EPICODE-CS0124
Build Week 1 - Team 1
Report Finale

Indice

Riferimenti e versioni

GdL Team 1:

Responsabile/referente del documento (di seguito Responsabili): Sedici

Responsabile sezione port e method scanner: D’Esposito, Marsilio

Responsabile brute force: Germani, Mineo, Sedici

TL: Sedici

Risorse a supporto revisione (di seguito Risorse): Team 1

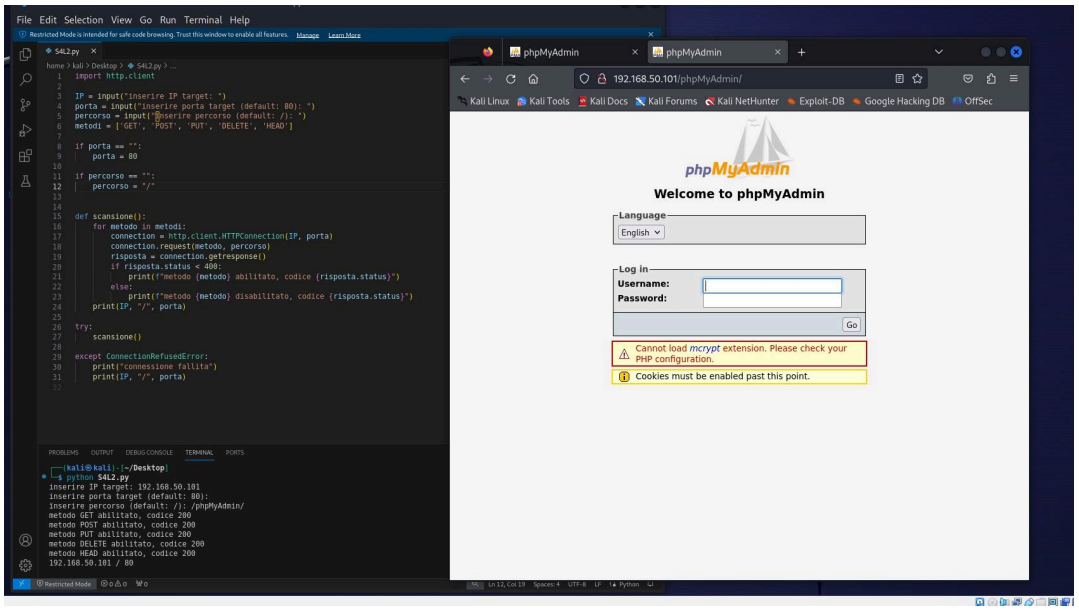
Versionamento

Versione	**Descrizione**	**Ruolo**	**Data**
1.0	Redazione documento	Responsabili	15/12/2024
1.1	Formattazione documento	TL	15/12/2024
1.2	Revisione	Team 1	16/12/2024

