Tổng hợp ND

Created By	
Last Edited By	

Foundations

Security Triad

Mô hình CIA (Confidentiality, Integrity and Availability)

- **Confidentiality** : tính bảo mật, bí mật đảm bảo chỉ những người đủ quyền mới được đọc thông tin.
- **Integrity** : tính toàn vẹn, chắc chắn dữ liệu là chính xác và không bị sửa đổi.
- **Availability** : tính sẵn sàng, đảm bảo khả năng truy xuất dữ liệu mọi lúc.

Network Topologies (cấu trúc mạng)

là sơ đồ mô tả về sự sắp xếp của các phần tử vật lý và logic của một mạng truyền thông.

Cấu trúc liên kết mạng đề cập đến cách thức mà các liên kết và nodes của một mạng được sắp xếp để hoạt động với nhau.

Các cấu trúc liên kết được phân thành một số loại chính như sau:

- Physical network topology: Cấu trúc liên kết mạng vật lý, là phương tiện truyền tín hiệu vật lý
- Logical network topology: Cấu trúc liên kết mạng logic, đề cập đến cách thức mà dữ liệu truyền qua mạng giữa các thiết bị, đồng thời chúng cũng độc lập - tách biệt với kết nối vật lý.

Các ví dụ về cấu trúc liên kết mạng logic là mạng Ethernet sử dụng cáp xoắn đôi.

Cấu trúc liên kết mạng vật lý (thường là mạng LAN) có 3 dạng cấu trúc khác nhau:

- Star Topology: Cấu trúc liên kết mạng dạng hình sao

  Kết nối mỗi thiết bị trong mạng với một Hub trung tâm. Các thiết bị chỉ có thể giao tiếp với nhau một cách gián tiếp thông qua Hub (giờ thay thế bằng Switch hoặc Router).

- Ring Topology: Cấu trúc liên kết mạng dạng vòng

  Tạo hai liên kết “điểm <-> điểm” chuyên dụng kết nối một thiết bị với hai thiết bị, tạo ra một vòng thiết bị qua đó dữ liệu được chuyển tiếp qua bộ lặp cho đến khi nó đến thiết bị đích.

- Linear Bus Topology: Cấu trúc liên kết mạng dạng tuyến

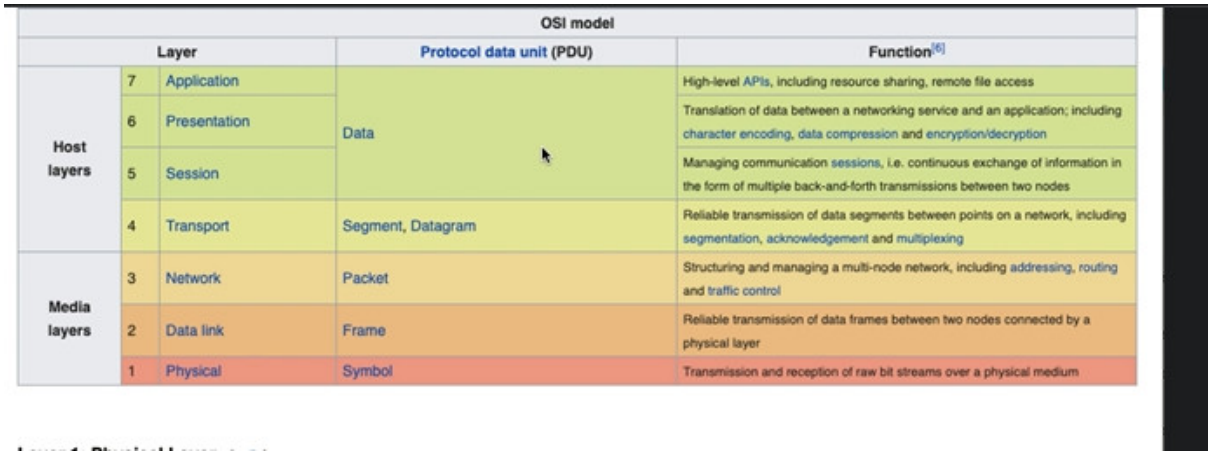
  Còn được gọi là cấu trúc liên kết mạng đường trục, cấu trúc liên kết mạng dạng tuyến.

  Đặc điểm của mạng dạng Bus là kết nối tất cả các thiết bị với một cáp chính thông qua đường dây thả.

  Ưu điểm của cấu trúc liên kết mạng bus nằm ở sự đơn giản của nó, vì cần ít cáp hơn so với các cấu trúc liên kết mạng khác giúp dễ dàng lắp đặt.

Communications Models

Mô hình kết nối hệ thống mở: OSI



OSI model

Layer			Protocol data unit (PDU)	Function[6]
Host layers	7	Application	Data	High-level APIs, including resource sharing, remote file access
	6	Presentation		Translation of data between a networking service and an application; including character encoding, data compression and encryption/decryption
	5	Session		Managing communication sessions, i.e. continuous exchange of information in the form of multiple back-and-forth transmissions between two nodes
	4	Transport	Segment, Datagram	Reliable transmission of data segments between points on a network, including segmentation, acknowledgement and multiplexing
Media layers	3	Network	Packet	Structuring and managing a multi-node network, including addressing, routing and traffic control
	2	Data link	Frame	Reliable transmission of data frames between two nodes connected by a physical layer
	1	Physical	Symbol	Transmission and reception of raw bit streams over a physical medium

- lớp 1: hệ thống cáp, switch

  Tất cả các yếu tố vật lý như cáp, thẻ giao diện mạng thiết bị chuyển mạch và bộ định tuyến

- lớp 2: Liên kết dữ liệu: định địa chỉ, so địa chỉ của lớp liên kết dữ liệu là địa chỉ kiểm soát truy cập phương tiện hoặc địa chỉ MAC

  Bất kỳ giao thức nào có luồng truyền thông và chuẩn bị sẵn sàng để đưa nó lên phương tiện truyền thông vật lý như Ethernet

- Lớp 3: mạng: nơi giao thức Internet hoặc IP live, là nơi nhận được địa chỉ IP hoặc một lớp mạng chịu trách nhiệm di chuyển từ một mạng sang mạng khác nơi liên kết dữ liệu thực sự chỉ nhận tin nhắn trên mang local

  các giao thức đảm nhận tin nhắn từ mạng này sang mạng khác như IP

- Lớp 4: truyền tải: UDP và TCP là nơi bắt đầu giải quyết bằng các cổng ở trên đó

  các giao thức cung cấp ghép kênh truyền thông và quản lý luồng giao tiếp end to end như TCP và UDP

- Lớp 5: bắt đầu đi vào lớp phiên xử lý các phiên. So bất cứ điều gì có một kết nối lâu dài phải được quản lý sẽ được xử lý tại đây

  Các giao thức duy trì thông tin về giao tiếp hai chiều tồn tại trong một khoảng thời gian, bao gồm NetBIOS và Giao thức đường hầm point to point

- Lớp 6: trình bày: bất kỳ: vd JPEG là một định dạng tồn tại mà lớp trình bày

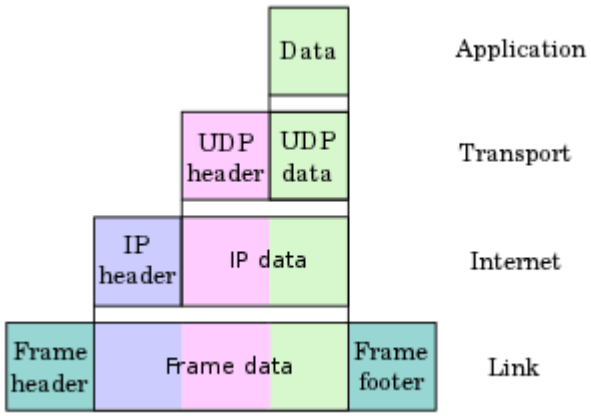
  bất cứ điều gì tập trung vào việc đại diện dữ liệu, bao gồm ASCII cũng như mã hóa

- Lớp 7: Ứng dụng: lớp có API cấp cao bao gồm file chia sẻ tài nguyên, remote truy cập tập tin

các giao thức tương tác với người dùng như HTTP

→ mỗi lớp có một đơn vị dữ liệu và giao thức khác nhau

Kiến trúc TCP/IP



- Lớp 1 = 1 2 :
- Lớp 2 = 3 network:
- Lớp 3 = 4 transport:
- Lớp 4 = 567 Application: giống với các lớp ứng dụng trình bày trong OSI

Đôi khi sẽ nghe thấy các lớp được gọi là bằng chứng số của chúng. Khi điều này được thực hiện, đó là mô hình OSI sẽ được sử dụng

VD: Lớp 7 là lớp ứng dụng, lớp 2 là lớp liên kết dữ liệu, khi nói về địa chỉ lớp 2 đang nói về địa chỉ kiểm soát truy cập phương tiện (MAC)

Hoặc khi nói đến đơn vị dữ liệu giao thức (PDU): là thuật ngữ sử dụng để mô tả dữ liệu bao gồm các tiêu đề và dữ liệu được đóng gói từ một lớp cụ thể.

Ở lớp 1, PDU là bit, đôi khi được gọi là biểu tượng

Ở lớp 2, PDU là khung

Ở lớp 3: gói tin mặc dù đây thường là thuật ngữ chung cho dữ liệu trên dây

Ở lớp 4: là phân đoạn cho TCP hoặc gói dữ liệu cho UDP

OSI vs TCP/IP :

Với đóng gói. Dữ liệu di chuyển từ lớp này sang lớp tiếp theo bằng cách yêu cầu mỗi lớp thêm thông tin đánh dấu lớp cụ thể đó. Quá trình này được gọi là đóng gói

VD: một đoạn dữ liệu được gửi đến lớp truyền tải TCP hoặc UDP sẽ thêm một bộ tiêu đề cung cấp thông tin cần thiết để máy chủ nhận biết phải làm gì với dữ liệu. Khi dữ liệu được tạo, nó sẽ di chuyển xuống qua các lớp khác nhau, bắt đầu từ lớp ứng dụng. Mỗi lớp có thể thêm thông tin tiêu đề đóng gói trên đường đi. Khi nhận được tin nhắn, quá trình được đảo ngược. Mỗi lớp loại bỏ các tiêu đề trong một quá trình được gọi à khử đóng gói. Điều quan trọng là phải nhận ra rằng mỗi lớp trên máy chủ gửi đang giao tiếp cùng với một lớp trên máy chủ nhận

Mô hình OSI không phải là mô hình giao tiếp duy nhất được sử dụng, mặc dù khi nói đến TCP/IP, nó ít hơn là một mô hình và nhiều hơn là một kiến trúc như được xây dựng. Họ xây dựng các giao thức mà họ cần và sau đó ánh xạ các giao thức mà họ có thành 4 lớp (như ảnh trên)

UDP / IP là gì?
Giao thức gói dữ liệu người dùng, hay UDP, là một giao thức truyền tải được sử dụng rộng rãi khác

Nhanh hơn TCP, nhưng nó cũng kém tin cậy hơn. UDP không đảm bảo tất cả các gói được phân phối và theo thứ tự, và nó không thiết lập kết nối trước khi bắt đầu hoặc nhận truyền

Internet Protocol

Giao thức Internet (IP) là một giao thức, hoặc tập hợp các quy tắc, để định tuyến và định địa chỉ các gói dữ liệu để chúng có thể di chuyển qua các mạng và đến đích chính xác. Dữ liệu truyền qua Internet được chia thành các phần nhỏ hơn, được gọi là gói. Thông tin IP được đính kèm với mỗi gói và thông tin này giúp các bộ định tuyến gửi các gói đến đúng nơi. Mỗi thiết bị hoặc miền kết nối với Internet đều được gán một địa chỉ IP và khi các gói được chuyển hướng đến địa chỉ IP được đính kèm với chúng, dữ liệu sẽ đến nơi cần thiết

Khi các gói đến đích, chúng được xử lý khác nhau tùy thuộc vào giao thức truyền tải nào được sử dụng kết hợp với IP. Các giao thức truyền tải phổ biến nhất là TCP và UDP

Trong mạng, giao thức là một cách tiêu chuẩn hóa để thực hiện một số hành động và định dạng dữ liệu nhất định để hai hoặc nhiều thiết bị có thể giao tiếp và hiểu nhau

Tất cả các gói dữ liệu IP phải trình bày thông tin nhất định theo một thứ tự nhất định và tất cả các địa chỉ IP đều tuân theo một định dạng chuẩn hóa.

Địa chỉ IP là một mã định danh duy nhất được gán cho một thiết bị hoặc miền kết nối với Internet. Mỗi địa chỉ IP là một chuỗi các ký tự, chẳng hạn như '192.168.1.1'.

Thông qua trình phân giải DNS, dịch tên miền mà con người có thể đọc được thành địa chỉ IP, người dùng có thể truy cập các trang web mà không cần ghi nhớ loạt ký tự phức tạp này. Mỗi gói IP sẽ chứa cả địa chỉ IP của thiết bị hoặc miền gửi gói tin và địa chỉ IP của người nhận dự định
IP được tạo bằng cách thêm tiêu đề IP vào mỗi gói dữ liệu trước khi nó được gửi đi. Tiêu đề IP chỉ là một loạt các bit và ghi lại một số thông tin về gói tin, bao gồm cả địa chỉ IP gửi và nhận.

- Độ dài tiêu đề
- Độ dài gói
- Time To Live (TTL) hoặc số bước nhảy mạng mà một gói tin có thể thực hiện trước khi nó bị loại bỏ
- Giao thức truyền tải nào đang được sử dụng (TCP, UDP, v.v.)

Tổng cộng có 14 trường cho thông tin trong tiêu đề IPv4, mặc dù một trong số chúng là tùy chọn.

Routing IP
Internet được tạo thành từ các mạng lớn được kết nối với nhau, mỗi mạng chịu trách nhiệm cho một số khối địa chỉ IP nhất định; những mạng lớn này được gọi là hệ thống tự trị (AS). Một loạt các giao thức định tuyến giúp định tuyến các gói tin trên các ASes dựa trên địa chỉ IP đích của chúng. Bộ định tuyến có các bảng định tuyến cho biết ASes nào mà các gói nên đi qua để đến đích mong muốn càng nhanh càng tốt. Các gói đi từ AS đến AS cho đến khi chúng đến được một gói nhận trách nhiệm về địa chỉ IP được nhắm mục tiêu. AS đó sau đó định tuyến nội bộ các gói đến đích.

Các giao thức đính kèm các tiêu đề gói tin ở các lớp khác nhau của mô hình OSI:

Các giao thức đính kèm tiêu đề gói tin ở các lớp khác nhau của mô hình OSI
Các gói có thể đi các tuyến đường khác nhau đến cùng một nơi nếu cần thiết, giống như một nhóm người lái xe đến một điểm đến đã thỏa thuận có thể đi theo các con đường khác nhau để đến đó.

TCP được thiết kế cho độ tin cậy, không phải tốc độ. Vì TCP phải đảm bảo tất cả các gói đến theo thứ tự, việc tải dữ liệu qua TCP / IP có thể mất nhiều thời gian hơn nếu một số gói bị thiếu.

TCP và IP ban đầu được thiết kế để sử dụng cùng nhau và chúng thường được gọi là bộ TCP / IP. Tuy nhiên, các giao thức truyền tải khác có thể được sử dụng với IP.

Bluetooth

Bluetooth là công nghệ giao tiếp tầm ngắn

Công nghệ Bluetooth là một hệ thống không dây sử dụng sóng vô tuyến cho mục đích liên lạc. Nó có khả năng giao tiếp với nhiều thiết bị khác nhau cùng một lúc mà không cần giao diện. Đây là một tiêu chuẩn mở để truyền giọng nói kỹ thuật số trong phạm vi ngắn và hỗ trợ dữ liệu từ điểm đến điểm và ứng dụng nhân tới điểm. Nó có một liên kết vô tuyến tầm ngắn và giá cũng thấp.

Cloud Computing

Cloud Computing là việc cung cấp các dịch vụ điện toán hoàn toàn qua Internet. Hay nói đúng hơn là việc cung cấp tài nguyên phù hợp với nhu cầu người dùng hoàn toàn thông qua Internet. Các dịch vụ ở đây có thể bao gồm máy chủ, lưu trữ, phần mềm …

Lúc này bạn có thể lưu trữ tài liệu của mình đâu đó “lở lửng trên những đám mây” bằng một vài giải pháp nào đó uy tín như Google Drive hay OneDrive. Và chỉ cần có kết nối Internet, bạn có thể truy cập vào những dữ liệu đó ở bất cứ nơi đâu và bất cứ khi nào

Lợi ích:

- Tiết kiệm chi phí
- Khả năng mở rộng linh hoạt về quy mô
- Các dịch vụ điện toán lớn chạy trên mạng lưới trung tâm dữ liệu an toàn → hiệu năng ổn định
- Bảo mật
- Tốc độ
- Năng suất
- Độ tin cậy

Ethical Hacking Testing Methodology

Open Source

Open source hay mã nguồn mở là phần mềm có bộ source code mà bất cứ ai cũng có thể tải về sử dụng, sửa đổi hoặc thêm một số cập nhật, tính năng vượt trội khác.

Thông thường, mã nguồn mở được phát hành miễn phí bởi các đơn vị cung cấp, doanh nghiệp lớn về lĩnh vực công nghệ.

Lợi ích của việc sử dụng Open source:

- Khả năng quản trị và điều khiển cao
- Khả năng sáng tạo không giới hạn
- Mức độ an ninh và bảo mật cao
- Khả năng ổn định tốt

Nmap

(Network Mapper): là tiện ích mã nguồn mở được sử dụng để quét và phát hiện các lỗ hổng trong mạng. Nmap được sử dụng bởi Pentesters và chuyên gia bảo mật khác để khám phá các thiết bị đang chạy trong mạng của họ.

Nó cũng hiển thị các dịch vụ và cổng của mọi máy chủ, cho thấy các mối đe dọa tiềm ẩn

Nmap linh hoạt, từ việc giám sát một máy chủ duy nhất đến một mạng rộng bao gồm hơn một trăm thiết bị. Cốt lõi của Nmap là chứa một cổng quét cổng thu để thu thập thông tin bằng cách sử dụng các gói cho một máy chủ. Nmap thu thập phản hồi của các gói này và cho biết một cổng đang mở hay đóng, đang mở hay được lọc

Thực hiện quét Nmap cơ bản:

Nmap có khả năng quét và phát hiện một IP, một dải IP, tên DNS và quét nội dung từ các tài liệu văn bản

Phân tích kết quả: Nmap chỉ quét 1000 cổng đầu tiên theo mặc định nhưng điều này có thể được thay đổi bằng các lệnh khác nhau

→ Bằng cách sử dụng khuôn khổ Nmap và Metasploit, có thể bảo mật cơ sở hạ tầng CNTT

Cả hai ứng dụng tiện ích này đều có sẵn trên nhiều nền tảng, nhưng kali Linux cung cấp cấu hình cài đặt sẵn để kiểm tra tính bảo mật của mạng

Trong mạn Lan máy tính, tất cả các thiết bị được kết nối đều có địa chỉ IP riêng. Và giao thức ping được hỗ trợ bởi mỗi máy tính. Giao thức ping có thể xác định xem máy tính có được kết nối với mạng hay không.

