ĐẠI HỌC QUỐC GIA TP. HỒ CHÍ MINH

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN

KHOA MẠNG MÁY TÌNH VÀ TRUYỀN THÔNG

UIT

Nguyễn Đại Nghĩa - 21521182

Phạm Hoàng Phúc - 21521295

Dương Phú Cường - 21521900

Lê Xuân Sơn - 21521386

ĐỀ CƯƠNG CHI TIẾT

Môn học: Pháp chứng kỹ thuật số

Lớp: NT334.P11.ATCL

CÁC KĨ THUẬT CHỐNG ĐIỀU TRA SỐ

GVHD: Lê Đức Thịnh

TP. HỒ CHÍ MINH, 2024

MỤC LỤC

I. Giới thiệu đồ án

Trong thời đại công nghệ số phát triển mạnh mẽ, thông tin cá nhân và dữ liệu số đang trở thành một trong những tài sản quý giá nhất mà các tổ chức và cá nhân có thể nắm giữ. Tuy nhiên, sự gia tăng các mối đe dọa từ hacker, tội phạm mạng và cả các cơ quan điều tra số đã đặt ra những thách thức lớn về bảo mật và quyền riêng tư. Các kĩ thuật chống điều tra số, hay còn gọi là anti-forensics, đã ra đời như một biện pháp đối phó nhằm che giấu hoặc làm biến dạng dữ liệu để tránh sự phát hiện, theo dõi và điều tra. Những kĩ thuật này bao gồm từ việc mã hóa, xóa bỏ vết tích dữ liệu đến làm mờ nhật ký truy cập, tất cả đều nhằm đảm bảo an toàn thông tin và quyền riêng tư cho người sử dụng.

Các kĩ thuật chống điều tra số không chỉ là công cụ phục vụ cho các hoạt động hợp pháp, như bảo vệ quyền riêng tư cá nhân hay bảo vệ các bí mật thương mại của doanh nghiệp, mà còn có thể bị lợi dụng trong các hoạt động bất hợp pháp như gian lận, rửa tiền hoặc tấn công mạng. Chính vì vậy, việc tìm hiểu và áp dụng các phương pháp này đòi hỏi phải có sự hiểu biết sâu sắc về cả mặt kỹ thuật và pháp lý.

II. Chi tiết

A. Pháp chứng mạng

Giới thiệu về Pháp chứng mạng:

Pháp chứng mạng (Network Forensics) là một nhánh của pháp chứng kỹ thuật số, tập trung vào việc giám sát, thu thập, ghi lại, phân tích và báo cáo dữ liệu mạng để xác định các hành vi, sự kiện có liên quan đến tội phạm mạng, các cuộc tấn công an ninh, hoặc các hoạt động bất thường trên mạng. Khác với pháp chứng ổ đĩa hoặc pháp chứng hệ điều hành, pháp chứng mạng tập trung vào việc điều tra các sự kiện xảy ra qua kết nối mạng, giúp tái hiện lại dòng dữ liệu giữa các máy tính, thiết bị và hệ thống mạng.

Mục tiêu chính của pháp chứng mạng là phát hiện, ghi nhận, và phân tích các dấu vết điện tử trên mạng, bao gồm cả các cuộc tấn công, truy cập trái phép, giao dịch dữ liệu bất thường, hay các hoạt động mã độc. Từ đó, các chuyên gia pháp chứng có thể tái hiện lại sự kiện, xác định nguồn gốc, và đưa ra bằng chứng cụ thể để hỗ trợ cho các cuộc điều tra pháp lý, hành chính, hoặc nội bộ của tổ chức.

Các thách thức trong Pháp chứng mạng:

Mặc dù pháp chứng mạng đóng vai trò quan trọng, nhưng nó cũng đối diện với nhiều thách thức lớn, đặc biệt trong bối cảnh an ninh mạng ngày càng phức tạp và tội phạm mạng ngày càng tinh vi. Một số thách thức chính bao gồm:

- Khối lượng dữ liệu khổng lồ: Với sự phát triển của Internet và các dịch vụ trực tuyến, lưu lượng dữ liệu mạng tăng trưởng theo cấp số nhân. Điều này làm cho việc thu thập, lưu trữ và phân tích tất cả dữ liệu trở nên rất khó khăn và đòi hỏi tài nguyên tính toán lớn. Các tổ chức phải sử dụng các phương pháp lọc và lựa chọn dữ liệu quan trọng, nhưng có nguy cơ bỏ sót các thông tin cần thiết.

- Mã hóa dữ liệu: Hiện nay, hầu hết các giao dịch trên mạng đều được mã hóa bằng các giao thức bảo mật như SSL/TLS (HTTPS). Điều này giúp bảo vệ dữ liệu người dùng, nhưng đồng thời cũng gây khó khăn cho các chuyên gia pháp chứng khi muốn phân tích lưu lượng. Mã hóa có thể che giấu nội dung của các gói tin, khiến cho việc phát hiện và điều tra các cuộc tấn công mạng khó khăn hơn rất nhiều.

- Tốc độ truyền dữ liệu và thời gian thực: Trong các cuộc tấn công mạng như DDoS, tốc độ truyền dữ liệu rất nhanh và lượng dữ liệu lớn. Việc phân tích và phản ứng kịp thời để phát hiện và ngăn chặn tấn công là một thách thức lớn. Đôi khi các công cụ pháp chứng không thể theo kịp tốc độ của cuộc tấn công và không thể phát hiện dấu vết kịp thời.

- Sự đa dạng của giao thức và công nghệ: Các hệ thống mạng sử dụng nhiều giao thức và công nghệ khác nhau, bao gồm IPv4, IPv6, HTTP/HTTPS, FTP, DNS, v.v. Các cuộc tấn công cũng có thể sử dụng các giao thức ít phổ biến hoặc thậm chí tùy chỉnh, khiến việc phân tích lưu lượng mạng trở nên phức tạp hơn.

- Mạng ẩn danh và dịch vụ proxy: Tội phạm mạng thường sử dụng các công cụ ẩn danh, chẳng hạn như Tor, VPN hoặc các dịch vụ proxy, để che giấu nguồn gốc của lưu lượng mạng. Điều này gây khó khăn cho việc truy vết kẻ tấn công và xác định

danh tính thật của chúng. Mạng Tor mã hóa lưu lượng và chuyển tiếp qua nhiều nút trước khi đến đích, làm giảm khả năng lần theo dấu vết từ hệ thống pháp chứng.

- Thiếu chuẩn hóa và công cụ pháp chứng mạng: Không phải tất cả các mạng và giao thức đều có chuẩn pháp chứng rõ ràng. Điều này dẫn đến khó khăn trong việc xác định phương pháp thu thập và phân tích chứng cứ. Các công cụ hiện có cũng chưa hoàn thiện và thường không tương thích với tất cả các hệ thống mạng, gây khó khăn trong việc thực hiện điều tra toàn diện.

Các kỹ thuật chống lại Pháp chứng mạng:

Trước những thách thức và tầm quan trọng của pháp chứng mạng, tội phạm mạng đã phát triển nhiều kỹ thuật và công cụ để gây khó khăn cho quá trình điều tra. Những kỹ thuật này thường nhằm mục tiêu ẩn danh, mã hóa hoặc làm nhiễu dữ liệu, khiến cho việc thu thập, phân tích và xác định các hành vi phạm tội trên mạng trở nên khó khăn hơn.

Dưới đây là chi tiết các kỹ thuật chính chống lại pháp chứng mạng, kèm theo mô tả, công cụ, các bước thực hiện và bất lợi khi sử dụng:

1. **Mã hóa lưu lượng mạng (Traffic Encryption)**

- ***Mô tả kỹ thuật*:**

Mã hóa lưu lượng mạng là một trong những kỹ thuật chính yếu được sử dụng để bảo vệ thông tin và dữ liệu trong quá trình truyền tải qua mạng. Mục tiêu của kỹ thuật này là đảm bảo rằng chỉ người gửi và người nhận mới có thể đọc được nội dung dữ liệu, trong khi các bên thứ ba (bao gồm cả những kẻ tấn công và các nhà điều tra pháp chứng) chỉ thấy các dữ liệu đã bị mã hóa mà không thể giải mã được nếu không có khóa.

Kỹ thuật mã hóa lưu lượng giúp tội phạm mạng giấu kín hoạt động của mình khỏi các hệ thống giám sát mạng hoặc các chuyên gia pháp chứng, đặc biệt là khi sử dụng các giao thức bảo mật như SSL/TLS (cho giao tiếp HTTPS), hoặc khi kết hợp với các dịch vụ VPN (Mạng ảo riêng) để mã hóa toàn bộ lưu lượng mạng.

Mã hóa bảo vệ dữ liệu bằng cách biến đổi nó thành dạng không thể đọc được nếu không có khóa giải mã. Các loại mã hóa phổ biến như AES (Advanced Encryption

Standard) hay RSA thường được sử dụng để bảo vệ dữ liệu trong khi truyền qua mạng.

- ***Công cụ sử dụng:***
  - VPN (Virtual Private Network): VPN là công cụ phổ biến nhất để mã hóa toàn bộ lưu lượng mạng giữa thiết bị của người dùng và máy chủ VPN, giúp giấu đi địa chỉ IP và đảm bảo rằng không ai, kể cả các nhà cung cấp dịch vụ Internet (ISP) hoặc kẻ tấn công trên mạng, có thể theo dõi nội dung của dữ liệu.

  - SSL/TLS (Secure Sockets Layer/Transport Layer Security): Giao thức bảo mật này được sử dụng để mã hóa các kết nối trên web, tạo ra kết nối an toàn giữa trình duyệt và máy chủ web thông qua HTTPS.

  - SSH (Secure Shell): Giao thức SSH được sử dụng để mã hóa các kết nối điều khiển từ xa và truyền tệp, giúp bảo vệ dữ liệu khỏi bị giám sát.

  - Tor (The Onion Router): Mạng Tor cho phép mã hóa và ẩn danh lưu lượng mạng bằng cách chuyển tiếp nó qua nhiều điểm nút trung gian, giúp giấu nguồn gốc của lưu lượng và mã hóa toàn bộ quá trình truyền tải.

- ***Các bước thực hiện:***

  Cài đặt và cấu hình VPN:

  Tải xuống một dịch vụ VPN, sau đó cấu hình thiết bị để tất cả lưu lượng đi qua máy chủ VPN.

  VPN mã hóa tất cả lưu lượng giữa người dùng và máy chủ VPN, sau đó giải mã và gửi dữ liệu đến đích. Từ góc nhìn của bất kỳ kẻ giám sát nào, toàn bộ lưu lượng chỉ là các gói tin mã hóa, không thể thấy nội dung dữ liệu hoặc xác định nguồn gốc thực sự của nó.

Sử dụng SSL/TLS:

Cài đặt chứng chỉ SSL/TLS trên máy chủ web và yêu cầu kết nối HTTPS từ các trình duyệt. Điều này đảm bảo rằng tất cả các dữ liệu được truyền tải giữa người dùng và máy chủ đều được mã hóa.

Khi người dùng truy cập một trang web qua HTTPS, dữ liệu sẽ được mã hóa bằng TLS trong suốt quá trình truyền, ngăn chặn việc bị kẻ tấn công nghe lén.

Sử dụng Tor để mã hóa và ẩn danh:

Cài đặt Tor Browser để truy cập internet thông qua mạng Tor. Tor sẽ mã hóa lưu lượng và chuyển tiếp nó qua nhiều điểm chuyển tiếp (relay), khiến việc xác định địa chỉ IP thật sự và nguồn gốc lưu lượng trở nên rất khó khăn.

Mỗi lớp chuyển tiếp sẽ chỉ biết địa chỉ IP trước đó và địa chỉ của lớp kế tiếp, trong khi nội dung dữ liệu vẫn được mã hóa.

- ***Bất lợi khi sử dụng mã hóa lưu lượng mạng***

Mặc dù mã hóa lưu lượng mạng là một kỹ thuật mạnh mẽ để bảo vệ quyền riêng tư và ẩn danh dữ liệu, nhưng nó cũng đi kèm với một số bất lợi:

Giảm hiệu suất mạng:

Mã hóa tiêu tốn tài nguyên tính toán, đặc biệt khi sử dụng các giao thức mã hóa mạnh như AES-256 hoặc RSA-2048. Điều này có thể làm giảm tốc độ truyền tải và thời gian phản hồi của mạng, đặc biệt là khi sử dụng VPN hoặc Tor.

Mạng Tor thường chậm do lưu lượng phải được chuyển tiếp qua nhiều điểm chuyển tiếp (relay), làm tăng độ trễ và giảm tốc độ tải dữ liệu.

Dễ bị phát hiện:

Các dịch vụ VPN, mặc dù mã hóa lưu lượng, nhưng có thể bị phát hiện bởi các hệ thống phát hiện xâm nhập (IDS/IPS) hoặc bị chặn bởi các nhà cung cấp dịch vụ Internet (ISP). Một số trang web hoặc dịch vụ thậm chí có thể chặn truy cập từ các địa chỉ IP liên quan đến VPN hoặc mạng Tor.

Mã hóa SSL/TLS cũng có thể bị giám sát thông qua phân tích hành vi hoặc meta-data (chẳng hạn như thông tin về kích thước gói tin, tần suất truy cập).

Yêu cầu cấu hình kỹ thuật:

Để triển khai SSL/TLS hoặc sử dụng VPN an toàn, yêu cầu một số kỹ năng kỹ thuật để cấu hình đúng cách và đảm bảo rằng không có lỗ hổng bảo mật trong quá trình cài đặt.

Cấu hình Tor yêu cầu kiến thức về mạng và bảo mật để tránh lộ thông tin trong quá trình truy cập.

Phụ thuộc vào bên thứ ba:

Khi sử dụng VPN, dữ liệu của người dùng phải đi qua máy chủ VPN của nhà cung cấp dịch vụ. Nếu nhà cung cấp VPN không đảm bảo bảo mật hoặc bị tấn công, dữ liệu của người dùng có thể bị lộ.

Trong trường hợp của Tor, mặc dù bảo mật tốt, nhưng cũng không hoàn toàn miễn nhiễm với các lỗ hổng tiềm năng từ các điểm chuyển tiếp (exit node).

- ***Kết luận về Mã hóa lưu lượng mạng:***

  Mã hóa lưu lượng mạng là một kỹ thuật rất hiệu quả để bảo vệ dữ liệu và đảm bảo quyền riêng tư trong quá trình truyền tải trên mạng, đặc biệt là trong các trường hợp muốn tránh bị giám sát hoặc truy vết bởi các hệ thống pháp chứng mạng. Tuy nhiên, như đã phân tích, việc sử dụng các công cụ mã hóa như VPN, SSL/TLS, và Tor không hoàn toàn hoàn hảo và có những hạn chế nhất định về mặt hiệu suất, khả năng bị phát hiện, và phụ thuộc vào cấu hình kỹ thuật.

  Bất chấp những hạn chế này, mã hóa vẫn là một trong những công cụ chính yếu mà các cá nhân và tổ chức sử dụng để chống lại pháp chứng mạng, ngăn chặn các điều tra viên pháp lý thu thập và phân tích dữ liệu mạng trong các cuộc điều tra tội phạm kỹ thuật số.

2. Sử dụng mạng ẩn danh (Anonymization via Proxy and Tor)

- ***Mô tả kỹ thuật***

Sử dụng mạng ẩn danh là một kỹ thuật quan trọng giúp người dùng che giấu danh tính thực sự và hoạt động trực tuyến của mình khỏi các hệ thống giám sát hoặc pháp chứng mạng. Mục tiêu chính của kỹ thuật này là làm mờ hoặc ẩn đi địa chỉ IP và nguồn gốc lưu lượng mạng, giúp cho việc truy vết trở nên khó khăn hơn, từ đó bảo vệ danh tính và ngăn chặn các cuộc điều tra số.

