

	VIETTEL AI RACE	Public 251
	ACK Flood Attack là gì? Điểm khác biệt gì so với các loại tấn công DDoS khác?	Lần ban hành: 1

Các cuộc tấn công DDoS (Distributed Denial of Service) ngày càng trở nên phổ biến và tinh vi, gây ra nhiều thiệt hại nghiêm trọng cho hệ thống mạng và dịch vụ trực tuyến. Một trong những hình thức tấn công DDoS đặc biệt nguy hiểm là tấn công ACK Flood. Vậy ACK Flood Attack là gì và điểm khác biệt của nó so với các loại tấn công DDoS khác ra sao?

1. ACK Flood Attack là gì?

ACK Flood Attack là một dạng tấn công mạng thuộc nhóm tấn công từ chối dịch vụ phân tán (DDoS), trong đó kẻ tấn công gửi một lượng lớn các gói tin ACK (Acknowledgment) giả mạo hoặc không hợp lệ đến một máy chủ hoặc hệ thống mạng mục tiêu.

ACK Flood lợi dụng cơ chế của giao thức TCP, cụ thể là cờ (flag) ACK trong TCP Header. Gói tin ACK hợp lệ được dùng để xác nhận đã nhận được gói dữ liệu từ một kết nối TCP đang diễn ra. Kẻ tấn công lợi dụng điều này để gửi các gói ACK không liên quan đến bất kỳ kết nối hợp lệ nào.

Mục đích của cuộc tấn công này là làm quá tải tài nguyên của máy chủ khi nó cố gắng xử lý và xác nhận các gói ACK giả, dẫn đến việc máy chủ không thể xử lý các yêu cầu hợp lệ khác, gây gián đoạn hoặc giảm hiệu suất đáng kể.

2. Cơ chế hoạt động của ACK Flood Attack

Để hiểu rõ hơn về cách thức hoạt động của ACK Flood, chúng ta cần hình dung quá trình xử lý gói tin của một máy chủ. Khi một máy chủ nhận được một gói tin TCP với cờ ACK được bật, nó sẽ thực hiện các bước sau:

Tra cứu bảng trạng thái kết nối (Connection State Table): Máy chủ sẽ tìm kiếm trong bảng này để xác định xem gói tin ACK đó có thuộc về một phiên làm việc TCP đang hoạt động hay không. Bảng này lưu trữ thông tin về tất cả các kết nối đang diễn ra, bao gồm địa chỉ IP nguồn/đích, cổng nguồn/đích và số thứ tự gói tin.

Xác nhận hoặc từ chối: Nếu tìm thấy một phiên làm việc phù hợp, máy chủ sẽ xử lý gói tin. Ngược lại, nếu không tìm thấy, nó sẽ gửi một gói tin RST (Reset) để đóng kết nối và giải phóng tài nguyên.

Trong một cuộc tấn công ACK Flood, kẻ tấn công sử dụng các công cụ như hping3 hoặc scapy để tạo ra hàng triệu gói tin ACK giả mạo, thường có địa chỉ IP nguồn (Source IP) bị làm giả (IP spoofing). Vì các gói tin này không thuộc về bất kỳ kết nối

	VIETTEL AI RACE	Public 251
	ACK Flood Attack là gì? Điểm khác biệt gì so với các loại tấn công DDoS khác?	Lần ban hành: 1

hợp lệ nào, máy chủ phải lặp đi lặp lại quy trình tra cứu và trả lời bằng các gói tin RST.

Quá trình này tuy đơn giản nhưng lại tiêu tốn tài nguyên CPU và bộ nhớ một cách khủng khiếp. Khi số lượng gói ACK tăng lên theo cấp số nhân, máy chủ sẽ bị quá tải, không còn đủ tài nguyên để xử lý các yêu cầu hợp lệ từ người dùng, dẫn đến tình trạng từ chối dịch vụ. Điều đáng nói là các gói ACK giả mạo này rất nhỏ (chỉ vài chục byte) và không chứa dữ liệu, khiến chúng có thể được gửi đi với tốc độ cực cao mà không cần băng thông lớn.

3. ACK Flood Attack khác biệt gì so với các loại tấn công DDoS khác?

Bảng so sánh ACK Flood Attack và các loại tấn công DDoS khác

Tiêu chí	ACK Flood Attack	SYN Flood Attack	HTTP Flood Attack	UDP Flood Attack	NTP Amplification
Mục tiêu tấn công	Thiết bị xử lý gói tin TCP, chủ yếu server và firewall	Server, khai thác quá trình bắt tay TCP (3 bước)	Máy chủ web hoặc ứng dụng, làm quá tải tài nguyên xử lý	Hệ thống nhận gói UDP, làm quá tải băng thông và CPU	Máy chủ NTP, lợi dụng UDP để khuếch đại lưu lượng
Cơ chế tấn công	Gửi nhiều gói ACK giả mạo, không chứa payload, gây tốn tài nguyên xử lý	Gửi nhiều gói SYN giả mạo, không hoàn thành bắt tay TCP 3 bước, gây kết nối "half-open"	Gửi nhiều yêu cầu HTTP hợp lệ hoặc không hợp lệ, làm quá tải xử lý ứng dụng	Gửi hàng ngàn gói UDP từ nhiều nguồn cùng lúc	Gửi các gói UDP giả mạo đến máy chủ NTP để khuếch đại lưu lượng tấn công

	VIETTEL AI RACE	Public 251
	ACK Flood Attack là gì? Điểm khác biệt gì so với các loại tấn công DDoS khác?	Lần ban hành: 1

