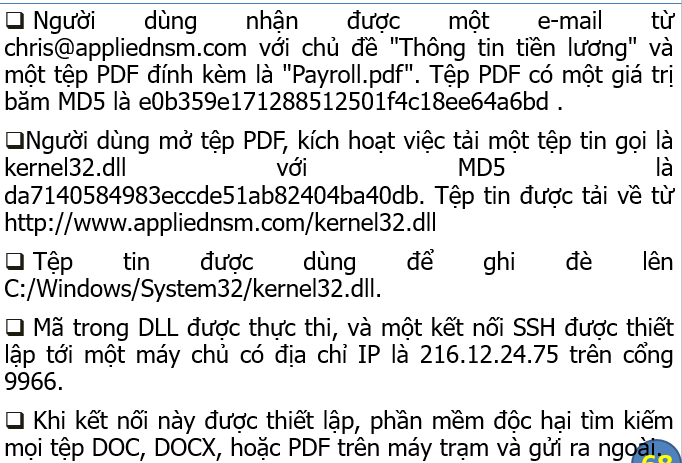
1. **Bài tập về tính toán dấu hiệu xâm nhập IOC. Tài liệu tham khảo [1] – Chương 2.1; [2]- Chương 7**



1. Người dùng đã nhận được một thư điện tử từ địa chỉ **chris@appliednsm.com** với tiêu đề "Thông tin tiền lương" và tập tin PDF đính kèm được đặt tên là "**Payroll.pdf**". Tập tin PDF này có giá trị băm MD5 là **e0b359e171288512501f4c18ee64a6bd**.
2. Người dùng đã mở tập tin PDF, gây ra việc tải xuống tập tin có tên kernel32.dll có giá trị băm MD5 là **da7140584983eccde51ab82404ba40db**. Tập tin được tải xuống từ địa chỉ **http://www.appliednsm.com/kernel32.dll**.
3. Tập tin được sử dụng để ghi đè lên **C:/Windows/System32/kernel32.dll**.
4. Mã trong tập tin DLL đã được thực thi và một kết nối SSH được thiết lập tới một máy chủ có địa chỉ IP là **216.12.24.75** trên cổng **9966**.
5. Khi kết nối được thiết lập, phần malware sẽ tìm kiếm mọi tập tin DOC, DOCX hoặc PDF trên máy trạm và gửi ra ngoài

IOC (B-1) (hành vi): người dùng nhận email có đính kèm tập tin

Giá trị:

* IOC(A-1): chris@appliednsm.com
* IOC(A-2): Thông tin tiền lương
* IOC(A-3): Payroll.pdf
* IOC(C-1): e0b359e171288512501f4c18ee64a6bd (C: được tính toán…)

IOC(B-2): Tập tin nghi ngờ được tải về từ website

Giá trị:

* IOC(A-4): Kernel32.dll
* IOC(C-2): da7140584983eccde51ab82404ba40db
* IOC(A-5): http://www.appliednsm.com/kernel32.dll

IOC(B-3): tập tin được dùng để ghi đè

Giá trị:

* IOC(A-6): tên file: kernel32 (đây là tập tin hệ thống, sẽ bị ghi đè bởi tập tin độc hại)

IOC(B-4): thực thi và kết nối có mã hóa

Giá trị:

* IOC(A-7): SSH
* IOC(A-8): 216.12.24.75
* IOC(A-9): port 9966

IOC(B-5): dữ liệu được gửi ra ngoài

* IOC(A-10): DOC,DOCX,PDF
* Các IOC được sử dụng cho hệ thống (phát hiện xâm nhập) (IDS, IPS, SIEM, Anti virus…)

Cần phải coi IOC là các biến. trong đó có những dấu hiệu chưa biết giá trị => để tổng quát hóa cuộc tấn công

1. **Bài tập về lập kế hoạch thu thập dữ liệu. [1]-Chương 2.2; [3]-Chương 2;**

Lựa chọn dữ liệu thu thập dựa vào khungACF (Applied Collection Framework)

* Giúp hệ thống chọn lọc dữ liệu thu thập, phân tích, lưu trữ

1. Xác định nguy cơ (Các mối đe dọa gây mất ATTT HT) dựa vào tài sản hệ thống: PC, server, firewall, switch, router, users…

**Bước 1**: Liệt kê tài sản hệ thống

* Đối với thuộc tính bí mật thì giá trị được xác định vào loại thông tin hoặc  
  loại thông tin hệ thống đó xử lý. Ví dụ: thông tin công khai thang điểm 1; thông tin riêng, thông tin cá nhân thang điểm 2; thông tin Mật thang điểm 3; thông tin Tối Mật thang điểm 4; thông tin Tuyệt Mật thang điểm 5.
* Đối với thuộc tính nguyên vẹn thì giá trị được xác định vào yêu cầu đối  
  với mức độ nguyên vẹn của thông tin hoặc loại thông tin mà hệ thống đó xử lý.  
  Ví dụ: tính nguyên vẹn thấp thang điểm 1; tính nguyên vẹn trung bình thang điểm 2; tính nguyên vẹn cao thang điểm 3; tính nguyên vẹn rất cao điểm 4; tính nguyên vẹn tuyệt đối thang điểm 5.
* Đối với thuộc tính sẵn sàng thì giá trị được xác định vào yêu cầu đối với  
  mức sẵn sàng của thông tin hoặc hệ thống thông tin đó. Ví dụ: tính sẵn sàng thấp thang điểm 1; tính tính sẵn sàng trung bình thang điểm 2; tính tính sẵn sàng cao thang điểm 3; tính tính sẵn sàng rất cao điểm 4; tính tính sẵn sàng tuyệt đối thang điểm 5.

Xác định tầm quan trọng của tài sản đó:

Gồm 5 mức: (1) thấp, (2) trung bình, (3) cao, (4) rất cao, (5) cực cao

Ví dụ: PC (2), server(3), switch(1)

**Bước 2**: Đánh giá nguy cơ

**Bước 3**: Xác định mức độ ảnh hưởng gồm 5 mức: (1) Không đáng kể, (2) nhỏ, (3) vừa phải, (4) nghiêm trọng, (5) đặc biệt nghiêm trọng

**Bước 4**: Xác định khả năng xảy ra (xác suất) gồm 5 mức: (1) ít khi, (2) thấp, (3) trung bình, (4) cao, (5) chắc chắn

**Bước 5**: Định lượng rủi ro = giá trị tài sản + mức độ ảnh hưởng + khả năng xảy ra

Gồm 5 mức: (1) thấp: 1-3, (2) trung bình: 4-6, (3) cao: 7-9, (4) rất cao: 10-12, (5) cực cao: 13-15

Ví dụ: R(server) = 3 (giá trị tài sản) + 4(mức độ ảnh hưởng) + 4(khả năng xảy ra) = 11(định lượng rủi ro) : rất cao

* Khả năng mất ATTT do server web rất cao
* Cần thu thập dữ liệu trên web server để giám sát

**\**Bài tập: Áp dụng ACF xác định dữ liệu thu thập cho hệ thống bán lẻ trực tuyến***

* Bước 1: Liệt kê tài sản hệ thống và xác định tầm quan trọng của từng tài sản đó:

PC: (2) trung bình

Server: (4) rất cao

Firewall: (3) cao

Switch: (2) trung bình

Router: (3) cao

Users: (4) rất cao

* Bước 2: Đánh giá nguy cơ:

PC: Nguy cơ vừa phải

Server: Nguy cơ rất cao

Firewall: Nguy cơ vừa phải

Switch: Nguy cơ không đáng kể

Router: Nguy cơ vừa phải

Users: Nguy cơ rất cao

* Bước 3: Xác định mức độ ảnh hưởng:

PC: Mức độ ảnh hưởng nhỏ

Server: Mức độ ảnh hưởng đặc biệt nghiêm trọng

Firewall: Mức độ ảnh hưởng vừa phải

Switch: Mức độ ảnh hưởng không đáng kể

Router: Mức độ ảnh hưởng nghiêm trọng

Users: Mức độ ảnh hưởng rất cao

* Bước 4: Xác định khả năng xảy ra:

PC: Khả năng xảy ra trung bình

Server: Khả năng xảy ra chắc chắn

Firewall: Khả năng xảy ra vừa phải

Switch: Khả năng xảy ra ít khi

Router: Khả năng xảy ra cao

Users: Khả năng xảy ra cao

* Bước 5: Định lượng rủi ro:
* PC: 2 (giá trị tài sản) + 2 (mức độ ảnh hưởng) + 3 (khả năng xảy ra) = 7 (định lượng rủi ro) : cao
* Server: 4 (giá trị tài sản) + 5 (mức độ ảnh hưởng) + 5 (khả năng xảy ra) = 14 (định lượng rủi ro) : cực cao
* Firewall: 3 (giá trị tài sản) + 3 (mức độ ảnh hưởng) + 3 (khả năng xảy ra) = 9 (định lượng rủi ro) : rất cao
* Switch: 2 (giá trị tài sản) + 1 (mức độ ảnh hưởng) + 1 (khả năng xảy ra) = 4 (định lượng rủi ro): trung bình
* Router: 5 + 5 + 4 = 14 (rủi ro cực cao)
* Users: 3 + 3 + 4 = 10 (rủi ro rất cao)

Từ kết quả trên, ta có thể thấy rằng các tài sản hệ thống như server, router có mức độ rủi ro cực cao, cần được giám sát chặt chẽ. Còn các tài sản như PC, switch, firewall và users có mức độ rủi ro khác nhau, nhưng đều cần được giám sát để phòng tránh các mối đe dọa đối với hệ thống bán lẻ trực tuyến. Do đó, ta cần thu thập dữ liệu liên quan đến các tài sản này để đưa ra các biện pháp bảo mật phù hợp.

1. **Bài tập về phân tích dữ liệu. [1]-Chương 2.2;**

2 phương pháp chính: **Điều tra quan hệ** và **tiến hành chuẩn đoán**

**\*Điều tra quan hệ:**

**Bước 1:**

Điều tra các đối tượng chính và Thực hiện điều tra sơ bộ về cảnh báo

* Xác định đối tượng (máy chủ, máy tính…)
* Xác định cảnh báo là thật hay giả, nếu các cảnh báo là thật thì thu thập tiếp các thông tin như IP, domain, tài nguyên tin cậy và nguy hiểm

**Bước 2:**

Điều tra các mối quan hệ chính và tương tác hiện tại

* Điều tra mối quan hệ trước đố cũng như hiện tại của máy tính tấn công và máy tính cần bảo vệ như 2 máy đã từng liên lạc, nếu có thì cổng, giao thức và dịch vụ nòa?
* Điều tra kỹ lưỡng các kết nối bằng cách thu thập dữ liệu PCAP, thực hiện phân tích gói, trích xuất các tập tin để phân tích phần mềm độ hại, tọa thống kê dữ liệu phiên…

**Bước 3:**

Điều tra các đối tượng thứ cấp và mối quan hệ

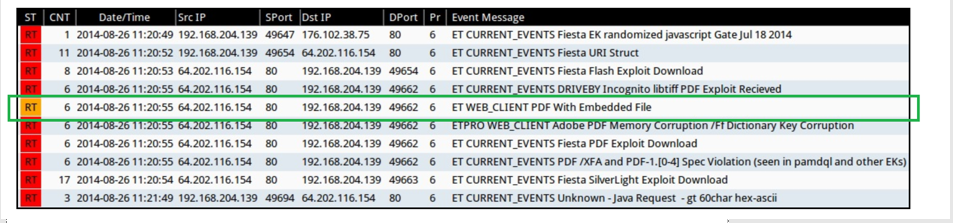
* Xác định các đối tượng thứ cấp
* Xác định mối quan hệ giữa các đối tượng thứ cấp và đối tượng chính

**Bước 4 (lặp lại):**

Điều tra bổ sung mối quan hệ của các đối tượng ở các mức độ khác

* Việc điều tra các đối tượng và các mối quan hệ nên được lặp lại nhiều lần khi cần thiết có thể đòi hỏi thêm các đối tượng mức 3, mức 4
* Nên đánh giá các đối tượng và các mối quan hệ một các đầy đủ trên cơ sở mỗi cấp độ trước khi chuyển sang mức kế tiếp để tránh mất các thông tin quan trọng

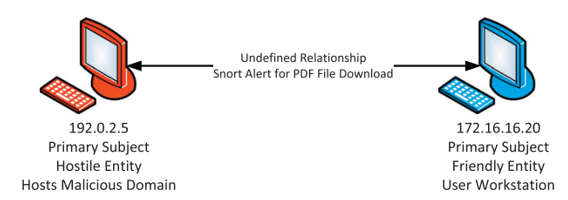
***\*Ví dụ:***



***\*Bài làm:***

**Bước 1:** Điều tra các đối tượng chính và thực hiện điều tra sơ bộ cho thấy:

* IP Attachker: 192.0.2.5
* IP Victim: 172.16.16.20
* PDF được tải về, giá trị MD5 của PDF được 23% engine phát hiện virus cho rằng là mã độc
* Điều tra tiếp



Friendly Intelligence for 172.16.16.20

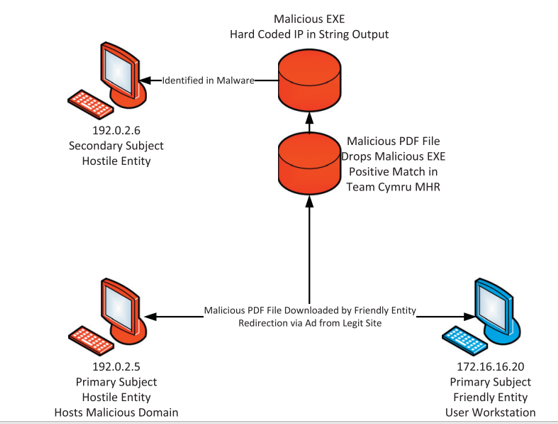
* Máy trạm của người dùng đang chạy Win 7
* Hệ thống không mở các dịch vụ nào cả
* Người dùng hệ thống này thường lướt web

Hostile Intelligence for 192.0.2.5

* Kiểm tra IP Blacklist với <http://www.ipvoid.com/> trả về 0 kết quả
* Kiểm tra IP Blacklist với <http://www.urlvoid.com/> trả về 5 kết quả cho tên miền nơi các tập tin PDF được tải về
* 192.0.2.5 không liên lạc với máy nào khác trong hệ thống mạng victim

