** è stata rilevata la presenza di diverse porte aperte, inclusa la porta 80 utilizzata per il protocollo HTTP. Questa configurazione rappresenta una potenziale vulnerabilità, che potrebbe essere sfruttata da attaccanti per ottenere accesso non autorizzato alla rete.
2. **Sia sul Web Server che sull'application server** risultano abilitati i metodi GET, POST, PUT e DELETE. La presenza di questi aumenta il rischio di attacchi, poiché potrebbero essere utilizzati per manipolare i dati e compromettere l'integrità e la sicurezza del sistema.

3. **Nel corso del test di robustezza** della pagina di login, è stata riscontrata una significativa vulnerabilità agli attacchi brute force. Anche con il livello di sicurezza impostato su "alto", è stato possibile accedere al sistema.

Questi risultati evidenziano diverse vulnerabilità che rappresentano seri rischi per la sicurezza. È quindi fondamentale adottare misure correttive per proteggere i dati e le informazioni sensibili contenuti nell'infrastruttura.

Attacchi Brute Force

Gli attacchi brute force consistono nel tentativo di indovinare le credenziali della vittima provando tutte le combinazioni possibili fino a individuare quella corretta. I criminali informatici impiegano diverse strategie per incrementare l'efficacia di tali attacchi. È fondamentale che le organizzazioni comprendano le varie tipologie di attacchi brute force per implementare misure difensive adeguate.

Alcuni tipi di attacchi brute force includono:

1. **Attacchi brute force semplici:** I criminali informatici provano a determinare la password dell'utente attraverso combinazioni basate su informazioni conosciute della vittima, ottenute online o tramite tecniche di social engineering.
2. **Attacchi dizionario:** Molti attacchi brute force si avvalgono di dizionari contenenti parole, frasi e password comuni reperibili su Internet.
3. **Attacchi brute force ibridi:** Questi attacchi combinano metodi semplici con dizionari. I criminali utilizzano informazioni note della vittima insieme a parole e frasi comuni. Ad esempio, possono combinare una data di nascita con una parola del dizionario.
4. **Attacchi brute force inversi:** In questi attacchi, i criminali utilizzano una lista di password note, spesso reperite nel dark web, e le testano su una lista di possibili nomi utente fino a trovare una combinazione valida.
5. **Credential stuffing:** Gli utenti tendono spesso a riutilizzare le stesse password su diversi siti web. Di conseguenza, se i criminali ottengono le credenziali di un utente su un sito, le testeranno su altri siti per accedere ad ulteriori account della vittima.

Contromisure e raccomandazioni

Gli amministratori di rete possono adottare diverse strategie per prevenire gli attacchi brute force. Il primo passo consiste nello **stabilire regole** sulla creazione delle password che impediscano agli utenti di utilizzare password deboli. Per sistemi non critici, le password dovrebbero avere almeno 10 caratteri e includere lettere maiuscole, minuscole, caratteri speciali e numeri. Per sistemi critici, **le password dovrebbero essere composte da almeno 12 caratteri**. Con le attuali capacità computazionali, ci vorrebbero decenni per decrittare una password crittografata tramite un attacco brute force.

Ulteriori strategie di difesa includono:

1. **Utilizzo di salt:** Un salt è un insieme di bit casuali utilizzato nell'hashing delle password. L'uso di un salt riduce le probabilità di successo degli attacchi brute force, poiché i cybercriminali dovrebbero conoscere sia la password sia il valore del salt.
2. **Limitazione dei tentativi di autenticazione:** L'applicazione può limitare il numero di tentativi di accesso prima di bloccare un account o richiedere un CAPTCHA in caso di troppi tentativi falliti. Questo sistema blocca o rallenta significativamente gli attacchi brute force automatizzati, rendendoli insostenibili. Una possibile implementazione prevede il blocco degli account dopo tre tentativi di accesso falliti.

