

REPORT BRUTEFORCE WEB SERVER

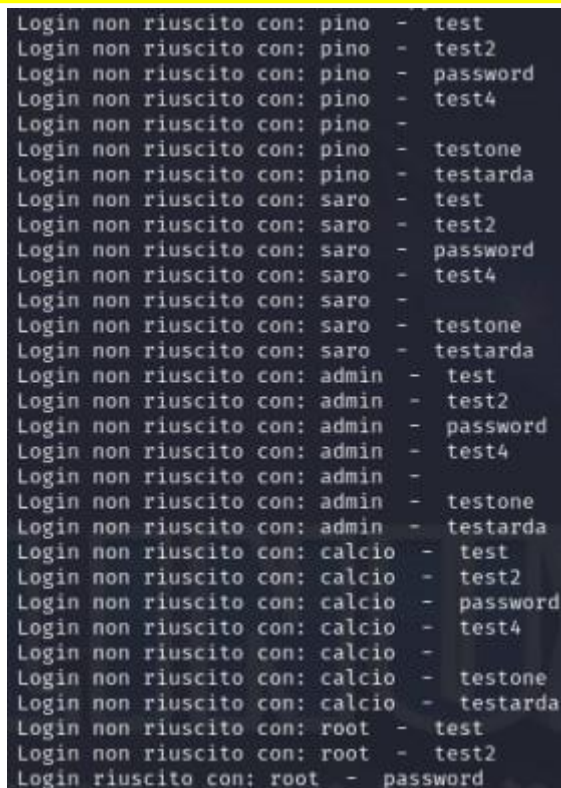
Gentile CISO di **Theta**,

In data 20/12/2023, come da voi richiesto, abbiamo effettuato una simulazione attacco bruteforce a dizionario per testare il login del web server, il tutto fatto in un ambiente simulativo.

L'esito della simulazione ha dato risultato "**negativo**".

Con il presente report le elenchiamo le criticità riscontrate e una serie di precauzioni per evitare che ciò avvenga in un contesto reale.

In primis le alleghiamo uno screenshot in cui può notare l'esito della simulazione d'attacco che ha portato all'exploit delle credenziali di accesso:



```
Login non riuscito con: pino - test
Login non riuscito con: pino - test2
Login non riuscito con: pino - password
Login non riuscito con: pino - test4
Login non riuscito con: pino - 
Login non riuscito con: pino - testone
Login non riuscito con: pino - testarda
Login non riuscito con: saro - test
Login non riuscito con: saro - test2
Login non riuscito con: saro - password
Login non riuscito con: saro - test4
Login non riuscito con: saro - 
Login non riuscito con: saro - testone
Login non riuscito con: saro - testarda
Login non riuscito con: admin - test
Login non riuscito con: admin - test2
Login non riuscito con: admin - password
Login non riuscito con: admin - test4
Login non riuscito con: admin - 
Login non riuscito con: admin - testone
Login non riuscito con: admin - testarda
Login non riuscito con: calcio - test
Login non riuscito con: calcio - test2
Login non riuscito con: calcio - password
Login non riuscito con: calcio - test4
Login non riuscito con: calcio - 
Login non riuscito con: calcio - testone
Login non riuscito con: calcio - testarda
Login non riuscito con: root - test
Login non riuscito con: root - test2
Login riuscito con: root - password
```

Criticità

- Eccessiva banalità delle credenziali utilizzate, esse infatti possono essere trovate nella maggior parte dei file di testo utilizzati per i bruteforce.
- La possibilità di eseguire infiniti tentativi di login, facilita notevolmente gli attacchi bruteforce.
- La facilità di recuperare il token nel codice html, che viene utilizzato per fare una richiesta di login.

Ottima la scelta della pagina di transizione tra il login e il pannello di controllo, rende l'attacco più complicato.

Consigli Login

1. Sugeriamo di scegliere una password composta da almeno 12 caratteri:
 - Caratteri alfanumerici, combinando maiuscole e minuscole
 - Caratteri speciali.Evitando parole di uso comune o informazioni personali come date di nascita, si consiglia inoltre di stabilire una policy di cambio password ogni 6 mesi
2. Come secondo consiglio suggeriamo di utilizzare un'autenticazione a due fattori per esempio un dispositivo che genera un codice temporaneo utilizzabile una sola volta, oppure un riconoscimento biometrico:
 - Impronte digitali
 - Il riconoscimento facciale.O ancora usare la posizione da cui si effettua il login (ad esempio se si effettua il login da un dispositivo diverso dal solito)
3. Si consiglia inoltre di introdurre un blocco dell'account dopo un determinato numero di tentativi dopo il quale sarà necessario l'intervento di un responsabile della sicurezza per sbloccarlo

Consigli Sicurezza Lato Server

1. Sarebbe opportuno bloccare le richieste ICMP per impedire ad un attaccante di scansionare la rete, questo ci protegge anche da determinati tipi di attacchi come il DDos.
2. E' consigliabile memorizzare la password nel database in forma criptata e non in chiaro.
3. Fare un audit delle porte per chiudere quelle non utilizzate in azienda riducendo la superficie dei possibili attacchi.
4. Si consiglia di cambiare i servizi delle porte standard (esempio : servizio ftp dalla porta 21 alla 2320)

Report Attacco E-Commerce Server

In data 21/12/2023 abbiamo invece eseguito dei test sul vostro server E-Commerce interno. Anche in questo caso l'esito è stato negativo. Come fatto per il precedente test le elenchiamo le criticità che abbiamo riscontrato. Le alleghiamo nuovamente uno screenshot in cui viene mostrata la vulnerabilità delle credenziali.

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

CRITICITA'

- Come in precedenza le credenziali utilizzate soffrono di un'eccessiva banalità, infatti "admin" e "password" si trovano comunemente in molte liste di credenziali
- Nessun sistema di sicurezza che rileva molteplici tentativi di login a breve distanza l'uno dall'altro

Ottima scelta lo script che fa passare un determinato numero di secondi fra un tentativo di accesso e l'altro, rallentando quindi l'attaccante.

Miglioramenti

1. Aumentiamo il numero minimo suggerito di caratteri per la password da 12 a 14 includendo un minimo di 3 caratteri speciali oltre a numeri e lettere.
2. Cambiare i metodi di autenticazione in due fattori usando:
 - Un Token fisico generatore di codici
 - Un' Autenticazione tramite app
3. Anche qui si consiglia il blocco dell'account dopo un determinato numero di tentativi sbagliati.