**Họ tên:** Nguyễn Huỳnh Minh Tiến

**MSSV:** 18110377

**Bài kiểm tra số 2** – môn ATTT (lớp chiều thứ 5)

Thời gian: 12:45 – 16:00

SV được phép tham khảo tài liệu

**Câu 1. (3 điểm) Malware là gì? Trình bày đặc điểm của một số loại malware phổ biến. Giải pháp phòng chống malware trong một hệ thống CNTT?**

**Trả lời:**

Phần mềm độc hại là một đoạn mã (có thể ở dạng phần mềm) được thiết kế có chủ ý để ảnh hưởng đến hệ thống máy tính. Sau khi được cài đặt vào hệ thống máy tính, nó có thể truy cập tài nguyên của hệ thống máy tính, có thể chia sẻ dữ liệu đến một số máy chủ từ xa mà không cần người dùng can thiệp hoặc có thể theo dõi chi tiết người dùng, v.v.

**Đặc điểm một số loại malware phổ biến:**

* **Viruses**

Vi-rút máy tính sửa đổi các tệp máy chủ hợp pháp khác (hoặc con trỏ tới chúng) theo cách mà khi tệp của nạn nhân được thực thi, vi-rút cũng được thực thi.

* **Worms**

Worm có khả năng tự nhân bản chính nó mà không cần cấy vào một tập tin lưu trữ. Chúng còn thường sử dụng Internet để lây lan, do đó gây thiệt hại nghiêm trọng cho một mạng lưới về tổng thể, trong khi virus thường chỉ nhắm vào các tập tin trên máy tính bị nhiễm. Worm lây lan chủ yếu là do các lỗ hổng bảo mật của hệ thống.

* **Trojans**

Trojans cải trang làm chương trình hợp pháp, nhưng chúng chứa các kiến trúc độc hại (chương trình độc hại ngụy trang như một cái gì đó được cho là lành tính).

Một Trojan phải được thực thi bởi nạn nhân của nó để thực hiện công việc của nó. Trojan thường đến qua email hoặc được người dùng tác động khi họ truy cập các trang web bị nhiễm. Loại Trojan phổ biến nhất là chương trình chống vi-rút giả, bật lên và tuyên bố bạn bị nhiễm, sau đó hướng dẫn bạn chạy chương trình để dọn dẹp PC của bạn. Người dùng mắc bẫy và Trojan chiếm quyền root.

* **Hybrids và Các hình thức khác**

Ngày nay, hầu hết các phần mềm độc hại là sự kết hợp của các chương trình độc hại truyền thống, thường bao gồm các phần của Trojan và sâu và đôi khi là virus. Thông thường chương trình phần mềm độc hại xuất hiện dưới dạng Trojan, nhưng sau khi được thực thi, nó sẽ tấn công các nạn nhân khác qua mạng như một con sâu (worm).

Nhiều chương trình phần mềm độc hại ngày nay được coi là rootkit hoặc chương trình tiềm ẩn. Về cơ bản, các chương trình phần mềm độc hại cố gắng sửa đổi hệ điều hành cơ bản để kiểm soát tối đa và ẩn khỏi các chương trình chống phần mềm độc hại. Để loại bỏ các loại chương trình này, bạn phải xóa thành phần kiểm soát khỏi bộ nhớ, bắt đầu bằng quá trình quét phần mềm chống phần mềm độc hại.

Các bot về cơ bản là sự kết hợp Trojan / worm, chúng cố gắng làm cho các máy khách bị khai thác riêng lẻ trở thành một phần của mạng độc hại lớn hơn. Botmasters có một hoặc nhiều máy chủ “chỉ huy và kiểm soát” mà máy khách bot đăng ký để nhận hướng dẫn cập nhật của họ. Botnet có kích thước từ vài nghìn máy tính bị xâm nhập đến các mạng khổng lồ với hàng trăm nghìn hệ thống dưới sự kiểm soát của một bậc thầy botnet. Những botnet này thường được thuê cho các tội phạm khác, những người sau đó sử dụng chúng cho mục đích bất chính của họ.

* **Ransomware**

Ransomware là các chương trình phần mềm độc hại mã hóa dữ liệu của nạn nhân và giữ nó làm con tin chờ thanh toán tiền điện tử, thường làm tê liệt các công ty, bệnh viện, sở cảnh sát và thậm chí toàn bộ thành phố.

Hầu hết các chương trình ransomware là Trojans, chúng phải được lan truyền thông qua kỹ thuật truyền thông. Sau khi được thực thi, chúng sẽ tìm kiếm và mã hóa các tập tin của người dùng trong vòng vài phút, mặc dù một số chủng loại sẽ thực hiện cách tiếp cận chờ đợi và xem.