Bạn được gửi yêu cầu ping đến máy tính và nếu nó phản hồi thì nó đã được kết nối

Nmap có một cách tiếp cận hơi khác, máy tính cũng phản hồi theo một cách nhất định đối với các gói mạng nhất định, tiện ích chỉ cần gửi các gói cần thiết và xem xét máy chủ nào đã gửi câu trả lời

Mọi thức trên cmd của Nmap không phải là một tùy chọn đều được coi là một đặc điểm kỹ thuật máy chủ mục tiêu

Trường hợp đơn giản nhất là xác định địa chỉ IP mục tiêu hoặc tên máy chủ để quét

Hơn thế cách Nmap tìm ra những dịch vụ nào đang chạy trên máy. Bản chất của tất cả các chương trình mạng là dựa trên các cổng. Để nhận được tin nhắn từ mạng, chương trình phải mở cổng trên máy tính của bạn và đợi các kết nối đến. Và để gửi tin nhắn qua mạng, bạn cần kết nối với một cổng chương trình (đích) khác. Sau đó chương trình sẽ cần mở cổng mà nó sẽ chờ phản hồi. Tiện ích nmap quét phạm vi cổng có sẵn trong quá trình quét mạng và cố gắng kết nối với từng cổng trong số chúng. Nếu kết nối thành công, trong hầu hết các trường hợp, bằng cách truyền một số gói, chương trình thậm chí có thể tìm ra phiên bản của phần mềm đang chờ kế nối đến cổng này

Password Cracking

John the Ripper là một trong những chương trình bẻ khóa mật khẩu nổi tiếng và được sử dụng rộng rãi nhất trên cửa sổ, Linux và cả hệ điều hành MacOS. Chương trình này là mã nguồn mở và đặc biệt nhằm mục đích bẻ khóa mật khẩu bằng vũ lực và cũng bằng từ điển, nó có khả năng bẻ khóa băm mật khẩu rất nhanh (tùy thuộc vào sức mạnh của bộ xử lý máy tính của bạn) và việc sử dụng nó thực sự đơn giản

John the Ripper là một công cụ bẻ khóa mật khẩu được viết bằng C và được các nhà phân tích bảo mật sử dụng rộng rãi để kiểm tra độ chắc chắn của khóa chống lại các cuộc tấn công vũ phu. Chương trình này có khả năng phá vỡ MD5, SHA-1 và nhiều hàm băm khác được sử dụng rộng rãi trong thế giới máy tính. Chương trình này có khả năng tự động phát hiện loại băm mà chúng tôi đang bẻ khóa, với mục đích giúp người dùng bẻ khóa nó dễ dàng hơn mà không phải lo lắng về loại băm mà nó đang cố gắng “phá vỡ”

Tấn công từ điển

Tải một hoặc nhiều bộ từ điển mật khẩu Internet dung lượng vài chục GB thì công cụ sẽ phụ trách test từng key này để tìm cách bẻ khóa mật khẩu. Quá trình này bao gồm việc tạo mã băm của mỗi mật khẩu, để sau này so sánh mã băm mà chúng ta muốn phá vỡ, nếu hàm băm giống nhau thì chúng ta đã phát hiện ra mật khẩu, nếu hàm băm không khớp thì đó không phải là khóa và chúng ta sẽ phải tiếp tục thử nghiệm

Check được cả số, chữ hoa, chữ thường và ký hiệu ngoài ra, nó còn có khả năng kết hợp các từ để kiểm tra nhiều sự kết hợp hơn nữa của mật khẩu và tìm khóa được sử dụng.

Tấn công vũ lực

Cuộc tấn công brute force bao gồm thử nghiệm tất cả các tổ hợp chữ cái, số và ký hiệu của một phím có độ dài nhất định.

Cách này chậm nhất vì nó sẽ kiểm tra tất cả các kết hợp và có thể mất hàng giờ, hàng ngày, thậm chí hàng năm để bẻ khóa mật khẩu đến một độ dài nhất định. Nhìn chung, việc bẻ khóa mật khẩu có hơn 12 ký tự sẽ khiến chúng ta mất nhiều thời gian để thực hiện nó bằng vũ lực

Rainbow Table Attack

Rainbow Table là một danh sách chứa các giá trị hash có số lượng mật khẩu ứng với số lượng ký tự nào đó. Sử dụng Rainbow Table có thể lấy một cách đơn giản giá trị hash được trích rút từ máy tính mục tiêu và thực hiện một tìm kiếm. Khi giá trị hash được tìm thấy trong bảng, bạn sẽ có mật khẩu. Rainbow Table thường được sử dụng trong phục hồi các mật khẩu chữ thô, lên đến một độ dài nhất định bao gồm một tập hạn chế các ký tự

Vulnerability Scanning

OpenVAS là một trình quét lỗ hổng đánh giá mạng mã nguồn mở và miễn phí. Nó giúp xác định các dịch vụ mạng lỗi thời, thiếu các bản vá bảo mật, máy chủ được cấu hình kém và các lỗ hổng khác

OpenVAS là một công cụ mạnh mẽ mang sức mạnh của nghiên cứu an ninh mạng vào tay bạn. Và có thể sử dụng nó để giám sát các thiết bị trong mạng và các trang web của mình trên các máy chủ từ xa

Nessus cho phép lập lịch giám sát nhất quán bất kỳ tài nguyên mạng nào có thể truy cập bằng nền tảng giám sát bảo mật cập nhật nhất hiện có. Mọi hệ thống, được tiếp xúc với Internet, đều được hưởng lợi từ việc giám sát bảo mật liên tục. Các quản trị viên hệ thống và các công ty bảo mật trên toàn cầu dựa vào loại dịch vụ này để kiểm tra thường xuyên tính toàn vẹn của các dịch vụ và nền tảng của họ

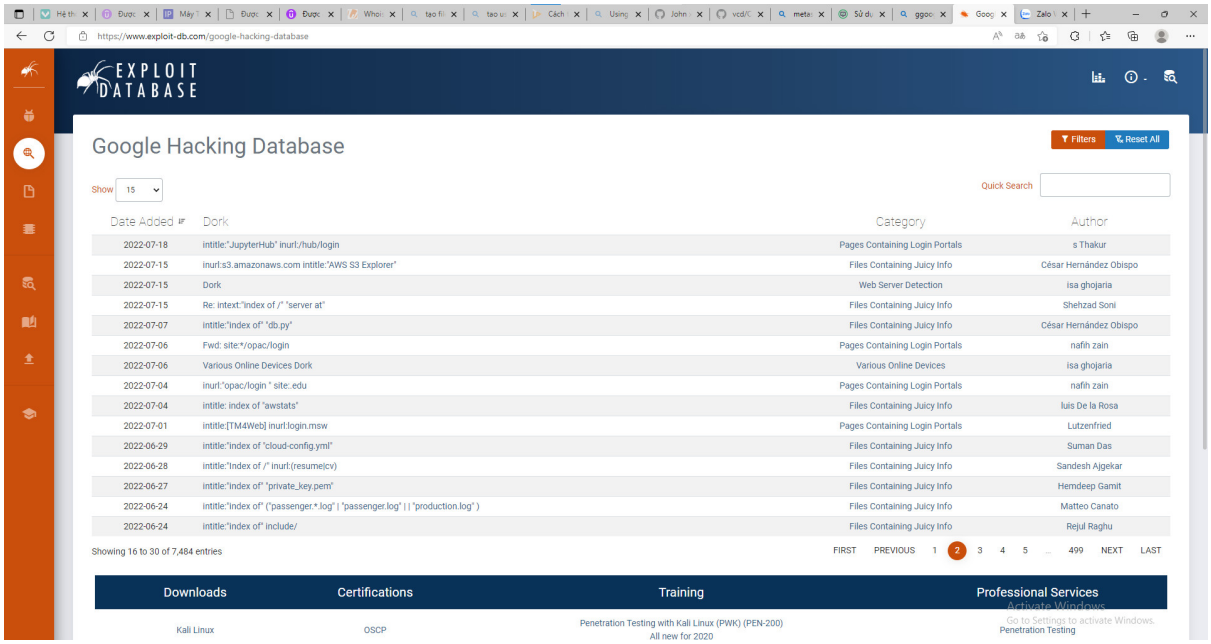
Nessus Remote Scan là một phần mềm quét lỗ hổng bên ngoài được lưu trữ bên ngoài được lưu trữ bên ngoài. Nó quét từ xa tất cả các cổng bên ngoài và tìm kiếm bất kỳ giao tiếp nào với các hệ thống bị nhiễm botnet hoặc khai thác tiềm năng từ các nguồn bên ngoài

Searching for Exploits

Google Hacking: sử dụng từ khóa để thực hiện search

VD: thêm site:microsoft.com vào key search

intext:"index of"
=> kết quả sẽ chắc chắn có index of
or intitle:"index of"



Metasploit

Đây là một công cụ kiểm tra thâm nhập có thể khai thác và xác nhận các lỗ hổng. Nó chứa cơ sở hạ tầng cơ bản, nội dung cụ thể và các công cụ cần thiết để kiểm tra thâm nhập và đánh giá bảo mật rộng lớn

Nó là một trong những khung khai thác nổi tiêng nhất và được cập nhật thường xuyên

Khai thác mới được cập nhật ngay sau khi chúng được xuất bản

Nó có nhiều công cụ được sử dụng để tạo không gian làm việc bảo mật cho hệ thống kiểm tra tra lỗ hổng và kiểm tra thâm nhập

Meterpreter

Một số lệnh cơ bản

1. Lệnh Keylogger

    ps: Hiện tất cả các tiến trình

migrate+PID: Chọn 1 tiến trình để giả mạo thành Keylogger

keyscan_start: Bắt đầu quá trình thu thập

keyscan_stop: Dừng quá trình thu thập

keyscan_dump: Hiện dữ liệu đã thu thập

2. Lệnh Webcam và Micro

record_mic: Ghi âm lại bằng MIC của victim

webcam_list: Hiện danh sách webcam

webcam_snap: Chụp ảnh bằng webcam của victim

3. Một vài lệnh khác

ps: Hiện các tiến trình trên máy victim

kill+PID: tắt 1 chương trình nào đó trên máy Victim

screenshot: chụp lại màn hình máy victim

sysinfo: Hiện thông tin máy Victim

shell: Vào cmd của Victim

4. Các lệnh dùng Tắt/ Khởi động lại máy

shutdown: Tắt máy

reboot: Khởi động lại

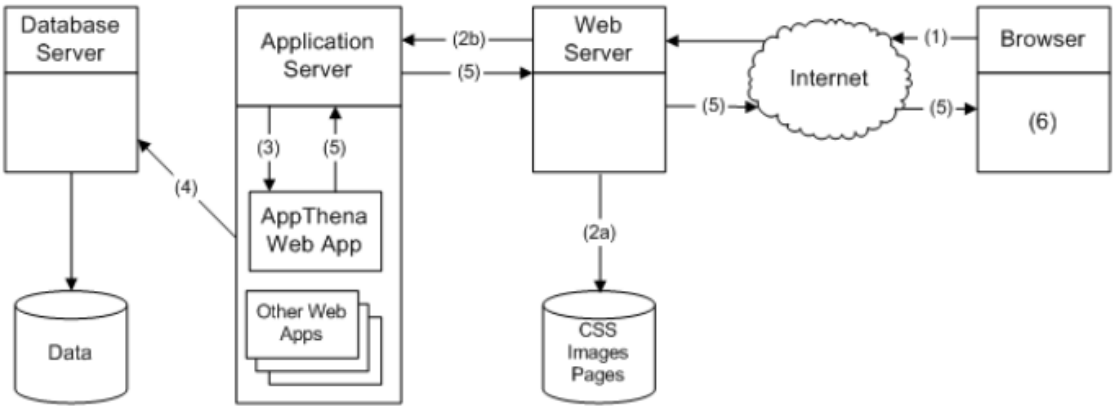
Web Application Testing

Web Application Architecture

Kiến trúc ứng dụng web mô tả sự tương tác giữa các ứng dụng, cơ sở dữ liệu db và các hệ thống phần mềm trung gian trên web. Kiến trúc ứng dụng có thể hoạt động đồng thời và linh hoạt.

Kiến trúc mạng có thể bảo vệ cung cấp một ngăn chặn và cô lập những kẻ tấn công trong môi trường. Nó cũng cung cấp những nơi mà có thể rút lui và quan sát

VD: khi mở một web:



Ngay sau khi người dùng nhấn nút Go sau khi nhập URL trên ô search bất kỳ browser nào. Máy chủ sẽ gửi các file phản hồi đến browser để đáp lại yêu cầu

Browser sau đó sẽ chạy các file này để hiển thị trang được yêu cầu

Cuối cùng, người dùng có thể tương tác với trang web

Điều quan trọng nhất cần lưu ý ở đây là các đoạn mã sẽ được trình duyệt web phân tích cú pháp. Ứng dụng web cũng hoạt động theo cách tương tự

Đoạn mã này có thể có hoặc không cung cấp hướng dẫn cụ thể để báo lại với browser về các phản hồi với các loại input khác nhau của người dùng

→ Web application architecture sẽ phải bao gồm tất cả các thành phần phụ cũng như các ứng dụng bên ngoài thay thế cho toàn bộ ứng dụng phần mềm (trong trường hợp nói trên là một trang web)

→ một web application architecture không chỉ phải hiệu quả mà còn phải đảm bảo độ tin cậy khả năng mở rộng và bảo mật mạnh mẽ

☐ `Cách web application architecture hoạt động:`

Với bất kỳ ứng dụng web điển hình nào, cũng sẽ cần 2 mã (chương trình con) khác nhau chạy song song là:

- Code từ phía máy khách (frontend): phần code nằm trong browser và phản hồi input của người dùng
- Code phía máy chủ (backend): nằm trên máy chủ và phản hồi các yêu cầu HTTP

Một nhà phát triển web sẽ quyết định xem mã trên phía máy chủ sẽ làm gì với mã trong trình duyệt - phía máy khách. Để viết mã từ phía máy chủ, cần sử dụng ngôn ngữ C#, Java, JS, Python, PHP, …..

Bất kỳ code nào có thể đáp ứng các yêu cầu HTTP đều có khả năng chạy trên phía máy chủ. Mã phía máy chủ chịu trách nhiệm tạo trang mà người dùng yêu cầu cũng như lưu trữ các loại dữ liệu khác nhau, bao gồm hồ hơ người dùng và đầu vào của họ

Sự kết hợp của CSS , HTML JS được sử dụng để viết mã phía máy khách, mã này sẽ được trình duyệt web phân tích cú pháp. Không giống mã phía máy chủ, code frontend có thể được người dùng nhìn thấy và chỉnh sửa, chỉ giao tiếp thông qua các yêu cầu HTTP và không thể đọc trực tiếp các tệp từ máy chủ

☐ `Các thành phần của Web application Architecture:`

- Thành phần UI/UX của ứng dụng web bao gồm: nhật ký hoạt động, trang tổng quát, thông báo, cài đặt, thống kê,…. Các thành phần này không liên quan gì đến hoạt động của kiến trúc ứng dụng web
- Các thành phần cấu trúc: Hai thành phần cấu trúc chính của web là phía máy khách (frontend) và máy chủ (backend)
- Thành phần phía máy khách: Các compenent phía máy khách được phát triển trong CSS, HTML, JS. vì nó tồn tại trong trình duyệt web của người dùng nên không cần có những điều chỉnh liên quan quan đến hệ điều hành hoặc thiết bị. Phần frontend đại diện cho chức năng của ứng dụng web mà người dùng tương tác cùng
- Thành phần phía máy chủ: Phần backend có thể được xây dựng bằng cách sử dụng một hoặc kết hợp nhiều ngôn ngữ lập trình cùng các framework bao gồm các ngôn ngữ như java, .NET, NodeJS, PHP Python, Ruby, Rails,…. Component của máy chủ phải có ít nhất hai thành phần là logic ứng dụng và cơ sở dữ liệu.

  Logic ứng dụng là trung tâm điều khiển chính của ứng dụng web trong khi cơ sở dữ liệu là nơi lưu trữ tất cả các dữ liệu một cách liên tục

  `Mô hình của các thành phần web application`

  Dựa vào tổng số máy chủ và db được sử dụng cho một ứng dụng web, mô hình của một web sẽ được quyết định. Các mô hình đó có thể là 1 trong 3 mô hình:

  - **Một máy chủ, một database**

    Đây là mô hình thành phần ứng dụng web đơn giản nhất nhưng cũng kém tin cậy nhất. Mô hình này sẽ chỉ sử dụng một máy chủ duy nhất cũng như một cơ sở dữ liệu duy nhất. Ứng dụng web được xây dựng trên mô hình

này sẽ ngừng hoạt động ngay sau khi máy chủ gặp sự cố. Do đó đây là mô hình kém tin cậy

Mô hình này thường không được sử dụng cho các ứng dụng web trên thực tế mà chỉ được sử dụng để chạy các dự án thử nghiệm cũng như với mục đích học hỏi và tìm hiểu các nguyên tác cơ bản ứng dụng web

- **Nhiều máy chủ Web, một database**

  Với mô hình này, máy chủ sẽ không lưu trữ bất kỳ dữ liệu nào, khi máy chủ web lấy thông tin từ một máy khách, nó sẽ xử lý thông tin và ghi vào db được quản lý bên ngoài máy chủ

  Cần có ít nhất hai máy chủ web cho mô hình thành phần ứng dụng web này.

  Đây sẽ là một lựa chọn an toàn, bởi khi một máy chủ gặp sự cố, máy chủ còn lại sẽ chịu trách nhiệm. Tất cả các yêu cầu được thực hiện sẽ được tự động chuyển hướng đến máy chủ mới và ứng dụng web sẽ tiếp tục thực hiện.

