

# Vulnerability Assessment

## Servizio DVMA

**Test eseguito:** Brute Force.

**Obbiettivo del test:** individuare la robustezza delle password che permette di accedere ai sistemi informatici, provando le combinazioni possibili da una lista di username e password più comuni.

### Potenziati Rischi:

Nonostante il numero elevato di combinazione possibili, la velocità di esecuzione dei moderni software e la facile reperibilità di informazioni relative alle credenziali più utilizzate permetterebbe facilmente a un qualunque mal intenzionato di tentare un attacco. Se un attaccante dovesse entrare nel sistema, potrebbe causare danni ingenti alle attività aziendali.

### Metodo:

È stato scritto un programma in python che tenta di effettuare un login tramite varie combinazioni di username e password. Questi dati sono presi da due file contenenti migliaia di password e username ritenuti tra le più comunemente utilizzate.

### Esecuzione del test:

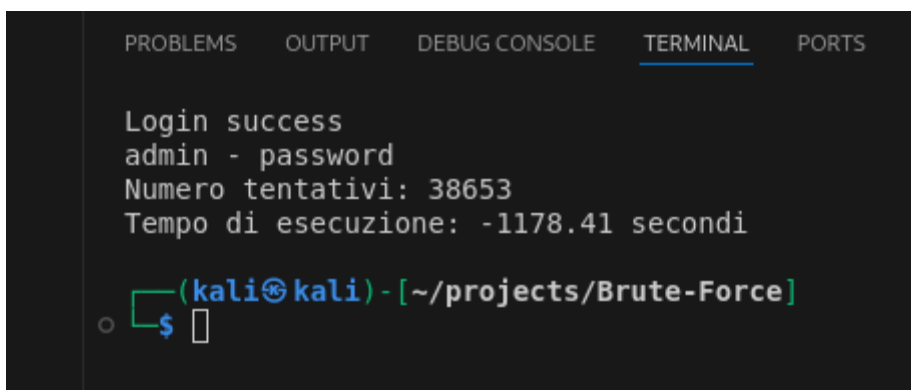
Al software sono stati forniti due file contenenti rispettivamente una lista di username e una di password.

Test:

Username:	403355
Password:	38651
Combinazioni possibili:	15.590.074.105

### Risultati:

Le credenziali sono state trovate **in meno di 20 minuti** con 38653 tentativi.



```
PROBLEMS  OUTPUT  DEBUG CONSOLE  TERMINAL  PORTS

Login success
admin - password
Numero tentativi: 38653
Tempo di esecuzione: -1178.41 secondi

(kali@kali) - [~/projects/Brute-Force]
$
```

Il risultato ottenuto è soggetto a variazioni che dipendono da vari fattori come il numero di macchine coinvolte, la loro potenza e i dati che dispongono. Questo vuol dire che potenzialmente il sistema potrebbe essere penetrato anche in un tempo inferiore a quello ottenuto.

**Valutazione del rischio:**

Considerando la debolezza delle credenziali, la facilità di accesso alle risorse per eseguire questo tipo di attacco e, soprattutto, i potenziali danni, consideriamo che questa vulnerabilità deve essere classificata come **CRITICA**.

**Soluzioni:**

Si consiglia le seguenti misure di sicurezza:

- Modifica quanto meno la password rispettando le seguenti norme:
  1. Lunghezza della password, almeno 8 caratteri;
  2. Complessità della password, almeno una lettera maiuscola, un numero, un simbolo;
  3. Evitare password standard come Password1!, oppure caratteri ripetuti;
  4. Cambio password periodico, ogni 3 mesi per esempio;
- Considerare la possibilità di implementare una verifica multifattoriale;
- Limitare il numero di tentativi di accesso eseguibili per un determinato utente;
- Eliminare risposte superflue da parte del web server come, ad esempio, "Login Failed"