* **Phần mềm độc hại không cần tệp – Fileless malware**

Fileless malware là một loại phần mềm độc hại khai thác và kiên trì phá hoại, không trực tiếp sử dụng tệp hoặc hệ thống tệp. Thay vào đó, chúng chỉ khai thác và phát tán trong bộ nhớ hoặc sử dụng các đối tượng non-file OS khác như các registry keys, API hoặc các tác vụ theo lịch trình.

Nhiều cuộc tấn công fileless bắt đầu bằng cách khai thác một chương trình hợp pháp hiện có, trở thành một tiến trình con mới được sinh ra, có thể sử dụng các công cụ hợp pháp hiện có được tích hợp trong HĐH (như Microsoft PowerShell). Kết quả cuối cùng là các cuộc tấn công fileless là rất khó phát hiện và dừng lại.

* **Phần mềm quảng cáo – Adware**

Phần mềm quảng cáo cố gắng đưa người dùng cuối bị xâm nhập vào các quảng cáo độc hại, không mong muốn. Một chương trình phần mềm quảng cáo phổ biến có thể chuyển hướng tìm kiếm trình duyệt của người dùng đến các trang web giống nhau có chứa các quảng cáo sản phẩm khác.

* **Quảng cáo độc hại – Malvertising**

Tội phạm mạng có thể trả tiền để đặt quảng cáo trên một trang web hợp pháp. Khi người dùng nhấp vào quảng cáo, mã trong quảng cáo sẽ chuyển hướng họ đến một trang web độc hại rồi cài đặt phần mềm độc hại trên máy tính của họ. Trong một số trường hợp, phần mềm độc hại được nhúng trong quảng cáo có thể tự động thực hiện mà không cần bất kỳ hành động nào từ người dùng, một kỹ thuật được gọi là tải xuống bằng cách lái xe trên đường.

Tội phạm mạng cũng đã được biết là thỏa hiệp các mạng quảng cáo hợp pháp cung cấp quảng cáo cho nhiều trang web, biến các trang web lớn trở thành vectơ cho quảng cáo độc hại, khiến người dùng của họ gặp nguy hiểm.

Mục tiêu của tội phạm mạng sử dụng quảng cáo độc hại là để kiếm tiền. Quảng cáo độc hại có thể cung cấp bất kỳ loại phần mềm độc hại kiếm tiền nào, bao gồm phần mềm ransomware, tập lệnh mã hóa hoặc Trojan ngân hàng.

* **Phần mềm gián điệp – Spyware**

Phần mềm gián điệp thường được sử dụng bởi những người muốn kiểm tra hoạt động trên máy tính của những người thân trong gia đình. Tất nhiên, trong các cuộc tấn công có chủ đích, bọn tội phạm có thể sử dụng phần mềm gián điệp để ghi lại các lần bấm phím của nạn nhân và có quyền truy cập vào mật khẩu hoặc tài sản trí tuệ.

* **Bots và Botnets**

Còn được gọi là robot, bot là các chương trình độc hại được thiết kế để xâm nhập vào máy tính và tự động trả lời và thực hiện các hướng dẫn nhận được từ máy chủ chỉ huy và điều khiển trung tâm. Bots có thể tự sao chép (như sâu) hoặc sao chép thông qua hành động của người dùng (như virus và Trojan).

Toàn bộ mạng lưới các thiết bị bị xâm nhập được gọi là botnet. Một trong những cách sử dụng phổ biến nhất của botnet là khởi chạy tấn công từ chối dịch vụ phân tán (DDoS) nhằm cố gắng làm cho máy hoặc toàn bộ miền không khả dụng.

* **Phần mềm chống vi rút giả mạo – Fake-Antivirus Malware**

Một sự lây nhiễm khiến bạn tin rằng giải pháp bảo mật của bạn đã tìm thấy một loạt phần mềm độc hại và cần nhiều tiền hơn để làm sạch nó.

Nó là những phần mềm giả mạo phần mềm chống virus, nhưng thực tế là không. Điều này thường được biết đến như là một Fake-Antivirus hoặc Scarware. Mục đích của nó là lừa bạn tin rằng máy tính của bạn bị lây nhiễm nghiêm trọng để bạn mua phiên bản đầy đủ của chúng để dọn sạch.

