Bài: 10.1 Từ chối dịch vụ - Khái niệm, kỹ thuật tấn công DoS/DDOS & Botnet

Xem bài học trên website để ủng hộ Kteam: 10.1 Từ chối dịch vụ - Khái niệm, kỹ thuật tấn công DoS/DDOS & Botnet

Mọi vấn đề về lỗi website làm ảnh hưởng đến bạn hoặc thắc mắc, mong muốn khóa học mới, nhằm hỗ trợ cải thiện Website. Các bạn vui lòng phản hồi đến Fanpage How Kteam nhé!

Tóm tắt

Ở chương này, chúng ta tập trung nghiên cứu **tấn công từ chối dịch vụ (DoS)** và **tấn công từ chối dịch vụ phân tán (DDOS)**. Chương này bao gồm kiến thức về các loại tấn công từ chối dịch vụ khác nhau, kĩ thuật tấn công, khái niệm botnet, công cụ tấn công và những chiến lược chống lại những tấn công này.

Khái niệm DoS/DDOS

Từ chối dịch vụ (DoS)

Từ chối dịch vụ là kiểu tấn công mà trong đó dịch vụ mà mạng hay hệ thống cung cấp bị từ chối. Dịch vụ có thể bị từ chối, giảm chức năng hay chặn truy cập đến tài nguyên, kể cả với người dùng chính thống. Có nhiều kĩ thuật để thực hiện tấn công từ chối dịch vụ như tạo một lượng lớn yêu cầu dịch vụ đến hệ thống mục tiêu. Hệ thống sẽ bị quá tải, dẫn đến từ chối dịch vụ yêu cầu.

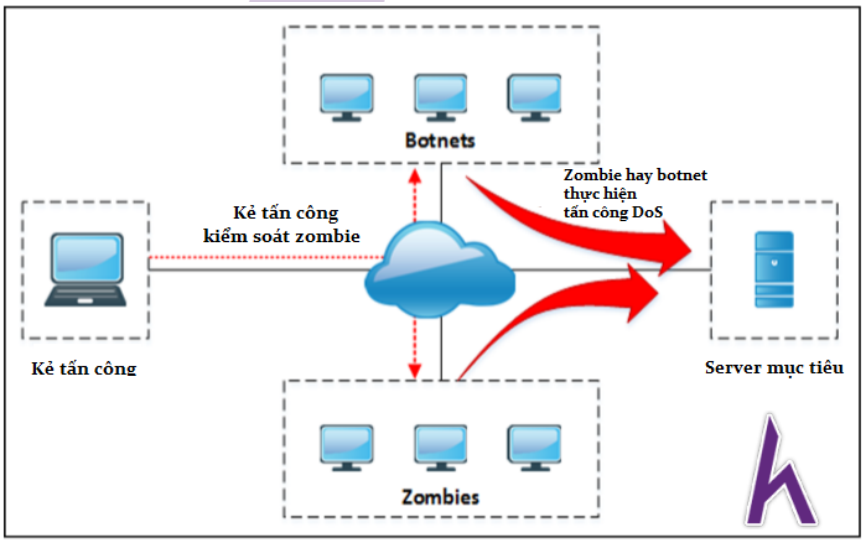

Figure 10-01 Denial-of-Service Attack

Những triệu chứng thường thấy khi bị tấn công DoS là:

- Hiệu suất máy chậm
- Mất kết nối mạng không dây hay có dây
- Từ chối truy cập đến dịch vụ mạng

Từ chối dịch vụ phân tán (DDoS)

Tương tự với tấn công DoS, trong tấn công từ chối dịch vụ phân tán, vô số hệ thống bị thỏa hiệp tham gia vào tấn công một mục tiêu để tạo tấn công từ chối dịch vụ. Tấn công này sử dụng botnet.

Cách thức hoạt động của tấn công từ chối dịch vụ phân tán

Thông thường, quy trình thiết lập một kết nối bao gồm việc user gửi yêu cầu đến server để xác thực. Server phản hồi với sự chấp thuận xác thực. User báo đã nhận được chấp thuận, sau đó kết nối được thiết lập và user được cho phép kết nối với server.

