TÌM HIỂU VỀ CÁC PHƯƠNG PHÁP TẤN CÔNG MẠNG TRONG 10 NĂM GẦN ĐÂY

Trần Huỳnh Khang[13], Nguyễn Tuấn Kiệt[14]

Tóm tắt: *Ngày nay, với sự tiến bộ của khoa học và công nghệ, thì mạng internet dần trở thành một phần quan trọng trong mọi lĩnh vực sống. Số lượng các dịch vụ liên quan đến internet ngày càng tăng, dẫn đến số lượng người sử dụng các dịch vụ này cũng tăng theo. Internet mang đến cho người sử dụng đa dạng thông tin về nội dung và hình thức. Bên cạnh những lợi ích mà internet mang lại thì cũng sẽ xuất hiện các mối nguy hiểm liên quan đến các vấn đề bảo mật thông tin. Đó là các hành động xâm nhập và khai thác trái phép các thông tin nhằm phục vụ các lợi ích riêng. Các hành động này ngày càng tăng cao khi nhu cầu sử dụng internet tăng lên. Chính vì vậy, mà các vấn đề liên quan đến thông tin mạng ngày càng được quan tâm và bảo vệ. Để có thể thực hiện tốt công tác bảo vệ, thì chúng ta cần phải hiểu về phương pháp và cách thức hoạt động của các hành vi trái phép này. Mục đích chính của việc tìm hiểu, là chỉ khi hiểu rõ các phương pháp này, thì chúng ta mới tìm ra các biện pháp ngăn ngừa hay phòng chống các cuộc tấn công làm ảnh hưởng đến các lợi ích của chính chúng ta. Đây được xem là phương án tốt nhất để giải quyết vấn đề này.*

Từ khóa: *Internet, Arpanet, WAN*

Abstract: *The advancement of science and technology makes the internet gradually become an important part of all areas of life nowadays. That the number of internet-related services is increasing leads to the growth of internet uses. The Internet gives its users information with different contents and forms. Regardless of the benefits of the internet, there are also dangers related to information security issues which are illegal infiltration and exploitation of information to serve a certain interest. These actions are increasing when the demand for using the internet goes up. Therefore, issues related to network information are increasingly concerned. In order to be able to supply effective protection, we need to understand how these illegal acts work. When we understand these methods, we are likely to find ways to prevent unexpected attacks . This is considered to be the best solution to this problem.*

Keywords: *Internet, Arpanet, WAN*

1. Giới Thiệu

Tháng 7 năm 1969, sư ra đợi của mạng ARPANET hay nói cách khác chính là tiền thân của mạng internet ngày nay do các nhà nghiêm cứu khoa học thuộc bộ quốc phòng mỹ phát

[13] Giảng viên Khoa Kỹ thuật - Công nghệ, Trường Đại học Nam Cần Thơ

[14] Sinh viên Khoa Kỹ thuật - Công nghệ, Trường Đại học Nam Cần Thơ

triển. Đây được xem là mạng liên khu vực (Wide Area Network - WAN) đầu tiên được xây dựng ở thời điểm này. Năm 1974, thuật ngữ "Internet" lần đầu xuất hiện và cho đến năm 1980 thì nó bắt đầu đi vào lịch sử và phát triển cho đến bây giờ. (Việt Nguyễn, 2021)

Internet (hay còn được gọi tắt là "mạng") là một hệ thống mạng được liến kết lại với nhau có phạm vi trên toàn thế giới. Internet cho phép người dùng ở mọi lúc mọi nơi, chỉ cần được kết nối với mạng máy tính sẽ có thể tìm được các thông tin dữ liệu cần thiết do những người dùng khác chia sẽ (ngoài ra chúng ta cũng có thể trò chuyện, gặp gỡ trực tiếp thông qua các thiết bị khác với yêu cầu các thiết bị này có kết nối với internet. (chaupm, 2019)

Internet giúp cho chúng ta tìm kiếm thông tin tài liệu một cách dễ dàng. Ngoài ra, các lĩnh vực khác như kinh doanh, giáo dục... cũng được phát triển hơn khi kết hợp cùng với internet. Với những lợi ích mà internet mạng lại cho con người trên toàn cầu, thì chúng ta đã thấy được tầm quan trọng của nó là cực kỳ to lớn. (semtek, 2019)

Bên cạnh những lợi ích mà internet mang lại cho chúng ta thì có không ích các rủi ro tiềm tàng với những mức độ nguy hiểm khác nhau. Theo thống kê, từ khi internet xuất hiện đã diễn ra vô số các cuộc tấn công. Các cuộc tấn công này xảy ra nhằm vào các mục đích tốt hoặc xấu do các cá nhân hay tổ chức thực hiện phục vụ cho các lợi ích riêng biệt. Với sự phát triển không ngưng của khoa học và công nghệ, thì giờ đây các cuộc tấn công mạng đang trở nên đa dạng và khó phòng chống hơn. Các cá nhân, tổ chức, doanh nghiệp không không đáp ứng được các kiến thức cần thiết về việc phòng chống về an ninh mạng sẽ dễ dàng trở thành các mục tiêu để tấn công. Vì vậy, chỉ khi ta hiểu rõ và xác định được các hình thức tấn công mạng để đưa ra các giải pháp phòng chống thông qua những hiểu biết và kiến thức về an ninh mạng thì chúng ta mới có thể thực hiện tốt công tác bảo vệ an toàn an ninh mạng. (ods, 2020) Hiểu được mức độ quan trọng của vấn đề cho nên chúng ta sẽ cùng nhau tìm hiểu về các phương pháp tấn công mạng phổ biến hiện nay.

