Logo, company name

Description automatically generated

**VNCERT/CC**

**Tìm Hiểu Về Các Khái Niệm Về Giám Sát**

**MỤC LỤC**

[I. HOẠT ĐỘNG GIÁM SÁT 2](#_Toc126801344)

[II. RÀ SOÁT CẤU HÌNH BẢO MẬT 6](#_Toc126801345)

[III. PHÒNG CHỐNG MÃ ĐỘC 12](#_Toc126801346)

[IV. SĂN LÙNG MỐI NGUY HẠI 16](#_Toc126801347)

[V. HUẤN LUYỆN DIỄN TẬP 19](#_Toc126801348)

# HOẠT ĐỘNG GIÁM SÁT

1. **Hoạt động giám sát là gì?**

* Hoạt động giám sát là quá trình theo dõi, đo lường và đánh giá mức độ hoạt động của mạng, hệ thống, thiết bị và phần mềm bằng cách sử dụng các công cụ, phần mềm và thiết bị. Mục tiêu của hoạt động hệ thống giám sát là đảm bảo mạng hoạt động an toàn, hiệu quả, không bị giật lag. Giúp phát triển và giải quyết sớm các sự cố trong mạng, giúp quản lý tài nguyên mạng hiệu quả hơn.

1. **Tại sao việc giám sát là quan trọng?**

* Bảo mật mạng: Giám sát mạng giúp phát hiện và đề phòng các cuộc tấn công mạng, giúp bảo vệ dữ liệu và hệ thống mạng.
* Giảm sự cố: Giám sát mạng giúp phát hiện và giải quyết sớm các sự cố trong mạng, giảm thời gian dừng hoạt động của mạng và giảm tổn thất kinh tế.
* Tăng hiệu suất: Giám sát mạng giúp đảm bảo mạng hoạt động hiệu quả và không bị giật lag, giúp tăng năng suất và giảm thời gian chờ của người dùng.
* Quản lý tài nguyên: Giám sát mạng giúp quản lý và sử dụng tài nguyên mạng hiệu quả, giúp đảm bảo rằng tài nguyên được sử dụng một cách hiệu quả và cải thiện tối ưu hóa hệ thống.

1. **Cách xây dựng một chương trình giám sát mạng hiệu quả?**

* Xác định nhu cầu giám sát: xác định rõ mục tiêu, yêu cầu và nhu cầu của mạng cần giám sát.
* Xác định phạm vị giám sát: xác định các thiết bị, dịch vụ và hế thống cần giám sát.
* Chọn công cụ giám sát: Chọn phần mềm giám sát hoặc dịch vụ giám sát thích hợp.
* Cấu hình và triển khai: Cấu hình các công cụ giám sát và triển khai chương trình giám sát.
* Thiết lập quy trình giám sát: Xác định các quy trình giám sát cần thực hiện và thiết lập các chuẩn đoán sớm và các thông báo cảnh báo.
* Thực hiện giám sát: Thực hiện việc giám sát theo quy trình và cập nhật dữ liệu giám sát liên tục.
* Xử lý và giải quyết sự cố: Xử lý và giải quyết các vấn đề phát sinh trong quá trình giám sát.

1. **Các phương pháp giám sát nào được sử dụng phổ biến?**

* Giám sát trực tiếp: sử dụng các công cụ và thiết bị để giám sát trực tiếp hoạt động mạng.
* Giám sát gián tiếp: sử dụng các công cụ và thiết bị để giám sát các dữ liệu được ghi lại từ mạng.
* Giám sát tự động: sử dụng phần mềm giám sát để tự động ghi lại và phân tích hoạt động của mạng.
* Giám sát thủ công: sử dụng nhân viên để giám sát và đánh giá hoạt động của mạng.

1. **Các phần mềm giám sát mạng được sử dụng phổ biến hiện nay?**

* Splunk: là một phần mềm giám sát và phân tích mạng mạnh mẽ và linh hoạt. Cho phép người dùng tổng hợp, phân tích và truy vấn dữ liệu log từ nhiều nguồn khác nhau để giúp phân tích hệ thống và các giải pháp vấn đề. Splunk cung cấp các công cụ trực quan và tìm kiếm thông minh để giúp người dùng tìm kiếm và phân tích dữ liệu một cách dễ dàng và hiệu quả.
* Zabbix: là một phần mềm giám sát mạng mã nguồn mở, cho phép giám sát và theo dõi tình trạng các thiết bị mạng, máy chủ, dịch vụ và các tiến trình. Zabbix cung cấp các tính năng như tạo cảnh báo, tạo biểu đồ và báo cáo, lưu trữ dữ liệu giám sát để giúp người quản trị có thể phát hiện và giải quyết các vấn đề mạng.
* Nagios: là một phần mềm giám sát mạng mã nguồn mở, cho phép người dùng giám sát và theo dõi tình trạng các thiết bị mạng, máy chủ, dịch vụ và các tiến trình. Nagios cung cấp các tính năng như gửi thông báo, tạo báo cáo và lưu trữ dữ liệu giám sát để giúp người quản trị có thể nhanh chóng phát hiện và giải quyết các sự cố mạng.