Các dịch vụ ẩn danh như Proxy và Tor cho phép người dùng chuyển lưu lượng mạng của mình qua các máy chủ trung gian hoặc các điểm nút (nodes) trước khi đến đích, giúp giấu đi địa chỉ IP thật và ẩn danh toàn bộ hoạt động. Điều này khác với mã hóa lưu lượng mạng, vì mục tiêu chính của mạng ẩn danh không phải là bảo vệ nội dung dữ liệu mà là che giấu địa chỉ IP và danh tính của người dùng.

- ***Phương pháp sử dụng Proxy***

Proxy hoạt động bằng cách đóng vai trò trung gian giữa người dùng và máy chủ đích, giúp người dùng giấu đi địa chỉ IP thực của mình. Khi sử dụng proxy, người dùng gửi yêu cầu đến máy chủ proxy, máy chủ này sau đó gửi yêu cầu đến đích và trả lại kết quả cho người dùng. Tất cả lưu lượng từ người dùng sẽ được chuyển qua máy chủ proxy, và địa chỉ IP của người dùng sẽ được thay thế bằng địa chỉ IP của proxy.

- ***Công cụ sử dụng Proxy***
  - SOCKS Proxy: Một loại proxy cấp thấp, không chỉ hỗ trợ giao thức HTTP mà còn cho các giao thức mạng khác như FTP, SMTP. SOCKS5 là phiên bản mới nhất và có thể kết hợp với mã hóa.
  - HTTP Proxy: Loại proxy này chỉ hỗ trợ lưu lượng HTTP. Địa chỉ IP của người dùng sẽ bị ẩn khi truy cập các trang web qua HTTP Proxy.

- ProxySwitchy: Tiện ích mở rộng cho trình duyệt giúp dễ dàng chuyển đổi giữa các máy chủ proxy khác nhau trong thời gian thực.

- ***Các bước thực hiện với Proxy***

  Chọn một dịch vụ Proxy: Chọn một dịch vụ SOCKS hoặc HTTP Proxy.

  Cấu hình Proxy: Cấu hình trình duyệt hoặc ứng dụng để sử dụng địa chỉ máy chủ proxy. Ví dụ, trên trình duyệt web, có thể vào cài đặt mạng để thêm địa chỉ proxy và số cổng.

  Chuyển lưu lượng qua Proxy: Khi cấu hình thành công, tất cả lưu lượng từ trình duyệt hoặc ứng dụng sẽ được gửi qua máy chủ proxy, giúp che giấu địa chỉ IP thực của người dùng.

- ***Bất lợi khi sử dụng Proxy***

  Bảo mật kém: Proxy, đặc biệt là các HTTP Proxy không cung cấp mã hóa cho dữ liệu truyền tải, nghĩa là nội dung dữ liệu vẫn có thể bị giám sát bởi các bên thứ ba, ngay cả khi địa chỉ IP được ẩn.

  Hiệu suất giảm: Sử dụng proxy có thể làm giảm tốc độ truy cập do phải đi qua máy chủ trung gian trước khi đến đích.

- ***Phương pháp sử dụng Tor***

  Tor là một mạng ẩn danh phi tập trung cho phép người dùng ẩn đi danh tính của mình bằng cách chuyển lưu lượng mạng qua nhiều điểm nút (relay nodes) trước khi đến đích. Tor sử dụng một mô hình "hành tây" (onion) để mã hóa dữ liệu qua nhiều lớp, mỗi lớp sẽ bị bóc ra tại một điểm nút, nhưng không có điểm nút nào biết được toàn bộ hành trình của lưu lượng.

  Mỗi điểm nút trên mạng Tor chỉ biết địa chỉ IP của điểm trước đó và điểm tiếp theo, nhưng không thể biết được nguồn gốc hoặc đích cuối cùng của lưu lượng.

Điều này khiến cho việc theo dõi và truy vết người dùng qua Tor trở nên rất khó khăn.

- ***Công cụ sử dụng Tor***
  - Tor Browser: Một trình duyệt mã nguồn mở được thiết kế đặc biệt để truy cập mạng Tor, cho phép người dùng truy cập các trang web mà không để lộ địa chỉ IP thực.
  - Whonix: Một hệ điều hành bảo mật sử dụng Tor để đảm bảo mọi lưu lượng mạng đi qua hệ thống đều được truyền qua mạng Tor, ẩn danh hoàn toàn.

- ***Bất lợi khi sử dụng Tor***

  Hiệu suất chậm: Do lưu lượng phải đi qua nhiều điểm nút trên mạng Tor, tốc độ truy cập thường chậm hơn nhiều so với việc truy cập trực tiếp.

  Khả năng bị chặn: Một số dịch vụ trực tuyến và mạng doanh nghiệp có thể phát hiện lưu lượng Tor và chặn các địa chỉ IP liên quan đến Tor, khiến cho người dùng không thể truy cập vào các dịch vụ này.

  Rủi ro từ exit node: Dữ liệu không được mã hóa sau khi rời khỏi mạng Tor tại "exit node", điều này có nghĩa là nếu dữ liệu không sử dụng HTTPS, nội dung có thể bị giám sát tại điểm này.

- ***So sánh giữa 2 phương pháp***

Đặc điểm	Proxy	Tor
Ẩn danh	Che giấu địa chỉ IP nhưng không hoàn toàn ẩn danh do máy chủ proxy có thể lưu trữ dữ liệu	Che giấu địa chỉ IP hiệu quả hơn nhờ mạng lưới phi tập trung
Mã hóa	Chỉ mã hóa dữ liệu nếu kết hợp với giao thức HTTPS	Mã hóa đa lớp qua mỗi điểm nút trong mạng Tor

Hiệu suất	Tốc độ nhanh hơn Tor nhưng vẫn chậm hơn so với kết nối trực tiếp	Tốc độ chậm hơn nhiều do lưu lượng phải đi qua nhiều điểm nút
Bảo mật	Bảo mật thấp, dữ liệu có thể bị theo dõi tại máy chủ proxy	Bảo mật cao hơn, nhưng dữ liệu không được mã hóa tại exit node nếu không sử dụng HTTPS
Khả năng bị phát hiện	Dễ bị phát hiện và chặn bởi các hệ thống IDS hoặc các dịch vụ trực tuyến	Khó phát hiện hơn, nhưng vẫn có thể bị chặn ở một số mạng hoặc dịch vụ
Mức độ ẩn danh	Thấp hơn Tor, phụ thuộc vào máy chủ proxy	Rất cao, khó truy vết người dùng do mạng phi tập trung và mã hóa nhiều lớp

- ***Kết luận về sử dụng mạng ẩn danh***

  Sử dụng mạng ẩn danh là một phương pháp quan trọng giúp che giấu danh tính và hoạt động mạng, đặc biệt hữu ích cho những người muốn tránh bị truy vết hoặc theo dõi trong môi trường mạng công khai. Proxy và Tor đều có ưu điểm và nhược điểm riêng, phù hợp với các mục tiêu khác nhau. Trong khi Proxy dễ sử dụng hơn và có tốc độ nhanh hơn, Tor cung cấp mức độ bảo mật và ẩn danh cao hơn nhờ mã hóa nhiều lớp và mạng lưới phi tập trung.

  Tuy nhiên, khi sử dụng mạng ẩn danh, người dùng phải chấp nhận các bất lợi về hiệu suất, khả năng bị chặn, và rủi ro bảo mật tại một số điểm trong quá trình truyền tải. Điều này đòi hỏi người dùng phải cân nhắc kỹ lưỡng và tuân thủ các biện pháp bảo mật bổ sung để bảo vệ quyền riêng tư và danh tính của mình.

3. Fragmentation and Packet Manipulation (Phân mảnh và thao tác gói tin)

- ***Mô tả kỹ thuật***

  Phân mảnh gói tin và thao tác gói tin là những kỹ thuật nhằm làm rối loạn quá trình truyền dữ liệu qua mạng và gây khó khăn cho việc phân tích lưu lượng mạng của các hệ thống pháp chứng. Phân mảnh là quá trình chia nhỏ một gói dữ liệu lớn thành nhiều phần nhỏ để truyền qua mạng, sau đó các gói tin này sẽ được tái hợp ở phía nhận. Trong khi đó, thao tác gói tin bao gồm các hành động chỉnh sửa, giả mạo hoặc làm biến đổi thông tin trong gói dữ liệu, như thay đổi địa chỉ IP, số cổng, hoặc nội dung gói tin để làm rối các hệ thống giám sát hoặc pháp chứng mạng.

- ***Những kỹ thuật này được sử dụng để:***

  Che giấu thông tin trong gói tin bằng cách chia nhỏ dữ liệu hoặc thay đổi các trường dữ liệu để gây khó khăn cho các công cụ phân tích.

  Tránh phát hiện: Các hệ thống giám sát và phát hiện xâm nhập thường gặp khó khăn khi phải theo dõi và tái hợp các gói tin đã bị phân mảnh hoặc thao tác.

  Đánh lạc hướng: Bằng cách giả mạo hoặc chỉnh sửa gói tin, kẻ tấn công có thể tạo ra các gói tin giả để đánh lạc hướng điều tra, khiến quá trình truy tìm nguồn gốc trở nên phức tạp hơn.

- ***Công cụ sử dụng***
  - Fragroute: Một công cụ mạnh mẽ được thiết kế để phân mảnh và thao tác các gói tin trên mạng. Fragroute cho phép người dùng chỉ định các quy tắc tùy chỉnh để sửa đổi, phân mảnh, và gửi gói tin theo các điều kiện nhất định. Đây là một công cụ thường được sử dụng trong các bài kiểm thử thâm nhập để kiểm tra tính an toàn của mạng.

  - Scapy: Scapy là một công cụ Python mạnh mẽ cho phép tạo, thao tác và gửi các gói tin tùy chỉnh. Nó cho phép người dùng tạo ra các gói tin IP, TCP, UDP, ICMP, và nhiều giao thức khác, đồng thời hỗ trợ việc phân mảnh và giả mạo gói tin.

- Hping3: Một công cụ dòng lệnh để tạo và thao tác các gói tin tùy chỉnh, giả mạo địa chỉ IP, và gửi các gói tin TCP, UDP, ICMP theo các thông số được chỉ định. Hping3 thường được sử dụng trong các bài kiểm tra bảo mật mạng để kiểm tra tính an toàn của hệ thống.

- ***Bất lợi khi sử dụng Fragmentation và Packet Manipulation***

  Mặc dù các kỹ thuật phân mảnh và thao tác gói tin mang lại lợi ích cho việc che giấu dữ liệu hoặc tránh bị phát hiện, nhưng chúng cũng đi kèm với một số bất lợi và rủi ro:

  Dễ bị phát hiện bởi hệ thống IDS/IPS:

  Các hệ thống phát hiện xâm nhập tiên tiến (IDS/IPS) có thể nhận diện các mẫu phân mảnh bất thường hoặc các hành vi thao tác gói tin và phát hiện ra cuộc tấn công. Chẳng hạn, việc phân mảnh quá mức hoặc các gói tin với các giá trị trường không hợp lệ có thể kích hoạt cảnh báo trong các hệ thống an ninh mạng.

  Hiệu suất mạng bị giảm:

  Việc phân mảnh gói tin có thể làm giảm hiệu suất mạng do phải truyền tải nhiều gói tin nhỏ thay vì một gói tin lớn, điều này cũng làm tăng độ trễ và giảm hiệu quả truyền thông. Nếu các gói tin bị phân mảnh quá nhiều, chúng cũng có thể không được tái hợp đúng cách ở phía nhận, gây mất dữ liệu.

  Khả năng phân tích và tái hợp dữ liệu:

  Mặc dù phân mảnh làm khó khăn cho việc phân tích dữ liệu, nhưng các hệ thống pháp chứng hiện đại có thể có khả năng tái hợp lại các gói tin đã bị phân mảnh nếu thu thập đầy đủ dữ liệu từ cả hai phía gửi và nhận.

  Lỗi tái hợp dữ liệu:

Trong một số trường hợp, phân mảnh gói tin có thể dẫn đến lỗi khi gói tin đến nơi không được tái hợp đúng cách, dẫn đến hỏng dữ liệu hoặc mất thông tin quan trọng.

- ***Kết luận về Fragmentation and Packet Manipulation***

Phân mảnh và thao tác gói tin là hai kỹ thuật mạnh mẽ giúp tội phạm mạng che giấu hành vi của mình và tránh bị phát hiện trong quá trình điều tra pháp chứng. Bằng cách chia nhỏ gói tin hoặc thay đổi thông tin trong gói tin, tội phạm có thể đánh lừa hệ thống phát hiện và làm khó khăn cho quá trình phân tích dữ liệu. Tuy nhiên, các kỹ thuật này cũng có những hạn chế như làm giảm hiệu suất mạng và có thể bị phát hiện bởi các hệ thống giám sát hiện đại.

Với sự phát triển của các công cụ và hệ thống IDS/IPS tiên tiến, khả năng phát hiện các hành vi bất thường trong quá trình phân mảnh và thao tác gói tin ngày càng được cải thiện. Do đó, mặc dù các kỹ thuật này có thể tạm thời gây khó khăn cho các nhà điều tra, nhưng nếu không được thực hiện cẩn thận, chúng vẫn có thể bị phát hiện và dẫn đến việc lộ dấu vết của tội phạm.

4. Steganography over Network Traffic (Giấu thông tin trong lưu lượng mạng)

- ***Mô tả kỹ thuật***

Steganography là một kỹ thuật dùng để giấu thông tin một cách kín đáo trong các dữ liệu khác mà không làm thay đổi đáng kể sự nhận diện của dữ liệu gốc. Khác với mã hóa, nơi dữ liệu được bảo vệ bằng cách biến đổi nó thành một dạng không thể đọc được nếu không có khóa giải mã, steganography tập trung vào việc giấu dữ liệu sao cho không ai biết được rằng dữ liệu đang tồn tại. Khi ứng dụng steganography vào lưu lượng mạng, mục tiêu chính là giấu dữ liệu trong các gói tin hoặc trường dữ liệu ít sử dụng của các giao thức mạng, làm cho các hệ thống giám sát hoặc pháp chứng khó phát hiện.

Steganography trong lưu lượng mạng có thể sử dụng nhiều phương pháp khác nhau để giấu thông tin trong các giao thức và gói tin mà vẫn giữ nguyên tính toàn

vẹn của luồng dữ liệu. Các thông tin ẩn có thể được chèn vào các phần không quan trọng của gói tin hoặc sử dụng kỹ thuật chèn dữ liệu vào các trường mà giao thức mạng cho phép, chẳng hạn như IP Options, TCP Options, hoặc thậm chí trong các dữ liệu ứng dụng như HTTP, DNS.

- ***Mục tiêu chính của steganography qua lưu lượng mạng***

  Giấu thông tin bí mật: Steganography qua lưu lượng mạng cho phép che giấu các dữ liệu nhạy cảm hoặc bất hợp pháp khỏi hệ thống giám sát, nhằm tránh bị phát hiện bởi các công cụ pháp chứng mạng.

  Tránh sự phát hiện: Các hệ thống giám sát thông thường khó có thể phát hiện ra các hoạt động steganography bởi các gói tin và lưu lượng mạng vẫn trông có vẻ hợp lệ, không có dấu hiệu rõ ràng của dữ liệu bị ẩn giấu.

  Gây nhiễu thông tin pháp chứng: Khi các nhà điều tra phân tích lưu lượng, thông tin giấu kín có thể không được phát hiện nếu không sử dụng các kỹ thuật phân tích đặc thù để tìm ra dữ liệu steganographic.

- ***Công cụ sử dụng***
  - Netcat: Một công cụ mạng dòng lệnh cơ bản cho phép truyền tải dữ liệu qua các giao thức TCP/UDP. Netcat có thể được sử dụng để truyền các tệp tin đã được giấu thông qua steganography qua các kênh mạng.

  - Scapy: Một công cụ mạnh mẽ cho phép tạo, thao tác, và gửi các gói tin tùy chỉnh. Scapy có thể được sử dụng để chèn dữ liệu vào các trường ít sử dụng của các giao thức mạng như TCP, IP, hoặc ICMP để giấu thông tin.

