EMAIL

EMAIL

Thư điện tử (email hay e-mail) là một phương thức trao đổi tin nhắn giữa những người sử dụng các thiết bị điện tử.

Một hệ thống email thường có 3 thành phần chính: Bộ phận trợ giúp người dùng (User Agent), Mail Server và các giao thức mà các thành phần này dùng để giao tiếp với nhau.

Người ta phân loại các giao thức như sau:

+ Giao thức giữa các mail servers bao gồm:

SMTP (Simple Mail Transfer Protocol): được các server dùng để chuyển thư qua lại với nhau. Thông tin chi tiết về giao thức này được mô tả trong tài liệu RFC 822.

+ Giao thức giữa mail server và user agent bao gồm:

POP3 (Post Offic Protocol version 3 [RFC 1939]): được user agent sử dụng để lấy thư về từ hộp thư của nó trên server.

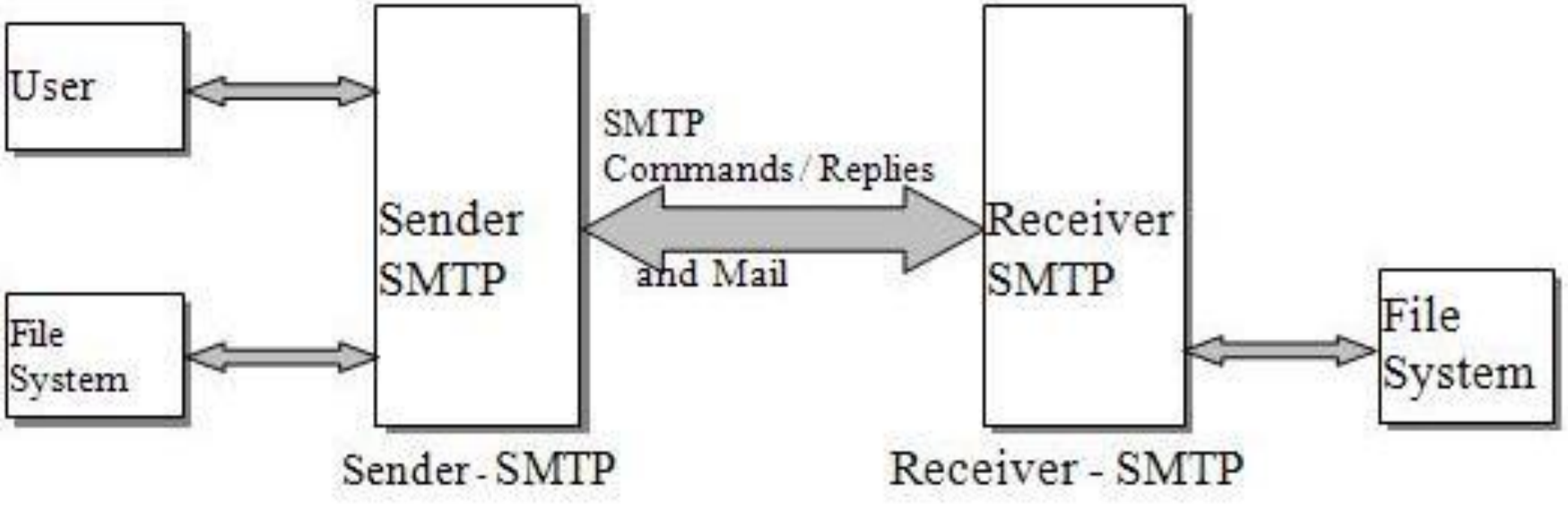
SMTP: được user agent sử dụng để gởi thư ra server.

IMAP: (Internet Mail Access Protocol [RFC 1730]): Có nhiều tính năng vượt trội hơn POP3. Ngoài ra IMAP còn cho phép gởi mail.

Giao thức SMTP

SMTP (viết tắt của Simple Mail Transfer Protocol) là giao thức truyền tải thư tín đơn giản. Nó là hệ thống chuyển tải các thư điện tử qua mạng Internet, máy chủ này sẽ hỗ trợ các phần mềm chuyên gửi mail như Google, Yahoo có thể gửi nhiều thư tín cùng một lúc tới các máy chủ khác nhau.

SMTP là thủ tục phát triển ở mức ứng dụng trong mô hình 7 lớp OSI cho phép gởi các bức điện trên mạng TCP/IP. SMTP được phát triển vào năm 1982 bởi tổ chức IETF (Internet Engineering Task Force). SMTP sử dụng cổng 25 của TCP.