Trong quy trình tấn công từ chối dịch vụ, kẻ tấn công sẽ gửi nhiều yêu cầu xác thực đến server. Những yêu cầu này có địa chỉ người nhận giả, nên server không thể tìm user để gửi chấp thuận xác thực. Quy trình xác thực sẽ chờ một khoảng thời gian nhất định, sau đó đóng session. Khoảng thời gian chờ thường kéo dài hơn một phút. Kẻ tấn công liên tục gửi yêu cầu gây ra nhiều kết nối mở trên server, từ đó dẫn đến từ chối dịch vụ.

Kĩ thuật tấn công DoS/ DDoS

Các mục cơ bản của tấn công DoS/ DDoS

Tấn công lưu lượng

Đây là tấn công thực hiện bằng cách gửi lượng lớn giao thông đến mục tiêu để làm quá tải khả năng tiêu thụ của băng thông. Mục đích của tấn công là làm chậm hiệu suất máy, suy giảm chất lượng dịch vụ. Thông thường, những tấn công này sử dụng hằng trăm **Gbps** của băng thông.

Tấn công phân tách

Đây là **tấn công phân tách IP datagram** thành vô số gói tin nhỏ hơn. Những gói tin đã phân tách này cần tập hợp lại ở đích và quá trình tập hợp này cần nhiều tài nguyên bộ định tuyến. Có hai loại tấn công thuộc tấn công phân tách:

1. Tấn công phân tách UDP và ICMP
2. Tấn công phân tách TCP

Tấn công TCP-State-Exhaustion

Đây là tấn công tập trung vào web server, tường lửa, cân bằng tải và các cơ sở hạ tầng khác để phá hoại kết nối bằng cách tiêu thụ bảng trạng thái kết nối. Mục tiêu của tấn công này là sử dụng hết số kết nối đồng thời mà thiết bị mục tiêu có thể hỗ trợ. **Tấn công phân tách TCP** phổ biến nhất là **ping of death**.

Tấn công tầng ứng dụng

Tấn công tầng ứng dụng DDoS còn được gọi là tấn công tầng 7 DDoS. Tấn công cấp ứng dụng DoS là một dạng tấn công DDoS, tập trung vào tầng ứng dụng của mô hình OSI. Tấn công tầng ứng dụng làm quá tải một dịch vụ hay tính năng của website hoặc ứng dụng dẫn đến từ chối hoặc suy giảm chất lượng dịch vụ.

Kĩ thuật tấn công DoS/DDoS

Tấn công băng thông

Tấn công băng thông cần vô số nguồn tạo ra lượng lớn yêu cầu để làm quá tải hệ thống mục tiêu. Tấn công phân tán DoS là một kĩ thuật hữu hiệu trong việc tạo ra lượng lớn yêu cầu đến mục tiêu. Ngược lại, tấn công DoS sử dụng một máy đơn không thể tạo ra đủ số yêu cầu để làm mục tiêu bị quá tải.

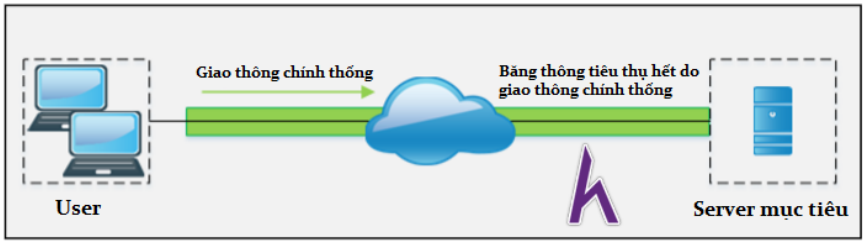

Figure 10-02 Before DDoS bandwidth attack

Như đã biết, **Zombie** là hệ thống đã thỏa hiệp bị chủ máy tính (kẻ tấn công) kiểm soát bằng **handler**. Zombie sẽ hỗ trợ cho kẻ tấn công thực hiện tấn công DDoS. Botnet, được giới thiệu ở phần sau, cũng được sử dụng để thực thị tấn công DDoS bằng cách gửi vô số gói tin **ICMP Echo** đến hệ thống mạng. Mục tiêu của tấn công băng thông là tiêu tốn hết lượng băng thông vốn dành cho sử dụng chính thống.