1.1. Khái Niệm

Tấn công mạng có thể được hiểu là hành vi sử dụng không gian mạng để thực hiện các hoạt động tấn công, xâm nhập vào một hệ thống mạng máy tính, cơ sở dữ liệu, hạ tầng mạng, thông tin dữ liệu, thiết bị của cá nhân hoặc tổ chức với mục đích tốt hoặc xấu. (security, 2020)

Lỗ hỏng bảo mật có thể hiểu tóm tắt là một hư hại trục trặc hay một điểm yếu trong một phần mềm hoặc một hệ thống mạng. Khoa học công nghệ càng phát triển thì các lỗ hỏng bảo mật càng xuất hiện nhiều hơn. Lỗ hỏng bảo mật là không thể tránh khỏi nhưng vấn đề lỗ hỏng có bị khai thác bởi các hacker hay không. Để tránh các rủi ro, nguy hiểm thì chúng ta cần phải đảm bảo tốt các vấn đề bảo mật. (Phạm Hải, 2018)

Hacker được định nghĩa là những người sử dụng máy tính hay các chuyên gia về phần mềm, an ninh mạng. Các hacker hiểu rõ về cách thức hoạt động của máy tính, mạng máy tính, phần cứng và phần mềm để phát tán vi-rút máy tính hay xâm nhập vào mát tính người khác. Mục đích của việc này là để thực hiện các hành động phạm pháp như thay đổi, đánh cắp, phá hoại thông tin phàn mềm, phần cứng, tài liệu được lưu trữ trên hệ thống máy tính người khác.

Tuy nhiên đó không phải mục đích duy nhất, một số hacker được thuê để thực hiện các hoạt động xâm nhập tìm kiếm lổ hỗng bảo mật để hạn chế và phòng chống khả năng bị tấn công được gọi là hoạt động kiểm thử xâm nhập. (Trịnh Duy Thanh, 2019)

Đối tượng tấn công mạng có thể là cá nhân, tổ chức, doanh nghiệp... thông qua hệ thống mạng. Đặc biệt các doanh nghiệp vừa và nhỏ luôn là mục tiêu của mọi cuộc tấn công nhằm vào các mục đích xấu(đánh cắp, phá hoại, lợi nhuận). (antoanthongtinhaiphong, 2020)

1.2. Phân Loại

Ngày nay, việc tấn công không gian mạng không chỉ để thực hiện các mục đích xấu (do các hacker mũ đen thực hiện) mà còn thực hiện nhằm kiểm thử, kiểm tra hệ thống năng cao bảo mật (đây là công việc thực hiện chính của hacker mũ trắng). Đặc điểm của 2 mục đích tấn công:

1.2.1. Kiểm thử xâm nhập

Kiểm thử xâm nhập (penetration testing): là phương pháp tấn công xâm nhập vào thiết bị, hệ thống mạng, cơ sở dữ liệu để đánh giá tính bảo mật của hệ thông nhằm tìm ra những lỗ hỏng có thể được khai thác. Kiểm thử xâm nhập được chia thành 5 bước: (Cát Tường, 2020)

- *Lập kế hoạch:* là xác định phạm vi và thu thập thông tin.

- *Quét:* là kiểm tra phản hồi của hệ thống (thường được sử dụng: phân tích tĩnh và phân tích động).

- *Kiểm soát khả năng truy cập:* là sử dụng các phương pháp tấn công để tìm ra lỗ hỏng và mức độ thiệt hại có thể xãy ra.

- *Duy trì là truy cập:* là xem thời gian tồn tại của lỗ hỏng (có đủ lâu để tấn công sâu vào hệ thống).

- *Phân tích:* đưa ra thống kê kết quả và đưa ra giải pháp.

1.2.2. Tấn công mạng (Cyber Attack (Chí Cường, 2020))

Là tất cả các hình thức tấn công xâm nhập trái phép vào thiết bị, hệ thống mạng, cơ sở dữ liệu với mục đích vi phạm dữ liệu (dánh cắp, thay đổi, mã hóa, phá hủy), gây gián đoạn, phát tán hoặc lợi dụng thông tin dữ liệu gây ảnh hưởng tiêu cực. Đây là hành vi trái pháp luật được thực hiện do một ca nhân hay tổ chức gây nên để phục vụ những lợi ích riêng tư.

Một số hình thức tấn công mạng trái phép như:

- *Tấn công bằng phần mềm độc hại (Malware attack):* cài phần mềm độc hại để chiếm quyền truy cập, theo dõi, phá hoại tài sản...

- *Tấn công giả mạo (Phishing attack):* giả mạo để đánh cắp dữ liệu....

- *Tấn công trung gian (Man-in-the-middle attack):* sử dùng phần mềm nghe lén để ghi lại thông tin dữ liệu người dùng.

1.3. Cách thức hoạt động

Để tấn công xâm nhập vào một hệ thống mạng, thì người tấn công cần thực hiện theo quy trình nhiều bước: (anningmang, 2020)

- *Tìm hiểu đối tượng (Reconnaissace):* là bước đầu quan trọng trong mọi cuộc tấn công để thu thập hiểu rõ thông tin về đối tượng (Theo dõi đối tượng, các dịch vụ hoạt động...).

- *Quét hệ thống (Scanning):* là bước tiếp theo để tìm hiểu sâu bên trong hệ thống. Tìm ra các lỗ hỏng để tấn công như: thăm do địa chỉ IP, hệ điều hành hay kiến trúc hệ thống mạng. Một vài phương pháp tấn công được sử dụng phổ biến là quét cổng, quét mạng...

- *Kiểm soát truy cập (Gainning access):* là kiểm soát chiếm quyền truy cập các hoạt động bên tỏng mạng như mức độ hệ điệu hành, mức đọ dịch vụ, mức độ mạng...

- *Duy trì kết nối (Maitaining access):* là các hoạt động can thiệp sâu vào hệ thống mạng như biến đổi, đánh cắp, phá hủy, phát tán...

