PHẦN A: TỔNG QUAN VỀ TẤN CÔNG MẠNG

I. Những sự kiện về các cuộc tấn công mạng

Nhìn lại 10 vụ tấn công mạng đình đám nhất trong nửa đầu năm 2017

WannaCry được ghi nhận là vụ hack sử dụng phần mềm tống tiền lớn nhất lịch sử tại nhiều quốc gia, tuy nhiên rất có thể đây chỉ là bề nổi của một loạt vấn đề xảy ra trong kỷ nguyên số mà chúng ta đang trải qua.

Nếu như vụ việc Yahoo bị hacker đánh cắp thông tin của hơn 1 tỷ người dùng vào năm 2016 đã là vô cùng tồi tệ, thì những cuộc tấn công mạng quy mô lớn, có tính chuyên nghiệp cao trong nửa đầu năm 2017 tiếp tục khiến người ta "sởn gai ốc" vì tần suất xuất hiện và những hậu quả của nó. Cùng điểm qua những vụ tấn công mạng nổi bật nhất đã xảy ra trong thời gian vừa qua.

1. Hacker đánh cắp email của 1,9 triệu khách hàng tại Bell

Bell - công ty viễn thông lớn nhất tại Canada vào hồi tháng 5 thông báo họ bị một "hacker ẩn danh" tấn công, ăn cắp dữ liệu gồm 1,9 triệu địa chỉ email của khách hàng. Hãng đã từ chối trả khoản tiền chuộc mà hacker yêu cầu, khiến cho một phần thông tin người dùng bị hacker tung lên mạng Internet.

2. Mạng xã hội Edmodo bị đánh cắp hơn 77 triệu tài khoản người dùng

Cũng trong tháng 5, Edmodo - trang mạng xã hội học tập phổ biến nhất thế giới hiện nay với hơn 77 triệu thành viên tại nhiều quốc gia được kết nối với nhau đã bị đánh cắp thông tin người dùng và rao bán trên trang web ngầm (Dark Web). Theo Motherboard, những thông tin bị đánh cắp bao gồm tài khoản, địa chỉ email và mật khẩu.

3. Máy chủ Handbrake bị tấn công khiến người dùng Mac nhiễm mã độc

Hàng nghìn người dùng MacBook đã đối mặt nguy cơ dính mã độc trojan chiếm quyền điều khiển sau khi Handbrake - một nhà phát triển ứng dụng hỗ trợ đổi file video liên kết với Apple. Ngay sau khi phát hiện ra sự việc, máy chủ bị ảnh hưởng đã đóng cửa để điều tra nhưng các nhà phát triển cảnh báo người dùng tải phần mềm từ máy chủ trong khoảng thời gian từ ngày 2/5 đến 6/5 vẫn có 50% nguy cơ bị dính trojan.

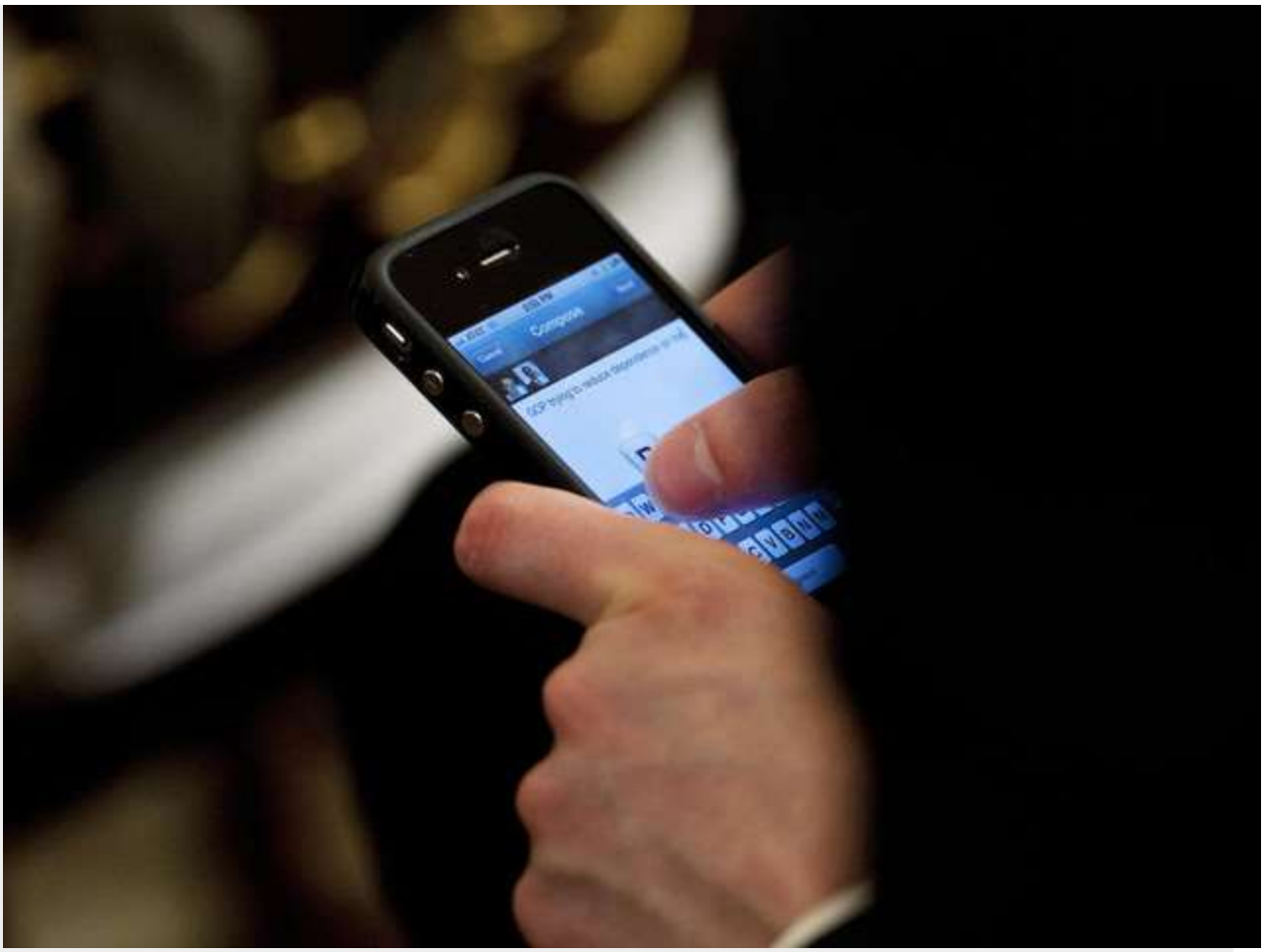
4. Công ty thanh toán tại Anh bị hacker cướp đánh cắp 270.000 tài khoản người dùng

Một công ty dịch vụ thanh toán tại Anh là Wonga đã bị hacker tấn công vào hồi tháng 4, khiến ít nhất 270.000 tài khoản người dùng bị ảnh hưởng. Vụ tấn công diễn ra chỉ vài tháng sau khi hacker chiếm đoạt 2,5 triệu bảng Anh (tương đương 73,7 tỷ VNĐ) từ hơn 9.000 tài khoản online tại ngân hàng Tesco Bank.

5. Mã độc tống tiền WannaCry lây lan diện rộng trên toàn thế giới

Được ghi nhận là vụ hack sử dụng phần mềm tống tiền lớn nhất lịch sử tại nhiều quốc gia, WannaCry đã khiến thế giới "chao đảo" trong gần một tuần vừa qua. Hacker đã đánh cắp công cụ này từ chính Cơ quan an ninh quốc gia Mỹ (NSA), sau đó sử dụng chúng với mục đích phát tán, kiếm tiền từ những người dùng bị lây nhiễm mã độc. Hệ quả là chỉ vài ngày sau đó, Quốc hội Mỹ đã họp và đưa ra một dự luật nhằm cấm chính phủ lưu giữ các vũ khí tấn công mạng tương tự.

6. Hacker đánh cắp 900GB dữ liệu quan trọng từ công ty giúp FBI hack iPhone



Vừa qua Cellebrite, công ty chuyên về giải mật của Israel - nổi tiếng sau vụ hack iPhone 5C giúp FBI trong khủng bố ở San Bernardino đã bị một nhóm hacker tấn công lấy đi 900GB dữ liệu từ ổ cứng và đe dọa sẽ công khai những thông tin này. Được biết, dữ liệu bị đánh cắp bao gồm: thông tin khách hàng, dữ liệu cơ sở và nhiều tài liệu kỹ thuật quan trọng miêu tả sản phẩm của công ty.

7. WikiLeaks công bố tài liệu chấn động về chương trình hack của CIA

WikiLeaks, trang web chuyên đăng tải những tài liệu bị rò rỉ từ chính phủ trên toàn thế giới, đã đăng tải hàng ngàn tài liệu được cho là tuyệt mật từ CIA hồi tháng 3, cho thấy cơ quan này có khả năng xâm nhập vào hầu như tất cả các thiết bị điện tử, từ smart TV, điện thoại di động đến xe tự lái... WikiLeaks cũng cáo buộc CIA có thể giải mã những nội dung được nhận và gửi qua các ứng dụng nhắn tin như WhatsApp, Signal, Telegram, Weibo, Confide và Cloakman bằng cách xâm nhập vào smartphone đang dùng các ứng dụng này.