  - DNSCat2: Công cụ này cho phép tạo các kênh liên lạc bí mật thông qua giao thức DNS. Thông tin có thể được giấu trong các truy vấn và phản hồi DNS mà không làm thay đổi hoạt động bình thường của giao thức DNS.

- ***Các kỹ thuật giấu thông tin trong lưu lượng mạng***

Giấu thông tin trong trường không sử dụng của các giao thức (Protocol Field Steganography)

·Nhiều giao thức mạng có các trường dữ liệu không sử dụng hoặc các trường tùy chọn mà có thể chứa thông tin mà không ảnh hưởng đến chức năng của gói tin. Ví dụ:

TCP Options: Trường TCP Options thường được sử dụng để tối ưu hóa việc truyền tải, nhưng một phần của nó có thể bị tận dụng để chứa thông tin giấu kín. Các thông tin này có thể được mã hóa hoặc chia thành các đoạn nhỏ để giấu trong nhiều gói tin.

IP Options: Trường IP Options trong tiêu đề IP cũng có thể chứa các dữ liệu bổ sung. Kỹ thuật giấu dữ liệu trong các tùy chọn này có thể làm cho các gói tin vẫn hợp lệ về mặt chức năng mà không bị phát hiện.

ICMP Payload: Giao thức ICMP có một trường payload mà thường chứa thông tin kiểm tra kết nối. Tuy nhiên, trường này có thể được lợi dụng để chứa dữ liệu giấu.

Giấu thông tin trong payload của các giao thức mạng (Data Hiding in Protocol Payloads)

Các giao thức như HTTP, DNS, và ICMP có các payload dữ liệu thường được sử dụng để truyền tải thông tin giữa các máy tính, nhưng chúng cũng có thể được lợi dụng để giấu thông tin bí mật.

HTTP Steganography: Dữ liệu có thể được giấu trong các header HTTP, trong nội dung của các trang web hoặc trong các trường của biểu mẫu HTTP (GET, POST).

DNS Steganography: Sử dụng các truy vấn và phản hồi DNS để truyền thông tin giấu kín mà không làm thay đổi hoạt động của giao thức DNS.

Giấu thông tin trong dữ liệu ứng dụng (Application Data Steganography)

Ngoài việc giấu dữ liệu trong các trường giao thức mạng, dữ liệu cũng có thể được giấu trong các tệp ứng dụng (như tệp văn bản, hình ảnh, âm thanh) trước khi truyền tải chúng qua mạng. Sau khi giấu thông tin vào một tệp (ví dụ, một hình ảnh JPEG), tệp này có thể được truyền qua giao thức HTTP hoặc FTP mà không ai biết rằng nó chứa dữ liệu bí mật.

- ***Bất lợi khi sử dụng steganography qua lưu lượng mạng***

Mặc dù steganography là một kỹ thuật mạnh mẽ để giấu dữ liệu trong lưu lượng mạng, nó cũng đi kèm với những bất lợi:

Dung lượng dữ liệu hạn chế:

Do các giao thức mạng có giới hạn về kích thước gói tin và các trường dữ liệu, lượng thông tin có thể giấu trong mỗi gói tin thường rất nhỏ. Việc giấu dữ liệu lớn có thể yêu cầu nhiều gói tin, làm tăng khả năng bị phát hiện.

Hiệu suất mạng:

Quá trình chia nhỏ dữ liệu và giấu thông tin trong nhiều gói tin hoặc trường dữ liệu có thể làm chậm tốc độ truyền tải và gây giảm hiệu suất mạng, đặc biệt khi phải gửi nhiều gói tin để chứa dữ liệu.

Khả năng bị phát hiện bởi các hệ thống phân tích chuyên sâu:

Các công cụ pháp chứng tiên tiến có thể phân tích chi tiết các trường không thường được sử dụng hoặc các hành vi bất thường trong lưu lượng mạng, từ đó phát hiện ra các thông tin bị giấu. Nếu kỹ thuật giấu dữ liệu không được thực hiện khéo léo, nó có thể dễ dàng bị phát hiện.

Cấu hình phức tạp:

Steganography yêu cầu cấu hình kỹ thuật chi tiết và phải đảm bảo rằng thông tin giấu kín không làm thay đổi hoạt động bình thường của lưu lượng mạng. Nếu không được thực hiện cẩn thận, nó có thể gây ra lỗi mạng hoặc khiến lưu lượng trở nên khả nghi.

- ***Kết luận về steganography qua lưu lượng mạng***

Steganography over network traffic là một phương pháp tinh vi để giấu thông tin trong lưu lượng mạng mà không làm thay đổi đáng kể các hoạt động mạng. Kỹ thuật này cho phép tội phạm mạng hoặc những kẻ tấn công che giấu thông tin nhạy cảm trong các gói tin hoặc các trường dữ liệu ít sử dụng của các giao thức, từ đó né tránh các hệ thống giám sát và pháp chứng mạng. Tuy nhiên, như mọi kỹ thuật giấu thông tin, steganography cũng có những hạn chế về dung lượng, hiệu suất và có thể bị phát hiện nếu sử dụng không khéo léo.

Việc sử dụng steganography trong lưu lượng mạng yêu cầu người thực hiện phải có hiểu biết sâu rộng về các giao thức mạng và công cụ để đảm bảo rằng dữ liệu được giấu một cách khéo léo mà không bị phát hiện bởi các công cụ pháp chứng mạng hiện đại.

5. Làm rối dữ liệu và nhật ký (Log Tampering and Noise Injection)

- ***Mô tả kỹ thuật***

Làm rối dữ liệu và nhật ký (Log Tampering) và tạo nhiễu (Noise Injection) là hai kỹ thuật trong chống pháp chứng nhằm mục tiêu làm sai lệch hoặc gây khó khăn cho quá trình phân tích dữ liệu của các điều tra viên. Kẻ tấn công có thể thay đổi hoặc xóa các bản ghi (logs) trên hệ thống, từ đó che giấu hoạt động bất hợp pháp hoặc làm rối loạn các manh mối quan trọng. Đồng thời, kỹ thuật tạo nhiễu giúp làm tăng khối lượng dữ liệu vô nghĩa, khiến việc phân tích dữ liệu thực trở nên phức tạp và tốn nhiều tài nguyên hơn.

a. Làm rối nhật ký (Log Tampering)

Nhật ký (logs) là một trong những nguồn dữ liệu quan trọng nhất đối với các điều tra viên pháp chứng. Chúng cung cấp thông tin chi tiết về các hoạt động diễn ra trên hệ thống, bao gồm việc đăng nhập, các kết nối mạng, thay đổi tệp tin, và các

lỗi hệ thống. Nếu kẻ tấn công có thể thay đổi, xóa hoặc làm sai lệch các bản ghi này, điều đó có thể làm mờ đi những bằng chứng quan trọng hoặc che giấu sự hiện diện của cuộc tấn công.

- ***Công cụ và phương pháp sử dụng***

  Timestomping (Làm mờ dấu vết thời gian)

  Mục tiêu: Thay đổi dấu thời gian của các tệp tin và nhật ký để làm sai lệch thứ tự và thời gian diễn ra các sự kiện.

  Công cụ: Timestomp (có sẵn trên hệ điều hành Kali Linux) hoặc các công cụ tùy chỉnh khác.

  Chi tiết: Kẻ tấn công có thể thay đổi các dấu thời gian của các tệp nhật ký hoặc tệp hệ thống để làm cho chúng xuất hiện như thể các sự kiện đã xảy ra vào những thời điểm khác nhau, gây rối loạn cho quá trình phân tích của điều tra viên.

  Xóa hoặc thay đổi nhật ký hệ thống

  Mục tiêu: Xóa hoàn toàn các bản ghi nhật ký về hoạt động đáng ngờ hoặc thay đổi thông tin để che giấu dấu vết.

  Công cụ: echo, sed, logrotate, metasploit.

  Chi tiết: Kẻ tấn công có thể sử dụng các lệnh hệ thống hoặc các công cụ như Metasploit để xóa hoặc sửa đổi các tệp nhật ký. Ví dụ, bằng cách xóa các dòng chứa thông tin về địa chỉ IP, thời gian đăng nhập hoặc hoạt động mạng của kẻ tấn công, hệ thống sẽ không còn ghi nhận lại các sự kiện này.

b. Tạo nhiễu dữ liệu (Noise Injection)

Tạo nhiễu là kỹ thuật tạo ra dữ liệu giả hoặc vô nghĩa nhằm làm nhiễu loạn quá trình thu thập và phân tích của điều tra viên. Kỹ thuật này có thể làm tăng khối lượng dữ liệu cần xử lý, khiến cho điều tra viên khó khăn trong việc phân biệt giữa dữ liệu thật và dữ liệu giả, từ đó làm chậm quá trình điều tra hoặc thậm chí khiến họ bỏ lỡ các bằng chứng quan trọng.

- ***Công cụ và phương pháp sử dụng***

  Tạo ra các kết nối mạng giả

  Mục tiêu: Tạo ra nhiều kết nối mạng giả để làm nhiễu log mạng và gây khó khăn cho việc xác định các hoạt động thực sự của kẻ tấn công.

  Công cụ: Hping3, Scapy.

  Chi tiết: Kẻ tấn công có thể sử dụng Hping3 để tạo ra nhiều gói tin TCP/UDP giả mạo, gây nhiễu trong lưu lượng mạng. Điều này làm tăng khối lượng lưu lượng mà điều tra viên phải phân tích, khiến cho quá trình xác định các hoạt động bất thường trở nên phức tạp hơn.

  Tạo ra các sự kiện hệ thống giả

  Mục tiêu: Tạo các sự kiện giả mạo trong nhật ký hệ thống nhằm làm rối loạn dòng thời gian và gây nhầm lẫn.

  Công cụ: echo, logger.

  Chi tiết: Bằng cách thêm các dòng log giả mạo hoặc các sự kiện không có thật vào nhật ký hệ thống, kẻ tấn công có thể làm cho điều tra viên nhầm lẫn về các sự kiện thực sự đã xảy ra. Ví dụ, tạo ra nhiều bản ghi đăng nhập giả mạo để làm nhiễu các bản ghi thực.

  Tạo dữ liệu mạng giả với Scapy

  Mục tiêu: Gửi các gói tin mạng giả mạo hoặc không hợp lệ để làm rối loạn hệ thống thu thập chứng cứ.

  Công cụ: Scapy.

  Chi tiết: Bằng cách tạo ra các gói tin có nội dung ngẫu nhiên hoặc không hợp lệ, kẻ tấn công có thể làm cho các hệ thống giám sát phải phân tích một lượng lớn dữ liệu không có ý nghĩa.

- ***Kết luận về Làm rối dữ liệu và nhật ký (Log Tampering và Noise Injection)***

  Làm rối dữ liệu và nhật ký (Log Tampering và Noise Injection) là những kỹ thuật mạnh mẽ trong chống pháp chứng mạng để ngăn cản hoặc gây khó khăn cho việc thu thập và phân tích dữ liệu của các điều tra viên. Bằng cách xóa bỏ hoặc thay đổi thông tin trong các bản ghi nhật ký, kẻ tấn công có thể làm sai lệch thông tin quan trọng, khiến cho điều tra viên không thể xác định chính xác thời gian, địa điểm hoặc phương pháp tấn công.

  Tạo nhiễu dữ liệu là một phương pháp bổ sung giúp làm tăng khối lượng dữ liệu cần phân tích, từ đó làm chậm quá trình điều tra và khiến điều tra viên khó khăn hơn trong việc phân biệt giữa dữ liệu thật và dữ liệu giả.

  Các kỹ thuật này yêu cầu kẻ tấn công có kiến thức sâu rộng về hệ thống và nhật ký, cũng như sử dụng thành thạo các công cụ như Metasploit, Timestomp, Hping3, và Scapy. Tuy nhiên, với sự phát triển của các hệ thống pháp chứng và giám sát tiên tiến, việc sử dụng các kỹ thuật này cần được thực hiện cẩn thận để tránh bị phát hiện.

Kết luận

Tổng kết lại, pháp chứng mạng là một lĩnh vực không thể thiếu trong bảo vệ an ninh mạng và điều tra tội phạm kỹ thuật số. Tuy nhiên, với sự phát triển không ngừng của các kỹ thuật chống lại pháp chứng, các chuyên gia điều tra số cần liên tục nâng cấp công cụ và kỹ thuật của mình để theo kịp sự tinh vi của tội phạm mạng.

Các kỹ thuật như mã hóa, ẩn danh, phân mảnh gói tin, steganography và giả mạo gói tin đều có khả năng gây khó khăn cho quá trình điều tra. Tuy nhiên, khi các kỹ thuật chống lại pháp chứng ngày càng được sử dụng rộng rãi, các hệ thống phát hiện và công cụ điều tra mạng cũng ngày càng tiên tiến, đòi hỏi các chuyên gia pháp chứng phải luôn sẵn sàng học hỏi và cập nhật kiến thức để đối phó với các thách thức mới.

Pháp chứng mạng, dù đối mặt với nhiều thách thức, vẫn là một công cụ thiết yếu trong việc bảo vệ các tổ chức và hệ thống khỏi tội phạm mạng. Sự kết hợp giữa các kỹ năng phân tích và công nghệ tiên tiến sẽ giúp các điều tra viên pháp chứng vượt qua các kỹ thuật chống lại điều tra và giữ vững an ninh trong không gian mạng.

B. Pháp chứng OS (Window)

Giới thiệu về Pháp chứng Windows:

Pháp chứng Windows (Windows Forensics) là một nhánh quan trọng của pháp chứng kỹ thuật số, tập trung vào việc điều tra và phân tích các hệ thống sử dụng hệ điều hành Microsoft Windows để phát hiện và tái tạo lại các sự kiện có liên quan đến các hoạt động trái pháp luật hoặc sự cố an ninh. Windows là hệ điều hành phổ biến nhất trên toàn cầu, do đó việc điều tra trên các hệ thống Windows là rất cần thiết trong quá trình khám phá bằng chứng kỹ thuật số.

Pháp chứng Windows bao gồm việc thu thập, phân tích, và lưu giữ các bằng chứng kỹ thuật số từ một loạt các nguồn trên hệ điều hành Windows như file hệ thống, các bản ghi nhật ký (logs), bộ nhớ, Registry, và dữ liệu ứng dụng. Pháp chứng viên có thể trích xuất thông tin về các hoạt động người dùng, ứng dụng đã chạy, file đã tạo, sửa đổi hoặc xóa, cũng như các cuộc kết nối mạng và các sự kiện hệ thống quan trọng khác.

Các thành phần chính trong pháp chứng Windows

Pháp chứng trên hệ điều hành Windows thường tập trung vào những khu vực sau:

File system (Hệ thống tệp)

NTFS (New Technology File System) là hệ thống tệp mặc định trên các phiên bản Windows hiện đại. Phân tích hệ thống tệp bao gồm việc khôi phục các tệp bị xóa, phân tích các thuộc tính file (metadata), và tìm kiếm các vùng dữ liệu ẩn (slack space, unallocated space).

Master File Table (MFT) trong NTFS chứa thông tin chi tiết về tất cả các tệp và thư mục trên hệ thống, bao gồm ngày tạo, ngày sửa đổi, và quyền truy cập.

Windows Registry

Windows Registry là một cơ sở dữ liệu lưu trữ các thông tin quan trọng về cấu hình hệ thống, các cài đặt ứng dụng, thông tin về người dùng, và các hành động đã diễn ra trên hệ thống. Điều tra Registry có thể giúp xác định những ứng dụng đã được cài đặt, các thiết bị đã được kết nối, và những file nào đã được mở gần đây.

Các khóa quan trọng trong Registry như Run keys, UserAssist, và MRU (Most Recently Used) giúp xác định những hành động của người dùng.

Event logs (Nhật ký sự kiện)

Event Viewer là nơi lưu trữ các bản ghi chi tiết về các sự kiện xảy ra trên hệ thống Windows, bao gồm các sự kiện đăng nhập, các thay đổi về cấu hình hệ thống, và các lỗi hệ thống.

Nhật ký sự kiện là một nguồn quan trọng để theo dõi hành vi của người dùng, sự cố hệ thống, hoặc các cuộc tấn công an ninh mạng.

