ĐỀ CƯƠNG PHÒNG CHỐNG VÀ ĐIỀU TRA TỘI PHẠM MÁY TÍNH

MỤC LỤC

Câu 1: Khái niệm tội phạm công nghệ cao, tội phạm máy tính

Tội phạm công nghệ cao:

- Theo từ điển Bách khoa Công an nhân dân Việt Nam:
  - Tội phạm công nghệ cao là loại tội phạm sử dụng những thành tựu mới của khoa học kỹ thuật và công nghệ hiện đại làm công cụ, phương tiện để thực hiện hành vi phạm tội một cách cố ý hoặc vô ý, gây nguy hiểm cho xã hội.
  - Chủ thể là những người có trình độ học vấn, chuyên môn cao, có thủ đoạn rất tinh vi, khó phát hiện.
  - Hậu quả gây ra bởi tội phạm công nghệ cao không chỉ là thiệt hại lớn về mặt kinh tế, xã hội mà còn xâm hại tới an ninh quốc gia.
- Theo tổ chức Cảnh sát hình sự quốc tế Interpol:
  - Tội phạm công nghệ cao là loại tội phạm sử dụng, lạm dụng những thiết bị kỹ thuật, dây chuyền công nghệ có trình độ công nghệ cao như một công cụ, phương tiện để thực hiện hành vi phạm tội.
  - Tội phạm công nghệ cao gồm hai dạng: tội phạm máy tính và tội phạm công nghệ thông tin – điều khiển học.
- Theo bộ tư pháp Mỹ:
  - Tội phạm công nghệ cao là bất cứ hành vi vi phạm pháp luật hình sự nào có liên quan đến việc sử dụng những hiểu biết về công nghệ máy tính trong việc phạm tội.
- Theo các chuyên gia về tội phạm học ở Việt Nam:
  - Nhóm thứ nhất: tội phạm công nghệ cao là các tội phạm mà khách thể của tội phạm xâm hại tới hoạt động bình thường của máy tính và mạng máy tính. (được quy định tại các điều 224, 225, 226 Bộ luật Hình sự nước CHXHCNVN năm 1999).
  - Nhóm thứ hai: tội phạm sử dụng công nghệ cao gồm các tội phạm truyền thống được quy định trong Bộ luật Hình sự nước

CHXHCNVN 1999, khi thực hiện hành vi phạm tội, người phạm tội sử dụng các công cụ làm công cụ, phương tiện thực hiện hành vi phạm tội.

Tội phạm máy tính:

- Dựa trên bộ Luật Hình sự 1999 sửa đổi 2009: tội phạm máy tình là hành vi vi phạm pháp luật do người có năng lực trách nhiệm hình sự sử dụng máy tính để thực hiện hành vi phạm tội, lưu trữ thông tin phạm tội hoặc xâm phạm tới hoạt động bình thường và an toàn của máy tính, hệ thống máy tính.
- Mọi loại tội phạm máy tính đều là tội phạm công nghệ cao.

Câu 2: Các dạng tội phạm máy tính

Chia làm 5 dạng chính:

1. Đánh cắp định danh.
    a. Giả mạo.
    b. Tấn công hoặc sử dụng phần mềm gián điệp.
    c. Truy cập trái phép dữ liệu.
    d. Dựa vào thông tin rác
2. Rình rập, quấy rối.
3. Truy cập bất hợp pháp tới hệ thống máy tính và các dữ liệu nhạy cảm.
4. Lừa đảo trực tuyến.
    a. Lừa đảo đầu tư.
    b. Lừa đảo giao dịch trực tuyến.
    c. Lừa đảo nhận/chuyển tiền.
    d. Vi phạm bản quyền dữ liệu.
5. Phát tán tin rác, mã độc.

Đánh cắp định danh:

- Theo Mỹ xác định: "tội phạm trộm cắp và lừa đảo danh tính là thuật ngữ dùng để chỉ các loại tội phạm ăn cắp, gian lận, lừa dối và sử dụng trái phép dữ liệu cá nhân của người khác".
- Mục đích của loại tội phạm này thường vì lợi ích kinh tế, động cơ tài chính, hoặc có thể để mạo danh người khác, hủy hoại danh tính.
- Việc truy cứu trách nhiệm hình sự đối với tội phạm loại này cần xem xét tới các phương tiện mà hành vi trộm cắp định danh sử dụng.
- Giả mạo: là quá trình ăn cắp các dữ liệu cá nhân từ các nạn nhân mục tiêu, thường được thực hiện qua email, thủ thuật này đang ngày càng trở nên phổ biến.
    - Tội phạm giả mạo có thể khó điều tra do nhiều nguyên nhân: nạn nhân thường không biết bị mắc lừa cho tới khi sự việc xảy ra khá lâu; tội phạm sử dụng ngay và có kỹ năng ẩn dấu vết; hoạt động lừa đảo được tiến hành trong thời gian hạn chế; trang web giả mạo thường thiết lập trên máy chủ công cộng hoặc máy tính thứ ba, các trang web được tháo dỡ ngay khi tội phạm có đủ thông tin cá nhân cần thiết.
- Tấn công hoặc sử dụng phần mềm gián điệp:
    - Tấn công: là một hoặc một chuỗi các hành động cố gắng vượt qua sự an toàn của hệ thống để truy cập vào dữ liệu không có chủ quyền. Có nhiều cách để tấn công, bao gồm tìm kiếm lỗ hổng của hệ điều hành, khai thác, tấn công từ xa hợp pháp truy cập vào hệ thoongs mục tiêu… Tấn công liên quan tới các thuật ngữ hacker mũ trắng, xám, đen (tự trình bày).
    - Phần mềm gián điệp: phục vụ mục tiêu thu thập dữ liệu cá nhân từ máy tính mục tiêu, thường liên quan đến một số phần mềm được tải về máy tính mục tiêu.

        - Các khả năng của phần mềm gián điệp: ghi lại tên, mật khẩu người dùng, các tổ hợp phím, trang web đã truy cập, có thể chụp màn hình định kỳ, ghi lại mọi hoạt động trên màn hình…

⇨ Tấn công và phần mềm gián điệp dễ bị điều tra hơn giả mạo do để lại dấu vết rõ ràng, dữ liệu thu phải truyền tới một đích nào đó.

- Truy cập dữ liệu trái phép: là hành vi truy cập dữ liệu mà không được phép. Hành vi phổ biến phổ biến là khi một người có quyền hợp pháp một số nguồn dữ liệu cụ thể hoặc là để truy cập dữ liệu không được phép hoặc sử dụng các dữ liệu một cách khá hơn so với cách họ được ủy quyền.
- Dựa vào thông tin rác: tội phạm có thể thu thập thông tin dữ liệu từ các phương tiện truyền dữ liệu như giấy, đĩa mềm, ổ đĩa… đã bị loại bỏ từ các thùng rác. Từ đó thu thập dữ liệu cá nhân phục vụ các mục đích xấu.

Rình rập, quấy rối:

- Là loại tội phạm mới và ngày càng phát triển, thủ phạm sử dụng Internet để sách nhiễu, đe dọa người khác.
- Mối đe dọa, quấy rối dựa trên 4 yếu tố sau:
    - Độ tin cậy: mối đe dọa cho là đáng tin cậy, phải có dấu hiệu hợp lý rằng nó có thể được thực hiện.
    - Tần suất: các mối đe dọa cô lập là mối quan tâm ít hơn một mô hình của quấy rối và đe dọa.
    - Đặc trưng: đề cập đến thủ phạm liên quan đến bản chất của các mối đe dọa, các mục têu của các mối đe dọa, các phương tiện thực hiện các mối đe dọa.
    - Cường độ: đề cập tới những giai điệu chung của truyền thông, bản chất của ngôn ngữ, cường độ của các mối đe dọa. Bất cứ mối đe dọa lớn lên vượt quá mức một người bình thường có thể nói, ngay cả trong một tình huống thù địch, các mối đe dọa sẽ trở thành mối quan tâm lớn hơn.

Truy cập bất hợp pháp tới hệ thống máy tính và các dữ liệu nhạy cảm:

- Tương tự như loại tội phạm đánh cắp định danh, tuy nhiên mục đích khác hơn. Các phương pháp thực hiện tương tự đánh cắp định danh: thông qua hacking, phần mềm gián điệp, các nhân viên truy cập dữ liệu, thông qua phương tiện truyền thông dữ liệu bị loại bỏ.
- Trộm cắp dữ liệu khó khăn trong việc ngăn chặn nhân viên được phép truy cập tới dữ liệu, khó phân biệt giữa truy cập được phép và trái phép.

Lừa đảo trực tuyến:

- Lừa đảo đầu tư: là phần tư vấn, môi giới đầu tư không hợp pháp, không phải là trào lưu mới mà cũng không hẳn là một hoạt động tội phạm. Phổ biến như các hình thức lừa đảo môi giới chứng khoán, lừa đảo qua email giả danh người nổi tiếng yêu cầu sự giúp đỡ trong việc chuyển giao tiền giữa các nước… Tội phạm này thường khó điều tra: phải truy tìm lại các email, các email thường gửi từ các tài khoản vô danh nên khó theo dõi.
- Lừa đảo giao dịch trực tuyến:
    - Không giao hàng hóa: người mua gửi tiền và người bán không giao hàng (dễ điều tra, truy tố).
    - Giao hàng có giá trị thấp hơn so với quảng cáo: khó điều tra và truy tố hơn.
    - Cung cấp hàng hóa không đúng thời hạn.
    - Không tiết lộ các thông tin liên quan về một sản phẩm hoặc các điều khoản của người bán.
- Lừa đảo nhận/chuyển tiền: liên quan tới việc trao đổi một lệnh chuyển tiền giả hoặc ký séc tiền thật.
- Vi phạm bản quyền dữ liệu: là các hành vi trộm cắp tài sản trí tuệ, có thể là bản quyền phần mềm, bài hát, đoạn phim…Vi phạm bản quyền dữ liệu thường là các vấn đề dân sự, được giải quyết bằng tiền.

Phát tán tin rác, mã độc hại:

- Phát tán tin rác là hành vi gửi các tin nhắn hoặc email chứa nội dung quảng cáo, marketing và được gửi một cách ồ ạt gây phiền toái cho người nhận. Phát tán mã độc là hành vi kẻ tấn công sử dụng các chương trình mã độc để lây nhiễm vào các hệ thống, phần mềm nhằm mục đích phá hoại hệ thống hoặc đánh cắp thông tin trái phép.

Câu 3: Một số hành vi của tội phạm máy tính

Các hành vi của tội phạm máy tính phổ biến bao gồm: trộm cắp thông tin, phát tán mã độc, lừa đảo, tấn công trái phép.

1. **Trộm cắp thông tin**
    - Giả mạo: là quá trình gửi email hàng loạt, mục đích từ một số nguồn hợp pháp và lôi kéo người nhận cung cấp thông tin cá nhân hoặc nhấn vào một liên kết trong email tới một trang web cung cấp thông tin cá nhân. Hình thức phổ biến nhất là giả mạo các website ngân hàng.
    - Sử dụng phần mềm gián điệp: cài đặt phần mềm gián điệp vào máy tính của mục tiêu và thu thập thông tin trực tiếp từ bàn phím, mèn hình, các hoạt động trên máy tính nạn nhân.
        - Phổ biến nhất là keylogger.
        - Tải các phần mềm từ website không chính thống.
        - Sử dụng các bản crack.
        - Một số phần mềm gián điệp cũng được sử dụng cho tấn công leo thang đặc quyền.
2. **Phát tán mã độc hại**
    - Gửi các email có đính kèm mã độc.
    - Chèn mã độc vào các website hợp pháp.
    - Cài đặt trong các chương trình phần mềm.

3. **Lừa đảo**
    - Lừa đảo thông qua giao dịch: gồm các hành vi như không giao hàng hóa, giao hàng có giá trị thấp hơn so với quảng cáo, không tiết lộ các thông tin liên quan về sản phẩm hoặc các điều khoản của người bán.
        - 3 khu vực giann lận giao dịch phổ biến trên Internet theo Ủy ban điện tử FTC: cò mồi, chào giá, bòn rút (tự phân tích).
    - Lừa đảo thông qua lôi kéo đầu tư kinh doanh bất hợp pháp.
    - Lừa đảo đầu tư.
    - Tư vấn đầu tư.
4. **Tấn công trái phép**
    - Tấn công thăm dò: thủ phạm tìm hiểu về hệ thống muốn đột nhập, bao gồm hệ thống báo động, an ninh, giờ hoạt động, tìm kiếm các lỗ hổng để có thể đột nhập vào.
        - Quét lỗ hổng.
    - Tấn công hệ thống và các thiết bị mạng:
        - Tấn công brute-force: xảy ra khi các công cụ phần mềm đang sử dụng chỉ đơn giản là mã hóa của chữ cái, số và biểu tượng có thể crack mật khẩu. Nó sẽ xuất hiện trong nhật ký của máy chủ như số lần đăng nhập thất bại trong thời gian ngắn.
        - Tấn công từ điển: một tập tin từ điển sẽ cho một tập tin văn bản đơn giản chứa mật khẩu thường sử dụng. Nó có thể là mật khẩu cụ thể liên quan đến mục tiêu và được nạp vào một ứng dụng crack, chạy với tài khoản người dùng đặt bởi các ứng dụng.
    - Tấn công vào CSDL và ứng dụng Web:
        - SQL Injection: là hình thức tấn công mà hacker nhập mã SQL trực tiếp vào một form web nhu mục đăng nhập hay một thanh địa chỉ trên trình duyệt, với mục đích là bẫy các trang web vào trình mã SQL truy cập vào CSDL thực hiện mã.