1. **Các công cụ hỗ trợ nào cần cho hoạt động giám sát?**

* Công cụ quản lý log: giúp lưu trữ và phân tích các bản ghi hoạt động của mạng, giúp phát hiện sự cố và đánh giá tình trạng mạng.
* Công cụ quản lý bảo mật: giúp bảo vệ mạng khỏi các tấn công bảo mật và giúp phát hiện sự cố bảo mật.
* Công cụ phân tích mạng: giúp phân tích hoạt động mạng và cung cấp thông tin về sức chứa, tốc độ và sự cố mạng.

1. **Cơ chế hoạt động của hệ thống giám sát mạng?**

Diagram

Description automatically generated

* Mỗi máy trinh sát sẽ có một danh sách những đối tượng mà máy trinh sát đó cần giám sát. Những đối tượng này có thể là file nhật ký hoạt động trên một máy tính, có thể là một dịch vụ trên hệ thống khác, cũng có thể là thành phần báo cáo trạng thái của Tường lửa/Bộ định tuyến… Dựa vào bản danh sách này, Máy trinh sát sẽ gửi truy vấn đến đối tượng để truy vấn thông tin. Thông tin thu thập được sẽ gửi đến Máy thu thập để chuẩn hóa trước khi lưu trữ vào cơ sở dữ liệu trung tâm. Tùy theo thiết kế của hệ thống, nếu những thông tin mà Máy trinh sát thu thập được có định dạng giống nhau thì sẽ không cần đến thành phần Máy thu thập.

1. **Các tiêu chuẩn và quy trình nào cần tuân theo trong hoạt động giám sát?**

Một số tiêu chuẩn và quy trình cần tuân theo để đảm bảo tính hiệu quả và cởi mở:

1. **Tiêu chuẩn ISO 27001**

* ISO 27001 là hệ thống tiêu chuẩn của Anh về hệ thống quản lý an ninh thông tin. Tiêu chuẩn ISO 27001 giúp quản lý an ninh thông tin một cách hiệu quả nhất. Thông tin bao gồm những dữ liệu được lưu lại dưới dạng điện tử hoặc dữ liệu được in ra – dữ liệu mềm và dữ liệu cứng.
* Thông qua việc áp dụng tiêu chuẩn ISO 27001 sẽ xác định được loại thông tin và xác định các mối nguy, rủi ro có thể xảy ra. Sau đó thiết lập hệ thống, thiết lập sự kiểm soát cũng như các quy trình để giảm thiểu các rủi ro.
* Lợi ích khi triển khai hệ thống quản lý an ninh theo tiêu chuẩn ISO 27001:
* Đảm bảo an toàn thông tin của tổ chức đối tác và khách hàng; giúp cho hoạt động của tổ chức luôn thông suốt và an toàn.
* Các sự cố an toàn thông tin do người dùng gây ra; sẽ được hạn chế tối đa khi nhân viên được đào tạo; nâng cao nhận thức về an toàn thông tin.
* Giúp hoạt động đảm bảo an toàn thông tin luôn được duy trì và cải tiến.

1. **Quy trình ITIL**

* ITIL (Information Technology Infrastructure Library) – Thư viện cơ sở hạ tầng CNTT. Cung cấp các quy trình cho hoạt động giám sát mạng và hệ thống.

1. **Quy trình COBIT**

* COBIT (Control Objectives for Information and related Technology. Cung cấp các tiêu chuẩn và quy trình cho việc quản lý và đánh giá hoạt động giám sát như quản lý rủi ro, quản lý chất lượng dữ liệu, quản lý bảo mật. Giúp cho các tổ chức đánh giá và cải thiện để tối ưu hóa tốc độ và hiệu suất.

1. **Tiêu chuẩn PCI DSS**

* Được xây dựng bởi tổ chức thanh toán thẻ và được sử dụng bởi các nhà cung cấp dịch vụ thanh toán. Mục tiêu của tiêu chuẩn PCI DSS là đảm bảo an toàn dữ liệu thanh toán và bảo vệ quyền riêng tư của khách hàng.

1. **Làm thế nào để xử lý và giải quyết các vấn đề phát sinh trong quá trình giám sát?**

Để xử lý và giải quyết các vấn đề phát sinh trong quá trình giám sát, các bước thực hiện gồm:

* Định vị vấn đề
* Sử dụng công cụ giám sát
* Xử lý vấn đề
* Kiểm tra kết quả

1. **Tác động của việc giám sát đến tốc độ và hiệu suất của mạng là gì?**

Việc giám sát mạng có thể tác động đến tốc độ và hiệu suất của mạng theo 2 cách:

* Sự giám sát cần thiết: Nếu một mạng không được giám sát, nó có thể gặp rất nhiều vấn đề về hiệu suất và tốc độ, ví dụ như sự gián đoạn mạng, tắc nghẽn băng thông và sự gián đoạn dịch vụ. Việc giám sát có thể giúp phát hiện và giải quyết các vấn đề này, tăng tốc độ và hiệu suất của mạng.
* Tác động từ một số công cụ giám sát: Có thể tải trọng mạng và giảm hiệu suất của nó.