* **Rootkits**

Mục đích của rootkit là để ẩn các chương trình độc hại đang chạy và thực hiện các hoạt động xấu trên hệ thống của nạn nhân (thu thập dữ liệu, đánh cắp danh tính, v.v.). Đây là lý do tại sao khi bị nhiễm các loại phần mềm độc hại khác nhau, rất có thể nạn nhân cũng đã bị một rootkit che giấu hoạt động của chúng trên hệ thống.

**Giải pháp phòng chống malware trong một hệ thống CNTT:**

* **Đào tạo nâng cao nhận thức của người dùng trong hệ thống** : Đào tạo và hướng dẫn nhân viên nhận diện được các thư điện tử độc hại
* **Cài đặt phần mềm Anti-Virus**
* **Chỉ cài đặt phần mềm hợp pháp:** Vì các phần mềm không hợp pháp thường chứa phần mềm độc hại trong đó.
* **Cài đặt phần mềm từ nguồn đã biết**
* **Cập nhật hệ điều hành:** vì các bản cập nhật này thường chứa các định nghĩa để phát hiện phần mềm độc hại.
* **Cập nhật bản vá phần mềm,** đặc biệt là các phần mềm anti-virus
* **Dùng Sanboxie:** Chạy các phần mềm không rõ nguồn gốc trong Sanboxie, sau khi xác định được phần mềm có chứa mã độc hay không thì mới xem xét chạy trên máy thật.
* **Sao lưu dự phòng:** Xác định dữ liệu quan trọng và lập chiến lược dự phòng hiệu quả. Có các bản sao lưu an toàn và cập nhật tất cả các thông tin quan trọng là một biện pháp bảo vệ quan trọng, đặc biệt là chống lại ransomware. Trong trường hợp ransomware tấn công một số thiết bị, có bản sao lưu gần nhất có nghĩa là bạn có thể khôi phục dữ liệu đó và hoạt động trở lại nhanh chóng.
* **Lập kế hoạch ứng phó khi xảy ra tấn công ransomeware**

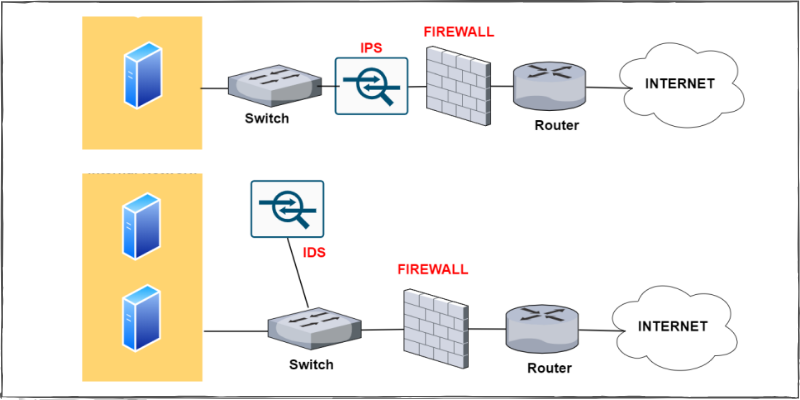
**Câu 2. (4 điểm) Trình bày đặc điểm của Firewall và IDS/IPS.** **Giải pháp triển khai Firewall và IDS/IPS trong hệ thống CNTT?**

* **Tường lửa:**
* Là một phần của hệ thống máy tính hoặc mạng được thiết kế để ngăn chặn lưu lượng truy cập trái phép từ mạng này sang mạng khác. Tường lửa giúp tách các thành phần đáng tin cậy và không đáng tin cậy của mạng; phân biệt các mạng trong một mạng đáng tin cậy.
* Các chức năng chính của tường lửa là lọc dữ liệu, chuyển hướng lưu lượng truy cập và bảo vệ chống lại các cuộc tấn công mạng.
* Tất cả lưu lượng truy cập giữa các vùng tin cậy sẽ đi qua tường lửa. Chỉ lưu lượng truy cập được ủy quyền, như được định nghĩa bởi chính sách bảo mật, mới được phép đi qua. Các bức tường lửa chính nó phải được miễn dịch với sự xâm nhập, mà ngụ ý bằng cách sử dụng một hệ thống cứng với hệ điều hành bảo đảm.
* **IDS/IPS:**
* IDS (Hệ thống **Phát hiện** Sự xâm nhập): là hệ thống phát hiện các dấu hiệu của tấn công xâm nhập, đồng thời có thể khởi tạo các hành động trên thiết bị khác để ngăn chặn tấn công. Nhận ra tấn công bằng cách phân tích bản sao của lưu lượng mạng. IDS không thực hiện các thao tác ngăn chặn truy xuất mà chỉ theo dõi các hoạt động trên mạng để tìm ra các dấu hiệu của tấn công và cảnh báo cho người quản trị mạng. Bên cạnh đó IDS sẽ đánh giá sự xâm nhập đáng ngờ khi nó đã diễn ra đồng thời phát ra cảnh báo, nó theo dõi được các cuộc tấn công có nguồn gốc từ bên trong một hệ thống.