Suggerimenti di massima importanza

In quanto azienda di cybersecurity, diamo massima priorità alla formazione del personale, in quanto gli attacchi all'anello più debole della catena (l'essere umano), sono sempre in costante crescita. **Con la nascita di nuove tecniche e l'implementazione di sistemi sempre più infallibili come le AI generative, è fondamentale istruire il proprio personale** (tecnico e non). Solo attraverso una preparazione continua e una costante vigilanza possiamo mitigare efficacemente le minacce emergenti e proteggere l'integrità dei nostri sistemi e dei dati sensibili aziendali.

1. **Formazione del personale:** Sensibilizzare ed istruire periodicamente il personale riguardo la sicurezza informatica, ed incoraggiarli a gestire in modo sicuro la propria vita digitale: credenziali, accessi, uso corretto di internet in generale e dei social media, ecc... Tutto questo può aiutare a ridurre drasticamente la **superficie d'attacco**. Il primo passo è stabilire delle regole sulla creazione delle password che impediscano agli utenti di impostare password poco sicure. Come abbiamo visto durante l'audit dei servizi Theta, le password molto deboli sono fortemente soggette ad attacchi di tipo brute force o dizionario.

2. Password manager e autenticazione a due o più fattori (MFA)

Sarebbe necessario che l'azienda Theta fornisca ai propri dipendenti un **password manager**: un vero e proprio caveau digitale che consente agli utenti di archiviare, generare e gestire le proprie password che riguardano applicazioni sia locali che servizi online.

Noi suggeriamo ProtonPass per le aziende: <https://proton.me/it/business/pass>

E' altresì importante apprendere ed implementare l'autenticazione a due o più fattori per ogni account di proprietà dei dipendenti. **Grazie alla MFA**, si andranno a rinforzare tutti gli account aggiungendo un controllo di accesso aggiuntivo oltre quello della password.

E' importante far eseguire ai propri dipendenti delle politiche di sicurezza di base come fossero un mantra, per cui:

- **Le password** non vanno assolutamente generate e ricordate a memoria.
- **Evitare** l'uso di post-it, fogliettini o quaderni per annotare le password.
- **Non utilizzare** la stessa password su più di un account.
- **Abilitare** l'autenticazione a due o più fattori utilizzando un app di autenticazione che sia affidabile (Authy, Aegis, Proton... in base alle priorità aziendali). Evitare categoricamente l'utilizzo del servizio SMS, poichè è vulnerabile ad attacchi di tipo simjacking e agli attacchi Man In The Middle.

Nel contesto della formazione è altresì necessario istruire i dipendenti sulle tecniche di attacchi basati su **ingegneria sociale** (Pishing, smashing, vishing ecc...). Nonchè guidarli sull'uso corretto del web, dei social media e di internet in generale. E' fondamentale sensibilizzare sul rischio di rivelare dettagli personali online in modo non controllato, poichè questo comportamento spesso aumenta significativamente la superficie d'attacco per eventuali blackhats. In questo modo, **promuovendo una cultura digitale consapevole e responsabile**, possiamo proteggere con maggiore efficacia le risorse aziendali e ridurre le compromissioni.

3. **Blocco degli indirizzi IP sospetti:** Se vengono effettuati troppi tentativi di accesso dallo stesso indirizzo IP, il sistema può bloccare automaticamente quell'IP per un certo periodo. L'amministratore potrebbe anche aggiungere manualmente l'indirizzo IP in una blacklist.
3. **Utilizzo del protocollo HTTPS:** Assicurarsi che tutti i link interni del sito web siano convertiti da HTTP a HTTPS, evitando che diventino irraggiungibili dopo il passaggio a HTTPS. Installare il certificato SSL sull'host del sito web e configurare i reindirizzamenti 301 da HTTP a HTTPS.
4. **Aggiornamenti regolari:** Mantenere il software e tutti i componenti utilizzati sempre aggiornati.
5. **Isolamento della sala server:** Limitare l'accesso fisico alla sala server solo agli utenti autorizzati.