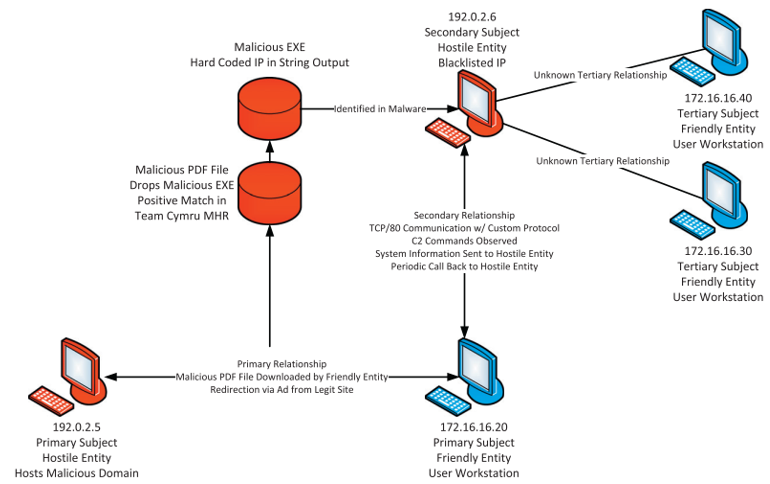
**Bước 2:**

* Tải và phân tích các gói tin trong khoảng thời gian có cảnh báo (10p trước và 10p sau cảnh báo)
* Thực hiện phân tích và xác định được:
* Victim đã chuyển hướng tới máy tính độc hại từ 1 quảng cáo của bên thứ 3 trên một trang web hợp pháp
* Victim tải tệp tin về và ngừng kết nối tới máy chủ lưu trữ 192.0.2.5
* Tải tệp tin lên Cuckoo sandbox để thực hiện phân tích mã độc tự động chỉ ra PDF có chứa mã thực thi và tệp thực thi có chứa địa chỉ IP 192.0.2.6, ngoài ra không còn thông tin nào khác



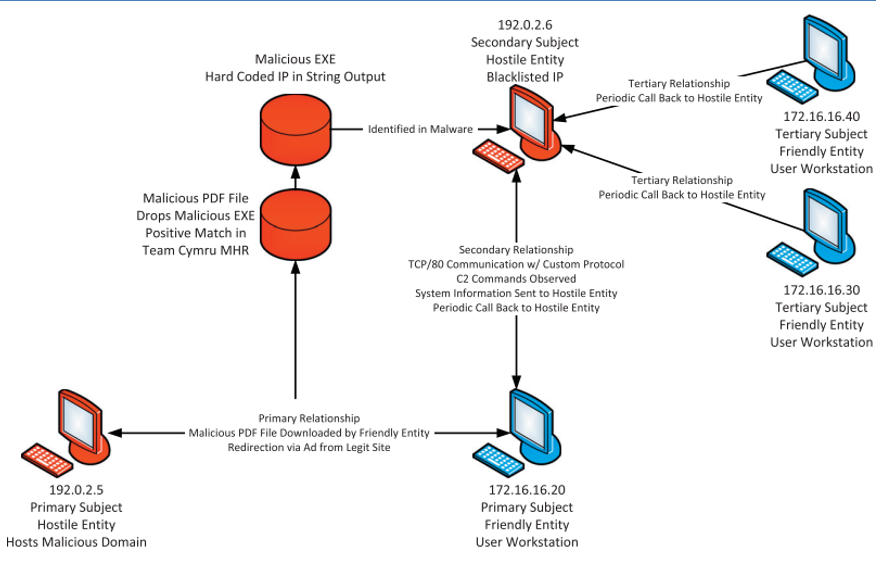
**Bước 3:**

* Xác định được đối tượng thứ cấp có IP 192.0.2.6
* Hostile Intelligence for 192.0.2.6:
* <http://www.ipvoid.com/> trả về 2 kết quả
* Dữ liệu NetFlow cho thấy victim (172.16.16.20) đã liên lạc với máy tính này sau 30p kể từ cảnh báo bao đầu
* Dữ liệu NetFlow chỉ ra 2 máy tính trong hệ thống mạng của victim cũng giao tiếp với IP này thoe định kỳ với lưu lượng thấp với IP lần lượt: 172.16.16.30 và 172.16.16.40
* Các máy giao tiếp qua cổng 80 bằng một giao thức sửa đổi cho phép gửi thông tin từ victim về máy chủ độc hại
* Trong một số trường hợp việc điều tra có thể kết thức ở đây với thông báo sự cố là 172.16.16.20 đã bị tấn công và 2 máy khác trong hệ thống cũng ó thể bị đã bị tấn công trước đó



**Bước 4:**

* Trong một số trường hợp, việc điều tra có thể kết thúc ở đây với thông báo sự cố là 172.16.16.20 đã bị tấn công và 2 máy khác trong hệ thống cũng có thể bị đã bị tấn công trước đó
* Thực hiện kiểm tra các gói dữ liệu truyền giữa các máy tính mức 3 (172.16.16.30 và 172.16.16.40) chp thấy nó cũng tham gia và hành vi callback tới máy chủ độc hại
* Xác định được các máy tính được bảo vệ ở mức 3 cũng bị tổn hại



**\*Chuẩn đoán khác biệt:**

**Bước 1: Xác định và liệt kê các dấu hiệu**

**Bước 2: xem xét và đnáh giá chuẩn đoán phổ biến nhất đầu tiền**

**Bước 3: Liệt kê tất cả chuẩn đoán có thể cho các dấu hiệu đã biết**

**Bước 4: Đánh giá mức ưu tiên trong danh sách ứng viên theo mức độ nghiêm trọng**

**Bước 5: Loại bỏ các điều kiện ứng viên và bắt đầu với cái nghiêm trọng nhất**

***Ví dụ:***

**Bước 1: Xác định và liệt kê các dấu hiệu**

Các dấu hiệu sau đây được quan sát qua cảnh báo IDS và điều điều tra các dữ liệu đã có:

1.Một máy chủ tin cậy bắt đầu gửi lưu lượng đến một địa chỉ IP ở Nga

2. Dữ liệu được gửi đều đặn sau mỗi 10 phút

3. Giao thức HTTPS được sử dụng để truyền tải dữ liệu

**Bước 2: xem xét và đánh giá chuẩn đoán phổ biến nhất đầu tiền**

Các dấu hiệu sau đây được quan sát qua cảnh báo IDS và điều điều tra các dữ liệu đã có:

1.Một máy chủ tin cậy bắt đầu gửi lưu lượng đến một địa chỉ IP ở Nga

2. Dữ liệu được gửi đều đặn sau mỗi 10 phút

3. Giao thức HTTPS được sử dụng để truyền tải dữ liệu

**Bước 3: Liệt kê tất cả chuẩn đoán có thể cho các dấu hiệu đã biết**

* Truyền thông bình thường
* Nhiễm mã độc
* Dữ liệu bị rò rỉ từ máy tính bị tấn công
* Cấu hình sai

