Điều tra địa chỉ IP nhằm ngăn chặn tấn công DDoS (từ chối dịch vụ phân tán) trong điện toán đám mây

Opeyemi Ayokunle Osanaiye

0. Tóm tắt

Đặt vấn đề: Tấn công DDoS được cho là mối đe dọa nguy hiểm nhất vào tính khả dụng/tính sẵn sàng của dịch vụ.

Mục tiêu: Tấn công DDoS nhằm ngăn chặn người dùng thông thường truy cập vào dữ liệu chung của dịch vụ bằng cách tấn công vào hệ thống, khiến cho hệ thống quá tải và tốn một lượng lớn băng thông mạng làm cạn kiệt tài nguyên.

Thủ thuật: Giả mạo IP để ẩn đi thông tin phía người thực hiện cuộc tấn công.

Nội dung bài báo:

- Đặt ra vấn đề và đưa ra các phương pháp khác nhau nhằm phát hiện việc giả mạo IP trong điện toán đám mây (Cloud Computing).
- Truy vết từ việc Điều tra pháp chứng Hệ điều hành (OS Fingerprinting) dựa trên Cơ sở nền tảng máy chủ (Host-based) bằng phương pháp Chủ động và Thụ động.
- Việc đã thực thi các giải pháp, thực thi từ đó đưa ra phân tích, đánh giá, kết luận và định hướng.

Các từ khóa:

- Cloud computing: điện toán đám mây
- DDoS attack: tấn công DDoS, tấn công từ chối dịch vụ phân tán (Distributed Denial of Service)
- IP Spoofing: giả mạo IP
- OS Fingerprinting: Điều tra pháp chứng Hệ điều hành

1. Giới thiệu

Điện toán đám mây (Cloud computing/Cloud) là công nghệ bao gồm:

- ❖ Lưới (grid)
- ❖ Tiện ích (utility)
- ❖ Cụm (cluster)
- ❖ Phân tán (distributed)

Nhằm cung cấp cho người dùng những nguồn tài nguyên tổng hợp dưới dạng dịch vụ.

Một mô hình dịch vụ đám mây có thể chia làm 3 loại:

- ❖ Phần mềm dịch vụ (SaaS)
- ❖ Nền tảng dịch vụ (PaaS)
- ❖ Cơ sở hạ tầng dịch vụ (IaaS)

Được triển khai sử dụng, khai thác với các phân quyền như:

- ❖ Công khai
- ❖ Riêng tư
- ❖ Cộng đồng/Nhóm
- ❖ Điện toán kết hợp

Các vấn đề về bảo mật trong cloud nói riêng và bảo mật nói chung luôn xoay quanh 3 vấn đề chính:

- ❖ Tính bảo mật
- ❖ Tính toàn vẹn
- ❖ Tính khả dụng/Tính sẵn sàng

Định nghĩa: Tấn công DDoS vào Cloud là mối đe dọa nguy hiểm nhất vào tính khả dụng/tính sẵn sàng của Cloud.

Mục tiêu: Tấn công DDoS nhằm ngăn chặn người dùng thông thường truy cập vào dữ liệu chung của Cloud bằng cách tấn công vào hệ thống, khiến cho hệ thống quá tải và tốn một lượng lớn băng thông mạng làm cạn kiệt tài nguyên của Cloud.

Thủ thuật: Giả mạo IP để ẩn đi thông tin phía người thực hiện cuộc tấn công DDoS vào Cloud.

2. Tấn công DDoS vào Cloud

(Do phần định nghĩa, mục tiêu và thủ thuật đã được đề cập trong phần giới thiệu nên sẽ không nhắc lại)

Cuộc tấn công được thực hiện như hình bên dưới.