Shadow Copies (Bản sao bóng)

Shadow Copies là các bản sao lưu tự động của tệp tin và thư mục, được tạo bởi tính năng Volume Shadow Copy của Windows. Các bản sao này có thể giúp khôi phục lại những file đã bị xóa hoặc bị thay đổi.

Prefetch Files

Prefetch Files là các tệp do Windows tạo ra nhằm tối ưu hóa quá trình khởi chạy ứng dụng. Chúng lưu trữ thông tin về các chương trình đã được chạy trên hệ thống, giúp điều tra viên xác định được các chương trình nào đã được mở gần đây.

Pagefile và Hibernation Files

Pagefile và hiberfil.sys chứa các dữ liệu tạm thời mà Windows lưu trữ khi bộ nhớ (RAM) đầy hoặc khi hệ thống chuyển sang trạng thái ngủ (hibernate). Các file này có thể chứa dữ liệu về các chương trình đang chạy, các tài liệu mở, hoặc các hoạt động mạng, và là nguồn thông tin quan trọng trong điều tra pháp chứng.

Browser Artifacts

Trình duyệt web lưu trữ các dữ liệu về hoạt động duyệt web của người dùng, bao gồm lịch sử truy cập, cookie, cache, và tệp tin tải xuống. Điều này có thể giúp xác định những trang web mà người dùng đã truy cập, thời gian truy cập, và những tệp tin nào đã được tải xuống.

Thùng rác (Recycle Bin)

Recycle Bin chứa các file đã bị người dùng xóa, nhưng chưa bị loại bỏ hoàn toàn khỏi hệ thống. Pháp chứng viên có thể phục hồi và phân tích các tệp này để xác định xem có tài liệu quan trọng nào đã bị xóa không.

Các thách thức trong pháp chứng Windows

Mặc dù pháp chứng Windows là một công cụ mạnh mẽ để điều tra số, nhưng nó cũng đối diện với nhiều thách thức:

Khối lượng dữ liệu khổng lồ: Một hệ thống Windows có thể chứa hàng triệu file và bản ghi, điều này làm cho việc phân tích toàn diện trở nên rất tốn thời gian và đòi hỏi các công cụ mạnh mẽ.

Mã hóa và bảo mật: Kẻ tấn công có thể sử dụng các phương pháp mã hóa hoặc các công cụ bảo mật khác để bảo vệ dữ liệu hoặc xóa bỏ dấu vết của mình, khiến việc phân tích và thu thập bằng chứng trở nên khó khăn.

Thao tác và làm giả: Kẻ tấn công có thể thay đổi hoặc xóa bỏ các nhật ký và các dấu vết khác trên hệ thống để che giấu các hoạt động trái phép, gây rối loạn quá trình điều tra.

Tính phức tạp của hệ điều hành: Hệ điều hành Windows có nhiều thành phần phức tạp và các phiên bản khác nhau, mỗi phiên bản có thể có những tính năng riêng biệt, làm cho việc điều tra yêu cầu sự hiểu biết chi tiết và chính xác về hệ thống.

Các kỹ thuật chống lại Pháp chứng Windows (Anti-forensics Techniques in Windows Forensics)

Trong bối cảnh chống pháp chứng Windows, các kỹ thuật anti-forensics được thiết kế để ngăn cản, làm mờ, hoặc vô hiệu hóa quá trình thu thập, phân tích và tái hiện lại các hành vi của người dùng trên hệ điều hành Windows. Mục tiêu chính của các kỹ thuật này là làm cho các nhà điều tra gặp khó khăn trong việc truy vết hoạt động của kẻ tấn công, giảm thiểu khả năng thu thập chứng cứ hoặc gây nhầm lẫn trong quá trình phân tích.

Dưới đây là các kỹ thuật phổ biến nhất trong chống pháp chứng Windows, cùng với mô tả, công cụ và bất lợi khi sử dụng.

1. Xóa Dữ liệu An toàn (Secure Deletion)

- ***Mô tả kỹ thuật***

Xóa dữ liệu an toàn (Secure Deletion) là một kỹ thuật được sử dụng để xóa bỏ vĩnh viễn dữ liệu từ các thiết bị lưu trữ, nhằm đảm bảo rằng dữ liệu không thể phục hồi được, ngay cả với các công cụ pháp chứng mạnh mẽ. Trong hệ điều hành Windows, khi người dùng xóa tệp bằng cách thông thường (như sử dụng lệnh "Delete"), dữ liệu không thực sự bị xóa khỏi ổ đĩa mà chỉ được đánh dấu là "đã xóa" trong hệ thống tệp. Dữ liệu này vẫn tồn tại trên ổ đĩa và có thể được khôi phục bằng các công cụ phục hồi dữ liệu.

Xóa dữ liệu an toàn bao gồm các phương pháp ghi đè nhiều lần lên dữ liệu gốc bằng các mẫu ngẫu nhiên hoặc không có ý nghĩa, từ đó làm cho việc khôi phục lại dữ liệu trở nên cực kỳ khó khăn hoặc không thể thực hiện được. Đây là một biện pháp chống lại các kỹ thuật pháp chứng nhằm khôi phục dữ liệu đã bị xóa, chẳng hạn như trong các trường hợp tội phạm mạng hoặc các cá nhân muốn bảo vệ thông tin nhạy cảm của mình.

- ***Các kỹ thuật xóa dữ liệu an toàn***

a. Ghi đè dữ liệu nhiều lần (Multiple Overwrite)

Nguyên lý: Phương pháp này hoạt động bằng cách ghi đè dữ liệu mới lên vùng chứa dữ liệu cũ nhiều lần với các mẫu ngẫu nhiên hoặc được xác định trước. Điều này làm cho các công cụ phục hồi dữ liệu không thể khôi phục lại dữ liệu gốc.

Chi tiết: Một tệp tin sẽ bị ghi đè nhiều lần, thường từ 3 đến 7 lần, hoặc theo chuẩn quân sự (DoD 5220.22-M), có thể ghi đè lên tới 35 lần (Gutmann method). Mỗi lần ghi đè sẽ thay thế dữ liệu hiện có bằng các mẫu ngẫu nhiên hoặc số 0, số 1.

b. Xóa tệp và ghi đè không gian trống (Wiping Free Space)

Nguyên lý: Khi tệp bị xóa, dữ liệu vẫn nằm trong các vùng không gian trống của ổ đĩa. Xóa không gian trống (wiping free space) là quá trình ghi đè lên toàn bộ vùng không gian trống trên ổ đĩa, đảm bảo rằng không có dữ liệu bị xóa nào còn tồn tại ở đó mà có thể khôi phục lại được.

Chi tiết: Sau khi một tệp bị xóa, công cụ xóa an toàn sẽ ghi đè lên toàn bộ không gian trống trên ổ đĩa nhiều lần để đảm bảo dữ liệu đã xóa thực sự không thể phục hồi.

c. Xóa tệp tin hoán trang (Pagefile) và file ngủ đông (Hibernate file)

Nguyên lý: Pagefile và hiberfile.sys là các tệp hệ thống lưu trữ dữ liệu tạm thời từ bộ nhớ RAM khi máy tính hết dung lượng hoặc chuyển sang trạng thái ngủ đông. Các tệp này có thể chứa thông tin nhạy cảm, như dữ liệu người dùng hoặc các tài liệu đang mở, và cần phải được xóa an toàn để bảo vệ thông tin.

Chi tiết: Xóa pagefile và hiberfile bằng cách ghi đè nhiều lần lên các tệp này đảm bảo rằng không có thông tin nào có thể bị phục hồi từ các tệp tạm thời này.

d. Xóa toàn bộ ổ đĩa (Wiping Entire Disk)

Nguyên lý: Phương pháp này được sử dụng khi cần xóa toàn bộ ổ đĩa lưu trữ. Thay vì chỉ xóa từng tệp tin, toàn bộ ổ đĩa sẽ bị ghi đè nhiều lần với các mẫu ngẫu nhiên. Kỹ thuật này thường được áp dụng khi muốn xóa sạch dữ liệu khỏi ổ cứng trước khi bán hoặc tái sử dụng thiết bị.

Chi tiết: Khi sử dụng phương pháp này, ổ đĩa sẽ được ghi đè toàn bộ, từ đầu đến cuối, loại bỏ hoàn toàn mọi dấu vết dữ liệu cũ.

- ***Các công cụ xóa dữ liệu an toàn phổ biến***

a. SDelete

SDelete là một công cụ dòng lệnh do Microsoft Sysinternals phát triển, giúp xóa an toàn tệp tin và không gian trống trên ổ đĩa bằng cách ghi đè nhiều lần lên dữ liệu. Công cụ này hỗ trợ các kỹ thuật như ghi đè một lần, hoặc tuân theo chuẩn xóa của Bộ Quốc phòng Mỹ (DoD 5220.22-M), nhằm đảm bảo rằng dữ liệu không thể khôi phục lại được.

b. CCleaner

CCleaner là một công cụ phổ biến có thể dọn dẹp hệ thống, bao gồm các tệp tạm, cookie, và các tệp không cần thiết. CCleaner cũng cung cấp chức năng xóa an toàn (secure delete), cho phép ghi đè lên các tệp tin đã xóa và không gian trống trên ổ đĩa nhiều lần để ngăn ngừa khả năng khôi phục.

c. BleachBit

BleachBit là một công cụ mã nguồn mở hỗ trợ xóa dữ liệu an toàn trên nhiều nền tảng khác nhau, bao gồm Windows. BleachBit không chỉ giúp xóa tệp tin mà còn có thể xóa các dấu vết ứng dụng (như cache trình duyệt, lịch sử tệp tin) và không gian trống trên ổ đĩa.

d. DBAN (Darik's Boot and Nuke)

DBAN là một công cụ xóa dữ liệu toàn bộ ổ đĩa (wiping entire disk). Công cụ này thường được sử dụng khi cần xóa sạch dữ liệu trước khi bán lại hoặc tái sử dụng thiết bị. DBAN hoạt động trên nhiều chuẩn xóa dữ liệu, như DoD 5220.22-M hoặc Gutmann, để đảm bảo rằng mọi dữ liệu cũ đều bị loại bỏ hoàn toàn.

e. Eraser

Eraser là một công cụ mã nguồn mở mạnh mẽ để xóa an toàn các tệp tin riêng lẻ hoặc toàn bộ ổ đĩa. Nó cung cấp nhiều phương pháp ghi đè, từ cách ghi đè đơn giản đến các phương pháp phức tạp hơn như Gutmann (35 lần ghi đè).

- ***Các rủi ro và bất lợi của kỹ thuật xóa dữ liệu an toàn***

  Tốn thời gian: Ghi đè nhiều lần lên dữ liệu, đặc biệt với các phương pháp phức tạp như Gutmann, có thể mất rất nhiều thời gian, đặc biệt là trên các ổ đĩa dung lượng lớn.

  Hiệu năng giảm: Trên các ổ đĩa SSD, ghi đè nhiều lần có thể làm giảm tuổi thọ của thiết bị. Điều này là do cơ chế lưu trữ dữ liệu của ổ đĩa SSD khác với ổ cứng HDD truyền thống, và mỗi lần ghi đè sẽ tiêu hao một phần tuổi thọ của thiết bị.

  Khó khăn khi sử dụng trên SSD: Các kỹ thuật ghi đè thông thường không hoạt động hiệu quả trên ổ đĩa SSD do cơ chế quản lý dữ liệu nội bộ của SSD. SSD có các phương thức tự động như TRIM để quản lý việc ghi đè, nhưng chúng không đảm bảo hoàn toàn việc xóa vĩnh viễn dữ liệu.

  Có thể bị nghi ngờ: Việc sử dụng các công cụ xóa an toàn có thể làm tăng nghi ngờ từ các nhà điều tra pháp chứng nếu họ phát hiện ra rằng các dữ liệu quan trọng đã bị xóa bằng phương pháp an toàn.

- ***Kết luận***

  Xóa dữ liệu an toàn là một kỹ thuật mạnh mẽ trong chống pháp chứng Windows, giúp bảo vệ thông tin nhạy cảm và ngăn chặn việc khôi phục dữ liệu bị xóa. Các công cụ và phương pháp ghi đè nhiều lần giúp đảm bảo rằng dữ liệu không còn khả năng phục hồi, làm giảm thiểu nguy cơ phát hiện bởi các nhà điều tra pháp chứng. Tuy nhiên, kỹ thuật này cũng có những rủi ro và hạn chế, bao gồm việc tốn thời gian, giảm hiệu năng của thiết bị lưu trữ và có thể gây nghi ngờ. Trong bối cảnh chống pháp chứng, xóa dữ liệu an toàn vẫn là một kỹ thuật quan trọng và hiệu quả khi cần bảo vệ thông tin khỏi việc bị khôi phục sau khi bị xóa.

2. Mã hóa Dữ liệu (Data Encryption)

- ***Mô tả kỹ thuật***

Mã hóa dữ liệu là một trong những kỹ thuật quan trọng nhất trong chống pháp chứng nhằm bảo vệ dữ liệu khỏi sự truy cập trái phép. Bằng cách biến đổi dữ liệu thành một định dạng không thể đọc được nếu không có khóa giải mã, mã hóa giúp ngăn cản các nhà điều tra pháp chứng hoặc các công cụ thu thập chứng cứ có thể truy xuất và phân tích nội dung. Mục tiêu chính của mã hóa là bảo mật thông tin bằng cách sử dụng các thuật toán mã hóa mạnh mẽ, đảm bảo rằng ngay cả khi dữ liệu bị thu thập, nó cũng không thể được sử dụng nếu không có quyền truy cập hợp lệ.

Mã hóa được sử dụng để bảo vệ dữ liệu ở nhiều cấp độ, bao gồm:

Mã hóa toàn bộ ổ đĩa (Full Disk Encryption - FDE):

Nguyên lý: Toàn bộ ổ đĩa, bao gồm cả hệ điều hành, dữ liệu người dùng, và các tập tin hệ thống, đều được mã hóa. Dữ liệu chỉ có thể truy cập được sau khi nhập đúng mật khẩu hoặc khóa giải mã khi khởi động hệ thống.

Mã hóa file và thư mục: Chỉ mã hóa những tệp tin hoặc thư mục nhạy cảm.

- ***Công cụ mã hóa phổ biến***

a. BitLocker (Mã hóa toàn bộ ổ đĩa - FDE)

BitLocker là một công cụ mã hóa ổ đĩa toàn phần (FDE) của Microsoft, có sẵn trong các phiên bản Windows từ Windows 7 trở đi. BitLocker mã hóa toàn bộ ổ đĩa hệ thống và bảo vệ nó bằng mật khẩu hoặc mã khóa khởi động.

b. VeraCrypt (Mã hóa tệp tin và ổ đĩa)

VeraCrypt là một công cụ mã hóa mã nguồn mở dựa trên TrueCrypt, cho phép mã hóa ổ đĩa và phân vùng, cũng như tạo các container mã hóa để lưu trữ dữ liệu an toàn.

c. AxCrypt (Mã hóa tệp tin đơn lẻ)

AxCrypt là một công cụ mã hóa mã nguồn mở, tập trung vào việc bảo mật tệp tin đơn lẻ. Nó cho phép người dùng mã hóa và giải mã các tệp tin một cách nhanh chóng với một mật khẩu đơn giản.

- ***Rủi ro và bất lợi của mã hóa dữ liệu trong chống pháp chứng Windows***

  Mất mật khẩu hoặc khóa giải mã: Nếu mất mật khẩu hoặc khóa giải mã, không có cách nào để truy cập lại dữ liệu đã mã hóa. Điều này có thể dẫn đến mất dữ liệu vĩnh viễn.

  Hiệu suất hệ thống giảm: Mã hóa toàn bộ ổ đĩa có thể làm giảm hiệu suất của hệ thống, đặc biệt là trên các thiết bị có cấu hình thấp. Việc truy xuất dữ liệu mã hóa cần nhiều tài nguyên hơn, làm chậm tốc độ đọc/ghi dữ liệu.

