[Câu 1: Vai trò của hệ thống giám sát trong việc đảm bảo an toàn hệ thống thông tin và mạng máy tính 2](#_Toc131461071)

[Câu 2: So sánh công nghệ giám sát ATTT với công nghệ phát hiện xâm nhập IDS 3](#_Toc131461072)

[Câu 3: So sánh giám sát an toàn mạng với giám sát an ninh liên tục 5](#_Toc131461073)

[Câu 4: Phân tích ưu và nhược điểm của hệ thống giám sát SIEM 7](#_Toc131461074)

[Câu 5: Trình bày một số sản phẩm giám sát ATTT mà em biết 9](#_Toc131461075)

[Câu 6: Kiến trúc và thành phần của hệ thống giám sát 10](#_Toc131461076)

[Câu 7: Phân tích một số chức năng quan trọng trong hệ thống giám sát 12](#_Toc131461077)

[Câu 8: Các loại dữ liệu đầu vào của hệ thống giám sát 14](#_Toc131461078)

[Câu 9: Phương pháp thu thập dữ liệu của hệ thống giám sát 14](#_Toc131461079)

[Câu 10: Lập kế hoạch thu thập dữ liệu theo Khung ACF (Applied Collection Framework) 17](#_Toc131461080)

[Câu 11: Phương pháp phân tích dữ liệu 18](#_Toc131461081)

[Câu 12: Lấy ví dụ và phân tích một số sự cố ATTT 20](#_Toc131461082)

[Câu 13: Vai trò của ứng phó sự cố trong đảm bảo ATTT 24](#_Toc131461083)

[Câu 14: Các bước ứng phó sự cố ATTT 25](#_Toc131461084)

[Dạng 1: Bài tập về tính toán dấu hiệu xâm nhập IOC. 28](#_Toc131461085)

[Dạng 2: Bài tập về lập kế hoạch thu thập dữ liệu. 30](#_Toc131461086)

[Dạng 3: Bài tập về phân tích dữ liệu 32](#_Toc131461087)

[Dạng 4: Bài tập về ứng phó sự cố ATTT. 38](#_Toc131461088)

1. ***Lý thuyết***
2. Vai trò của hệ thống giám sát trong việc đảm bảo an toàn hệ thống thông tin và mạng máy tính
3. So sánh công nghệ giám sát ATTT với công nghệ phát hiện xâm nhập IDS
4. So sánh giám sát an toàn mạng với giám sát an ninh liên tục
5. Phân tích ưu nhược điểm của hệ thống giám sát
6. Trình bày một số sản phẩm giám sát ATTT mà em biết
7. Kiến trúc và thành phần của hệ thống giám sát
8. Phân tích một số chức năng quan trọng trong hệ thống giám sát
9. Các loại dữ liệu đầu vào của hệ thống giám sát
10. Phương pháp thu thập dữ liệu của hệ thống giám sát
11. Lập kế hoạch thu thập dữ liệu theo Khung ACF (Applied Collection Framework)
12. Phương pháp phân tích dữ liệu
13. Lấy ví dụ và phân tích một số sự cố ATTT
14. Vai trò của ưng phó sự cố trong đảm bảo ATTT
15. Các bước ứng phó sự cố ATTT
16. ***Bài tập***
17. Bài tập về tính toán dấu hiệu xâm nhập IOC. Tài liệu tham khảo [1] – Chương 2.1; [2]- Chương 7
18. Bài tập về lập kế hoạch thu thập dữ liệu. [1]-Chương 2.2; [3]-Chương 2;
19. Bài tập về phân tích dữ liệu. [1]-Chương 2.2;
20. Bài tập về ứng phó sự cố ATTT. [1]-Chương 3,4; [4], [5]

Đề cương

# Câu 1: Vai trò của hệ thống giám sát trong việc đảm bảo an toàn hệ thống thông tin và mạng máy tính

Khái niệm: Hệ thống giám sát an toàn thông tin (SIEM - security information and event managent) là hệ thống dực thiết kế nhằm thu thập thông tin nhật ký các sự kiện an ninh từ các thiết bị đầu cuối và phân tích chúng với mục đích phát hiện và kịp thời ứng phó, cho phép tổ chức hạn chế được các rủi ro, tiết kiệm thời gian và nhân lực.

Hệ thống giám sát có vai trò quan trọng trong việc đảm bảo an toàn hệ thống thông tin và mạng máy tính. Các chức năng chính của hệ thống giám sát bao gồm:

* Giám sát hoạt động của hệ thống: Hệ thống giám sát cung cấp thông tin về các hoạt động đang diễn ra trong hệ thống và mạng máy tính. Điều này giúp cho các quản trị viên hệ thống có thể phát hiện các hành vi bất thường, tấn công từ bên ngoài hoặc các lỗi trong hệ thống.
* Phát hiện tấn công mạng: Hệ thống giám sát giúp phát hiện các tấn công mạng từ bên ngoài, như các cuộc tấn công từ chối dịch vụ (DoS), tấn công mạng lưới và tấn công phishing. Nó cũng có thể phát hiện các tấn công từ bên trong, chẳng hạn như các cuộc tấn công mạng có mục đích tiêu cực hoặc lừa đảo.
* Cảnh báo và đưa ra các giải pháp an ninh: Khi hệ thống giám sát phát hiện một sự cố an ninh, nó sẽ tự động gửi thông báo đến các quản trị viên hệ thống để họ có thể xử lý nhanh chóng. Nó cũng có thể đưa ra các giải pháp an ninh để khắc phục các lỗ hổng bảo mật trong hệ thống.
* Theo dõi chính sách bảo mật: Hệ thống giám sát cũng giúp theo dõi và bảo vệ các chính sách bảo mật, đảm bảo rằng các quy định an ninh được tuân thủ đầy đủ và các hoạt động không phù hợp sẽ được phát hiện và xử lý.
* Định tuyến và quản lý lưu lượng mạng: Hệ thống giám sát có thể giúp các nhà quản trị điều hướng và quản lý lưu lượng mạng. Những thông tin này cũng có thể được sử dụng để tối ưu hóa cấu hình mạng và đảm bảo băng thông mạng đủ cho nhu cầu sử dụng.
* Quản lý bảo mật: Hệ thống giám sát cũng đóng vai trò quan trọng trong việc giám sát và quản lý bảo mật mạng. Nó giúp đảm bảo các chính sách bảo mật được thực thi, theo dõi các sự kiện an ninh, phát hiện các tấn công mạng và bảo vệ các tài nguyên mạng quan trọng.

Tóm lại, hệ thống giám sát đóng vai trò rất quan trọng trong việc đảm bảo an toàn hệ thống thông tin và mạng máy tính. Nó giúp phát hiện và ngăn chặn các tấn công mạng, cung cấp cảnh báo và đưa ra các giải pháp an ninh để khắc phục các lỗ hổng bảo mật và giúp theo dõi và bảo vệ các chính sách bảo mật.

# Câu 2: So sánh công nghệ giám sát ATTT với công nghệ phát hiện xâm nhập IDS

**\*Giống nhau:**

* Đều là các công nghệ nhận diện các mối đe dọa bảo mật mạng: Cả ATTT và IDS đều có khả năng nhận diện và phát hiện các mối đe dọa bảo mật mạng, đặc biệt là trong trường hợp các tấn công từ bên ngoài vào hệ thống.
* Đều có khả năng cảnh báo và ngăn chặn các đe dọa: Cả hai công nghệ đều có khả năng cảnh báo cho người quản trị hệ thống về các mối đe dọa bảo mật mạng, từ đó ngăn chặn các hành vi tấn công.
* Đều có khả năng theo dõi và kiểm soát các hoạt động mạng: Hai công nghệ này đều có khả năng theo dõi và giám sát các hoạt động mạng trong thời gian thực, giúp phát hiện và xử lí các tình huống khẩn cấp một cách nhanh chóng và hiệu quả.
* Đều có khả năng phản ứng nhanh trong trường hợp xảy ra vấn đề bảo mật: Cả hai công nghệ ATTT và IDS đều có khả năng phản ứng nhanh trong trường hợp xảy ra các vấn đề bảo mật mạng, giúp ngăn chặn tác động xấu lên hệ thống.

**\*Khác nhau:**

Cả hai công nghệ giám sát An toàn thông tin và công nghệ phát hiện xâm nhập IDS đều là các công nghệ quan trọng trong lĩnh vực bảo mật mạng. Tuy nhiên, chúng có các điểm khác nhau như sau:

Mục đích sử dụng:

* Công nghệ giám sát An toàn thông tin thường được sử dụng để giám sát và quản lý các hệ thống bảo mật, giúp ngăn chặn các cuộc tấn công trước khi chúng có thể gây hại cho hệ thống.
* Công nghệ phát hiện xâm nhập IDS thường được sử dụng để phát hiện các cuộc tấn công đang diễn ra hoặc đã xảy ra trên hệ thống, giúp cho người quản trị có thể phản ứng kịp thời và ngăn chặn những hậu quả tiềm ẩn.