- *Xóa dấu vết (Clearning tracks):* là bước cuối cùng. Sau khi bị các hoạt động can thiệp vào hệ thống sẽ lưu lại các lỗ hỏng do bị tấn cống. Người tấn công cần thực hiện các hành động xóa dáu vết nhằm tránh bị phát hiện.

Theo thống kê, các cuộc tấn công mạng vẫn được diễn ra hàng năm. Thời gian các cuộc tấn công là không cố định và nó diễn ra với mức độ cũng như quy mô là khác nhau (xu hướng tăng lên theo thời gian). Trong tương lai các cuộc tấn công sẽ diễn ra mức độ khó khăn và nhiều hơn. An ninh mạng phát triển dẫn đến các lỗ hỏng bảo mật mới sẽ được xuất hiện đồng nghĩa với việc các rủi ro, nguy cơ cũng sẽ xuất hiện theo. Để chuẩn bị tốt công tác bảo mật về an ning mạng thì cần hiểu và biết rõ về các phương pháp tấn công mạng là rất cần thiết. Vì vậy, để hiểu rõ thì chúng ta sẽ cùng tìm hiểu về các phương pháp tấn công mạng phổ biến trong những năm trở lại đây.

2. Tìm hiểu các phương pháp tấn công mạng trước năm 2010

Tấn công không gian mạng đã và đang trở thành vấn đề đặc biệt nghiêm trọng. Ngay sau khi sự ra đời của công nghệ mạng máy tính, thì khái niệm tấn công mạng đã hình thành và phát triển mạnh mẽ cho đến ngày nay.

2.1. Tấn công Phreaking

Đầu những năm 1994, khi mà mạng internet vẫn còn trong quá trình hình thành thì đã xuất hiện một số cuộc tấn công không gian mạng. Điển hình là cuộc tấn công của một nhóm hacker được gọi là Phonemasters. Nhóm hacker này đã sử dụng kỹ thuật gọi là phreaking. (fas, 1996)

Phreaking là một thuật ngữ để miêu tả cho hành động xâm nhập vào mạng viễn thông. Phreaking xuất hiện từ những năm 1970, mục tiêu ban đầu của phreaking được dùng để khám phá và khai thác mạng điện thoại. Về sau, phreaking được các hacker cải tiến và phát triển để đánh cắp thông tin. (filegi, 2020)

2.2. Kỹ thuật tấn công từ chối dịch vụ (Dos Và Ddos)

Một cuộc tấn công không gian mạng nhằm vào Yahoo, eBay, eTrade, Amazon.com... diễn ra vào năm 2000 đã gây ra những thiệt hại vô cùng to lớn. Năm 2007, một số trang web của chính phủ, các ngân hàng, trường học nằm tại Estonia đã bị các hacker tấn công. Tất cả các cuộc tấn công trên đều được các hacker sử dụng chung một kỹ thuật là tấn công từ chối dịch vụ (DoS). (aptech, 2011)

Tấn công từ chối dịch vụ hay còn được gọi là DoS (Denial of Service) là một cuộc tấn công với lượng lớn máy ảo mục đích chính là làm gián đoạn, dừng hoạt động của một máy chủ hay một hệ thống mạng. Hành động này khiến cho các truy cập từ người dùng đến máy chủ hay hệ thống mạng không thể thực hiện được.

Tấn công từ chối dịch vụ phân tán DdoS (Distributed Denial of Service) là phương thức nâng cao và được phát triển hơn so với DoS. Giống với DoS, thì tấn công bằng DDoS cũng sử dụng các máy ảo để tấn công nhưng các máy ảo này được tập hợp từ nhiều nguồn khác nhau không giống với DoS khi chỉ được tạo ra từ một nguồn duy nhất. (Quách Tỉnh, 2020)

Một kỹ thuật tấn công từ chối dịch vụ phổ biên hiện nay:

Kỹ thuật SYN Flood: là phương thức tấn công nhắm vào TCP, tấn công này sử dụng toàn bộ tài nguyên của máy chủ có sẵn khiến cho máy chủ không còn đủ lưu lượng để đáp ứng cho các truy cập hợp pháp. Tấn công bằng SYN Flood các hacker cần thực hiện theo quy trình các bước:

- Bước 1: Kẻ tấn công sẽ sử dụng các máy ảo để gửi một lượng lớn các packet tin SYN đến máy chủ đã các định.

- Bước 2: Theo nguyên lý hoạt động của máy chủ, thì sẽ mở sẵn một cổng kết nối để nhận các yêu cầu. Khi có yêu cầu kết nối thì máy chủ sẽ phản hồi lại từng yêu cầu đó. Sau đó, sẽ mở tiếp một cổng khác để nhận yêu cầu khác.

- Bước 3: Bình thường, máy chủ sẽ nhận lại các packet ACK sau khi đã phản hồi. Tuy nhiên các kẻ tấn công sẽ không gửi các gói packet này mà tiếp tục gửi các packet SYN. Với yêu cầu kết nối mới, thì máy chủ sẽ duy trì kết nối cổng cũ và mở cổng mới để nhận yêu cầu tiếp theo. Tuy nhiên khi lượng lớn các yêu cầu gữi đến khiến cho các cổng có sẵn trên máy chủ bị quá tải dẫn đến máy chủ không ổn định hoặc dừng hoạt động. (vnso, 2019)

2.3. Tấn công SQL Injections

Một trong những tội phạm công nghệ nổi tiếng trên thế giới chính là Albert Gonzalez. Từ năm 2005 cho đến năm 2007 thì Albert Gonzalez đã cùng với các hacker khác tạo thành một nhóm để tấn công thông tin trên mạng và gây thiệt hại cho nhiều tổ chức ở Mỹ. Lợi dụng những lỗ hỏng bảo mật mà nhóm này đã sử dụng kỹ thuật SQL injections để xâm nhập và đánh cặp thông tin. (Trần Hải, 2018)