Mô hình tổng quát sử dụng giao thức SMTP

CÁC KHÁI NIỆM LIÊN QUAN

+ MIME
+ BASE64

MIME

Giao thức mở rộng thư điện tử Internet đa mục đích hay MIME (Multipurpose Internet Mail Extensions) là một tiêu chuẩn Internet về định dạng cho thư điện tử. Hầu như mọi thư điện tử Internet được truyền qua giao thức SMTP theo định dạng MIME. Vì gắn liền với chuẩn SMTP và MIME nên đôi khi thư điện tử Internet còn được gọi là thư điện tử SMTP/MIME.

BASE64

Base64 là một chương trình mã hóa chuỗi ký tự bằng cách dùng thay thế các ký tự trong bảng mã ASCII 8 bit thông dụng thành bảng mã 6 bit. Nó thường được sử dụng để mã hóa các tập tin đa phương tiện (hình ảnh, âm thanh, video,…). Ký tự 64 trong Base64 là đại diện cho 64 ký tự trong bãng mã ASCII. Base64 thường được sử dụng trong việc truyền tải email.

Mã hoá file theo chuẩn Base64.

Chuẩn Base64 là một tập hợp gồm các ký tự (theo đúng thứ tự) : từ A đến Z, từ a đến z, từ 0 đến 9, dấu +, dấu /

Tổng cộng là 64 ký tự biểu diễn 64 giá trị từ 0 đến 63. Như vậy, ký tự từ A đến Z biểu diễn cho các giá trị từ 0 đến 25, từ a đến z biểu diễn cho giá trị từ 26 đến 51, từ 0 đến 9 biểu diễn cho giá trị từ 52 đến 61, dấu + biểu diễn cho giá trị 62, dấu / biểu diễn cho giá trị 63.

Một ký tự biểu diễn theo mã ASCII sẽ dùng 8 bits. Một ký tự theo Base64 sẽ dùng 6 bits. Như vậy, một file ở dạng Base64 sẽ có kích thước lớn hơn khi ở dạng ASCII. Cụ thể, sẽ lớn gấp 4/3 lần (8 bits/6 bits).

Để chuyển đổi file sang dạng Base64, ta thực hiện theo các bước như sau :

1. Đọc nội dung file dưới dạng bit.
2. Cứ 6 bits ta tách thành một nhóm để xử lý.
3. Tra bảng mã Base64, mỗi nhóm 6 bits sẽ có giá trị tương ứng với một ký tự.
4. Ghi ra file các ký tự đó.

⇒ https://www.base64encode.org/

⇒ https://www.base64decode.org/

MÃ ĐỘC

Mã độc (Malware - Malicious Software)là phần mềm xâm nhập, hoạt động trên hệ thống mà không được sự cho phép của người sử dụng.

Một số hành vi của mã độc:

+ Thu thập các thông tin từ các máy chủ, máy tính cá nhân.

+ Ghi lại thông tin bàn phím, chụp ảnh màn hình, nghe lén, quay lén.

+ Lợi dụng tài nguyên máy tính để đào tiền ảo, quảng cáo …

=> Tất cả mô tả có tại bwiki.bkav.com và malware behavior

MÃ ĐỘC

Đặc điểm của mã độc:

+ Hoạt động lén lút, tiến trình không có giao diện, không icon.

+ File thực thi được cất trong các thư mục như %temp% để người dùng không phát hiện.

+ Mã độc thường có tính năng khởi động cùng hệ điều hành để có thể chạy lên mỗi khi người dùng bật máy (Tính năng này có thể thực hiện đơn giản bằng cách tạo một value tại đường dẫn Registry: HKCU\Software\Microsoft\Windows\CurrentVersion\Run)

BÀI TẬP

Viết một chương trình ghi lại các thao tác nhập từ bàn phím vào một file log (Sử dụng kỹ thuật Hook đã học từ tuần 4).

File log này sẽ được định kỳ gửi về hòm thư email.

Lưu ý:

Các thông tin ghi nhận được sẽ được lưu trong file log theo cấu trúc: Tên cửa sổ + Nội dung key log. Khi người dùng đổi cửa sổ cần cập nhật lại tên cửa sổ đang thao tác.

Nâng cao: Hoàn thiện chương trình mã độc từ chương trình ở trên

+ Tiến trình chạy không có giao diện, không có icon.

+ Khi kích đúp file mã độc ở desktop, file mã độc sẽ tự xóa chính nó và tự sao chép vào thư mục %temp%, thuộc tính của file mã độc ở %temp% là thuộc tính ẩn.

+ Mã độc có tính năng khởi động cùng máy tính mỗi máy tính được bật (Thao tác với Registry, đã được học ở tuần 2).

END.