- Tấn công XSS: kẻ tấn công nhúng mã Javascript vào hyperlinks của một trang web, điều này cho phép kẻ xâm nhập quyền kiểm soát các thông tin cá nhân, trang web quảng cáo, hoặc tồi tệ hơn là truy nhập vào thông tin tài khoản và có quyền tham gia và toàn bộ trang web.
- Chiếm quyền điều khiển: là hành động kiểm soát một phiên người dùng sau khi có thành công hay tạo ra xác thực ID. Là kiểu tấn công đòi hỏi mức độ cao về kỹ năng. 3 kỹ thuật chính thường được sử dụng là: brute – force, calculate, steal…

Câu 4: Các bước thực hiện điều tra tội phạm máy tính

Bao gồm 5 bước:

1. Quan sát, bảo vệ hiện trường vụ án.
2. Ghi và lập tài liệu về hiện trường.
3. Bảo quản chứng cứ.
4. Tiến hành điều tra.
5. Lập báo cáo điều tra.

Bước 1: quan sát, bảo vệ hiện trường.

- Đảm bảo hiện trường vụ án: tắt các thiết bị đang hoạt động, ngăn không cho bất kỳ ai truy cập.
- Xác định khu vực phạm tội.
- Hạn chế số lượng người được tiếp cận với hiện trường và tất cả các tài liệu tương tác với hiện trường vụ án: trong một số trường hợp, các hệ thống liên quan cần thiết cho hoạt động của nạn nhân cần được theo dõi. Ví dụ máy chủ CSDL của công ty đã bị hack và dữ liệu bị đánh cắp, họ sẽ vẫn cần máy chủ để tiếp tục hoạt động kinh doanh: triển khai máy chủ tạm thời, sao chép dữ liệu tới ổ đĩa mới, gắn ổ đĩa mới lên máy chủ tạm thời và tiếp tục cho hoạt động.

Bước 2: ghi và lập tài liệu về hiện trường.

- Không được chạm vào bát cứ gì cho tới khi bắt đầu thu thập bằng chứng.
- Ghi lại các chứng cứ thu thập được:
    - Quay video:
        - Ghi lại toàn bộ khung cảnh của hiện trường.
        - Phải luôn nêu ở đầu vieo người đã làm đoạn băng và chắc chắn thời gian là chính xác.
        - Nếu có tình tiết nổi bật thì phải có nhận xét về nó: cách thức kết nối được gắn vào máy tính hay các thiết bị khác, mô tả của căn phòng.
        - Cẩn thận với những lời nói trong video.
    - Chụp ảnh:
        - Trình bày một cách rõ nét và chi tiết: ngày tháng chụp, thời gian chụp, địa điểm chụp. => đảm bảo được thiết lập đúng.
        - Với một số loại máy ảnh (máy ảnh số hoặc máy film 35mm) cần sử dụng một tài liệu để ghi lại thông tin.
        - Theo “Crime Scene and Evidence Photographer’s Guide”:
            - Xây dựng quy trình hoạt động chuẩn.
            - Bảo vệ các hình ảnh kỹ thuật số ban đầu: nên thực hiện các thử nghiệm với 1 bản sao; không để mất tập tin ban đầu.
            - Bảo tồn ảnh ở định dạng ban đầu.
    - Các dây cáp gắn vào máy tính có thể cần phải tô màu để tránh nhầm lẫn:
        - Ghi lại các thiết bị gắn vào dây cáp.
        - Khi hoàn tất, ngắt kết nối các thiết bị với nhau.
- Các thông tin cần được ghi lại thành 1 bảng các sự kiện – tài liệu về hiện trường:

- Mô tả thời gian, ngày tháng.
- Các hành vi phạm tội.
- Các vật chứng bị tịch thu.
- Người xác nhận.

=> Ngăn chặn mất mát, thiệt hại vật chất, hoặc tiêu hủy chứng cứ.

Bước 3: bảo vệ chứng cứ.

- Tại hiện trường:
  - Đặt từng hạng mục thu được vào túi chứng cứ, đánh dấu đúng.
  - Đeo găng tay chống tĩnh trong khi thu thập và đưa vào túi bằng chứng.
  - Giữ bằng chứng nguyên vẹn cho đến khi mang đến khu vực an toàn của bộ phận điều tra.
- Khi vận chuyển:
  - Không để nhân viên, điều tra viên không có nghĩa vụ đặt bằng chứng trong xe của họ.
  - Dùng tủ khóa để bảo vệ các bằng chứng. Nếu lượng bằng chứng lớn cần đến một phòng để bảo vệ.
  - Bằng chứng phải được bảo vệ an toàn, lưu ý về nơi đặt chúng. Ví dụ máy tính không đặt bên cạnh loa hộp lớn bởi các máy tính có thể bị ảnh hưởng bởi các nam châm trong loa.