8. DaFont bị hack, để lộ gần 700.000 tài khoản người dùng

DaFont.com - diễn đàn cung cấp phông chữ miễn phí nổi tiếng nhất trong tháng qua đã thông báo họ bị hacker truy cập vào cơ sở dữ liệu, đánh cắp được 699,464 tài khoản người dùng, đồng thời phá vỡ hơn 98% hệ thống mật khẩu của họ. Những thông tin bị đánh cắp bao gồm địa chỉ email, tất cả các tin nhắn cá nhân và dòng thảo luận của người dùng trên trang web.

9. Hơn 60 trường Đại học và các cơ quan Chính phủ Mỹ đã bị tấn công bởi mã độc malware

Nhiều trường học và cơ quan Chính phủ Mỹ bị tấn công bởi mã độc khai thác lỗ hổng SQL injection, cho phép hacker có quyền truy cập vào các thông tin nhạy cảm có giá trị để bán trên chợ đen (Black Market) của tội phạm mạng. Các tổ chức đã bị tấn công bao gồm Ủy ban Điều tiết Bưu chính, Cơ quan Dịch vụ và Nguồn lực Y tế, Bộ Gia cư và Phát triển Đô thị, và Cơ quan Khí quyển và Đại dương Quốc gia.

10. Hàng trăm ngàn tài khoản trên diễn đàn cảnh sát Mỹ bị đánh cắp

Vụ hack lịch sử từ năm 2015 đã lặp lại vào tháng 2/2017 khi một hacker tấn công vào PoliceOne - diễn đàn dành cho lực lượng cảnh sát Mỹ. Theo báo cáo, đã có hơn 715.000 tài khoản bị đánh cắp, bao gồm các thành viên đang làm tại FBI hay DHS. Các dữ liệu bị đánh cắp bao gồm tên người dùng, mật khẩu được mã hóa bằng thuật toán MD5, địa chỉ email, ngày sinh của những người dùng đăng ký làm thành viên của trang mạng.

II. HIỂU BIẾT VỀ CÁC CUỘC TẤN CÔNG MẠNG

Đối với các cuộc tấn công bằng việc khai thác các lỗ hổng, yêu cầu các hacker phải hiểu biết về các vấn đề bảo mật trên hệ điều hành hoặc các phần mềm và tận dụng kiến thức này để khai thác các lỗ hổng.

1. Tấn công bị động (Passive attack)

Trong một cuộc tấn công bị động, các hacker sẽ kiểm soát traffic không được mã hóa và tìm kiếm mật khẩu không được mã hóa (Clear Text password), các thông tin nhạy cảm có thể được sử dụng trong các kiểu tấn công khác. Các cuộc tấn công bị động bao gồm phân tích traffic, giám sát các cuộc giao tiếp không được bảo vệ, giải mã các traffic mã hóa yếu, và thu thập các thông tin xác thực như mật khẩu.

Các cuộc tấn công chặn bắt thông tin hệ thống mạng cho phép kẻ tấn công có thể xem xét các hành động tiếp theo. Kết quả của các cuộc tấn công bị động là các thông tin hoặc file dữ liệu sẽ bị rơi vào tay kẻ tấn công mà người dùng không hề hay biết.

2. Tấn công rải rác (Distributed attack)

Đối với các cuộc tấn công rải rác yêu cầu kẻ tấn công phải giới thiệu mã, chẳng hạn như một chương trình Trojan horse hoặc một chương trình back-door, với một thành phần "tin cậy" hoặc một phần mềm được phân phối cho nhiều công ty khác và tấn công user bằng cách tập trung vào việc sửa đổi các phần mềm độc hại của phần cứng hoặc phần mềm trong quá trình phân phối,... Các cuộc tấn công giới thiệu mã độc hại chẳng hạn như back door trên một sản phẩm nhằm mục đích truy cập trái phép các thông tin hoặc truy cập trái phép các chức năng trên hệ thống.

3. Tấn công nội bộ (Insider attack)

Các cuộc tấn công nội bộ (insider attack) liên quan đến người ở trong cuộc, chẳng hạn như một nhân viên nào đó "bất mãn" với công ty của mình,…các cuộc tấn công hệ thống mạng nội bộ có thể gây hại hoặc vô hại.

Người trong cuộc cố ý nghe trộm, ăn cắp hoặc phá hoại thông tin, sử dụng các thông tin một cách gian lận hoặc truy cập trái phép các thông tin.

4. Tấn công Phishing

Trong các cuộc tấn công phising, các hacker sẽ tạo ra một trang web giả trông "giống hệt" như các trang web phổ biến. Trong các phần tấn công phising, các hacker sẽ gửi một email để người dùng click vào đó và điều hướng đến trang web giả mạo. Khi người dùng đăng nhập thông tin tài khoản của họ, các hacker sẽ lưu lại tên người dùng và mật khẩu đó lại.

5. Các cuộc tấn công của không tặc (Hijack attack)

Trong các cuộc tấn công của không tặc, các hacker sẽ giành quyền kiểm soát và ngắt kết nối cuộc nói chuyện giữa bạn và một người khác.

6. Tấn công mật khẩu (Password attack)

Đối với các cuộc tấn công mật khẩu, các hacker sẽ cố gắng "phá" mật khẩu được lưu trữ trên cơ sở dữ liệu tài khoản hệ thống mạng hoặc mật khẩu bảo vệ các tập tin.

Các cuộc tấn công mật khẩu bao gồm 3 loại chính: các cuộc tấn công dạng từ điển (dictionary attack), brute-force attack và hybrid attack.

Cuộc tấn công dạng từ điển sử dụng danh sách các tập tin chứa các mật khẩu tiềm năng.

7. Khai thác lỗ hổng tấn công (Exploit attack)

Đối với các cuộc tấn công bằng việc khai thác các lỗ hổng, yêu cầu các hacker phải hiểu biết về các vấn đề bảo mật trên hệ điều hành hoặc các phần mềm và tận dụng kiến thức này để khai thác các lỗ hổng.

8. Buffer overflow (lỗi tràn bộ đệm)

Một cuộc tấn công buffer attack xảy ra khi các hacker gửi dữ liệu tới một ứng dụng nhiều hơn so với dự kiến. Và kết quả của cuộc tấn công buffer attack là các hacker tấn công truy cập quản trị hệ thống trên Command Prompt hoặc Shell.

9. Tấn công từ chối dịch vụ (denial of service attack)

Không giống như các cuộc tấn công mật khẩu (Password attack), các cuộc tấn công từ chối dịch vụ (denial of service attack) ngăn chặn việc sử dụng máy tính của bạn hoặc hệ thống mạng theo cách thông thường bằng valid users.

Sau khi tấn công, truy cập hệ thống mạng của bạn, các hacker có thể:

- Chặn traffic.

- Gửi các dữ liệu không hợp lý tới các ứng dụng hoặc các dịch vụ mạng, dẫn đến việc thông báo chấm dứt hoặc các hành vi bất thường trên các ứng dụng hoặc dịch vụ này.

- Lỗi tràn bộ nhớ đệm.

10. Tấn công theo kiểu Man-in-the-Middle Attack

Đúng như cái tên của nó, một cuộc tấn công theo kiểu Man-in-the-Middle Attack xảy ra khi cuộc nói chuyện giữa bạn và một người nào đó bị kẻ tấn công theo dõi, nắm bắt và kiểm soát thông tin liên lạc của bạn một cách minh bạch.

Các cuộc tấn công theo kiểu Man-in-the-Middle Attack giống như một người nào đó giả mạo danh tính để đọc các tin nhắn của bạn. Và người ở đầu kia tin rằng đó là bạn, bởi vì kẻ tấn công có thể trả lời một cách tích cực để trao đổi và thu thập thêm thông tin.

11. Tấn công phá mã khóa (Compromised-Key Attack)

Mã khóa ở đây là mã bí mật hoặc các con số quan trọng để "giải mã" các thông tin bảo mật. Mặc dù rất khó để có thể tấn công phá một mã khóa, nhưng với các hacker thì điều này là có thể. Sau khi các hacker có được một mã khóa, mã khóa này sẽ được gọi là mã khóa gây hại.

Hacker sử dụng mã khóa gây hại này để giành quyền truy cập các thông tin liên lạc mà không cần phải gửi hoặc nhận các giao thức tấn công. Với các mã khóa gây hại, các hacker có thể giải mã hoặc sửa đổi dữ liệu.

12. Tấn công trực tiếp

Những cuộc tấn công trực tiếp thông thường được sử dụng trong giai đoạn đầu để chiếm quyền truy nhập bên trong. Một phương pháp tấn công cổ điển là dò tìm tên người sử dụng và mật khẩu. Đây là phương pháp đơn giản, dễ thực hiện và không đòi hỏi một điều kiện đặc biệt nào để bắt đầu. Kẻ tấn công có thể sử dụng những thông tin như tên người dùng, ngày sinh, địa chỉ, số nhà vv.. để đoán mật khẩu. Trong trường hợp có được danh sách người sử dụng và những thông tin về môi trường làm việc, có một chương trình tự động hoá về việc dò tìm mật khẩu này.