  Ưu điểm của mô hình này là dễ dàng vận hành hệ thống và chủ động phòng chống các nguy cơ tấn công từ hacker

  → do vậy, độ tin cậy của mô hình này sẽ tốt hơn so với mô hình cơ sở dữ liệu vốn có

- **Nhiều máy chủ web, nhiều database**

  Đây là mô hình thành phần ứng dụng web hiệu quả nhất vì cả máy chủ và db đều ít xảy ra lỗi. Có hai lựa chọn cho loại mô hình này.

  - Một là lưu trữ dữ liệu giống nhau ở tất cả các db
  - Hoặc phân phối nó đồng đều giữa các db

  Đối với những hệ thống cung cấp dịch vụ lớn, đòi hỏi phải có nhiều tài nguyên mới đủ phục vụ người dùng thì mô hình này là giải pháp tối ưu nhất

Các loại kiến trúc ứng dụng web

Bất kỳ trang web nào đang hoạt động cũng đều có những vấn đề. Để đảm bảo một ứng dụng web có thể mang lại hiệu suất tối đa, ứng dụng web phải:

- Tránh được sự cố thường xuyên
- Dễ dàng sử dụng
- Thời gian phản hồi nhanh
- Hỗ trợ các tiêu chuẩn và công nghệ mới nhất

- Tăng cường sử dụng các biện pháp bảo mật để giảm nguy cơ xâm nhập độc hại
- Giải quyết truy vấn một cách nhất quán và thống nhất

→ Các tính năng mạnh mẽ, khả năng phản hồi, bảo mật của một ứng dụng web chịu ảnh hưởng rất nhiều bởi mô hình và kiểu kiến trúc ứng dụng web

SQL Injection

SQL Injection là một kỹ thuật lợi dụng những lỗ hổng về câu truy vấn của các ứng dụng. Được thực hiện bằng cách chèn thêm một đoạn SQL để làm sai lệnh đi câu truy vấn ban đầu, từ đó có thể khai thác dữ liệu từ database. **SQL injection** có thể cho phép những kẻ tấn công thực hiện các thao tác như một người quản trị web, trên cơ sở dữ liệu của ứng dụng.

☐ **Ví dụ thực tiễn SQL Injection**

Ví dụ, trong form đăng nhập, người dùng nhập dữ liệu, trong trường tìm kiếm người dùng nhập văn bản tìm kiếm, trong biểu mẫu lưu dữ liệu, người dùng nhập dữ liệu cần lưu. Tất cả các dữ liệu được chỉ định này đều đi vào cơ sở dữ liệu.

Thay vì nhập dữ liệu đúng, kẻ tấn công lợi dụng lỗ hổng để insert và thực thi các câu lệnh SQL bất hợp pháp để lấy dữ liệu của người dùng… SQL Injection được thực hiện với ngôn ngữ lập trình SQL. SQL (Structured Query Language) được sử dụng để quản lý dữ liệu được lưu trữ trong toàn bộ cơ sở dữ liệu.

Tuy nhiên ngày nay chứng ta thường làm việc trên những framework hiện đại. Các framework đều đã được test cẩn thận để phòng tránh các lỗi, trong đó có SQL Injection.

☐ **Sự nguy hiểm của SQL Injection**

- Hack tài khoản cá nhân.
- Ăn cắp hoặc sao chép dữ liệu của trang web hoặc hệ thống.
- Thay đổi dữ liệu nhạy cảm của hệ thống.
- Xóa dữ liệu nhạy cảm và quan trọng của hệ thống.
- Người dùng có thể đăng nhập vào ứng dụng với tư cách người dùng khác, ngay cả với tư cách quản trị viên.
- Người dùng có thể xem thông tin cá nhân thuộc về những người dùng khác, ví dụ chi tiết hồ sơ của người dùng khác, chi tiết giao dịch của họ,…

- Người dùng có thể sửa đổi cấu trúc của cơ sở dữ liệu, thậm chí xóa các bảng trong cơ sở dữ liệu ứng dụng.
- Người dùng có thể kiểm soát máy chủ cơ sở dữ liệu và thực thi lệnh theo ý muốn.

XML Entity Injection

Hay còn được gọi là XXE injection là 1 lỗ hổng được đánh giá mức độ nghiêm trọng là 4/10 Web Application Security Risks của OWASP

XXE là một lỗ hổng bảo mật web cho phép hacker tấn công can thiệp vào quá trình xử lý dữ liệu XML của application

XXE là ?

Là ngôn ngữ đánh dấu mở rộng được thiết kế với mục đích lưu trữ truyền dữ liệu và cả người và máy đều có thể đọc được

Struct:

```
<?xml version="1.0" encoding="UTF-8"?>
  <application>
      <title>eMB</title>
      <company>MB</company>
      <year>2021</year>
      <price>40000000</price>
  </application
```

Giải thích:

Dòng 1: khai báo XML (XML declaration) (không bắt buộc)

Phần thân bao gồm nhiều cặp thẻ khác nhau tạo nên các phần tử khác nhau và lồng vào nhau tạo thành cấu trúc dạng cây. Sẽ có quy định về cú pháp, cách khai báo, cách lồng các phần tử, thuộc tính,…..

- External Entity: Entity tham chiều đến nội dung một file bên ngoài tài liệu XML. Entity là một khái niệm có thể được sử dụng như một kiểu tham chiếu đến dữ liệu, cho phép thay thế 1 ký tự đặc biệt, 1 khối văn bản hay toàn bộ nội dung 1 file vào trong tài liệu XML

  Một số kiểu entity: character, parameter, named (internal), external,…

```
<!DOCTYPE order SYSTEM "order.dtd">
<!DOCTYPE ran SYSTEM "/dev/random">
<!DOCTYPE request [
```

```
    <!ENTITY include SYSTEM "c:\secret.txt">
]>
```

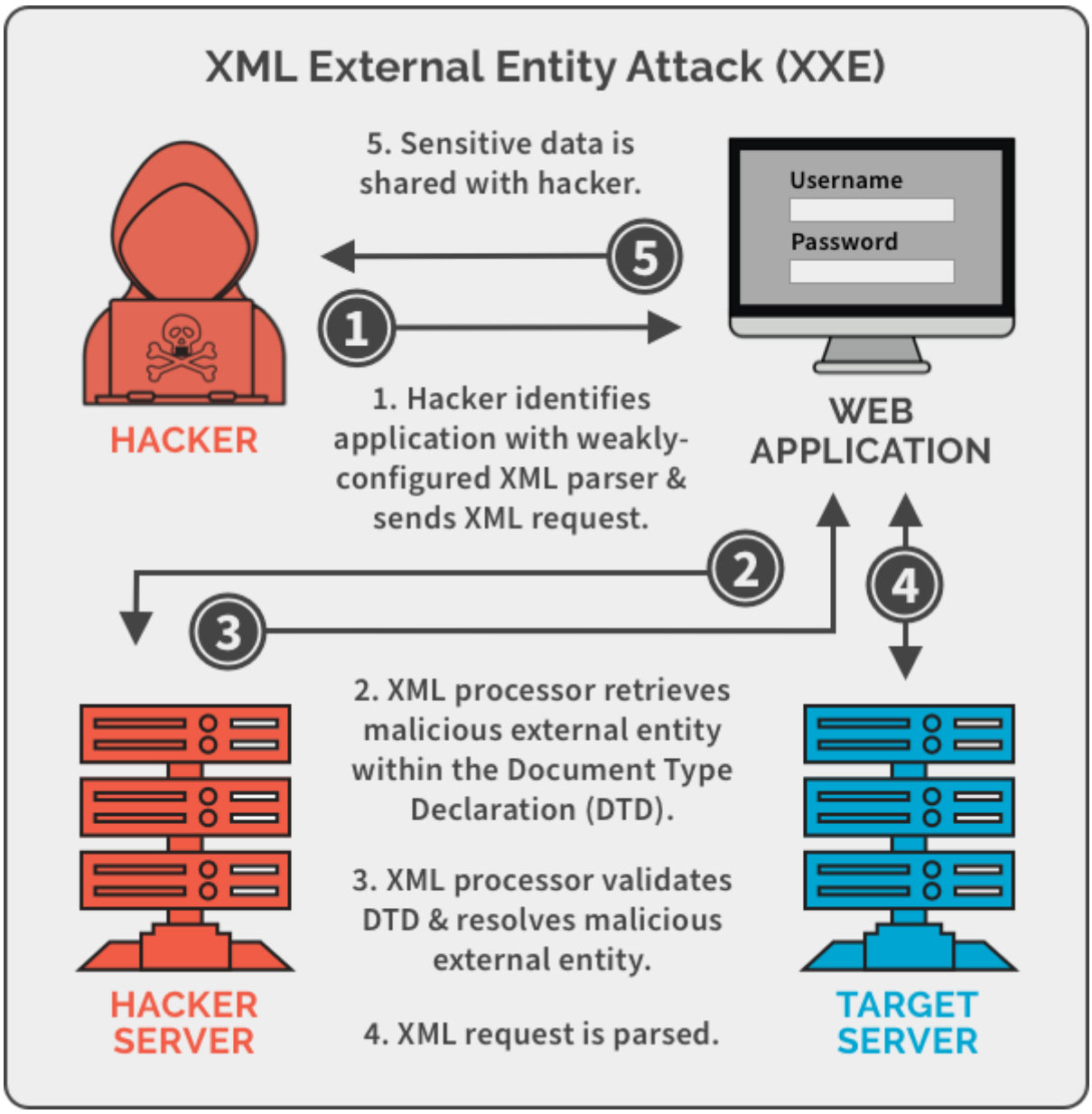
⇒ XXE là lỗ hổng lợi dụng tính năng phân tích cú pháp của XML dùng để phân tích cú pháp đầu vào XML từ người dùng. Dựa vào đó hacker có thể truy cập các tệp cục bộ, chạy các lệnh, quét các dịch vụ và các cổng nội bộ truy cập mạng nội bộ, từ đó thực hiện nhiều phương pháp tấn công tương ứng

Làm thế nào để lỗ hổng XXE phát sinh

Lỗi XXE phát sinh do bên trong XML có chứa các tính năng nguy hiểm và XML cho phép sử dụng các công cụ phân tích các tính năng này

Các loại tấn công XXE

- Exploit XXE to retireve files(Khai thác XXE để truy xuất file) : External entity được xác định có chứa nội dung của file và trả về trong phản hồi của ứng dụng.
- Exploit XXE to perform SSRF attacks(Khai thác XXE để thực hiện các cuộc tấn công SSRF) : External entity được xác định dựa trên URL đến hệ thống back-end.
- Exploit blind XXE exfiltrate data out-of-band(Khai thác lỗ hổng XXE mù ngoài luồng dữ liệu exfiltrate): Dữ liệu nhạy cảm có thể được truyền từ máy chủ ứng dụng đến máy chủ của hacker.
- Exploit blind XXE to retire data via error messages(Khai thác lỗ hổng XXE mù để truy xuất dữ liệu thông qua thông báo lỗi): Nơi mà hacker dùng các thông báo lỗi để phân tích dữ liệu nhạy cảm.



1. Hacker xác định ứng dụng yếu đã cấu hình trình phân tích cú pháp XML và gửi yêu cầu XML
2. Bộ xử lý XML truy xuất thực thể độc hại bên ngoài DTD
3. Bộ xử lý XML xác thực: DTD và giải quyết thực thể độc hại bên ngoài
4. Yêu cầu XML được phân tích cú pháp
5. Dữ liệu được chia sẻ với hacker

Hacker có thể tận dụng tối đa các thực thể bên ngoài XML để sử dụng lỗ hổng này nhằm sử dụng chức năng bên ngoài của nó. Trong nhiều trường hợp thì lỗ hổng XXE cũng có thể là 1 ví dụ về cách hacker có thể tận dụng cấu hình sai này của trình phân tích cú pháp XML về cơ bản biến nó thành 1 máy chủ proxy để chúng có

thể thực hiện các cuộc tấn công Select query về phía máy chủ và truy cập vào mạng nội bộ hoặc có thể kết nối với các máy chủ công cộng bên ngoài từ sau tường lửa.

Hacker có thể sử dụng định nghĩa thực thể XML và định danh hệ thống trên trình phân tích cú pháp XML để chỉ chấp nhận các yêu cầu được tạo ra thủ công độc hại chứa các tệp XML dường như vô hại đối với tường lửa hoặc ứng dụng vì chức năng của các dịch vụ đó dường như không bị tấn công trực tiếp

Tìm và kiểm tra lỗ hổng XXE

Đa số các lỗ hổng XXE thì có thể tìm được thông qua chức năng scanner vulnerabilities của Burp

Ngoài ra có thể check thủ công:

- Kiểm tra khả năng truy xuất tệp bằng cách xác định một external entity dựa trên một tệp hệ điều hành nổi tiếng và sử dụng thực thể đó trong dữ liệu được trả về trong phản hồi của ứng dụng
- Kiểm tra các lỗ hổng blind XXE bằng cách xác định 1 external entity bên dựa trên URL của 1 hệ thống mà bạn kiểm soát và giám sát. Chức năng Burp Collaborator của Burp có thể hỗ trợ phần này
- Kiểm tra xem máy có dễ bị injection và dữ liệu không phải là XML do người cung cấp trong tài liệu XML phía máy chủ hay không, bằng cách sử dụng XInclude attack để cố gắng truy xuất hệ điều hành nổi tiếng.

XInclude là một phần của đặc tả XML cho phép một tài liệu XML được xây dựng từ các tài liệu con.

> Có thể đặt một cuộc tấn công XInclude trong bất kỳ giá trị dữ liệu nào trong tài liệu XML, do đó, cuộc tấn công có thể được thực hiện trong các tình huống mà chỉ cần kiểm soát một mục dữ liệu duy nhất được đặt vào tài liệu XML phía máy chủ

Để thực hiện một cuộc tấn công XInclude, cần tham chiếu không gian tên XInclude và cung cấp đường dẫn đến tệp mà bạn muốn đưa vào:

```
<foo xmlns: xi = "http://www.w3.org/2001/XInclude">
<xi: include parse = "text" href = "file: /// etc / passwd" /> </foo>
```

Ngăn chặn XXE

Các lỗ hổng XXE đều phát sinh do thư viện phân tích cú pháp XML của ứng dụng hỗ trợ các tính năng XML tiềm ẩn nguy hiểm mà ứng dụng không cần hoặc có ý

định sử dụng

Cách dễ nhất và hiệu quả nhất là vô hiệu hóa những chức năng tiềm ẩn nguy hiểm đó

- Bất cứ khi nào có thể, hãy sử dụng các định dạng dữ liệu ít phức tạp hơn như JSON và tránh tuần tự hóa dữ liệu nhạy cảm
- Vá hoặc nâng cấp tất cả các bộ xử lý và thư viện XML được ứng dụng hoặc trên hệ điều hành cơ bản sử dụng. Sử dụng bộ kiểm tra phụ thuộc. Cập nhật SOAP lên cao hơn (1.2)
- Triển khai xác thực, lọc đầu vào tích cực phía máy chủ để ngăn chặn dữ liệu thù địch trong các tài liệu, tiêu đề hoặc nút XML
- Xác minh răng chức năng tải lên tập XML hoặc XSL kiểm tra XML đến bằng cách sử dụng xác thực XSD hoặc tương tự
- Các công cụ kiểm tra bảo mật ứng dụng tĩnh có thể phát hiện XXE trong mã nguồn, nhưng xem xét mã thủ công là giải pháp thay thế tốt nhất trong các ứng dụng phức tạp với nhiều tích hợp

Cross Site Scripting

Là một trong những kỹ thuật tấn công phổ biến, được liệt vào danh sách những kỹ thuật tấn công nguy hiểm nhất với ứng dụng web. Cross site scripting là một lỗi bảo mật cho phép người tấn công chèn các đoạn script nguy hiểm vào trong source code ứng dụng web. Nhằm thực thi các đoạn mã độc JS để chiếm phiên đăng nhập của người dùng

- Stored XSS: là dạng tấn công mà hacker chèn trực tiếp các mã độc vào cơ sở dữ liệu của website.

  Dạng tấn công này xảy ra khi các dữ liệu được gửi lên server không được kiểm tra kỹ lưỡng mà lưu trực tiếp vào cơ sở dữ liệu

  Khi người dùng truy cập vào trang web này thi những đoạn script độc hại sẽ được thực thi chung với quá trình load trang web

- Reflected XSS: Khác với stored xss, Reflected đoạn mã khai thác sẽ không được lưu trữ trên server

  Một ví dụ điển hình là kết quả trả về của module search

  Reflected là dạng tấn công thường gặp nhất trong các loại hình XSS, hacker không gửi dữ liệu độc hại lên server nạn nhân mà gửi trực tiếp link có chứa mã

độc cho người dùng, khi người dùng click vào link này thì trang web sẽ được load chung với các đoạn script độc hại.

Reflected thường dùng để ăn cắp cookie, chiếm session,… của nạn nhân hoặc cài keylogger, trojan,… vào máy tính nạn nhân

Có nhiều hướng để khai thác thông qua lỗi Reflected XSS, một trong những cách được biết đến nhiều nhất là chiếm phiên làm việc (session) của người dùng, từ đó có thể truy cập được dữ liệu và chiếm được quyền của học trên website

- Dom based XSS

  Là kỹ thuật khai thác xss dựa trên việc thay đổi cấu trúc DOM của tài liệu, cụ thể HTML

Cách thực hiện tấn công:

Tấn công XSS nghĩ là gửi và chèn lệnh script độc hại, những mã độc này thường được viết với ngôn ngữ lập trình phía client như JS, HTML, …. Tuy nhiên cách tấn công này thường sử dụng JS và HTML

Cách tấn công này có thể được thực hiện theo nhiều cách khác nhau, phụ thuộc vào loại tấn công XSS, 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

Nguyên nhân chính của loại tấn công này là xác thực đầu vào dữ liệu người dùng không phù hợp, dữ liệu độc hại từ đầu vào có thể nhập vào dữ liệu đầu ra.