---

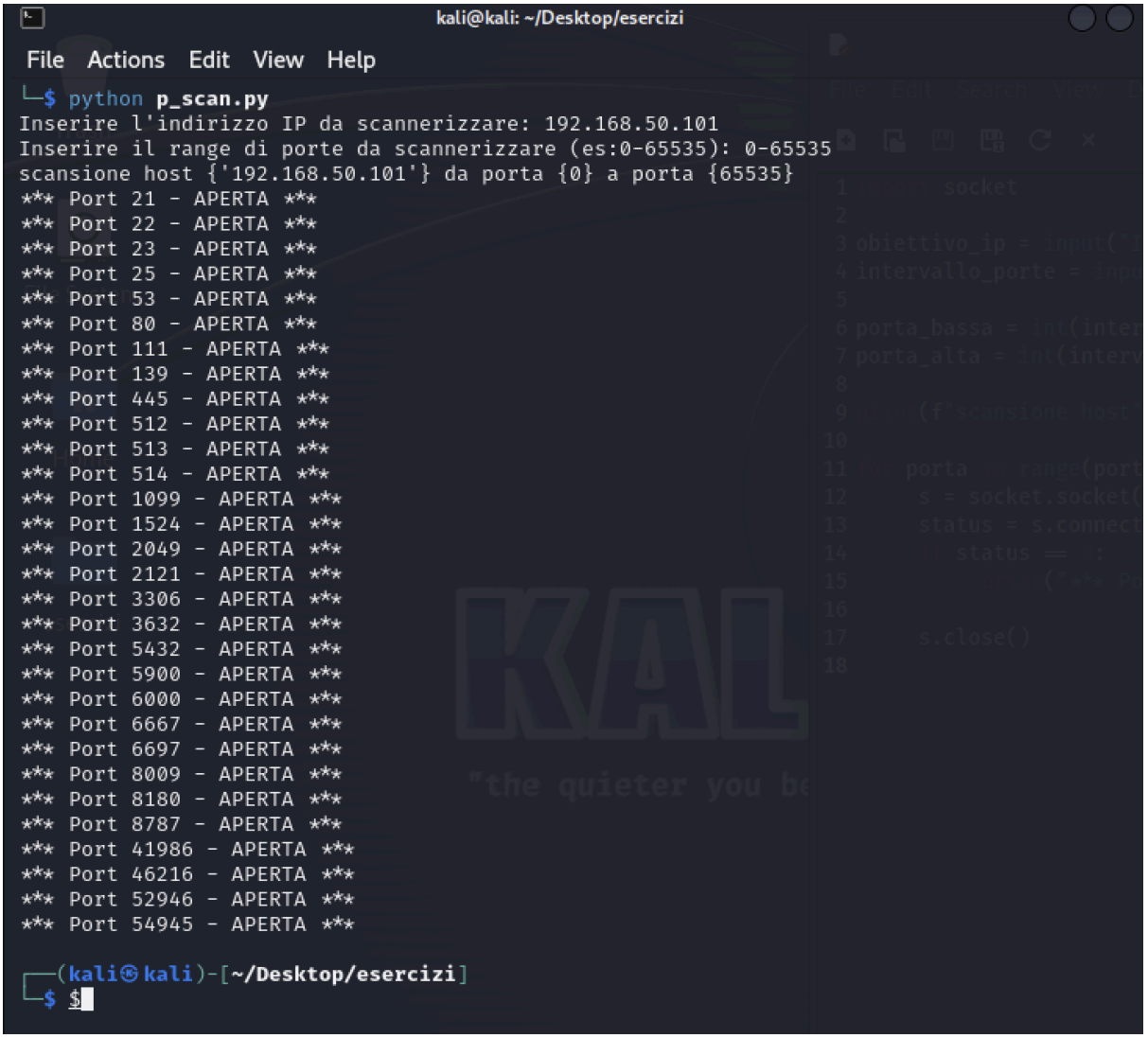
1. Method Scan

Come evidenziato nell'immagine, il team ha sviluppato un codice Python al fine di poter individuare quali metodi HTTP sono abilitati su un percorso specifico all'interno di una data porta di un indirizzo IP (socket).
Nel caso specifico, il team ha utilizzato l'applicazione sul percorso /phpMyAdmin/ dell'indirizzo 192.168.50.101 presente sul laboratorio virtuale predisposto ad effettuare il pentesting per conto della società Theta.
I risultati mostrano che il percorso sopra citato ha i permessi per tutti i metodi HTTP inseriti all'interno dell'applicazione sviluppata dal team.



2. Port Scanner

Il team ha sviluppato un programma in Python per il Port Scanning con l'obiettivo di verificare quali porte fossero aperte su un determinato indirizzo IP.
Questo strumento ci permette di fare un'analisi delle possibili vulnerabilità di rete, identificando eventuali punti di accesso non autorizzati.
Il programma effettua una scansione delle porte sull'indirizzo IP scelto dall'utente, identificando quali porte sono aperte, dando la possibilità all'utente stesso di specificare il range di porte su cui effettuare i test.
Inizialmente abbiamo sviluppato il programma in modo da scansionare quali porte TCP (Transmission Control Protocol) fossero aperte sull'indirizzo IP (192.168.50.101), da noi scelto, specificando quali porte verificare. In questo caso sono state analizzate tutte le porte (0-65535).