Một chương trình có thể dễ dàng lấy được từ Internet để giải các mật khẩu đã mã hoá của hệ thống unix có tên là crack, có khả năng thử các tổ hợp các từ trong một từ điển lớn, theo những quy tắc do người dùng tự định nghĩa. Trong một số trường hợp, khả năng thành công của phương pháp này có thể lên tới 30%.

Phương pháp sử dụng các lỗi của chương trình ứng dụng và bản thân hệ điều hành đã được sử dụng từ những vụ tấn công đầu tiên và vẫn được tiếp tục để chiếm quyền truy nhập. Trong một số trường hợp phương pháp này cho phép kẻ tấn công có được quyền của người quản trị hệ thống (root hay administrator).

Hai ví dụ thường xuyên được đưa ra để minh hoạ cho phương pháp này là ví dụ với chương trình sendmail và chương trình rlogin của hệ điều hành UNIX.

Sendmail là một chương trình phức tạp, với mã nguồn bao gồm hàng ngàn dòng lệnh của ngôn ngữ C. Sendmail được chạy với quyền ưu tiên của người quản trị hệ thống, do chương trình phải có quyền ghi vào hộp thư của những người sử dụng máy. Và Sendmail trực tiếp nhận các yêu cầu về thư tín trên mạng bên ngoài. Đây chính là những yếu tố làm cho sendmail trở thành một nguồn cung cấp những lỗ hổng về bảo mật để truy nhập hệ thống.

Rlogin cho phép người sử dụng từ một máy trên mạng truy nhập từ xa vào một máy khác sử dụng tài nguyên của máy này. Trong quá trình nhận tên và mật khẩu của người sử dụng, rlogin không kiểm tra độ dài của dòng nhập, do đó kẻ tấn công có thể đưa vào một xâu đã được tính toán trước để ghi đè lên mã chương trình của rlogin, qua đó chiếm được quyền truy nhập.

13. Nghe trộm

Việc nghe trộm thông tin trên mạng có thể đưa lại những thông tin có ích như tên, mật khẩu của người sử dụng, các thông tin mật chuyển qua mạng. Việc nghe trộm thường được tiến hành ngay sau khi kẻ tấn công đã chiếm được quyền truy nhập hệ thống, thông qua các chương trình cho phép đưa card giao tiếp mạng (Network Interface Card-NIC) vào chế độ nhận toàn bộ các thông tin lưu truyền trên mạng. Những thông tin này cũng có thể dễ dàng lấy được trên Internet.

14. Giả mạo địa chỉ

Việc giả mạo địa chỉ IP có thể được thực hiện thông qua việc sử dụng khả năng dẫn đường trực tiếp (source-routing). Với cách tấn công này, kẻ tấn công gửi các gói tin IP tới mạng bên trong với một địa chỉ IP giả mạo (thông thường là địa chỉ của một mạng hoặc một máy được coi là an toàn đối với mạng bên trong), đồng thời chỉ rõ đường dẫn mà các gói tin IP phải gửi đi.

15. Vô hiệu các chức năng của hệ thống

Đây là kiểu tấn công nhằm tê liệt hệ thống, không cho nó thực hiện chức năng mà nó thiết kế. Kiểu tấn công này không thể ngăn chặn được, do những phương tiện được tổ chức tấn công cũng chính là các phương tiện để làm việc và truy nhập thông tin trên mạng.

Ví dụ sử dụng lệnh ping với tốc độ cao nhất có thể, buộc một hệ thống tiêu hao toàn bộ tốc độ tính toán và khả năng của mạng để trả lời các lệnh này, không còn các tài nguyên để thực hiện những công việc có ích khác.

16. Lỗi của người quản trị hệ thống

Đây không phải là một kiểu tấn công của những kẻ đột nhập, tuy nhiên lỗi của người quản trị hệ thống thường tạo ra những lỗ hổng cho phép kẻ tấn công sử dụng để truy nhập vào mạng nội bộ.

17. Tấn công vào yếu tố con người

Kẻ tấn công có thể liên lạc với một người quản trị hệ thống, giả làm một người sử dụng để yêu cầu thay đổi mật khẩu, thay đổi quyền truy nhập của mình đối với hệ thống, hoặc thậm chí thay đổi một số cấu hình của hệ thống để thực hiện các phương pháp tấn công khác.

Với kiểu tấn công này không một thiết bị nào có thể ngăn chặn một cách hữu hiệu, và chỉ có một cách giáo dục người sử dụng mạng nội bộ về những yêu cầu bảo mật để đề cao cảnh giác với những hiện tượng đáng nghi.

Nói chung yếu tố con người là một điểm yếu trong bất kỳ một hệ thống bảo vệ nào, và chỉ có sự giáo dục cộng với tinh thần hợp tác từ phía người sử dụng có thể nâng cao được độ an toàn của hệ thống bảo vệ.

PHẦN B: TẤN CÔNG TỪ CHỐI DỊCH VỤ

I. Dos attack là gì ?

Dos là gì ?

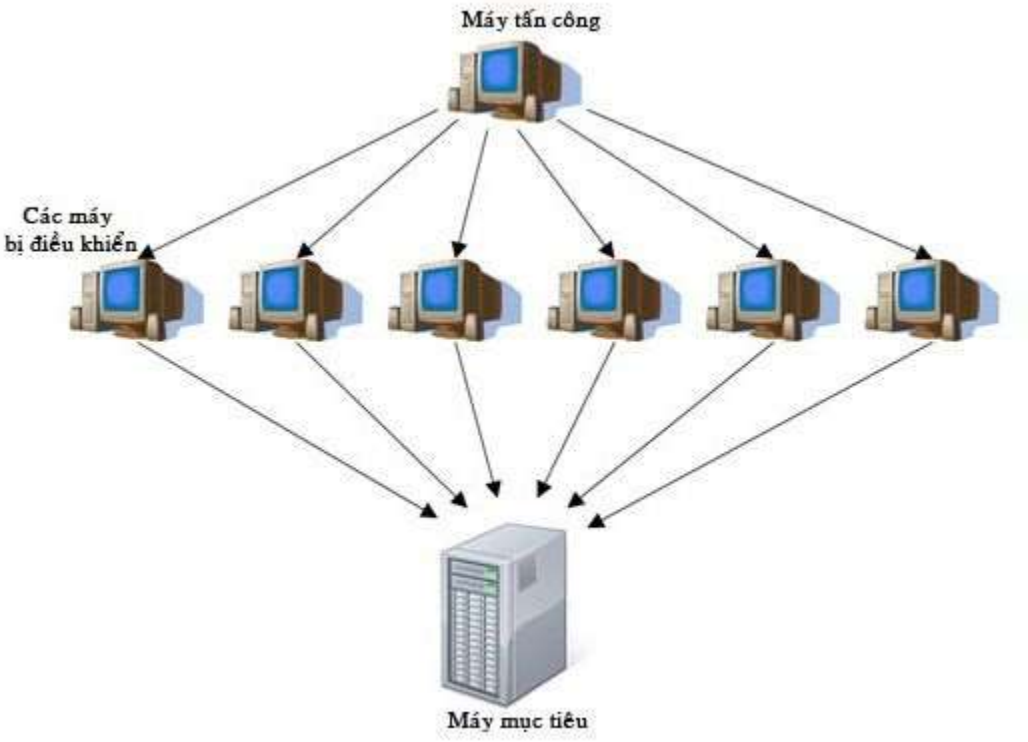
Dos có tên đầy đủ là Denial Of Service – là một hình thức tấn công từ chối dịch vụ. Đây là hình thức tấn công khá phổ biến, nó khiến cho máy tính mục tiêu không thể xử lý kịp các tác vụ và dẫn đến quá tải => die là điều tất yếu. Các cuộc tấn công DOS này thường nhắm vào các máy chủ ảo (VPS) hay Web Server của ngân hàng, tài chính hay là các trang thương mại điện tử…..
Tấn công DOS thường chỉ được tấn công từ một địa điểm duy nhất, tức là nó sẽ xuất phát tại một điểm và chỉ có một dải IP thôi => bạn có thể phát hiện và ngăn chặn được.

Một số kiểu tấn công Dos mà hacker vẫn thường dùng đó là :

1. SYN Flood Attack
2. Ping Flood Attack
3. Teardrop Attack
4. Peer-to-Peer Attacks

DDos là gì ?