  Bị phát hiện dễ dàng: Nếu các nhà điều tra phát hiện ra rằng một hệ thống đã được mã hóa nhưng không có mật khẩu giải mã, điều này có thể làm gia tăng nghi ngờ về hành vi chống pháp chứng.

  Cần quản lý mật khẩu an toàn: Việc mã hóa yêu cầu người dùng phải bảo mật mật khẩu hoặc khóa giải mã một cách cẩn thận. Mất thông tin này không chỉ gây mất dữ liệu mà còn có thể khiến người dùng dễ bị lộ thông tin nhạy cảm nếu khóa bị đánh cắp.

Không bảo vệ hoàn toàn: Mã hóa chỉ bảo vệ dữ liệu trong trạng thái "đang lưu trữ". Nếu hệ thống đang hoạt động và người dùng đã mở khóa ổ đĩa, dữ liệu vẫn có thể bị truy xuất hoặc phân tích bởi các nhà điều tra nếu họ có quyền truy cập vào hệ thống tại thời điểm đó.

- ***Các chiến lược mã hóa để chống pháp chứng Windows***

  Mã hóa toàn bộ ổ đĩa: Để bảo vệ tối đa, người dùng nên mã hóa toàn bộ ổ đĩa hệ thống và các ổ đĩa lưu trữ khác bằng các công cụ như BitLocker hoặc VeraCrypt. Điều này đảm bảo rằng tất cả dữ liệu, bao gồm cả các tệp hệ thống và file tạm, đều được bảo vệ.

  Sử dụng mã hóa file ẩn: VeraCrypt cung cấp tính năng "container ẩn", cho phép tạo một phân vùng hoặc tệp tin ẩn trong ổ đĩa đã mã hóa. Ngay cả khi người dùng bị ép cung cấp mật khẩu, container ẩn vẫn giữ dữ liệu nhạy cảm an toàn.

  Mã hóa kết hợp với xóa an toàn: Sau khi mã hóa dữ liệu, nếu không cần thiết lưu trữ nữa, người dùng có thể sử dụng các công cụ xóa an toàn như SDelete để đảm bảo rằng dữ liệu đã được xóa không thể khôi phục được.

- ***Kết luận về Mã hóa Dữ liệu trong chống pháp chứng Windows***

  Mã hóa dữ liệu là một kỹ thuật quan trọng và mạnh mẽ trong việc chống pháp chứng trên hệ điều hành Windows. Việc sử dụng mã hóa giúp ngăn chặn các nhà điều tra truy cập trái phép vào dữ liệu nhạy cảm và cung cấp lớp bảo vệ vững chắc đối với các cuộc điều tra pháp chứng. Tuy nhiên, người dùng phải đối mặt với những rủi ro như mất mật khẩu, hiệu suất hệ thống giảm và khả năng bị nghi ngờ khi phát hiện dữ liệu mã hóa. Do đó, mã hóa cần được sử dụng cẩn thận, kết hợp với các biện pháp bảo vệ khác như xóa an toàn và quản lý mật khẩu để đạt hiệu quả tối ưu trong việc ngăn chặn thu thập chứng cứ.

3. Làm mờ Dấu thời gian (Timestomping)

- ***Mô tả kỹ thuật***

Làm mờ dấu thời gian (Timestomping) là một kỹ thuật trong chống pháp chứng nhằm thay đổi hoặc làm giả các dấu thời gian của tệp tin và thư mục trên hệ thống để gây khó khăn cho quá trình điều tra kỹ thuật số. Dấu thời gian trên các tệp tin và hệ thống Windows chứa thông tin quan trọng về thời gian tạo tệp (creation time), chỉnh sửa cuối cùng (modification time), và truy cập lần cuối (access time). Những thông tin này thường được sử dụng để xác định thứ tự và thời điểm xảy ra các hành động trên hệ thống, chẳng hạn như thời gian một tệp tin được tạo, sao chép, sửa đổi, hoặc truy cập.

Bằng cách thay đổi các dấu thời gian, kẻ tấn công có thể làm cho các sự kiện trở nên khó hiểu hoặc không chính xác, khiến các nhà điều tra gặp khó khăn trong việc tái hiện lại dòng thời gian của sự kiện. Điều này có thể dẫn đến việc bỏ qua các bằng chứng quan trọng hoặc gây nhầm lẫn trong quá trình điều tra.

Các dấu thời gian trong hệ thống tệp NTFS

Trong hệ điều hành Windows, đặc biệt là hệ thống tệp NTFS, mỗi tệp tin và thư mục đều có ba dấu thời gian quan trọng:

Create Time (Thời gian tạo): Thời gian mà tệp tin được tạo lần đầu tiên trên hệ thống.

Modify Time (Thời gian chỉnh sửa): Thời gian tệp tin được sửa đổi lần cuối, chẳng hạn như nội dung của tệp tin bị thay đổi.

Access Time (Thời gian truy cập): Thời gian lần cuối cùng tệp tin được truy cập (chỉ đọc, không cần chỉnh sửa).

Entry Modified Time (Thời gian thay đổi bản ghi): Thời gian mà bản ghi MFT (Master File Table) của tệp tin bị sửa đổi.

- ***Lợi ích của kỹ thuật Timestomping trong chống pháp chứng***

  Làm rối loạn dòng thời gian: Khi dấu thời gian bị thay đổi, các nhà điều tra không thể xác định chính xác thời điểm một tệp tin được tạo hoặc thay đổi. Điều này làm cho dòng thời gian của sự kiện trở nên mơ hồ và không thể tái hiện chính xác.

  Che giấu hoạt động: Kẻ tấn công có thể thay đổi dấu thời gian của một tệp tin để làm cho nó trông như đã được tạo từ trước hoặc sau một thời điểm nhất định, từ đó che giấu hoạt động của mình và khiến điều tra viên bỏ qua tệp tin quan trọng.

  Đánh lạc hướng điều tra: Timestomping có thể được sử dụng để tạo ra các dấu hiệu giả, làm điều tra viên tập trung vào các sự kiện sai lệch hoặc không quan trọng, từ đó làm họ đi lệch hướng.

- ***Công cụ sử dụng để làm mờ dấu thời gian***

1. Timestomp (Metasploit Framework)

   Timestomp là một công cụ nổi tiếng trong Metasploit Framework, cho phép kẻ tấn công thay đổi các dấu thời gian của tệp tin trên hệ điều hành Windows. Công cụ này hỗ trợ thay đổi thời gian tạo, chỉnh sửa, và truy cập của tệp, làm cho việc điều tra trở nên phức tạp hơn.

2. BulkFileChanger (NirSoft)

   BulkFileChanger là một công cụ từ NirSoft cho phép người dùng chỉnh sửa thuộc tính của nhiều tệp tin cùng lúc, bao gồm việc thay đổi các dấu thời gian như thời gian tạo, sửa đổi và truy cập. Công cụ này hữu ích cho việc thao tác nhanh chóng trên một lượng lớn tệp tin.

3. SetFileTime (Command Line Tool)

SetFileTime là một công cụ dòng lệnh, cho phép thay đổi dấu thời gian của tệp tin thông qua giao diện dòng lệnh. Công cụ này thường được sử dụng trong các kịch bản tự động hóa để thay đổi dấu thời gian của nhiều tệp một cách nhanh chóng.

- ***Bất lợi khi sử dụng Timestomping***

Có thể bị phát hiện: Mặc dù thay đổi các dấu thời gian có thể làm rối loạn quá trình điều tra, nhưng các công cụ pháp chứng hiện đại có thể phát hiện các hành vi timestomping. Ví dụ, khi các dấu thời gian không khớp nhau (như thời gian truy cập trước thời gian tạo), điều này có thể tạo ra nghi ngờ.

Không xóa được các bằng chứng khác: Timestomping chỉ thay đổi dấu thời gian của tệp tin, nhưng không xóa bỏ các bằng chứng khác liên quan đến tệp tin đó, chẳng hạn như các bản ghi hệ thống (logs), thông tin trong Windows Registry, hoặc các bản sao lưu trong Shadow Copies.

Lưu dấu vết trong nhật ký hệ thống: Quá trình thay đổi dấu thời gian có thể bị ghi lại trong các bản ghi nhật ký sự kiện (event logs) của hệ thống, đặc biệt nếu hệ thống giám sát các hành vi bất thường trên tệp tin.

Khó thực hiện trên các hệ thống được giám sát kỹ lưỡng: Trong các môi trường bảo mật cao, các hệ thống phát hiện xâm nhập (IDS/IPS) có thể theo dõi sự thay đổi của tệp tin và phát hiện ra các hành vi timestomping bất thường.

- ***Kết luận về Timestomping***

Timestomping là một kỹ thuật chống pháp chứng phổ biến, cho phép kẻ tấn công làm rối loạn quá trình điều tra bằng cách thay đổi hoặc giả mạo các dấu thời gian

của tệp tin và thư mục. Kỹ thuật này giúp che giấu các hoạt động của kẻ tấn công, làm cho việc tái hiện lại các sự kiện trở nên khó khăn hơn cho điều tra viên.

Tuy nhiên, mặc dù Timestomping có thể tạo ra sự nhầm lẫn và gây khó khăn cho quá trình điều tra, nó không phải là biện pháp hoàn hảo và vẫn có thể bị phát hiện bởi các công cụ pháp chứng hiện đại. Điều này đòi hỏi kẻ tấn công phải sử dụng kỹ thuật này một cách tinh vi và kết hợp với các phương pháp chống pháp chứng khác để đạt được hiệu quả tối ưu.

4. Xóa hoặc thay đổi Registry (Registry Tampering)

- ***Mô tả kỹ thuật***

Xóa hoặc thay đổi Registry (Registry Tampering) là một kỹ thuật trong chống pháp chứng Windows, nơi kẻ tấn công xóa bỏ, chỉnh sửa, hoặc làm giả thông tin trong Windows Registry để che giấu các hoạt động hoặc dữ liệu nhạy cảm. Windows Registry là một cơ sở dữ liệu quan trọng trong hệ điều hành Windows, lưu trữ thông tin về cấu hình hệ thống, phần mềm đã cài đặt, người dùng, và các hoạt động đã diễn ra trên hệ thống. Điều này khiến Registry trở thành một mục tiêu quan trọng trong các cuộc điều tra pháp chứng kỹ thuật số.

Bằng cách thay đổi các mục trong Registry, kẻ tấn công có thể che giấu:

Phần mềm đã cài đặt hoặc đã chạy.

Các thiết bị đã kết nối.

Các hoạt động mạng hoặc đăng nhập.

Thông tin về người dùng.

Các nhà điều tra pháp chứng dựa vào dữ liệu trong Registry để xác định các hành động đã diễn ra trên hệ thống. Vì vậy, việc thay đổi hoặc xóa bỏ các mục Registry

có thể gây khó khăn cho quá trình điều tra và làm cho các bằng chứng trở nên không chính xác hoặc không còn tồn tại.

- ***Tầm quan trọng của Registry trong điều tra pháp chứng Windows***

  Một số thông tin quan trọng được lưu trữ trong Registry bao gồm:

  Run Keys: Các khóa Registry điều khiển các chương trình tự động khởi động khi Windows bắt đầu. Các điều tra viên thường kiểm tra các Run keys để tìm xem phần mềm độc hại có tự động khởi chạy trên hệ thống không.

  UserAssist: Đây là nơi lưu trữ thông tin về các chương trình mà người dùng đã mở gần đây. Pháp chứng viên có thể sử dụng mục này để biết được những tệp tin và chương trình nào đã được truy cập gần đây.

  MRU Lists (Most Recently Used): Lưu trữ danh sách các tệp tin và tài liệu được người dùng truy cập gần đây, bao gồm đường dẫn và tên tệp. Điều này giúp điều tra viên xác định những tệp tin nào đã được người dùng mở.

  USB Devices: Thông tin về các thiết bị ngoại vi, chẳng hạn như USB và ổ cứng gắn ngoài, đã được kết nối với hệ thống. Điều này có thể giúp pháp chứng viên biết được có thiết bị nào đã được sử dụng để sao chép dữ liệu hay không.

  Network Connections: Thông tin về các kết nối mạng, bao gồm địa chỉ IP, tên máy chủ, và thời gian kết nối, có thể giúp điều tra các hoạt động mạng hoặc tấn công từ xa.

- ***Các kỹ thuật thay đổi hoặc xóa Registry (Registry Tampering)***

1. Xóa mục Registry quan trọng

Mục tiêu: Xóa bỏ các khóa Registry lưu trữ thông tin quan trọng về các chương trình đã chạy, các thiết bị đã kết nối hoặc các hoạt động gần đây trên hệ thống.

Cách thực hiện: Kẻ tấn công có thể sử dụng regedit (công cụ chỉnh sửa Registry của Windows) hoặc reg.exe (công cụ dòng lệnh) để xóa các khóa Registry nhạy cảm. Điều này có thể giúp xóa bỏ các dấu vết về phần mềm độc hại hoặc các thiết bị USB đã kết nối.

2. Thay đổi thông tin trong Registry

Mục tiêu: Thay đổi các giá trị trong Registry để làm giả thông tin hoặc gây nhầm lẫn cho điều tra viên.

Cách thực hiện: Kẻ tấn công có thể chỉnh sửa giá trị của các khóa Registry để tạo ra thông tin giả, chẳng hạn như thay đổi thời gian khởi động của chương trình hoặc tạo ra các bản ghi không chính xác.

3. Tạo mục Registry giả

Mục tiêu: Tạo ra các khóa Registry giả mạo để đánh lạc hướng điều tra viên, làm họ tập trung vào các dấu vết không liên quan hoặc sai lệch.

Cách thực hiện: Kẻ tấn công có thể tạo ra các mục Registry giả để làm cho điều tra viên tin rằng các chương trình hoặc thiết bị cụ thể đã được sử dụng, trong khi thực tế chúng không hề tồn tại trên hệ thống.

4. Thay đổi quyền truy cập Registry

Mục tiêu: Hạn chế hoặc chặn quyền truy cập vào các khóa Registry quan trọng để ngăn điều tra viên xem xét hoặc thay đổi chúng.

Cách thực hiện: Kẻ tấn công có thể thay đổi quyền truy cập trên các khóa Registry để ngăn cản việc kiểm tra hoặc thay đổi chúng. Điều này có thể được thực hiện bằng cách thay đổi quyền trên các khóa hoặc tệp tin Registry, tạo ra các lỗi khi điều tra viên cố gắng truy cập.

5. Xóa lịch sử hoạt động trong Registry

Mục tiêu: Xóa bỏ các bản ghi về hoạt động người dùng, chẳng hạn như các tệp đã mở gần đây hoặc các chương trình đã chạy, để ngăn chặn điều tra viên xác định các hành động trước đó.

Cách thực hiện: Kẻ tấn công có thể xóa các bản ghi như MRU lists hoặc UserAssist để loại bỏ mọi dấu vết về các hoạt động gần đây của người dùng.

- ***Công cụ sử dụng để thay đổi hoặc xóa Registry***

1. Regedit

Regedit là công cụ chỉnh sửa Registry tích hợp sẵn trong Windows. Nó cho phép người dùng xem và thay đổi các khóa Registry trên hệ thống. Kẻ tấn công có thể sử dụng regedit để tìm và xóa các mục Registry nhạy cảm hoặc thay đổi giá trị của chúng.

2. Reg.exe

Reg.exe là một công cụ dòng lệnh của Windows cho phép chỉnh sửa Registry từ command prompt. Công cụ này rất hữu ích trong các kịch bản tự động hóa, nơi kẻ tấn công có thể chạy các lệnh để xóa hoặc thay đổi nhiều khóa Registry một cách nhanh chóng.

3. Autoruns (Sysinternals)

Autoruns là một công cụ mạnh mẽ giúp xem tất cả các chương trình tự động khởi chạy khi Windows khởi động, bao gồm các khóa Registry liên quan đến quá trình khởi động. Kẻ tấn công có thể sử dụng Autoruns để xem và xóa các khóa liên quan đến các chương trình độc hại nhằm che giấu sự hiện diện của chúng.