SQL Injections là kỹ thuật tấn công không gian mạng thông qua các lỗ hổng của câu truy vấn được sử dụng trong ứng dụng. Để thực hiện được thì các hacker cần chèn thêm một đoạn SQL để thay đổi chức năng, từ đó các hacker sẽ chiếm quyền và khai thác mọi thông tin dữ liệu. (Nhật Linh, 2020)

Blind SQL injection còn được goi SQL Inferential SQL là một dạng tấn công của SQL injection tương tác với cơ sở dữ liệu. Phương pháp này sử dụng các thuật toán đoán biết. Đối với các trường hợp trang web hay phần mềm được thiết lập ẩn thông báo, hiển thị chi tiết lỗi thì Blind SQL ịnections đặc biệt hữu dụng. (Nguyễn Mạnh, 2019)

3. Tìm hiểu các phương pháp tấn công mạng từ năm 2010 trở lại đây

Trong những năm trở lại đây thì tấn công không gian mạng đã phát triển lên nhiều mức độ khác nhau, mạnh mẽ hơn, tinh vi hơn. Các phương pháp mới ra đời kéo theo số vụ tấn công xảy ra ngày càng tăng lên và mức độ ảnh hưởng, thiệt hại cũng vì thế mà tăng theo. Bên dưới là điển hình cho một số phương pháp và kỹ thuật mà các hacker vụ tấn công không gian mạng từ năm 2010 đến nay.

3.1. Tấn công spear phishing

Năm 2011, được xem là năm bùng nổ của các hacker. Các cuộc tấn công mạng diễn ra liên tục chỉ trong vòng 20 ngày nhắm vào các tổ chức lớn trên thế giới như Citigroup, IMF(quỹ tiền tệ quốc tế) gây ra những hậu quả khó lường. Trong đó phải kể đến công ty email lớn nhất thế giới, Epsilon bị tấn công bởi các hacker. Bằng việc chủ quan với các nguy cơ rủi ro bởi các cuộc tấn công trước đó dẫn đến một tấn công và đánh cắp toàn bộ thông tin. Phương pháp mà các hacker áp dụng chính là kỹ thuật spear phishing một dạng cải tiến hơn của phreaking một loại tấn công đã xuất hiện từ rất lâu. (Văn Cường, 2011)

Tấn công mạng Phishing được xem là hình thức tấn công mạng đơn giản nhất và cũng có độ hiệu quả cũng như mức độ nguy hiểm cao nhất. Khác với một số hacker khác phải khai thác lỗ hỏng bảo mật thì các hacker sử dụng phương pháp tấn công này chủ yếu lừa người dùng tự trao thông tin dữ liệu cho kẻ tấn công.

Khi tấn công không gian mạng bằng phương pháp Phishing, kẻ tấn công cần thực hiện theo một quy trình có nguyên lý. Quy trình này bao gồm:

- Lên kế hoạch: Những kẻ tấn công này sẽ xác định mục tiêu là cá nhân, tổ chức hay doanh nghiệp nào "đủ khả năng đáp ứng các yêu cầu" để trở thành nạn nhân và xác định cách lấy địa chỉ email khách hàng của cá nhân, tổ chức hay doanh nghiệp đó. Kẻ tấn công thường áp dụng phương pháp gửi lượng lớn email và thu thập địa chỉ email như những spammer.

- Thiết lập: Sau khi đã thành công xác định được tổ chức, cá nhân hay doanh nghiệp là nạn nhân, kể tấn công sẽ tiến hành phát tán email và bắt đầu thu thập thông tin và dữ liệu. Thông thường, kẻ tấn công sẽ sử dụng một địa chỉ email cùng với đó là một trang web nào đó.

- Tấn công: Đây là bước đặc biệt quan trọng của mọi cuộc tấn công- kẻ tấn công sẽ gửi một dạng thông báo giả mạo, giống như những thông báo đến từ một nguồn đáng tin cậy của nạn nhân tin tưởng.

- Thu thập: khi người dùng hoàn thành các yêu cầu. Kẻ tấn công sẽ thu thập thông tin mà nạn nhân điền vào các trang Web hoặc các cửa sổ nhập thông tin.

- Đánh cắp dữ liệu cá nhân và thực hiện các hành vi lừa đảo: sau khi đã thu thập được thông tin mà kẻ tấn công cần để thực hiện các hoạt động mua bán bất hợp pháp hoặc thậm chí là tiến hành lừa đảo.

Spear Phishing là một kỹ thuật tấn công giả mạo, giả danh một đối tướng để lừa đảo, thu thập thông tin của mục tiêu. Đây là hình thức tấn công phi kỹ thuật bởi vì nó tấn cộng dựa vào tâm lý người dung hoặc sai lầm do thiếu kiến thức về an ninh mạng. Email được xem là công cụ tấn công chính của Spear Phishing. Spear Phishing mang những đặc tính đặc biệt như: sử dụng đe dọa từ nhiều nguồn(kết hợp giữa thư điện tử, các kỹ thuật tấn công tự động, các đường dẫn linh động....), tấn công vào các lỗ hỏng bảo mật(zero-day, plug-in và các phần mềm độc hại...), tấn công theo nhiều bước(khởi tạo các lỗ hỏng bảo mật kết hợp với các phần mềm độc hại bên ngoài, rò rĩ dữ liệu...), không mang đặc tính của thư rác(với những đặc điểm khác với tấn công thư rac cho nên nó dễ dàng vượt qua các bộ lọc thư rác). (PV, 2015)

Ngày nay, tấn công bằng kỹ thuật Spear Phishing đã trở nên phổ biến và phát triển thành nhiều mức độ khác nhau. Vì vậy mà công tác bảo vệ hay hạn chế tấn công không gian mạng bằng kỹ thuật này cũng trở nên khó khăn hơn.