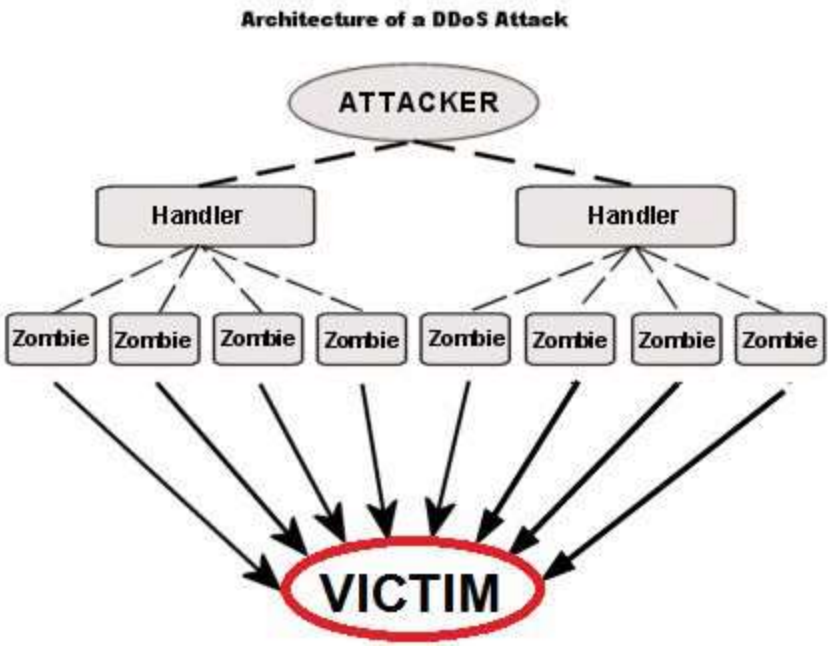
Ddos có tên đầy đủ là Distributed Denial Of Service – là một biến thể của loại tấn công DOS. Đây là một hình thức tấn công từ chối dịch vụ phân tán, nó làm cho người bị tấn công không thể sử dụng một dịch vụ nào đó, nó có thể khiến bạn không thể kết nối với một dịch vụ internet, hoặc nó có thể làm ngưng hoạt động của một chiếc máy tính, một mạng lan nội bộ hoặc thậm chí là cả một hệ thống mạng.
ấn công DDOS mạnh hơn DOS rất nhiều, điểm mạnh của hình thức này đó là nó được phân tán từ nhiều dải IP khác nhau, chính vì thế người bị tấn công sẽ rất khó phát hiện để ngăn chặn được.



Kẻ tấn công (Hacker) không chỉ sử dụng máy tính của họ để thực hiện một cuộc tấn công vào một trang web hay một hệ thống mạng nào đó, mà họ còn lợi dùng hàng triệu máy tính khác để thực hiện việc này.

Tại sau họ lại có thể điều được hàng triệu máy tính trên khắp thế giới ?

Nguyên nhân là do rất nhiều người đang dùng các phần mềm Crack, hay phần mềm lậu được chia sẻ tràn lan trên mạng bị chèn mã độc, virus….



Một số kiểu tấn công DDos mà hacker vẫn hay sử dụng đó là:

1. Đánh vào băng thông (Bandwidth).
2. Tấn công vào Giao thức.
3. Tấn công bằng cách gói tin bất thường.
4. Tấn công qua phần mềm trung gian.
5. Các công cụ tấn công dùng Proxy ví dụ như: Trinoo, Flood Network (TFN), Trinity, Knight, Kaiten, MASTER HTTP, LOIC, DDOS UDP, DOS ProC5, SYN-Flood-DOS…..

Làm thế nào để biết bạn đang bị tấn công DDOS ?

Một số cách nhận biết về một cuộc tấn công từ chối dịch vụ đó là:

- Mạng chậm một cách bất thường khi bạn mở file hoặc một website/ blog nào đó.
- Bạn không thể truy cập được vào một trang web/blog nào đó.
- Hoặc là bạn không thể truy cập vào được một trang web/blog nào cả.
- Lượng thư rác tăng đột biến.

Mục đích tấn công DOS hay DDOS của hacker là gì ?

- Làm tiêu tốn tài nguyên của hệ thống, có thể làm hết băng thông, đầy dung lượng lưu trữ trên đĩa hoặc tăng thời gian xử lý.
- Phá vỡ các thành phần vật lý của mạng máy tính.
- Làm tắc nghẽn thông tin liên lạc ra bên ngoài.
- Phá vỡ các thông tin cấu hình như thông tin định tuyến
- Phá vỡ các trạng thái thông tin như việc tự động reset lại các phiên TCP.
- Làm quá tải năng lực xử lý, dẫn đến hệ thống không thể thực thi bất kì một công việc nào khác.

- Những lỗi gọi tức thì trong microcode của máy tính.
- Những lỗi gọi tức thì trong chuỗi chỉ thị, dẫn đến máy tính rơi vào trạng thái hoạt động không ổn định hoặc bị đơ.
- Những lỗi có thể khai thác được ở hệ điều hành dẫn đến việc thiếu thốn tài nguyên hoặc bị thrashing. Ví dụ như sử dụng tất cả các năng lực có sẵn dẫn đến không một công việc thực tế nào có thể hoàn thành được.
- Gây crash hệ thống.
- Tấn công từ chối dịch vụ iFrame: Trong một trang HTML có thể gọi đến một trang web nào đó với rất nhiều yêu cầu và trong rất nhiều lần cho đến khi băng thông của trang web đó bị quá hạn.

=> Nói tóm lại Dos hay DDOS là một cuộc tấn công, làm quá tải tài nguyên hệ thống, làm nghẽn đường truyền… dẫn tới việc gián đoạn hoặc là hệ thống đó bị treo luôn và không thể sử dụng được.

Node: Ddos – tấn công từ chối dịch vụ là một việc làm vi phạm phát luật, vi phạm chính sách sử dụng internet của LAB (Internet Architecture Board). Chính vì vậy, đối với các cuộc tấn công Ddos lớn, mà người tấn công bị phát hiện có thể sẽ bị bóc lịch lâu dài.

Ngăn chặn các cuộc tấn công DDOS như thế nào ?
Thông thường, khi bị DDOS thì các các chủ website/blog sẽ tìm cách để biết được các địa chỉ IP có lượt truy cập tăng bất thường => sau đó sẽ cho chúng vào danh sách đen (Blacklist) để ngăn chặn chúng kịp thời, tránh làm nghẽn mạng.
Ngoài ra, để bảo mật hơn thì các hệ thống còn có thể sử dụng tường lửa (Firewall) để phòng chống và hạn chế các cuộc tấn công, cũng như hạn chế được sức mạnh thực của nó

đó là đối với các cuộc tấn công mạng với quy mô nhỏ hacker thực tập đang thử nghiệm , test Tools … thì chúng ta còn có thể ngăn chặn được, chứ thực tế là KHÔNG THỂ ngăn cản đối với các cao thủ hoặc một cuộc tấn công với quy mô lớn.

vụ Google Việt Nam bị DDos vào ngày 23 tháng 2 năm 2015 chứ. Đến một hệ thống lớn như vậy mà hacker còn có thể đánh sập được huống chi mấy trang web cỏn con ở trong nước. Việc hacker tấn công DDOS được Google Việt Nam chứng tỏ hacker có thể tấn công vào bất cứ trang web nào mà họ muốn.

Hoặc nói không đâu xa đó là vụ hệ thống web của công ty VCCorp cũng bị đánh sập khiến nhiều trang lớn như *dantri.com.vn, genk.vn, muachung*… không thể truy cập được – và kết luận cuối cùng đó là do hacker đã lợi dụng, cài phần mềm gián điệp vào phần mềm Adobe Flash Player. Và gần đây nhất đó là hệ thống của Netlink, các trang báo lớn như *nguoiduatin.vn, doisongphapluat.com, techz.vn, tinmoi.vn*… cũng bị đánh sập hoàn toàn, phải mất mấy hôm thì hệ thống mới có thể hoạt động trở lại được.

vụ của hãng VietnamAirlines nữa chứ… đây thực sự là một vụ tấn công cực kỳ nguy hiểm, hacker đã có thể chiếm quyền điều khiển toàn bộ hệ thống, phát tán các clip S.E.X tại sân bay, tuyên truyền phản động, chủ quyền biển đảo, làm nhục đất nước chúng ta…. nếu muốn biết thêm thông tin thì tra Google về vụ này nhé. Theo một số nguồn phân tích thì nguyên nhân là do một số máy tính của hệ thống sử dụng Microsoft Office bản Crack

=> Để tránh biến máy tính của bạn thành các botnet hay các zoombie thì ngay từ bây giờ hãy hạn chế sử dụng các phần mềm crack và cài đặt phần mềm diệt virut cho máy tính.

II. CÁC KỸ THUẬT TẤN CÔNG DOS

SYN Flood:

SYN Flood khai thác điểm yếu trong chuỗi kết nối TCP, được gọi là bắt tay ba chiều. Máy chủ sẽ nhận được một thông điệp đồng bộ (SYN) để bắt đầu "bắt tay". Máy chủ nhận tin nhắn bằng cách gửi cờ báo nhận (ACK) tới máy lưu trữ ban đầu, sau đó đóng kết nối. Tuy nhiên, trong một SYN Flood, tin nhắn giả mạo được gửi đi và kết nối không đóng => dịch vụ sập.

UDP Flood:

User Datagram Protocol (UDP) là một giao thức mạng không session. Một UDP Flood nhắm đến các cổng ngẫu nhiên trên máy tính hoặc mạng với các gói tin UDP. Máy chủ kiểm tra ứng dụng tại các cổng đó nhưng không tìm thấy ứng dụng nào.