**Bước 4: Sắp xếp danh sách ưu tiên theo mức độ nghiêm trọng**

* Ưu tiên 1: số liệu rò rỉ từ máy tính bị tấn công (cao nhất)
* Ưu tiên 2: nhiễm mã độc
* Ưu tiên 3: cấu hình sai
* Ưu tiên 4: liên lạc bình thường

**Bước 5: Loại bỏ dần các phán đoán**

* Ưu tiên 1: dữ liệu rò rỉ từ máy tính bị tấn công
* Ưu tiên 2: nhiễm mã độc
* Ưu tiên 3: cấu hình sai
* Ưu tiên 4: truyền thông bình thường

1. **Bài tập về ứng phó sự cố ATTT. [1]-Chương 3,4; [4], [5]**

**\*Xử lý sự cố bị tấn công từ chối dịch vụ:**

**Bước 1**:

Tiếp nhận sự cố

* Lưu lượng mạng chậm, chập chờn
* Không truy cập được dịch vụ
* Cảnh báo tấn công từ IDS, SIEM

Ứng phó ban đầu:

* Tạm dừng các dịch vụ
* Chuyển hướng dịch vụ

**Bước 2**: Phân tích điều tra, tìm kiếm nguyên nhân

* Xác định loại hình tấn công: Dos hay DDoS or DRDos
* Xác định giao thức: ICMP or TCP or UDP
* Xác định nguồn và đich:IP nguồn, IP đích
* Xác định thời gian
* Xác định tần suất

**Bước 3**: Xử lý, khôi phục sự cố:

* Sử dụng Firewall lọc lưu lượng, chặn nguồn
* Sử dụng router biên: Acess control List (ACL)
* Kết hợp IPS (Viettel, VNPT, FPT, …) lọc nguồn
* Kết hợp với tổ chức cơ quan chức năng (Ví dụ: VN Cert)
* Khôi phục dịch vụ

**Bước 4**: Tổng kết, đánh giá, đưa ra bài học

* Đánh giá
* Nguyên nhân
* Đề xuất giải pháp phòng thủ
* Time out, webserver
* Nâng cấp băng thông
* Load Balancing

**\*Người dùng không truy cập được tài nguyên**

**Bước 1**: Tiếp nhận sự cố: kiểm tra sự cố, ứng cứu ban đầu

**Bước 2**: xác định nguyên nhân dẫn tới người dùng không truy cập được tài nguyên

* Máy chủ bị tấn công DoS
* Dữ liệu bị phá hủy
* Cấu hình sai
* Mất kết nối mạng
* Tài khoản bị hạn chế
* Không có quyền truy cập tài nguyên
* Dữ liệu bị mã hóa
* Mất điện, thảm họa thiên tai

**Bước 3**: xử lý ứng cứu sự cố

* Tùy trường hợp để xử lý sự cố
* Khôi phục tài nguyên

**Bước 4**: đánh giá

Đánh giá nguyên nhân xảy ra sự cố, bài học kinh nghiệm giải pháp phòng chống

**Bài 1: Người dùng không truy cập được tài nguyên mạng**

B1: Tiếp nhận sự cố:

Lỗi "Không kết nối được với máy chủ" hoặc "Không tìm thấy trang web" khi truy cập các trang web hoặc ứng dụng.

Thời gian trả lời của các yêu cầu truy cập tăng cao, hoặc các yêu cầu truy cập bị treo hoặc thất bại.

Không thể kết nối với các thiết bị mạng khác như máy chủ hoặc máy tính khác trong mạng nội bộ.

Các thông báo lỗi xuất hiện khi cố gắng kết nối với các tài nguyên mạng như máy chủ, máy tính hoặc ổ đĩa mạng.

Ứng cứu ban đầu:

Kiểm tra kết nối mạng: Kiểm tra kết nối mạng của người dùng và đảm bảo rằng máy tính hoặc thiết bị của họ đã được kết nối với mạng.

Kiểm tra tài nguyên mạng: Kiểm tra các tài nguyên mạng khác như máy chủ hoặc ổ đĩa mạng để đảm bảo rằng chúng đang hoạt động bình thường.

Khởi động lại thiết bị: Khởi động lại thiết bị, bao gồm cả máy tính, router và modem để khắc phục các sự cố phần mềm và phần cứng có thể xảy ra.

Kiểm tra địa chỉ IP: Kiểm tra địa chỉ IP để đảm bảo rằng nó chưa bị trùng lặp với địa chỉ IP của các thiết bị khác trong mạng.

Kiểm tra tường lửa: Kiểm tra tường lửa và cài đặt đúng các quy tắc để đảm bảo rằng các tài nguyên mạng được phép truy cập thông qua các cổng tương ứng.

Thực hiện một số thao tác đơn giản: Như xóa bộ nhớ cache, kiểm tra đường truyền Internet hoặc tạm ngừng các ứng dụng hoạt động để xem có giúp giải quyết sự cố hay không.

B2: Phân tích, điều tra:

Vấn đề kết nối mạng: Các vấn đề về kết nối mạng như mạng chậm, mất kết nối hoặc bị gián đoạn có thể làm người dùng không thể truy cập được tài nguyên mạng.

Lỗi DNS: Lỗi DNS có thể làm cho người dùng không thể truy cập được các tên miền hoặc trang web cụ thể.

Lỗi cấu hình: Các lỗi cấu hình trên router, modem hoặc tường lửa có thể gây ra sự cố không thể truy cập được tài nguyên mạng.

Các tấn công mạng: Các tấn công như tấn công từ chối dịch vụ (DDoS) hoặc tấn công mã độc có thể làm gián đoạn kết nối mạng hoặc làm cho tài nguyên mạng không thể truy cập được.

Các lỗi phần mềm hoặc phần cứng: Lỗi phần mềm hoặc phần cứng trên các thiết bị mạng như máy tính, router hoặc modem có thể gây ra sự cố không thể truy cập được tài nguyên mạng.

Các lỗi cấu hình DNS: Các lỗi cấu hình DNS như sai địa chỉ IP hoặc sai cấu hình DNS có thể làm người dùng không thể truy cập được tài nguyên mạng.

Các lỗi bảo mật: Các lỗ hổng bảo mật hoặc các cuộc tấn công bảo mật có thể làm gián đoạn kết nối mạng và làm cho người dùng không thể truy cập được tài nguyên mạng.

B3:

Xử lý lỗi cấu hình

Kiểm tra cấu hình: Kiểm tra lại các cài đặt cấu hình trên router, modem hoặc tường lửa và đảm bảo rằng chúng đang hoạt động đúng cách.

Thiết lập lại thiết bị: Nếu không thể tìm ra nguyên nhân của sự cố, hãy thiết lập lại router, modem hoặc tường lửa để đặt lại cấu hình mặc định. Lưu ý rằng thiết lập lại các thiết bị này sẽ xoá tất cả các cài đặt và mật khẩu hiện có.

Cập nhật firmware: Nếu sự cố là do lỗi firmware, hãy cập nhật firmware cho thiết bị để đảm bảo rằng nó đang chạy phiên bản firmware mới nhất.

Kiểm tra cấu hình mạng: Kiểm tra lại cấu hình mạng trên các thiết bị được kết nối với router, modem hoặc tường lửa để đảm bảo rằng chúng đang hoạt động đúng cách và không gây ra các xung đột mạng.