Phương pháp hoạt động:

* Công nghệ giám sát An toàn thông tin thường sử dụng các phương pháp quét và phân tích dữ liệu để giám sát và phát hiện các hành vi không đúng quy định hoặc các tấn công từ bên ngoài.
* Công nghệ phát hiện xâm nhập IDS sử dụng các luật, các kỹ thuật phân tích dữ liệu, hoặc các phương pháp máy học để phát hiện các hành vi tấn công đang diễn ra hoặc đã xảy ra trên hệ thống.

Khả năng phát hiện và ngăn chặn:

* Công nghệ giám sát An toàn thông tin có khả năng phát hiện sớm các hành vi không đúng quy định hoặc các tấn công từ bên ngoài, giúp ngăn chặn các cuộc tấn công trước khi chúng có thể gây hại cho hệ thống.
* Công nghệ phát hiện xâm nhập IDS có khả năng phát hiện các hành vi tấn công đang diễn ra hoặc đã xảy ra trên hệ thống, giúp cho người quản trị có thể phản ứng kịp thời và ngăn chặn những hậu quả tiềm ẩn.

Khả năng phân tích và báo cáo:

* Công nghệ giám sát An toàn thông tin có khả năng phân tích và báo cáo chi tiết về các hành vi không đúng quy định hoặc các tấn công từ bên ngoài, giúp cho người quản trị có thể phát hiện các lỗ hổng trong hệ thống và đưa ra các biện pháp bảo mật phù hợp.
* Công nghệ phát hiện xâm nhập IDS cũng có khả năng phân tích và báo cáo về các hành vi tấn công đang diễn ra hoặc đã xảy ra trên hệ thống, giúp người quản trị có thể hiểu được các mối đe dọa đang tiềm ẩn và đưa ra các biện pháp phòng ngừa và khắc phục.

Độ tin cậy:

* Cả hai công nghệ đều phụ thuộc vào chất lượng của dữ liệu đầu vào và độ chính xác của các thuật toán phân tích để đưa ra kết quả đáng tin cậy.
* Tuy nhiên, trong trường hợp các tấn công phức tạp, IDS có thể cho ra nhiều kết quả giả mạo hoặc không chính xác, trong khi đó công nghệ giám sát An toàn thông tin có thể phát hiện và ngăn chặn các cuộc tấn công này trước khi chúng có thể gây hại cho hệ thống.

Tóm lại, công nghệ giám sát An toàn thông tin và công nghệ phát hiện xâm nhập IDS đều có vai trò quan trọng trong bảo vệ an toàn thông tin và bảo mật mạng. Sự lựa chọn giữa hai công nghệ này phụ thuộc vào mục đích sử dụng, yêu cầu bảo mật cụ thể của hệ thống, cũng như khả năng triển khai và quản lý của người quản trị.

# Câu 3: So sánh giám sát an toàn mạng với giám sát an ninh liên tục

**\*Giống nhau:**

* Mục tiêu chung: Cả hai loại giám sát đều nhằm đảm bảo an toàn, bảo mật và ổn định cho hệ thống mạng.
* Sự cần thiết của sự can thiệp: Cả giám sát an toàn mạng và giám sát an ninh liên tục đều yêu cầu có sự can thiệp nhanh chóng để giải quyết các vấn đề liên quan đến bảo mật mạng.
* Tập trung vào phát hiện sự cố: Cả hai loại giám sát đều tập trung vào phát hiện các sự cố an toàn mạng, bao gồm các mối đe dọa mới và tiềm ẩn, và đưa ra cảnh báo để ngăn chặn các cuộc tấn công.
* Sử dụng các công cụ giám sát: Cả giám sát an toàn mạng và giám sát an ninh liên tục đều sử dụng các công cụ giám sát và phân tích dữ liệu để phát hiện các mối đe dọa và sự cố an toàn mạng.
* Tính liên tục: Cả hai loại giám sát đều cần thực hiện liên tục, đảm bảo rằng hệ thống mạng được giám sát và bảo vệ một cách liên tục và toàn diện.

**\*Khác nhau:**

Giám sát an toàn mạng và giám sát an ninh liên tục là hai khái niệm khác nhau, mặc dù cùng liên quan đến việc bảo vệ an toàn thông tin và bảo mật mạng. Dưới đây là một số điểm khác nhau giữa hai khái niệm này:

Phạm vi:

* Giám sát an toàn mạng tập trung vào việc giám sát các hoạt động liên quan đến mạng, bao gồm các hệ thống, thiết bị, ứng dụng và dữ liệu truyền qua mạng.
* Giám sát an ninh liên tục tập trung vào việc giám sát các hoạt động liên quan đến an ninh, bao gồm cả mạng, hệ thống và con người.

Mục đích:

* Mục đích của giám sát an toàn mạng là phát hiện và ngăn chặn các mối đe dọa mạng, bảo vệ an toàn thông tin và bảo mật mạng.
* Mục đích của giám sát an ninh liên tục là phát hiện và ngăn chặn các mối đe dọa về an ninh, bao gồm cả các mối đe dọa về thực thể, bảo vệ nhân viên và các tài sản quan trọng của công ty.

Công nghệ:

* Giám sát an toàn mạng sử dụng các công nghệ giám sát mạng, bao gồm phân tích dữ liệu mạng, giám sát băng thông, phát hiện xâm nhập, quản lý đăng nhập và giám sát các thiết bị.
* Giám sát an ninh liên tục sử dụng các công nghệ giám sát an ninh, bao gồm camera giám sát, cảm biến, bảo mật vật lý và giám sát hành vi con người.

Phương pháp:

* Giám sát an toàn mạng thường được thực hiện theo kiểu định kỳ hoặc thời gian thực, dựa trên các quy tắc, chính sách và tiêu chuẩn bảo mật của công ty.
* Giám sát an ninh liên tục thường được thực hiện 24/7 và liên tục giám sát các hoạt động trên mạng và các khu vực quan trọng trong công ty.

Kết quả:

* Kết quả của giám sát an toàn mạng là các báo cáo về các mối đe dọa mạng và các biện pháp phòng ngừa và khắc phục.
* Kết quả của giám sát an ninh liên tục là các báo cáo về các hoạt động đáng ngờ, bất thường hoặc các sự kiện có thể đe dọa đến an ninh của công ty.

Động lực:

* Giám sát an toàn mạng thường được triển khai để đáp ứng các yêu cầu bảo mật và quản lý rủi ro của công ty, cũng như đảm bảo tuân thủ các quy định pháp lý.
* Giám sát an ninh liên tục thường được triển khai để giảm thiểu các mối đe dọa an ninh và giảm thiểu rủi ro cho công ty, cũng như đảm bảo an ninh vật lý và bảo vệ nhân viên.

Quản lý:

* Giám sát an toàn mạng thường được quản lý bởi các chuyên gia an toàn thông tin và kỹ thuật viên mạng.
* Giám sát an ninh liên tục thường được quản lý bởi các chuyên gia an ninh, giám sát an ninh và nhân viên bảo vệ.

Tóm lại, giám sát an toàn mạng và giám sát an ninh liên tục là hai khái niệm khác nhau, nhưng đều là các phương pháp quan trọng trong việc bảo vệ an toàn thông tin và bảo mật mạng của một công ty. Các công nghệ và phương pháp giám sát phù hợp sẽ tùy thuộc vào các nhu cầu và yêu cầu bảo mật của công ty.

# Câu 4: Phân tích ưu và nhược điểm của hệ thống giám sát SIEM

Khái niệm:

Hệ thống giám sát an toàn thông tin (SIEM - security information and event managent) là hệ thống dực thiết kế nhằm thu thập thông tin nhật ký các sự kiện an ninh từ các thiết bị đầu cuối và phân tích chúng với mục đích phát hiện và kịp thời ứng phó, cho phép tổ chức hạn chế được các rủi ro, tiết kiệm thời gian và nhân lực.