3.2. Tấn công malware (phần mềm chứa mã độc)

Tấn công bằng kỹ thuật Spear Phishing đã hoạt động hiểu quả trong khoản thời gian khá dài, các hình thức tấn công theo các năm vẫn có nét chúng về phương pháp và kỹ thuật. Tuy nhiên đến đầu năm 2017 thì lại bùng nỗ một cuộc tấn công với cộng mới được gọi là hiện tượng Wanna Cry. Hiện tượng mới này đã làm ảnh hưởng nặng nề đến tổ chức và các doanh nghiệp.

Kỹ thuật Wanna Cry đánh dấu lần đầu tiên tấn công mã độc được thực hiện bằng 1 con sâu máy tính (worm). Khi tấn công vào hệ thống thì Wanncry sẽ tạo các cặp khóa RSA-2048. Kỹ thuật này sau khi tấn công mày tính mục tiêu sẽ thực hiện các quá trình mã hóa dữ liệu bằng các thuật toán RSA và AES. (PC World VN, 2017)

Tấn công malware là thuật ngữ dùng để chỉ chung cho các kỹ thuật tấn công bằng mã độc. 2 kỹ thuật được xem là tốt nhất của phương pháp tấn công malware là virus và worm.

3.2.1. Virus: Virus có thể lây nhiễm nhưng phải thông qua các phương tiện khác. Virus chỉ có thể lan truyền qua các máy tính khác chưa nhiễm mã độc bằng các đính mã vào các tập tin được truyền. Virus được cấu tạo từ 3 phần: Replicator: sau khi khởi động chương trình chính thì đồng thời virus cũng được kích hoạt, và ngay lập tức chúng sẽ phát tán malcode; Concealer: phương pháp mà virus sử dụng để lẩn tránh qua các phần mềm diệt vitrut như anti-malware; Payload: như đã nói, payload được hiểu là malcode của một virus, được sử dụng để vô hiệu hóa các chức năng của hệ thống máy tính và phá hủy, xóa bỏ dữ liệu.

3.2.2. Worm: hay còn được gọi là sâu máy tính với khả năng tinh vi hơn so với virus. Sâu máy tính có khả năng đặc biệt là tự sao chéo mà không cần các hoạt động từ người dùng như virus. Ngoài ra khi kết hợp cùng với internet, thì sâu máy tính sẽ đáp ứng được các yêu cầu của malware hơn so với virus. Sâu máy tính được cấu tạo từ: Penetration tool: Là malcode có nhiệm

vụ khai thác những lỗ hổng bảo mật trên máy tính của nạn nhân để dành quyền truy cập; Installer: Công cụ hỗ trợ thâm nhập giúp sâu máy tính vượt qua hệ thống phòng thủ đầu tiên. Kế tiếp, installer sẽ đảm nhận công viêc vận chuyển thành phần chính của malcode vào máy tính của nạn nhân; Discovery tool: Khi đã hoàn thành việc xâm nhập vào hệ thống máy tính, sâu máy tính sử dụng các thuật toán để tìm kiếm những máy tính khác trên mạng, gồm địa chỉ email, danh sách máy chủ và các truy vấn DNS; Scanner: Sâu sử dụng một công cụ hỗ trợ có khả năng kiểm tra để xác định những mục tiêu mới trong penetration tool; Payload: Malcode có thể tồn tại trên mỗi hệ thống máy tính của nạn nhân. Những malcode này có thể là bất cứ thứ gì, nó có thể là một ứng dụng truy cập từ xa đến từ một key logger (phần mềm bàn phím gián điệp) được dùng để thu thập tên đăng nhập và mật khẩu của người dùng.

Tấn công bằng phương pháp malware vẫn đang phát triển rất nhanh. Với sâu máy tính được phát hiện mới nhất hiện nay là Conficker. Hầu hết các sâu máy tính hiện nay đều có phòng tránh và xóa bỏ bởi các phần mềm anti-malware. (Tuấn Phong, 2019)

3.3. Một số phương pháp tấn công phổ biến hiện nay

Theo thống kê hiện nay thì tấn công không gian mạng vẫn đang âm thầm phát triển. Mặc dù các cuộc tấn công không gian mạng không diễn ra một cách liên tục như ở giai đoạn đỉnh điểm. Điển hình là đã xuất hiện thêm nhiều hình thức tấn công với kỹ thuật và mức độ khác nhau từ nhỏ đến lớn.

Tấn công bị động (Passive attack): các hacker sẽ kiểm tra gói dữ liệu không được mã hóa dựa trên kỹ thuật Wireshark để tìm ra thông tin tài khoản, mật khẩu có thể sử dụng cho mục đích tấn công khác. Tấn công bị động được thực hiện theo quy trình từng bước: phân tích gói dữ liệu, theo dõi các cuộc giao tiếp thua thập thông tin, giải mã các gói dữ liệu được mã hóa yếu...

Tấn công rải rác (Distributed attack): Đối với các cuộc tấn công được thực hiện theo kỹ thuật rải rác, kỹ thuật này yêu cầu kẻ tấn công phải giới thiệu được mã code, chẳng hạn như một chương trình hay phần mềm Trojan horse hoặc một chương trình back-door. Với khả năng "tin cậy" hoặc một chương trình phần mềm được phân phối cho nhiều hệ thống máy tính khác và tấn công người dùng bằng cách tập trung vào việc sửa đổi các phần mềm độc hại của phần cứng hoặc phần mềm trong quá trình lan truyền,... Các cuộc tấn công thực hiện với phương pháp giới thiệu mã độc hại chẳng hạn như back door trên một hệ thống nhằm mục đích truy cập trái phép các thông tin hoặc truy cập trái phép các chức năng trên hệ thống.