Kiểm tra tường lửa: Nếu router hoặc modem được kết nối với tường lửa, hãy kiểm tra cấu hình tường lửa để đảm bảo rằng chúng không chặn kết nối đến tài nguyên mạng.

Xử lý các tấn công mạng

Tăng cường bảo mật: Nâng cao bảo mật hệ thống bằng cách cập nhật phần mềm, thiết lập mật khẩu mạnh, giới hạn quyền truy cập cho người dùng và cài đặt phần mềm diệt virus.

Kiểm tra và xóa mã độc: Sử dụng phần mềm diệt virus hoặc công cụ quét mã độc để phát hiện và xóa mã độc khỏi hệ thống.

Cấu hình tường lửa: Cấu hình tường lửa để chặn các truy cập đến tài nguyên mạng từ các địa chỉ IP bị nghi ngờ hoặc từ các địa chỉ IP có lưu lượng truy cập lớn đến một tài nguyên cụ thể.

Sử dụng các công cụ giám sát mạng: Sử dụng các công cụ giám sát mạng để theo dõi lưu lượng mạng và phát hiện các hoạt động bất thường.

Sử dụng dịch vụ chuyên nghiệp: Sử dụng dịch vụ chuyên nghiệp để chống lại các tấn công mạng như DDoS hoặc tấn công mã độc.

Tăng cường khả năng chịu tải: Tăng cường khả năng chịu tải của hệ thống bằng cách tăng băng thông mạng hoặc sử dụng các giải pháp như CDN (Content Delivery Network).

Sự cố cấu hình DNS

Kiểm tra địa chỉ IP: Kiểm tra địa chỉ IP của các máy chủ DNS được cấu hình trong hệ thống và đảm bảo rằng chúng đúng.

Kiểm tra cấu hình DNS: Kiểm tra cấu hình DNS trong hệ thống và đảm bảo rằng chúng đúng. Đặc biệt, cần kiểm tra các bản ghi DNS (DNS record) như A record, CNAME record, MX record, và TXT record để đảm bảo rằng chúng được cấu hình đúng.

Xóa bộ đệm DNS: Nếu bộ đệm DNS (DNS cache) của hệ thống bị lỗi, có thể xóa bộ đệm để cập nhật lại các bản ghi DNS mới nhất.

Khởi động lại dịch vụ DNS: Nếu các bước trên không giải quyết được vấn đề, có thể khởi động lại dịch vụ DNS trên hệ thống để đảm bảo rằng nó hoạt động đúng.

Sử dụng dịch vụ DNS bên ngoài: Nếu các bước trên không giải quyết được vấn đề, có thể sử dụng dịch vụ DNS bên ngoài để truy cập tài nguyên mạng.

B4: Bài học kinh nghiệm:

Quản lý cấu hình hệ thống mạng đầy đủ và chính xác để giảm thiểu các lỗi cấu hình có thể gây ra sự cố.

Tạo bản sao lưu dữ liệu định kỳ và đảm bảo khả năng phục hồi nhanh chóng khi có sự cố xảy ra.

Tăng cường bảo mật mạng, bao gồm các biện pháp như cập nhật phần mềm định kỳ, giám sát hoạt động mạng và triển khai các giải pháp bảo mật phù hợp.

Thiết lập một quy trình giải quyết sự cố rõ ràng và hiệu quả, bao gồm các bước tiếp nhận, xác định nguyên nhân, xử lý và đánh giá sự cố.

Đào tạo nhân viên về kỹ năng giải quyết sự cố và các quy trình quản lý mạng để cải thiện khả năng phục vụ và giảm thiểu thời gian giải quyết sự cố.

Tương tác chặt chẽ với nhà cung cấp dịch vụ mạng để đảm bảo rằng họ cung cấp các giải pháp và hỗ trợ phù hợp khi có sự cố xảy ra.

**Bài 2: Sự cố lộ thông tin bí mật**

B1: Tiếp nhận sự cố

Nhận được các email lạ hoặc các cuộc gọi lạ từ các tổ chức hoặc cá nhân không rõ danh tính yêu cầu xác nhận thông tin hoặc cung cấp thông tin nhạy cảm.

Phát hiện các hoạt động không thể giải thích được trên tài khoản của mình, chẳng hạn như các giao dịch lạ hoặc các thay đổi thông tin tài khoản.

Phát hiện các tệp hoặc thư mục mới xuất hiện trên máy tính của mình mà mình không nhớ đã tạo ra.

Nhận được thông báo từ nhà cung cấp dịch vụ mạng rằng tài khoản của mình đã bị tấn công hoặc bị đánh cắp.

Nhận thấy máy tính hoạt động chậm hơn thông thường, chẳng hạn như khởi động chậm, thời gian tải ứng dụng kéo dài hoặc truy cập internet chậm hơn.

Phát hiện các file hay thư mục của mình bị mất mát hoặc không thể truy cập được.

Ứng phó ban đầu:

Thay đổi mật khẩu ngay lập tức cho các tài khoản liên quan đến thông tin bị lộ.

Khóa các tài khoản liên quan đến thông tin bị lộ để tránh các tác động tiếp theo từ người tấn công.

Thông báo cho nhà cung cấp dịch vụ mạng, ngân hàng hoặc các tổ chức khác liên quan để họ có thể hỗ trợ và giải quyết vấn đề.

Quét máy tính của mình bằng phần mềm diệt virus hoặc chương trình chống phần mềm độc hại để phát hiện và loại bỏ các chương trình độc hại.

Đặt mật khẩu mạnh và khác nhau cho mỗi tài khoản và sử dụng phương pháp xác thực hai yếu tố để tăng cường bảo mật.

Tránh cung cấp thông tin cá nhân cho các trang web hoặc tổ chức không rõ nguồn gốc.

B2: Phân tích điều tra, tìm kiếm nguyên nhân

Tấn công mạng: Các hình thức tấn công như tấn công mạng tấn công từ chối dịch vụ (DDoS), tấn công tràn bộ đệm (Buffer overflow), tấn công mã độc, tấn công giả mạo địa chỉ IP (IP Spoofing) có thể làm lộ thông tin bí mật của người dùng.

Lỗi phần mềm: Các lỗ hổng phần mềm có thể cho phép tin tặc tấn công trực tiếp vào máy tính của người dùng và lấy cắp thông tin bí mật.

Phần mềm độc hại: Phần mềm độc hại như virus, spyware, trojan horse có thể lấy cắp thông tin bí mật từ máy tính của người dùng mà họ không hay biết.

Mạng không bảo mật: Nếu mạng không được bảo mật đúng cách, tin tặc có thể lấy cắp thông tin bí mật từ các gói tin được gửi qua mạng.

Sai sót của nhân viên: Sai sót của nhân viên như lỡ để thông tin bí mật rò rỉ, quên mật khẩu, sử dụng mật khẩu yếu có thể dẫn đến việc lộ thông tin bí mật.

Sử dụng các trang web hoặc ứng dụng không đáng tin cậy: Sử dụng các trang web hoặc ứng dụng không đáng tin cậy có thể dẫn đến việc người dùng bị lừa để cung cấp thông tin bí mật cho tin tặc.

B3: xử lý và khôi phục sự cố

Ngắt kết nối mạng và tắt thiết bị liên quan: Khi phát hiện có người dùng bị lộ thông tin bí mật, cần ngắt kết nối mạng và tắt các thiết bị liên quan ngay lập tức để ngăn chặn tin tặc tiếp tục truy cập vào thông tin bí mật.