# RÀ SOÁT CẤU HÌNH BẢO MẬT

1. **Làm cách nào để rà soát cấu hình một thiết bị?**

Có một số cách để rà soát cấu hình thiết bị, tùy thuộc vào loại thiết bị đó:

* Sử dụng công cụ quản lý thiết bị: Nhiều nhà sản xuất cung cấp công cụ quản lý thiết bị, cho phép bạn xem và sửa đổi cấu hình thiết bị.
* Sử dụng phần mềm quản lý mạng: Các phần mềm quản lý mạng, như SolarWinds hoặc Nagios, cung cấp thông tin chi tiết về cấu hình thiết bị trong mạng.
* Sử dụng dùng lệnh: Có một số dòng lệnh, như “ipconfig” trên Windows hoặc “ifconfig” trên Linux, cho phép bạn xem thông tin cấu hình mạng của thiết bị.

Lưu ý rằng cách rà soát cấu hình của một thiết bị có thể khác nhau tùy thuộc vào từng loại thiết bị và hệ điều hành.

1. **Tại sao cần phải rà soát cấu hình thiết bị?**

Rà soát cấu hình thiết bị cần thiết vì nhiều lý do sau đây:

* Bảo mật: Rà soát cấu hình thiết bị giúp xác định các lỗ hổng bảo mật và đảm bảo rằng các thiết bị đang hoạt động theo cấu hình an toàn.
* Tối ưu hoạt động: Rà soát cấu hình thiết bị giúp xác định các thiết bị hoạt động hiệu quả và giúp điều chỉnh cấu hình để tối ưu hoạt động.
* Dễ dàng quản lý: Rà soát cấu hình giúp quản trị viên mạng có một cái nhìn tổng quan về hình của tất cả các thiết bị trong mạng, giúp quản lý mạng dễ dàng hơn.
* Dễ dàng phục hồi sau sự cố: Rà soát cấu hình giúp quản trị viên mạng có thể dễ dàng phục hồi cấu hình ban đầu của thiết bị sau sự cố.

Vì vậy, rà soát cấu hình thiết bị là một phần quan trọng của quản lý mạng và giúp đảm bảo rằng mạng hoạt động một cách hiệu quả.

1. **Làm sao để tăng cường bảo mật cho cấu hình của thiết bị?**

Có một số biện pháp có thể sử dụng để tăng cường bảo mật cho cấu hình của thiết bị:

* Sử dụng mật mã: Sử dụng mật mã để bảo vệ cấu hình và dữ liệu của thiết bị.
* Cập nhật phần mềm: Luôn cập nhật phần mềm và hệ điều hành của thiết bị để đảm bảo rằng nó đăng sử dụng phiên bản mới nhất và bảo mật.
* Cấm truy cập không được phép: Thiết lập các quy tắc truy cập để chặn truy cập không được phép đến thiết bị.
* Sử dụng tường lửa: Sử dụng tường lửa để bảo vệ thiết bị khỏi các cuộc tấn công mạng.
* Sao lưu cấu hình: Sao lưu cấu hình thiết bị thường xuyên để có thể phục hồi nhanh chóng sau một sự cố.
* Sử dụng chứng chỉ SSL/TLS: Sử dụng chứng chỉ SSL/TLS để mã hóa dữ liệu truyền đi giữa thiết bị và máy chủ.

Tắt các dịch vụ không cần thiết.

1. **Các thiết bị nào cần được rà soát cấu hình?**

Có rất nhiều loại thiết bị cần được rà soát cấu hình, bao gồm:

* Máy tính: Bất kỳ máy tính nào đang hoạt động trong mạng cũng cần được rà soát cấu hình để đảm bảo an toàn và tính khả dụng của nó.
* Routers: Routers là thiết bị quan trọng để giữ liên lạc giữa các thiết bị trong mạng và cần được rà soát cấu hình để đảm bảo an toàn và hiệu suất hoạt động.
* Switches: Switches cũng giống như routers và cần được rà soát cấu hình đảm bảo tính năng và an toàn của mạng.
* Firewalls: Firewalls là thiết bị quan trọng để bảo vệ mạng và cần được rà soát cấu hình để đảm bảo tính năng và an toàn.
* Thiết bị lưu trữ dữ liệu: Thiết bị lưu trữ dữ liệu như máy chủ, đĩa cứng, NAS,… cần được rà soát cấu hình để đảm bảo tính năng và an toàn dữ liệu.

Thiết bị đầu cuối: Thiết bị đầu cuối như máy in, máy scan, máy fax,… cũng cần.

1. **Công cụ và kỹ thuật nào có thể sử dụng để thực hiện rà soát cấu hình thiết bị?**

Có nhiều công cụ và kỹ thuật có thể sử dụng để thwujc hiện rà soát cấu hình thiết bị, bao gồm:

* Công cụ quản lý thiết bị: Các công cụ quản lý thiết bị như Cisco IOS, Juniper JUNOS,… cho phép người quản trị mạng rà soát soát cấu hình và thực hiện các thao tác cấu hình từ xa.
* Công cụ quản lý mạng: Các công cụ quản lý mạng như SolarWinds, Nagios,… cho phép người quản trị mạng kiểm soát và theo dõi trạng thái của các thiết bị trong mạng.
* Công cụ quét dữ liệu: Các công cụ quét dữ liệu như Nmap, Nessus,… cho phép người quản trị mạng quét và phát hiện các lỗ hổng bảo mật trên thiết bị.
* Công cụ chứng thực: Các công cụ chứng thực như Kerberos, RADIUS,… cho phép người quản trị mạng xác thực và kiểm soát truy cập đến các thiết bị trong mạng.