Tấn công bị động (Passive attack): các hacker sẽ kiểm tra gói dữ liệu không được mã hóa dựa trên kỹ thuật Wireshark để tìm ra thông tin tài khoản, mất khẩu có thể sử dụng cho mục đích tấn công khác. Tấn công bị động được thực hiện theo quy trình từng bước: phân tích gói dữ liệu, theo dõi các cuộc giao tiếp thua thập thông tin, giải mã các gói dữ liệu được mã hóa yếu...

Tấn công trung gian (Man-in-the-Middle Attack): giống như cái tên của nó, một cuộc tấn công theo kỹ thuật Man-in-the-Middle Attack xảy ra khi cuộc nói chuyện giữa một người và một

người nào đó bị kẻ tấn công theo dõi, nắm bắt, kiểm soát và thu thập thông tin liên lạc của cuộc trò chuyện một cách bí mật mà người bị tấn công không thể biết. Các cuộc tấn công theo phương pháp Man-in-the-Middle Attack giống như kỹ thuật tấn công Spear Phishing. Kẽ tân công sẽ giả mạo danh tính một người nào đó để đọc các tin nhắn của người dùng. Và người ở đầu kia sẽ tin rằng đó là người trò chuyện thật sự, bởi vì kẻ tấn công có thể trả lời một cách nhanh chóng, tích cực để thực hiện hành vi trao đổi và thu thập thêm thông tin. (Nhật Minh 2018)

Trên đây là các phương pháp kỹ thuật tấn công không gian mạng phổ biến còn được sử dụng bởi những kẻ tấn công. Các phương pháp này mặc dù đã xuất hiện từ khá lâu nhưng nó vẫn được sử dụng qua các gian đoạn khác nhau bằng cách pháp triển và cải tiến để nó trở nên mạnh mẽ và nguy hiểm hơn.

4. Kết Luận

An ninh mạng hiện nay trên thế giới nói chung và tại mỗi quốc gia nói riêng đang pháp triển theo chiều hương khá phức tạp. Không gian mạng, đặc biệt là lỗ hỏng bảo mật được xem là mục tiêu chính của các cuộc tấn công. Bộ luật về an ninh mạng đã được ban hành và áp dụng trên toàn thế giới, quy đinh những hành động nào là đúng, những hành động nào là bất hợp pháp. Từ đó tiến hành xử lý các trường hợp trái với quy định. Mặc dù các bộ luật đã xuất hiện, tuy nhiên mỗi cá nhân, tổ chức, hay doanh nghiệp vẫn phải đặc biệt quan tâm và tuân thủ các vấn đề về bảo mật an ninh mạng.

Sau khi đã tìm hiểu và trang bị được những kiến thức cơ bản về vấn đề bảo mật an ninh mạng. Thì chúng ta đã hiểu rõ được khái niệm về tấn công mạng, lỗ hổng bảo mật, thế nào là hacker và các phương pháp cũng như kỹ thuật tấn công mạng mà các hacker sử dụng phổ biến hiện nay. Mục đích của bài nghiên cứu là hiểu rõ về an ninh mạng, sau đó tìm và đề xuất các biện pháp hay phương pháp tốt nhất giải quyết các vấn đề liên quan đến an ninh mạng.

Trong tương lai, an ninh mạng sẽ và phát triển hơn. Các cuộc tấn công nhắm đến không gian mạng vẫn sẽ tiếp tục diễn ra với những phương pháp mới, công nghệ mới. Việc bị tấn công bởi các hacker là không thể tránh khỏi. Vì vậy để đảm bảo an toàn an ninh mạng, thì mỗi cá nhân, tổ chức, quốc gia trên thế giới... cần thực hiện các phương pháp khoa học theo từng gian đoạn, từng tầng lớp, độ tuổi... Một số biện pháp tối ưu như: thực tốt công tác giáo dục đến học sinh sinh viên, tuyên truyền và kêu gọi tuân thủ các quy định về an ninh mạng, tổ chức và doanh nghiệp cần phải đáp ứng tốt các vấn đề bảo mật (thích nghi và xử lý rủi ro, biến đổi an ninh mạng một cách nhanh chóng trong thời đại số).

TÀI LIỆU THAM KHẢO

[1] Việt Nguyễn, 04/01/2021, "Lịch sử Internet ra đời năm nào? Ai phát minh ra Internet? ", 15 january 2021, https://beginer.com/lich-su-internet-ra-doi-nam-nao-ai-phat-minh-ra-internet.

[2] chaupm, 23/04/2019, " Mạng internet là gì? Phân biệt internet và network", 15 january 2021, https://bizflycloud.vn/tin-tuc/mang-internet-la-gi-phan-biet-internet-va-network-20190423104157185.htm.

[3] semtek, 9/11/2019, "Mạng Internet là gì? Những lợi ích của mạng internet trong cuộc sống", 15 january 2021, https://www.semtek.com.vn/mang-internet/.

[4] ods, 4/9/2020, "CÁC HÌNH THỨC TẤN CÔNG MẠNG PHỔ BIẾN HIỆN NAY VÀ CÁCH PHÒNG TRÁNH", 15 january 2021, https://www.ods.vn/tai-lieu/cac-hinh-thuc-tan-cong-mang-pho-bien-hien-nay-va-cach-phong-tranh.html.

[5] security, 2020, "TẤN CÔNG MẠNG LÀ GÌ | TỔNG QUAN VỀ TẤN CÔNG MẠNG", 15 january 2021, https://securitybox.vn/2899/tong-quan-ve-tan-cong-mang/#1_Tan_cong_mang_la_gi.