Lớp mạng bị tấn công	Lớp 4 (TCP transport layer)		Lớp 7 (ứng dụng)	Lớp 4 (UDP transport layer)	
Đặc điểm nhận dạng	Gói tin ACK không hợp lệ, khó phân biệt với gói tin hợp lệ	Kết nối TCP mở không hoàn thành, nhiều kết nối "half-open"	Lượng lớn yêu cầu HTTP đến máy chủ	Lượng lớn gói UDP đến máy chủ	Lưu lượng UDP cực lớn đến máy chủ
Khó khăn trong phòng chống	Gói ACK thường hợp lệ, không chứa payload nên khó lọc	Gây quá tải tài nguyên do giữ kết nối "half-open" lâu	Yêu cầu HTTP hợp lệ nên khó phân biệt với lưu lượng chính thống	Lưu lượng lớn và đa dạng nguồn, khó chặn	Lợi dụng máy chủ NTP trung gian, khuếch đại lưu lượng

4. Làm thế nào để phát hiện và ngăn chặn ACK Flood Attack?

4.1 Cách phát hiện ACK Flood Attack

- **Giám sát lưu lượng:** Theo dõi lưu lượng gói tin ACK bất thường tăng đột biến, đặc biệt là các gói ACK không hợp lệ hoặc từ các nguồn không đáng tin cậy.
- **Sử dụng IDS/IPS:** Hệ thống phát hiện và ngăn chặn xâm nhập (IDS/IPS) có khả năng nhận diện các mẫu tấn công ACK Flood bằng cách phân tích lưu lượng và hành vi mạng.
- **Kiểm tra trạng thái hệ thống:** Giám sát CPU và bộ nhớ của server và firewall. Khi các tài nguyên này bị tiêu thụ đột ngột mà không có lý do rõ ràng, đó có thể là dấu hiệu của một cuộc tấn công.

	VIETTEL AI RACE	Public 251
	ACK Flood Attack là gì? Điểm khác biệt gì so với các loại tấn công DDoS khác?	Lần ban hành: 1

4.2. Cách ngăn chặn ACK Flood Attack

- Cấu hình firewall và bộ lọc gói tin: Thiết lập firewall để chặn hoặc hạn chế các gói ACK đến từ các nguồn không hợp lệ hoặc đáng ngờ, chỉ cho phép các gói tin ACK từ nguồn tin cậy.
- Sử dụng hệ thống IPS (Intrusion Prevention System): IPS có khả năng phát hiện và loại bỏ các gói ACK không hợp lệ trước khi chúng gây ảnh hưởng đến server.
- Giảm thời gian timeout kết nối: Thiết lập thời gian timeout kết nối ngắn hơn giúp loại bỏ nhanh các kết nối không hoạt động hoặc không hợp lệ, giảm tải cho hệ thống.
- Sử dụng CDN (Content Delivery Network): CDN giúp phân phối tải trên nhiều máy chủ toàn cầu, giảm áp lực lên server chính và lọc các gói ACK không cần thiết.
- Tăng cường bảo mật hệ thống: Cập nhật phần mềm, sử dụng mật khẩu mạnh, mã hóa dữ liệu và giám sát hệ thống để ngăn chặn việc bị chiếm quyền điều khiển làm nguồn phát tấn công.
- Sử dụng dịch vụ chống DDoS chuyên nghiệp: Các dịch vụ này có khả năng phát hiện và chặn các cuộc tấn công ACK Flood trước khi chúng gây ra sự cố nghiêm trọng.

5. Tác động của ACK Flood Attack

- Làm quá tải hệ thống: Tiêu hao tài nguyên CPU, RAM của máy chủ và các thiết bị mạng (firewall, router), dẫn đến hiệu suất giảm sút nghiêm trọng.
- Gây từ chối dịch vụ: Khi máy chủ không thể xử lý các yêu cầu hợp lệ, dịch vụ bị gián đoạn, người dùng không thể truy cập website, ứng dụng hoặc các dịch vụ trực tuyến.
- Tạo lá chắn cho tấn công khác: Các cuộc tấn công ACK Flood đôi khi được sử dụng như một "lá chắn" để đánh lạc hướng đội ngũ an ninh mạng, trong khi kẻ tấn công thực hiện các hành vi xâm nhập khác vào hệ thống.

6. Mối liên hệ với các cuộc tấn công khác

ACK Flood thường được sử dụng trong các cuộc tấn công phức hợp (multi-vector attack). Kẻ tấn công có thể kết hợp ACK Flood (tấn công lớp 4) với HTTP Flood (tấn công lớp 7) để đồng thời làm quá tải cả tầng giao thức và tầng ứng dụng. Điều này khiến việc phòng thủ trở nên khó khăn hơn, đòi hỏi các giải pháp bảo mật phải toàn diện và có khả năng phân tích đa lớp.

7. Kết luận

Khác với các hình thức tấn công DDoS khác như SYN Flood hay UDP Flood, ACK Flood tập trung vào lớp giao thức TCP ở tầng 4, khiến việc phát hiện và ngăn chặn trở

	VIETTEL AI RACE	Public 251
	ACK Flood Attack là gì? Điểm khác biệt gì so với các loại tấn công DDoS khác?	Lần ban hành: 1

nên khó khăn hơn do các gói tin giả mạo gần như giống hệt gói tin hợp lệ. Việc hiểu rõ đặc điểm và cơ chế của ACK Flood sẽ giúp các tổ chức, doanh nghiệp chủ động hơn trong việc xây dựng các giải pháp phòng chống hiệu quả, bảo vệ hệ thống mạng trước các mối đe dọa ngày càng tinh vi này.