Lưu ý: nếu dữ liệu bị thay đổi bằng bất kỳ cách nào, nó có thể không được chấp nhận tại tòa án.

Bước 4: tiến hành điều tra.

- Các công việc cần thực hiện:
  - Thu thập và phân tích chứng cứ từ các linh kiện phần cứng.
  - Thu thập và phân tích chứng cứ từ hệ thống.

- Thu thập và phân tích chứng cứ từ email, điện thoại, thiết bị mạng…
- Nhiệm vụ: tìm ra các bằng chứng phạm tội và các hành vi phạm tội, để từ đó có thể quy trách nhiệm trước tòa án.

Bước 5: lập báo cáo điều tra.

- Mô tả toàn bộ các bước tiến hành điều tra từ lúc bắt đầu cho đến khi kết thúc.
- Là hồ sơ lưu trữ cho các công tác xử lý về sau.

Câu 5: Thu thập và phân tích chứng cứ từ mạng

Quá trình thu thập và phân tích chứng cứ từ mạng bao gồm phân tích gói tin và phân tích thống kê lưu lượng mạng.

1. **Phân tích gói tin**
   - Lắng nghe các gói tin hoạt động trên mạng (thông qua 1 máy nghe – sniffer).
   - Phân tích: các giao thức, quá trình bắt tay, các luông thông tin lưu chuyển trên mạng.

   Từ quá trình phân tích chỉ ra được:

   ⇨ Cấu tạo mạng.
   ⇨ Ai đang ở trên mạng.
   ⇨ Ai hoặc cái gì đang sử dụng băng thông.
   ⇨ Khả năng bị tấn công và các hành vi phá hoại.
   ⇨ Các ứng dụng không được bảo mật.
   - Cần lưu ý vị trí đặt máy nghe: đặt máy nghe đúng vị trí vật lý trong một mạng máy tính, nơi có số lượng lớn các thiết bị mạng phần cứng được sử dụng để kết nối các thiết bị với nhau.
   - Có nhiều công cụ hỗ trợ phân tích gói tin, phổ biến như Wireshark, Ettercap…

2. **Phân tích thống kê lưu lượng mạng**
    - Đo lượng thông lượng trong mạng:
        - Dữ liệu tối đa trong mỗi giây của một liên kết thông tin liên lạc hay một truy cập mạng.
        - Ví dụ: chuyển mội tập tin lớn từ một hệ thống sang một hệ thống khác và đo thời gian cần thiết để hoàn tất. Chia kích thước tập tin theo thời gian để có được kết quả theo megabit, kilobit, bit trên mỗi giây.
    - ⇨ Phát hiện các tấn công lên băng thông mạng (tấn công DDOS) hoặc tấn công chặn bắt thông tin trong hệ thống (tấn công ARP).
    - Các công cụ sử dụng đo băng thông sử dụng để xác định băng thông tối đa của một mạng hoặc kết nối internet: NetScp, Spirent Test Center, JDSU…

Câu 6: Thu thập và phân tích chứng cứ từ hệ thống

Quá trình thu thập và phân tích chứng cứ từ hệ thống bao gồm các quá trình thu thập dữ liệu từ trình duyệt, nhật ký trò chuyện và thu thập dữ liệu từ các file log hệ thống.

1. **Dữ liệu từ trình duyệt, nhật ký trò chuyện**
    - Bất kỳ các ứng dụng được sử dụng để giao tiếp trên Internet đều có khả năng chứa các chứng cứ: trình duyệt web, email khách hàng, các bản ghi trò chuyện.
    - Tìm kiếm chứng cứ trong các trình duyệt:
        - Lịch sử duyệt web.
        - Kiểm tra địa chỉ: thanh địa chỉ ghi lại những địa chỉ web mà tội phạm đã gõ vào.
        - Tìm kiếm thông qua các phần hiển thị: các trình duyệt thường lưu lại các thuật ngữ tìm kiếm được nhập trước đó.

⇨ Các tội phạm chuyên nghiệp thường không dùng biểu tượng của trình duyệt trên màn hình máy tính nên cần tìm kiếm tất cả các trình duyệt trên máy tính.

- Tìm chứng cứ thông qua nhật ký trò chuyện: các chat room cũng có thể được sử dụng để trao đổi thông tin giữa các tội phạm. Các phần mềm chat (Yahoo, MSN, Wechat, Zalo…) thường giữ ít nhất một bản ghi tạm thời của cuộc hội thoại => có thể tìm kiếm các manh mối có giá trị.