Hệ thống giám sát SIEM (Security Information and Event Management) là một giải pháp quan trọng để giám sát và phát hiện các hoạt động bất thường trong hệ thống thông tin. Dưới đây là một số ưu và nhược điểm của hệ thống giám sát SIEM:

Ưu điểm:

* Phát hiện các sự cố bảo mật nhanh chóng: SIEM có thể giúp phát hiện các cuộc tấn công, virus, malware và các hoạt động bất thường trong hệ thống thông tin một cách nhanh chóng.
* Tích hợp dữ liệu từ nhiều nguồn: SIEM có thể kết nối và tích hợp dữ liệu từ nhiều nguồn khác nhau, bao gồm các bản ghi nhật ký, các sự kiện mạng và hệ thống, các ứng dụng và các thiết bị bảo mật.
* Tích hợp chức năng phân tích và báo cáo: SIEM có thể tự động phân tích dữ liệu để tìm ra các xu hướng và mô hình, và tạo ra các báo cáo để hỗ trợ việc giám sát và quản lý bảo mật.
* Hỗ trợ cho các chuẩn bảo mật: SIEM hỗ trợ các chuẩn bảo mật như PCI-DSS, HIPAA, ISO 27001 và NIST, giúp đảm bảo tuân thủ các yêu cầu bảo mật của ngành và quản lý bảo mật hiệu quả hơn.
* Tính linh hoạt cao: SIEM có thể tùy chỉnh để đáp ứng các yêu cầu cụ thể của từng doanh nghiệp, giúp tăng tính linh hoạt và khả năng tùy chỉnh của giải pháp.
* Tính toàn diện: Hệ thống giám sát SIEM có khả năng giám sát, phân tích và đưa ra cảnh báo về các sự kiện an ninh mạng từ nhiều nguồn khác nhau như bản ghi log, firewall, IDS, IPS, antivirus, hay các thiết bị khác trên hệ thống mạng. Nhờ đó, hệ thống giám sát SIEM giúp tăng tính toàn diện trong việc phát hiện các mối đe dọa an ninh mạng.
* Khả năng phân tích sâu: Hệ thống giám sát SIEM có khả năng phân tích sâu các sự kiện để đưa ra cảnh báo cho những sự kiện quan trọng nhất. Điều này giúp tối đa hóa khả năng phát hiện sớm các mối đe dọa đến an ninh mạng.
* Khả năng giám sát thời gian thực: Hệ thống giám sát SIEM có khả năng giám sát thời gian thực các sự kiện an ninh mạng, đưa ra cảnh báo và hỗ trợ cho các biện pháp phòng ngừa và ứng phó nhanh chóng khi có sự cố xảy ra.
* Khả năng tùy biến cao: Hệ thống giám sát SIEM có khả năng tùy biến cao, cho phép người dùng tự định nghĩa các quy tắc, tiêu chí để phát hiện các sự kiện an ninh mạng.

Nhược điểm:

* Chi phí cao: Hệ thống giám sát SIEM yêu cầu đầu tư ban đầu cao để triển khai và vận hành. Bên cạnh đó, chi phí cho các bản cập nhật, bảo trì và nâng cấp cũng có thể tăng lên theo thời gian.
* Khó khăn trong triển khai và cấu hình: SIEM là một giải pháp phức tạp, yêu cầu kỹ năng chuyên môn để triển khai và cấu hình. Điều này có thể tạo ra những khó khăn cho các tổ chức không có nhân lực hoặc kỹ năng phù hợp.
* Nhiễu loạn và thông tin lỗi thời: SIEM có thể tạo ra nhi ễu loạn trong quá trình thu thập dữ liệu, vì vậy các sự cố bảo mật không được phát hiện hoặc báo cáo chính xác. Ngoài ra, các thông tin cũng có thể lỗi thời hoặc không đầy đủ, do đó dẫn đến những sai sót trong quá trình phân tích và đưa ra các quyết định.
* Không phát hiện được các cuộc tấn công mới: SIEM phụ thuộc vào việc phân tích các mô hình và xu hướng hiện tại để phát hiện các hoạt động bất thường. Tuy nhiên, nó không thể phát hiện được các cuộc tấn công mới hoặc tinh vi mà chưa có trong cơ sở dữ liệu.
* Không thể giải quyết các vấn đề bảo mật một mình: SIEM chỉ là một phần trong việc quản lý bảo mật và không thể giải quyết được các vấn đề bảo mật một mình. Các tổ chức cần phải kết hợp nó với các giải pháp bảo mật khác để đảm bảo an toàn cho hệ thống thông tin của mình.

Tóm lại, hệ thống giám sát SIEM là một giải pháp quan trọng trong việc giám sát và phát hiện các hoạt động bất thường trong hệ thống thông tin. Tuy nhiên, nó cũng có một số nhược điểm như chi phí cao, khó khăn trong triển khai và cấu hình, nhiễu loạn và thông tin lỗi thời, không phát hiện được các cuộc tấn công mới và không thể giải quyết các vấn đề bảo mật một mình.

# Câu 5: Trình bày một số sản phẩm giám sát ATTT mà em biết

Khái niệm:

Hệ thống giám sát an toàn thông tin (SIEM - security information and event managent) là hệ thống dực thiết kế nhằm thu thập thông tin nhật ký các sự kiện an ninh từ các thiết bị đầu cuối và phân tích chúng với mục đích phát hiện và kịp thời ứng phó, cho phép tổ chức hạn chế được các rủi ro, tiết kiệm thời gian và nhân lực.

Có rất nhiều sản phẩm giám sát an toàn thông tin có sẵn trên thị trường hiện nay. Dưới đây là một số ví dụ:

* **Splunk Enterprise Security**: Là một giải pháp SIEM cho phép giám sát, phát hiện và phản ứng đối với các mối đe dọa bảo mật trên toàn bộ hệ thống thông tin của tổ chức.
* **McAfee Enterprise Security Manager**: Là một giải pháp SIEM chuyên nghiệp, cung cấp khả năng phát hiện và giải quyết các cuộc tấn công bảo mật, bao gồm cả các cuộc tấn công phức tạp và tinh vi.
* **SolarWinds Security Event Manager**: Là một giải pháp SIEM đơn giản và dễ sử dụng, cung cấp các tính năng như phát hiện đối tượng bất thường và cảnh báo an ninh.
* **IBM Security QRadar**: Là một giải pháp SIEM cho phép phát hiện và phản ứng đối với các mối đe dọa bảo mật, bao gồm cả các cuộc tấn công mới và tinh vi.
* **LogRhythm Security Intelligence Platform**: Là một giải pháp SIEM cung cấp khả năng phát hiện các hoạt động bất thường, đánh giá mức độ nguy hiểm và đưa ra các cảnh báo cho các nhân viên an ninh.
* **AlienVault USM**: Sản phẩm giám sát mạng và thông tin của AlienVault cung cấp khả năng phát hiện xâm nhập, giám sát mạng, quản lý sự kiện bảo mật và phân tích bảo mật.
* **RSA NetWitness**: Sản phẩm giám sát mạng và thông tin của RSA cung cấp khả năng phát hiện xâm nhập, giám sát mạng, quản lý sự kiện bảo mật và phân tích bảo mật.
* **Fortinet FortiSIEM**: Sản phẩm giám sát mạng và thông tin của Fortinet cung cấp khả năng phát hiện xâm nhập, giám sát mạng, quản lý sự kiện bảo mật và phân tích bảo mật
* **Cisco Stealthwatch**: Sản phẩm giám sát mạng của Cisco cung cấp khả năng giám sát mạng và phát hiện các mối đe dọa trên mạng thông qua phân tích lưu lượng mạng.
* **Wazuh Open Source Security Analytics**: được phát triển bởi công ty Wazuh Inc., nó cung cấp các tính năng như giám sát tệp tin, giám sát nhật ký, phát hiện xâm nhập, quản lý cấp phép, và giám sát hệ thống mạng

Ngoài ra, còn nhiều sản phẩm khác như AlienVault Unified Security Management, RSA NetWitness Platform, Micro Focus ArcSight, hay TrendMicro Deep Security. Tùy thuộc vào nhu cầu và yêu cầu của tổ chức, có thể chọn ra sản phẩm phù hợp để giám sát và bảo vệ hệ thống thông tin của mình.

# Câu 6: Kiến trúc và thành phần của hệ thống giám sát

Hệ thống giám sát SIEM gồm 3 phần chính:

Thành phần thu thập dữ liệu (Collector):

* Collector là thành phần thu thập dữ liệu từ các nguồn khác nhau trong hệ thống mạng. Các nguồn này bao gồm logs, events, packets, flows, … Collector có thể được đặt trên các thiết bị mạng, server, firewall, IDS/IPS hay các ứng dụng.
* Collector có chức năng thu thập dữ liệu liên tục và gửi nó đến thành phần phân tích và lưu trữ dữ liệu. Các thông tin thu thập được từ Collector đóng vai trò quan trọng trong việc phát hiện các mối đe dọa đến hệ thống mạng.

Thành phần phân tích và lưu trữ dữ liệu (Engine + Database) bao gồm hai thành phần chính:

* Correlation Engine (còn được gọi là Security Analytics Platform) là trung tâm của hệ thống SIEM, nơi dữ liệu thu thập từ Collector được xử lý và phân tích để tìm ra các mẫu hoạt động bất thường. Correlation Engine sử dụng các thuật toán phân tích dữ liệu và các quy tắc để đánh giá mức độ nghiêm trọng của các sự kiện, cảnh báo người quản trị khi phát hiện các hành động đe dọa hoặc tấn công vào hệ thống mạng.
* Database (hay còn gọi là Event Storage) là thành phần lưu trữ dữ liệu của hệ thống SIEM. Dữ liệu này bao gồm các logs, events, cảnh báo, thông tin về các hành động và các luồng dữ liệu. Database phải được thiết kế để hỗ trợ lưu trữ dữ liệu lớn và có thể truy vấn nhanh chóng.
* Thành phần phân tích và lưu trữ dữ liệu có chức năng phân tích các dữ liệu thu thập được từ Collector để tìm ra các mối đe dọa tiềm ẩn, đánh giá mức độ nghiêm trọng và lưu trữ dữ liệu.

