MULTITHREAD, PROXY, BATCH, AND IMAGE-CLASSIFY: A MULTI-FEATURED APPROACH TO CRACK HTTP AUTHENTICATION

Duy (Dave) Nguyen, Kaung Thant (John) Win

Objective

Crack an HTTP authentication system by maximizing password spraying & CAPTCHA cracking speeds while avoiding getting blocked by the server.

Terminology

Password Spraying: A type of brute-force attack where a fixed set of passwords is brute-forced against a larger set of usernames.

Proxy: An intermediary server that forwards client requests and changes the client's IP address with the proxy server's.

EC2: A virtual server hosted on the Amazon Web Services (AWS).

Rate Limit: The number of allowed requests to the server per second.

Botnet: A collection of machines controlled by a single remote machine.

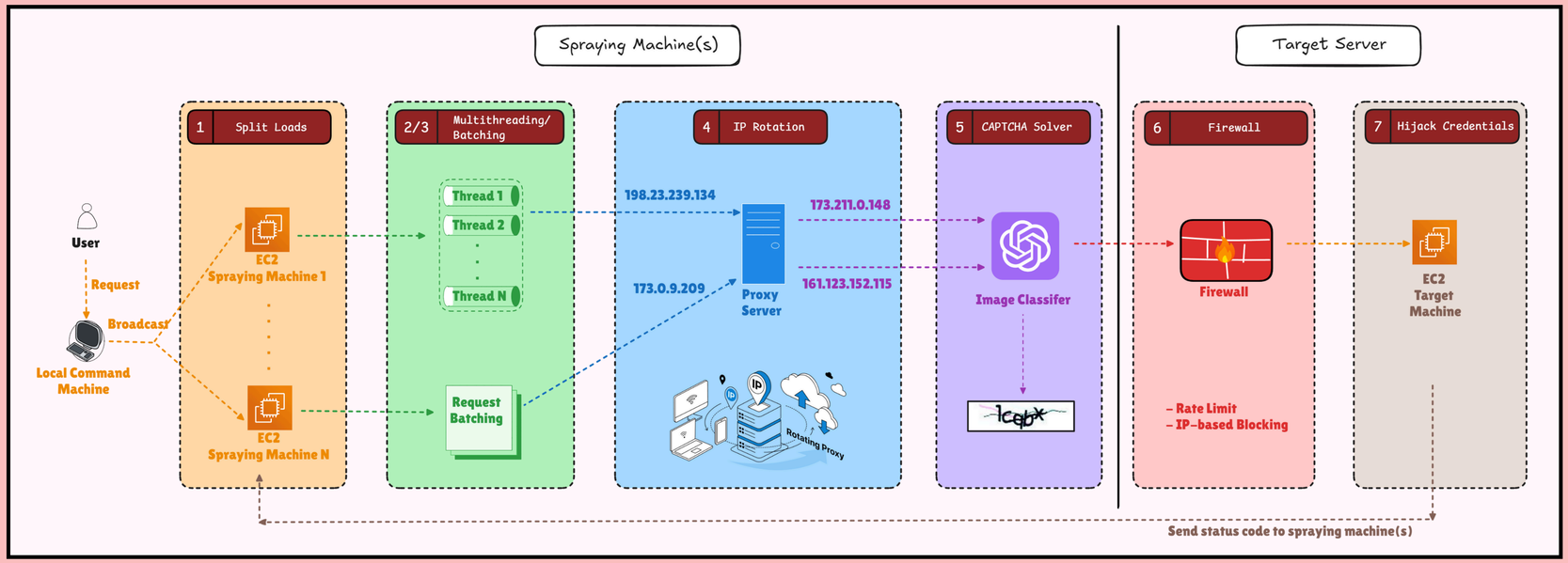
Setup

- 1 Target Machine hosted on an AWS EC2 Instance
  - (uses HTTP Auth and text-based CAPTCHA)
- 1 central command machine on Local Host
- 3 different spraying machines on 3 AWS EC2 instances

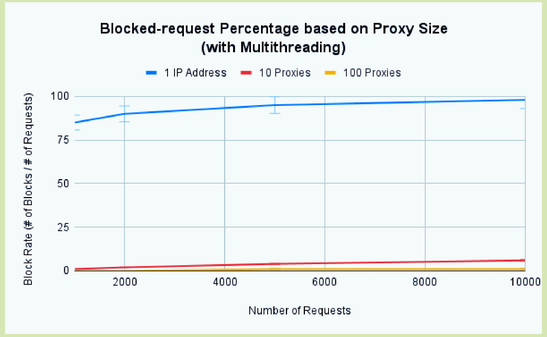
Features

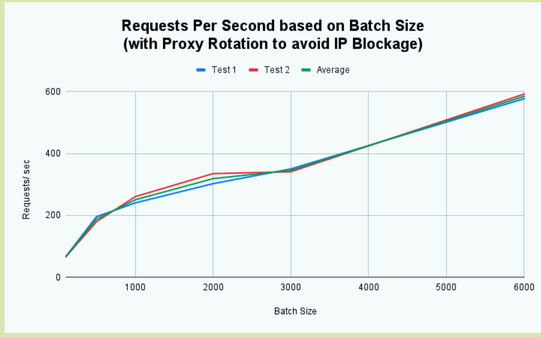
1) Scale with AWS EC2	Create multiple spraying machines, controlled by a local command machine, using EC2.
2) Multithread	Multithread to increase log-in request speed.
3) Batch + Synchronize	Instead of waiting for server responses after each request, send multiple requests in a batch and have a Synchronize function to collect all the responses at once.
4) Rotate IP	Rotate IP addresses constantly using proxies to avoid getting blocked.
5) Classify Images	Use a pre-trained OCR model to crack CAPTCHA texts.
6) Firewall	Implement server security using rate limiting and IP-address blocking.
7) Hijack credentials	After successful log-in, send cracked credentials from spray machine(s) to command machine.

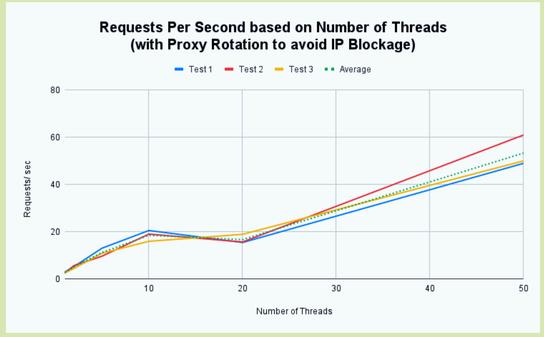
Attack Flowchart



Results







Future Work

Auto-Scaling and Load Balancing: Implement auto-scaling policies to create more spray machines when others go down + balance load across proxies and requests to maintain even distribution.

Dynamic adjustments with AI: Automatically tune rate limits, proxy selection, and batch sizes in real-time with AI based on features like response time, success rate, and server load.

CAPTCHA Expansion: Using other machine learning techniques, test and improve prediction accuracy for image-based CAPTCHA and re-CAPTCHA, the latest version from Google.

Acknowledgements

We would like to thank Jeff Ondich and Mike Tie for their guidance and technical expertise, to our friends Anh Minh, Amadou Toure and Roo Case for their suggestions and advice.

References

Scan the QR code above.