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 nhân hoặc bất kỳ hình thức giả nào đang được hiển thị cho người sử dụng. Có một số hình thức tấn công XSS có thể xảy ra:

- Cross site scripting có thể xảy ra trên tập lệnh được thực hiện ở phía client
- Trang web hoặc form giả mạo được hiển thị cho người dùng (nơi nạn nhân nhập thông tin đăng nhập hoặc nhấp vào liên kết độc hại)
- Trên các trang web có quảng cáo được hiển thị
- Email độc hại được gửi đến nạn nhân. Tấn công xảy ra khi tin tặc tìm kiếm những lỗ hổng trên website và gửi nó làm đầu vào độc hại. Tập lệnh độc hại

được tiêm vào mã lệnh và sau đó được gửi dưới dạng đầu ra cho người dùng cuối

Ngăn ngừa, lọc và vá các lỗ hổng XSS

Đối với người dùng thì ta cần phải cân nhắc khi click và link, kiểm tra các link thật kĩ trước khi click. Đặc biệt trên mạng xã hội. Cần cảnh giác trước khi click vào xem 1 link nào đó được chia sẻ

Đối với người thiết kế và phát triển ứng dụng web với những dữ liệu, thông tin nhập của người dùng, người thiết kế và phát triển ứng dụng web cần thực hiện vào bước cơ bản sau:

- chỉ chấp nhận những dữ liệu hợp lệ
- từ chối nhận các dữ liệu hỏng
- liên tục kiểm tra và lọc dữ liệu
- tạo ta danh sách những thẻ HTML được phép sử dụng, xóa bỏ các thẻ, coi đoạn scritp đó như là đoạn trích dẫn lỗi
- lọc dấu nháy
- xóa ký tự >, < hoặc output endcoding các ký tự đó
- cho phép nhập dữ liệu đặc biệt nhưng sẽ mã hóa theo chuẩn riêng

Malware Operations

Malware types

Định nghĩa:

Phần mềm độc hại (malicious software) là thuật ngữ chung cho các ứng dụng nguy hiểm. Đó là một thuật ngữ thích hợp hơn cho phần mềm xấu hơn là virus.

Dùng để chỉ các loại khác chẳng hạn như virus, trojan, ransomware,….

→ sẽ được nghe đến nhiều ứng dụng chẳng hạn như Malwarebytes được coi là giải pháp *chống phần mềm độc* hại thay vì chỉ là chống virus

1. Virus

Virus là một chương trình độc hại có khả năng tự sao chép bằng cách chèn mã của nó vào các chương trình khác để tự phát tán xung quanh

Một loại loại virus thường được đưa vào một hệ thống khi ai đó chạy một tệp bị nhiễm từ tệp đính kèm email hoặc ổ USB. Đây cũng là cách mà rất nhiều phần mềm độc hại khác xâm nhập vào một hệ thống. Đặc điểm phân biệt virus và các loại malware khác đó là virus được gắn vào một chương trình khác và tự sao chép bằng cách sửa đổi các phần mềm khác nhau mà bạn không hề hay biết

Virus đã tồn tại trong nhiều thập kỷ, virus đầu tiên xuất hiện trong tự nhiên vào đầu những năm 1980. Chúng từng phổ biến hơn vào thập kỷ 1990 và đầu những năm 2000, nhưng gần đây đã trở nên ít phổ biến hơn so với các kiểu tấn công khác

2. Sâu (worm)

Một con sâu tương tự như một con virus, sự khác biệt là sâu tự lây lan thay vì gắn vào và lây nhiễm cho các chương trình. Sâu thường lan truyền trên mạng, khai thác lỗ hổng để nhảy từ máy này sang máy khác

Khi sâu tiếp tục lây lan, chúng sẽ lây nhiễm vào máy mới với tốc độ nhanh hơn. Ở mức tối thiểu, điều này làm lãng phí băng thông của mạng, trong khi những loại sâu độc hại hơn có thể phát tán ransomware hoặc các vấn đề khác trên toàn bộ mạng lưới của một doanh nghiệp

3. Trojan

Trojan horse thường được gọi là trojan là một chương trình độc hại đánh lừa bạn nghĩ rằng đó là một công cụ hợp pháp

Tên gọi này bắt nguồn từ câu chuyện về con ngựa thành Troy khi người Hy Lạp cổ đại để lại một con ngựa gỗ trở đầy binh lính của họ gần thành Troy. Người thành Troy dắt ngựa vào thành nghĩ rằng họ đã đánh thắng tuy nhiên trong đêm những người lính Hy Lạp nhảy xuống ngựa và mở của cho phần còn lại của quân đội của họ vào qua các cổng thành, thành công đánh chiếm thành Troy

Trojan máy tính hoạt động theo cách tương tự. Trojan ngụy trang thành phần mềm chính hãng, chẳng hạn như biểu mẫu để điền hoặc một ứng dụng hữu ích. Tuy nhiên khi vào hệ thống của bạn, trojan sẽ mang theo 1 payload(phần dữ liệu thực sự được truyền đi của một gói tin giữa hai phía mà không chứa dữ liệu giao thức hay siêu dữ liệu). điều này thường mở ra một cửa hậu (backdoor) giúp tin tặc truy cập vào máy tính của bạn mà không biết

Trong trường hợp khác, trojan có thể xóa các tệp của bạn, gây lây nhiễm ransomware hoặc các hoạt động tương tự

4. Phần mềm quảng các (adware)

Là một loại phần mềm độc hại tạo ra các quảng cáo để kiếm tiền cho nhà phát triển của nó, trong khi các phần mềm sống nhờ quảng cáo rất phổ biến trong các ứng dụng dành cho thiết bị di động và thậm chí một số công cụ dành cho máy tính để bàn, phần mềm quảng cáo còn tiến xa hơn khi ‘nhấn chìm’ người dùng vào một cơn lũ quảng cáo

Ví dụ : Phần mềm quảng cáo có thể đưa thêm quảng cáo vào mọi trang web bạn truy cập hoặc thay đổi công cụ tìm kiếm của trình duyệt của bạn thành công cụ lừa đảo được thiết kế để chuyển hướng bạn đến các trang web kiếm nhiều tiền hơn cho chủ sở hữu. Một số phần mềm quảng cáo cũng tạo ra các popup windows trên màn hình của bạn mà rất khó đóng lại

Có một ranh giới nhỏ giữa quảng cáo hợp pháp như một cách kiếm tiền từ ứng dụng và các chương trình được thiết kế để spam cửa sổ bật lên nhằm làm phiền bạn

Phần mềm quảng cáo thường được đóng gói vào hệ thống cùng với phần mềm hợp pháp thông qua các tùy chọn đã được chọn sẵn trong quá tình cài đặt

5. Phần mềm gián điệp (spyware)

Là các chương trình theo dõi việc sử dụng máy tính của bạn và báo cáo lại cho một thực thể nào đó để phục vụ một số mục đích nhất định

Hầu hết các chương trình và thậm chí cả hệ điều hành như win 10 thu thập dữ liệu về việc sử dụng của bạn và báo cáo lại cho nhà phát triển nhằm cải thiện các công cụ của họ. Sự khác biệt của phần mềm gián điệp là nó thu thập dữ liệu này mà không cho người dùng không hề hay biết

Trong khi phần mềm gián điệp thường thu thập dữ liệu cho mục đích quảng cáo, những phần mềm tệ hại hơn cũng có thể thu thập thông tin nhạy cảm như thông tin đăng nhập. Phần mềm gián điệp cấp cao bao gồm keylogger, là những chương trình ghi lại mọi thao tác gõ phím bạn thực hiện trên máy của mình

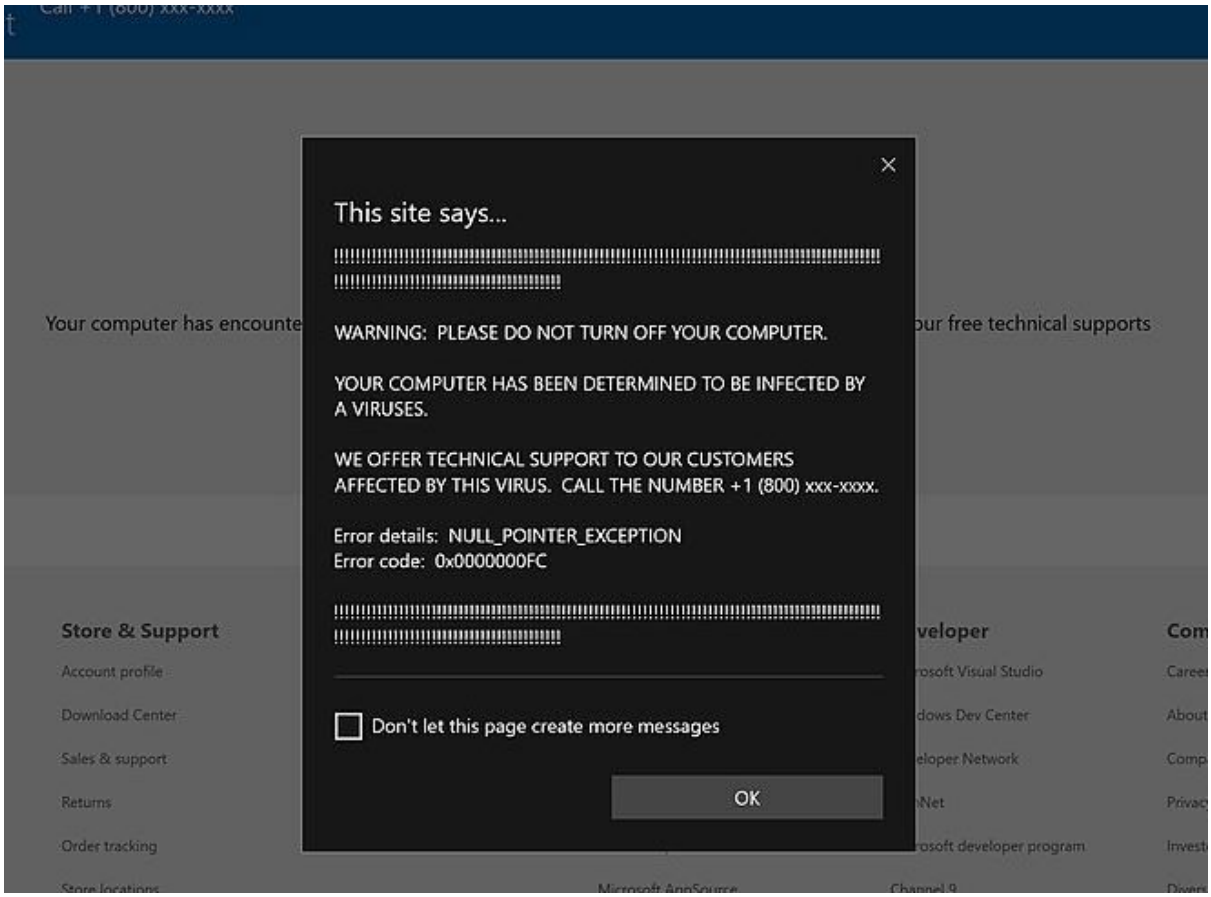
6. Phần mềm tống tiền (Ransomware)

Từ cuối 2010 đã có sự tăng vọt trong mức độ phổ biến của ransomware. Đó là một loại phần mềm độc hại nguy hiểm mã hóa nội dung trong máy tính của bạn, ngăn bạn tiếp cận với các tệp của riêng bạn.

Ransomware yêu cầu bạn trả tiền cho người tạo ra nó, thường thông qua một phương thức không thể truy xuất được như Bitcoin, để lấy khóa mã hóa và mở khóa các tệp của bạn

Cách tốt nhất để giữ an toàn trước ransomware là chuẩn bị sẵn một kế hoạch. Việc thường xuyên sao lưu dữ liệu sẽ cho phép bạn khôi phục chúng nếu bạn bị tấn công bởi ransomware. Cho dù bạn trả tiền, không có gì đảm bảo rằng kẻ tấn công sẽ cung cấp cho bạn chìa khóa đồng thời việc này sẽ khuyến khích loại hành vi này trong tương lai

7. Phần mềm hù dọa (Scareware)



Scareware gần giống ransomware ngoại trừ nó chỉ giả vờ nguy hiểm

Thông thường phần mềm hù dọa hiển thị dưới dạng các quảng các trực tuyến lừa đảo chiếm đoạt trình duyệt của bạn. Nó hiển thị một thông báo cảnh báo virus giả mạo, tuyên bố rằng ‘Microsoft’ hoặc một công ty khác đã phát hiện ra sự cố trên máy tính của bạn và hướng dẫn bạn gọi đến một số điện thoại hoặc tỉa xuống phần mềm chống virus để khắc phục sự cố

Nếu bạn gọi đến số điện thoại bạn sẽ nói chuyện với những kẻ lừa đảo muốn bạn trả tiền cho một quá trình dọn dẹp vô ích. Phần mềm diệt virus giả mạo cũng vậy nó yêu cầu bạn trả tiền cho một ứng dụng vô giá trị để kẻ gian có thể kiếm tiền

Rất may bạn thường có thể đóng cửa sổ bật lên phần mềm sợ hãi và bỏ qua thông báo của chúng. Chúng được thiết kế để lợi dụng nỗi sợ hãi của mọi người mà không thực sự gây hại cho máy tính

8. Rootkit

Là một thuật ngữ hợp nhất tài khoản root của quản trị viên trên hệ thống Unix và Kit là bộ mà họ sử dụng, là một loại phần mềm độc hại có quyền truy cập vào các phần bị hạn chế của máy tính, sau đó ngụy trang hoặc tự ẩn đi

Thông thường rootkit được cài đặt khi kẻ tấn công có quyền truy cập quản trị vào một máy tính. Sau khi rootkit được cài đặt, nó có quyền làm bất cứ điều gì chủ sở hữu muốn trên hệ thông. Rootkit lạm dụng điều này để che giấu sự xâm nhập của nó - ví dụ: để che giấu sự hiện diện của nó khỏi ứng dụng chống virus đã cài đặt

Một phần mềm độc hại có toàn quyền kiểm soát hệ thống của bạn rõ ràng là rất nguy hiểm. Đôi khi bạn sẽ phải cài đặt lại hoàn toàn hệ điều hành để loại bỏ rootkit

9. Botnet

Mạng botnet là kết quả của một cuộc tấn công bằng phần mềm độc hại hơn là một loại phần mềm độc hại cụ thể, nhưng nó vẫn có liên quan đến chủ đề chúng ta đang đề cập đến

Botnet là sự kết hợp của robot và mạng network là một thuật ngữ dùng để chỉ một nhóm máy tính hoặc các thiết bị kết nối mạng khác là nô lệ của một thực thể nào đó. Thực thể đó sử dụng các máy đó để thực hiện một nhiệm vụ, chẳng hạn như tấn công DDOS, gửi thư rác hoặc ngầm nhấp vào quảng cáo để kiếm tiền cho chủ sở hữu

máy tính có thể trở thành một phần của mạng botnet do chạy trojan hoặc tệp bị nhiễm khác. Phần lớn thời gian máy tính của bạn sẽ tiếp tục hoạt động bình thường, vì vậy bạn có thể không biết rằng mình đã trở thành một phần của mạng botnet

10. Khai thác lỗ hổng

Mặc dù không phải là một dạng phần mềm độc hại nhưng khai thác exploit và lỗ hổng bảo mật là những thuật ngữ quan trọng trong bảo mật trực tuyến. Bởi vì không có lập trình viên hoặc phần mềm nào là hoàn hảo, mọi chương trình hệ điều hành và trang web đều có một số lỗ hổng. các tác nhân độc hại cố gắng tìm ra những lỗ hổng này, khai thác chúng để chạy phần mềm độc hại hoặc các hoạt động tương tự

Ví dụ: Giả sử ai đó đã phát hiện ra lỗi cho phép bạn tạo tài khoản quản trị mới không có mật khẩu trông windows bằng cách làm theo một số bước nhất định. Ai có thể

viết phần mềm độc hại để chạy các bước này trên PC của ai đó, giành quyền truy cập quản trị viên, sau đó thực hiện các hoạt động phá hoại

Cách tốt nhất để giữ an toàn trước những mối đe dọa này là luôn cập nhật hệ điều hành và tất cả các phần mềm của bạn. Các nhà phát triển sẽ vá những vấn đề này khi họ phát hiện ra chúng, vì vậy việc sử dụng phiên bản mới nhất sẽ giúp bạn an toàn trước những khai thác cũ

11. Hiểu mối đe dọa từ các phần mềm độc hại phổ biến nhất

Đôi khi có sự chông chéo: một trojan có thể được sử dụng để chạy ransomware nhưng hầu hết các loại phần mềm độc hại đều có một tính năng riêng khiến chúng ta trở nên khác biệt

Mặc dù bạn không thể bảo vệ mình 100% nhưng một số thói quen sẽ giảm đáng kể khả năng lây nhiễm phần mềm độc hại

Static Analysis

Phân tích tĩnh cơ bản bao gồm kiểm tra tệp thực thi mà không cần xem hướng dẫn thực tế. Phân tích tĩnh cơ bản có thể xác nhân xem một tệp có độc hại hay không, cung cấp thông tin về chức năng của nó và đôi khi cung cấp thông tin cho phép bạn tạo chữ ký mạng đơn giản. Phân tích tĩnh cơ bản rất đơn giản và có thể nhanh chóng, nhưng phần lớn nó không hiệu quả trước phần mềm độc hại tinh vi và nó có thể bỏ lỡ các hành vi quan trọng

Kỹ thuật phân tích tĩnh malware

1. Tải kết quả lên VirusTotal

   Kỹ thuật đầu tiên trong phân tích tĩnh là tải tệp thực thi đáng ngờ lên VirusTotal, chạy tệp thực thi chống lại một số giải pháp AV và đưa ra kết quả

   VD: tệp dưới nói rằng tỉ lệ phát hiện là 17/57

2. Tìm chuỗi

   Tìm kiếm thông qua các chuỗi có thể là một cách đơn giản để có được gợi ý về chức năng của một chương trình