4. Metasploit Framework

Metasploit là một công cụ tấn công mạnh mẽ, trong đó bao gồm các module có thể thay đổi hoặc xóa bỏ các mục Registry trên hệ thống mục tiêu. Kẻ tấn công có thể sử dụng Metasploit để thực hiện các hành động chống pháp chứng bằng cách thay đổi Registry từ xa.

- ***Bất lợi khi sử dụng Registry Tampering***

  Dễ bị phát hiện: Các nhà điều tra pháp chứng có thể phát hiện ra hành vi Registry Tampering khi họ nhận thấy các mục Registry quan trọng bị xóa hoặc có dấu hiệu bị thay đổi. Ngoài ra, nhiều hệ thống phát hiện xâm nhập (IDS/IPS) có thể theo dõi và ghi lại những thay đổi bất thường trong Registry.

  Lưu dấu vết trong nhật ký sự kiện: Việc thay đổi hoặc xóa các mục Registry có thể bị ghi lại trong các bản ghi nhật ký sự kiện của hệ thống, làm lộ hành vi của kẻ tấn công. Điều này có thể làm gia tăng nghi ngờ và dẫn đến điều tra sâu hơn.

  Không thể xóa hoàn toàn thông tin: Mặc dù có thể xóa hoặc thay đổi các mục Registry, nhưng vẫn có các bản sao lưu của Registry hoặc các bản ghi hệ thống khác lưu trữ thông tin này. Các nhà điều tra có thể khôi phục lại các bản sao này để phân tích thông tin đã bị xóa.

  Gây lỗi hệ thống: Việc xóa nhầm các mục Registry quan trọng có thể làm hỏng hệ thống hoặc gây ra lỗi, dẫn đến các hành động bất thường bị phát hiện.

- ***Kết luận về Registry Tampering***

  Registry Tampering là một kỹ thuật mạnh mẽ trong chống pháp chứng Windows, giúp kẻ tấn công xóa bỏ hoặc làm giả thông tin quan trọng trong Windows Registry, từ đó che giấu hoạt động và gây khó khăn cho quá trình điều tra. Bằng cách thay đổi hoặc xóa các mục Registry, kẻ tấn công có thể xóa dấu vết về chương trình độc hại, các tệp đã mở, hoặc các thiết bị đã kết nối.

  Tuy nhiên, kỹ thuật này cũng đi kèm với những rủi ro. Các nhà điều tra pháp chứng có thể phát hiện ra dấu vết của Registry Tampering qua các bản sao lưu,

nhật ký sự kiện hoặc các hệ thống phát hiện xâm nhập. Do đó, mặc dù Registry Tampering có thể gây khó khăn cho điều tra viên, nhưng nó không phải là biện pháp hoàn hảo và cần được kết hợp với các kỹ thuật khác để đạt hiệu quả tối đa.

5. Sử dụng tệp hibernation và pagefile trong chống pháp chứng Windows

- ***Mô tả kỹ thuật***

Tệp hibernation (hiberfil.sys) và tệp hoán trang (pagefile.sys) là hai tệp hệ thống quan trọng trên hệ điều hành Windows, được sử dụng để lưu trữ dữ liệu tạm thời từ bộ nhớ RAM trong những trường hợp hệ thống chuyển sang trạng thái ngủ đông (hibernation) hoặc khi bộ nhớ vật lý (RAM) không đủ và cần phải sử dụng không gian ổ đĩa làm bộ nhớ bổ sung.

Cả hai tệp này đều chứa nhiều thông tin quan trọng có thể bao gồm:

Tài liệu mở: Các tài liệu hoặc chương trình đang hoạt động trên hệ thống có thể được lưu trữ tạm thời trong hibernation hoặc pagefile.

Mật khẩu và khóa mã hóa: Dữ liệu nhạy cảm như mật khẩu, khóa mã hóa có thể bị lưu trữ tạm thời trong bộ nhớ và từ đó bị ghi vào pagefile hoặc tệp hibernation.

Các tiến trình đang chạy: Tất cả các tiến trình đang hoạt động có thể bị lưu lại trong những tệp này khi hệ thống cần giải phóng bộ nhớ hoặc chuyển sang trạng thái ngủ đông.

Do những tệp này chứa thông tin quan trọng, các nhà điều tra pháp chứng thường thu thập và phân tích hiberfil.sys và pagefile.sys để tìm bằng chứng liên quan đến các hành động hoặc dữ liệu nhạy cảm trên hệ thống. Tuy nhiên, kẻ tấn công có thể lợi dụng hoặc xóa bỏ các tệp này để gây khó khăn cho việc thu thập chứng cứ và điều tra.

a. Tệp hibernation (hiberfil.sys)

- ***Chức năng của tệp hibernation***

  Hibernation là một tính năng trên Windows, cho phép hệ thống lưu toàn bộ trạng thái của bộ nhớ RAM vào một tệp gọi là hiberfil.sys trên ổ cứng trước khi máy tính chuyển sang trạng thái ngủ đông. Khi máy tính được khởi động lại, tất cả các tài liệu và tiến trình trước đó sẽ được khôi phục lại từ tệp hibernation.

  Tệp hiberfil.sys có kích thước tương đương với dung lượng RAM của máy tính và có thể chứa dữ liệu quan trọng như tài liệu đang mở, mật khẩu, khóa mã hóa, và các phiên làm việc của chương trình đang chạy.

- ***Lợi dụng tệp hibernation trong chống pháp chứng***

  Che giấu dữ liệu tạm thời: Kẻ tấn công có thể lợi dụng tệp hiberfil.sys để lưu trữ thông tin nhạy cảm mà họ không muốn lưu trên các tệp tin thông thường. Khi hệ thống chuyển sang chế độ ngủ đông, thông tin này sẽ được lưu vào hiberfil.sys, làm cho nó trở nên khó phát hiện hơn.

  Xóa tệp hibernation: Sau khi thực hiện các hành vi bất hợp pháp, kẻ tấn công có thể xóa hiberfil.sys để xóa sạch các bằng chứng tạm thời. Việc này đảm bảo rằng không có dữ liệu nào liên quan đến các tài liệu đang mở hoặc các tiến trình đang chạy còn tồn tại trên hệ thống khi máy tính bị tắt hoặc chuyển sang trạng thái ngủ đông.

- ***Công cụ sử dụng***

  powercfg: Lệnh dòng của Windows để quản lý các chế độ năng lượng và tính năng hibernation. Kẻ tấn công có thể sử dụng lệnh này để vô hiệu hóa chế độ hibernation và xóa tệp hiberfil.sys.

  SDelete: Công cụ từ Microsoft Sysinternals để xóa an toàn tệp tin và ghi đè nhiều lần lên dữ liệu bị xóa để đảm bảo không thể khôi phục.

- ***Bất lợi khi sử dụng***

  Dễ bị phát hiện: Việc vô hiệu hóa hibernation có thể bị phát hiện bởi các nhà điều tra pháp chứng, đặc biệt nếu tệp hiberfil.sys chứa thông tin nhạy cảm đã bị xóa một cách bất thường.

  Mất thông tin quan trọng: Nếu vô hiệu hóa hibernation mà không cẩn thận, các tiến trình đang chạy và thông tin quan trọng có thể bị mất vĩnh viễn, khiến kẻ tấn công mất đi các thông tin mà họ có thể cần sau này.

b. *Tệp hoán trang (pagefile.sys)*

- ***Chức năng của tệp pagefile***

  Pagefile.sys là tệp hoán trang của hệ điều hành Windows, được sử dụng để lưu trữ các dữ liệu từ RAM khi bộ nhớ vật lý (RAM) không đủ để chứa tất cả các tiến trình và dữ liệu hiện tại. Hệ điều hành sẽ chuyển dữ liệu tạm thời này sang pagefile.sys trên ổ đĩa để giải phóng bộ nhớ RAM.

  Pagefile có thể chứa nhiều loại dữ liệu nhạy cảm, bao gồm mật khẩu, khóa mã hóa, dữ liệu từ các tiến trình đang chạy, và thông tin về các tài liệu đang mở. Vì pagefile là một tệp hệ thống được Windows sử dụng liên tục, nên nó thường bị bỏ qua trong các cuộc điều tra thông thường, nhưng lại chứa nhiều thông tin quan trọng.

- ***Lợi dụng tệp pagefile trong chống pháp chứng***

  Giấu dữ liệu trong pagefile: Kẻ tấn công có thể sử dụng pagefile như một nơi lưu trữ tạm thời cho các dữ liệu nhạy cảm. Vì pagefile.sys được hệ điều hành sử dụng liên tục, nó có thể chứa các thông tin quan trọng mà kẻ tấn công không muốn lưu trên các tệp tin thông thường.

Xóa pagefile để xóa dấu vết: Kẻ tấn công có thể cấu hình Windows để tự động xóa pagefile.sys mỗi khi hệ thống tắt hoặc khởi động lại. Điều này sẽ giúp xóa sạch các dữ liệu tạm thời khỏi hệ thống, đảm bảo rằng các thông tin nhạy cảm không còn lưu trữ khi hệ thống được tắt.

- ***Công cụ sử dụng***

  Local Security Policy: Trong cài đặt bảo mật của Windows, kẻ tấn công có thể cấu hình hệ thống để tự động xóa pagefile.sys khi tắt máy.

  SDelete: Giống như tệp hibernation, SDelete có thể được sử dụng để xóa và ghi đè lên pagefile.sys, đảm bảo rằng không có dữ liệu nào có thể khôi phục được.

- ***Bất lợi khi sử dụng***

  Giảm hiệu suất hệ thống: Nếu pagefile bị xóa mỗi khi hệ thống tắt, điều này có thể làm giảm hiệu suất khi khởi động hệ thống do pagefile phải được tái tạo từ đầu.

  Có thể bị phát hiện: Hành động xóa pagefile mỗi khi hệ thống tắt có thể gây nghi ngờ cho các điều tra viên, đặc biệt khi tệp này chứa nhiều thông tin quan trọng mà lẽ ra không nên bị xóa.

- ***Kết luận về việc sử dụng tệp hibernation và pagefile trong chống pháp chứng***

  Tệp hibernation và pagefile là hai nguồn dữ liệu quan trọng có thể chứa nhiều thông tin nhạy cảm về hoạt động của người dùng và hệ thống. Kẻ tấn công có thể lợi dụng hoặc xóa bỏ các tệp này để gây khó khăn cho quá trình điều tra pháp chứng. Bằng cách vô hiệu hóa hibernation, cấu hình để xóa pagefile, hoặc sử dụng các công cụ xóa an toàn như SDelete, kẻ tấn công có thể xóa sạch các bằng chứng tạm thời khỏi hệ thống.

Tuy nhiên, các nhà điều tra pháp chứng có thể phát hiện và khôi phục các thông tin bị xóa bằng cách phân tích nhật ký sự kiện hoặc sử dụng các công cụ pháp chứng bộ nhớ mạnh mẽ. Vì vậy, mặc dù việc xóa hoặc thay đổi tệp hibernation và pagefile có thể gây khó khăn cho quá trình điều tra, nhưng nó không đảm bảo an toàn tuyệt đối và cần được thực hiện cẩn thận kết hợp với các kỹ thuật khác.

Kết luận về Chống Pháp chứng Windows

Chống pháp chứng Windows là một lĩnh vực phức tạp và đa dạng, bao gồm nhiều kỹ thuật nhằm mục tiêu ngăn chặn, làm mờ, hoặc vô hiệu hóa quá trình thu thập và phân tích bằng chứng kỹ thuật số trên các hệ thống Windows. Trong quá trình điều tra pháp chứng kỹ thuật số, Windows là hệ điều hành phổ biến nhất, và do đó cũng là mục tiêu chính của các đối tượng muốn che giấu hành vi bất hợp pháp hoặc bảo vệ dữ liệu nhạy cảm.

Các kỹ thuật chống pháp chứng tập trung vào việc xóa dấu vết, thay đổi dữ liệu, làm rối loạn dòng thời gian hoặc làm khó khăn cho quá trình phân tích và khôi phục dữ liệu của các nhà điều tra.

Mặc dù các kỹ thuật chống pháp chứng có thể gây khó khăn cho quá trình thu thập và phân tích bằng chứng, nhưng chúng không phải là hoàn hảo. Nhiều kỹ thuật chống pháp chứng có thể bị phát hiện bởi các hệ thống bảo mật tiên tiến, các công cụ pháp chứng hiện đại, hoặc các bản ghi hệ thống còn lại. Các nhà điều tra pháp chứng có nhiều cách để phát hiện ra những hành vi bất thường hoặc cố gắng xóa dấu vết, bao gồm phân tích nhật ký sự kiện, khôi phục các tệp đã xóa, và so sánh các bản sao lưu hệ thống.

Kỹ thuật chống pháp chứng không chỉ yêu cầu kiến thức sâu rộng về hệ điều hành Windows, mà còn phải được thực hiện một cách tinh vi và phối hợp với các biện pháp khác để đảm bảo tính hiệu quả. Trong nhiều trường hợp, các hành vi chống pháp chứng có thể làm tăng sự nghi ngờ và dẫn đến các cuộc điều tra kỹ lưỡng hơn, đặc biệt nếu các hành vi như xóa sạch dữ liệu hoặc thay đổi Registry bị phát hiện.

C. Pháp chứng bộ nhớ (Ram)

- **Giới thiệu về pháp chứng bộ nhớ**: Tầm quan trọng và các thách thức trong việc phân tích dữ liệu trên bộ nhớ trong điều tra số.

  - Là kỹ thuật điều tra máy tính bằng việc ghi lại bộ nhớ RAM của hệ thống thời điểm có dấu hiệu nghi ngờ, hoặc đang bị tấn công để tiến hành điều tra, giúp cho việc xác định nguyên nhân cũng như các hành vi đã xảy ra trên hệ thống, cung cấp các chứng cứ phục vụ cho việc xử lý tội phạm.

  - Tầm quan trọng : Pháp chứng bộ nhớ đóng vai trò quan trọng trong các cuộc điều tra số bằng cách cung cấp những hiểu biết có giá trị về hoạt động của hệ thống thông qua việc phân tích RAM. Khác với phương pháp điều tra đĩa truyền thống gặp khó khăn trong việc truy cập dữ liệu đã mã hóa, pháp chứng bộ nhớ có thể khôi phục khóa mã hóa và mật khẩu được lưu trữ trong RAM, giúp truy cập thông tin quan trọng dễ dàng hơn. Ngoài ra, pháp chứng bộ nhớ cho phép các nhà điều tra xem xét các tiến trình đang chạy, từ đó phát hiện các ứng dụng đang được sử dụng trong thời gian tấn công và dữ liệu ẩn trong bộ nhớ. Phương pháp này cung cấp cái nhìn chi tiết và chính xác nhất về những gì đang diễn ra trên hệ thống tại thời điểm bị tấn công, khắc phục các hạn chế của các phương pháp truyền thống.

  - Thách thức :

  + Tính tạm thời của dữ liệu: Dữ liệu trong RAM rất dễ mất khi hệ thống bị tắt hoặc khởi động lại, do đó việc thu thập phải được thực hiện nhanh chóng trước khi mất dấu vết.

  + Khối lượng dữ liệu lớn: Bộ nhớ RAM hiện đại có dung lượng rất lớn, dẫn đến việc thu thập và phân tích trở nên phức tạp, đòi hỏi công cụ và thời gian xử lý đáng kể.

  + Yêu cầu kỹ thuật cao: Pháp chứng bộ nhớ đòi hỏi kiến thức sâu về cấu trúc hệ thống và cách quản lý bộ nhớ của hệ điều hành, cũng như kỹ năng sử dụng các công cụ chuyên dụng như Volatility, Rekall.

  + Nguy cơ làm thay đổi dữ liệu: Khi thu thập dữ liệu từ hệ thống đang chạy, có nguy cơ dữ liệu sẽ bị thay đổi hoặc hư hỏng, ảnh hưởng đến tính toàn vẹn của bằng chứng.

  + Fileless Malware: Các phần mềm độc hại không lưu trên đĩa cứng mà chỉ tồn tại trong bộ nhớ, khiến việc phát hiện chúng càng khó khăn hơn nếu không sử dụng các phương pháp pháp chứng bộ nhớ.