Thành phần quản trị tập trung (Management) là nơi người quản trị có thể theo dõi và quản lý hệ thống SIEM. Thành phần này bao gồm:

* Dashboard: là giao diện người dùng cho phép người quản trị xem các cảnh báo và sự kiện quan trọng, các báo cáo thống kê và tình trạng của hệ thống SIEM.
* Alert Management: là thành phần cho phép người quản trị quản lý cảnh báo được phát hiện bởi hệ thống SIEM. Alert Management cho phép người quản trị xem và xác nhận các cảnh báo, giải thích nguyên nhân và thực hiện các hành động cần thiết để giải quyết các vấn đề.
* Rule Management: là thành phần cho phép người quản trị thiết lập các quy tắc để giám sát các sự kiện trên hệ thống mạng. Rule Management cũng cho phép người quản trị tùy chỉnh các quy tắc hiện có để đáp ứng nhu cầu của họ.
* User Management: là thành phần cho phép người quản trị quản lý tài khoản người dùng và quyền truy cập vào hệ thống SIEM. User Management cũng cung cấp các chức năng để giám sát và theo dõi hoạt động của người dùng trên hệ thống.
* Report Management: là thành phần cho phép người quản trị tạo các báo cáo về các sự kiện và hoạt động trên hệ thống mạng. Report Management cung cấp các công cụ để tạo và tùy chỉnh các báo cáo, giúp người quản trị hiểu rõ hơn về các mối đe dọa và hoạt động trên hệ thống mạng của họ.

Tóm lại, hệ thống giám sát SIEM có kiến trúc phân tán và bao gồm ba thành phần chính: Collector, Engine + Database và Management. Mỗi thành phần có các chức năng riêng biệt nhưng hoạt động cùng nhau để phát hiện và đánh giá các mối đe dọa và hoạt động bất thường trên hệ thống mạng.

# Câu 7: Phân tích một số chức năng quan trọng trong hệ thống giám sát

Hệ thống giám sát SIEM (Security Information and Event Management) có nhiều chức năng quan trọng giúp giải quyết các vấn đề bảo mật và đảm bảo an toàn thông tin trên hệ thống mạng. Dưới đây là một số chức năng quan trọng trong hệ thống giám sát SIEM:

* Data aggregation: Chức năng này giúp hệ thống SIEM thu thập các dữ liệu từ nhiều nguồn khác nhau như các thiết bị mạng, hệ thống ứng dụng, log file, hệ thống điều khiển truy cập,... để đưa về một trung tâm quản lý dữ liệu, giúp người quản trị dễ dàng quản lý và phân tích dữ liệu.
* Threat Intelligence Feeds: Chức năng này cung cấp thông tin về các mối đe dọa bảo mật mới nhất, các chuỗi tấn công và các thông tin tình báo bảo mật. Nó cho phép hệ thống SIEM phát hiện và phản ứng nhanh chóng trước các mối đe dọa mới nhất.
* Correlation: Chức năng này cho phép hệ thống SIEM phân tích các dữ liệu thu thập được để tìm ra các kết nối, quan hệ giữa các sự kiện và các hành vi bất thường, giúp xác định các tấn công mạng.
* Analytics: Chức năng này cho phép hệ thống SIEM áp dụng các thuật toán phân tích dữ liệu để phát hiện các hành vi bất thường, các hoạt động nghi ngờ và các tấn công mạng tiềm ẩn.
* Alerting: Chức năng này thông báo cho người quản trị khi có các sự kiện bất thường xảy ra trên hệ thống mạng, giúp họ phản ứng nhanh chóng và ngăn chặn các tấn công mạng.
* Dashboard: Chức năng này hiển thị các dữ liệu quan trọng như các sự kiện, các tấn công mạng, các hành vi bất thường và các thông tin bảo mật khác trên một giao diện đồ họa, giúp người quản trị dễ dàng quản lý và theo dõi các tình trạng bảo mật trên hệ thống mạng.
* Compliance: Chức năng này đảm bảo hệ thống SIEM tuân thủ các tiêu chuẩn bảo mật quy định, giúp các tổ chức đáp ứng các yêu cầu về bảo mật thông tin và tuân thủ các quy định về an ninh thông tin.
* Log Retention: Chức năng này giúp hệ thống SIEM lưu trữ các dữ liệu thu thập được trong một kho lưu trữ dữ liệu lâu dài, giúp người quản trị dễ dàng truy cập và tìm kiếm các thông tin quan trọng khi cần thiết.
* Forensic Analysis: Chức năng này cho phép hệ thống SIEM thu thập và lưu trữ các dữ liệu về các sự kiện bảo mật, các tấn công mạng và các hành vi bất thường. Nó cũng cho phép phân tích sâu các sự kiện bằng các công cụ phân tích, giúp phát hiện và phân tích các vấn đề bảo mật trên hệ thống mạng.
* Threat Hunting: Chức năng này cho phép người quản trị tìm kiếm các mối đe dọa bảo mật tiềm ẩn và các tấn công mạng mà hệ thống SIEM chưa phát hiện được. Nó cung cấp cho người quản trị các công cụ và kỹ thuật để phân tích các dữ liệu bảo mật và tìm ra các hoạt động bất thường trên hệ thống mạng.
* Incident Response: Chức năng này cho phép hệ thống SIEM tự động phản ứng và ngăn chặn các tấn công mạng khi xảy ra. Nó cung cấp cho người quản trị các công cụ để xử lý các vấn đề bảo mật và giúp họ giảm thiểu thiệt hại khi có các sự kiện bảo mật xảy ra.
* SOC Automation: Chức năng này cho phép tự động hóa các tác vụ trong quá trình quản lý và giám sát bảo mật trên hệ thống mạng, giúp giảm thiểu sự phụ thuộc vào con người trong quá trình giám sát và xử lý các vấn đề bảo mật. Nó cung cấp cho người quản trị các công cụ để quản lý và tự động hóa các quy trình, giúp tăng tính hiệu quả và giảm thiểu rủi ro.

Trên đây là một số chức năng quan trọng trong hệ thống giám sát SIEM. Việc triển khai và sử dụng hệ thống SIEM đòi hỏi sự hiểu biết sâu rộng về các thành phần, các tính năng và các kỹ thuật liên quan đến an ninh mạng. Các chuyên gia an ninh mạng và các nhà quản trị mạng cần phải hiểu rõ về hệ thống SIEM và cách sử dụng nó để đảm bảo an toàn và bảo mật cho hệ thống mạng của mình.

# Câu 8: Các loại dữ liệu đầu vào của hệ thống giám sát

Hệ thống giám sát SIEM sử dụng nhiều nguồn dữ liệu đầu vào khác nhau để thu thập thông tin về các sự kiện bảo mật trên hệ thống mạng. Các loại dữ liệu đầu vào chính của hệ thống giám sát SIEM bao gồm:

* Full content data: Đây là các dữ liệu đầy đủ về nội dung các gói tin truyền tải trên mạng, bao gồm cả nội dung văn bản, hình ảnh, âm thanh, video và các tệp đính kèm. Dữ liệu này được sử dụng để phân tích chi tiết về các sự kiện bảo mật trên mạng.
* Extracted content: Đây là các dữ liệu đã được trích xuất từ full content data, bao gồm các thông tin cụ thể về các sự kiện bảo mật trên mạng, ví dụ như các địa chỉ IP, cổng, giao thức, địa chỉ MAC, các mã độc và các tệp tin độc hại.
* Session data: Đây là các dữ liệu liên quan đến các phiên truy cập trên mạng, bao gồm các thông tin về người dùng, địa chỉ IP, thời gian, các giao thức và cổng sử dụng trong phiên truy cập đó.
* Transaction data: Đây là các dữ liệu liên quan đến các giao dịch trên mạng, bao gồm các thông tin về các giao dịch tài chính, các giao dịch mua bán trực tuyến và các giao dịch khác.
* Statistical data: Đây là các dữ liệu thống kê liên quan đến các hoạt động trên mạng, bao gồm các thông tin về lưu lượng mạng, thời gian hoạt động, tần suất truy cập, số lượng kết nối và các chỉ số khác.
* Alert/log data: Đây là các dữ liệu liên quan đến các thông báo cảnh báo và tệp log được tạo ra bởi các thiết bị bảo mật và mạng, bao gồm các thông tin về các sự kiện bảo mật, lỗi hệ thống và các hoạt động quản trị hệ thống.

Các loại dữ liệu đầu vào này được thu thập và phân tích để giúp hệ thống giám sát mạng và bảo mật phát hiện các sự kiện bảo mật đáng ngờ và giúp nhân viên SOC đưa ra các biện pháp phòng chống và xử lý các sự cố bảo mật trên hệ thống mạng.

