Credential Stuffing & Password Spraying

Credential stuffing and password spraying are two related but distinct techniques used by attackers to gain unauthorized access to accounts and systems by exploiting weak or reused passwords.

Lets look into Credential Stuffing first:

Credential Stuffing

Credential stuffing is a type of brute force attack that involves using lists of stolen or leaked username and password combinations to attempt to gain access to other accounts or systems.

Here's how it works:

- Attackers obtain large databases of usernames and passwords from previous data breaches or leaks.
- They use automated tools to try these credential combinations across various websites, applications, or services.
- If a username and password combination is valid on a particular platform, the attacker gains access to that account.

Credential stuffing attacks rely on the fact that many users reuse the same passwords across multiple accounts, making it possible to exploit a single compromised credential on multiple platforms.

Lets consider a real life scenario where this could happen. So, suppose we found leaked creds for uber.com online. Now, if these are the internal employee accounts rather than customer data, then we can use them in products like office 365.

So, if you don't know, most of the organizations uses Micrsoft Office 365 suite for their businesses. So, we get one successful hit from outside using the breached creds then we hit a easy goldmine of information as now we can use that internal account to access the whole network of the company, or send phishing emails on behalf of the user, the exploitation possibilities will be endless then.

Password Spraying

Password spraying is a type of brute force attack where an attacker attempts to access a large number of accounts by using a few commonly used passwords

Here's how it works:

- The attacker gets a list of usernames, like employee email addresses from a company website or leaked data.
- They choose a few very common, easy-to-guess passwords that many people use, like **"password123"** or **"123456"**.
- Then Using automated tools, the hacker systematically tries those same few passwords against each username in the list, one by one.
- If any of the accounts happen to be using one of those common passwords, the attacker can gain unauthorized access to those accounts.

The key difference from a regular brute force attack is that password spraying uses a small number of passwords across many accounts, rather than trying many passwords on a single account. This helps avoid triggering account lockouts that happen after too many failed login attempts on one account.

Password spraying works because many people still use very weak, easily guessable passwords, and often reuse the same password across multiple accounts. So if one of those common passwords is used on multiple accounts, the attacker can gain access to all of them.

One common example of Password Spraying can be on Office 365 suite again and in the internal network connected with Active Directory. I will not discuss active directory attacks as of now but lets try try password spray on the Xiaomi portal that we used before.

So that was something that we done manually with Burpsuite. What if we want to attack the real accounts that are using Office 365. Then, we can use a tool called TrevorSpray.

https://github.com/blacklanternsecurity/TREVORspray

Trevorspray uses a email list and perform password spray to the Microsoft Office 365 Oauth endpoint. But the thing to note here is that in real engagements, Microsoft will definetly block your IP address after certain no. of attempts. So, you gotta use a lot of proxies, so that each request comes from a different IP address. For now, lets see how we can use trevorspray.

```
trevorspray -u ~/Desktop/usernames.txt -p 'Password123' --url
https://login.windows.net/b439d764-cafe-babe-ac05-
2e37deadbeef/oauth2/token
```