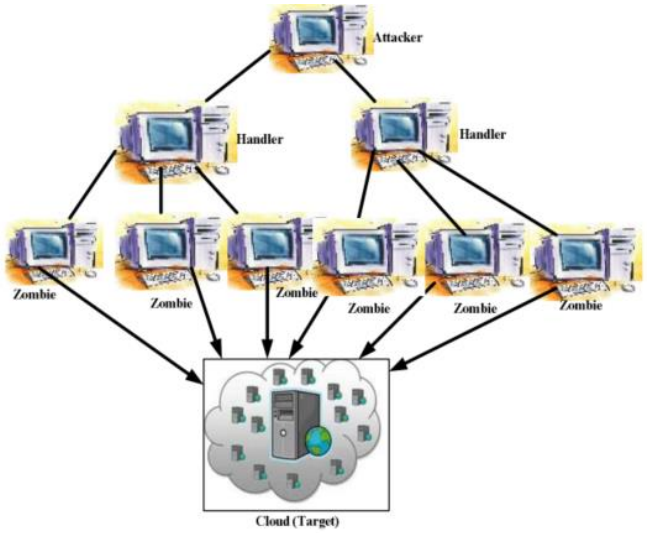


Figure 1. DDoS attack in Cloud

3. Các phương pháp phòng chống giả mạo IP trong tấn công DDoS vào Cloud

Để phòng tránh các vấn đề đó, đã có một số phương pháp đã được đề xuất: (gồm 5 phương pháp được đề xuất, phần này trình bày 4 phương pháp và phương pháp Điều tra pháp chứng Hệ điều hành OS Fingerprinting sẽ được trình bày trong một phần riêng)

Hop-Count Filter (HCF)

- Định nghĩa: Là một phương pháp được dùng để lọc nhiều gói tin bằng cách sử dụng giá trị Time-to-Live (TTL) từ header của các gói tin thu được từ bảng IP2HC.
- Ưu điểm: Bằng cách kiểm tra xem các gói tin có được chấp nhận hay không? Những gói tin được chấp nhận nếu những giá trị của nó phù hợp và ngược lại nếu những giá trị của nó không phù hợp sẽ bị đánh dấu là giả mạo và bị từ chối. Từ đó phát hiện được gói tin giả mạo.
- Hạn chế: Do tất cả các Hệ điều hành không có cùng sử dụng một giá trị Time-to-Live (TTL) ban đầu, từ đó không

thể tạo được sự tương thích trong quá trình lấy giá trị Time-to-Live (TTL) ban đầu.

ANTID (AntiDDoS)

- Định nghĩa: Là một phương pháp được dùng để phát hiện và lọc các gói tin giả mạo trong cuộc tấn công DDoS. Bằng việc kiểm tra thông tin là mỗi gói tin chỉ có một đường dẫn pháp chứng/dấu vết mà từ đó xác định được lộ trình của gói tin sau đó xác định được địa chỉ IP của nó.
- Ưu điểm: Bằng khả năng phân biệt được các đường dẫn IP khác nhau được thực hiện bởi các IP khác nhau, máy chủ lập được bản đồ máy khách giao tiếp và địa chỉ IP của các máy khách truy cập đến đường dẫn tương ứng.
- Hạn chế: Do nếu địa chỉ IP giả mạo không tồn tại trên ánh xạ của nó thì không thể phát hiện các gói tin IP giả mạo.

Trace route

- Định nghĩa: Là một công cụ mạng để phát hiện đường dẫn mà gói tin đã truyền qua.
- Ưu điểm: Bằng cách đếm số bước di chuyển tới nguồn của gói tin (nguồn thật không bị giả mạo).
- Hạn chế: Do nếu có tường lửa sẽ bị sai số ở số bước di chuyển do bị tường lửa tác động sẽ trả về giá trị cho tường lửa và sẽ không đúng với số bước di chuyển thật. Tốc độ xử lý chậm.