HTTP Flood:
HTTP Flood gần giống như các yêu cầu GET hoặc POST hợp pháp được khai thác bởi một hacker. Nó sử dụng ít băng thông hơn các loại tấn công khác nhưng nó có thể buộc máy chủ sử dụng các nguồn lực tối đa.
Ping of Death:

Ping of Death điều khiển các giao thức IP bằng cách gửi những đoạn mã độc đến một hệ thống. Đây là loại DDoS phổ biến cách đây hai thập kỷ nhưng đã không còn hiệu quả vào thời điểm hiện tại.

Smurf Attack:
Smurf Attack khai thác giao thức Internet (IP) và ICMP (Internet Control Message Protocol) sử dụng một chương trình phần mềm độc hại gọi là smurf. Nó giả mạo một địa chỉ IP và sử dụng ICMP, sau đó ping các địa chỉ IP trên một mạng nhất định.
Fraggle Attack:

Fraggle Attack sử dụng một lượng lớn lưu lượng UDP vào mạng phát sóng của router. Nó giống như một cuộc tấn công Smurf, sử dụng UDP nhiều hơn là ICMP.

Slowloris:

Slowloris cho phép kẻ tấn công sử dụng nguồn lực tối thiểu trong một cuộc tấn công và các mục tiêu trên máy chủ web. Khi đã kết nối với mục tiêu mong muốn, Slowloris giữ liên kết đó mở

càng lâu càng tốt với HTTP tràn ngập. Kiểu tấn công này đã được sử dụng trong một số DDoSing kiểu hacktivist (tấn công vì mục tiêu chính trị) cao cấp, bao gồm cuộc bầu cử tổng thống Iran năm 2009. Việc giảm thiểu ảnh hưởng với loại hình tấn công này là rất khó khăn.

Application Level Attacks:

Application Level Attacks khai thác lỗ hổng trong các ứng dụng. Mục tiêu của loại tấn công này không phải là toàn bộ máy chủ, mà là các ứng dụng với những điểm yếu được biết đến.

NTP Amplification:

NTPAmplification khai thác các máy chủ NTP (Network Time Protocol), một giao thức được sử dụng để đồng bộ thời gian mạng, làm tràn ngập lưu lượng UDP. Đây là reflection attack bị khuếch đại. Trong reflection attack bất kỳ nào đều sẽ có phản hồi từ máy chủ đến IP giả mạo, khi bị khuếch đại, thì phản hồi từ máy chủ sẽ không còn tương xứng với yêu cầu ban đầu. Vì sử dụng băng thông lớn khi bị DDoS nên loại tấn công này có tính phá hoại và volumne cao.

Advanced Persistent DoS (APDoS):

Advanced Persistent DoS (APDoS) là một loại tấn công được sử dụng bởi hacker với mong muốn gây ra những thiệt hại nghiêm trọng. Nó sử dụng nhiều kiểu tấn công được đề cập trước đó HTTP Flood, SYN Flood, v.v...) và thường nhắm tấn công theo kiểu gửi hàng triệu yêu cầu/giây. Các cuộc tấn công của APDoS có thể kéo dài hàng tuần, phụ thuộc vào khả năng của hacker để chuyển đổi các chiến thuật bất cứ lúc nào và tạo ra sự đa dạng để tránh các bảo vệ an ninh.

Zero-day DDoS Attacks:

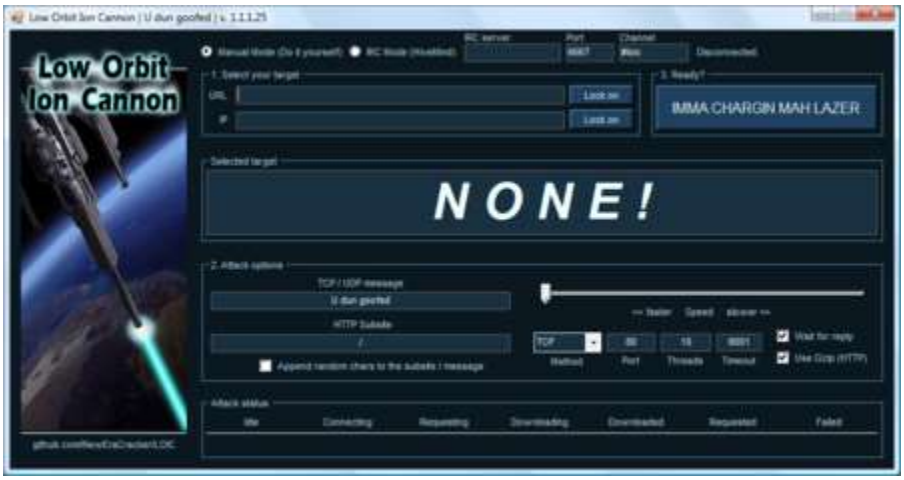
Zero-day DDoS Attacks là tên được đặt cho các phương pháp tấn công DDoS mới, khai thác các lỗ hổng chưa được vá.

III. MỘT SỐ CÔNG CỤ (TOOLS) DÙNG ĐỂ TẤN CÔNG DOS- DDOS

1. LOIC (Low Orbit Ion Canon)

LOIC là một trong những công cụ tấn công DOS phổ biến nhất có sẵn trên Internet. Công cụ này đã được sử dụng bởi nhóm tin tặc nổi tiếng Anonymous chống lại nhiều mạng của các công ty lớn vào năm ngoái. Anonymous đã không chỉ sử dụng công cụ này, mà còn yêu cầu người dùng Internet tham gia tấn công DDOS của họ thông qua IRC.

Nó có thể được sử dụng đơn giản bởi một người dùng duy nhất để thực hiện một cuộc tấn công DOS trên các máy chủ nhỏ. Công cụ này thực sự dễ sử dụng, ngay cả đối với người mới bắt đầu. Công cụ này thực hiện một cuộc tấn công DOS bằng cách gửi các yêu cầu UDP, TCP hoặc HTTP đến máy chủ nạn nhân. Bạn chỉ cần biết địa chỉ IP của máy chủ và công cụ sẽ thực hiện phần còn lại.



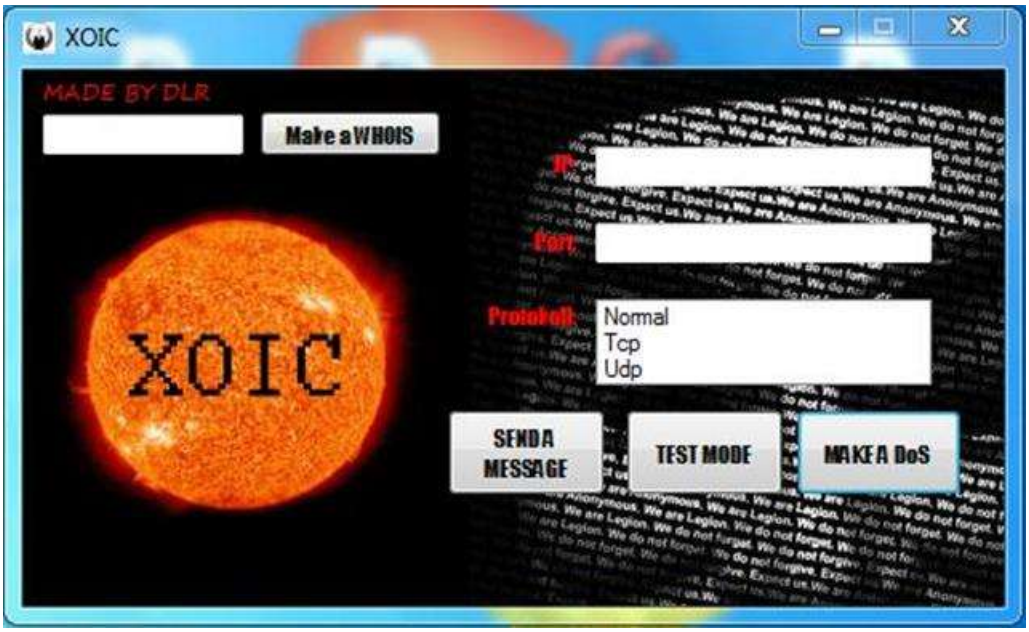
Bạn có thể xem ảnh chụp nhanh của công cụ ở trên. Nhập URL hoặc địa chỉ IP và sau đó chọn các tham số tấn công. Nếu bạn không chắc chắn, bạn có thể để mặc định. Khi bạn làm xong mọi thứ, hãy nhấp vào nút lớn nói "IMMA CHARGIN MAH LAZER" và nó sẽ bắt đầu tấn công trên máy chủ đích. Trong một vài giây, bạn sẽ thấy rằng trang web đã ngừng đáp ứng các yêu cầu của bạn.

Công cụ này cũng có chế độ HIVEMIND. Nó cho phép kẻ tấn công kiểm soát các hệ thống LOIC từ xa để thực hiện một cuộc tấn công DDOS. Tính năng này được sử dụng để kiểm soát tất cả các máy tính khác trong mạng zombie của bạn. Công cụ này có thể được sử dụng cho cả các cuộc tấn công DOS và các cuộc tấn công DDOS vào bất kỳ trang web hoặc máy chủ nào.