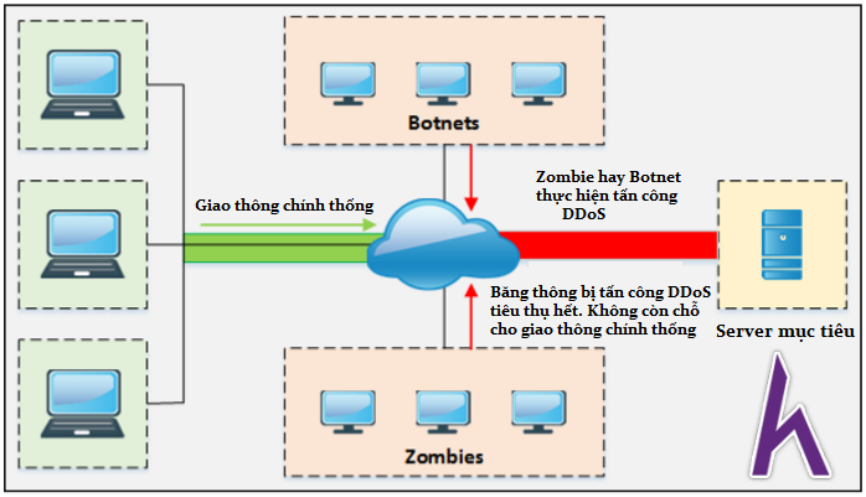

Figure 10-03 After DDoS bandwidth attack

Sau khi so sánh các số liệu trên, bạn sẽ hiểu cách thức hoạt động của tấn công từ chối dịch vụ phân tán bằng cách tiêu thụ hết băng thông sao cho giao thông chính thống bị từ chối.

Tràn yêu cầu dịch vụ

Đây là một dạng tấn công DDoS, trong đó kẻ tấn công gửi vô số yêu cầu đến dịch vụ như ứng dụng web hay web server cho đến khi dịch vụ bị quá tải. Người dùng chính thống sẽ bị từ chối kết nối bởi vì các kết nối TCP lặp đi lặp lại của tấn công đã tiêu thụ hết tài nguyên.

Tấn công SYN/ Ngập

Tấn công SYN hay **ngập SYN** khai thác quy trình bắt tay ba bước. Kẻ tấn công gửi nhiều yêu cầu SYN đến server mục tiêu để làm tắc nghẽn hệ thống. Yêu cầu SYN gửi đến có địa chỉ IP nguồn giả nên không thể tìm thấy nạn nhân. Nạn nhân chờ thông báo từ địa chỉ IP nhưng không có phản hồi nào. Thời gian chờ này làm hệ thống tắc nghẽn kết nối bởi vì hệ thống không nhận được ACK. Một kết nối không hoàn chỉnh có thể bị nghẽn khoảng 75 giây.