TCP interactive

- Định nghĩa: Là một giao thức kết nối đảm bảo việc gửi các gói tin đáng tin cậy bằng cách gửi các gói tin ACK cho mỗi gói giữa nguồn và đích.
- Ưu điểm: Bằng việc nguồn không phản hồi bất kỳ thông tin nào nếu gói tin được gửi đến là giả và không tồn tại từ đó phát hiện được gói tin giả mạo.
- Hạn chế: Nếu hacker phát hiện được phương pháp đang sử dụng và từ đó viết 1 chương trình dự đoán số SYN từ gói SYN/ACK từ đó phản hồi lại và tấn công.

4. Điều tra pháp chứng Hệ điều hành (OS Fingerprinting)

Định nghĩa:

- Là phương pháp giám sát một gói tin để xác định được Hệ điều hành mà máy gửi gói tin đó đang sử dụng.

Được sử dụng nhằm:

- Kiểm tra hạn sử dụng của Hệ điều hành
- Phát hiện và khắc phục lỗi của những Hệ điều hành dễ bị tấn công
- Phát hiện hacker

Có 2 phương pháp được thực hiện:

- Chủ động
- Bị động

Ưu điểm:

- Do được phát triển để tương thích nhiều Hệ điều hành khác nhau, từ đó có những ngăn xếp TCP/IP tương ứng phù hợp bằng chữ ký số độc lập, duy nhất.

Tính năng:

Khi tiến hành điều tra pháp chứng Hệ điều hành một gói tin IP, tương ứng với những Hệ điều hành khác nhau, có thể thu thập được những thông tin khác nhau ở header của gói tin TCP/IP. Những thông tin đó bao gồm:

- Time-to-Live (TTL) ban đầu
- Kích thước Window
- IP không phân mảnh tùy ý
- IP dịch vụ tùy ý

Những thông tin này được khai thác ở header của IP tở các gói tin SYN/TCP hay SYN/ACK.

Phương pháp:

Việc điều tra pháp chứng Hệ điều hành cần được xét đến yếu tố Chủ động hay Bị động.

Với phương pháp Chủ động:

- Gửi một gói tin thăm dò được thiết lập chuyên biệt tới nguồn yêu cầu
- Công cụ phổ biến: Nmap, Xprobe2, SinFP

Với phương pháp Bị động:

- Kiểm tra thông tin ở header
- Công cụ phổ biến: p0f (Passive OS ingerprint), OSF (passive OS fingerprinting for iptables) và Ettercap

Phân tích công cụ Nmap trong phương pháp Chủ động:

- Định nghĩa Là công cụ phổ biến nhất trong việc lập bảng đồ mạng.
- Cơ chế hoạt động: Bằng cách cung cấp tính năng quét bằng cách gửi 15 đầu dò gồm các gói tin TCP, UDP và ICMP để mở và đóng các cổng của máy chủ được chỉ định. Sau đó nhận lại các gói tin có các header chứa thông tin để xác định Hệ điều hành. Bằng cách này, có thể so sánh sự tương thích giữa những thông tin thu thập được với cơ sở dữ liệu Hệ điều hành.

Phân tích công cụ p0f trong phương pháp Bị động:

- Định nghĩa: Là công cụ điều tra pháp chứng Bị động, được tạo ra bởi Michal Zalewski vào năm 2000.
- Cơ chế hoạt động: Bằng cách phân tích các header của gói tin TCP/IP để xác định Hệ điều hành máy chủ. Cách này sẽ thực hiện điều tra pháp chứng bằng cách lấy gửi một gói tin SYN gửi đi và nhận gói tin SYN/ACK từ máy chủ. Từ đó nó hạn chế được các công cụ dò tìm Hệ điều hành đang hoạt động bằng việc không gửi các gói tin thăm dò tới.

Thông tin bên ngoài: những ứng dụng kể trên em tìm hiểu được hỗ trợ khá nhiều trên nền tảng Linux. Ngoài trên Kali Linux cũng sẽ được cài sẵn tích hợp trong Hệ điều hành lúc vừa mới được cài đặt giúp cho việc nghiên cứu về phòng chống giả mạo IP để tấn công DDoS trở nên thuận tiện hơn.