Thay đổi mật khẩu: Người dùng nên thay đổi mật khẩu của tài khoản bị ảnh hưởng ngay sau khi phát hiện sự cố.

Cập nhật phần mềm và các bản vá bảo mật: Các lỗ hổng phần mềm và bảo mật có thể cho phép tin tặc tấn công trực tiếp vào máy tính của người dùng và lấy cắp thông tin bí mật. Vì vậy, cần đảm bảo phần mềm và hệ điều hành được cập nhật lên phiên bản mới nhất và các bản vá bảo mật được cài đặt.

Sử dụng phần mềm diệt virus và tường lửa: Sử dụng phần mềm diệt virus và tường lửa có thể giúp phát hiện và ngăn chặn các phần mềm độc hại truy cập vào máy tính của người dùng.

Kiểm tra hệ thống bảo mật: Kiểm tra hệ thống bảo mật để đảm bảo rằng các chính sách bảo mật đang được áp dụng đầy đủ và hiệu quả.

Cập nhật các chính sách bảo mật và đào tạo nhân viên: Cập nhật các chính sách bảo mật để đảm bảo rằng các thông tin bí mật được bảo vệ và đào tạo nhân viên về các quy trình bảo mật và giám sát để đảm bảo rằng các chính sách được tuân thủ đúng cách.

Thông báo cho các cơ quan chức năng: Nếu sự cố liên quan đến việc người dùng bị lộ thông tin bí mật nghiêm trọng, cần thông báo cho các cơ quan chức năng để được hỗ trợ trong việc xử lý sự cố và bảo vệ quyền lợi của người dùng.Top of Form

bươBottom of Form

Bước 4: Tổng kết, đánh giá và đưa ra bài học

Tăng cường kiểm soát truy cập: Đảm bảo rằng các tài khoản người dùng chỉ có quyền truy cập vào các tài nguyên cần thiết để thực hiện công việc của họ. Các tài khoản quản trị viên nên được giám sát chặt chẽ và cần có các quy trình xác thực đáng tin cậy để đảm bảo chỉ những người được ủy quyền mới có thể truy cập vào hệ thống.

Tăng cường bảo mật mạng: Sử dụng các giải pháp bảo mật mạng như tường lửa, mã hóa và phát hiện xâm nhập để bảo vệ mạng khỏi các cuộc tấn công từ bên ngoài. Các giải pháp bảo mật mạng hiện đại có khả năng phát hiện và ngăn chặn các cuộc tấn công từ bên ngoài trước khi chúng có thể gây ra thiệt hại.

Đảm bảo tính bảo mật của ứng dụng: Các ứng dụng phải được thiết kế với tính bảo mật cao, bao gồm các biện pháp bảo vệ như kiểm tra dữ liệu đầu vào, bảo vệ chống lại tấn công SQL injection, mã hóa dữ liệu và cập nhật định kỳ để khắc phục các lỗ hổng bảo mật mới.

Đào tạo nhân viên về an ninh mạng: Đào tạo nhân viên về các nguy cơ an ninh mạng và cách đối phó với chúng là rất quan trọng. Các chương trình đào tạo có thể bao gồm các bài giảng về bảo mật mạng, các trò chơi giả lập để thử nghiệm kỹ năng bảo mật, và các cuộc tập trung để tăng cường kỹ năng và hiểu biết về an ninh mạng.

Điều tra và phân tích sự cố: Điều tra và phân tích sự cố để hiểu rõ nguyên nhân và tìm ra các điểm yếu trong hệ thống. Điều này có thể giúp cải thiện bảo mật mạng bằng cách đưa ra các biện pháp khắc phục cụ thể và cải tiến quy trình bảo mật.

**Bài 3: Sự cố hệ thông nhiễm mã độc**

B1: Tiếp nhận sự cố

Tốc độ hoạt động của hệ thống giảm đáng kể.

Khởi động lại hệ thống không thành công hoặc chậm chạp.

Thông tin cá nhân hoặc tài khoản bị truy cập hoặc thay đổi mà không có sự cho phép của người dùng.

Các chương trình hoạt động không đúng cách hoặc không mở được.

Trình duyệt web thường xuyên bị chuyển hướng đến các trang web không mong muốn.

Thông báo bảo mật xuất hiện thường xuyên.

Máy tính gửi hoặc nhận số lượng lớn email hoặc thông tin không rõ nguồn gốc.

Dung lượng ổ cứng giảm đáng kể mà không có lý do rõ ràng.

Ứng cứu ban đầu

Cô lập hệ thống: Ngay khi phát hiện có dấu hiệu của mã độc, cần ngắt kết nối mạng hoặc cô lập hệ thống khỏi các hệ thống khác trong mạng để ngăn chặn sự lan truyền của mã độc sang các thiết bị khác trong mạng.

Khởi động lại hệ thống: Việc khởi động lại hệ thống sẽ làm giảm các hoạt động của mã độc và cho phép các công cụ quét virus hoạt động tốt hơn.

Chạy công cụ quét virus: Sử dụng các công cụ quét virus để phát hiện và loại bỏ các mã độc, cũng như kiểm tra các tập tin, ứng dụng, dịch vụ và tiến trình đang hoạt động trên hệ thống.

Tắt các tiến trình đáng ngờ: Tắt các tiến trình đáng ngờ hoặc không cần thiết để giảm thiểu các hậu quả của việc nhiễm virus.

Cập nhật các phần mềm bảo mật: Cập nhật các phần mềm bảo mật mới nhất để ngăn chặn sự xâm nhập của các mã độc.

Điều tra nguyên nhân: Xác định nguyên nhân dẫn đến sự cố và phân tích để tìm ra giải pháp xử lý triệt để.

Thông báo cho đơn vị liên quan: Thông báo cho đơn vị liên quan như nhà cung cấp dịch vụ bảo mật, các đơn vị chuyên trách về an ninh mạng để có được sự hỗ trợ và tư vấn trong việc giải quyết sự cố.

B2: Phân tích điều tra, tìm kiếm nguyên nhân

Email lừa đảo (phishing): Tấn công này thường được thực hiện bằng cách gửi email giả mạo, thường là có đính kèm hoặc liên kết độc hại, để lừa người dùng cung cấp thông tin đăng nhập hoặc khai thác lỗ hổng trong hệ thống.

Phần mềm độc hại: Các phần mềm độc hại, bao gồm virus, trojan và phần mềm độc hại khác, có thể được tải xuống và cài đặt trên hệ thống của người dùng thông qua các trang web độc hại hoặc các liên kết độc hại.

Lỗ hổng bảo mật: Các lỗ hổng bảo mật trong hệ thống, bao gồm cả phần mềm và phần cứng, có thể được khai thác bởi các tấn công gia nhập, tấn công từ chối dịch vụ (DDoS), mã độc hoặc các tấn công khác.

Kết nối không an toàn: Kết nối không an toàn, bao gồm cả kết nối mạng không an toàn và kết nối không bảo mật với các ứng dụng và dịch vụ trực tuyến, có thể dẫn đến việc bị nhiễm mã độc hoặc bị tấn công.