Điều quan trọng nhất bạn nên biết là LOIC không làm gì để ẩn địa chỉ IP của bạn. Nếu bạn đang có kế hoạch sử dụng LOIC để thực hiện một cuộc tấn công DOS, hãy nghĩ lại. Sử dụng proxy sẽ không giúp bạn vì nó sẽ nhấn máy chủ proxy chứ không phải máy chủ mục tiêu. Vì vậy, bằng cách sử dụng công cụ này chống lại một máy chủ có thể tạo ra một rắc rối cho bạn.

2. XOIC

XOIC là một công cụ tấn công DOS tốt đẹp khác. Nó thực hiện một cuộc tấn công DOS một máy chủ bất kỳ với một địa chỉ IP, một cổng do người dùng lựa chọn, và một giao thức người dùng lựa chọn. Các nhà phát triển XOIC cho rằng XOIC mạnh hơn LOIC theo nhiều cách. Giống như LOIC, nó đi kèm với một GUI dễ sử dụng, vì vậy người mới bắt đầu có thể dễ dàng sử dụng công cụ này để thực hiện các cuộc tấn công trên các trang web hoặc máy chủ khác.



Nói chung, công cụ này đi kèm với ba chế độ tấn công. Việc đầu tiên, được gọi là chế độ thử nghiệm, là rất cơ bản. Thứ hai là chế độ tấn công DOS bình thường. Cái cuối cùng là chế độ tấn công DOS đi kèm với thông báo TCP / HTTP / UDP / ICMP.

Nó là một công cụ hiệu quả và có thể được sử dụng chống lại các trang web nhỏ. Không bao giờ thử nó với trang web của riêng bạn. Bạn có thể sẽ làm hỏng máy chủ của trang web của riêng bạn.

Tải xuống XOIC: http://sourceforge.net/projects/xoic/

3. HULK (HTTP tải không thể chịu được King)

HULK là một công cụ tấn công DOS tốt đẹp khác, tạo ra một yêu cầu duy nhất cho mỗi và mọi yêu cầu được tạo ra để lưu lượng truy cập bị xáo trộn tại một máy chủ web. Công cụ này sử dụng nhiều kỹ thuật khác để tránh phát hiện tấn công thông qua các mẫu đã biết.

Nó có một danh sách các tác nhân người dùng đã biết để sử dụng ngẫu nhiên với các yêu cầu. Nó cũng sử dụng giả mạo tham chiếu và nó có thể bỏ qua các công cụ lưu bộ nhớ đệm, do đó nó trực tiếp truy cập vào nhóm tài nguyên của máy chủ.

Nhà phát triển của công cụ đã thử nghiệm nó trên một máy chủ web IIS 7 với RAM 4 GB. Công cụ này đã đưa máy chủ xuống dưới một phút.

Tải xuống HULK tại đây: http://packetstormsecurity.com/files/112856/HULK-Http-Unbearable-Load-King.html

4. DDOSIM — Trình mô phỏng DDOS Lớp 7

DDOSIM là một công cụ tấn công DOS phổ biến khác. Như tên cho thấy, nó được sử dụng để thực hiện các cuộc tấn công DDOS bằng cách mô phỏng một số máy chủ zombie. Tất cả các máy chủ zombie tạo kết nối TCP đầy đủ đến máy chủ đích.

Công cụ này được viết bằng C ++ và chạy trên các hệ thống Linux.

Đây là những tính năng chính của DDOSIM

Mô phỏng một số zombie trong tấn công

Địa chỉ IP ngẫu nhiên

Các cuộc tấn công dựa trên kết nối TCP

Các cuộc tấn công DDOS lớp ứng dụng

HTTP DDoS với các yêu cầu hợp lệ

HTTP DDoS với các yêu cầu không hợp lệ (tương tự như tấn công DC ++)

DDoS SMTP

TCP kết nối lũ trên cổng ngẫu nhiên

Tải xuống DDOSIM tại đây: http://sourceforge.net/projects/ddosim/

Đọc thêm về công cụ này tại đây: http://stormsecurity.wordpress.com/2009/03/03/application-layer-ddos-simulator/

5. R-U-Dead-Yet

R-U-Dead-Yet là một công cụ tấn công HTTP post DOS. Nói tóm lại, nó còn được gọi là RUDY. Nó thực hiện một cuộc tấn công DOS với một trình biểu mẫu trường dài thông qua phương thức POST. Công cụ này đi kèm với một menu giao diện điều khiển tương tác. Nó phát hiện các biểu mẫu trên một URL nhất định và cho phép người dùng chọn các biểu mẫu và trường nào sẽ được sử dụng cho một cuộc tấn công DOS dựa trên POST.

Tải xuống RUDY: https://code.google.com/p/r-u-dead-yet/

6. Tor's Hammer

Tor's Hammer là một công cụ kiểm tra DOS tốt đẹp khác. Nó là một công cụ viết chậm được viết bằng Python. Công cụ này có thêm một lợi thế: Nó có thể được chạy qua một mạng TOR để ẩn danh trong khi thực hiện tấn công. Nó là một công cụ hiệu quả có thể giết chết các máy chủ Apache hoặc IIS trong vài giây.

Tải xuống TOR's Hammer tại đây: http://packetstormsecurity.com/files/98831/

7. PyLoris

PyLoris được cho là một công cụ kiểm tra cho các máy chủ. Nó có thể được sử dụng để thực hiện các cuộc tấn công DOS trên một dịch vụ. Công cụ này có thể sử dụng các proxy SOCKS và các kết nối SSL để thực hiện một cuộc tấn công DOS trên một máy chủ. Nó có thể nhắm mục tiêu các giao thức khác nhau, bao gồm HTTP, FTP, SMTP, IMAP và Telnet. Phiên bản mới nhất của công cụ này đi kèm với GUI đơn giản và dễ sử dụng. Không giống như các công cụ tấn công DOS truyền thống khác, công cụ này trực tiếp truy cập dịch vụ.

Tải xuống PyLoris: http://sourceforge.net/projects/pyloris/

8. POST HTTP của OWASP DOS

Nó là một công cụ tốt để thực hiện các cuộc tấn công DOS. Bạn có thể sử dụng công cụ này để kiểm tra xem máy chủ web của bạn có thể bảo vệ tấn công DOS hay không. Không chỉ để bảo vệ, nó cũng có thể được sử dụng để thực hiện các cuộc tấn công DOS chống lại một trang web.

Tải xuống tại đây: https://code.google.com/p/owasp-dos-http-post/

9. DAVOSET

DAVOSET là một công cụ tốt để thực hiện các cuộc tấn công DDOS. Phiên bản mới nhất của công cụ này đã thêm hỗ trợ cho cookie cùng với nhiều tính năng khác. Bạn có thể tải xuống DAVOSET miễn phí từ Packetstormsecurity.

Tải xuống DavoSET: http://packetstormsecurity.com/files/123084/DAVOSET-1.1.3.html

10. GoldenEye HTTP từ chối dịch vụ công cụ

GoldenEye cũng là một công cụ tấn công DOS đơn giản nhưng hiệu quả. Nó được phát triển bằng Python để thử nghiệm các cuộc tấn công DOS, nhưng mọi người cũng sử dụng nó như một công cụ hack.

Tải xuống GoldenEye: http://packetstormsecurity.com/files/120966/GoldenEye-HTTP-Denial-Of-Service-Tool.html

Phát hiện và ngăn chặn tấn công từ chối dịch vụ

Một cuộc tấn công DOS là rất nguy hiểm cho một tổ chức, vì vậy điều quan trọng là phải biết và có một thiết lập để ngăn chặn một. Các biện pháp phòng chống các cuộc tấn công DOS liên quan đến việc phát hiện và sau đó chặn lưu lượng giả mạo. Một cuộc tấn công phức tạp hơn là khó ngăn chặn. Nhưng có một vài phương pháp mà chúng ta có thể sử dụng để chặn tấn công DOS bình thường. Cách dễ nhất là sử dụng tường lửa với các quy tắc cho phép và từ chối. Trong trường hợp đơn giản, các cuộc tấn công đến từ một số lượng nhỏ địa chỉ IP, vì vậy bạn có thể phát hiện các địa chỉ IP đó và sau đó thêm một quy tắc chặn trong tường lửa.

Nhưng phương pháp này sẽ thất bại trong một số trường hợp. Chúng ta biết rằng một bức tường lửa đến ở một mức độ rất sâu bên trong hệ thống phân cấp mạng, do đó một lượng lớn lưu lượng có thể ảnh hưởng đến bộ định tuyến trước khi đến tường lửa.

Blackholing và sinkholing là các phương pháp mới hơn. Blackholing phát hiện lưu lượng truy cập tấn công giả mạo và gửi nó đến một lỗ đen. Sinkholing định tuyến tất cả lưu lượng truy cập đến địa chỉ IP hợp lệ nơi lưu lượng truy cập được phân tích. Ở đây, nó từ chối các gói tin trở lại.