Sơ đồ khối phân tích điều tra việc giả mạo IP

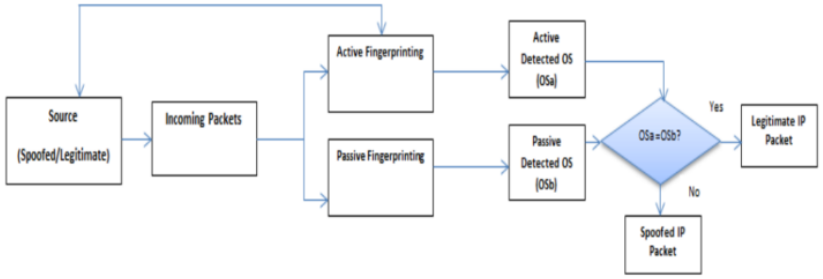


Figure 2. IP Spoofing Detection Block

5. Đánh giá giải pháp

Cả phương pháp Chủ động và Bị động đều hoạt động như sơ đồ khối ở phần vừa được đề cập ở cả 2 chế độ Tích cực và Ngầm định ứng với mỗi phương pháp.

Trong các trường hợp thì chương trình sẽ được ở chế độ Ngầm định chạy và khi có trường hợp nhận một lượng lớn các gói tin cùng gửi về 1 địa điểm sao cho nó đủ lớn để gây ra việc từ chối dịch vụ phân tán (DDoS) trên Cloud thì khi đó chương trình sẽ bật sang chế độ hoạt động Tích cực nhằm chống lại cuộc tấn công.

Trong quá trình tấn công thì những gói tin IP có thể đến từ nguồn thật tạo ra hoặc từ nguồn giả mạo.

Trong thời gian chạy phương pháp Bị động, việc thu thập và phân tích gói tin có chứa header TCP/IP được thực hiện bằng ứng dụng p0f. Việc điều tra pháp chứng Hệ điều hành được thực hiện bằng việc phân tích độ tương thích bằng cách phân tích header với cơ sở dữ liệu Hệ điều hành của p0f của để xác định Hệ điều hành.

Trong thời gian chạy phương pháp Chủ động, việc gửi gói thăm dò được thiết lập chuyên biệt tới nguồn yêu cầu bằng ứng dụng Nmap. Nếu địa chỉ IP giả là một địa chỉ Chủ động thì nó sẽ gửi gói tin phản hồi sao cho Nmap có thể bắt được và sử dụng để xác định Hệ điều hành từ cơ sở dữ liệu.

Hai hệ điều hành trong 2 phương pháp Chủ động và Bị động sẽ được so sánh với nhau về độ tương thích. Nếu không tương thích sẽ bị đánh dấu là giả mạo và ngược lại nếu tương thích sẽ được đánh dấu là hợp lệ.

6. Thực thi

Những thông số được sử dụng để thực thi:

- Mã nguồn mở: XCP 1.6
- Vi xử lý: Intel core i5 64 bit
- RAM 8GB
- Ổ cứng: 500GB

XCP sử dụng 4 máy ảo chạy các dịch vụ Cloud khác nhau và Ubuntu 12.04 được dùng để chạy Nmap và p0f.

