Day 11 – Brute Force Attack

Brute Force Attack

Cos'è un Attacco Brute Force?

Un **attacco Brute Force** è una tecnica in cui un hacker tenta di ottenere l'accesso a un sistema provando tutte le combinazioni possibili di password o chiavi di crittografia. Questo metodo si basa sulla forza bruta, senza l'uso di sofisticati strumenti di hacking, e può essere efficace contro password semplici o corte. Sebbene richieda tempo e risorse, può essere automatizzato, rendendolo una minaccia concreta, soprattutto per account con password deboli o riutilizzate.

Brute Force Attack

Tipi di Attacchi Brute Force

L'attacco **Brute Force Semplice** consiste nel provare ogni combinazione possibile di caratteri (lettere, numeri e simboli) fino a trovare la password corretta. Questo metodo è molto lento, ma garantisce risultati per password corte, mentre il tempo necessario aumenta esponenzialmente con la lunghezza della password.
L'**attacco a Dizionario** sfrutta una lista predefinita di parole comuni, come "password" o "123456", per tentare di indovinare la password. È più rapido dell'attacco semplice, ma si basa sull'uso di password deboli.
I **Credential Dumps** utilizzano credenziali rubate da precedenti violazioni di sicurezza. Questo metodo è efficace se l'utente ha riutilizzato le stesse credenziali in più account.
Infine, il **Credential Stuffing** automatizza il tentativo di utilizzare credenziali trapelate su vari siti web. È un metodo veloce e sfrutta la tendenza degli utenti a riutilizzare le password su più piattaforme.

Brute Force Attack

Come Proteggersi dagli Attacchi Brute Force

•**Utilizza password lunghe o passphrase**: Crea password complesse e difficili da indovinare, preferibilmente usando una combinazione di caratteri, numeri e simboli.

•**Autenticazione a più fattori (MFA)**: Aggiungi un secondo livello di protezione richiedendo un codice univoco generato da un'app o inviato via SMS oltre alla password.

•**Sii vigile!**: Evita phishing o email sospette che ti chiedono di accedere o cambiare password. Verifica sempre la fonte prima di eseguire azioni sensibili.

Per le organizzazioni, è fondamentale tenere presente che:
Bisogna controllare le **superfici d'attacco**, cioè: identificare e limitare quali asset e servizi devono essere esposti pubblicamente (es. SSH, HTTP). Verificare se devono essere esposti o possono essere limitati.

Brute Force Attack

Strumenti Utilizzati per eseguire degli attacchi Brute Force

•**Hydra**: Strumento di cracking password estremamente veloce che supporta molteplici protocolli di rete come SSH, FTP, HTTP.

•**John the Ripper**: Popolare software di cracking password progettato per rilevare password deboli, spesso utilizzato per test di sicurezza.

•**Hashcat**: Potente software di recupero password in grado di sfruttare la potenza delle GPU per attacchi brute force e altri metodi di cracking.