# Câu 9: Phương pháp thu thập dữ liệu của hệ thống giám sát

Các phương pháp thu thập dữ liệu phổ biến là: hubs,span/mirror ports,taps ngoài ra còn có phương pháp Pull và Push

**Hubs**

hub là một thiết bị mạng cơ bản được sử dụng để kết nối các thiết bị mạng với nhau.

Hub hoạt động như một trung tâm chuyển tiếp dữ liệu giữa các thiết bị mạng, cho phép chúng giao tiếp với nhau thông qua giao thức mạng

là một nơi tập trung các dữ liệu được thu thập từ nhiều nguồn khác nhau. Các nguồn dữ liệu có thể bao gồm các trang web, ứng dụng, cơ sở dữ liệu, tệp tin, hoặc các thiết bị đo lường và cảm biến

Ưu điểm:

* Giá thành thấp
* Dễ dàng sử dụng
* Nhược điểm

Nhược điểm:

* Hạn chế tốc độ truyền dữ liệu (Hubs hoạt động ở half duplex sẽ làm giảm hiệu suất xuống 100 mbps)
* Dễ gây ra xung đột mạng, khi Hubs bị sự cố sẽ dẫn đến việc kết nối bị ngắt

**Span/mirror ports**

SPAN Port là một tính năng của một switch mạng, cho phép các gói tin mạng được sao chép (hay "chụp") và chuyển đến một cổng (port) khác để được giám sát hoặc phân tích.

Các gói tin được sao chép từ các cổng vào (ingress) hoặc ra (egress) của switch và chuyển đến một cổng được cấu hình là cổng SPAN. Các cổng này được sử dụng để kết nối đến một máy chủ giám sát (monitoring server) hoặc một thiết bị phân tích (analysis device) để phân tích các dữ liệu gói tin đó.

Tính năng SPAN Port là rất hữu ích trong các môi trường mạng khi cần phân tích hoặc giám sát lưu lượng mạng

Ưu điểm:

* Tích hợp sẵn trên hầu hết các switch
* Chi phí tương đối rẻ (60$ - SOHO D-link 8 port gigabit)
* Có khả năng chuyển dữ liệu ở chế độ full duplex

Nhược điểm:

* Việc cấu hình SPAN port khá phức tạp
* Có thể xảy ra tình trạng mất gói khi cấu hình Mirror ports vì dữ liệu được gửi đến cổng giám sát cao hơn so với khả năng của cổng
* Loại bỏ nhãn VLAN của gói tin, làm cho việc phân tích VLAN khó khăn hơn
* Một số nhà sx chỉ cung cấp khả năng cấu hình cho một hoặc hai cổng giám sát
* Gây quá tải cho switch, ảnh hưởng đến hoạt động của mạng

**Network TAPs**

TAP là thiết bị dùng để sao chép dữ liệu giữa hai điểm trên hệ thống mạng (router-firewall, switch-switch, host-switch…)

Tất cả các gói tin được sao chép sẽ chuyển đến cổng giám sát

Đây là giải pháp tiên tiến nhất, kết hợp các ưu điểm của Hub và Mirror ports

Ưu điểm:

* Có khả năng chuyển tiếp được các lỗi tầng vật lý
* Không cần phải cấu hình, dễ dàng kết nối
* Hỗ trợ tối đa khả năng sao chép dữ liệu ở tốc độ cao
* Độ trễ giữa các gói tin được giữ nguyên, hỗ trợ cho quá trình phân tích gói
* Không ảnh hưởng đến hiệu suất của switch

Nhược điểm:

* Kết nối bị ngắt khi thi công, lắp đặt
* Chi phí cao hơn so với Hubs và Mirroring port

**Phương pháp kéo (Pull Method)**

Các sự kiện được phát sinh và lưu trữ trên chính các thiết bị sẽ được lấy về bởi các bộ Collector.

**Phương pháp đẩy (Push Method)**

Các sự kiện từ các thiết bị, máy trạm, máy chủ… sẽ được tự động chuyển về các Collector theo thời gian thực hoặc sau mỗi khoảng thời gian phụ thuộc vào việc cấu hình trên các thiết bị tương ứng.

Collector của Log Server sẽ thực hiện việc nghe và nhận các sự kiện khi chúng xảy ra.

# Câu 10: Lập kế hoạch thu thập dữ liệu theo Khung ACF (Applied Collection Framework)

ACF là khungg làm việc được xây dựng để làm giảm sự phức tạp của việc thu thập dữ liệu. Giúp tổ chức đánh giá các nguồn dữ liệu cần tập trung trong quá trình thu thập dữ liệu. Nó gồm 4 giai đoạn sau:

**Xác định nguy cơ:**

Trước tiên, cần xác định các nguy cơ an ninh mạng có thể xảy ra trong tổ chức. Các nguy cơ này có thể được xác định từ các tài liệu về an ninh mạng, các sự cố bảo mật trước đây, hoặc bằng cách tạo một danh sách các cuộc tấn công phổ biến.

Các nguy cơ thường tác động đến 3 tính chất: Tính bảo mật, tính toàn vẹn và tính sẵn sàng.

Từ những nguy cơ đã xác định được chúng ta sẽ thấy được các kỹ thuật và công nghệ cần sử dụng để giải quyết các nguy cơ đó như: Máy chủ web (web server), Máy chủ cơ sở dữ liệu ( Database server), Máy chủ lưu trữ tệp tin (File server),…

**Định lượng rủi ro:**

Khi xác định được một danh sách các nguy cơ, cần xác định xem nguy cơ nào cần được ưu tiên

Thực hiện bằng cách tính toán rủi ro gây ra bởi các nguy cơ tiềm ẩn:

***Ảnh hưởng (I) \* Xác suất (P) = Rủi ro (R)***

* Ảnh hướng là tác động của nguy cơ đến tổ chức
* Xác suất là khả năng nguy cơ xuất hiện
* Mức độ rủi ro mà nguy cơ gây ra đối với sự an toàn của mạng

**Xác định nguồn dữ liệu**

Đi từ nguy cơ có hệ số rủi ro cao nhất và xem xét khả năng có ther bị khai thác

Ví dụ: để kiểm tra nguy cơ tấn công máy chủ lữu trữ tệp tin cần:

* Xác định cấu trúc của máy chủ
* Vị trí trên mạng
* Người có quyền truy cập
* Đường dẫn mà dữ liệu đi vào

Dựa vào đó để kiểm tra cả 2 nguồn dữ liệu dựa trên mạng và dựa trên máy chủ

**Chọn lọc dữ liệu**

Liên quan đến các bước kỹ thuật chiều sâu và cần phải xem xét tất cả các nguồn dữ liệu riêng để xác định giá trị của nó.

* Ví dụ: Chi phí co việc lưu trữ, xử lý và quản lý một nguồn dữ liệu có thể lớn hơn nhiều so với giá trị mà nó mang lại, thì đó không phải là nguồn dữ liệu tốt

Cần phân tích chi phí/lợi ích của các nguồn dữ liệu

* Tài nguyên phần cứng, phần mềm, nhân công, việc tổ chức và lưu trữ dữ liệu,…
* Số lượng dữ liệu và thời gian lưu trữ dữ liệu
* Cần phải giảm tối thiểu chi phí lưu trữ dữ liệu và tăng tối đa độ quan tâm về dữ liệu hữu ích dùng trong việc phân tích

Trên cơ sở đố, xây dựng cơ ở hạ tầng thích hợp cho việc thu thập dữ liệu

Dữ liệu liên tục được thu thập, được sử dụng ho phát hiện xâm nhập và phân tích theo sự phát triển hệ thống mạng của tổ chức, và sẽ luôn cần phải xem xét lại chiến lược thu thập dữ liệu

# Câu 11: Phương pháp phân tích dữ liệu

**\*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

**\*Chuẩn đoán khác biệt:**

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

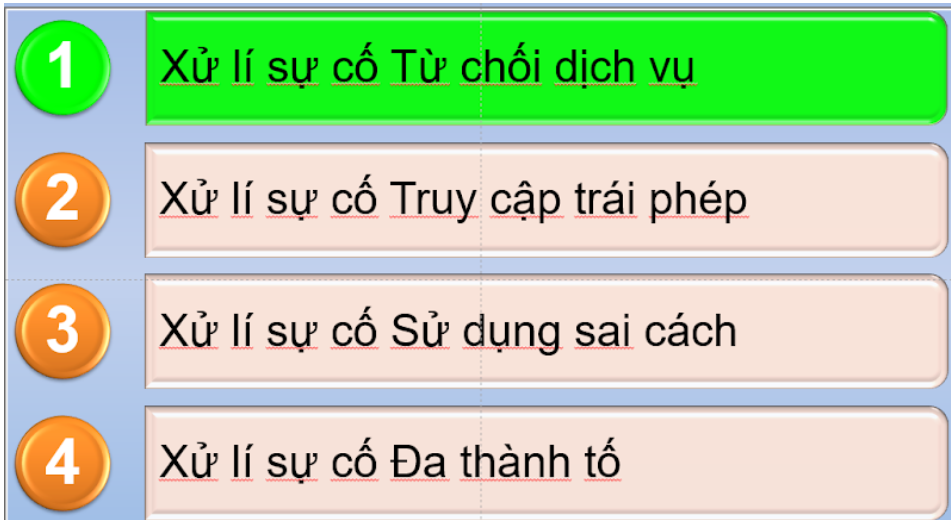
**Bước 2: xem xét và đnáh giá chuẩn đoán phổ biến nhất đầu tiền**