2. Thu thập dữ liệu từ các file log hệ thống

- Windows log:
  - Log ứng dụng: sự kiện đăng nhập bởi các ứng dụng.
  - Log bảo mật: việc sử dụng tài nguyên, số lần đăng nhập thành công/thất bại.
  - Log setup: sự kiện liên quan đến cài đặt ứng dụng.
  - Log hệ thống: các sự kiện liên quan các thành phần hệ thống.
  - Log sự kiện chuyển tiếp: các sự kiện thu thập được từ máy tính từ xa.
- Linux log:
  - /var/log/faillog: thông tin đăng nhập người dùng không thành công.
  - /var/log/kern.log: các thông điệp từ nhân của hệ điều hành.
  - /var/log/lpr.log: nhật ký máy in.
  - /var/log/mail.*: nhật ký máy chủ email.
  - /var/log/mysql: nhật ký máy chủ CSDL MySQL.
  - /var/log/apache2/*: các hoạt động liên quan tới máy chủ web apache.
  - /var/log/apport.log: nhật ký các ứng dụng bị treo.
  - /var/log/user.log: chứa bản ghi hoạt động của người dùng.

3. **Phục hồi dữ liệu bị xóa**
    - Phục hồi dữ liệu từ hệ điều hành Windows: khôi phục dữ liệu từ thùng rác, từ ổ đĩa.
    - Phục hồi dữ liệu từ hệ điều hành Linux:
        - Thông báo cho người dùng hệ thống: lệnh wall

            System is going down to… please save your work. Press CTRL+D to send message.
        - Khởi động lại máy và vào chế độ single user.
        - Sử dụng cú pháp:

grep -b ‘search-text /dev/partition > file.txt

hoặc grep -a -B[size before] -A[size after] ‘text’/dev/[your_partition] > file.txt

Ví dụ: # grep -i -a -B10 -A100 nixCraft’ /dev/sda1 > file.txt

        - Xem file.txt.

4. **Các vị trí quan trọng cần kiểm tra đối với hệ thống**
    - Trong Windows:
        - C:\Program Files: nơi cài đặt hầu hết các chương trình, nơi thường được tìm kiếm các phần mềm gián điệp, công cụ hack, phần mềm liên quan đến tội phạm máy tính.
        - C:\Windows: nơi lưu trữ các hệ điều hành.
        - C:\Windows\System32: chứa các file hệ thống quan trọng DLLs.
        - C:\Users\username\Documents: vị trí mặc định của các tài liệu.
        - C:\Users\username\Pictures: vị trí mặc định lưu hình ảnh của Windows.
        - C:\Users\username\Favorites: nơi Internet Explorer lưu trữ thư mục yêu thích của mỗi người dùng, nơi có thể tìm những trang web mà tội phạm có thể đánh dấu.

        - C:\Users\username\Desktop: màn hình máy tính người dùng.
        - C:\Users\username\Downloads: vị trí mặc định cho bất kỳ chương trình tải về từ Internet.
    - Trong Linux:
        - /home: tương tự thư mục C:\Users trong Windows.
        - /root: thư mục cho người quản trị có quyền root.
        - /var: chứa các mục quản trị như các bản ghi, cần kiểm tra kỹ lưỡng.
        - /temp: chứa các tập tin tạm thời.
        - /etc: chứa các tập tin cấu hình, các tội phạm thường thay đổi file cấu hình => cần so sánh các tập tin cấu hình trên máy tính bị nghi ngờ với phiên bản sao lưu.

Câu 7: Thu thập và phân tích chứng cứ từ nguồn khác

Quá trình thu thập và phân tích chứng cứ từ nguồn khác bao gồm các công việc như: truy tìm địa chỉ IP, chứng cứ từ Email, thiết bị mạng, điện thoại di động, tường lửa, hệ thống phát hiện xâm nhập.

1. **Truy tìm địa chỉ IP**
    - Sử dụng các lệnh truy vấn địa chỉ: tracert, traceroute.
    - Sử dụng Whois.
    - Sử dụng Visual Route.
2. **Chứng cứ từ Email**
    - Các phương pháp áp dụng:
        - Theo dõi nguồn gốc của Email: dựa vào tiêu đề, dựa vào công cụ.
        - Thu thập thông tin từ máy chủ Email: các email bị xóa có thể còn lưu lại trên máy chủ, các dữ liệu có thể liên quan đến bên thứ 3 – nhà cung cấp dịch vụ Internet (liên quan đến bản quyền).