Come possiamo notare dalla scansione fatta sull'indirizzo IP target, il programma ha restituito i risultati che sono presenti nell'immagine.
La presenza di porte TCP aperte non è necessariamente un rischio, ci sono alcune porte TCP che è necessario che siano aperte per il funzionamento di servizi essenziali, come ad esempio la porta 80 spesso risulti aperta per consentire il traffico HTTP.
Il sistema potrebbe essere esposto a rischi di sicurezza quando risultano aperte porte non associate ad alcun servizio. È buona norma mantenere sempre aggiornati i software e fare le dovute configurazioni del Firewall.

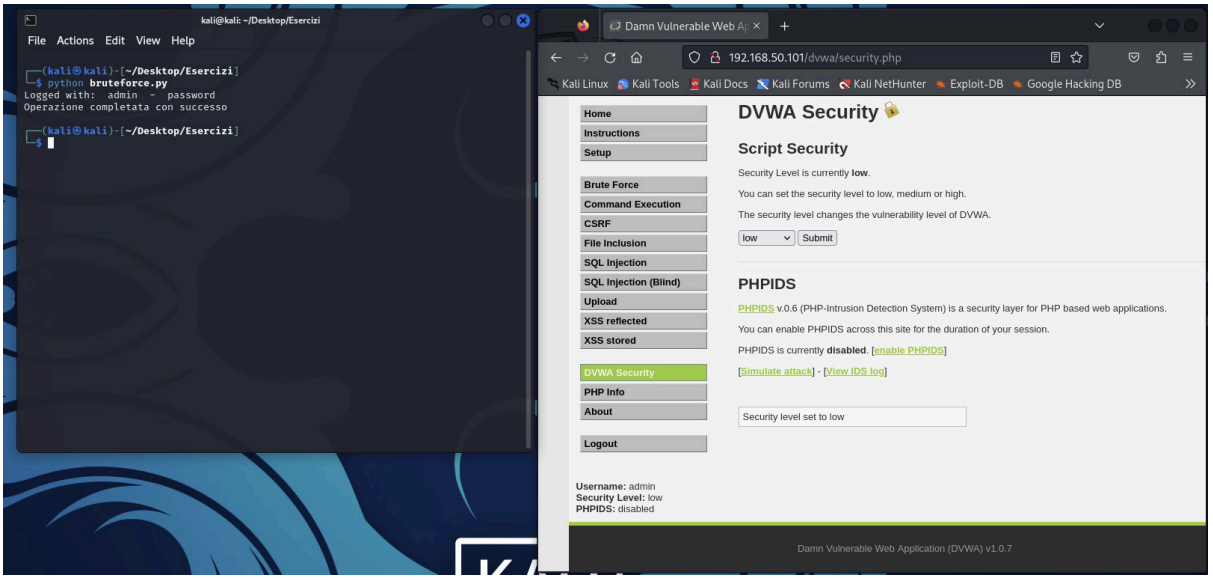
3. Attacco Brute Force DVWA login