[6] Phạm Hải, 17/12/2018, "Lỗ hổng bảo mật - những hiểu biết căn bản", 15 january 2021, https://quantrimang.com/lo-hong-bao-mat-nhung-hieu-biet-can-ban-93098.

[7] Trịnh Duy Thanh, 11/12/2019, "Làm thế nào để trở thành một Hacker chuyên nghiệp", 16 january 2021, https://bkhost.vn/posts/hacker-la-gi.

[8] antoanthongtinhaiphong, 6/7/2020, "TẤN CÔNG MẠNG LÀ GÌ? TIN TẶC ĐÃ TẤN CÔNG DOANH NGHIỆP NHƯ THẾ NÀO?", 17 january 2021, http://antoanthongtinhaiphong.gov.vn/tan-cong-mang-la-gi-tin-tac-da-tan-cong-doanh-nghiep-nhu-the-nao/.

[9] Cát Tường, 28/12/2020, "Pentest là gì? Tìm hiểu về Penetration Testing (kiểm thử thâm nhập", 17 january 2021, https://quantrimang.com/tim-hieu-ve-penetration-testing-162644

[10] Chí Cường, 8/4/2020, "", 17 january 2021, https://cuongquach.com/cyber-attack-la-gi-tan-cong-mang.html.

[11] anningmang, 2020, "Cyber Attack là gì? Làm sao để hạn chế tấn công mạng ?", 18 january 2021, https://anninhmang.net/tu-hoc-quan-tri-mang/tu-hoc-an-ninh-mang/cac-giai-doan-tan-cong-cua-hacker/.

[12] fas, 5/6/1996, "THE CASE STUDY: ROME LABORATORY, GRIFFISS AIR FORCE BASE, NY INTRUSION", 18 january 2021, https://fas.org/irp/congress/1996_hr/ s960605b.htm.

[13] filegi, 2020, "Định nghĩa Phreaking là gì?", 19 january 2021, https://filegi.com/tech-term/phreaking-2162/.

[14] aptech, 16/5/2011, "", 20 january 2021, https://aptech.vn/kien-thuc-tin-hoc/tan-cong-ddos-hung-than-cua-cac-trang-web.html.

[15] Quách Tỉnh, 18/12/2020, "Tấn công DDoS, "hung thần" của các trang web, 20 january 2021, https://quantrimang.com/tim-hieu-ve-tan-cong-tu-choi-dich-vu-dos-34926.

[16]) vnso, 1/10/2019, "SYN flood attack DDoS là gì ? Cách thức phòng chống !", 21 january 2021, https://vnso.vn/syn-flood-attack-ddos-la-gi-cach-thuc-phong-chong/.

[17] Trần Hải, 15/03/2018, "Tội phạm công nghệ cao trong thế giới phẳng", 21 january 2021, https://suckhoedoisong.vn/toi-pham-cong-nghe-cao-trong-the-gioi-phang-n142201.html.

[18] Nhật Linh, 24/11/2020, "SQL Injection là gì? Cách phòng chống tấn công SQL Injection", 21 january 2021, https://quantrimang.com/tan-cong-kieu-sql-injection-va-cac-phong-chong-trong-asp-net-34905.

[19] Nguyễn Mạnh, 24/5/2019, "Blind SQL injection là gì? Blind injection khác với các loại SQL injection khác như thế nào?", 21 january 2021, https://viblo.asia/p/blind-sql-injection-la-gi-blind-injection-khac-voi-cac-loai-sql-injection-khac-nhu-the-nao-3Q75wX0DKWb.

[20] Văn Cường, 17/6/2011, "2011- Năm của hacker", 21 january 2021, https://saigondautu.com.vn/ho-so/2011-nam-cua-hacker-12497.html.

[21] PV, 16/8/2015, "Spear Phishing - Phương thức lừa đảo qua mạng có mục tiêu", 21 january 2021, http://www.taichinhdientu.vn/bao-mat/spear-phishing-phuong-thuc-lua-dao-qua-mang-co-muc-tieu-146014.html.

[22] PC World VN, 8/6/2017, "WannaCry - Lời cảnh báo đại dịch ransomware", 22 january 2021, http://www.pecc1.com.vn/d4/news/WannaCry-Loi-canh-bao-dai-dich-ransomware-8-1007.aspx.

[23] Tuấn Phong, 17/12/2019, "Malware là gì? Có những loại malware nào?", 22 january 2021, https://quantrimang.com/10-loai-malware-dien-hinh-58733.

[24] Nhật Minh 25/07/2018, "Tổng hợp các kiểu tấn công mạng phổ biến hiện nay", 22 january 2021 , https://quantrimang.com/cac-kieu-tan-cong-mang-22.

[25] Anninhmang, 2020, "Một số cách tấn công trong mạng và phần mềm hỗ trợ", 23 january 2021, https://anninhmang.net/tu-hoc-quan-tri-mang/tu-hoc-an-ninh-mang/mot-so-cach-tan-cong-trong-mang/.

[26] Đình Trung, 26/1/2021 , "Một số biện pháp kỹ thuật phòng chống tấn công từ chối dịch vụ", 23 january 2021, https://kontum.gov.vn/pages/detail/6678/Thong-tin-can-biet.html.

[27] Võ Văn Đông, 25/12/2020, "Một số hình thức tấn công phổ biến trong mạng LAN và giải pháp ngăn chặn", 22 january 2021, https://cpc.vn/vi-vn/Tin-tuc-su-kien/Tin-tuc-chi-tiet/articleId/40065.

[28] Digistar, 2020, "Tấn công từ chối dịch vụ DOS và DDOS", ", 23 january 2021, https://www.digistar.vn/tan-cong-tu-choi-dich-vu-dos-va-ddos-phan-1/.