(Mô tả như hình bên dưới)

TABLE I: XEN CLOUD PLATFORM 1.6 VM SPECIFICATION

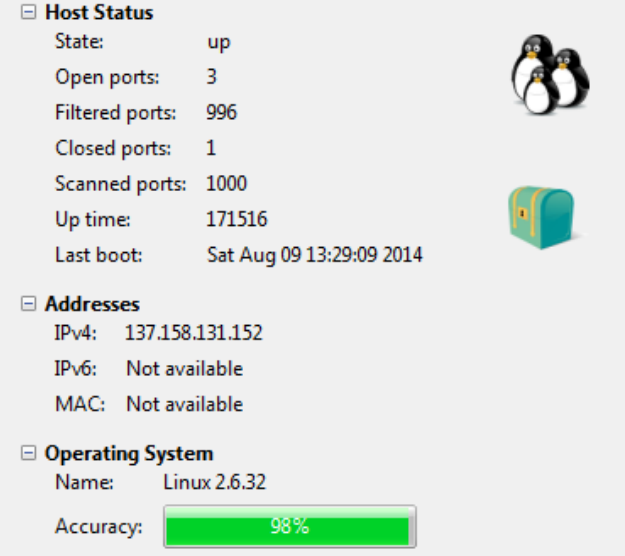
Virtual Machine OS	Product Name	Kernel Version
Centos 6.5	Final	2.6.32
Debian 7.6	Wheezy	3.2
Ubuntu 12.04 LTS	Precise	3.11
Ubuntu 14.04 LTS	Trusty	3.13

7. Đánh giá và phân tích

Để đánh giá thực nghiệm, các kết nối đầu ra và vào đã được triển khai trên nền tảng cloud. Có 2 trường hợp giả định được đặt ra để đánh giá 1 là chỉ toàn người dùng thông thường và 2 là bao gồm cả người dùng thông thường và hacker.

Trường hợp 1: Chỉ toàn người dùng thông thường

Trong quá trình thực thi, với phương pháp Bị động gói tin SYN được p0f phân tích là được kết nội với máy có Hệ điều hành là Win XP. Còn với phương pháp Chủ động gói tin SYN cũng được Nmap phân tích là được kết nội với máy có Hệ điều hành là Win XP. Và cũng trả về trường hợp kết quả về cùng Hệ điều hành Linux 2.6 giữa hai ứng dụng p0f và Nmap trong lúc thực thi.



Trường hợp 2: Bao gồm cả người dùng thông thường và hacker

Giống nhau: cả 2 đều tạo lưu lượng và chạy được từ bên ngoài môi trường Cloud.

Trước khi xác minh thì địa chỉ nguồn của các gói tin được sử dụng để kiểm tra nguồn thật. Sau đó quá trình xác minh thì kiểm tra sự tương thích giữa 2 Hệ điều hành trong phương pháp Thụ động và Chủ động. Nếu là người dùng thông thường thì kết quả đều trả về là Win XP còn nếu trường hợp là thì kết quả trả về không tương thích nhau về Hệ điều hành.

```
<Mon Sep 22 16:45:22 2014> 137.158.131.169:8160 - Windows XP/2000 (RFC1323+, w+, tstamp-) [GENERIC]
  Signature: [8192:127:1:52:M1460,N,W2,N,N,S:.:Windows:?]
  -> 137.158.131.199:80 (distance 1, link: ethernet/modem)
<Mon Sep 22 16:45:26 2014> 137.158.131.169:8161 - Windows XP/2000 (RFC1323+, w+, tstamp-) [GENERIC]
  Signature: [8192:127:1:52:M1460,N,W2,N,N,S:.:Windows:?]
  -> 137.158.131.199:22 (distance 1, link: ethernet/modem)
```

8. Kết luận và định hướng

Bài báo này đã đưa ra các phương pháp khác nhau nhằm xác định nguồn thật của các gói tin nhằm phát hiện giả mạo IP trong tấn công DDoS. Bài báo đề xuất phương pháp Điều tra pháp chứng Hệ điều hành bằng phương pháp Chủ động và Bị động để xác định nguồn thực của gói tin bằng cách xác định độ tương thích của Hệ điều hành trong Cloud.

Định hướng mục tiêu trong tương lai là có thể tự động hóa quy trình để đạt được kết quả tốt hơn và hạn chế tác động của người lập trình viên hay quản trị viên.