Kỹ thuật định tuyến: Kỹ thuật định tuyến cho phép người dùng quản trị mạng định tuyến gói tin đến các thiết bị trong mạng.

1. **Làm cách nào để rà soát cấu hình một hệ thống?**

Có nhiều cách để rà soát cấu hình một hệ thống, bao gồm:

* Sử dụng công cụ quản lý thiết bị: Sử dụng công cụ quản lý thiết bị để rà soát cấu hình của từng thiết bị trong hệ thống.
* Sử dụng công cụ quản lý mạng: Sử dụng công cụ quản lý mạng để theo dõi và kiểm soát trạng thái của từng thiết bị trong hệ thống.
* Sử dụng công cụ quét dữ liệu: Sử dụng công cụ quét dữ liệu để phát hiện các lỗ hổng bảo mật trên từng thiết bị trong hệ thống.
* Sử dụng công cụ chứng thực: Sử dụng công cụ chứng thực để xác thực và kiểm soát truy cập đến từng thiết bị trong hệ thống.
* Sử dụng kỹ thuật định tuyến: Sử dụng kỹ thuật định tuyến để định tuyến gói tin đến từng thiết bị trong hệ thống.

Lưu ý: Việc rà soát cấu hình hệ thống cần được thực hiện thường xuyên và cập nhật để bảo đảm an toàn.

1. **Làm sao để biết rằng hệ thống đã bị nhiễm độc?**

Có một số dấu hiệu và cách để xác định rằng hệ thống của bạn đã bị nhiễm độc, bao gồm:

* Sự chậm trễ trong hoạt động của hệ thống: Nếu hệ thống của bạn chậm hơn bình thường, có thể là dấu hiệu của virus hoạt động trong nền.
* Lỗi hệ thống: Nếu bạn gặp các lỗi không giải thích trong hoạt động của hệ thống, có thể là dấu hiệu của vi-rút hoạt động.
* Truy cập bất thường đến hệ thống: Nếu bạn nhận được thông báo về các truy cập bất thường đến hệ thống, có thể là dấu hiệu của virus đang cố gắng truy cập vào hệ thống.
* Tăng trưởng lưu lượng mạng: Nếu bạn thấy lưu lượng mạng tăng một cách bất thường, có thể là dấu hiệu của virus đang truyền dữ liệu ra ngoài hệ thống.
* Sự thay đổi trong tệp hoặc thư mục: Nếu bạn thấy các tệp hoặc thư mục trên hệ thống của bạn đã thay đổi thì chứng tỏ có dấu hiệu của virus xâm nhập vào.
* Hiện tượng lạ: Nếu hệ thống của bạn hoạt động không như mong đợi, ví dụ như tự động mở các trang web hoặc chạy các tập lệnh không mong muốn, có thể là dấu hiệu hệ thống bị nhiễm độc.

Để xác minh rằng hệ thống của bạn bị nhiễm độc, bạn cần chạy các phần mềm diệt virus và kiểm tra tập tin hệ thống để tìm và xóa bất kỳ phần mềm độc hại nào.

1. **Liệu có cách nào để tránh việc mã độc tấn công vào hệ thống?**

Có nhiều cách để tránh việc mã độc tấn công vào hệ thống, bao gồm:

* Sử dụng phần mềm diệt virus và firewall để bảo vệ hệ thống.
* Cập nhật phần mềm và hệ điều hành thường xuyên để bảo vệ chống lại các lỗ hổng bảo mật.
* Chọn mật khẩu mạnh và thay đổi nó thường xuyên.
* Không cài đặt phần mềm từ nguồn không xác thực hoặc nhấp vào các liên kết độc hại.
* Sử dụng tính năng bảo mật động của hệ thống, chẳng hạn như tính năng bảo mật của thư điện tử hoặc trình duyệt web.

Hạn chế quyền truy cập của người dùng để giới hạn sự tấn công của mã độc.

1. **Làm thế nào để đảm bảo tính tương thích của cấu hình hệ thống với các thiết bị khác?**

Để đảm bảo tính tương thích của hệ thống với các thiết bị khác, bạn cần làm những việc sau:

* Chọn các thiết bị phù hợp: Chọn các thiết bị có thể hoạt động tốt với hệ thống của bạn và có thể tương thích với nhau.
* Sử dụng phiên bản phần mềm chính xác: Sử dụng phiên bản phần mềm mới nhất và chính xác để đảm bảo tính tương thích giữa các thiết bị.
* Tìm hiểu về tính tương thích: Trước khi mua bất kỳ thiết bị nào, hãy tìm hiểu về tính tương thích của nó với hệ thống của bạn.
* Sử dụng các cấu hình chuẩn: Sử dụng các cấu hình chuẩn để đảm bảo tính tương thích giữa các thiết bị.
* Cập nhật phần mềm: Để đảm bảo tính tương thích, hãy cập nhật phần mềm của các thiết bị thường xuyên.