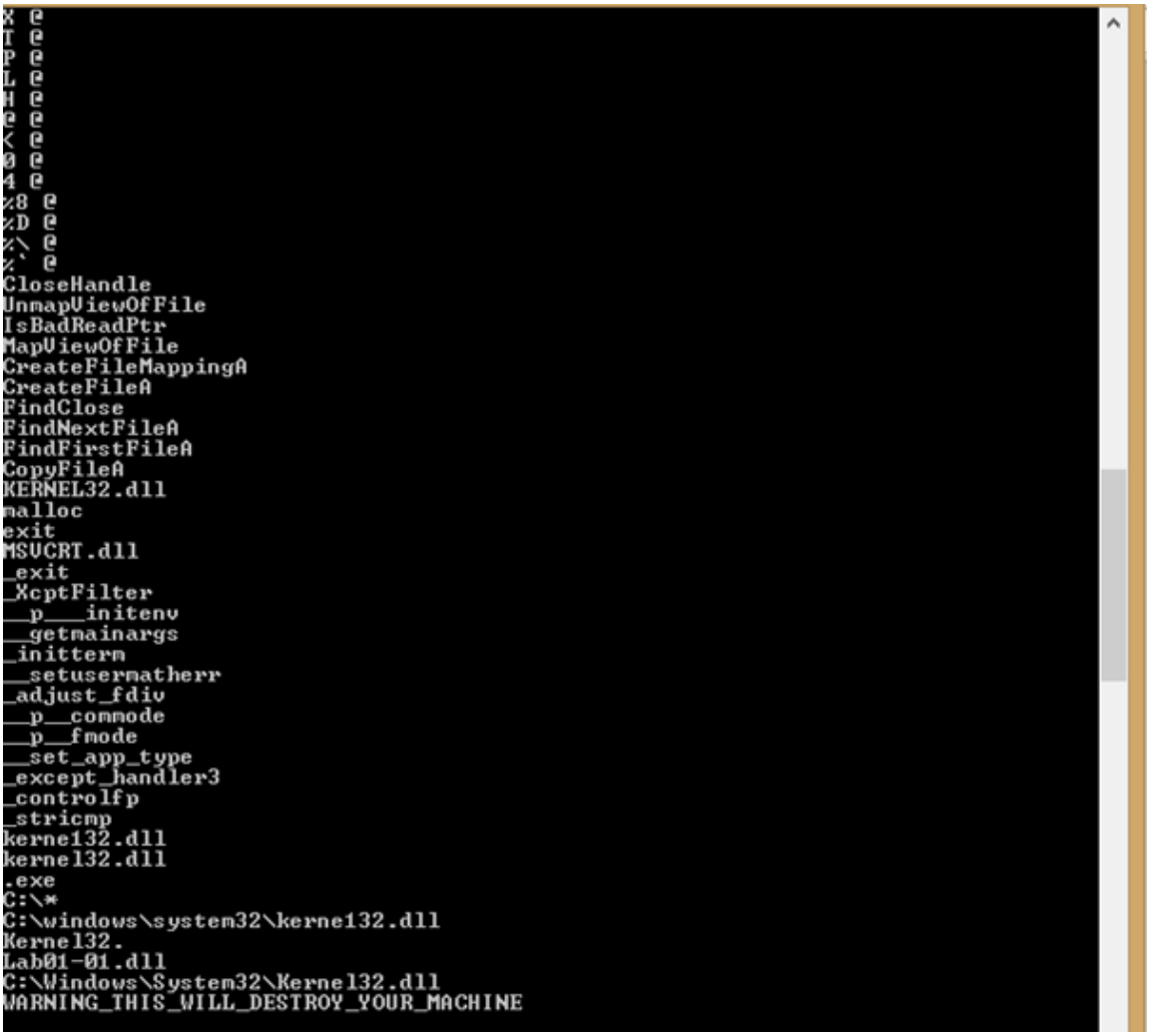
   VD: nếu chương trình truy cập một URL thì sẽ thấy URL được truy cập được lưu trữ dưới dạng một chuỗi trong chương trình

   Microsoft có một tiện ích gọi là ‘String’. khi chuỗi tìm kiếm tệp thực thi cho các chuỗi ASCII và Unicode, nó sẽ bỏ qua ngữ cảnh và định dạng, để nó có thể phân tích bất kỳ loại tệp nào và phát hiện các chuỗi trên toàn bộ tệp (mặc dù điều này cũng có nghĩa là nó có thể xác định byte ký tự là chuỗi khi chúng không phải là chuỗi). Chuỗi tìm kiếm một chuỗi ba chữ cái hoặc nhiều hơn các ký tự ASCII và Unicode, tiếp theo là một ký tự kết thúc chuỗi

   VD về các chuỗi mà từ đó thông tin quan trọng có thể được tiết lộ. Sử dụng tiện ích Strings, các tệp có thể được tìm kiếm bằng lệnh ‘cmd: Strings <filename>’

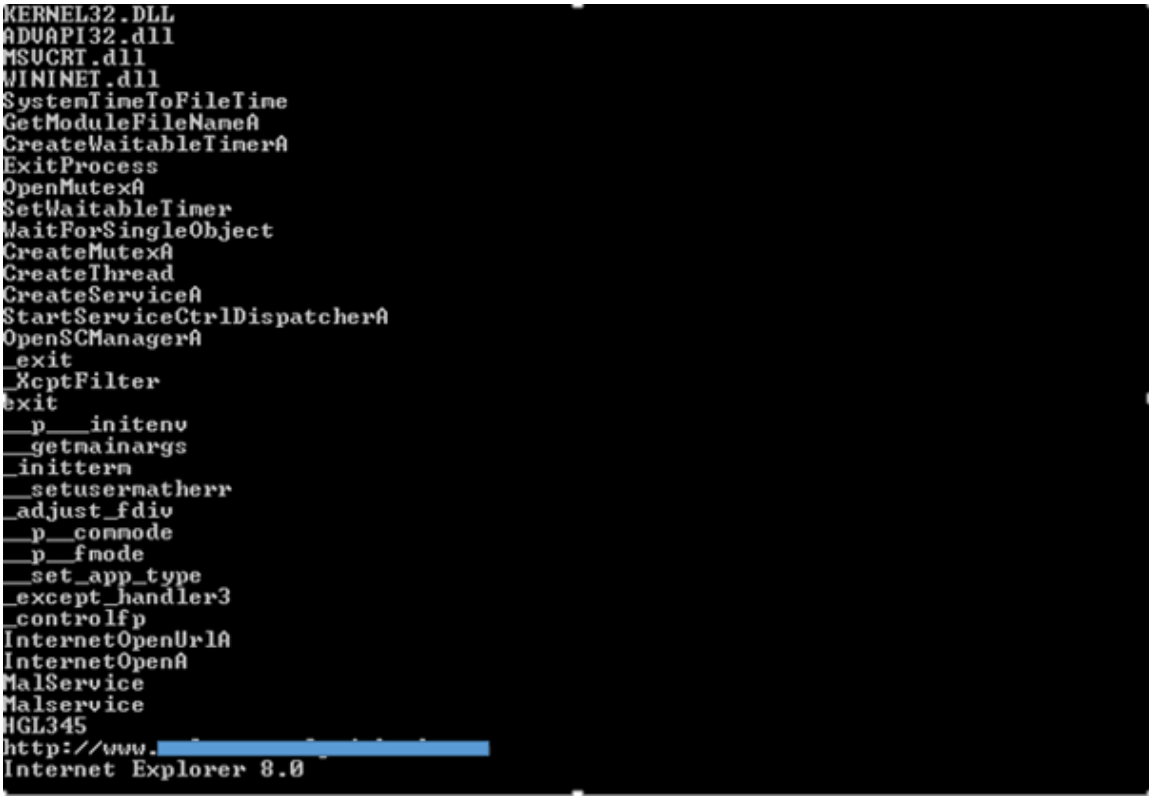
   VD: Dưới đây là một chuỗi trích xuất các từ khóa từ một tệp thực thi độc hại. Như chúng ta có thể thấy, nó cung cấp thông tin tốt có chức năng như ‘FindNextFileA’ và ‘FindFirstFileA’, cho thấy rằng tệp thực thi này sẽ tìm kiếm một tệp và sau đó kết hợp điều đó với ‘ CopyFileA’ có nghĩa là nó sẽ tìm thấy một tệp và thay thế nó bằng một tệp khác.

   Một điểm quan trọng khác cần lưu ý đó là về ‘Kerne132.dll’. Đây là một văn bản gây hiểu lầm và không nên nhầm lẫn với ‘Kernel32.dll’



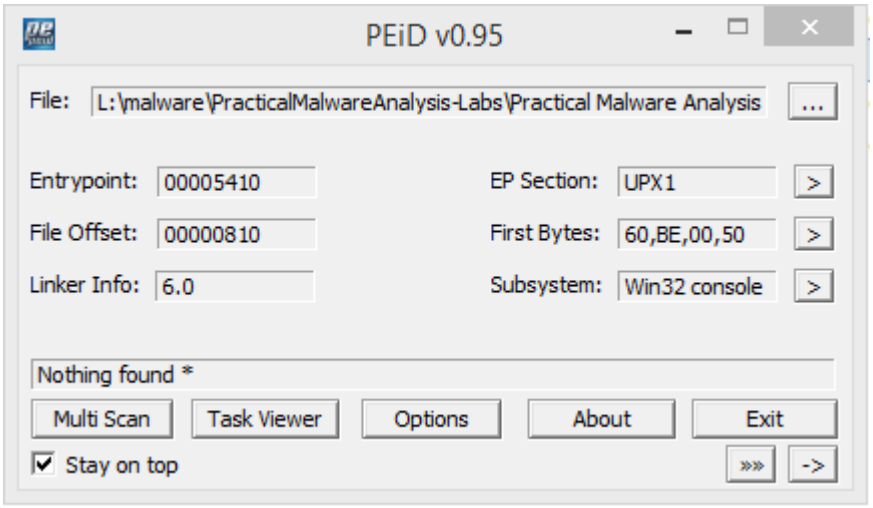
VD2: Dưới đây là một trích xuất khác từ một tiện ích string. Nó cho chúng ta thấy rằng việc sử dụng ‘CreateProcessA’ sẽ tạo ra một quy trình. Các lệnh như ‘Exec’ và ‘Sleep’ được sử dụng để điều khiển môt tệp từ xa. Nó cũng có thể là một bot, và sau đó là một trường IP, có thể là IP của một máy chủ điều khiển

VD3: Về việc trích xuất bằng cách sử dụng chuỗi. Các trường thú vị là ‘InternetOpenURLA’ nói rằng nó sẽ kết nối với một số máy chủ bên ngoài để tải xuống thứ gì đó và sau đó chúng tôi cũng có một tệp http://, thậm chí còn làm rõ địa chỉ máy chủ mà nó sẽ kết nối và tải xuống



Làm cách nào để kiểm tra xem mã phần mềm độc hại có bị xáo trộn hay không?

Thông thường, những người viết phần mềm độc hại làm xáo trộn mã của họ để các tệp khó đọc. Khi một chương trình đóng gọi chạy, một chương trình bao bọc cũng chạy xung quanh để giải nén nó. Với phân tích tĩnh, thực sự rất khó để dự đoán tệp nào được đóng gói trừ khi rõ ràng là chúng là như vậy. Ví dụ: các công cụ như PEid đôi khi có thể cho biết rằng các tệp được đóng gói rồi. Trong hình dưới, rõ ràng là các tệp được đóng gói bằng UPX



Các tệp được đóng gói UPX có thể được giải nén bằng lệnh sau:

- upx –o <newfilename> -d <packedfilename>

Phần tệp PE

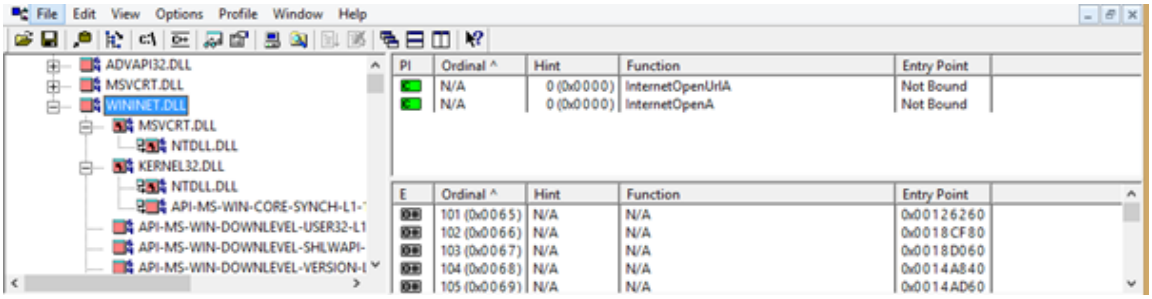
Thu thập thông tin từ định dạng tệp thực thi di động (PE)

Định dạng tệp PE được sử dụng bởi các tệp thực thi Windows, DDL, v.v. Nó chứa thông tin cần thiết cho bộ tải hệ điều hành Windows để chạy mã. Trong khi kiểm tra các tệp PE, chúng tôi có thể phân tích chức năng nào đã được nhập, xuất và loại liên kết nào ở đó, tức là thời gian chạy, tĩnh hoặc động.

Phần tệp PE

Tệp PE chứa tiêu đề và một số phần quan trọng hơn. Trong các phần này có một số thông tin hữu ích. Chúng ta cũng hãy hiểu những phần này.

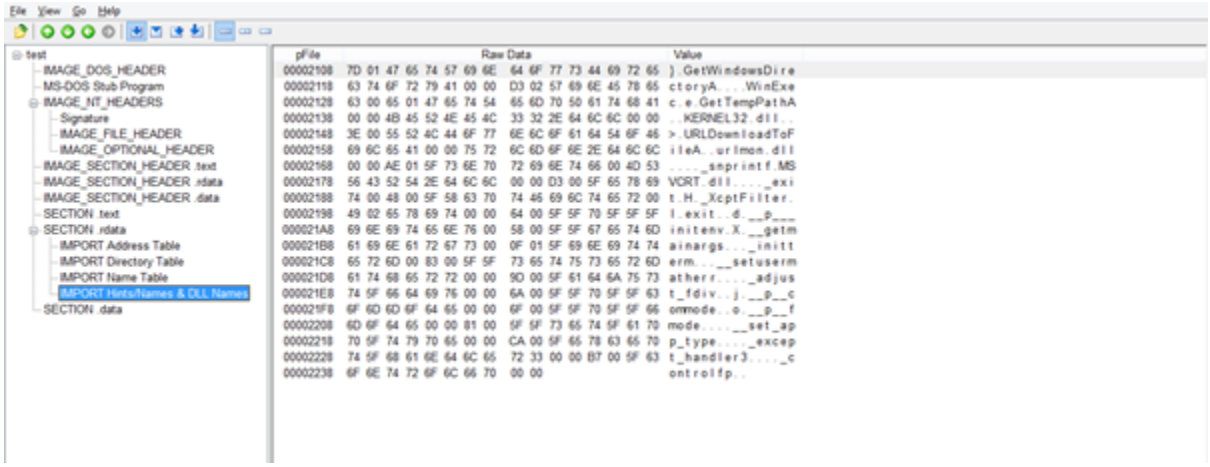
- .text: chứa mã thực thi.
- .rdata: Các phần này chỉ lưu giữ dữ liệu có thể truy cập globally.
- .data: Lưu trữ global data được truy cập thông qua chương trình.
- .rsrc: Các phần này lưu trữ các tài nguyên cần thiết cho tệp thực thi.
- Hầu hết những người viết phần mềm độc hại thường sử dụng liên kết động trong mã của họ. Ví dụ: với việc sử dụng công cụ Dependency Walker, chúng ta có thể thấy trong ảnh chụp màn hình bên dưới rằng trong WININET.dll là các chức năng như "InternetOpenUrlA", nói rằng phần mềm độc hại này sẽ tạo kết nối với một số máy chủ bên ngoài. Lưu ý: Wininet.dll chứa các chức năng mạng cấp cao hơn thực hiện các giao thức như FTP, HTTP và NTP.



- Bên dưới tiêu đề, có một phần phụ có tên là "IMAGE_FILE_HEADER", chứa trường dấu thời gian. Dấu thời gian này hiển thị thời gian biên dịch của tệp thực thi. Đây là thông tin rất quan trọng, vì nếu thời gian cũ, thì có thể có trường hợp các giải pháp AV có thể có chữ ký xung quanh nó. Tuy nhiên, trường này không đáng tin cậy, vì trình biên dịch có thể được thay đổi dễ dàng bởi người viết phần mềm độc hại.

- Giả sử từ phân tích tĩnh, một nhà phân tích dự đoán rằng tệp thực thi sẽ tạo ra một quy trình và sau đó giả sử lệnh exec và sleep sau đây được tìm thấy, nhưng không có thông tin nào được tìm thấy về DLL tương ứng, có chức năng kết nối với máy chủ khác. Trong trường hợp đó, tài nguyên được ẩn với tệp thực thi. Mở phần .rsrc của tệp PE bằng một công cụ như Resource Hacker để có thêm thông tin về phần mềm độc hại.

Dưới đây là phân tích tài nguyên trên bằng PEview.


File View Go Help
test
IMAGE_DOS_HEADER
MS-DOS Stub Program
IMAGE_NT_HEADERS
Signature
IMAGE_FILE_HEADER
IMAGE_OPTIONAL_HEADER
IMAGE_SECTION_HEADER .text
IMAGE_SECTION_HEADER .rdata
IMAGE_SECTION_HEADER .data
SECTION .text
SECTION .rdata
IMPORT Address Table
IMPORT Directory Table
IMPORT Name Table
IMPORT Hints/Names & DLL Names
SECTION .data
pFile
Raw Data
Value
00002108 7D 01 47 65 74 57 69 6E 64 6F 77 73 44 69 72 65 }.GetWindowsDire
00002118 63 74 6F 72 79 41 00 00 D3 02 57 69 6E 45 78 65 ctoryA....WinExe
00002128 63 00 65 01 47 65 74 54 65 6D 70 50 61 74 68 41 c.e.GetTempPathA
00002138 00 00 4B 45 52 4E 45 4C 33 32 2E 64 6C 6C 00 00 ..KERNEL32.dll..
00002148 3E 00 55 52 4C 44 6F 77 6E 6C 6F 61 64 54 6F 46 >.URLDownloadToF
00002158 69 6C 65 41 00 00 75 72 6C 6D 6F 6E 2E 64 6C 6C ileA..urlmon.dll
00002168 00 00 AE 01 5F 73 6E 70 72 69 6E 74 66 00 4D 53 ...._snprintf.MS
00002178 56 43 52 54 2E 64 6C 6C 00 00 D3 00 5F 65 78 69 VCRT.dll....._exi
00002188 74 00 48 00 5F 58 63 70 74 46 69 6C 74 65 72 00 t.H._XcptFilter.
00002198 49 02 65 78 69 74 00 00 64 00 5F 5F 70 5F 5F 5F I.exit..d.__p___
000021A8 69 6E 69 74 65 6E 76 00 58 00 5F 5F 67 65 74 6D initenv.X.__getm
000021B8 61 69 6E 61 72 67 73 00 0F 01 5F 69 6E 69 74 74 ainargs..._initt
000021C8 65 72 6D 00 83 00 5F 5F 73 65 74 75 73 65 72 6D erm..__setuserm
000021D8 61 74 68 65 72 72 00 00 9D 00 5F 61 64 6A 75 73 atherr...._adjus
000021E8 74 5F 66 64 69 76 00 00 6A 00 5F 5F 70 5F 5F 63 t_fdiv..j.__p__c
000021F8 6F 6D 6D 6F 64 65 00 00 6F 00 5F 5F 70 5F 5F 66 ommode..o.__p__f
00002208 6D 6F 64 65 00 00 81 00 5F 5F 73 65 74 5F 61 70 mode....__set_ap
00002218 70 5F 74 79 70 65 00 00 CA 00 5F 65 78 63 65 70 p_type...._excep
00002228 74 5F 68 61 6E 64 6C 65 72 33 00 00 B7 00 5F 63 t_handler3....._c
00002238 6F 6E 74 72 6F 6C 66 70 00 00 ontrolfp..