Hai thành phần quan trọng nhất cấu tạo nên hệ thống IDS là sensor (bộ cảm nhận) có chức năng chặn bắt và phân tích lưu lượng trên mạng và các nguồn thông tin khác để phát hiện dấu hiệu xâm nhập (signature); signature database là cơ sở dữ liệu chứa dấu hiệu của các tấn công đã được phát hiện và phân tích. Cơ chế làm việc của signature database giống như virus database trong các chuơng trình antivirus, do vậy, việc duy trì một hệ thống IDS hiệu quả phải bao gồm việc cập nhận thường xuyên cơ sở dữ liệu này.

IDS có 2 loại thường dùng:

* **NIDS:** Sử dụng cảm biến để giám sát tất cả lưu lượng mạng, không thể xem các hoạt động trong chính máy tính.
* **HIDS:** Cài đặt trên máy trạm/Máy chủ, để xem hoạt động bất thường.
* IPS (Hệ thống **Ngăn chặn** xâm nhập): là hệ thống được phát triển mở rộng dựa trên khả năng của các hệ thống phát hiện tấn công xâm nhập (Intrusion Detection System – IDS). IPS chặn đứng trước khi tấn công đến mạng bên trong. Cung cấp khả năng bảo vệ mạng dựa vào định danh, phận loại và ngăn chặn mối đe dọa đã biết hoặc chưa... IPS nằm trên đường đi của dữ liệu, chủ động, nên có thể ngăn chặn trước khi bị tấn công.
* **Giải pháp triển khai Firewall và IDS/IPS trong hệ thống CNTT:**



* **Firewall:** Thường được đặt ở phía trước của mạng để kiểm soát lưu lượng, cho phép hoặc chặn lưu lượng giữa các vùng mạng khác nhau (Chặn hoặc cho phép các gói ở cấp độ mạng). Thường hoạt động đến Lớp 4 để cho phép hoặc chặn địa chỉ IP và các cổng. Thường có nhiều giao diện mạng vật lý để phân đoạn mạng thành các vùng bảo mật khác nhau.
* **IPS/IDS:** Thường được đặt sau tường lửa dưới dạng nội tuyến hoặc ngoài băng tần. Chuyên dụng để kiểm tra các gói tin mạng để so khớp chúng với chữ ký của các cuộc tấn công độc hại đã biết. Khi đó, lưu lượng mạng bị tắc nghẽn hoặc báo động được phát ra (Phát hiện các cuộc tấn công và chặn lưu lượng truy cập trực tiếp hoặc gửi báo động). Phát hiện bất thường dựa trên chữ ký, dựa trên quy tắc, thống kê, v.v. yêu cầu hệ thống phần cứng phải có hiệu suất cao để thực hiện Deep Packet Inspection và không làm chậm lưu lượng.

**Câu 3.** **(3 điểm) Trình bày các mục tiêu của kỹ thuật mật mã; các ứng dụng mật mã trong an toàn thông tin.**

* **Các mục tiêu của kỹ thuật mật mã:**
* Bảo mật (Confidentiality): Thông tin không bao giờ có thể được tiết lộ cho người không được phép xem thông tin đó.
* Nhận dạng (Identification) và xác thực (Authentication): Trước khi bất kỳ thông tin nào được trao đổi, hãy xác định và sau đó cho phép cả người gửi và người nhận.
* Tính toàn vẹn (Integrity): Thông tin không được sửa đổi trong lưu trữ hoặc quá cảnh. Bất kỳ sửa đổi phải được phát hiện.
* Không từ chối (Non-repudiation): Không thể từ chối việc tạo/truyền tin nhắn. Điều này cung cấp tính hợp pháp "kỹ thuật số" và truy xuất nguồn gốc của một giao dịch.
* **Các ứng dụng của mật mã trong an toàn thông tin:**

Ứng dụng của mật mã vào thực tế thông qua một số giao thức bảo mật là:

* Keberos: là giao thức dùng để chứng thực dựa trên mã hóa đối xứng.
* Chuẩn chứng thực X509: dùng trong mã hóa khóa công khai.
* Secure Socket Layer (SSL): là giao thức bảo mật Web, được sử dụng phổ biến trong Web và thương mại điện tử.
* PGP và S/MIME: bảo mật thư điện tử email.