Nếu bạn làm những việc trên, bạn sẽ có thể đảm bảo tính tương thích của hệ thống với thiết bị.

1. **Liệu có cách nào để xem xét lại và cải thiện cấu hình hệ thống?**

Có nhiều cách để xem xét lại và cải thiện cấu hình hệ thống. Một số trong số đó bao gồm:

* Đánh giá hiệu suất: Xem xét các chỉ số hiệu suất như tốc độ xử lý, sử dụng bộ nhớ và sử dụng đĩa cứng để đánh giá hiệu suất của hệ thống và tìm các cách để cải thiện nó.
* Xem xét sử dụng tài nguyên: Xem xét sử dụng tài nguyên của hệ thống để tìm cách giảm thiểu sử dụng bộ nhớ và đĩa cứng không cần thiết.
* Cập nhật phần mềm: Cập nhật các phần mềm và hệ điều hành để đảm bảo hệ thống đang sử dụng phiên bản mới nhất và tốt nhất.
* Tối ưu hóa cấu hình hệ thống: Tìm cách tối ưu hóa cấu hình hệ thống bằng cách thay đổi cấu hình hoặc thêm thiết bị nếu cần thiết.
* Nâng cấp phần cứng: Nâng câp CPU, RAM hoặc đĩa cứng để cải thiện hiệu suất hệ thống.

Tối ưu hóa các cấu hình hệ thống và cấu hình mạng để cải thiện tốc độ truy cập và giảm latencia.

# PHÒNG CHỐNG MÃ ĐỘC

1. **Thế nào là bóc gỡ mã độc trên mạng máy tính?**

Bóc gỡ mã độc trên mạng máy tính là quá trình phát hiện và loại bỏ các mã đọc trên máy tính hoặc mạng máy tính. Nó có thể thực hiện bằng cách sử dụng phần mềm diệt virus, quét mạng máy tính, xác định và loại bỏ các tập tin hay phần mềm bị nhiễm mã độc. Việc bóc gỡ mã độc là quan trọng để giữ an toàn thông tin và bảo vệ sức khỏe máy tính của bạn.

1. **Lợi ích của việc thực hiện rà soát, bóc gỡ mã độc với mục đích bảo mật là gì?**

Việc thực hiện rà soát, bóc gỡ mã độc có nhiều lợi ích cho việc bảo mật hệ thống, bao gồm:

* Phát hiện và loại bỏ các mã độc: Rà soát và bóc gỡ mã độc giúp phát hiện và loại bỏ những mã độc đang tồn tại trong hệ thống, giúp bảo vệ dữ liệu và tài khoản người dùng.
* Giảm rủi ro bị tấn công: Khi phát hiện và loại ỏ mã độc, hệ thống sẽ được bảo vệ khỏi các tấn công mã độc.
* Giảm rủi ro mất dữ liệu: Khi mã độc tấn công và hệ thống, nó có thể xóa hoặc thay đổi dữ liệu, việc rà soát và bóc gỡ mã độc giúp giảm rủi ro mất dữ liệu.
* Tăng độ tin cậy của hệ thống: Khi hệ thống được bảo vệ chắc chắn khỏi các mã độc, người dùng sẽ có độ tin cậy cao hơn về hệ thống.
* Giảm chi phí phải sữa chữa: Nếu hệ thống bị tấn công bởi mã độc, chi phí phải sữa chữa có thể rất cao, việc rà soát và bóc gỡ mã độc sẽ làm giảm đi sự rủi ro của hệ thống.

1. **Bóc gỡ mã độc trong tư tưởng bảo mật là gì?**

Bóc gỡ mã độc trong tư tưởng bảo mật là một phương pháp nghiên cứu và đánh giá các lỗ hổng bảo mật trong mã độc, phần mềm hoặc hệ thống. Nó bao gồm việc phát hiện và sửa lỗi, mở rộng bảo mật và tối ưu hóa các hệ thống, phần mềm và mã độc. Các kỹ sư bảo mật sử dụng các công cụ và kỹ thuật phổ biến để kiểm tra các lỗ hổng bảo mật trong mã độc và cung cấp giải pháp bảo mật để bảo vệ hệ thống.

1. **Tại sao bóc gỡ mã độc là quan trọng với bảo mật?**

Bóc gỡ mã độc là quan trọng với bảo mật bởi vì nó giúp phát hiện và loại bỏ các mã độc từ hệ thống hoặc phần mềm. Mã độc là một loại mã hủy hoại hoặc tấn công, có thể gây hại cho hệ thống, dữ liệu hoặc người dùng. Nếu mã độc không được phát hiện và loại bỏ, nó có thể gây ra sự cố an toàn, mất dữ liệu hoặc cho phép tấn công bất hợp pháp tới hệ thống. Bằng cách bóc gỡ mã độc, chúng ta có thể giữ cho hệ thống và dự liệu an toàn và bảo mật.