Kernel32.dll	User32.dll	User32.dll (continued)
CreateDirectoryW	BeginDeferWindowPos	**ShowWindow**
CreateFileW	CallNextHookEx	ToUnicodeEx
CreateThread	CreateDialogParamW	TrackPopupMenu
DeleteFileW	CreateWindowExW	TrackPopupMenuEx
ExitProcess	DefWindowProcW	TranslateMessage
FindClose	DialogBoxParamW	UnhookWindowsHookEx
FindFirstFileW	EndDialog	UnregisterClassW
FindNextFileW	GetMessageW	UnregisterHotKey
GetCommandLineW	GetSystemMetrics	
GetCurrentProcess	GetWindowLongW	**GDI32.dll**
GetCurrentThread	GetWindowRect	GetStockObject
GetFileSize	GetWindowTextW	SetBkMode
GetModuleHandleW	InvalidateRect	SetTextColor
GetProcessHeap	IsDlgButtonChecked	
GetShortPathNameW	IsWindowEnabled	**Shell32.dll**
HeapAlloc	LoadCursorW	CommandLineToArgvW
HeapFree	LoadIconW	SHChangeNotify
IsDebuggerPresent	LoadMenuW	SHGetFolderPathW
MapViewOfFile	MapVirtualKeyW	ShellExecuteExW
OpenProcess	MapWindowPoints	ShellExecuteW
ReadFile	MessageBoxW	
SetFilePointer	**RegisterClassExW**	**Advapi32.dll**
WriteFile	**RegisterHotKey**	RegCloseKey
	SendMessageA	RegDeleteValueW
	SetClipboardData	RegOpenCurrentUser
	SetDlgItemTextW	RegOpenKeyExW
	SetWindowTextW	RegQueryValueExW
	SetWindowsHookExW	RegSetValueExW

→ Bảng trên liệt kê các tập tin DLLs và các hàm import Functions từ một tập tin mã độc

Như hầu hết các chương tình có kích thước trung bình, tập tin thực thi này chứ một số lượng lớn các hàm import functions. Nhưng chỉ một số nhỏ các import function là quan trọng trong việc phân tích mã độc. Khi bạn không chắc chắn về một hàm chức

năng nào đó, bạn cần tìm kiếm và xác định nó là gì. bạn có thể tham khảo những hàm chức năng quan trọng đối với việc phân tích mã độc trong phần phụ lục, hoặc có thể tìm kiếm chúng trên hệ thống trực tuyến MSDN

Thông thường, sẽ không nhận biết được mã độc này có phải là một tập tin keylogger tiềm năng hay không, và sẽ cần phải tìm kiếm các chức năng mà sẽ cung cấp manh mối để giúp xác định đây có phải là mã độc hay không. Cta cần tập trung vào các chức năng cung cấp các gợi ý về chức năng của chương trình đang xét

Các hàm import functions được liệt kê từ tệp tin Kernel32.dll trong hình trên cho cta biết phần mềm này có thể mở và thao tác các tiến trình như OpenProcess, GetCurrentProcess và GetProcessHeap, và các tập tin như ReadFile, CreateFile, WriteFile. Những hàm chức năng FindFirstFile và FindNextFile là những hàm đặc biệt mà chúng ta có thể sử dụng để thông qua các thư mục

Các hàm import function được liệt kê từ tập tin User32.dll thậm chí còn quan trọng hơn nữa. Một số lượng lớn của các hàm chức năng thao tác trên giao diện đồ họa (như là RegisterClassEx, SetWindowText và ShowWindow) cho thấy một khả năng rất cao phần mềm này sẽ có một giao diện đồ họa (mặc dù giao diện GUI này không nhất thiết phải hiển thị cho người sử dụng)

Hàm chức năng SetWindowsHookEx thường được sử dụng trong phần mềm gián điệp (spyware) và là cách phổ biến nhất mà các phần mềm keylogger ghi nhận các thông tin đầu vào từ bàn phím máy tính

Hàm chức năng RegisterHotkey cũng khá là đáng quan tâm. Chúng đăng ký một phím nóng (hot key) như là CTRL SHIFT -P

Các hàm import functions được liệt kê từ tập tin GDI32.dll là một hàm có liên quan tới đồ họa và chỉ đơn giản là xác nhận chương trình này có thể có một giao diện đồ họa. Các hàm import functions được liệt kê từ tập tin Shell32.dll cho chúng ta biết đây là một tính năng phổ biến của các phần mềm độc hại cũng như các chương trình hợp pháp

Các hàm import functions được liệt kê từ tập tin Advapi32.dll cho chúng ta biết chương tình này sử dụng các registry, điều này cho chúng ta biết chúng ta nên tìm các chuỗi strings mà giống như các khóa của Registry. Các chuỗi Registry trông rất giống như các thư mục. Trong trường hợp này, chúng ta tìm thấy chuỗi trong

Software\Microsoft\Windows\CurrentVersion\Run, đây là một khóa Registry (thường được sử dụng bởi các phần mềm độc hại) dùng để điều khiển các chương trình được chạy tự động khi Windows khởi động.

Tập tin thực thi này cũng có một số hàm export function như LowLevelKeyboardProc và LowLevelMouseProc. Một số tài liệu của Microsoft cho rằng, “Hàm thủ tục LowLevelKeyboardProc là một ứng dụng đã được xác định hoặc là thư viện đã được xác định gọi lại các chức năng đã sử dụng với hàm chức năng SetWindowsHookEx”. Nói cách khác, chức năng này được sử dụng với SetWindowsHookEx để xác định những chức năng sẽ được gọi khi một sự kiện được xác định xảy ra, trong trường hợp này, là sự kiện ghi nhận bàn phím ở mức độ thấp. Các tài liệu cho SetWindowsHookEx giải thích thêm rằng chức năng này sẽ được gọi lên khi khi các sự kiện bàn phím ở mức thấp xảy ra.

Các tài liệu của Microsoft sử dụng tên LowLevelKeyboardProc, và các lập trình viên trong trường hợp này đã làm tốt công việc của mình. Chúng ta đã có thể lấy được các thông tin có giá trị bởi vì các lập trình viên đã không làm mờ tên của các hàm export function.

Việc sử dụng các thông tin thu thập được từ một phân tích tĩnh của các import function và export function, chúng ta có thể rút ra một số kết luận đáng kể hoặc xây dựng một số giả thuyết về phần mềm độc hại này. Trong một số trường hợp, nó có thể được xem là một local keylogger sử dụng hàm SetWindowsHookEx để ghi nhận lại các thao tác trên bàm phím. Chúng ta cũng có thể phỏng đoán nó có một giao diện đồ họa mà chỉ hiển thị đối với một số người dùng cụ thể nào đó, và phím nóng được đăng ký với hàm RegisterHotKey để giúp người phát tán mã độc gọi giao diện đồ họa của chương trình bằng phím nóng và xem nội dung các thao tác bàn phím được ghi lại. Chúng ta có thể tiếp tục suy đoán từ các hàm chức năng registry và sự tồn tại của Software\Microsoft\Windows\CurrentVersion\Run điều mà chương trình này tự thiết lập chính nó để nạp lúc khởi động hệ thống.

PackedProgram.exe: A Dead End

Hình minh họa bên dưới cho ta thấy một danh sách đầy đủ các hàm import function từ một khía cạnh khác của phần mềm độc hại mà ta chưa biết. Sự ngắn gọn của danh sách này cho chúng ta biết rằng phần mềm này đã được đóng gói hoặc đã được làm mờ đi, điều này khẳng định thực tế rằng không thể đọc ra được các chuỗi Strings. Một trình biên dịch của Windows sẽ không tạo ra một chương trình mà các hàm import function có số lượng ít như thế, thậm chí một chương trình xuất ra Hello World còn có nhiều hàm chức năng hơn thế.

Table 1-3: DLLs and Functions Imported from *PackedProgram.exe*

Kernel32.dll	User32.dll
GetModuleHandleA	MessageBoxA
LoadLibraryA	
GetProcAddress	
ExitProcess	
VirtualAlloc	
VirtualFree	

Cần xây dựng lab phân tích phần mềm độc hại và sandbox của riêng mình. Kỹ thuật cơ bản nhất là triển khai một số máy ảo bị cô lập (linux và windows) hoặc bạn có thể triển khai một số sandbox phân tích phần mềm độc hại sẵn sàng sử dụng như cuckoo sandbox hoặc Flare VM

Phương pháp phân tích malware: trong hầu hết các trường hợp, là một nhà phân tích phần mềm độc hại, cần thực hiện các kỹ thuật phân tích sau:

- Phân tích tĩnh: nó đang thu thập thông tin về ứng dụng độc hại mà không chạy nó
- Phân tích động: phân tích cách phần mềm độc hại hoạt đọng sau khi chạy nó trong sandbox
- Phân tích bộ nhớ: thi thập và phân tích các thành phần lạ bộ nhớ để tìm hiểu về phần mềm độc hại

Mẫu phần mềm độc hại và bộ dữ liệu:

Cần phải có một số mẫu độc hại để có thể bắt đầu thực hành những gì đàn sử dụng. Nhiều nhà phân tích nhà nghiên cứu và tổ chức đang chia sẻ một số mẫu phần mềm độc hại và bộ dữ liệu học máy học với cộng đồng cho mục đích giáo dục, ví dụ:

- Bộ dữ liệu phần mềm độc hại Android http://amd.arguslab.org
- Điểm chuẩn phần mềm độc hại Endgame cho nghiên cứu: https://github.com/endgameinc/ember

- http://practicalmalwareanalysis.com/labs/
- https://zeltser.com/malware-sample-sources/
- http://www.tekdefense.com/downloads/malware-samples/
- http://syrianmalware.com/
- https://malwr.com/

Phần tích phần mềm độc hại tĩnh

Mẫu: "TheZoo”

TheZoo là một dự án được tạo ra để làm cho khả năng phân tích phần mềm độc hại mở và có sẵn cho công chúng, vì đã phát hiện ra rằng hầu hết tất cả các phiên bản phần mềm độc hại đều rất khó kiếm theo cách cho phép phân tích → quyết định thu thập tất cả chúng một cách dễ tiếp cận và an toàn

TheZoo được sinh ra bởi Yaval tisf Nativ và hiện được duy trì bởi Shahak Shalev

Đây là phần mềm độc hại trực tiếp và nguy hiểm chúng được mã hóa và khóa

Network Design

Định nghĩa:

Network design là thiết kế mạng - một thuật ngữ thuộc nhóm Technology Terms - CNTT

Độ phổ biến: 5/10

Thiết kế mạng đề cập đến việc lập kế hoạch thi hành một cơ sở hạ tầng mạng máy tính

Giải thích ý nghĩa:

Thiết kế mạng liên quan đến việc đánh giá tìm hiểu và xác định phạm vi mạng được thực hiện. Việc thiết kế toàn bộ mạng lưới thường được biểu diễn dưới dạng một sơ đồ mạng đóng vai trò như các kế hoạch chi tiết để thực hiện mạng vật lý.

Yêu cầu thiết kế mạng , xác định yêu cầu thiết kế?

Quá trình thiết kế mạng bắt đầu từ việc thu thập thông tin khách hàng, để có được yêu cầu của khách hàng, bạn cần giao tiếp với các kỹ sư mạng, nhân viên đơn vị kinh doanh và quản lý công ty

Bạn có thể xác định các yêu cầu của khách hàng bằng cách nói chuyện vs KH

Là một người thiết kế mạng, cần các bước sau để xác định các yêu cầu của khách hàng:

- Xác định các ứng dụng và dịch vụ mạng mà tổ chức muốn chạy trong mạng cntt
- Xác định các mục tiêu của tổ chức
- Xác định các ràng buộc và hạn chế tổ chức có thể có, những hạn chế này có thể liên quan đến chi phí
- Xác định các mục tiêu kỹ thuật
- Xác định các ràng buộc kỹ thuật có thể có

Sau khi hoàn thành các bước trên, sau đó cần phân tích dữ liệu và phát triển một thiết kế mạng

Cần xác định các ứng dụng hiện tại và theo kế hoạch , xác định tầm quan trọng của từng ứng dụng

VD: email có quan trọng như hỗ trợ khách hàng không? Dịch vụ Voip có bắt buộc không?

Xác định các ứng dụng và dịch vụ mạng:

Tìm ra tất cả các ứng dụng cần thiết cho một tổ chức và liệt kê chúng

Bạn cần tìm hiểu những ứng dụng mạng nào cần tính khả dụng cao và băng thông cao mà bạn cần để tạo và chuẩn bị một kế hoạch cho các ứng dụng và dịch vụ này

Các loại ứng dụng được lên kế hoạch

Bạn cần xác định một ứng dụng cho các dịch vụ cần thiết khác nhau như vậy, như cho email, máy chủ trao đổi và ở cuối máy khách để cộng tác và dịch vụ thoại như Trình quản lý cuộc gọi Cisco hoặc Microsoft Lynccan được sử dụng và cũng giống nhau cho các dịch vụ khác như duyệt web, chia sẻ tệp và cơ sở dữ liệu.

Cũng phải tìm hiểu tầm quan trọng kinh doanh của các ứng dụng khác nhau và gắn nhãn chúng là quan tọng, ? hay không

VD: đối với một số email của tổ chức có thể là một ứng dụng quan trọng so với tin nhắn tức thời

Ngoài ra, hãy liệt kê các dịch vụ mạng bổ sung như bảo mật, chất lượng dịch vụ (QoS), quản lý mạng, tính khả dụng cao, truyền thông hợp nhất, tính di động và ảo hóa

Xác định mục tiêu của tổ chức

Mục tiêu của tổ chức có liên quan đến sự phát triển của công ty

→ cần xác định xem mục tiêu của công ty là cải thiện hỗ trợ khách hàng, thêm dịch vụ khách hàng mới, tăng khả năng cạnh tranh hay giảm tốc độ, Nó có thể là sự kết hợp của những mục tiêu này, với một sô trong số chúng quan trọng hơn là những mục tiêu khác.

Một số mục tiêu của tổ chức như sau:

- Chất lượng dịch vụ
- Tăng khả năng cạnh tranh
- Giảm chi phí
- Cải thiện hỗ trợ khách hàng
- Thêm dịch vụ khách hàng mới

Xác định các ràng buộc và hạn chế có thể có của tổ chức

Các hạn chế và hạn chế về tổ chức bao gồm giới hạn về chi phí, nhân sự, chính sách và thời gian. Tổ chức có thể có một số hạn chế liên quan đến chi phí và bạn có thẻ được cung cấp một ngân sách hoặc khung thời gian nhất định để hoàn thành dự án. Tổ chức có thể yêu cầu dự án được hoàn thành trong một khung thời gian không hợp lý. Nó có thể có nhân sự hạn chế để hỗ trợ các nỗ lực đánh giá và thiết kế hoặc nó có thể có những hạn chế về chính sách để áp dụng các tiêu chuẩn và giao thức nhất định

VD: đối với một số tổ chức bạn có thể cần thực hiện các chính sách khác nhau và mức độ bảo mật nhất định vì các yêu cầu và chưng nhận HIPPA.

Xác định các mục tiêu kỹ thuật

Các mục tiêu kỹ thuật hỗ trợ các mục tiêu của tổ chức và các ứng dụng được hỗ trợ

Một số mục tiêu kỹ thuật bao gồm:

- Cải thiện an ninh mạng
- Thực hiện QoS
- Cải thiện thời gian phản hồi, thông lượng mạng
- Giảm lỗi mạng và thời gian chết (tính khả dụng cao)
- Đơn giản hóa việc quản lý mạng
- Cải thiện độ tin cậy của các ứng dụng quan trọng
- Cập nhật công nghệ tiên tiến với các công nghệ mới nhất
- Cải thiện khả năng mở rộng của mạng

Xác định các ràng buộc kỹ thuật có thể có

Thiết kế mạng có thể bị ảnh hưởng với các ràng buộc kỹ thuật khác nhau. Các ứng dụng kế thừa có thể vẫn tồn tại phải được hỗ trợ trong tương lai và các ứng dụng này có thể yêu cầu một giao thức kế thừa có thể giới hạn một thiết kế. Hạn chế kỹ năng bao gồm cáp hiện có điều đò không hỗ trợ công nghệ mới, băng thông thấp có thể không hỗ trợ các ứng dụng mới. Vì vậy, bạn cần tìm tất cả các hạn chế kỹ thuật và giải pháp chống lại từng hạn chế

Mô tả mạng hiện có

Đặc trưng cho mạng hiện có là bước thứ hai của phương pháp thiết kế mạng. Trong bước này, bạn cần xác định cơ sở hạ tâng và dịch vụ hiện có của mạng hiện đang chạy. Bạn có thể sử dụng các công cụ khác nhau để phân tích lưu lượng mạng hiện có và các công cụ để kiểm tra và giám sát lưu lượng mạng

Để mô tả mạng hiện cóm cần truy cập trang web và tất cả các tài liệu hiện có liên quan đến mạng hiện tại là nguồn tuyệt vời để có được thông tin liên quan đến mạng hiện có. Đôi khi không có thông tin tài liệu tồn tại. Bạn nên chuẩn bị sử dụng các công cụ khác nhau để lấy thông tin và có quyền truy cập để đăng nhập vào các thiết bị mạng để lấy thông tin

Cụ thể các bước thu thập thông tin:

1. **Xác định tất cả thông tin và tài liệu tổ chức hiện có:**

Thoát khỏi tài liệu mạng có thể cung cấp cho bạn thông tin khác nhau như:

- Tên trang web
- Định vị trang web
- Liên hệ trên trang web
- Bố trí cáp và theo dõi trong tòa nhà
- Vị trí phòng máy chủ
- Giờ hoạt động của văn phòng
- Thông tin cấu trúc mạng như:
    - Vị trí và loại máy chủ và thiết bị mạng
    - Công nghệ WAN và tốc độ mạch
    - Công suất sử dụng

- Thông tin mạng logic bao gồm định địa chỉ IP, giao thức định tuyến, quản lý mạng và ACL bảo mật

2. **Thực hiện kiểm tra mạng thêm chi tiết vào mô tả của mạng**

   Để thu thập thông tin của mạng hiện có, bạn có thể thực hiện kiểm tra mạng , kiểm toán với sự trợ giúp của tài liệu hiện có, các công cụ phần mềm quản lý mạng hiện có và với một số công cụ kiểm tra khác.