**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**

# Câu 12: Lấy ví dụ và phân tích một số sự cố ATTT



1. **Xử lí sự cố Từ chối dịch vụ**

Tấn công từ chối dịch vụ (DoS) ngăn chặn người dùng có quyền được truy cập hệ thống, mạng hoặc các ứng dụng bằng cách làm nghẽn tài nguyên mạng

Dấu hiệu của một cuộc tấn công DoS trên mạng:

* Báo cáo của người dùng về việc không thể truy cập hệ thống và dịch vụ
* Mất kết nối không xác định
* Cảnh báo từ hệ thống phát hiện xâm nhập mạng …

Chuẩn bị xử lý sự cố cho DoS:

* Liên hệ các nhà cung cấp dịch vụ Internet (ISP) và các đại lý cấp 2 của họ để xác định cách họ có thể giúp xử lý cuộc tấn công DoS trên mạng
* Liên hệ các tổ chức như CERT và Trung tâm Khiếu nại tội phạm Internet (IC3) để được giúp đỡ xử lý cuộc tấn công DoS
* Cấu hình và triển khai Hệ thống Phát hiện Xâm nhập (IDS) và phần mềm phòng ngừa để phát hiệu lưu lượng DoS
* Thực hiện giám sát tài nguyên đang tiêu thụ để thiết lập sử dụng băng thông mạng
* Kiểm tra các trang web cung cấp số liệu về độ trễ giữa các ISP khác nhau và giữa các địa chỉ vật lý khác nhau, hay còn gọi là giám sát sức khoẻ Internet …

Chiến lược phản hồi DoS:

* Hấp thụ tấn công
* Giảm tải dịch vụ
* Tắt các dịch vụ

Ngăn chặn sự cố DoS:

* Cấu hình mạng sao cho chặn toàn bộ lưu lượng dịch vụ đến và đi không cần thiết
* Hạn chế một số giao thức như ICMP chỉ được sử dụng một tỷ lệ băng thông nhất định
* Thực hiện dự phòng cho các chức năng chính

1. **Truy cập trái phép**

Truy cập trái phép nghĩa là khi một người truy cập vào hệ thống hoặc tài nguyên mạng mà không có quyền tương ứng

Ví dụ về truy cập trái phép:

* + Thực hiện nâng quyền (rooting) từ xa đến máy chủ email
  + Thay đổi nội dung máy chủ web
  + Đoán hoặc bẻ khoá mật khẩu ứng dụng
  + Sao chép dữ liệu nhạy cảm mà không có quyền
  + Cài đặt và chạy chương trình nghe lén trên máy trạm
  + Sử dụng máy chủ FTP để truyền bá tệp tin nhạc và phần mềm lậu.
  + Truy cập mạng nội bộ bằng cách kết nối tới modem không bảo mật.
  + Truy cập máy trạm sử dụng ID giả.

Dấu hiệu nhận biết máy chủ bị xâm hại trái phép:

* Phát hiện những công cụ hoặc lỗ hổng đáng ngờ
* Lưu lượng mạng bất thường
* Thay đổi cấu hình hệ thống ví dụ: service, port, interface, …
* Thay đổi dữ liệu trái phép
* Sử dụng trái phép tài khoản của người dùng chuẩn

Chuẩn bị xử lý sự cố:

* Cấu hình IDPS cho mạng và máy chủ để phát hiện và cảnh báo nỗ lực truy cập trái phép
* Sử dụng máy chủ nhật ký tập trung để các thông tin quan trọng từ máy chủ trên toàn tổ chức được lưu trữ trong vị trí an toàn cụ thể
* Chính sách mật khẩu tốt được áp dụng cho toàn bộ người dùng ứng dụng, hệ thống, domain tin cậy hoặc tổ chức
* Cho quản trị viên hệ thống nhận thức được trách nhiệm của họ trong việc xử lý các sự cố truy cập trái phép

Ngăn chặn sự cố:

* An ninh mạng: Di chuyển tất cả các hệ thống và dịch vụ công khai sang vùng DMZ đã được đảm bảo an toàn, …
* Bảo mật máy chủ: Chạy các dịch vụ với đặc quyền thấp nhất có thể nhằm giảm tải thiệt hại khi bị khai thác thành công, …
* Xác thực và phân quyền:
* Chuẩn bị chính sách mật khẩu thích hợp
* Cần yêu cầu xác thực mạnh để truy cập các tài nguyên quan trọng
* Tạo các tiêu chuẩn xác thực và ủy quyền cho nhân viên và nhà thầu tuân theo khi đánh giá hoặc phát triển phần mềm
* Thiết lập các thủ tục cấp phép và hủy cấp phép tài khoản người dùng

1. **Xử lí sự cố Sử dụng sai cách**

Sự cố sử dụng sai cách xảy ra khi người dùng thực hiện các hành động vi phạm đến chính sách sử dụng máy tính (hành vi không được chấp nhận)

Ví dụ:

* Cài đặt công cụ bẻ khóa mật khẩu
* Tải xuống tài liệu khiêu dâm
* Gửi thư rác quảng cáo công việc kinh doanh cá nhân
* Gửi email gây khó chịu cho đồng nghiệp
* Lưu trữ các trang web trái phép trên máy tính của công ty
* Sử dụng các dịch vụ chia sẻ để phân phối hoặc mua các tài liệu vi phạm bản quyền
* Gửi dữ liệu quan trọng ra bên ngoài công ty

Các trường hợp sử dụng sai cách liên quan tới các tổ chức bên ngoài có thể gây ra nhiều tổn thất hơn cho tổ chức dưới dạng thiệt hại về danh tiếng và tính pháp lý.

**Phát hiện sự cố truy cập không phù hợp**

Trường hợp sử dụng dịch vụ trái phép:

* + Cảnh báo từ hệ thống phát hiện xâm nhập
  + Lưu lượng mạng thất thường
  + Cài đặt phần mềm mới trên máy tính
  + Tạo các tệp hoặc thư mục mới có tên bất thường
  + Tăng mức sử dụng tài nguyên
  + Báo cáo từ người dùng
  + Các mục nhật ký của ứng dụng

Trường hợp tiếp cận các tài liệu sai cách:

* + Cảnh báo từ hệ thống phát hiện xâm nhập
  + Báo cáo từ người dùng
  + Các mục nhật ký của ứng dụng
  + Các tệp bất thường trên máy tính, máy chủ và trên phương tiện di động

Trường hợp tấn công tổ chức bên ngoài:

* + Cảnh báo từ hệ thống phát hiện xâm nhập
  + Báo cáo từ tổ chức bên ngoài
  + Các mục nhật ký của mạng, máy chủ và ứng dụng

**Chuẩn bị xử lý sự cố:**

* Xây dựng các chính sách bảo mật phối hợp với bộ phận nhân sự và đại diện bộ phận pháp lý để xử lý các sự cố sử dụng không hợp lệ
* Thảo luận với thành viên của nhóm bảo mật vật lý của tổ chức về hành vi của người dùng nội bộ
* Trao đổi với người có liên quan của bộ phận pháp lý về vấn đề trách nhiệm pháp lý, đặc biệt là đối với những loại sự cố nhắm vào các tổ chức bên ngoài
* Cài đặt IDS, phần mềm lọc nội dung email, các công cụ kiểm soát bảo mật để xác định các loại hoạt động nhất định
* Thiết lập nhật ký hoạt động người dùng như lệnh FTP, truy vấn web, header email

**Khuyến nghị:**

* Trao đổi với bộ phận nhân sự và đại diện bộ phận pháp lý để thảo luận về việc xử lý các sự cố sử dụng sai cách
* Trao đổi với đại diện bộ phận pháp lý của tổ chức để thảo luận về các vấn đề trách nhiệm pháp lý
* Cài đặt IDS để phát hiện một số kiểu sử dụng sai cách
* Thiết lập nhật ký hoạt động của người dùng
* Thiết lập bộ lọc cho máy chủ email để ngăn chuyển tiếp thư trái phép
* Sử dụng phần mềm lọc thư rác để lọc thư rác trên máy chủ email
* Cài đặt phần mềm lọc URL

1. **Xử lí sự cố Đa thành tố**

Là sự cố nhiều thành phần bao gồm sự kết hợp của hai hoặc nhiều cuộc tấn công trong một hệ thống

Ví dụ của sự cố nhiều thành phần:

* + Tấn công mã độc bằng cách sử dụng email
  + Máy trạm và máy chủ khác cùng hệ thống bị lây nhiễm bởi mã độc của kẻ tấn công
  + Máy trạm bị lây nhiễm này có thể được sử dụng để khởi động cuộc tấn công DDoS tới tổ chức khác

**Chuẩn bị cho nhiều sự cố thành phần:**

* Phần mềm IDS và ghi nhật ký trung nên được sử dụng để phân tích sự cố
* Yêu cầu nhóm xử lý sự cố xem xét các tình huống liên quan đến các sự cố thành phần
* Rất khó để phân tích các sự cố đa thành tố, vì người xử lý sự cố có thể không biết rằng sự cố bao gồm nhiều giai đoạn
* Khi tất cả các tiền chất và điểm báo đều có thể truy cập được từ một điểm duy nhất, thì người xử lý sự cố phải xem xét đó có phải sự cố đa thành tố hay không.