Ví dụ về các kỹ thuật:

- **Mã hóa bộ nhớ (Memory Encryption):** Phân tích các kỹ thuật mã hóa và công cụ giúp bảo vệ dữ liệu trong RAM. **(mô tả, công cụ sử dụng, các bước thực hiện,** Bất lợi khi sử dụng các kỹ thuật này**...)**

  - Mô tả : mã hóa bộ nhớ là quá trình bảo vệ dữ liệu lưu trữ trong RAM bằng cách mã hóa nó, nhằm ngăn chặn truy cập trái phép, kể cả khi kẻ tấn công có được quyền truy cập vật lý vào thiết bị.

  - Công cụ : Trusted Platform Module (TPM).

  - Các bước thực hiện :

  + Xác định vùng dữ liệu nhạy cảm cần mã hóa trong bộ nhớ.

  + Mã hóa vùng bộ nhớ.

  + Giải mã dữ liệu khi cần truy cập và mã hóa lại ngay sau khi xử lý xong.

  - Bất lợi :

  + Giảm hiệu suất hệ thống do yêu cầu mã hóa/giải mã liên tục.

  + Quản lý khóa mã hóa phức tạp, đặc biệt trong môi trường nhiều người dùng.

- **Công cụ chống pháp chứng bộ nhớ**: Giới thiệu các công cụ và cách chúng có thể xóa hoặc mã hóa dữ liệu trong bộ nhớ.

  - Mô tả : công cụ chống pháp chứng bộ nhớ được thiết kế để xóa hoặc mã hóa dữ liệu trong bộ nhớ nhằm ngăn cản các công cụ pháp chứng khôi phục thông tin nhạy cảm.

  - Công cụ : RAMWipe, VeraCrypt, EnCase, TACTIC.

  - Các bước thực hiện:

  + Xác định các khu vực bộ nhớ chứa thông tin nhạy cảm mà có khả năng bị khai thác trong quá trình điều tra pháp chứng.

  + Sử dụng các công cụ chống pháp chứng để xóa hoặc mã hóa dữ liệu nhạy cảm trong bộ nhớ.

+ Đảm bảo xóa sạch bộ nhớ định kỳ hoặc khi không cần dùng đến dữ liệu nhạy cảm.

- Bất lợi:

+ Các công cụ tiên tiến có thể phát hiện được các kỹ thuật chống pháp chứng này.

+ Việc xóa dữ liệu có thể gây mất thông tin quan trọng không thể khôi phục.

- **Kỹ thuật tiêm mã và rỗng hóa tiến trình (Code Injection and Process Hollowing)**: Phân tích các phương pháp như DLL Injection và Process Hollowing.

- Mô tả : Tiêm mã và rỗng hóa tiến trình là các phương pháp mà kẻ tấn công có thể tiêm mã độc vào tiến trình đang chạy hoặc thay thế mã của một tiến trình hợp pháp bằng mã độc.

- Công cụ : Process Hacker 2.

- Các bước thực hiện :

+ Chọn tiến trình hợp pháp để tiêm mã độc vào.

+ Sử dụng DLL Injection để tiêm mã độc hoặc Process Hollowing để thay thế mã của tiến trình đang chạy bằng mã độc.

+ Khởi động lại tiến trình để mã độc được thực thi.

- Bất lợi:

+ Dễ bị phát hiện bởi các phần mềm bảo mật.

+ Các kỹ thuật bảo mật hệ điều hành hiện đại như ASLR và DEP có thể ngăn chặn tiêm mã.

- **Rootkit và thao tác với nhân hệ thống (Rootkit and Kernel Manipulation)**: Mô tả cách sử dụng rootkit và các kỹ thuật kernel manipulation để làm sai lệch thông tin trong bộ nhớ.

- Mô tả : Rootkit là phần mềm độc hại được thiết kế để giành quyền kiểm soát hệ thống ở mức kernel, cho phép thao tác với nhân hệ điều hành nhằm ẩn mã độc hoặc các hoạt động của kẻ tấn công.

- Công cụ: Hacking Team's RCS, ZeuS Rootkit, Metasploit.

- Các bước thực hiện:

+ Cài đặt rootkit vào nhân hệ điều hành để giành quyền kiểm soát sâu trong hệ thống.

+ Sử dụng rootkit để thao tác với kernel, ẩn các tiến trình, tệp tin, hoặc thay đổi thông tin trong bộ nhớ.

+ Rootkit cho phép kiểm soát các cuộc gọi hệ thống, làm sai lệch thông tin.

- Bất lợi:

+ Có thể gây ra lỗi hoặc phá hỏng hệ điều hành nếu thực hiện sai cách.

+ Dễ bị phát hiện bởi các công cụ kiểm tra toàn vẹn hệ thống như rkhunter.

- **Kỹ thuật làm mờ dữ liệu trong bộ nhớ (Memory Obfuscation)**: Trình bày các kỹ thuật như Polymorphic Malware và Encrypted Executables.

- Mô tả : Các kỹ thuật làm mờ dữ liệu trong bộ nhớ giúp che giấu mã độc bằng cách mã hóa hoặc thay đổi liên tục cấu trúc mã trong quá trình thực thi.

- Công cụ sử dụng: Polymorphic Engine, Themida.

- Các bước thực hiện:

+ Sử dụng kỹ thuật Polymorphic để thay đổi mã nguồn của phần mềm độc hại mỗi lần nó thực thi.

+ Sử dụng các tệp thực thi được mã hóa, mã độc chỉ giải mã khi cần chạy.

+ Kết hợp các kỹ thuật làm mờ dữ liệu với các phương pháp chống phân tích khác để tránh bị phát hiện.

- Bất lợi:

+ Quá trình giải mã và làm mờ mã có thể làm chậm hiệu suất.

+ Phần mềm bảo mật hiện đại có thể phát hiện các hành vi bất thường.

- **Kỹ thuật thay đổi bộ nhớ nhanh và cấp phát lại bộ nhớ (Anti-memory Analysis and Anti-debugging Techniques):** Mô tả các phương pháp như Fast-Flux .

  - Mô tả : Các kỹ thuật chống phân tích bộ nhớ và chống gỡ lỗi giúp thay đổi liên tục vị trí và trạng thái của dữ liệu trong bộ nhớ làm cho việc phân tích bộ nhớ trở nên khó khăn.

  - Công cụ : Metasploit.

  - Các bước thực hiện :

  + Tìm module hỗ trợ fast-flux phù hợp.

  + Cấu hình thông số tấn công.

  + Chọn payload.

  + Tấn công.

  + Duy trì kết nối và điều khiển .

  - Bất lợi :

  + Tiêu tốn tài nguyên của hệ thống do phải thay đổi nhanh chóng và liên tục trạng thái của bộ nhớ.

  + Phát sinh hành vi bất thường mà các công cụ bảo mật có thể phát hiện.

- **Kỹ thuật giấu thông tin trong bộ nhớ (Memory Steganography):** Trình bày các kỹ thuật steganography trong bộ nhớ.

  - Mô tả : Steganography trong bộ nhớ là kỹ thuật giấu thông tin trong các vùng bộ nhớ ít được kiểm tra, thường là các vùng dữ liệu không quan trọng.

  - Công cụ : Steganography tools (Hydan, Snow).

  - Các bước thực hiện :

  + Giấu dữ liệu vào các vùng bộ nhớ không được sử dụng hoặc ít được chú ý như các khoảng trống trong tiến trình.

  + Sử dụng công cụ steganography để mã hóa và giấu thông tin một cách không dễ phát hiện.

- Bất lợi :

+ Tốn nhiều tài nguyên bộ nhớ.

+ Các công cụ bảo mật có thể phát hiện các khu vực bộ nhớ bị che giấu nếu quét toàn bộ hệ thống.

Tóm lại : Anti-digital forensics trên bộ nhớ (RAM) tập trung vào các kỹ thuật nhằm che giấu, thay đổi, hoặc phá hoại thông tin trong bộ nhớ để ngăn cản quá trình điều tra kỹ thuật số. Các phương pháp này giúp tội phạm mạng ẩn giấu dấu vết, đồng thời khiến việc phát hiện và phân tích mã độc, dữ liệu nhạy cảm trở nên phức tạp hơn.

D. Pháp chứng Mobile

- **Giới thiệu về pháp chứng di động**: Tầm quan trọng và các thách thức trong việc phân tích dữ liệu trên thiết bị di động trong điều tra số.

  - Giới thiệu : Pháp chứng di động tập trung vào việc thu thập và phân tích dữ liệu từ các thiết bị di động như điện thoại thông minh và máy tính bảng. Với sự phổ biến của các thiết bị di động trong đời sống hàng ngày và công việc, chúng chứa rất nhiều thông tin quan trọng như tin nhắn, email, danh bạ, hình ảnh, video, và thông tin vị trí, đóng vai trò thiết yếu trong nhiều cuộc điều tra.

  - Tầm quan trọng : giúp điều tra tội phạm, phục hồi dữ liệu đã xóa và theo dõi hành vi người dùng, cung cấp bằng chứng quan trọng cho các cuộc điều tra.

  - Thách thức :

  + Sự đa dạng của hệ điều hành và thiết bị.

  + Dữ liệu được mã hóa và bảo mật sinh trắc học.

  + Dữ liệu phân tán trên bộ nhớ trong, thẻ nhớ và đám mây.

  + Pháp lý và quyền riêng tư cần tuân thủ khi thu thập và phân tích dữ liệu.

Ví dụ về các kỹ thuật:

- **Mã hóa dữ liệu**: Phân tích các kỹ thuật mã hóa thiết bị và ứng dụng để bảo vệ dữ liệu.

  - Mô tả : Mã hóa dữ liệu là quá trình chuyển đổi thông tin thành định dạng không thể đọc được mà chỉ có thể giải mã bằng khóa bí mật. Điều này giúp bảo vệ dữ liệu trong quá trình lưu trữ và truyền tải.

  - Công cụ : AES, RSA, TLS/SSL.

  - Các bước :

  + Chọn thuật toán mã hóa (AES, RSA).

  + Tạo khóa mã hóa.

  + Mã hóa dữ liệu bằng thuật toán đã chọn.

  + Lưu trữ hoặc truyền tải dữ liệu đã mã hóa.

  - Bất lợi:

  + Chi phí tính toán cao cho việc mã hóa và giải mã.

  + Quản lý khóa trở nên phức tạp; nếu mất khóa, dữ liệu không thể khôi phục.

- **Xóa dữ liệu an toàn**: Mô tả các phương pháp xóa dữ liệu như Factory Reset, Remote Wipe, và các công cụ Secure File Shredding.

  - Mô tả: Xóa dữ liệu an toàn là các phương pháp đảm bảo rằng dữ liệu không thể khôi phục được sau khi bị xóa.

  - Công cụ:

  + Factory Reset (Đặt lại về cài đặt gốc).

  + Remote Wipe (Xóa từ xa).

  + Secure File Shredding Tools (Như Eraser, CCleaner).

- Các bước thực hiện:

+ Chọn phương pháp xóa (Factory Reset, Remote Wipe).

+ Thực hiện lệnh xóa dữ liệu.

+ Xác minh rằng dữ liệu đã bị xóa hoàn toàn.

- Bất lợi:

+ Factory Reset chỉ xóa dữ liệu mà không mã hóa; dữ liệu có thể bị phục hồi.

+ Remote Wipe yêu cầu thiết bị kết nối internet.

+ Công cụ Shredding có thể tốn thời gian và không đảm bảo xóa hoàn toàn nếu không được cấu hình đúng.

- **Kỹ thuật ẩn dữ liệu**: Giải thích các kỹ thuật ẩn dữ liệu với các thư mục và ứng dụng ẩn.

- Mô tả: Giấu dữ liệu nhạy cảm trong các thư mục hoặc ứng dụng không đáng ngờ để tránh bị phát hiện.

- Công cụ:

+ Hidden folders: Thư mục ẩn trong hệ thống tệp.

+ Ứng dụng Vault (Như Keepsafe, Gallery Vault): Ứng dụng cho phép ẩn ảnh và video.

- Các bước thực hiện:

+ Tạo thư mục ẩn hoặc cài đặt ứng dụng Vault.

+ Di chuyển dữ liệu nhạy cảm vào thư mục hoặc ứng dụng này.

- Bất lợi:

+ Có thể bị phát hiện nếu người dùng không cẩn thận.

+ Không hoàn toàn bảo mật nếu thiết bị bị truy cập trái phép.

- **Công cụ chống pháp chứng**: Mô tả các công cụ và ứng dụng như Anti-Forensic Apps và Tampering Detection Tools.

  - Mô tả: Các công cụ này giúp bảo vệ thông tin và ngăn chặn việc thu thập dữ liệu không mong muốn trong các cuộc điều tra.

  - Công cụ:

  + Anti-Forensic Apps (Như Crypt4Free, Stealth Mode): Ứng dụng để mã hóa và giấu dữ liệu.

  + Tampering Detection Tools (Như Tripwire): Phát hiện sự thay đổi không mong muốn trong hệ thống tệp.

  - Các bước thực hiện:

  + Cài đặt các ứng dụng chống pháp chứng.

  + Cấu hình bảo mật cho các ứng dụng này.

  + Giám sát và kiểm tra hoạt động của thiết bị.

  - Bất lợi:

  + Có thể bị phát hiện trong cuộc điều tra pháp lý.

  + Một số công cụ có thể gây ra xung đột với ứng dụng khác.

- **Kỹ thuật liên lạc an toàn**: Phân tích các công cụ như Burner Phones, Disposable Phone Numbers và tin nhắn tự hủy.

  - Mô tả: Sử dụng các phương pháp và công cụ để đảm bảo thông tin liên lạc được bảo mật và không thể theo dõi.

  - Công cụ:

  + Burner Phones: Điện thoại tạm thời không được liên kết với danh tính của người dùng.

  + Disposable Phone Numbers (Như Google Voice): Số điện thoại tạm thời cho các giao tiếp nhạy cảm.

+ Tin nhắn tự hủy (Như Signal, Telegram): Tin nhắn tự hủy sau khi được đọc.

- Các bước thực hiện:

+ Mua hoặc thuê điện thoại tạm thời.

+ Sử dụng số điện thoại tạm thời cho các giao tiếp nhạy cảm.

+ Gửi tin nhắn tự hủy cho thông tin nhạy cảm.

- Bất lợi:

+ Sử dụng điện thoại tạm thời có thể gây nghi ngờ.

+ Tin nhắn tự hủy có thể không đảm bảo an toàn nếu không sử dụng ứng dụng đáng tin cậy.

- **Bẻ khóa và quyền root:** Giới thiệu về jailbreak, rooting và ROM tùy chỉnh để tăng cường quyền kiểm soát trên thiết bị.

  - Mô tả: Bẻ khóa và root cho phép người dùng truy cập đầy đủ vào hệ thống, giúp tăng cường quyền kiểm soát trên thiết bị.

  - Công cụ:

  + Jailbreak tools (Như Cydia, Unc0ver): Dùng để jailbreak iOS.

  + Rooting tools (Như Magisk, SuperSU): Dùng để root Android.

  - Các bước thực hiện:

  + Tải và cài đặt công cụ bẻ khóa/root.

  + Thực hiện bẻ khóa/root theo hướng dẫn.

  + Cài đặt các ứng dụng tùy chỉnh.

  - Bất lợi:

  + Mất bảo hành thiết bị.

  + Tăng rủi ro bảo mật và khả năng bị tấn công.

+ Một số ứng dụng hoặc tính năng có thể không hoạt động đúng cách trên thiết bị đã bẻ khóa/root.

- **Steganography trên thiết bị di động**: Mô tả các kỹ thuật giấu dữ liệu trong ảnh, video và bộ nhớ đệm ứng dụng.

  - Mô tả: Kỹ thuật giấu dữ liệu bên trong các tệp tin khác (như hình ảnh hoặc video) giúp bảo vệ thông tin nhạy cảm.