3. **Chứng cứ từ các thiết bị mạng**
    - Kiểm tra switch, router để tìm chứng cứ:
        - Kết nối trực tiếp đến cổng Console của thiết bị.
        - Thiết lập kết nối thông qua mạng: sử dụng SSH.
        - Một số lệnh kiểm tra: show version, show running-config, show startup-config, show ip route.
4. **Chứng cứ từ điện thoại di động**
    - Các thông tin có thể thu thập như: hình ảnh, video, tin nhắn văn bản, tin SMS, thời gian gọi, cuộc gọi đã nhận, cuộc gọi nhỡ, thời gian cuộc gọi, tên danh bạ, các số điện thoại.
    - Các quy tắc cần lưu ý khi điều tra:
        - Luôn ghi lại nơi sản xuất, model, bất kỳ chi tiết nào về tình trạng điện thoại.
        - Chụp lại hình ảnh ban đầu của điện thoại.
        - Xem xét thẻ sim của điện thoại.
5. **Chứng cứ từ tường lửa**
    - Kiểm tra file log của tường lửa: nhật ký kết nối mạng ghi lại kết nối thành công hay thất bại, nhật ký ứng dụng.
    - Xem xét hệ thống tường lửa đã bị thỏa hiệp bởi kẻ tấn công hay chưa, xác định phương thức kẻ tấn công sử dụng để thỏa hiệp (thực hiện bằng cách ghi lại bộ nhớ RAM, xem xét các ứng dụng, giao thức đang sử dụng, cấu hình hệ thống).
6. **Chứng cứ từ hệ thống xâm nhập**
    - Tương tự như hệ thống tường lửa.

Câu 8: Kỹ thuật, công nghệ phòng chống tội phạm máy tính

Bao gồm: tường lửa, hệ thống IDS/IPS, ngăn chặn mã độc, mã hóa, một số kỹ thuật, công nghệ khác.

1. **Tưởng lửa**
    - Là thiết bị hoặc hệ thống dùng để điều khiển luồng lưu thông giữa các vùng mạng hoặc giữa các máy tính và mạng. Cũng có thể hiểu là một cơ chế để ngăn cách bảo vệ mạng tin tưởng khỏi mạng không tin tưởng.
    - Cơ chế hoạt động: kiểm soát tất cả lưu thông và truy cập giữa các vùng cần bảo vệ:
        - Những dịch vụ (port) nào bên trong được phép truy cập từ bên ngoài và ngược lại.
        - Những node mạng (user, địa chỉ IP) nào từ bên ngoài được phép truy cập đến các dịch vụ bên trong và ngược lại.
    - Phân loại: lọc gói, kiểm tra trạng thái, ứng dụng.
        - Tường lửa kiểm tra trạng thái là bộ lọc có kết hợp chặt chẽ với thông lấy từ lớp 4 của mô hình OSI. Nó cho phép client kết nối trực tiếp với server, có khả năng thực hiện kiểm tra tại bất kỳ phần nào của gói tin.

	Ưu điểm	Nhược điểm
Lọc gói	• Giá thành thấp. • Hoạt động nhanh. • Có khả năng chống lại tấn công từ chối dịch vụ, tấn công ở tầng thấp.	• Chỉ giới hạn kiểm soát gói tin ở header. • Không kiểm soát thông tin ở tầng cao (network trở lên). • Khả năng ghi log kém. • Xác thực người dùng khó khăn
Ứng dụng	• Hoạt động tới lớp 7. • Có khả năng xác thực. • Ít bị tấn công spoofing. • Có khả năng ghi lại nhiều thông tin nhật ký.	• Hoạt động chậm. • Không phù hợp với đường truyền đòi hỏi tốc độ cao hoặc ứng dụng đòi hỏi thời gian thực. • Khả năng hỗ trợ cho các ứng dụng và giao thức mới kém. •

2. Hệ thống IDS/IPS

- Phát hiện xâm nhập: quá trình giám sát các sự kiện xảy ra trong một hệ thống máy tính hoặc mạng và phân tích chúng để tìm ra các dấu hiệu của sự xâm nhập hoặc dấu hiệu về khả năng hệ thống bị xâm nhập.
- Phòng chống xâm nhập: hành vi của hệ thống tự động ngăn chặn các xâm nhập trái phép, có khả năng gây hại cho hệ thống.
- Hệ thống phát hiện xâm nhập: phần mềm hay thiết bị chuyên dụng làm nhiệm vụ tự động thực hiện các hành động phát hiện xâm nhập.
- Hệ thống phòng chống xâm nhập: phần mềm hay thiết bị chuyên dụng có khả năng phát hiện xâm nhập và có thể ngăn chựn các nguy cơ gây mất an ninh.

- Phương pháp phát hiện: dựa trên dấu hiệu, dựa trên sự bất thường, dựa trên phân tích trạng thái.