   Sau khi thu thập các tài liệu hiện có, bạn phải có quyền truy cập vào phần mềm quản lý hiện có. Khách hàng có thể đã có các công cụ CiscoWorks mà từ đó bạn có thể có được các mô hình và thành phần cứng cũng như các phiên bản phần mềm.

   Bạn cũng có thể lấy bộ định tuyến hiện có và cấu hình chuyển mạch. Kiểm tra mạng sẽ cung cấp cho bạn danh sách thiết bị mạng, mô hình phần cứng phiên bản phần mềm, cấu hình thiết bị mạng, tốc độ giao diện, liên kết, CPU, băng thông và sử dụng bộ nhớ

   Trong mạng nhỏ, bạn có thể có được thông tin cần thiết thông qua đánh giá vật lý, nhưng đối với mạng lớn hơn, việc đánh giá thủ công rất tốn thời gian. Đánh giá thủ công bao gồm việc sử dụng các lệnh để tìm cấu hình của các thiết bị khác nhau, thông thường hiển thi lệnh cung cấp cho bạn thông tin liên quan đến thông tin thiết bị như kiểu máy, cấu hình… Một số ví dụ về lệnh hiển thị Cisco là:

   - Hiển thị cấu hình đang chạy
   - Thể hiện hỗ trợ kỹ thuật
   - Hiển thị phiên bản
   - Hiển thị giao diện
   - Hiển thi tóm tắt Ip
   - Hiển thị quá trình CPU
   - Hiển thị nhật ký

   Đối với mạng lớn, bạn có thể sử dụng các công cụ phân tích và kiểm tra mạng khác nhau bao gồm:

   - Công cụ kiểm tra mạng
     - Giải pháp CiscoWorks: Ánh xạ mạng và thu thập cấu trúc liên kết mạng, các phiên bản phần cứng và phần mềm và cấu hình

- Nhận dạng ứng dụng dựa trên mạng (NBAR): Nhận dạng ứng dụng dựa trên mạng do Cisco phát triển như một phần của nền tảng Mảng nội dung để triển khai các dịch vụ mạng thông minh như tài nguyên sẵn có được sử dụng hiệu quả nhất có thể
- NetFlow: Cung cấp chế độ xem các luồn lưu lượng mạng trên giao diện mạng cụ thể
- Cisco Operations Manager : cũng là một công cụ tiện dụng
- Một số công cụ của bên thứ ba là AirMagnet Survey PRO, Stats Manager, Yellowjacket, Redcell engineering pro, NetcordiaNEtMRI, Neformix, NetQoS và Pari Networks
- Công cụ phân tích mạng
  - Đối với thông tin cấp ứng dụng bạn có thể cần các chi tiết của gói IP , bạn có thể sử dụng các công cụ và phần mềm phân tích khác nhau. Công cụ phân tích mạng bao gồm:
    - NetformxDesignXpert Enterprise
    - CNS NetFlow Collector Engine
    - Cisco Embedded Resource Manager (ERM) (trình quản lý nhúng tài nguyên của Cisco)
  - Các công cụ của bên thứ ba: Chẳng hạn như Sniffer, AirMagnetWifi Analyzer, BVS Yellowjacket802.11, NetIQ Vivinet Assessor, NetcordiaNetMRI và

Cách thiết kế | mạng Phương pháp thiết kế tám bước - W7cloud

Thiết kế cấu trúc liên kết mạng và các giải pháp

Trong bước này hoặc phần tử của phương pháp thiết kế tám bước, phải chọn cấu trúc liên kết mạng và cần chuẩn bị giải pháp mạng cho tổ chức.

Cách tiếp cận tốt nhất để thiết kế cấu trúc liên kết mạng là cách tiếp cận cấu trúc cho phép bạn phát triển giải pháp tối ưu với hi phí thấp hơn với việc đáp ứng tất cả các yêu cầu của khách hàng như năng lức, tính linh hoạt, chức năng, hiệu suất, khả năng mở rộng tính khả dụng

Giải pháp mạng bao gồm những thứ như công nghệ WAN, dịch vụ mạng LAN và tất cả các thiết bị mà qua đó bạn có thể triển khai giải pháp mạng này

Bạn có thể bắt đầu quá trình thiết kế mạng với thông tin mà bạn trích xuất thông qua:

1. Thông tin và tài liệu hiện có
2. Kiểm toán mạng
3. Phân tích lưu lượng truy cập

Cisco khuyên bạn nên sử dụng phương pháp tiếp cận từ trên xuống dưới để thiết kế cấu trúc liên kết mạng và giải pháp là một phần của giai đoạn Thiết kế bạn có thể sử dụng phương pháp PPDIOO hoặc cách tiếp cận từ trên xuống được sử dụng điều đó bắt đầu với ác yêu cầu của tổ chức trước khi xem xét các công nghệ. Networks design được thử nghiệm bằng cách sử dụng mạng thí điểm hoặc mạng nguyên mẫu trước khi chuyển sang giai đoạn thực hiện. Thiết kế từ trên xuống chỉ có nghĩa là bắt đầu thiết kế của bạn từ lớp trên cùng của mô hình OSI và làm việc theo cách của bạn xuống. THiết kế từ trên xuống điều chỉnh mạng và cơ sở hạ tầng vật lý phù hợp với nhu cầu của ứng dụng mạng.

Với cách tiếp cận từ trên xuống, các thiết bị và công nghệ mạng không được chọn cho đến khi các yêu cầu của ứng dụng được phân tích

Lập kế hoặc triển khai mạng

Bước thứ 4 là bước lập kế hoạch triển khai mạng liên quan đến mức độ tốt của tài liệu, sơ đồ và các tài liệu liên quan khác. Trong tài liệu, nên có quy tình từng bước của từng khía cạnh của mạng module và có chi tiết đầy đủ để thực hiện từng bước.

Tài liệu phải có kế hoạch khôi phục cho mỗi bước, nếu có sự cố xẩy ra, bạn có thể quay lại bước trước đó và sau khi sửa đổi, bạn có thể thực hiện lại bước đó một lần nữa

Một khía cạnh quan trọng khác của kế hoạch triển khai mạng là xác định khung thời gian cho từng bước hoặc từng module, bạn có thể bao gồm các nhà quản lý dự án của mình cho các mục đích này. Ngoài ra cần đảm bảo rằng bao gồm bài test ở mọi bước trong quy trình

Và để đơn giản bạn có thể chia nhỏ các quy trình phức tạp thành các phần nhỏ để cung cấp sự hiểu biết tốt hơn và dễ thực hiện hơn

Xây dựng một mạng nguyên mẫu hoặc một trang web test thử nghiệm thiết kế mạng

Trong quá trình thiết kế và triển khai mạng khi bạn hoàn thành một module mạng mới hoặc triển khai thiết kế đến trang wen nhỏ, trước khi triển khai đầy đủ, đó là một

thực tiễn tốt nhấ để thử nghiệm giải pháp mới. Thử nghiệm này có thể được thực hiện theo một trong hai cách:

1. **Mạng nguyên mẫu:**

   Là một tập hợp con của thiết kế đầy đủ, được thử nghiệm trong một môi trường biệt lập. Prototype không thể kết nối với mạng hiện có. Lợi ích của việc sử dụng một nguyên mẫu là cho phép thử nghiệm thiết kế mạng trước khi nó được triển khai trước khi ảnh hưởng đến một mạng sản xuất.

   Khi triển khai một công nghệ mới như IPSec bạn có thể muốn thực hiện thử nghiệm nguyên mẫu trước khi triển khai nó vào mạng lưới hoạt động

2. **Trang web thử nghiệm**

   Là một vị trí trực tiếp thực tế đóng vai trò là trang web thử nghiệm trước khi giải pháp được triển khai cho tất cả các địa điểm trong doanh nghiệp.

   Một thí điểm cho phép các vấn đề trong thế giới thực được phát hiện trước khi triển khai giải pháp thiết kế mạng cho phần còn lại của internet

→ Với cả nguyễn mẫu và thí điểm, thử nghiệm thành công dẫn đến việc chứng minh thiết kế và phát triển với việc thực hiện. Một thất bại dẫn đến việc sửa chữa thiết kế và lặp lại các thử nghiệm để sửa chữa bất kỳ thiết sót nào

Ghi lại đầy đủ các thiết kế tài liệu thiết kế mạng

Ghi lại dự án là cách thực hành tốt nhất và có một số lợi thế và lợi ích trong tương lai

Tài liệu thiết kế mô tả các yêu cầu kinh doanh, cũng bao gồm kiến trúc mạng cũ, yêu cầu mạng, thiết kế, kế hoạch và thông tin cấu hình cho mạng mới

Các kiến trúc sư và nhà phân tích mạng sử dụng nó để ghi lại những thay đổi mạng mới và nó xứng đáng làm tài liệu cho doanh nghiệp. Đối với tài liệu thiết kế mạng, bạn có thể làm theo quy trình tiêu chuẩn để tạo tài liệu. Thủ tục này bao gồm giới thiệu dự án, yêu cầu thiết kế, chi tiết về mạng hiện có, thiết kế, bằng chứng khái niệm, thực hiện kế hoạch và phụ lục.

Mô tả ngắn gọn về từng module

- Giới thiệu: mô tả thông tin giới thiệu liên quan đến mục đích của dự án và lý do thiết kế mạng
- Yêu cầu thiết kế liệt kê các yêu cầu, ràng buộc và mục tiêu của tổ chức

- Cơ sở hạ tầng mạng hiện có bao gồm các sơ đồ cấu trúc liên kết logic (lớp 3) , sơ đồ vật lý, kết quả kiểm toán, phân tích mạng lưới, các giao thức định tuyến, tóm tắt các ứng dụng, danh sách các bộ định tuyến mạng, thiết bị chuyển mạch và các thiết bị khác, cấu hình và mô tả các vấn đề
- Thiết kế mạng chứa thông tin thiết kế cụ thể chẳng hạn như cấu trúc liên kết logic và vật lý, sơ đồ mạng, địa chỉ IP, giao thức định tuyến và cấu hình bảo mật
- Bằng chứng về kết quả khái niệm từ thử nghiệm thí điểm trực tiếp hoặc nguyên mẫu
- Implementation Plan - kế hoạch triển khai bao gồm các bước chi tiết để nhân viên mạng thực hiện cài đặt mới và thay đổi
- Phụ lục chứa danh sách các thiết bị mạng, cấu hình và thông tin bổ sung được sử dụng trong thiết kế mạng

Thực hiện thiết kế

Trong giai đoạn thực hiện kỹ sư mạng thực hiện thiết kế của mạng. Trong giai đoạn này thực hiện các bước tài liệu, sơ đồ mạng thực

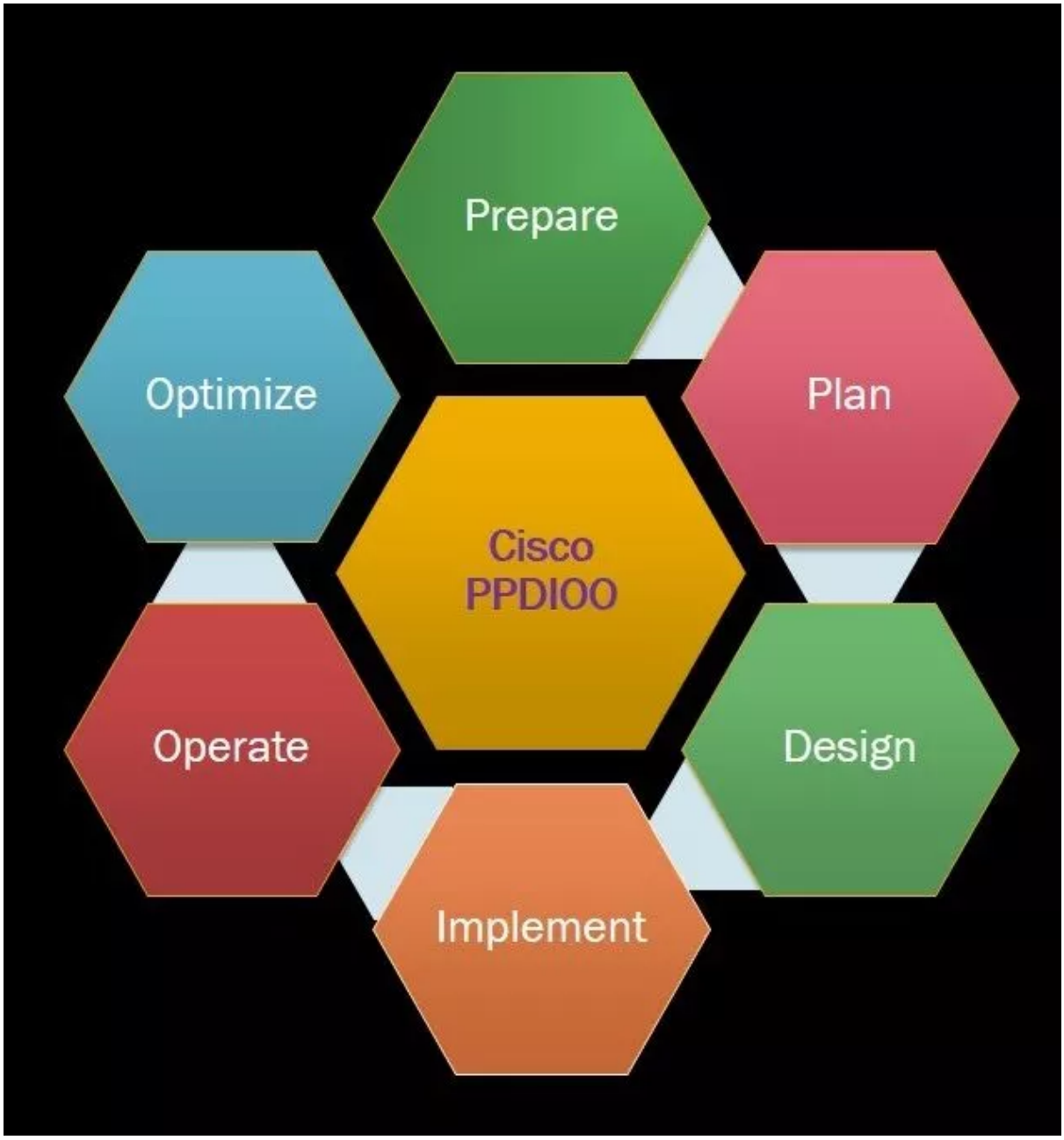
Sáu bước đầu tiên của mô hình thiết kế 8 bước có liên quan đến CCDA và nơi bạn phải thiết kế và ghi lại dự án vì hai bước còn lại liên quan đến việc thực hiện và xác minh là một phần của CCNP

Xác minh, giám sát và sửa đổi khi cần thiết

Khi mạng của bạn được triển khai đầy đủ thì công việc của bạn là chạy và vận hành mạng đúng cách, bạn phải giám sát các thiết bị mạng, lưu lượng truy cập và các khía cạnh bảo mật khác. Bạn có thể thực hiện sửa đổi nếu bạn tìm thấy điều gì đó không ổn với hoạt động mạng trong quá trình giám sát mạng. Ngoài ra, nếu bạn cần thêm một số dịch vụ và tính năng khác, bạn cũng có thể thêm các dịch vụ này.

PPDIOO

Là vòng đời mạng được xác định bởi Cisco. PPDIOO có sáu giai đoạn hoặc bước để thiết kế mạng và các giai đoạn thiết kế này như sau:



- Chuẩn bị
- Kế hoạch
- Thiết kế
- Thực hiện
- Hành quân
- Tối ưu hóa

Ưu điểm lợi ích của PPDIOO:

Ưu điểm chính của PPDIOO là giảm TCO (tổng chi phí sở hữu), ngay từ đầu quá trình có thể đánh giá và xác nhận các yêu cầu công nghê. Cũng có thể lập kế hoặc đúng đắn cho những thay đổi trong cơ sở hạ tầng và những thay đổi về yêu cầu đối với tài nguyên.