  - Công cụ:

  + Ứng dụng steganography (Như StegApp, OpenStego): Dùng để nhúng dữ liệu trong tệp.

  + Kỹ thuật mã hóa hình ảnh: Ẩn dữ liệu trong tệp ảnh.

  - Các bước thực hiện:

  + Chọn tệp tin để giấu dữ liệu.

  + Sử dụng ứng dụng để nhúng dữ liệu vào tệp tin.

  + Lưu tệp tin đã được giấu dữ liệu. Tệp tin này có thể được chia sẻ mà không ai có thể nhận ra rằng nó chứa thông tin nhạy cảm.

  - Bất lợi:

  + Dễ bị phát hiện nếu không sử dụng đúng cách.

  + Khó khăn trong việc lấy lại thông tin nếu không nhớ phương pháp giấu.

  + Kích thước của dữ liệu cần giấu thường bị giới hạn bởi kích thước của tệp gốc; giấu quá nhiều dữ liệu có thể làm cho tệp không ổn định hoặc dễ bị nghi ngờ.

E. Pháp chứng đĩa (Disk)

Tổng quan về disk forensics:

Disk forensics là một nhánh của Computer forensics, tập trung vào việc thu thập, phân tích và bảo quản bằng chứng trên các thiết bị lưu trữ như ổ đĩa máy tính, USB hay thẻ nhớ.

Mục tiêu chính của disk forensics là thu thập và bảo quản bằng chứng số, phục hồi dữ liệu bị xóa và tìm kiếm thông tin của các file ẩn.

Thách thức của disk forensics:

Dữ liệu trên ổ đĩa thường được mã hóa để bảo vệ khỏi truy cập trái phép, việc giải mã dữ liệu này có thể gặp rất nhiều khó khăn.

Sự phổ biến của các thiết bị lưu trữ di động và đám mây đòi hỏi disk forensics phải có khả năng xử lý nhiều định dạng và loại thiết bị khác nhau.

Thu thập và phân tích dữ liệu trên các ổ đĩa lớn hoặc phức tạp có thể đòi hỏi nhiều thời gian và công sức.

Kỹ thuật chống lại disk forensics:

1. Mã hóa dữ liệu:

Sử dụng các thuật toán mã hóa mạnh mẽ như AES để mã hóa dữ liệu trong file, folder hoặc mã hóa toàn bộ ổ cứng. Dữ liệu đã được mã hóa sẽ không thể đọc được nếu không có khóa giải mã, từ đó gây khó khăn cho việc thu thập bằng chứng.

Công cụ thực hiện:

VeraCrypt, FileVault (MacOS), BitLocker (Windows)

Hạn chế:

Ảnh hưởng đến hiệu suất vì phải tốn tài nguyên cho việc mã hóa mà giải mã dữ liệu

Đòi hỏi công sức và chi phí khi triển khai trên các hệ thống lớn phức tạp

Mã hóa làm việc phục hồi dữ liệu trở nên khó khăn hơn.

Cần bảo quản khóa giải mã cẩn thận.

2. Xóa dữ liệu an toàn (Data wiping):

Sử dụng các phần mềm chuyên dụng để xóa dữ liệu một cách an toàn bằng cách ghi đè file hoặc băm nhỏ file để ngăn chặn phục hồi dữ liệu.

Công cụ thực hiện:

SDelete, WipeFile, DBAN

Hạn chế:

Trong một số trường hợp, dữ liệu được xóa vẫn có thể được phục hồi bằng các phần mềm phục hồi dữ liệu chuyên dụng, dẫn đến nguy cơ thông tin bí mật bị rò rỉ.

Việc khôi phục dữ liệu trở nên khó khăn hoặc gần như không thể.

3. Che giấu dữ liệu

Sử dụng kỹ thuật Steganography để che giấu dữ liệu trong các file ảnh, âm thanh hoặc video.

Công cụ thực hiện:

Steghide, SilentEye, OutGuess

Hạn chế:

Kích thước dữ liệu cần ẩn giấu có giới hạn, nếu kích thước quá lớn sẽ dễ bị phát hiện.

Quá trình ẩn dữ liệu bằng Steganography có thể dẫn đến mất mát hoặc biến dạng dữ liệu gốc.

Nếu một phương pháp steganography không đủ tinh vi, thông tin ẩn có thể bị phát hiện dễ dàng bằng các công cụ phân tích.

F. Pháp chứng Image File

Tổng quan về Image file forensics

Image file forensics là một phần của computer forensics, kỹ thuật này tập trung vào việc phân tích hình ảnh để thu thập thông tin, chứng cứ hoặc dữ liệu quan trọng từ các file ảnh.

Mục tiêu chính của Image file forensics là xác định tính xác thực của hình ảnh, xác định xem hình ảnh đã bị chỉnh sửa hay không và tìm ra thông tin ẩn trong các tập tin hình ảnh.

Thách thức của Image file forensics:

Các công cụ xử lý hình ảnh ngày nay cho phép chỉnh sửa một cách khéo léo, dẫn tới việc phát hiện sự thay đổi trở nên khó khăn

Hình ảnh có thể tồn tại ở nhiều định dạng khác nhau như JPEG, PNG, TIFF và RAW. Việc xử lý và phân tích các định dạng này đòi hỏi kiến thức chuyên sâu về cách thức hoạt động của từng định dạng

Thông tin metadata trong hình ảnh có thể bị sửa đổi hoặc trùng lặp để gây nhầm lẫn. Việc xác định tính toàn vẹn của metadata và thời gian chỉnh sửa đòi hỏi kiến thức chuyên sâu về cách thức hoạt động của hệ thống.

Các kỹ thuật chống lại image file forensics

Chỉnh sửa metadata

Sửa đổi hoặc loại bỏ thông tin metadata liên quan trong các file hình ảnh để đánh lạc hướng cho các nhà điều tra về nguồn gốc hoặc lịch sử của hình ảnh.

Các công cụ thực hiện:

ExifTool

Hạn chế:

Mặc dù metadata đã được chỉnh sửa, dấu vết của việc chỉnh sửa vẫn có thể được phát hiện thông qua các phân tích forensics phức tạp

Mã hóa dữ liệu:

Mã hóa các file hình ảnh để ngăn chặn truy cập trái phép và làm cho việc trích xuất dữ liệu trở nên phức tạp hơn

Công cụ thực hiện

VeraCrypt, BitLocker

Hạn chế:

Ảnh hưởng đến hiệu suất vì phải tốn tài nguyên cho việc mã hóa mà giải mã dữ liệu

Đòi hỏi công sức và chi phí khi triển khai trên các hệ thống lớn phức tạp

Mã hóa làm việc phục hồi dữ liệu trở nên khó khăn hơn.

Cần bảo quản khóa giải mã cẩn thận.

Che dấu vết:

Sử dụng các công cụ để thay đổi timestamps, thay đổi thuộc tính file để gây khó khăn cho việc điều tra.

Công cụ thực hiện: BulkFileChanger

Hạn chế:

Việc xóa, mã hóa hoặc chỉnh sửa dữ liệu có thể để lại dấu vết bất thường trong cấu trúc file hoặc hệ thống file.

Các thay đổi về thời gian, quyền sở hữu, hoặc cấu trúc file có thể không khớp với hoạt động hợp lý trên thiết bị

Một số vùng dữ liệu bị xóa hoặc ghi đè hoàn toàn có thể bị coi là cố ý che giấu thông tin, dễ gây nghi ngờ.

Steganography:

Sử dụng các công cụ thay đổi thuộc tính file để ẩn giấu các dữ liệu khác

Công cụ thực hiện: JSHide&Seek

Hạn chế:

Steganography chỉ cho phép giấu một lượng nhỏ dữ liệu trong một tệp tin mà không gây nghi ngờ. Nếu cần che giấu lượng lớn dữ liệu, tệp tin dễ bị phát hiện hoặc bị nghi ngờ.

Nhúng quá nhiều dữ liệu vào một file có thể làm giảm chất lượng, tạo ra khác biệt có thể nhận biết

III. Kết luận

Sự gia tăng của các kỹ thuật chống điều tra số phản ánh một xu hướng không thể tránh khỏi trong thời đại kỹ thuật số hiện nay: nhu cầu bảo vệ quyền riêng tư và dữ liệu cá nhân ngày càng trở nên quan trọng. Các công cụ này đã và đang giúp người dùng nắm quyền kiểm soát thông tin của họ, bảo vệ dữ liệu khỏi các cuộc tấn công mạng và giảm thiểu nguy cơ bị theo dõi trái phép. Tuy nhiên, với việc công nghệ này cũng có thể bị lạm dụng trong các hoạt động phi pháp, câu hỏi về tính hợp pháp và đạo đức của việc sử dụng các kỹ thuật chống điều tra số ngày càng được đặt ra.

Tính pháp lý và sự minh bạch trong việc sử dụng các kỹ thuật chống điều tra số cần được quản lý và điều chỉnh chặt chẽ bởi các quy định pháp luật rõ ràng. Điều này giúp đảm bảo rằng các công nghệ chống điều tra chỉ được sử dụng cho các mục đích chính đáng như bảo vệ quyền riêng tư cá nhân, bảo vệ thông tin thương mại và chống lại các mối đe dọa từ tội phạm mạng, thay vì che giấu hoạt động bất hợp pháp. Việc tạo ra các quy chuẩn, nguyên tắc hướng dẫn cụ thể trong việc sử dụng các công cụ chống điều tra sẽ góp phần tạo ra sự cân bằng giữa quyền riêng tư và an ninh công cộng.

Cuối cùng, các kĩ thuật chống điều tra số không chỉ là một lĩnh vực kỹ thuật thuần túy mà còn là một phần quan trọng trong cuộc tranh luận về quyền riêng tư, an ninh và đạo đức trong thế giới số hiện đại. Việc nghiên cứu và phát triển các công cụ này cần phải đi kèm với trách nhiệm và ý thức rõ ràng về những hậu quả mà nó có thể gây ra cho xã hội. Nếu được quản lý một cách đúng đắn, các kĩ thuật chống điều tra số có thể trở thành công cụ quan trọng giúp con người bảo vệ quyền lợi và thông tin của mình trong thế giới số đầy phức tạp. Ngược lại, nếu lạm dụng hoặc sử dụng sai mục đích, chúng có thể trở thành mối đe dọa lớn đối với an ninh xã hội và các giá trị pháp lý.

IV. Nguồn tham khảo

Anti-forensics: Techniques, detection and countermeasures

Anti-forensics: A practitioner perspective

Digital forensics vs. Anti-digital forensics: Techniques, limitations and recommendations

5 anti-forensics techniques to trick investigators

Anti-Forensics Techniques

Computer Forensics: Anti-Forensic Tools & Techniques

V. Câu hỏi trắc nghiệm

Câu 1: Kỹ thuật nào được sử dụng để thu thập dữ liệu mạng phục vụ điều tra pháp chứng?

A. Packet Sniffing

B. Disk Imaging

C. Memory Dumping

D. File Carving

Câu 2: Kỹ thuật nào được dùng để ngụy trang lưu lượng mạng hợp pháp nhằm làm nhiễu điều tra?

A. Traffic Padding

B. Load Balancing

C. NAT

D. Packet Fragmentation

Câu 3: Chống pháp chứng mạng có thể sử dụng kỹ thuật nào để làm xáo trộn thứ tự gói tin?

A. Packet Shuffling

B. Packet Dropping

C. Packet Encryption

D. Packet Duplication

1. Chống pháp chứng Hệ điều hành (Window)

Câu 4: Để làm nhiễu dữ liệu trong nhật ký hệ thống Windows, có thể:

A. Sửa nội dung file nhật ký

B. Xóa toàn bộ file nhật ký

C. Thêm thông tin giả vào file nhật ký

D. Tất cả các phương án trên

Câu 5: Kỹ thuật nào được sử dụng để ngăn pháp chứng phân tích các file hệ thống?

A. Mã hóa các tệp hệ thống

B. Thay đổi quyền truy cập tệp

C. Chuyển đổi hệ thống tệp thành định dạng không tương thích

D. Tất cả các phương án trên

Câu 6: Để xóa dấu vết đăng nhập trên Windows, tập tin nào cần được sửa đổi hoặc xóa?

A. NTUSER.DAT

B. Pagefile.sys

C. WindowsUpdate.log

D. HOSTS file

Câu 7: Khi sử dụng tệp nhật ký giả mạo, yếu tố nào cần được chú ý?

A. Tính nhất quán thời gian

B. Dung lượng tệp

C. Định dạng tệp

D. Tất cả các phương án trên

Câu 8: Khi chống pháp chứng RAM, lý do tại sao cần làm đầy bộ nhớ bằng dữ liệu ngẫu nhiên?

A. Để làm chậm quá trình điều tra

B. Để xóa dữ liệu nhạy cảm trước đó

C. Để che giấu dấu vết mã độc

D. Để tăng tốc độ hệ thống

Câu 9: Công cụ pháp chứng nào thường được sử dụng để thu thập dữ liệu từ RAM?

A. Volatility

B. DBAN

C. FTK Imager

D. Recuva

Câu 10: Tại sao việc xóa bộ nhớ RAM bằng cách tắt nguồn máy tính không luôn hiệu quả?

A. Dữ liệu trong RAM có thể được phục hồi bằng kỹ thuật Cold Boot

B. Dữ liệu trong RAM được sao lưu tự động

C. RAM có khả năng lưu trữ dữ liệu lâu dài

D. RAM không bị xóa ngay cả khi mất điện

Câu 11: Phương pháp nào làm cho việc khôi phục dữ liệu trên ổ đĩa trở nên khó khăn?

A. Overwriting (Ghi đè)

B. Disk Partitioning (Chia phân vùng)

C. File Compression (Nén tệp)

D. Backup dữ liệu

Câu 12: Khi mã hóa ổ đĩa, yếu tố nào đảm bảo rằng dữ liệu không thể bị khôi phục?

A. Sử dụng mật khẩu mạnh

B. Sử dụng thuật toán mã đủ hoá mạnh

C. Không dể lộ khoá mã hoá

D. Tất cả các yếu tố trên

Câu 13: Phần mềm pháp chứng nào thường được dùng để phân tích ổ đĩa?

A. FTK Imager

B. Volatility

C. Wireshark

D. FTK Toolkit

Câu 14: Tệp nào trên thiết bị di động thường chứa dữ liệu nhạy cảm nhất?

A. Backup file

B. Log file

C. Temporary file

D. Cache file

Câu 15: Kỹ thuật nào có thể che giấu thông tin về vị trí thiết bị di động?

A. Tắt GPS

B. Sử dụng ứng dụng giả mạo vị trí

C. Xóa lịch sử vị trí

D. Tất cả các phương án trên

Câu 16: Khi dữ liệu trên thiết bị di động bị xóa, tại sao pháp chứng vẫn có thể khôi phục được?

A. Dữ liệu bị xóa vẫn lưu trong bộ nhớ flash

B. Hệ thống lưu bản sao dữ liệu vào các tệp ẩn

C. Dữ liệu không thực sự bị ghi đè

D. Tất cả các lý do trên

Câu 17: Kỹ thuật nào thường được sử dụng để ẩn dữ liệu trong file hình ảnh?

A. Steganography

B. Mã hóa tệp

C. Thay đổi phần mở rộng tệp

D. Split File

Câu 18: Công cụ pháp chứng nào được sử dụng để phát hiện steganography trong ảnh?

A. Stegdetect

B. FTK Imager

C. Cellebrite

D. DiskDigger

Câu 19: Công cụ pháp chứng nào được sử dụng thực hiện steganography trong ảnh?

A. Stegdetect

B. FTK Imager

C. Steghide

D. DiskDigger

Câu 20: Khi thay đổi metadata trong ảnh, thông tin nào thường được sửa đổi?

A. Thời gian chụp ảnh

B. Độ phân giải ảnh

C. Kích thước ảnh

D. Màu sắc ảnh

Đáp án:

1 A 2 A 3 A 4 D 5 D 6 A 7 D 8 B 9 A 10 A 11 A 12 D
13 A 14 A 15 D 16 D 17 A 18 A 19 C 20 A