**Tuân theo Chiến lược ngăn chặn để ngăn chặn nhiều sự cố thành phần**

* Bất kỳ sự cố nào cũng có thể là sự cố đa thành tố. Do đó quy trình xử lý sự cố không nên dừng lại sau khi phát hiện dấu hiệu của một sự cố cụ thể
* Việc khám phá và chứa đựng tất cả các thành phần của một sự cố đòi hỏi thời gian và nỗ lực
* Những người xử lý giỏi và có kinh nghiệm có thể đoán được sự cố có các thành phần khác hay không

**Khuyến nghị**

* Sử dụng nhật ký tập trung và phần mềm liên kết sự kiện
* Tìm kiếm dấu hiệu trong các bộ phận khác sau khi kiểm soát sự cố
* Ưu tiên việc phân tách và kiểm soát từng thành phần của sự cố

# Câu 13: Vai trò của ứng phó sự cố trong đảm bảo ATTT

Ứng phó sự cố là một quá trình ứng phó với các sự cố có thể đã xảy ra do vi phạm bảo mật trong hệ thống hoặc mạng

Mục tiêu của ứng phó sự cố là xử lý các sự cố theo cách giảm thiểu thiệt hại, giảm thời gian và chi phí khắc phục

Nó đóng một vai trò quan trọng khi bảo mật của hệ thống bị xâm phạm

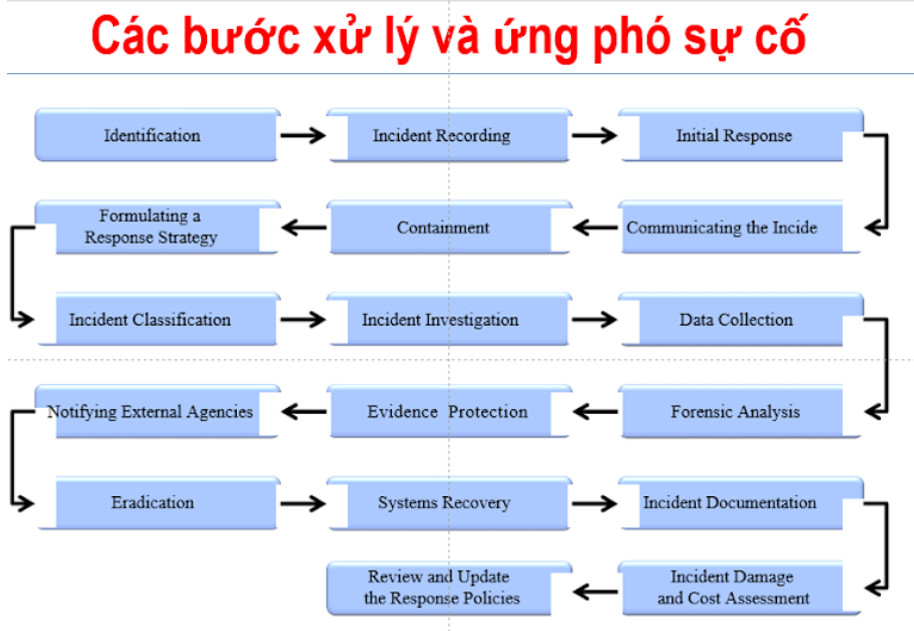
Vai trò của ứng phó sự cố trong đảm bảo an toàn thông tin:

* Đảm bảo tính sẵn sàng: Ứng phó sự cố giúp đảm bảo tính sẵn sàng cho hệ thống thông tin. Điều này có nghĩa là khi có sự cố xảy ra, hệ thống có thể nhanh chóng phát hiện, giải quyết và khôi phục lại hoạt động bình thường một cách nhanh chóng.
* Phát hiện các mối đe dọa: Ứng phó sự cố giúp phát hiện các mối đe dọa mới và các cuộc tấn công tiềm ẩn trong hệ thống. Điều này giúp các chuyên gia bảo mật có thể phản ứng kịp thời để giảm thiểu thiệt hại.
* Xử lý các sự cố bảo mật: Ứng phó sự cố giúp giảm thiểu thời gian phản ứng khi có các sự cố bảo mật xảy ra. Các nhân viên chuyên trách an ninh mạng có thể nhanh chóng ứng phó với các sự cố bảo mật, giảm thiểu thiệt hại cho hệ thống.
* Cải thiện khả năng phục hồi: Ứng phó sự cố giúp cải thiện khả năng phục hồi của hệ thống thông tin. Sau khi xử lý sự cố, hệ thống sẽ được khôi phục lại hoạt động bình thường trong thời gian ngắn nhất có thể.
* Đảm bảo tuân thủ các quy định và chính sách bảo mật: Ứng phó sự cố giúp đảm bảo tuân thủ các quy định và chính sách bảo mật. Các nhân viên chuyên trách an ninh mạng sẽ giám sát và xử lý các sự cố để đảm bảo rằng hệ thống luôn tuân thủ các quy định và chính sách bảo mật.
* Giảm thiểu tác động của sự cố: Sau khi sự cố đã xảy ra, ứng phó sự cố cho phép tổ chức giảm thiểu tác động của sự cố đối với hệ thống hoạt động và tổng thể của tổ chức.
* Khắc phục sự cố: Ứng phó sự cố giúp tổ chức khắc phục sự cố nhanh chóng và hiệu quả, giải quyết vấn đề và đưa hệ thống hoạt động trở lại bình thường một cách an toàn và nhanh chóng.
* Kiểm tra và đánh giá: Sau khi sự cố đã được giải quyết, ứng phó sự cố giúp tổ chức kiểm tra và đánh giá các chính sách, quy trình và hệ thống của mình, đồng thời xây dựng các kế hoạch cải tiến để cải thiện và nâng cao khả năng ứng phó sự cố trong tương lai.

Tóm lại, ứng phó sự cố rất quan trọng trong việc đảm bảo an toàn thông tin. Nó giúp đảm bảo tính sẵn sàng, phát hiện các mối đe dọa, xử lý các sự cố bảo mật, cải thiện khả năng phục hồi và đảm bảo tuân thủ các quy định và

# Câu 14: Các bước ứng phó sự cố ATTT

***GG làm:***



**B1. Xác định và phân loại sự cố**:

Giai đoạn xác định bao gồm xác nhận, xác định và báo cáo sự cố. Điều này liên quan đến việc thu thập thông tin về vụ việc, chẳng hạn như bản chất, mức độ nghiêm trọng và phạm vi của nó. Bước này giúp xác định phản ứng thích hợp và các nguồn lực cần thiết để giải quyết sự cố.

**B2. Ngăn chặn sự cố**

Bước tiếp theo là ngăn chặn sự cố để ngăn chặn thiệt hại thêm. Điều này có thể liên quan đến việc ngắt kết nối các hệ thống bị ảnh hưởng khỏi mạng, tắt các hệ thống bị ảnh hưởng hoặc thực hiện các biện pháp khác để cô lập sự cố

**B3. Điều tra sự cố**

Sau khi xử lý sự cố, cần tiến hành điều tra để xác định nguyên nhân sự cố và mức độ thiệt hại. Điều này có thể liên quan đến việc phân tích nhật ký, phỏng vấn nhân chứng và kiểm tra các hệ thống bị ảnh hưởng.

**B4. Thông báo cho các bên liên quan**

Sau khi điều tra hoàn tất, các bên liên quan sẽ được thông báo về vụ việc. Điều này có thể bao gồm nhân viên, khách hàng và các bên khác có thể đã bị ảnh hưởng bởi sự cố.

**B5. Khắc phục sự cố**

Bước tiếp theo là khắc phục sự cố. Điều này có thể liên quan đến việc vá các lỗ hổng, khôi phục dữ liệu từ bản sao lưu hoặc thực hiện các biện pháp khác để giải quyết nguyên nhân của sự cố và ngăn sự cố xảy ra lần nữa.

**B6. Theo dõi và xem xét**

Sau khi sự cố đã được khắc phục, điều quan trọng là phải theo dõi hệ thống xem có bất kỳ dấu hiệu tái diễn nào không. Điều này có thể liên quan đến việc triển khai các biện pháp bảo mật bổ sung, chẳng hạn như hệ thống phát hiện xâm nhập và xem xét các chính sách và thủ tục để xác định các lĩnh vực cần cải thiện.