1. **Những mục tiêu nào được đặt ra trong việc thực hiện bóc gỡ mã độc với mục tiêu bảo mật?**

Trong việc thực hiện bóc gỡ mã độc với mục tiêu bảo mật, các mục tiêu chính bao gồm:

* Phát hiện và loại bỏ các mã độc trong hệ thống hoặc phần mềm.
* Đảm bảo tính an toàn và bảo mật của dữ liệu và hệ thống.
* Giảm rủi ro từ các tấn công bất hợp pháp.
* Tăng tính minh bạch và khả năng phục hồi trong trường hợp xảy ra sự cố.
* Tăng tính tương thích với các thiết bị và hệ thống khác.
* Đảm bảo tính đồng bộ và tính nhất quán của cấu hình hệ thống.

Cải thiện hiệu suất và tốc độ của hệ thống.

1. **Yara Rules là gì ?**

Quy tắc YARA là một cách xác định phần mềm độc hại (hoặc các tệp khác) bằng cách tạo quy tắc tìm kiếm các đặc điểm nhất định. YARA ban đầu được phát triển bởi Victor Alvarez của Virustotal và chủ yếu được sử dụng trong nghiên cứu và phát hiện phần mềm độc hại. Nó được phát triển với ý tưởng mô tả các mẫu xác định các chủng cụ thể hoặc toàn bộ họ phần mềm độc hại.

1. **Yara Rules hoạt động như thế nào? Các trường hợp sử dụng?**

Các quy tắc YARA giống như một phần của ngôn ngữ lập trình, chúng hoạt động bằng cách xác định một số biến chứa các mẫu được tìm thấy trong một mẫu phần mềm độc hại. Nếu một số hoặc tất cả các điều kiện được đáp ứng, tùy thuộc vào quy tắc, thì nó có thể được sử dụng để xác định thành công một phần mềm độc hại.

Khi phân tích một phần của phần mềm độc hại, các nhà nghiên cứu sẽ xác định các mẫu và chuỗi duy nhất trong phần mềm độc hại cho phép họ xác định nhóm mối đe dọa và họ phần mềm độc hại mà mẫu được quy cho. Bằng cách tạo quy tắc YARA từ một số mẫu từ cùng một họ phần mềm độc hại, có thể xác định nhiều mẫu có thể liên quan đến cùng một chiến dịch hoặc tác nhân đe dọa.

Khi điều tra một phần mềm độc hại, nhà phân tích có thể tạo quy tắc YARA cho một mẫu mới mà họ đang điều tra. Sau đó, quy tắc này có thể được sử dụng để tìm kiếm cơ sở dữ liệu phần mềm độc hại riêng của họ hoặc các kho lưu trữ trực tuyến như VirusTotal để tìm các mẫu tương tự.

Nếu nhà phân tích phần mềm độc hại làm việc cho một tổ chức triển khai IPS hoặc nền tảng được YARA hỗ trợ khác được sử dụng để [bảo vệ phần mềm độc hại](https://www.varonis.com/blog/malware-protection/?hsLang=en" \t "_blank) , thì các quy tắc YARA có thể được sử dụng làm công cụ ứng phó sự cố để phát hiện các tệp nhị phân độc hại trong tổ chức.

**Trường hợp sử dụng**

YARA đã được chứng minh là cực kỳ phổ biến trong cộng đồng infosec, lý do là có một số trường hợp sử dụng để triển khai YARA:

* Xác định và phân loại phần mềm độc hại
* Tìm các mẫu mới dựa trên các mẫu dành riêng cho gia đình
* Người ứng phó sự cố có thể triển khai các quy tắc YARA để xác định các mẫu và thiết bị bị xâm nhập

Việc chủ động triển khai các quy tắc YARA tùy chỉnh có thể tăng khả năng phòng vệ của tổ chức

1. **Nguyên lý IOC là gì? Tại sao dùng IOC?**

IOC (Indicator of Compromise) là một dấu hiệu được sử dụng để xác định việc tấn công mạng. Nó có thể là một địa chỉ IP, tên miền, tên tệp, mã hash hoặc bất kỳ thông tin nào khác mà các nhà sản xuất phần mềm bảo mật đã xác định là liên quan đến một tấn công mạng.

Tại sao dùng IOC:

* Giúp cho các nhà quản trị mạng và các nhà sản xuất phần mềm bảo mật nhanh chóng phát hiện các tấn công mạng trong môi trường mạng của họ.
* Giúp cho các nhà quản trị mạng đánh giá mức độ nghiêm trọng của tấn công mạng và xác định cách để xử lý nó.

Giúp cho các nhà sản xuất phần mềm bảo mật cập nhật và cải thiện các giải pháp bảo mật của họ dựa trên thông tin về tấn công mạng mới nhất.