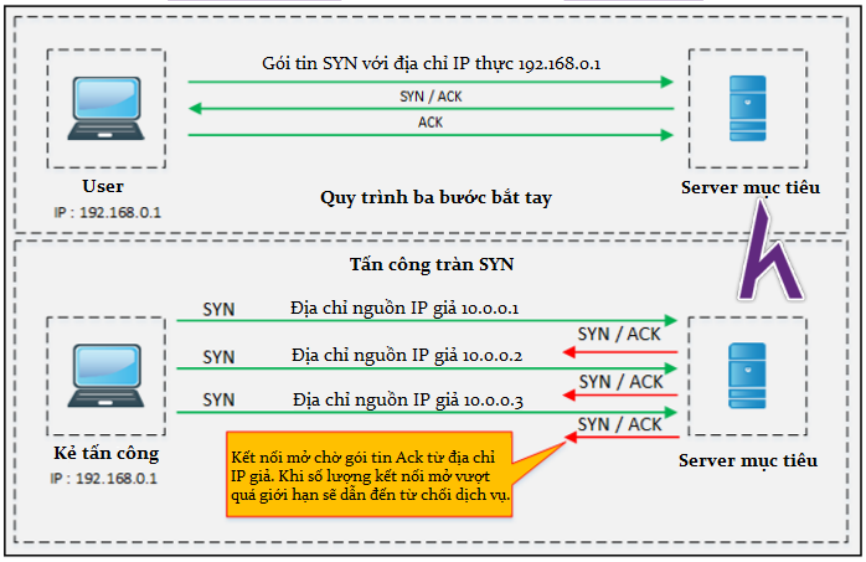

Figure 10-04 SYN Flooding

Tấn công tràn ICMP

Giao thức tin nhắn kiểm soát Internet (ICMP) là dạng tấn công trong đó kẻ tấn công sử dụng yêu cầu ICMP. ICMP là giao thức hỗ trợ mà thiết bị mạng sử dụng để thông báo thông tin, lỗi và chỉ số. Những yêu cầu và phản hồi này tiêu thụ tài nguyên của thiết bị mạng. Do đó, tài nguyên thiết bị bị cạn kiệt.

Tấn công ngang hàng

Tấn công này lợi dụng lỗi của các server ngang hàng hoặc kĩ thuật trao đổi lưu lượng ngang hàng sử dụng giao thức **Kết nối trực tiếp** (DC++) để thực thi một tấn công DDoS. Hầu hết mạng ngang hàng đều thuộc client DC++. Mỗi mạng dựa trên client DC++ đều được liệt kê trong hub. Mạng ngang hàng được triển khai giữa nhiều host. Một khi nó bị thoái hiệp, kẻ tấn công dễ dàng điều khiển nó thực hiện tấn công DDoS. Tấn công DoS hay DDoS có độ ảnh hưởng khác nhau dựa trên các topo mạng ngang hàng.

Tấn công từ chối dịch vụ vĩnh viễn

Tấn công từ chối dịch vụ vĩnh viễn tập trung vào phá hoại ngầm phần cứng thay vì từ chối dịch vụ. Phần cứng bị tấn công sẽ bị hủy hoại, cần thay thế hoặc cài đặt lại phần cứng. PdoS được thực hiện bằng một phương pháp mang tên "**Phlashing**" có khả năng gây ra những phá hoại không thể phục hồi cho phần cứng, hoặc "**Bricking a system**" bằng cách gửi những cập nhật phần cứng giả, khi những mã ác ý vô tình được thực thi, nó sẽ gây tổn thương đến phần cứng.

Tấn công tràn tầng ứng dụng

Tấn công này tập trung vào tầng ứng dụng với mục tiêu là server ứng dụng hoặc ứng dụng đang chạy trên máy tính client. Kẻ tấn công tìm lỗi trong ứng dụng hoặc hệ điều hành là lợi dụng chúng để qua mặt hệ thống kiểm soát, từ đó lấy được quyền kiểm soát đặc quyền đối với ứng dụng, hệ thống hoặc mạng.

Tấn công từ chối dịch vụ phản xạ (DRDoS)

Quá trình khởi chạy tấn công này bao gồm cả nạn nhân trung gian và nạn nhân thứ cấp. Kẻ tấn công gửi yêu cầu đến nạn nhân trung gian để chuyển hướng giao thông đến nạn nhân thứ cấp. Nạn nhân thứ cấp chuyển hướng giao thông đến mục tiêu. Sự tham gia của nạn nhân trung gian và thứ cấp là để giả mạo tấn công.