**B7. Ghi lại sự cố**

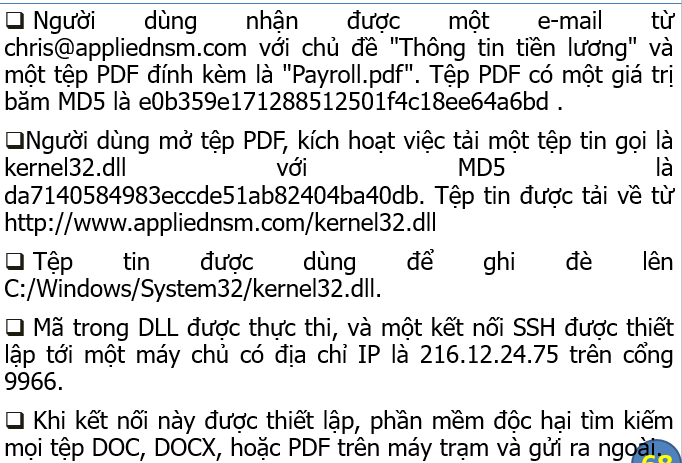
Cuối cùng, sự cố nên được ghi lại để tham khảo trong tương lai. Điều này có thể bao gồm một báo cáo chi tiết về sự cố, bao gồm nguyên nhân, tác động và cách ứng phó, cũng như bất kỳ thay đổi nào được thực hiện đối với các chính sách và thủ tục để ứng phó với sự cố.

***Chat làm:***

* Định danh và phân loại sự cố: Bước này nhằm mục đích xác định sự cố đang xảy ra là gì, phân loại nó theo độ ưu tiên và mức độ nghiêm trọng. Nó đóng vai trò quan trọng trong việc giúp cho đội ngũ ứng phó nhanh chóng xác định tài nguyên cần thiết để xử lý sự cố.
* Phân tích và đánh giá: Bước này đưa ra các giải pháp để giải quyết sự cố. Nó bao gồm việc phân tích và đánh giá các tác động của sự cố đến hệ thống và các tài nguyên liên quan, đánh giá mức độ tổn thất có thể gây ra và xác định các giải pháp khắc phục sự cố.
* Ứng phó và xử lý: Bước này thực hiện các giải pháp đã được xác định ở bước trước để giải quyết sự cố. Nó bao gồm các hoạt động như phục hồi, khôi phục hệ thống và các tài nguyên, giám sát các tác động của sự cố đến hệ thống và các tài nguyên liên quan, xác nhận rằng sự cố đã được giải quyết và trả lời cho các vấn đề liên quan đến việc xử lý sự cố.
* Theo dõi và đánh giá: Bước này là để đảm bảo rằng sự cố đã được giải quyết đúng cách và đánh giá các biện pháp phòng ngừa cho những sự cố tương tự trong tương lai. Nó bao gồm giám sát các chỉ số liên quan đến an ninh mạng, phát hiện các bất thường mới và cập nhật các giải pháp ứng phó sự cố.
* Tổng kết và báo cáo: Bước này là để tổng hợp các thông tin liên quan đến sự cố và đưa ra báo cáo cho các bên liên quan. Nó giúp cho các bên có thể nắm bắt được tình trạng an ninh mạng và có các giải pháp phòng ngừa, đảm bảo an ninh mạng được đẩy lên một tầm cao mới.

**BÀI TẬP**

# Dạng 1: Bài tập về tính toán dấu hiệu xâm nhập IOC.



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

# Dạng 2: Bài tập về lập kế hoạch thu thập dữ liệu.

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.

# Dạng 3: Bài tập về phân tích dữ liệu

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

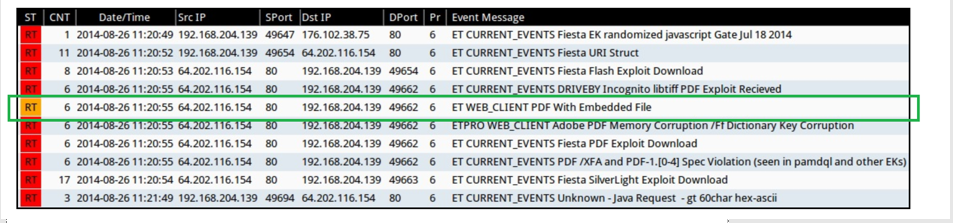
* Xác định các đối tượng thứ cấp
* Xác định mối quan hệ giữa các đối tượng thứ cấp và đối tượng chính

**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

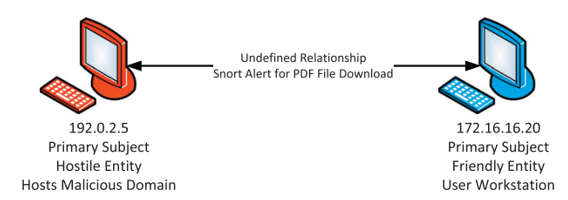
***\*Ví dụ:***



***\*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

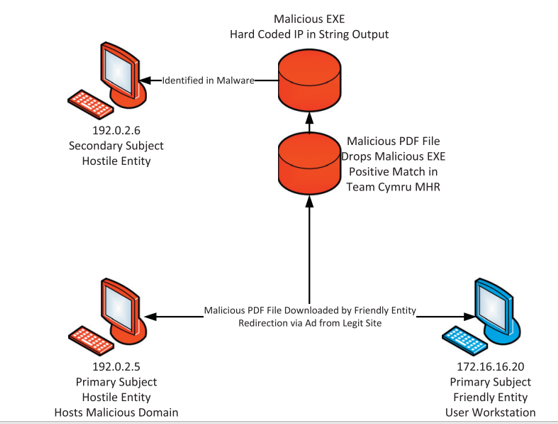
* Máy trạm của người dùng đang chạy Win 7
* Hệ thống không mở các dịch vụ nào cả
* Người dùng hệ thống này thường lướt web

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

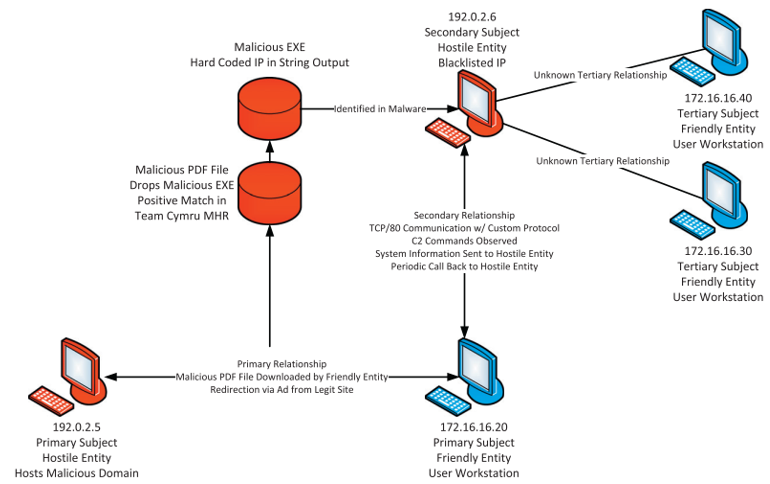
**Bước 2:**

* 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



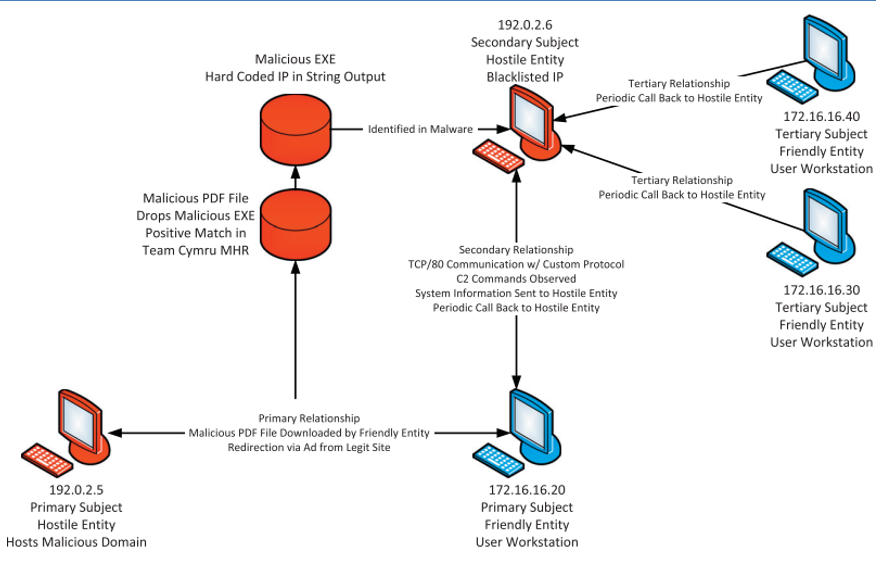
**Bước 3:**

* 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

# Dạng 4: Bài tập về ứng phó sự cố ATTT.

**\*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.