PPDIOO cũng cải thiện tính khả dụng của mạng vì đang sử dụng thiết kế mạng chắc chắn và tất cả chỉ theo cách đang xác thực các hoạt động mạng của mình. Nó cũng tăng tốc độ truy cập vào các tài nguyên và ứng dụng mạng

Một điều quan trong cần lưu ý là vòng đời mạng của bạn có thể khong cần thiết trải qua tất cả các giai đoạn theo thứ tự xác định. Nó hoàn toàn có khả năng đi vào giai đoạn chuẩn bị, giai đoạn lập kế hoạch, giai đoạn thiết kế và giai đoạn thực hiện và sau đó có thể phải quay lại giai đoạn lập kế hoạch để thực hiện một số thay đổi và sau đó phải đi vào giai đoạn thiết kế thực hiện các thay đổi thành thiết kế

1. Chuẩn bị:

   Giai đoạn đầu tiên là Chuẩn bị, nơi bạn bắt đầu thiết lập các yêu cầu và mục tiêu kinh doanh của mình. CNTT và cơ sở hạ tầng mạng của một tổ chức liên quan trực tiếp đến mục tiêu kinh doanh của tổ chức đó. Thông thường trong giai đoạn này, ban giám đốc hoặc quản lý cấp cao của tổ chức có liên quan với tư cách là một nhà thiết kế mạng, bạn cần liệt kê tất cả các cơ sở hạ tầng có thể có cho công nghệ của mình mà bạn có thể triển khai cho công ty đó. bạn có thể xây dựng một trường hợp kinh doanh trong giai đoạn này, điều này có thể cung cấp cho bạn những lý do tài chính cho chiến lược mạng tổng thể

2. Giai đoạn lập kế hoạch:

   Bạn có thể bắt đầu giai đoạn kế hoạch bằng cách thu thập thông tin và liệt kê tất cả các yêu cầu bao gồm tất cả các yêu cầu dịch vụ và yêu cầu bảo mật. Bạn cũng cần suy nghĩ về tất cả các loại quản trị và hợp đồng mà một tổ chức có với các tổ chức khác nhau

   VD như ‘HIPPA’, ‘GLBA’ chỉ thị bảo vệ dữ liệu của EU. Bạn cần đảm bảo an ninh mạng của mình bằng cách lập kế hoạch và thiết kế mạng với các phương pháp hay nhất. Bạn cũng cần xem xét quy trình quản lý mạng, bạn có thể cần phải làm việc về quản lý lỗi, quản lý cấu hình, quản lý bảo mật và quản lý kế toán để hoàn thiện kế hoạch mạng

   Trong giai đoạn lập kế hoạch, cần phân tích tất cả các yêu cầu và lập kế hoạch để thực hiện các phương pháp hay nhất, bạn cần phân tích tất cả các yêu cầu và lập kế hoạch để thực hiện các phương pháp hay nhất, bạn cần tạo một kế hoạch dự án giúp bạn quản lý nhiệm vụ của mình, xác định xác bên chịu trách

nhiệm, xác định quy tắc, đặt cột mốc quan trọng của bạn để xác định các tài nguyên mà bạn cần để thiết kế và triển khai mạng. Bạn cũng có thể làm theo kế hoạch dự án này cho các giai đoạn còn lại của vòng đời mạng

3. Design

   Giống như các giai đoạn trước, giai đoạn thiết kế dựa trên yêu cầu của bất kỳ doanh ngiệp nào vì nó song song với các yêu cầu kỹ thuật, nó bao gồm tính khả dụng cao và đảm bảo phần mềm và phần cứng. Nó cũng tập trung vào tính sẵn sàng cao của các giao thức định tuyến, độ tin cậy, khả năng mở rộng và bảo mật

   Trong giai đoạn thiết kế, chúng tôi tạo các danh sách, sơ đồ báo cáo khác nhau theo kế hoạch dự án và sau khi hoàn thành những việc trên, cập nhật kế hoạch dự án với các sửa đổi giai đoạn thiết kế, có thể đơn giản hóa bằng các bước:

   1. Xác định các yêu cầu mạng

   - Bắt đầu với việc xác định các ứng dụng va dịch vụ yêu cầu và cũng xem xét các ứng dụng hiện tại. Cũng chuẩn bị tầm quan trọng và tính quan trong của các ứng dụng khác cho một tổ chức, ví dụ trong một email tổ chức được coi là một hệ thống quan trọng so với việc gây rối ngay lập tức, cả hai đều có tầm quan trọng và mức độ quan trọng khác nhau
   - Xem xét lưu lượng dữ liệu và tìm cách có thể ánh xạ các phân tích này với các mục tiêu của tổ chức
   - Tìm ra tất cả các ràng buộc có thể đạt được các mục tiêu của tổ chức, ví dụ như hạn chế chính sách như HIPPA hoặc chính sách tổ chức, các hạn chế về chính sách bảo mật chẳng hạn như không cho phép các ứng dụng và dịch vụ phù hợp như EIGRP. Bạn cũng có thể có những hạn chế như chỉ sử dụng các giải pháp Linux/ Unix, chỉ sử dụng các giao thức tiêu chuẩn mở như OSPF, RIP và IS - IS. Ngoài ra, có thể có tài nguyên hạn chế như nhóm nhỏ hơn để xây dựng mạng
   - Xác định cho bạn các mục tiêu kỹ thuật thông thường các mục tiêu này có liên quan đến việc xác định các mục tiêu phần cứng và phần mềm để đạt được các mục tiêu của tổ chức
   - Xác định các hạn chế có thể có đối với các mục tiêu kỹ thuật

   2. Đặc trưng cho mạng hiện có

      Ở đây xác định các tính năng và đặc điểm chính của mạng, cũng chọn các công cụ để giám sát và quản lý. Đặc trưng của mạng hiện có là một quá

trình thu thập thông tin

- Biên dịch tất cả các thông tin và tài liệu hiện có
- Tiến hành kiểm tra mạng, nó cũng bao gồm tốc độ dữ liệu, phiên bản IOS và bản cập nhật Windows
- Chuẩn bị phân tích lưu lượng như băng thông, thời gian phản hồi mạng, cơ chế QoS, VLAN riêng cho VOIP và dữ liệu, thực hiện phân tích lưu lượng

3. Thiết kế cấu trúc liên kết mạng và giải pháp

- Đối với việc thiết kế cấu trúc liên kết mạng, cách tiếp cận tốt nhất mà Cisco đề xuất là cách tiếp cận từ trên xuống, điều đó có nghĩa là bắt đầu từ lớp 7 của mô hình OSI sang lớp 1
    - Không chọn bất kỳ giải pháp hoặc công cụ nào trước khi hoàn thiện các yêu cầu ứng dụng
    - Kết hợp SONA vào các phương pháp thiết kế cùng với các yêu cầu của tổ chức
- CCDA là tất cả về thiết kế mạng và chủ yêu tập trung vào giai đoạn chuẩn bị, lập kế hoạch và thiết kế, bạn có thể xem xét các mô hình và phương pháp thiết kế khác nhau từ khóa học CCDA

4. **Giai đoạn thực hiện**

- Giai đoạn thực hiện có liên quan đến cấu hình và hoạt động, ở đây cần xác định tất cả cấu hình của thiết bị của mình và cũng xác định thời gian liên quan đến các cấu hình này.
- Trong giai đoạn thực hiện này nếu muốn thay đổi bất cứ điều gì thì cần phải thông báo nó cho tát cả các thành viên trong nhóm và cũng thực hiện các sửa đổi thích hợp trong Giai đoạn kế hoạch và thiết kế cho phù hợp, cũng xác định các hướng dẫn thích hợp và cung cấp RFC nếu được yêu cầu. Và bất kỳ thay đổi nào thực hiện trong giai đoạn thực hiện này phải được kiểm tra trước khi chuyển sang giai đoạn tiếp theo

5. **Giai đoạn hoạt động:**

- Trong giai đoạn vận hành, cần đề cập đến các hoạt động hằng ngày của cơ sở hạ tâng mạng của mình, đây sẽ là quản lý các thành phần giám sát, tạo báo cáo, bảo trì định kỳ, nâng cấp hệ điều hành, IOS của bộ định tuyến .
- Giai đoạn hoạt động là thử nghiệm thực tế về thiết kế của mạng của bạn, bạn cần xác định lỗi trên liên quan đến mạng. Giám sát hoạt động của các thiết bị và

thiết bị mạng khác nhau

6. **Tối ưu hóa giai đoạn:**

- Giai đoạn tối ưu hóa là một quản lý mạng chủ động, bạn có thể xác định và giải quyết vấn đề trước khi họ chuyển sang toàn bộ cơ sở mạng của thiết kế tốt của bạn. Trong giai đoạn tối ưu hóa, bạn có thể sửa đổi thiết kế mạng nếu sự cố sắp xảy ra. Để giải quyết vấn đề, bạn có thể quay lại các giai đoạn trước của mình, chẳng hạn như giai đoạn chuẩn bị và lập kế hoạch, thực hiện các thay đổi ở đó và sau đó kiểm tra lại các thay đổi trong giai đoạn vận hành hoặc tối ưu hóa

Defensible Network Architecture

Phòng thủ theo chiều sâu đề cập đến một chiến lược an ninh mạng trong đó có nhiều sản phẩm và phương pháp được sử dụng để bảo vệ mạng

Phòng thủ theo chiều sâu (DID) là một chiến lược an ninh mạng sử dụng nhiều sản phẩm và phương pháp bảo mật để bảo vệ mạng, thuộc tính web và tài nguyên của một tổ chức. Nó đôi khi được sử dụng thay thế cho nhau với thuật ngữ ‘bảo mật nhiều lớp’ vì nó phụ thuộc vào các giải pháp bảo mật ở nhiều lớp kiểm soát - vật lý, kỹ thuật và quản trị - để ngăn những kẻ tấn công tiếp cận mạng được bảo vệ hoặc tài nguyên tại chỗ

Ban đầu, phòng thủ chuyên sâu mô tả một số chiến lược quân sự trong đó một tuyến phòng thủ bị hy sinh để ngăn chặn các lực lượng đối lập. Mặc dù có tên tương tự, nhưng cách tiếp cận đó không song song với chiến lược bảo mật này, trong đó nhiều sản phẩm hoạt động cùng nhau để ngăn chặn những kẻ tấn công và các mối đe dọa khác

Tại sao phòng thủ theo chiều sâu là cần thiết?

Nguyên tắc chỉ đạo của chiến lược phòng thủ theo chiều sâu là ý tưởng rằng một sản phẩm bảo mật đơn lẻ không thể bảo vệ hoàn toàn mạng khỏi mọi cuộc tấn công mà nó có thể phải đối mặt. Tuy nhiên, việc triển khai nhiều sản phẩm và phương pháp bảo mật có thể giúp phát hiện và ngăn chặn các cuộc tấn công khi chúng phát sinh, cho phép các tổ chức giảm thiểu hiệu quả một loạt các mối đe dọa. Cách tiếp cận này ngày càng trở nên quan trọng khi các tổ chức mở rộng mạng lưới, hệ thống và người dùng của họ

Một ưu điểm khác của bảo mật phân lớp là dự phòng. Nếu kẻ tấn công bên ngoài hạ gục một tuyến phòng thủ hoặc một mối đe dọa nội gián xâm phạm một phần mạng của tổ chức, các biện pháp bảo mật khác có thể giúp hạn chế và giảm thiểu thiệt hại cho toàn bộ mạng. Ngược lại. chỉ sử dụng một sản phẩm bảo mật sẽ tạo ra một

điểm lỗi duy nhất; nếu nó bị xâm phạm, toàn bộ mạng hoặc hệ thống có thể bị vi phạm hoặc hỏng

Những sản phẩm an ninh nào được sử dụng chuyên sâu trong phòng thủ chiều sâu?

Mặc dù các chiên lược phòng thủ theo chiều sâu khác nhau tùy theo nhu cầu của tổ chức và các nguồn lực sẵn có, nhưng chúng thường bao gồm một hoặc nhiều sản phẩm trong các danh mục sau:

- **Các biện pháp kiểm soát an ninh vật lý bảo vệ hệ thống CNTT:** Tòa nhà công ty, trung tâm dữ liệu và các tài sản vật lý khác chống lại các mối đe dọa như giả mạo, trộm cắp hoặc truy cập trái phép. Chúng có thể bao gồm các loại phương pháp giảm sát và kiểm soát truy cập khác nhau , chẳng hạn như camera an ninh, hệ thống báo động, máy quét thẻ ID và bảo mật sinh trắc học (VD: đầu đọc dấu vân tay, hệ thống nhận dạng khuôn mặt ,….)
- **Các biện pháp kiểm soát bảo mật kỹ thuật** bao gồm phần cứng và mềm cần thiết để ngăn chặn vi phạm dữ liệu, các cuộc tấn công DDOS và các mối đe dọa khác nhắm vào các mạng và ứng dụng. Các sản phẩm bảo mật phổ biến ở lớp này bao gồm tường lửa, cổng web an toàn (SWG), hệ thống phát hiện hoặc ngăn chặn xâm nhập (IDS/ IPS), công nghệ cách ly trình duyệt, phần mềm phát hiện và phản hồi điểm cuối (EDR), phần mềm ngăn chặn mất dữ liệu (DLP), tường lửa ứng dụng web (WAF) và phần mềm chống phần mềm độc hại ,…
- **Kiểm soát an ninh quản trị đ**ề cập đến các chính sách do quản trị viên hệ thống và nhóm bảo mật đặt ra nhằm kiểm soát quyền truy cập vào hệ thống nội bộ, tài nguyên của công ty cũng như dữ liệu và ứng dụng nhạy cảm khác. Nó cũng có thể bao gồm đào tạo nhận thức về bảo mật để đảm bảo rằng người dùng thực hành vệ sinh an ninh tốt, giữ bí mật dữ liệu và tránh để hệ thống, thiết bị và ứng dụng gặp rủi ro không cần thiết

Những thông lệ an ninh nào được sử dụng trong phòng thủ theo chiều sâu?

Ngoài các sản phẩm và chính sách bảo mật, các tổ chức cần thực hiện các biện pháp bảo mật mạnh mẽ để hạn ché rủi ro đối với mạng và tài nguyên của họ. Chúng có thể bao gồm một hoặc nhiều điều sau:

- **Quyền truy cập ít đặc quyền** là nguyên tắc cấp cho người dùng quyền chỉ truy cập vào các hệ thống và tài nguyên mà họ cần cho vai trò của mình. Điều này giúp giảm thiểu rủi ro cho phần còn lại của mạng nếu thông tin đăng nhập của người dùng bị xâm phạm và người dùng trái phép cố gắng thực hiện một cuộc tấn công hoặc truy cập vào dữ liệu nhạy cảm

- **Xác thực đa yếu tố (MFA)** như tên gọi của nó, yêu cầu nhiều hình thức xác thực để xác minh danh tính của người dùng hoặc thiết bị trước khi cho phép truy cập vào mạng hoặc ứng dụng. Xác thực đa yếu tố thường bao gồm thực hành mật khẩu mạnh mẽ (mật khẩu phức tạp, khó đoán và thường xuyên thay đổi) thiết lập các biện pháp kiểm soát chặt chẽ cho các thiết bị và xác minh danh tính thông qua các thiết bị và công cụ bên ngoài

  (Nhập mã xác minh từ thiết bị di động ,….)

  Mã hóa bảo vệ dữ liệu nhạy cảm khỏi bị tiếp xúc với các bên trái phép hoặc độc hại. Thông tin được giấu bằng cách chuyển đổi văn bản thô sang bản mã

- **Việc phân đoạn mạng** giúp hạn chế sự tiếp xúc của các hệ thống và dữ liêu nội bộ với các nhà cung cấp, nhà thầu và những người dùng bên ngoài khác.

  VD thiết lập mạng không dây riêng biệt cho người dùng nội bộ so với mạng bên ngoài cho phép các tổ chức bảo vệ tốt hơn thông tin nhạy cảm khỏi các bên trái phép. Việc phân đoạn mạng cũng có thể giúp các nhóm bảo mật ngăn chặn các mối đe dọa nội gián, hạn chế sự lây lan của phần mềm độc hại và tuân thủ các quy định về dữ liệu.

- **Phân tích hành vi** có thể giúp phát hiện các mô hình lưu lượng truy cập bất thường và các cuộc tấn công khi chúng xảy ra. Nó thực hiện điều này bằng cách so sánh hành vi của người dùng với đường cơ sở của hành vi bình thường đã được quan sát trong quá khứ. Bất kỳ sự bất thường nào có thể kích hoạt hệ thống bảo mật chuyển hướng lưu lượng độc hại và ngăn chặn các cuộc tấn công được thực hiện.

- **Bảo mật Zero Trust** là một triết lý bảo mật bao gồm nhiều khái niệm ở trên, với giả định rằng các mối đe dọa đã hiện diện bên trong một mạng và không có người dùng, thiết bị hoặc kết nối nào được tin cậy theo mặc định.

  Đây chỉ là một vài trong số các phương pháp nên được sử dụng trong cách tiếp cận bảo mật phân lớp. Khi các kiểu tấn công tiếp tục phát triển để khai thác các lỗ hổng trong các sản phẩm bảo mật hiện có, các sản phẩm và chiến lược mới phải được phát triển để lật đổ chúng.

Bảo mật phân lớp khác với bảo mật tích hợp như thế nào?

Một chiến lược phòng thủ có chiều sâu hiệu quả không chỉ đòi hỏi các biện pháp kiểm soát an ninh theo lớp mà còn cả các phương pháp bảo mật tích hợp. Mặc dù những thuật ngữ này nghe có vẻ giống nhau, nhưng chúng mang những ý nghĩa hơi khác nhau:

- **Bảo mật phân lớp**, như được mô tả ở trên, đề cập đến việc sử dụng nhiều sản phẩm và phương pháp bảo mật để bảo vệ tổ chức trước một loạt các mối đe dọa vật lý và mạng.
- **Bảo mật tích hợp** đảm bảo rằng nhiều sản phẩm bảo mật hoạt động với nhau để cải thiện khả năng phát hiện và giảm thiểu các mối đe dọa. Một chiến lược bảo mật có thể được phân lớp, nhưng không được tích hợp, trong khi chiến lược bảo mật tích hợp được phân lớp theo bản chất.

Hãy nghĩ về bảo mật nhiều lớp như một bộ áo giáp được lấy từ nhiều người bán. Một số mảnh áo giáp có thể mới hơn hoặc chất lượng cao hơn những mảnh khác; mặc dù người mặc được bảo vệ khỏi nhiều loại tác hại vật lý, nhưng có thể có khoảng trống giữa các mảnh áo giáp khác nhau hoặc những điểm yếu nơi người mặc dễ bị tấn công hơn.

Ngược lại, bảo mật tích hợp giống như một bộ áo giáp tùy chỉnh. Nó có thể bao gồm các phần khác nhau (kiểm soát an ninh), nhưng chúng vốn được thiết kế để phối hợp với nhau nhằm bảo vệ người mặc – không để lại khoảng trống hoặc điểm yếu.

Tuy nhiên, khi định cấu hình các giải pháp an ninh mạng, việc mua nhiều sản phẩm bảo mật từ một nhà cung cấp không phải lúc nào cũng đảm bảo rằng một tổ chức đang nhận được những lợi ích của phương pháp tích hợp. Để biết thêm về chủ đề này, hãy xem “Tương lai của bảo mật ứng dụng web”.

Security Controls

Kiểm soát bảo mật là thực hiện để bảo vệ các dạng dữ liệu và cơ sở hạ tầng khác nhau quan trọng đối với một tổ chức. Bất kỳ loại biện pháp bảo vệ hoặc biện pháp đối phó nào được sử dụng để tránh, phát hiện, chống lại hoặc giảm thiểu rủi ro bảo mật đối với tài sản vật lý, thông tin, hệ thống máy tính hoặc các tài sản khác đều được coi là kiểm soát an ninh.

Các loại kiểm soát bảo mật

Có một số loại kiểm soát bảo mật có thể được triển khai để bảo vệ phần cứng, phần mềm, mạng và dữ liệu khỏi các hành động và sự kiện có thể gây mất mát hoặc hư hỏng. Chẳng hạn:

- Kiểm soát an ninh vật lý bao gồm những thứ như hàng rào chu vi trung tâm dữ liệu, khóa, bảo vệ, thẻ kiểm soát truy cập, hệ thống kiểm soát truy cập sinh trắc học, camera giám sát và cảm biến phát hiện xâm nhập.
- Kiểm soát bảo mật kỹ thuật số bao gồm những thứ như tên người dùng và mật khẩu, xác thực hai yếu tố, phần mềm chống vi-rút và tường lửa.

- Kiểm soát an ninh mạng bao gồm bất kỳ thứ gì được thiết kế đặc biệt để ngăn chặn các cuộc tấn công vào dữ liệu, bao gồm giảm thiểu DDoS và hệ thống ngăn chặn xâm nhập.
- Kiểm soát bảo mật đám mây bao gồm các biện pháp bạn thực hiện khi hợp tác với nhà cung cấp dịch vụ đám mây để đảm bảo bảo vệ cần thiết cho dữ liệu và khối lượng công việc. Nếu tổ chức của bạn chạy khối lượng công việc trên đám mây, bạn phải đáp ứng các yêu cầu về bảo mật của công ty hoặc chính sách kinh doanh và các quy định của ngành.