Bypassing the Rate Limiting

using IP Rotation in Brute forcing

AGENDA

- What is IP Rotation
- How to Set Up IP rotation
- Demo
- Mitigation

What is IP Rotation ?

IP address rotation is a process where assigned IP addresses are distributed to a device at random or at scheduled intervals by an administrator or IP address rotation software.

How to Set UP IP Rotation ?

There are many IP ROTATION Services available in online for free tier and paid.

Paid   - Luminati , Oxylabs , Smart Proxy .

Free   - Burpsuite with IP Rotator Plugin .

Reference :

Bypassing IP Based Blocking with AWS API Gateway

How to Rotate IP ADDRESS in Brute Force Attack

Mitigations

- The Web Application should implement CAPTCHAS in the OTP generation fields, form submission , generation of email field which will stop the DOS attack.
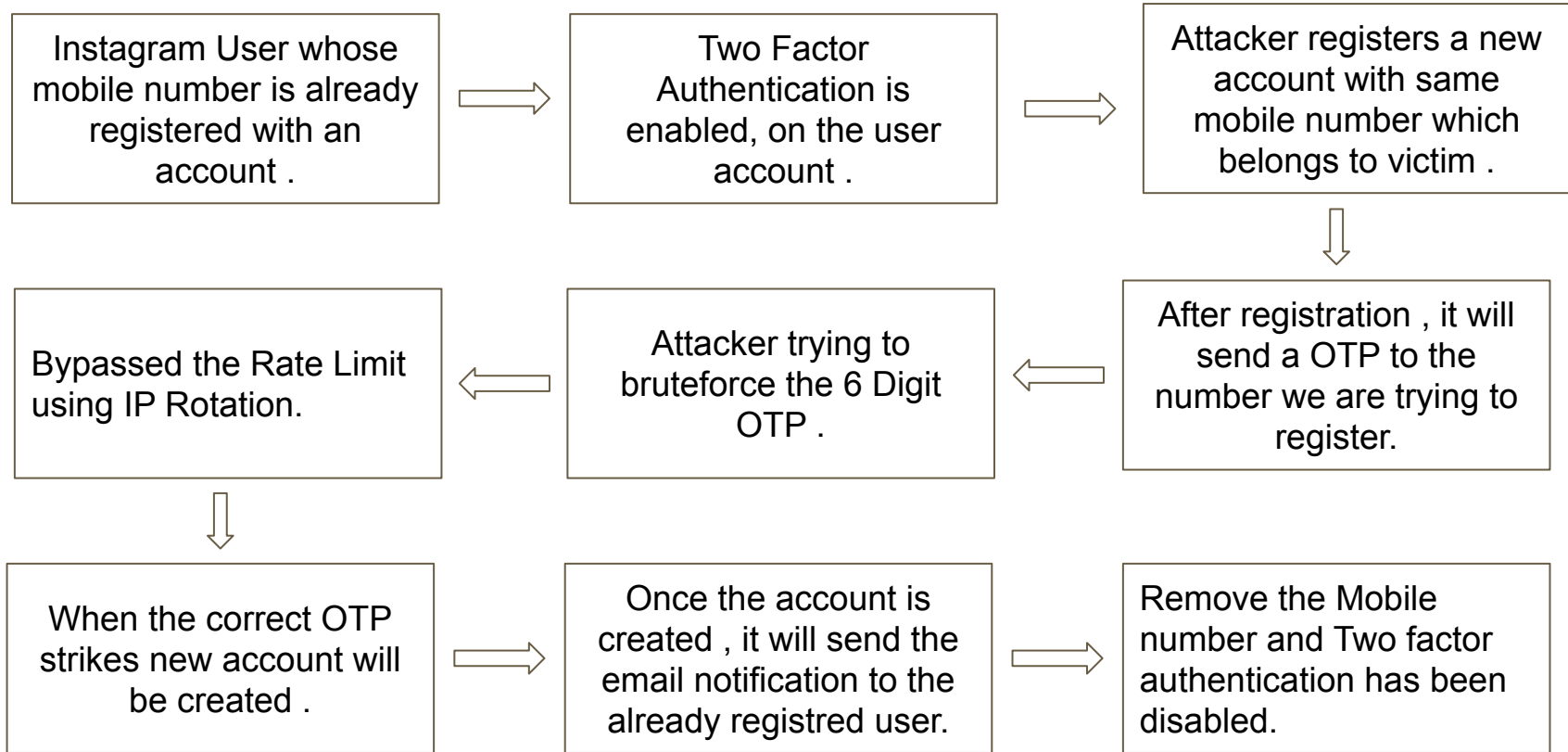
- If the attack is using an open proxy to bypass the rate limit , the open proxy Ip address should be blocked.

```
┌─────────────────────────┐      ┌─────────────────────────┐      ┌─────────────────────────┐
│  Instagram User whose   │      │     Two Factor          │      │ Attacker registers a new│
│ mobile number is already│ ──▷  │  Authentication is      │ ──▷  │   account with same     │
│   registered with an    │      │  enabled, on the user   │      │  mobile number which    │
│       account .         │      │     account .           │      │  belongs to victim .    │
└─────────────────────────┘      └─────────────────────────┘      └─────────────────────────┘
                                                                               │
                                                                               ▽
┌─────────────────────────┐      ┌─────────────────────────┐      ┌─────────────────────────┐
│                         │      │   Attacker trying to    │      │ After registration , it │
│ Bypassed the Rate Limit │ ◁──  │  bruteforce the 6 Digit │ ◁──  │  will send a OTP to the │
│   using IP Rotation.    │      │       OTP .             │      │  number we are trying to│
│                         │      │                         │      │       register.         │
└─────────────────────────┘      └─────────────────────────┘      └─────────────────────────┘
           │
           ▽
┌─────────────────────────┐      ┌─────────────────────────┐      ┌─────────────────────────┐
│  When the correct OTP   │      │   Once the account is   │      │ Remove the Mobile       │
│ strikes new account will│ ──▷  │  created , it will send │ ──▷  │ number and Two factor   │
│     be created .        │      │  the email notification │      │ authentication has been │
│                         │      │ to the already registred│      │ disabled.               │
│                         │      │       user.             │      │                         │
└─────────────────────────┘      └─────────────────────────┘      └─────────────────────────┘
```

Reference

- [How I was able to remove your Instagram Phone number](#)

- [How I Could Have Hacked Any Instagram Account](#)

- [How I Hacked Instagram Again](#)