Bruteforce Attacks

Brute force attacks are a type of cyber attack where an attacker attempts to gain unauthorized access to a system or application by systematically trying all possible combinations of credentials, such as usernames and passwords. This method relies on sheer computational power and persistence to eventually guess the correct credentials.

In simpler terms -

Imagine you have a locked door, and the only way to open it is by entering the correct combination code. A brute force attack is like having someone stand in front of that door and try every possible combination of numbers, one by one, until they eventually stumble upon the right code that unlocks the door.

The hacker uses a program or script that automates this process of guessing and trying different username/password combinations rapidly. It systematically goes through common passwords, dictionary words, dates, names, and every other possible character combination until it finds the correct login credentials.

Types of Bruteforce attacks

There are mainly 4 types of bruteforce attacks:

- **Simple Bruteforce Attack** - Simple Bruteforce attack is where we as a hacker try all possible combination to get the password right.

Suppose, the password is 1234. So in a typical bruteforce attack where we only know that the password can be number. We will try all possible combinations. Like 1,2,34, and so on and when we will reach the number one thousand two hundred and thirty four or we can say 1234, then we will get a successful hit.

So, bruteforce attack do work but are time consuming and need a not of computational power.

- **Dictionary attacks** - In this type of attack, we simply give a wordlist containing dictionary words like apple, password, monkey etc to our bruteforce program and try to get access with it. The idea behind is that people usually use simple, easy to remember dictionary words as their password. So, there is a high chance of us getting into their account with dictionary type attack. One more thing to note is that, this attack is very fast as compared to a bruteforce attack if you a decent computer.

- **Hybrid attacks** - Hybrid attacks mixes properties of dictionary attack and bruteforce attack by mutating the wordlist. It uses permutation and combination of different words with different symbols to generate a focused wordlist.

Lets say we have a password in our dictionary based wordlist file that is - Summer. Now in Hybrid attack we just uses different combination with the word, like we add the current year to it Summer2024. Now this is a new password, like this there could a number of combination we can make for each password.

- **Credential Stuffing** - Credential Stuffing is basically using the breached usernames and password combinations to access accounts on different services and application in the hope that the target has not changed his password or he/she is reusing the same password on every platform.

Now lets see the practical demonstration of a bruteforce attack. But before that, one thing to note here is that there are two types of password attacks - online and offline.

The type of password attack we are discussing here is online, where we have to generally interact with a login panel or prompt. There is a offline cracking of passwords also where we cracked the hashed password into the plain text ones But that is not the part of this module.

Okay! So Now, we have a mission to get in to our metasploitable machine via SSH and steal the nuclear code secret from it.

I have changed my root password from the default one to a custom one which i like, as learned from the previous section about the risks of default password.

So, now what can i do ?

I can use the number one tool for online password attack that is Hydra.

```
hydra -l root -P wordlist.txt ssh://IP
```

Attacking HTTP POST Login Form with Hydra

1. Capture the POST request via Burpsuite.
2. Also check the failed login attempt string.
3. Perform bruteforce using hydra.

```
hydra -l molly -P wordlist.txt 10.10.135.55 http-post-form
"/login:username=^USER^&password=^PASS^:Your username or password is
incorrect." -V
```

- Performing bruteforcing HTTP basic authentication (HTTP-GET).

```
hydra -l admin -P ~/Desktop/Wordlist/rockyou.txt 192.168.247.201 http-get
/
```

Now that we have learned, how we can perform online password attacks with Hydra. Lets address some facts about password and bruteforce attacks in real life.

While brute forcing is an effective technique against weak or easily-guessable passwords. But it might not work against longer and not commonly used passwords. The longer and more complex the password, the harder it becomes for the attack to succeed in a reasonable time.

Let me show you what i am talking about.

https://www.proxynova.com/tools/brute-force-calculator/ -> mypasswordisstrong

https://www.passwordmonster.com/ -> Igotsomeveggiesfor100$

These considerations were for the offline bruteforce attacks. Now lets talk about the challenges we face in online ones.

- **Account Lockouts**: Many websites will lock an account after too many failed login attempts. This prevents us from endlessly guessing passwords for that account.
- **Speed Bumps**: Websites may intentionally add delays or rate limits after each failed login attempt to slow down brute force attacks.
- **CAPTCHAs**: Those annoying puzzles you have to solve are designed to prevent automated bots from rapidly trying password combinations.
- **Multi-Factor Authentication**: Even if the password is guessed correctly, We would still need to bypass additional verification steps like one-time codes sent to target's phone.
- **IP Blocking**: If a website detects too many failed login attempts from the same IP address, it may block that IP to stop the attack.
- **Monitoring and Detection**: Advanced security systems can identify patterns of suspicious behaviour and take countermeasures against potential brute force attacks.
- **Computational Power**: As passwords get longer and more complex, the number of possible combinations increases exponentially, requiring immense computing resources for the attack to succeed in a reasonable time.