	Nội dung	Ưu điểm	Nhược điểm
Dựa trên dấu hiệu	Hệ thống sẽ thu thập các thông tin của các truy cập và so sánh với các mẫu dấu hiệu đặc trưng về tấn công đã được lưu trong hệ thống	• Nhanh chóng phát hiện ra các tấn công đã được xác định trước. • Giúp người quản trị có thể theo dõi được tấn công. • Ít tạo ra cảnh báo sai.	• Cần phải thường xuyên cập nhật các mẫu tấn công mới. • Không có khả năng nhớ các yêu cầu trước đó khi đang xử lý yêu cầu hiện tại.
Dựa trên sự bất thường	Các hoạt động bình thường của hệ thống sẽ được ghi nhận và lưu lại thành một hồ sơ theo dõi. Nếu có bất kỳ hành động không bình thường, hệ thống sẽ theo dõi, phân tích để cảnh báo	• Có khả năng phát hiện tấn công mới. • Không cần dựa vào mẫu có sẵn để phát hiện tấn công. • Có thể dựa vào đó để bổ sung các tấn công mới và mẫu tấn công.	• Yêu cầu người quản trị cần phải hiểu biết nhiều về tấn công. • Tạo ra nhiều cảnh bảo nhầm.
Dựa trên phân tích trạng thái của giao thức	Phân tích các hành vi của giao thức được sử dụng trên cơ sở biết được các định nghĩa về các hoạt động hợp lệ của giao thức để nhận ra hành vi tấn công.	• Có thể phát hiện được tấn công dựa trên giao thức.	• Không thể phát hiện các tấn công mà không vi phạm giao thức, ví dụ thực hiện nhiều hành động với giao thức được phép: Dos. • Có thể hiểu nhầm một vài giao thức được phép sử dụng trong ứng dụng hoặc hệ thống đặc biệt thành hành động tấn công.

- Phân loại: network – based, host – based.

Network-based	Host-based
• Giám sát các lưu thông qua mạng nhằm bảo vệ các thiết bị hoặc các phân đoạn mạng đặc biệt. • Phân tích các hành động tại lớp mạng hoặc lớp ứng dụng để phát hiện sự bất thường. • Được triển khai tại các đường biên giữa các mạng, gần firewall hay router, VPN server, remote access server, mạng không dây.	• Giám sát các hành động, sự kiện trên host nhằm phát hiện sự kiện bất thường trên chính host đó: lưu thông qua mạng, hệ thống log, tiến trình/ứng dụng đang hoạt động, thay đổi về cấu hình hệ thống và ứng dụng. • Được triển khai trên host, server, desktop, laptop…

3. Ngăn chặn mã độc

- Xử lý malware theo 4 bước:
  - Công tác chuẩn bị.
  - Nhận dạng và phân tích.
  - Ngăn chặn, tiêu diệt và khôi phục.
  - Công tác sau sự cố.
- Triển khai từ trên xuống:
  - Ngăn chặn virus tại các cửa ngõ.
  - Ngăn chặn virus tại các điểm có nhiều giao dịch.
  - Hạn chế việc nhiễm virus tại các desktop.
- Nguyên tắc chúng để phòng tránh và chống virus: ngăn chặn các con đường lây nhiễm.
  - Áp dụng các chính sách.
  - Nâng cao nhận thức.
  - Khắc phục các lỗ hổng bảo mật, cập nhật các bản vá lỗi thường xuyên.
  - Sử dụng các giải pháp kỹ thuật: hệ thống anti-virus…

4. **Mã hóa**
    - Hai phương pháp: mã hóa đối xứng và mã hóa bất đối xứng.
    - Mã hóa đối xứng:
        - Sử dụng một khóa để mã hóa và giải mã.
        - Xử lý nhanh nhưng độ an toàn không cao.
    - Mã hóa bất đối xứng:
        - Sử dụng hai khóa khác nhau để mã hóa và giải mã.
        - Xử lý chậm hơn, nhưng độ an toàn và tính thân thiện trong quản lý khóa cao.
    - Mã hóa thường có vai trò trong các giao dịch điện tử, chữ ký điện tử, hệ thống PKI.
5. **Các giải pháp khác**
    - Sử dụng giải pháp xác thực mạng.
    - Mạng riêng ảo.
    - Dò quét, đánh giá điểm yếu.
    - Chống tấn công mạng không dây…

Câu 9: Nâng cao nhận thức người sử dụng trong phòng chống tội phạm máy tính

- Cần thường xuyên cập nhật hệ điều hành và phần mềm.
- Sử dụng tài khoản không phải là quản trị viên bất cứ khi nào có thể.
- Sử dụng mật khẩu đủ mạng để đặt cho các tài khoản.
- Cần xem xét cẩn thận trước khi nhấp vào các liên kết hay tải xuống bất kỳ cái gì.
- Cần kiểm tra trước khi mở tệp đính kèm email hay hình ảnh.
- Không tin tưởng cửa sổ bật lên yêu cầu tài xuống phần mềm.
- Cẩn thận khi chia sẻ file trên web.
- Sử dụng phần mềm diệt virus.