Botnet

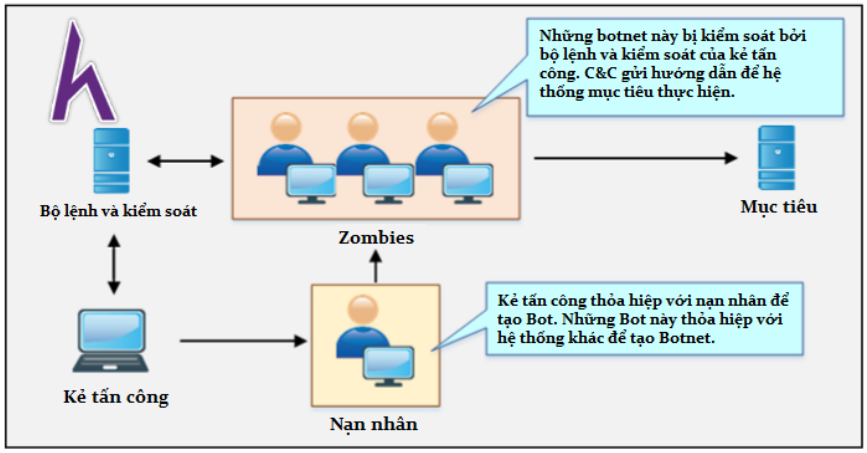

Figure 10-05 Typical Botnet Setup

Botnet dùng để thực hiện một nhiệm vụ liên tục. Những botnet ác ý truy cập đến hệ thống bằng script và code ác ý, nó cảnh báo chủ máy tính khi hệ thống bị botnet kiểm soát. Thông qua chủ máy tính, kẻ tấn công có thể kiểm soát hệ thống và gửi yêu cầu để thực hiện tấn công DoS.

Thiết lập Botnet

Botnet được thiết lập bằng cách cài đặt một bot trên máy nạn nhân thông qua **ngựa Trojan**. **Ngựa Trojan** mang bot giả làm payload được chuyển tiếp đến nạn nhân bằng phishing hay chuyển hướng đến website ác ý hoặc website chính thống thỏa hiệp. Khi **Trojan** được thực thi, máy tính nạn nhân sẽ bị nhiễm độc và bị kiểm soát bởi **handler**. **Handler** là Bộ lệnh và kiểm soát (**CandC**) sẽ gửi hướng dẫn đến hệ thống nhiễm độc (**Bots**) để tấn công lên mục tiêu chính.

Quét máy dễ xâm nhập

Có nhiều kĩ thuật để quét máy dễ xâm nhập bao gồm **Random**, **Hit-list**, **Topological**, **Subnet**, và **Permutation scanning**. Bảng dưới cho thấy mô tả ngắn gọn các phương pháp quét:

Phương pháp	Mô tả
Random (phương pháp quét ngẫu nhiên)	Máy nhiễm độc dò ngẫu nhiên địa chỉ IP để tạo không gian địa chỉ IP và quét chúng tìm lỗ hổng bảo mật. Khi tìm được một máy dễ tổn thương, nó xâm nhập và lây nhiễm máy đó bằng script dùng để nhiễm độc chính nó. Phương pháp quét ngẫu nhiên lan truyền nhiễm độc rất nhanh bởi vì nó thỏa hiệp với nhiều host.
Hit-list (phương pháp quét theo danh sách)	Kẻ tấn công sẽ thu thập thông tin về nhiều máy dễ xâm nhập để tạo một hit-list. Tiếp theo, kẻ tấn công tìm được mục tiêu và lây nhiễm độc cho nó. Sau khi lây nhiễm một máy, danh sách được chia thành hai, một nửa được giao cho hệ thống mới thỏa hiệp. Quy trình quét trong hit-list chạy cùng lúc. Kĩ thuật này dùng để bảo đảm mã độc được lan truyền và cài đặt trong thời gian ngắn.
Topological (Phương pháp quét topo)	Phương pháp này thu thập thông tin từ hệ thống nhiễm độc để tìm mục tiêu mới/ Ban đầu máy thỏa hiệp tìm URL từ đĩa, sau đó lây nhiễm và kiểm tra lỗ hổng bảo mật. Nếu URL chính xác thì phương pháp này có độ chính xác rất cao.
Subnet (Phương pháp quét Subnet)	Kĩ thuật này thực hiện để host thỏa hiệp quét mục tiêu trong mạng cục bộ của nó sau một tường lửa. Mục tiêu của kĩ thuật này là tạo một đội quân zombie trong thời gian ngắn.
Permutation Scanning (quét hoán vị)	Quét hoán vị sử dụng hoán vị ngẫu nhiên giả. Trong kĩ thuật này, máy nhiễm độc chia sẻ hoán vị ngẫu nhiên giả của địa chỉ IP. Nếu phát hiện một hệ thống đã nhiễm độc bằng hit-list hoặc một phương pháp khác, nó bắt đầu quét từ IP tiếp theo trong danh sách. Nếu phát hiện một hệ thống đã nhiễm độc trong danh sách hoán vị, nó bắt đầu quét từ một điểm ngẫu nhiên trong danh sách.

Lan truyền code ác ý

Có 3 phương pháp lan truyền code ác ý phổ biến nhất bao gồm lan truyền trung tâm, back-chaining và tự quản.