Phần mềm cập nhật không đầy đủ: Việc không cập nhật các phiên bản phần mềm mới nhất và các bản vá bảo mật có thể dẫn đến các lỗ hổng bảo mật trong hệ thống, làm cho hệ thống dễ bị tấn công và nhiễm mã độc.

Cập nhật và cài đặt phần mềm bảo mật: Cập nhật các bản vá bảo mật mới nhất và cài đặt phần mềm bảo mật để ngăn chặn các tấn công từ các lỗ hổng phần mềm.

Sử dụng phần mềm chống virus/malware: Cài đặt và chạy phần mềm chống virus/malware để phát hiện và loại bỏ các mã độc.

Sử dụng Firewall: Thiết lập tường lửa để ngăn chặn các tấn công từ mạng bên ngoài và kiểm soát lưu lượng mạng.

Thực hiện backup dữ liệu định kỳ: Thực hiện sao lưu dữ liệu thường xuyên và lưu trữ ở nơi an toàn để phòng trường hợp bị mất dữ liệu do mã độc tấn công.

Kiểm tra email và tải file cẩn thận: Kiểm tra kỹ email và tải file chỉ từ các nguồn đáng tin cậy.

Đào tạo nhân viên: Đào tạo nhân viên về cách sử dụng internet và email một cách an toàn, và cách phát hiện và báo cáo các tấn công từ mã độc.

Quản lý quyền truy cập: Thiết lập quản lý quyền truy cập đối với người dùng, giới hạn quyền truy cập của người dùng đến các phần mềm và tài liệu cần thiết.

Kiểm tra và quản lý thiết bị: Kiểm tra và quản lý thiết bị của các người dùng để đảm bảo không có thiết bị nào bị nhiễm mã độc.

Cài đặt chính sách bảo mật: Cài đặt các chính sách bảo mật để giảm thiểu nguy cơ bị tấn công từ các mã độc.

Thực hiện đánh giá bảo mật: Thực hiện đánh giá bảo mật định kỳ để phát hiện và khắc phục các lỗ hổng bảo mật.

B3: xử lý, khôi phục sự cố

Cập nhật và cài đặt phần mềm bảo mật: Cập nhật các bản vá bảo mật mới nhất và cài đặt phần mềm bảo mật để ngăn chặn các tấn công từ các lỗ hổng phần mềm.

Sử dụng phần mềm chống virus/malware: Cài đặt và chạy phần mềm chống virus/malware để phát hiện và loại bỏ các mã độc.

Sử dụng Firewall: Thiết lập tường lửa để ngăn chặn các tấn công từ mạng bên ngoài và kiểm soát lưu lượng mạng.

Thực hiện backup dữ liệu định kỳ: Thực hiện sao lưu dữ liệu thường xuyên và lưu trữ ở nơi an toàn để phòng trường hợp bị mất dữ liệu do mã độc tấn công.

Kiểm tra email và tải file cẩn thận: Kiểm tra kỹ email và tải file chỉ từ các nguồn đáng tin cậy.

Đào tạo nhân viên: Đào tạo nhân viên về cách sử dụng internet và email một cách an toàn, và cách phát hiện và báo cáo các tấn công từ mã độc.

Quản lý quyền truy cập: Thiết lập quản lý quyền truy cập đối với người dùng, giới hạn quyền truy cập của người dùng đến các phần mềm và tài liệu cần thiết.

Kiểm tra và quản lý thiết bị: Kiểm tra và quản lý thiết bị của các người dùng để đảm bảo không có thiết bị nào bị nhiễm mã độc.

Cài đặt chính sách bảo mật: Cài đặt các chính sách bảo mật để giảm thiểu nguy cơ bị tấn công từ các mã độc.

Thực hiện đánh giá bảo mật: Thực hiện đánh giá bảo mật định kỳ để phát hiện và khắc phục các lỗ hổng bảo mật.

B4: Tổng kết đánh giá, đưa ra bài học

Tăng cường phòng chống mã độc: Mã độc là mối đe dọa đáng lo ngại cho hệ thống thông tin và toàn bộ mạng. Do đó, việc tăng cường phòng chống mã độc là rất cần thiết để bảo vệ hệ thống thông tin của tổ chức hoặc doanh nghiệp.

Nâng cao nhận thức an ninh thông tin: Đào tạo nhân viên và người dùng về an ninh thông tin là rất quan trọng. Điều này giúp người dùng có thể nhận biết được các dấu hiệu cảnh báo và hành động kịp thời để giảm thiểu tác động của mã độc.

Thường xuyên sao lưu dữ liệu: Việc sao lưu dữ liệu định kỳ giúp đảm bảo rằng tổ chức có thể phục hồi lại dữ liệu trong trường hợp xảy ra sự cố nhiễm mã độc.

Cập nhật phần mềm và hệ điều hành thường xuyên: Việc cập nhật phần mềm và hệ điều hành thường xuyên giúp bảo mật hệ thống, đồng thời giảm thiểu các lỗ hổng bảo mật và các lỗ hổng khác có thể được khai thác bởi tội phạm mạng.

Sử dụng phần mềm bảo mật: Việc sử dụng phần mềm bảo mật là một biện pháp rất hiệu quả để phòng chống mã độc và các tấn công mạng khác. Các giải pháp bảo mật như phần mềm diệt virus, phần mềm tường lửa và các công nghệ bảo mật khác giúp giảm thiểu rủi ro của các cuộc tấn công mạng.

**Bài 4: Sự cố phân quyền**

B1: Tiếp nhận sự cố

Người dùng không thể truy cập hoặc thực hiện các thao tác trên các tài nguyên, ứng dụng hoặc chức năng mà họ có quyền truy cập.

Người dùng có thể truy cập hoặc thực hiện các thao tác trên các tài nguyên, ứng dụng hoặc chức năng mà họ không có quyền truy cập.

Các tài khoản người dùng bị sa thải hoặc bị khóa không đúng cách.

Các tài khoản người dùng bị tạo ra hoặc cho phép truy cập vào các tài nguyên, ứng dụng hoặc chức năng mà không được phép.

Các tài nguyên hoặc dịch vụ bị ảnh hưởng bởi quyền truy cập không đúng hoặc không hợp lệ.

Ứng cứu ban đầu:

Kiểm tra lại các quyền truy cập và vai trò của người dùng và đảm bảo rằng chúng được cấu hình đúng. Nếu cần thiết, cập nhật lại các quyền truy cập hoặc thêm vai trò mới để đảm bảo rằng người dùng có quyền truy cập đầy đủ vào các tài nguyên mà họ cần.

Kiểm tra xem có sự cố nào với hệ thống quản lý phân quyền. Nếu có lỗi hoặc sự cố xảy ra với phần mềm quản lý phân quyền, cần sửa lỗi hoặc nâng cấp để đảm bảo rằng phần mềm hoạt động đúng và đáp ứng được các yêu cầu của người dùng.

Kiểm tra các đặc quyền hệ thống và đảm bảo rằng chúng được cấu hình đúng và được giới hạn đối với những người dùng có nhu cầu sử dụng.

Kiểm tra các chính sách bảo mật và đảm bảo rằng chúng được cấu hình đúng và đáp ứng được các yêu cầu của người dùng.