Ống sạch là một phương pháp xử lý DOS gần đây. Trong phương pháp này, tất cả lưu lượng truy cập được chuyển qua một trung tâm làm sạch, ở đó, các phương pháp khác nhau được thực hiện để lọc lưu lượng truy cập ngược lại. Tata Communications, Verisign, và AT & T là những nhà cung cấp chính của loại hình bảo vệ này.

Là người dùng Internet, bạn cũng nên chăm sóc hệ thống của mình. Tin tặc có thể sử dụng hệ thống của bạn như một phần của mạng lưới zombie của họ. Vì vậy, luôn cố gắng bảo vệ hệ thống của bạn. Luôn cập nhật hệ thống của bạn với các bản vá lỗi mới nhất. Cài đặt một giải pháp diệt virus tốt. Luôn chú ý khi cài đặt phần mềm. Không bao giờ tải xuống phần mềm từ các nguồn không đáng tin cậy hoặc không xác định. Nhiều trang web phục vụ phần mềm độc hại để cài đặt Trojans trong hệ thống người dùng vô tội.

Phần kết luận

Trong bài này, chúng tôi đã tìm hiểu về tấn công từ chối dịch vụ và các công cụ được sử dụng để thực hiện tấn công. Các cuộc tấn công DOS được sử dụng để sụp đổ máy chủ và dịch vụ gián đoạn. Sony đã phải đối mặt với cuộc tấn công này trong một thời gian dài và mất hàng triệu đô la. Đó là một bài học lớn cho các công ty khác dựa vào thu nhập dựa trên máy chủ. Mỗi máy chủ nên thiết lập một cách để phát hiện và chặn các cuộc tấn công DDOS. Tính khả dụng của các công cụ miễn phí giúp dễ dàng thực hiện tấn công DOS đối với trang web hoặc máy chủ. Mặc dù hầu hết các công cụ này chỉ dành cho các cuộc tấn công DOS, một vài công cụ hỗ trợ mạng

zombie cho các cuộc tấn công DDOS. LOIC là công cụ tấn công DOS được sử dụng phổ biến nhất và phổ biến nhất. Trong vài năm qua, nó đã được sử dụng nhiều lần bởi tin tặc chống lại mạng của công ty lớn, vì vậy chúng tôi không bao giờ có thể phủ nhận khả năng tấn công.

Vì vậy, mỗi công ty nên chăm sóc nó và thiết lập mức độ bảo vệ tốt chống lại tấn công DOS.

PHẦN C: CÁCH PHÒNG CHỐNG DOS (DDOS)

I. NHỮNG BIỆN PHÁP ĐỐI PHÓ DOS - DDOS

Cách đơn giản hiệu quả mà chúng tôi thực hiện là ngắt kết nối máy nạn nhân khỏi mạng BootNet của tin tặc. TABATECH.VN chia thành 3 nhóm giải pháp chống tấn công DOS (DDOS):

Phòng chống DOS (DDOS) theo thời điểm xử lý tấn công
– Thời điểm trước khi xảy ra tấn công: Tại các bước này thực hiện các công việc về phòng vệ, ngăn chặn các cuộc tấn công có thể xảy ra. Các bước thực hiện đó là:

- Rào chính sách bảo mật chặt chẽ.
- Cập nhật hệ thống và vá lỗ hổng thường xuyên.
- Có hệ thống theo dõi realtime bất thường xảy ra trong hệ thống và cảnh báo khi có sự cố.

– Thời điểm trong khi bị tấn công
Các công việc ở bước này là phát hiện, nhận dạng và ngăn chặn tấn công càng nhanh càng tốt để dịch vụ vẫn hoạt động được.
– Thời điểm sau khi xảy ra tấn công
Đây là các bước thực hiện sau khi cuộc tấn công đã xảy ra, bao gồm lần dấu vết và truy tìm nguồn gốc cuộc tấn công. Cần truy tìm theo log ghi nhận được để phân tích và ngăn chặn các cuộc tấn công tiềm ẩn có thể xảy ra sắp tới.
Phòng chống DOS (DDOS) theo vị trí triển khai
Phòng chống DOS (DDOS) theo giao thức mạng
Phòng chống DDoS tại tầng TCP

- Lọc gói tin dựa theo địa chỉ IP, theo các chính sách đã được thiết lập sẵn.
- Tăng Backlogs size để tăng khả năng chấp nhận kết nối mới của hệ thống máy đích.
- Giảm thời gian chờ nhận gói tin xác thực kết nối TCP-ACK, giúp máy chủ hủy bỏ các kết nối không được xác thực trong khoảng thời gian ngắn, điều này giúp giải phóng lượng tài nguyên đang bị chiếm dữ của các kết nối ko tin cậy.
- SYN Flood là một dạng tấn công từ chối dịch vụ dựa theo giao thức TCP thường gặp, để chặn được hiệu quả có thể dùng cách sử dụng SYN Cookies với mục đích chỉ cấp tài nguyên cho những yêu cầu hợp lệ.

Phòng chống DDoS tại tầng ứng dụng

- Giới hạn tối thiểu các hành vi truy cập, ví dụ như giới hạn kết nối đồng thời truy cập từ 1 IP hay giới hạn tỷ lệ kết nối không quá 100 request trong 1 phút. Nếu quá ngưỡng này truy cập sẽ bị block.
- Coi log trong Log ứng dụng là công cụ chính để rà soát các bất thường, hành vi rà quét.

Kết luận:
DOS (DDOS) là dạng tấn công mạng nguy hiểm, hiện chưa có giải pháp tổng quát cụ thể nào để phòng chống tấn công DOS (DDOS) do tính phức tạp tinh vi của chúng. Vì vậy ngay từ bây giờ chúng ta nên rào chính sách bảo mật chặt chẽ trên hệ thống của mình, hãy nhớ "phòng hơn chống", hãy là người chủ động trước sự phá hoại của tin tặc.
Tùy vào tính huống kẻ tấn công thực hiện để lên phương án phòng chống, kiểm tra xem chúng

đánh vào tầng nào (TCP, Application,..), đánh theo cơ chế nào từ đó xem hệ thống chúng ta có lỗ hổng gì không, chắc chắn sẽ có cách thích hợp để xử lý chúng.

II. CÔNG CỤ PHÒNG CHỐNG

5 công cụ phòng chống tấn công DDoS để bảo vệ công ty của bạn

1.Cloudflare

Bảo vệ lớp 3 và 4 của Cloudfare hấp thụ một cuộc tấn công trước khi nó đến một máy chủ, bộ cân bằng tải, tường lửa và bộ định tuyến nào không.

Bảo vệ lớp 7 của nó phân biệt giữa lưu lượng có lợi và có hại. Khách hàng của Cloudflare bao gồm Cisco, Nasdaq, MIT và… cuộc thi bài hát Eurovision.

2. Mạng F5

Mạng F5 Silverline có khả năng lọc lưu lượng truy cập lớn và cung cấp sự bảo vệ ngay tại chỗ, trên đám mây hoặc kết hợp cả hai.

Nó cung cấp bảo vệ trên các cấp 3 đến 7. Silverline có thể ngăn chặn các mạng có khối lượng lớn, ngăn chặn chúng tiếp cận mạng của công ty. Hỗ trợ 24/7 có sẵn.

3. Hoa sen đen

Dịch vụ Bảo vệ mạng của công ty được thiết kế tập trung vào ngành công nghiệp lưu trữ và có thể được dán nhãn màu trắng để sử dụng.

Bảo vệ cho công cụ Dịch vụ có thể được lọc và ủy quyền ở Lớp 4, và các yêu cầu được giảm nhẹ ở lớp 7. Nó cũng có bằng sáng chế đang chờ giải quyết về công nghệ Phân tích Hành vi Con người, để cải thiện dịch vụ của mình.

4. Mạng lưới Arbor

Từ bộ phận bảo mật của Netscout, Arbor Cloud cung cấp cả bảo vệ đám mây trên trang web cho các cuộc tấn công của nhà nước đối với cơ sở hạ tầng bảo mật.

Nó cũng cung cấp dịch vụ quét lưu lượng truy cập đa nhu cầu, theo yêu cầu và hỗ trợ DDoS 24/7 thông qua Trung tâm hoạt động bảo mật của nó.

5. Incapsula

Danh sách Top Ten Reviews liệt kê cho Incapsula một giải thưởng vàng cho dịch vụ bảo vệ DDoS trong năm nay. Nó có một mạng lưới trung tâm dữ liệu toàn cầu, vì vậy có thể cung cấp nhiều trung tâm chà xát hơn nhiều nhà cung cấp khác.

Nó cung cấp bảo vệ chăn chống DDoS hoặc như là một luôn luôn trên dịch vụ hoặc theo yêu cầu, và một đội ngũ an ninh 24/7.