Lan truyền nguồn trung tâm

Phương pháp này cần nguồn trung tâm nơi cài đặt bộ công cụ tấn công. Khi kẻ tấn công khai thác máy dễ xâm nhập, nó mở kết nối trên hệ thống nhiễm độc để nghe truyền tệp. Sau đó, bộ công cụ được sao chép từ nguồn trung tâm. Bộ công cụ này được tự động cài đặt sau khi chuyển từ nguồn trung tâm, dùng để thực hiện các tấn công sau này. Cơ chế chuyển tệp được dùng để truyền code ác ý thường là HTTP, FTP hoặc RPC.

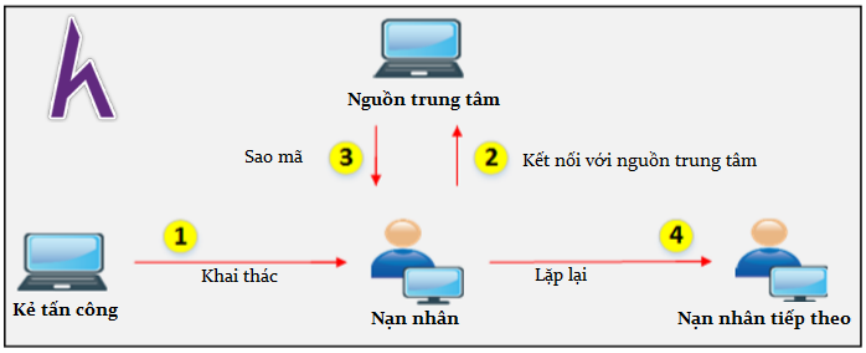

Figure 10-06 Central Source Propagation

Lan truyền móc xích ngược

Lan truyền móc xích ngược yêu cầu bộ công cụ tấn công cài đặt trên máy kẻ tấn công. Khi kẻ tấn công khai thác máy dễ xâm nhập, nó mở kết nối trên hệ thống nhiễm độc để nghe truyền tệp. Sau đó, bộ công cụ được sao chép từ nguồn trung tâm. Khi cài đặt toolkit trên hệ thống nhiễm độc xong, nó sẽ tìm các hệ thống dễ xâm nhập khác và quá trình lại tiếp tục.

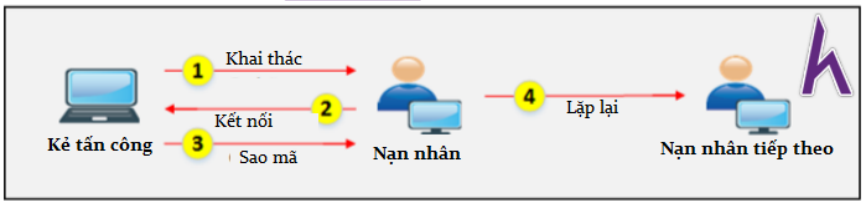

Figure 10-07 Back-Channing Propagation

Lan truyền tự quản

Trong quá trình này, kẻ tấn công khai thác và gửi code ác ý đến hệ thống dễ xâm nhập. Toolkit được cài đặt và tìm các hệ thống dễ xâm nhập khác. Khác với phương pháp lan truyền nguồn trung tâm, phương pháp này không cần nguồn trung tâm bởi vì nó tự cài đặt toolkit trên hệ thống của mình.

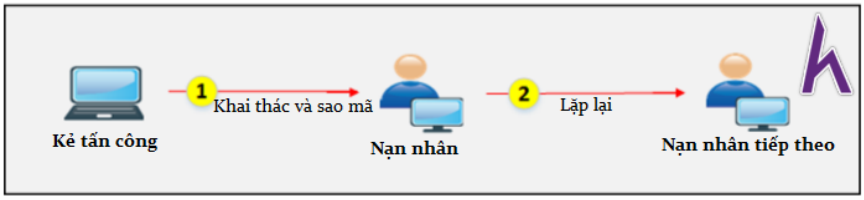

Figure 10-08 Autonomous Propagation

Botnet Trojan

- Blackshades NET
- Cythosia Botnet và Andromeda Bot
- PlugBot