Kiểm tra hệ thống để phát hiện và loại bỏ các lỗ hổng bảo mật, chẳng hạn như các lỗ hổng trong phần mềm hoặc các tài khoản người dùng bị xâm nhập.

Tăng cường hệ thống giám sát và báo động để phát hiện sớm các sự cố liên quan đến phân quyền và có biện pháp xử lý kịp thời.

Tạo ra một kế hoạch khẩn cấp và đào tạo nhân viên để đối phó với các sự cố về phân quyền và giảm thiểu thiệt hại khi chúng xảy ra.

Nâng cao ý thức cho người dùng và đào tạo để họ hiểu rõ về cách sử dụng đúng các tài nguyên và quyền truy cập của họ trong hệ thống.

B2: Phân tích điều tra, tìm kiếm nguyên nhân

Lỗi cấu hình: Việc cấu hình hệ thống không chính xác có thể dẫn đến việc người dùng không được phân quyền đúng mức.

Tấn công đánh cắp thông tin: Kẻ tấn công có thể lợi dụng các lỗ hổng bảo mật trong hệ thống để đánh cắp thông tin đăng nhập của người dùng và sử dụng nó để truy cập vào các tài khoản không được phân quyền.

Tấn công từ chối dịch vụ (DoS): Tấn công DoS có thể làm gián đoạn hoạt động của hệ thống và làm cho người dùng không thể đăng nhập hoặc không được phân quyền.

Tấn công dò mật khẩu: Kẻ tấn công có thể dò mật khẩu của người dùng để đăng nhập vào tài khoản của họ và truy cập vào các tài nguyên không được phân quyền.

Lỗ hổng bảo mật: Những lỗ hổng bảo mật trong hệ thống có thể bị kẻ tấn công lợi dụng để truy cập vào các tài nguyên không được phân quyền.

Lỗi phần mềm: Một số lỗi phần mềm có thể làm cho người dùng có thể truy cập vào các tài nguyên không được phân quyền.

Sử dụng phần mềm độc hại: Sử dụng phần mềm độc hại có thể làm cho kẻ tấn công có thể truy cập vào các tài nguyên không được phân quyền.

B3: Xử lý, khôi phục sự cố

Đánh giá lại phân quyền hệ thống: Kiểm tra lại quyền truy cập của từng tài khoản, đảm bảo chỉ có những người được ủy quyền mới có quyền truy cập vào các tài nguyên nhạy cảm. Nếu cần thiết, điều chỉnh lại phân quyền hệ thống.

Kiểm tra và cập nhật các phần mềm bảo mật: Các phần mềm bảo mật, như phần mềm chống virus, tường lửa, phần mềm quản lý phân quyền, cần được kiểm tra và cập nhật để đảm bảo tính bảo mật cho hệ thống.

Theo dõi hoạt động của người dùng: Sử dụng các công cụ theo dõi hoạt động của người dùng để phát hiện và ngăn chặn các hành vi bất thường hoặc đáng ngờ trên hệ thống.

Thực hiện kiểm tra bảo mật định kỳ: Thực hiện kiểm tra bảo mật định kỳ để phát hiện và khắc phục các lỗ hổng bảo mật có thể bị khai thác để thực hiện các tấn công liên quan đến sự cố phân quyền.

Đào tạo nhân viên: Các nhân viên cần được đào tạo về các biện pháp bảo mật thông tin, phân quyền và quản lý tài khoản để giảm thiểu nguy cơ xảy ra sự cố.

Xác định nguyên nhân và giải quyết triệt để: Xác định nguyên nhân gây ra sự cố và giải quyết triệt để để đảm bảo rằng sự cố không tái diễn.

Báo cáo và đánh giá sự cố: Báo cáo và đánh giá sự cố để rút kinh nghiệm, đưa ra các giải pháp cải thiện và tăng cường bảo mật hệ thống.

B4: Tổng kết đánh giá

Sự cố về phân quyền là một trong những vấn đề phổ biến và có thể xảy ra bất cứ khi nào trong quá trình phát triển và quản lý hệ thống. Để tránh sự cố này, cần thực hiện các biện pháp bảo mật và kiểm tra định kỳ các cấu hình phân quyền.

Bài học kinh nghiệm quan trọng là việc cập nhật và kiểm tra định kỳ các cấu hình phân quyền để tránh sự cố về phân quyền. Ngoài ra, việc đào tạo nhân viên về an ninh mạng cũng rất quan trọng để ngăn chặn các tấn công và giảm thiểu rủi ro. Bên cạnh đó, việc sử dụng các công cụ bảo mật mạng cũng là một biện pháp quan trọng để giảm thiểu nguy cơ bị tấn công.

Với kinh nghiệm từ sự cố này, nhà quản trị hệ thống và an ninh mạng cần học hỏi và nâng cao kiến thức của mình để giải quyết các vấn đề về bảo mật và phân quyền một cách hiệu quả hơn trong tương lai.

**Bài 5: Sự cố tấn công giao diện web bị thay đổi**

Bước 1: Tiếp nhận sự cố

• Giao diện web bị thay đổi

• Không thể truy cập vào trang web

• Các tính năng hoạt động không đúng như mong muốn

Ứng phó ban đầu:

• Tạm ngưng truy cập vào trang web

• Kiểm tra ngay các hệ thống khác để xác định phạm vi và mức độ của sự cố

Bước 2: Phân tích điều tra, tìm kiếm nguyên nhân

• Xác định loại hình tấn công: SQL Injection, XSS, hoặc Brute Force

• Xác định giao diện web bị thay đổi: bằng cách kiểm tra source code hoặc đối sánh với bản sao lưu trữ

• Xác định thời gian và tần suất của các hoạt động tấn công

Bước 3: Xử lý, khôi phục sự cố:

• Cập nhật các bản vá lỗi mới nhất để khắc phục lỗ hổng bảo mật

• Chặn IP và nguồn tấn công bằng cách sử dụng tường lửa (Firewall) hoặc IPS (Intrusion Prevention System)

• Giám sát hoạt động của trang web bằng các công cụ bảo mật như WAF (Web Application Firewall)

• Phục hồi giao diện web bị thay đổi

Bước 4: Tổng kết, đánh giá, đưa ra bài học

* Sự cố tấn công giao diện web bị thay đổi là một vấn đề nghiêm trọng và có thể gây ra những hậu quả nặng nề cho doanh nghiệp hoặc tổ chức
* Các nguyên nhân có thể là lỗi trong thiết kế hoặc triển khai giao diện web, lỗ hổng bảo mật trong hệ thống, nhân viên không có kỹ năng và kiến thức đủ để xử lý sự cố hoặc tấn công mạng từ bên ngoài.
* Bài học kinh nghiệm: Tổ chức cần thiết lập các chính sách kiểm soát quyền truy cập chặt chẽ để chỉ cho phép các người dùng được phép truy cập vào các trang web nhất định. Sử dụng các công cụ bảo mật web, kiểm tra bảo mật thường xuyên, giáo dục và đào tạo nhân viên, người dùng. Bên cạnh đó, việc sử dụng các công cụ bảo mật mạng cũng là một biện pháp quan trọng để giảm thiểu nguy cơ bị tấn công.
* Thực hiện các biện pháp bảo mật hiệu quả để giảm thiểu rủi ro của các sự cố tương tự xảy ra trong tương lai.