III. KIỂM TRA THÂM NHẬP DOS-DDOS

Phần này đọc thêm, link hướng dẫn: https://toc.123doc.org/document/704660-24-kiem-tra-tham-nhap-dos-ddos.htm

PHẦN D: HƯỚNG DẪN VÀ DEMO CÁCH THỨC TẤN CÔNG:

- Sử dụng tools trên github: GoldenEye-master, link: https://github.com/jseidl/GoldenEye
- Video clip tham khảo: https://www.youtube.com/watch?v=Li8s4QtsYYY

GoldenEye Layer 7 (KeepAlive + NoCache) Công cụ kiểm tra DoS
Goldeneye mắt vàng
GoldenEye là một ứng dụng python cho PURPOSES KIỂM TRA AN NINH CHỈ!

GoldenEye là một công cụ kiểm tra HTTP DoS.

Tấn công Vector khai thác: HTTP Giữ Alive + NoCache
Sử dụng
SỬ DỤNG: ./goldeneye.py <url> [TÙY CHỌN]

TÙY CHỌN:
Gắn cờ Mô tả Mặc định
-u, --useragents Tệp với tác nhân người dùng để sử dụng (mặc định: được tạo ngẫu nhiên)
-w, - Workers Số lượng công nhân đồng thời (mặc định: 50)
-s, --sockets Số lượng ổ cắm đồng thời (mặc định: 30)
-m, --method HTTP Method để sử dụng 'get' hoặc 'post' hoặc 'random' (mặc định: get)
-d, --debug Bật Chế độ gỡ lỗi [đầu ra chi tiết hơn] (mặc định: Sai)
-n, --nosslcheck Không xác minh Chứng chỉ SSL (mặc định: Đúng)
-h, --help Hiển thị trợ giúp này

Tiện ích
util / getuas.py - Tìm nạp danh sách tác nhân người dùng từ http://www.useragentstring.com/pages/useragentstring.php các trang con (ví dụ: ./getuas.py http://www.useragentstring.com/pages/Browserlist/) YÊU CẦU BEAUTIFULSOUP4
res / lists / useragents - Danh sách văn bản (một dòng trên mỗi dòng) của chuỗi Tác nhân Người dùng (từ http://www.useragentstring.com)

Changelog
2016-02-06 Thêm hỗ trợ cho việc không xác minh chứng chỉ SSL
2014-02-20 Thêm các tác nhân người dùng được tạo ngẫu nhiên (vẫn tuân thủ RFC).
2014-02-19 Đã xóa các giới thiệu và tác nhân người dùng ngớ ngẩn. Cải thiện sự ngẫu nhiên của người giới thiệu. Đã thêm hỗ trợ danh sách tác nhân người dùng bên ngoài.

2013-03-26 Thay đổi từ luồng thành đa xử lý. Vẫn còn một số lỗi để giải quyết như tôi vẫn không biết làm thế nào để propperly tắt máy quản lý.
2012-12-09 Phát hành lần đầu

Làm
Thay đổi từ getopt thành argparse
Thay đổi từ string.format () thành dạng printf
Giấy phép
Phần mềm này được phân phối theo Giấy phép Công cộng GNU phiên bản 3 (GPLv3)

THÔNG BÁO PHÁP LÝ
PHẦN MỀM NÀY ĐƯỢC CUNG CẤP CHO CHỈ SỬ DỤNG GIÁO DỤC! NẾU BẠN THAM GIA TRONG BẤT KÌ HOẠT ĐỘNG LĨNH VỰC CỦA ĐÔ THỊ KHÔNG BẤT KỲTRÁCH NHIỆM CHO NÓ. SỬ DỤNG PHẦN MỀM NÀY BẠN ĐỒNG Ý VỚI CÁC ĐIỀU KHOẢN NÀY.

Công cụ này là công cụ dos có nghĩa là đặt tải nặng trên máy chủ HTTP

để đưa họ đến đầu gối của họ bằng cách cạn kiệt hồ bơi tài nguyên.

Thực hiện demo trên hệ điều hành kali linux

Trang web DoS trong Kali Linux bằng GoldenEye

Tôi đã nói về việc thử nghiệm một số công cụ DoS có thể đặt tải nặng trên các máy chủ HTTP để đưa chúng đến đầu gối của chúng bằng cách làm cạn kiệt các nhóm tài nguyên. GoldenEye là công cụ đầu tiên trong số những công cụ này và nó là một trong những công cụ mới nhất mà tôi phát hiện ra trong GitHub. Bạn có thể làm các trang web với GoldenEye và đưa nó xuống gần như trong vòng 30 giây tùy thuộc vào độ lớn của bộ nhớ của họ. Tất nhiên, nó sẽ không hoạt động trên các máy chủ và máy chủ được bảo vệ phía sau WAF, IDS, nhưng đây là một công cụ tuyệt vời để kiểm tra Máy chủ Web của riêng bạn để kiểm tra tải và sửa đổi các quy tắc iptables / Firewall của bạn.

Bạn cũng có thể DoS sử dụng hping3 để mô phỏng các cuộc tấn công tương tự hoặc khai thác PHP để tấn công các trang web WordPress. Ngoài ra còn có một số công cụ tuyệt vời cho phép bạn xem các cuộc tấn công DDoS trực tiếp trên toàn thế giới trong thời gian thực.

Từ bài viết của nhà văn GoldenEye:

Công cụ này chỉ dành cho mục đích nghiên cứu và mọi hành vi sử dụng độc hại của công cụ này đều bị cấm.

GoldenEye là một ứng dụng python cho PURPOSES KIỂM TRA AN NINH CHỈ!

GoldenEye là một công cụ kiểm tra HTTP DoS.

Tấn công Vector khai thác: HTTP Giữ Alive + NoCache

Các loại tấn công DoS hoặc DDoS

Chúng ta hãy xem xét một số thông tin cơ bản về các cuộc tấn công DoS hoặc DDoS. Về cơ bản có ba loại tấn công DoS và DDoS:

Lớp ứng dụng DoS và các cuộc tấn công DDoS

Các lớp giao thức DoS và các cuộc tấn công DDoS

Tấn công DoS và DDoS dựa trên khối lượng

Lớp ứng dụng DoS và các cuộc tấn công DDoS

Các tấn công DoS và DDoS của lớp ứng dụng là các cuộc tấn công nhắm vào các lỗ hổng của Windows, Apache, OpenBSD hoặc các lỗ hổng phần mềm khác để thực hiện tấn công và làm hỏng máy chủ.

Các lớp giao thức DoS và các cuộc tấn công DDoS

Một cuộc tấn công DoS và DDoS giao thức là một cuộc tấn công ở cấp độ giao thức. Danh mục này bao gồm Synflood, Ping of Death và hơn thế nữa.

Tấn công DoS và DDoS dựa trên khối lượng

Loại tấn công DoS và DDoS này bao gồm lũ ICMP, lũ lụt UDP và các loại lũ khác được thực hiện thông qua các gói giả mạo.

Từ DoS và DDoS được sử dụng lỏng lẻo như khi bạn tấn công từ một máy đơn lẻ, nó thường được coi là tấn công DoS. Nhân một kẻ tấn công duy nhất từ một botnet (hoặc một nhóm) sau đó nó trở thành một cuộc tấn công DDoS. Có rất nhiều giải thích cho nó, nhưng chỉ biết rằng không có vấn đề mà loại tấn công nó được, họ đều là bất lợi cho một máy chủ / mạng.

Cuộc tấn công

```
root@kali:~/GoldenEye/GoldenEye-master# ./goldeneye.py http://10.0.0.101/
```

toàn bộ cuộc tấn công chỉ kéo dài 30 giây.

Kết quả

Đây là những gì tôi đã thấy ở cuối máy chủ

Tôi có một lượng lớn bộ nhớ miễn phí và chỉ 11 công nhân httpd.

Sau khi tấn công

Tôi hiện chỉ có 101 triệu bộ nhớ miễn phí và 174 công nhân httpd.

Chỉ mất 15 giây để đẩy máy chủ này đến giới hạn.

PHẦN E: TÀI LIỆU THAM KHẢO

https://vi.scribd.com/document/158605145/T%E1%BA%A4N-CONG-DoS-VA-CACH-PHONG-CH%E1%BB%90NG-pdf
http://dantri.com.vn/suc-manh-so/nhin-lai-10-vu-tan-cong-mang-dinh-dam-nhat-trong-nua-dau-nam-2017-20170520204717802.htm
https://quantrimang.com/cac-kieu-tan-cong-mang-22
https://vn-zoom.org/threads/tan-cong-dos-la-gi-denial-of-service-attack.86/
https://blogchiasekienthuc.com/dan-cong-nghe/dos-ddos-la-gi-hacker-tan-cong-ddos-bang-cach-nao.html
https://quantrimang.com/tim-hieu-ve-tan-cong-tu-choi-dich-vu-dos-34926
https://resources.infosecinstitute.com/dos-attacks-free-dos-attacking-tools/#gref
https://tabatech.vn/cach-phong-chong-tan-cong-ddos/
https://www.cbronline.com/business/5-ddos-attack-prevention-tools-to-protect-your-company-4692345/
https://toc.123doc.org/document/704660-24-kiem-tra-tham-nhap-dos-ddos.htm
https://www.blackmoreops.com/2015/05/18/dos-website-in-kali-linux-using-goldeneye/