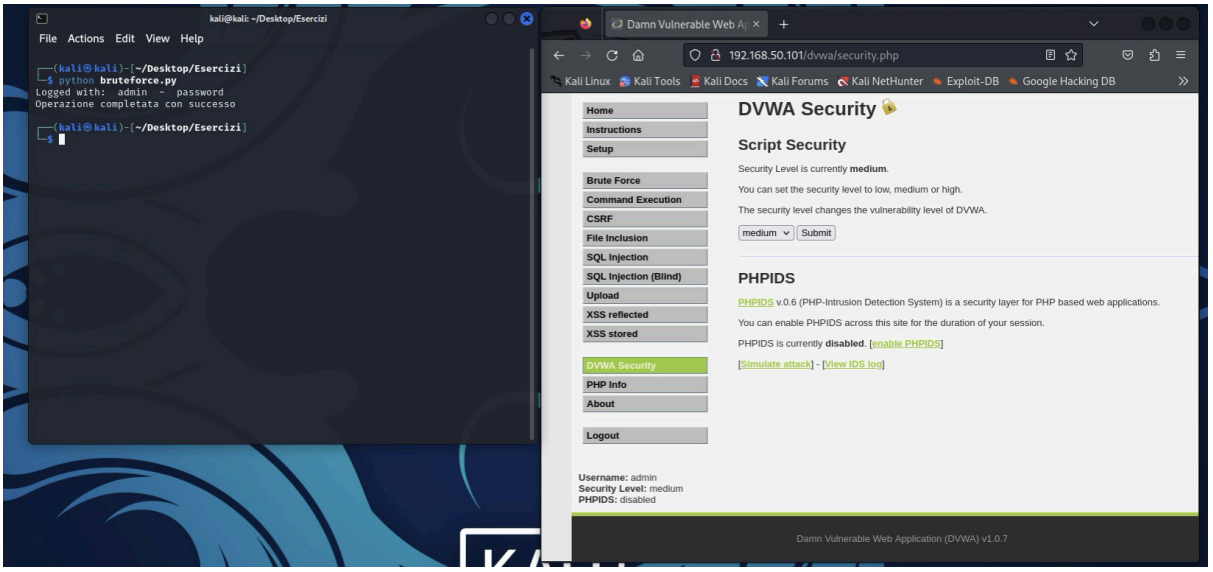
Il CISO ha esplicitamente richiesto al team di non effettuare nessun test invasivo in ambiente di produzione, e il team ha creato le due componenti nei laboratori di test, così da poter effettuare il tutto in sicurezza, separando gli ambienti di test dagli ambienti di produzione.
Dopo aver scritto il programma di attacco Brute Force in Python si iniziano i test sul server DVWA nella pagina di login. Gli attacchi Brute Force consistono nell'individuare l'username e la password, provando tutte le possibili combinazioni di lettere, caratteri speciali e numeri.

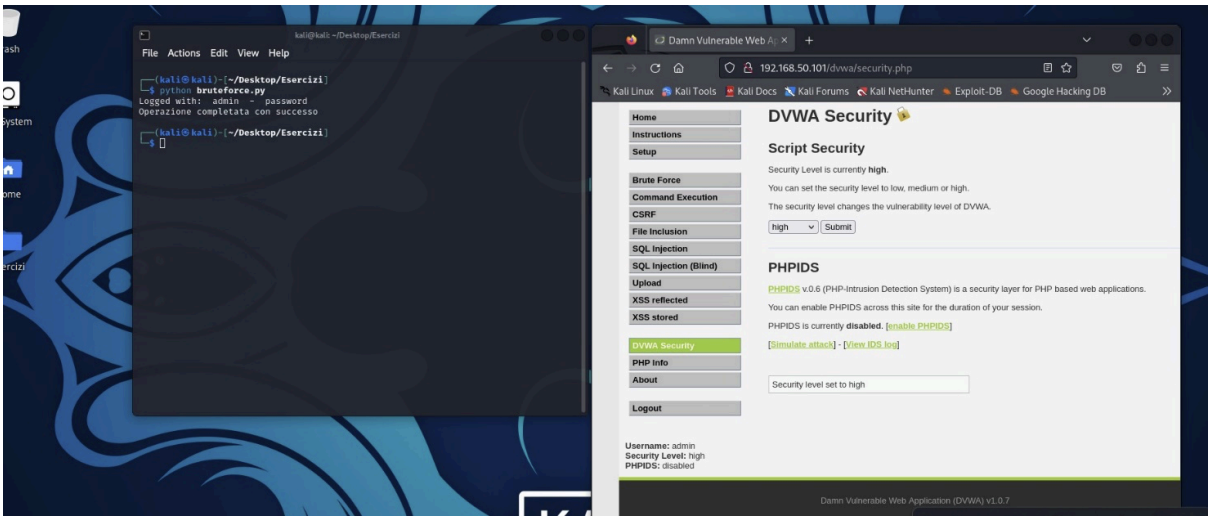
Nel Server DVWA sono presenti tre livelli di sicurezza:

- **Low** – Livello completamente vulnerabile che non possiede alcuna misura di sicurezza.
- **Medium** – Livello in cui vediamo una cattiva pratica di sicurezza, l'uso cioè di password facilmente individuabili.
- **High** – Livello in cui troviamo un mix di cattive pratiche di sicurezza.

Come si può osservare dagli screen gli attacchi brute force hanno avuto esito positivo, la differenza principale che si è potuto constatare è la diversità di tempistica nello scovare password e username. Infatti, partendo dal livello **low security** il programma in Python ha impiegato circa **5 minuti** per portare a termine l'operazione con successo.
Passando al livello **medium security** la tempistica è aumentata – circa **7 minuti.**
Per quanto riguarda il livello **high security** invece abbiamo riscontrato una tempistica di circa **11 minuti**. Queste prove sono state eseguite con dei file .txt/.lst contenenti gli username e le password più comuni (sono stati utilizzati dei dictionary provenienti da Kali Linux e anche da GitHub).
I test effettuati con il file più corposo proveniente da GitHub hanno esteso ulteriormente le tempistiche dell'attacco.







4. Attacco Brute Force DVWA - Pagina test Brute Force

Per eseguire l'attacco Brute Force (di seguito BF) sulla pagina interna di DVWA dedicata ai test, ci siamo avvalsi dell'utilizzo di WireShark, tramite il quale abbiamo monitorato i pacchetti in ingresso e in uscita e identificato le componenti del header e del payload necessarie per completare il codice Python ed eseguire l'attacco.

Quindi tramite l'utilizzo dei cookies, abbiamo effettuato una normale connessione alla pagina interna e utilizzato la stessa tipologia di codice presente nel paragrafo precedente.

L'attacco è andato a buon fine e abbiamo rilevato che, come nel caso precedente, la variazione dei livelli di sicurezza non ha portato a grandi differenze se non sui tempi di esecuzione.

5. Attacco Brute Force phpMyAdmin

Per eseguire l'attacco Brute Force (di seguito BF) sulla pagina di login phpMyAdmin, ci siamo avvalsi dell'utilizzo di WireShark, tramite il quale abbiamo monitorato i pacchetti in ingresso e in uscita e identificato le componenti del header e del payload necessarie per completare il codice Python ed eseguire l'attacco.

Quindi tramite l'utilizzo dei cookies e dei token presenti nella pagina di login, il team è riuscito ad ottenere una corretta risposta dal server e ad accedere.

L'attacco è andato a buon fine e abbiamo rilevato che, come nel caso precedente, la variazione dei livelli di sicurezza non ha portato a grandi differenze se non sui tempi di esecuzione.

6. Azioni per la mitigazione dei rischi

Al fine di ridurre al minimo i rischi legati alla rete aziendale della compagnia Theta il team ha proposto una serie di contromisure con lo scopo di proteggere i dati interni dell'azienda.