[29] VNIST, 25/4/2020, "Khác biệt giữa tấn công DoS và DDoS", 23 january 2021, https://vnist.vn/khac-biet-giua-tan-cong-dos-va-ddos/ .

[30] Nguyễn Thanh Tùng, 10/5/2020, "Tấn công TCP Syn Flood", 23 january 2021, https://ngtung.medium.com/t%E1%BA%A5n-c%C3%B4ng-tcp-syn-flood-4dea6b426917.

[31] Academy, 2020, "Phishing là gì?", 23 january 2021, https://academy.binance.com/vi/articles/what-is-phishing.

[32] Nguyettt, 13/6/2018, "Spear Phishing - Hãy coi chừng "bạn bè" của bạn", 23 january 2021, https://bizflycloud.vn/tin-tuc/spear-phishing-hay-coi-chung-ban-be-cua-ban-20180612184241881.htm.

[33] apsachieveonline, 2020, "Spear Phishing là gì và làm thế nào để bảo vệ bản thân khỏi nó", 23 january 2021, https://apsachieveonline.org/spear-phishing-la-gi-va-lam-the-nao-de-bao-ve-ban-than-khoi-no/.

[34] vietnambiz, 18/10/2019, "Sâu máy tính (Computer Worm) là gì? Làm thế nào để ngăn chặn sâu máy tính?", 23 january 2021, https://vietnambiz.vn/sau-may-tinh-computer-worm-la-gi-lam-the-nao-de-ngan-chan-sau-may-tinh-20191018111536798.htm.

[35] Hoàng Anh Hồng, 9/2020, "Virus - Worm - Trojan khác nhau như thế nào?", 23 january 2021, https://tinhte.vn/thread/virus-worm-trojan-khac-nhau-nhu-the-nao.3190578/.

[36] congnghedt, 2020, "Để Trở Thành Chuyên Gia Bảo Mật (Module7 - P1) Sự Khác Biệt Giữa Virus Và Worm", 23 january 2021, https://congnghecit.com/de-tro-thanh-chuyen-gia-bao-mat-module7-p1-su-khac-biet-giua-virus-va-worm.html.

[37] Doan Thi Hanh, 19/2020, "Man-in-the-Middle Attack (MITM)", 23 january 2021, https://viblo.asia/p/man-in-the-middle-attack-mitm-aWj53LMbK6m.

[38] Darksider, 2020-07-03, "Bạn Đã Biết Tự Bảo Vệ Trước Tấn Công MITM?", 23 january 2021, https://codelearn.io/sharing/ban-da-biet-tu-bao-ve-truoc-tan-cong-mitm.

[39] Hoàng Tùng, 7/5/2018, "Tìm hiểu về tấn công Man in the middle", 23 january 2021, https://ssl.vn/tim-hieu-ve-tan-cong-man-in-the-middle.html.

[40] Nguyễn Hợp Quang, 13/5/2019, "Cách thực hiện tấn công MITM (MAN-IN-THE-MIDDLE ATTACK) bằng ETTERCAP", 23 january 2021, https://kipalog.com/posts/Cach-thuc-hien-tan-cong-MITM--MAN-IN-THE-MIDDLE-ATTACK---bang-ETTERCAP.

[41] Securitybox, 2020, "6 HÌNH THỨC TẤN CÔNG MẠNG PHỔ BIẾN VÀ CÁCH PHÒNG CHỐNG HIỆU QUẢ", ", 23 january 2021, https://securitybox.vn/9668/cac-hinh-thuc-tan-cong-mang-pho-bien-va-cach-phong-chong/.

[42] Resources, 2020, "Các phương thức tấn công mạng và cách phòng chống", 23 january 2021, https://resources.cystack.net/cac-phuong-thuc-tan-cong-mang-va-cach-phong-chong/.

[43] Willandway, 4/9/2020, "Các hình thức tấn công mạng phổ biến năm 2020", 23 january 2021, https://willandway.vn/cac-hinh-thuc-tan-cong-mang-pho-bien/.

[44] Long Văn, 2020, "Các hình thức tấn công mạng hiện nay và giải pháp hạn chế hiệu quả", 23 january 2021, https://longvan.net/cac-hinh-thuc-tan-cong-mang-hien-nay-va-giai-phap-han-che-hieu-qua.html.

[45] Topdev, 2020, "SQL Injection là gì? Cách giảm thiểu và phòng ngừa SQL Injection", 23 january 2021, https://topdev.vn/blog/sql-injection/.

[46] Gia Hiệp, 2020, "SQL Injection là gì ? Có bao nhiêu kiểu tấn công SQL Injection ?", 23 january 2021, https://giaphiep.com/blog/sql-injection-la-gi-co-bao-nhieu-kieu-tan-cong-sql-injection-26088.

[47] Antoanthongtin, 10/6/2016, "Tối ưu hóa tấn công BLIND SQL INJECTION", 23 january 2021, http://antoanthongtin.gov.vn/giai-phap-khac/toi-uu-hoa-tan-cong-blind-sql-injection-101512.

[48] Securitydaily, 7/9/2016, "Tối ưu thời gian khai thác Blind SQL injection", 23 january 2021, https://securitydaily.net/toi-uu-thoi-gian-khai-thac-blind-sql-injection/.

[49] Vietsunshine, 14/8/2018, "Malware là gì? có những loại Malware nào? cơ chế hoạt động của Malware.", 23 january 2021, https://www.vietsunshine.com.vn/2018/08/14/malware-la-gi-co-nhung-loai-malware-nao-co-che-hoat-dong-cua-malware/.

[50] Vũ Trần, 2/12/2020, "TẤN CÔNG MẠNG (CYBER-ATTACK) LÀ GÌ?", 23 january 2021, https://cyberkid.vn/tan-cong-mang-la-gi/.