CS50 CYBERSECURITY
FINAL PROJECT

DDOS ON CLOUDFLARE

By: Pranjali Raval

FINAL PROJECT PRESENTATION

- Name- Pranjali Raval
- eDX Username - PranjaliRaval
- Github Username - PranjaliRaval
- Date of Recording - 21 November 2024
- Topic - DDos on Cloudflare that set new benchmark in cyberattack

INTRODUCTION

- In October of 2024 , Cloudflare, a web performance and security company faced largest-ever Distributed Denial of Service (DDoS) attack, setting a new benchmark in volumetric cyberattacks
- The attack targeted continuous online services, specifically financial and enterprise systems, aiming for maximum disruption.
- This attack set a new record for DDoS volumes underscoring critical importance of scalable defenses in an era where DDoS attacks are growing exponentially .

RELEVENCE TO COURSE

- The attack tragetted on victim was DDos
- What is DDos? - DDos is malicoius attempt from unauthorised adversary to target and disrupt the normal functioning of a targeted server, service, or network by overwhelming it with a flood of internet traffic, making target deny the service to genuine user
- In the case of Cloudflare's recent mitigation of a record-breaking 38 terabits-per-second (Tbps) DDoS attack which lasted 65 seconds.

ATTACK DETAILS

- **Massive Traffic Volume:** The attack generated 38 Tbps of traffic, making it the largest DDoS attack ever recorded. This volume was designed to overwhelm even highly resilient systems.

A botnet consisting of thousands or even millions of compromised devices (IoT devices, servers, etc.) was used to generate and direct this malicious traffic.

- **Volume Generation:** The sheer size of the botnet enabled the attackers to generate traffic at a scale of 38 Tbps. This exceeded the capacity of most traditional DDoS mitigation systems.

ATTACK DETAILS

- **Advanced Techniques: HTTP Floods:** Sent large numbers of HTTP requests to mimic legitimate user behavior, making it harder to filter out malicious traffic.

Protocol Spoofing: Faked legitimate traffic, including mimicking browsers like Google Chrome, to bypass detection mechanisms

UDP Amplification: Exploited protocols like DNS and SSDP to amplify the size of the attack traffic by sending small requests that triggered large responses directed at the target.

TECHNICAL ANAYSIS

- **Scale and Complexity**: The attack’s peak traffic of 38 Tbps dwarfed previous records, with its volume capable of overwhelming even large-scale network infrastructures.

- Utilized advanced spoofing techniques, making malicious traffic indistinguishable from legitimate requests.

TECHNICAL ANAYSIS

- **Methodology:** Relied heavily on a botnet comprising compromised IoT devices.

Leveraged UDP amplification techniques, such as DNS amplification, which boosted the bandwidth of attack traffic.

- **HTTP Flooding with Protocol Spoofing:** The attackers generated millions of HTTP requests that mimicked legitimate browser behavior, overwhelming application-layer resources (web servers).

72% of traffic appeared to come from Google Chrome, leveraging browser fingerprinting to bypass traditional detection systems.

MITIGATION BY CLOUDFLARE

- **Global Traffic Distribution:** Cloudflare's anycast network, spanning over 300+ cities worldwide, distributed the attack traffic across its entire network. This architecture ensured no single data center was overwhelmed.
-

By routing malicious traffic to the closest data center, Cloudflare absorbed and filtered the attack traffic without affecting legitimate users.

IMPACT OF ATTACK

- **Security Implications** : Exploitation of IoT Devices

The attack demonstrated the increasing trend of IoT devices being used in botnets. Many IoT devices have insecure configurations, allowing attackers to compromise them and turn them into part of a botnet, thereby amplifying the attack.

This highlights the need for improved security in IoT devices to prevent them from being used in future attacks.

IMPACT OF ATTACK

- **Rise of Multi-Vector Attackss** : The multi-layered nature of the attack—targeting both the application layer (Layer 7) and network layer (Layer 3/4)—reflects the growing sophistication of DDoS techniques.

Attackers increasingly use a mix of methods, including UDP amplification and HTTP floods, making detection and mitigation more challenging for traditional systems.

CONCLUSION

- The 38 Tbps DDoS attack on Cloudflare highlighted the growing scale and complexity of cyber threats. Despite the overwhelming traffic, Cloudflare's advanced mitigation strategies, including Anycast networks and real-time traffic analysis, successfully neutralized the attack.

- This incident emphasizes the need for continuous innovation in DDoS defense technologies and better security for vulnerable IoT devices. As cyberattacks grow in sophistication, businesses must adopt scalable, multi-layered defense systems to stay ahead of evolving threats.