6.1. Firewall perimetrale

Il firewall è un dispositivo hardware che, agendo su diversi livelli del modello ISO/OSI, filtra i pacchetti in entrata e in uscita applicando delle regole che contribuiscono alla sicurezza della rete.
Il firewall perimetrale protegge la rete interna da minacce provenienti dall'esterno, formando un perimetro di difesa tra la rete interna e Internet. I firewall possono filtrare ciò che arriva dalla rete esterna sulla base di diversi tipi di criteri, non sempre basati sulla sicurezza informatica, possono servire a limitare gli utilizzi della rete sulla base di decisioni interne, come per esempio la censura di siti con contenuti non pertinenti l'attività lavorativa che possono distrarre il lavoratore. Il firewall divide la rete in due sottoreti: una esterna che comprende la rete non sicura (solitamente Internet), mentre l'altra, interna, comprendente una sezione più o meno grande di un insieme di computer locali. In alcuni casi, come per la compagnia Theta, si crea l'esigenza di avere una terza sottorete, detta DMZ (zona demilitarizzata), per contenere i sistemi che devono essere isolati dalla rete interna, ma che devono essere protetti dal firewall in quanto esposti sulla rete internet pubblica.
Il firewall è solo uno dei componenti di una strategia di sicurezza informatica, e non può essere considerato sufficiente per la protezione di una rete che necessita di molti accorgimenti hardware e software.

6.2. Formare il personale sulle BSP (Bad Security Practice), regolamento accessi, gestione risorse informatiche

La formazione sulle best practices da utilizzare durante il normale svolgimento dell'attività lavorativa è fondamentale per implementare la sicurezza dei sistemi. Ad oggi si calcola che circa l'85% degli attacchi informatici sia derivante da errori umani (ad esempio phishing).

Password best practices: secondo quanto consigliato anche dal GDPR, è importante seguire delle norme precise quando si imposta una password per un'utenza. Ad esempio, come suggerito dalle suddette linee guida, la password dovrebbe essere composta da:

- almeno 8 caratteri
- le vecchie password non vanno utilizzate
- non inserire informazioni personali o password contenute all'interno dei dizionari della proprio lingua
- utilizzare frasi di senso non compiuto
- deve contenere almeno un carattere minuscolo, uno maiuscolo, un numero e un carattere speciale
- utilizzare, ove possibile, la MFA (Multi Factor Authentication)

- non condividerla con altri utenti
- cambiare periodicamente la password

Su quest'ultimo punto il garante della privacy si è espresso in modo parzialmente negativo in quanto modificare le password con una eccessiva frequenza potrebbe portare l'utente ad utilizzare password troppo simili tra loro e sequenziali (come da esempio, password1, password2, etc.) che sarebbero troppo facili da individuare. Il consiglio è quello di impostare una password sufficientemente complessa e mantenere quella.

GDPR: è importante che annualmente all'interno dell'impresa venga erogata la formazione in merito alle privacy policies che vengono costantemente aggiornate, soprattutto se nell'impresa non è presente un DPO (Data protection officer) esterno. Questo consente di sensibilizzare gli utenti per un uso più consapevole della tecnologia e soprattutto sulle regole che non devono in alcun modo essere violate in merito alla diffusione di dati protetti.

Utilizzo risorse aziendali: le risorse concesse dall'azienda per il normale svolgimento dell'attività lavorativa devono essere utilizzate solo per tale scopo e non per uso personale in modo da ridurre al minimo la possibilità di violazioni. Inoltre è buona norma impostare delle politiche per la gestione del furto/smarrimento di tali risorse (cancellazione remota dei dati e criptazione del contenuto dei sistemi di archiviazione)

Utilizzo di risorse informatiche non autorizzate: è buona norma non utilizzare risorse private per accedere ai servizi aziendali, in quanto non sono controllate e potenzialmente non sicure, diventando così nuovi vettori di attacco.

Utilizzo caselle e-mail: le caselle e-mail assegnate, pur essendo protette dal GDPR e quindi non accessibili al datore di lavoro, non devono mai essere utilizzate per scopi personali, in quanto potrebbero diventare un vettore per ulteriori attacchi di phishing.

Credenziali di accesso e autorizzazioni: non devono esistere credenziali di accesso, soprattutto amministrative, che siano condivise tra più utenti. Tutte le utenze devono essere nominali o assegnate ad un solo utente, e tale assegnazione deve essere tracciata e gestita dall'amministratore dei sistemi informativi.