1. **IOC được hình thành như thế nào?**

IOC (Indicator of Compromise) được hình thành như sau:

* Phân tích tấn công: Khi một tấn công mạng được phát hiện, các nhà sản xuất phần mềm bảo mật và các nhà quản trị mạng sẽ tiến hành phân tích tấn công để xác định các dấu hiệu của tấn công.
* Xác định dấu hiệu: Sau khi phân tích tấn công, các nhà sản xuất phần mềm bảo mật và các nhà quản trị mạng sẽ xác định các dấu hiệu của tấn công như địa chỉ IP, tên miền, tên tệp, mã hash hoặc bất kì thông tin nào khác.
* Đăng ký dấu hiệu: Sau khi xác định dấu hiệu, các nhà sản xuất phần mềm bảo mật và các nhà quản trị mạng sẽ đăng ký dấu hiệu này vào cơ sở dữ liệu của họ.

Sử dụng dấu hiệu: Sau khi đăng ký dấu hiệu, các nhà quản trị mạng có thể sử dụng dấu hiệu này để phát hiện các tấn công mạng trong môi trường mạng của họ.

1. **Liệu có cách nào để sử dụng IOC để phát hiện các tấn công mạng trong quá trình sử dụng mạng?**

Có thể sử dụng chức năng IOC để phát hiện các tấn công mạng. IOC là những dấu hiệu nhận dạng của một tấn công, chẳng hạn như địa chỉ IP, tên miền, tập tin hoặc chương trình mã độc. Bạn có thể sử dụng các công cụ phát hiện IOC, như các hệ thống bảo mật mạng, để kiểm tra các dữ liệu và hành vi mạng của bạn để tìm kiếm các dấu hiệu của tấn công và thực hiện xử lý kịp thời.

# SĂN LÙNG MỐI NGUY HẠI

1. **Những loại mối nguy hại nào thường được xuất hiện trong mạng?**

* Virus, worm, trojan, phishing, spyware, adware, ransomware và malware.

1. **Kỹ thuật nào được sử dụng để phát hiện mối nguy hại trong mạng?**

* Quét virus: các phần mềm khi đã nhận diện được mẫu thì hoàn toàn có thể làm sạch virus khỏi máy tính.
* Kiểm tra toàn bộ thao tác ghi đĩa
* Phát hiện nguồn tấn công: không phải hiện tượng bất thường nào cũng do virus gây ra, cần phân biệt giữa virus và không phải virus.
* Kiểm tra sự bất thường của các tiến trình trong hệ thống.
* Kiểm tra sự thay đổi của file: xóa file, thay thể file mới hoặc thuộc tính của file bị thay đổi .
* Kiểm tra sự thay đổi, tác động lên hệ thống registry, các file hệ thống
* Luôn cập nhật phần mềm antivirus trong máy

1. **Bảo vệ máy tính khỏi mối nguy hại bằng cách nào?**

* Cài đặt các bản cập nhật mới nhất từ Microsoft update
* Sử dụng trình quét an toàn của Microsoft
* Sử dụng công cụ loại bỏ phần mềm độc hại của window
* Chạy bộ bảo vệ Microsoft ngoại tuyến
* Bật tường lửa

1. **Phần mềm diệt virus có hiệu quả như thế nào trong việc săn lùng mối nguy hại?**

* Giúp ngăn chặn và loại bỏ các mối nguy hại được phát hiện trên hệ thống.

1. **Làm sao để phát hiện xem máy tính của bạn bị mối nguy hại hay không?**

* kiểm tra máy tính bị theo dõi qua lịch sử mở file
* Kiểm tra máy tính bị theo dõi qua lịch sử trình duyệt Web
* Kiểm tra đăng nhập lạ trên máy tính

1. **Cách nào để loại bỏ mối nguy hại khi nó đã được phát hiện?**

* Sử dụng phần mềm diệt virus và diệt spyware
* Tắt các dịch vụ và chức năng không cần thiết trên máy tính
* Tạo sao lưu dữ liệu và đặt biệt mật khẩu mạnh cho tài khoản
* Xem xét việc sử dụng các dịch vụ bảo mật tích hợp để phát hiện và loại bỏ mối nguy hại
* Hợp tác với nhà cung cấp phần mềm bảo mật để xử lý mối nguy hại.

1. **Tại sao chúng ta cần săn lùng mối nguy hại thường xuyên?**

* Giúp phát hiện và xử lý nhanh chóng những mối nguy hại trước khi họ gây ra thiệt hại
* Giữ cho hệ thống mạng an toàn và bảo mật
* Tránh mất dữ liệu quan trọng và tài khoản cá nhân
* Giữ cho tính toàn vẹn và tính minh bạch của thông tin trong mạng.
* Tránh mất tín dụng và uy tín của doanh nghiệp hoặc tổ chức.

1. **Cách nào để ngăn chặn mối nguy hại trong tương lai?**

* Sử dụng phần mềm bảo mật chuyên nghiệp
* Thực hiện cập nhật hệ điều hành và phần mềm định kỳ
* Tuân thủ nguyên tắc an toàn mạng
* Tạo mật khẩu mạnh và đổi thường xuyên
* Sử dụng các thiết bị cấu hình bảo mật mạng chuyên nghiệp.