Costi e servizi

1. Valutazione della Sicurezza

- **Audit di Sicurezza:** Analisi completa dei sistemi, reti e applicazioni per identificare vulnerabilità e rischi. 7000€
- **Penetration Testing:** Test di penetrazione per simulare attacchi e valutare la resistenza dei sistemi. 6000€

2. Servizi di Monitoraggio e Gestione

- **Monitoraggio 24/7:** Servizi di monitoraggio continuo dei sistemi per individuare e rispondere a incidenti di sicurezza. 2.500€/mese
- **Gestione dei Log:** Raccolta, analisi e archiviazione dei log di sistema per rilevare attività sospette. 1200€/mese
- **Threat Intelligence:** Raccolta e analisi di dati sulle minacce per anticipare e prevenire attacchi. 500€/mese

3. Sicurezza della Rete

- **Firewall:** Implementazione e gestione di firewall per proteggere la rete. 6.000€ (Hardware e configurazione) + 2.500€ /anno (Licenze e manutenzione)
- **Sistemi di Rilevamento/Prevenzione delle Intrusioni (IDS/IPS):** Installazione e gestione di IDS/IPS per rilevare e prevenire intrusioni. 11.000€ (Hardware e configurazione) + 6.000€/anno (monitoraggio continuo e manutenzione)
- **VPN:** Configurazione di reti private virtuali per garantire connessioni sicure. 4.000€ + 1.000€/anno

4. Sicurezza degli Endpoint

- **Antivirus/Antimalware:** Soluzioni per proteggere dispositivi endpoint da malware e altre minacce. 3.500€
- **Gestione degli Endpoint:** Strumenti per gestire e proteggere dispositivi come laptop, smartphone e tablet. 4.800€
- **Patch Management:** Gestione e applicazione delle patch di sicurezza su tutti i dispositivi endpoint. 1.500€

5. Sicurezza delle Applicazioni

- **Web Application Firewall (WAF):** Protezione delle applicazioni web da attacchi come SQL injection e cross-site scripting. 13.000€ (Hardware, licenze WAF e configurazione) + 2.000€/anno (monitoraggio continuo)
- **Secure Development Training:** Formazione per sviluppatori su pratiche di sviluppo sicuro. 8.000€/anno

6. Formazione e Consulenza

- **Formazione sulla Sicurezza:** Programmi di formazione per dipendenti su pratiche di sicurezza informatica. 200€/dipendente 20.000€
- **Consulenza sulla Sicurezza:** Servizi di consulenza per sviluppare politiche e procedure di sicurezza. 15.000€
- **Simulazioni di Phishing:** Esecuzione di campagne di phishing simulate per valutare la consapevolezza dei dipendenti. 5.500€

7. Gestione degli Incidenti

- **Piano di Risposta agli Incidenti:** Sviluppo di un piano per rispondere a incidenti di sicurezza. 10.000€
- **Supporto in caso di Incidente:** Servizi di supporto per gestire e mitigare incidenti di sicurezza. 20.000€ + 10.000€/incidente
- **Analisi Forense:** Servizi di analisi forense per investigare e comprendere incidenti di sicurezza. 15.000€/incidente

8. Backup e Disaster Recovery

- **Soluzioni di Backup:** Implementazione e gestione di soluzioni di backup per proteggere i dati. 12.500€
- **Piano di Disaster Recovery:** Sviluppo e test di un piano di disaster recovery per garantire la continuità operativa. 20.000€ (sviluppo) + 7.000€/anno (Test e aggiornamenti)
- **Servizi di Recupero Dati:** Servizi per il recupero dei dati in caso di incidenti. 10.000€/incidente

9. Software e Strumenti di Sicurezza

- **Licenze Software:** Acquisto di licenze per software di sicurezza. 38.000€
- **Strumenti di Monitoraggio:** Acquisto e configurazione di strumenti per il monitoraggio della sicurezza. 31.000€
- **Hardware di Sicurezza:** Acquisto di hardware necessario per implementare soluzioni di sicurezza (es. appliance firewall). 40.000€