6.3. Tenere aggiornati i software

Le policies di aggiornamento dei software dovrebbero essere impostate sui server che gestiscono centralmente i terminali, in modo che l'utente sia obbligato ad aggiornare i sistemi operativi. In generale controllare settimanalmente gli aggiornamenti di tutti i software presenti sulle macchine dovrebbe essere una priorità dell'utente.

6.4. Installare un antivirus aziendale

Acquisire uno strumento antivirus con controllo centralizzato potrebbe essere l'opzione più sicura ed economica. Oltre a proteggere le singole macchine, consentirebbe al Team dedicato alla sicurezza informatica di monitorare eventuali comportamenti anomali sui PC che potrebbero essere ignorati dai singoli utenti.

6.5. Eseguire dei vulnerability test periodici

Nel caso di rilascio di nuovi software o componenti di grandi dimensioni all'interno dei server esistenti, sarebbe opportuno ripetere i test di vulnerabilità per verificare che tutto sia in linea con gli standard di sicurezza attualmente in essere.

6.6. Abilitare sistemi di autenticazione a due fattori (2FA)

Qualora si utilizzino servizi SaaS o altri tipi di servizi tramite internet che richiedono l'accesso con credenziali di autenticazione, è fortemente consigliato l'utilizzo di un sistema di autenticazione a 2 fattori che deve essere reso obbligatorio per le utenze amministrative.

6.7. VPN e tunnel SSH

Nel caso di smart working o di contrattualizzazione di società esterne per il monitoraggio e il controllo della rete e dei server, è fortemente consigliato l'utilizzo di VPN e/o tunnel SSH al fine di rendere più sicuro il passaggio di dati.

6.8. Certificato SSL

Risulta necessario l'acquisto di un certificato SSL da applicare al portale in modo da utilizzare il protocollo HTTPS durante le connessioni ai server, rendendo più sicura la trasmissione dei dati.

7. Conclusioni

7.1. Attacco Port Scan e Method Scan

Gli attacchi hanno rilevato la presenza di porte TCP aperte e Metodi abilitati che potrebbero non essere necessari al corretto funzionamento dei sistemi. Il team consiglia all'azienda di revisionare le porte e i metodi emersi dalla presente analisi per assicurarsi che abbiano una reale utilità. In caso contrario si consiglia di chiudere/disabilitare i canali non necessari (anche tramite firewall) per ridurre al minimo i vettori di attacco.

7.2. Attacco Brute Force

Gli attacchi Brute Force non hanno rilevato particolari vulnerabilità utilizzando i dictionary standard.
L'unica eccezione è stata l'individuazione di una utenza amministrativa con una password debole.
L'errore da correggere è quindi duplice:

- come precedentemente riportato, è fondamentale che non esista un utenza amministrativa generica che non sia correttamente assegnata ad un utente. Se ne consiglia la disabilitazione.
- la password debole utilizzata non dovrebbe essere consentita dal sistema in fase di immissione della coppia utente-password.

Si consiglia infine di seguire le best practices descritte nei paragrafi precedenti.

Inoltre si consiglia di inserire in ogni pagina di login un sistema che impedisca ad un utente di inserire username e password senza controllo, ossia che dopo un numero di inserimenti errati, blocchi l'accesso per un tempo ragionevole o blocchi definitivamente l'utenza che dovrà essere ripristinata dagli amministratori di sistema.

Questo processo di mitigazione, renderebbe l'attacco Brute Force eccessivamente dispendioso per gli attaccanti indipendentemente dalla potenza delle macchine utilizzate durante l'attacco stesso, aumentando contestualmente il rapporto costi/benefici.

Infine si consiglia di aggiungere ulteriori livelli di sicurezza, come appunto il MFA, in modo da vanificare o almeno rendere più complesso un attacco Brute Force.