1. **Tác động của mối nguy hại trên cơ sở dữ liệu của mạng là gì?**

* Mất dữ liệu: Mối nguy hại có thể xóa hoặc sửa đổi dữ liệu trong cơ sở dữ liệu, dẫn đến mất mát hoặc thiệt hại cho doanh nghiệp hoặc cá nhân.
* Truy cập trái phép: Mối nguy hại có thể cho phép truy cập trái phép đến dữ liệu của mạng, để lừa đảo hoặc tấn công các hệ thống khác.
* Lộ thông tin riêng tư: Mối nguy hại có thể truy cập hoặc lộ thông tin riêng tư, gây tổn hại cho danh tiếng và uy tín của cá nhân hoặc doanh nghiệp.
* Chi phí cao: Giải quyết vấn đề mối nguy hại trên cơ sở dữ liệu của mạng có thể tốn kém nhiều chi phí, bao gồm chi phí cho việc phát hiện và xử lý sự cố, v.v.
* Tổn thất uy tín: Mối nguy hại trên cơ sở dữ liệu của mạng có thể gây tổn thất uy tín cho doanh nghiệp hoặc cá nhân

1. **Những biện pháp nào để bảo vệ thông tin trong mạng khỏi mối nguy hại?**

* Sử dụng mật khẩu mạnh: Tạo mật khẩu mạnh và thay đổi nó thường xuyên có thể giúp bảo vệ tài khoản của bạn khỏi các mối nguy hại.
* Sử dụng phần mềm bảo mật: Sử dụng phần mềm bảo mật, bao gồm việc cập nhật thường xuyên, có thể giúp phát hiện và chặn các mối nguy hại trước khi chúng gây hại.
* Không cung cấp thông tin cá nhân: Không cung cấp thông tin cá nhân qua mạng, bao gồm số điện thoại, địa chỉ email, v.v., có thể giúp giảm rủi ro bị lừa đảo hoặc tấn công.
* Sử dụng kết nối an toàn: Sử dụng kết nối an toàn, chẳng hạn như kết nối HTTPS, có thể giúp bảo vệ thông tin truyền đi qua mạng khỏi bị truy cập hoặc lộ.
* Sử dụng tính năng xác thực hai yếu tố: Sử dụng tính năng xác thực hai yếu tố có thể giúp bảo vệ tài khoản của bạn khỏi các mối nguy hại.

# HUẤN LUYỆN DIỄN TẬP

1. **Diễn tập đối kháng là gì**: là các đội dựa vào khả năng của bản thân để tiến hành vá các lỗ hổng của mình cũng như tìm và tấn công vào lổ hổng của mục tiêu
2. **Tên gọi của các đội**: Blue Team (phòng thủ), Red Team (tấn công)
3. **Phạm vi chủ đề của diễn tập**: hệ điều hành, website, điều tra nguồn gốc dữ liệu, nguồn gốc email, phòng tránh mã độc, chặn backdoor, …
4. **lợi ích của diễn tập đối kháng:** rèn luyện được các kỹ năng cần có như: khả năng phân tích lổ hổng của các phiên bản phần mềm đang sử dụng, phiên bản của hệ điều hành và các lỗ hổng có thể tồn tại trong đó, …
5. **Ai là người tham gia diễn tập:** cán bộ phụ trách CNTT các Sở, ban, ngành và UBND các huyện, thị xã, thành phố; thành viên Đội Ứng cứu sự cố an toàn thông tin mạng tỉnh, Doanh nghiệp.
6. **Mục đích của diễn tập này là gì:** nâng cao nhận biết về tầm quan trọng của an ninh mạng trong các bộ máy nhà nước cũng như là trong doanh nghiệp cho các chỉ huy lãnh đạo
7. **Diễn tập theo kịch bản là gì**: là một sự kiện được lên kế hoạch trong đó một tổ chức mô phỏng các cuộc tấn công mạng, sự cố bảo mật thông tin và các loại gián đoạn khác.
8. **Các kịch bản thường được diễn tập:**

* Phishing Email
* Spearphishing Email
* Denial of Service (DoS)
* Adding an Unauthorized Device
* Website (Login, Upload File, …)

1. **Các nguồn tham khảo về diễn tập theo kịch bản:** attackdefense.com, tryhackme.com
2. **Các thuật ngữ và định nghĩa hay được sử dụng trong diễn tập:**

* **CERT:** Com puter Emergency Response Team (Đội ứng cửu sự cô khẩn cấp)
* **Phishing**: là hành vi giả mạo như là một thực thè đảng tin cậy (website của các cơ quan, tổ chức, các website xã hội phổ biến, các trung tâm chi trả trực tuyến ,...) đề lấy cắp thông tin nhạy cảm như tên nsười dùng, mật khẩu, các chi tiết thẻ tín dụng... thông qua các giao tiếp trên mạng.
* **Deface**: Là tấn công thay đồi nội dung website của nạn nhân thông qua lỗ hông bảo mật.
* **Phát tán Malware**: là hành vi phát lán các phần mềm độc hại (virus, backdoor...) qua môi trường internet.
* **DoS** (Denial o f Service) - tấn công từ chối dịch vụ bằng cách chiếm dụng m ột lượng lớn tài nguyên mạng, tài nguyên hệ thống như băng thông, bộ nhớ, khả nàng xừ lý ... và làm mất khả năng đáp ứng yêu cầu dịch vụ từ các khảch hàne khác.