**MỤC LỤC**

[**1.Trình bày khái niệm “*Bằng chứng số*”.** 2](#_Toc171234352)

[**2.** **Lấy ví dụ minh họa về bằng chứng số.** 2](#_Toc171234353)

[**3. Các định dạng lưu trữ phổ biến, ưu và nhược điểm từng định dạng.** 2](#_Toc171234354)

[**4. Các định dạng sao lưu phổ biến, ưu và nhược điểm từng định dạng.** 4](#_Toc171234355)

[**5. Trình bày phương pháp và các công cụ thu thập bộ nhớ Volatile và Non-Volatile trên Hệ điều hành Windows?** 4](#_Toc171234356)

[**6. Tìm hiểu về quy trình, công cụ, các công việc cần thực hiện khi thực hiện công việc điều tra số trên Windows.** 6](#_Toc171234357)

[**7.Trình bày phương pháp và các công cụ thu thập bộ nhớ Volatile và Non-Volatile trên Hệ điều hành Linux ?** 11](#_Toc171234358)

[**8. Tìm hiểu về quy trình, công cụ, các công việc cần thực hiện khi thực hiện công việc điều tra số trên Linux, liệt kê các thư mục quan trọng khi thực hiện công việc điều tra số trên Linux.** 12](#_Toc171234359)

[**9. Trình bày các kỹ thuật Anti-forensic trên hệ điều hành Windows và đưa ra một ví dụ cụ thể?** 16](#_Toc171234360)

[**10. Trình bày các kỹ thuật Anti-forensic trên hệ điều hành Linux và đưa ra một ví dụ cụ thể? (như câu 9)** 18](#_Toc171234361)

[**11. Quy trình điều tra số mạng ( Network forensics)** 18](#_Toc171234362)

[**12. Các kiến thức về ổ đĩa NTFS, FAT32, Ext4.** 20](#_Toc171234363)

[**13. Các kiến thức thu thập, tạo bảo sao, phân tích bằng chứng số.** 24](#_Toc171234364)

[**14. Một số các thuật ngữ như chain-of-custody, digital eviden.** 26](#_Toc171234365)

[**15. Các nơi chứa nhật ký của các hệ điều hành Linux, Windows ( eventlog, security log…) Và hiểu về các định dạng nhật ký**. 28](#_Toc171234366)

[**16. Phân tích sự khác nhau về điều tra số bộ nhớ Volatile và Non-Volatile trên Hệ điều hành Linux?** 29](#_Toc171234367)

[**17. Sinh viên phân tích sự khác nhau về điều tra số bộ nhớ Volatile và Non-Volatile trên Hệ điều hành Windows?** 30](#_Toc171234368)

[**18. Phương pháp tạo bản sao cho dữ liệu tĩnh trên hệ điều hành và ví dụ cụ thể?** 31](#_Toc171234369)

[**19. Sinh viên trình bày khi tiếp cận để điều tra một máy tính đang bật sử dụng hệ điều hành Linux thì sẽ cần thu thập dữ liệu động nào? Nêu ví dụ cụ thể và các công cụ cần sử dụng.** 32](#_Toc171234370)

**ĐỀ CƯƠNG ÔN THI MÔN ĐIỀU TRA SỐ KHÓA: AT17**

**1.Trình bày khái niệm “*Bằng chứng số*”.**

***Khái niệm* “*Bằng chứng số*”*:***

* Bằng chứng số chỉ bao gồm chuỗi các bit
* Bằng chứng số là hữu hạn trong cả không gian và thời gian
* Bằng chứng số là chứng cứ dấu vết.
* Bằng chứng số thì tiềm ẩn trong tự nhiên.
* Độ phức tạp của tính toán làm giới hạn việc phân tích Pháp chứng số
* Luận thuyết cơ bản của Pháp chứng số là “Cái gì chưa rõ ràng, nhất quán thì không phải là thật”.

***Nơi có thể tìm bằng chứng số:***

* Trong các tập tin ghi lịch sử truy cập internet
* Trong các tập tin Cach sinh ra khi truy cập internet
* Tại các vùng đĩa chưa cấp phát hoặc file slack
* Lưu trữ các tập tin, thư mục, tên tập tin
* Thông tin ngày lưu trữ tập tin
* Ẩn/nhúng trong phần mềm
* Trong các tập tin chia sẻ
* Trong các e-mail

**2.** **Lấy ví dụ minh họa về bằng chứng số.**

1. Email:

* Tình huống: Một nhân viên bị cáo buộc tiết lộ thông tin mật của công ty cho đối thủ cạnh tranh.
* Bằng chứng số: Các email giữa nhân viên này và đối thủ cạnh tranh chứa thông tin mật được tìm thấy và sử dụng làm bằng chứng trong cuộc điều tra.

2. Tập tin máy tính:

* Tình huống: Một nhân viên bị nghi ngờ đã cài đặt phần mềm độc hại vào hệ thống của công ty.
* Bằng chứng số: Các tập tin cài đặt phần mềm độc hại được tìm thấy trên máy tính của nhân viên này và nhật ký hệ thống cho thấy thời điểm cài đặt phần mềm trùng khớp với thời gian nhân viên truy cập vào hệ thống.

3. Nhật ký truy cập (Log files):

* Tình huống: Một trang web bị tấn công bởi hacker và gây ra thiệt hại nghiêm trọng.
* Bằng chứng số: Nhật ký truy cập của trang web cho thấy các địa chỉ IP và thời gian truy cập bất thường, giúp truy ra nguồn gốc của cuộc tấn công.

**3. Các định dạng lưu trữ phổ biến, ưu và nhược điểm từng định dạng.**

Có 3 kiểu định dạng dữ liệu thu thập:

* Định dạng thô
* Định dạng độc quyền
* Định dạng nâng cao (AFF)

**+ Định dạng thô:**

* Để bảo quản bằng chứng số, cần phải sao chép dữ liệu dạng bit vào tệp tin lưu trữ.
* Kỹ thuật sao chép tạo ra các tệp tin đơn giản của một tập dữ liệu hoặc ổ đĩa nghi ngờ.
* Các đầu ra của các tệp này được lưu dạng định dạng thô.

|  |  |
| --- | --- |
| Ưu điểm | Nhược điểm |
| - Truyền dữ liệu nhanh chóng  - Có thể bỏ qua các lỗi đọc dữ liệu nhỏ trên ổ nguồn  - Hầu hết các công cụ điều tra máy tính có thể đọc định dạng thô | - Yêu cầu nhiều dung lượng lưu trữ như đĩa gốc hoặc tập dữ liệu  - Các công cụ (miễn phí) có thể không thu thập được các sector lỗi trên ổ nguồn |

**+ Định dạng độc quyền:**

Các công cụ điều tra thương mại có các định dạng riêng để thu thập bằng chứng kỹ thuật số. Các định dạng độc quyền thường cung cấp các tính năng tương ứng với các công cụ phân tích của nhà cung cấp, chẳng hạn như:

|  |  |
| --- | --- |
| Ưu điểm | Nhược điểm |
| -Tuỳ chọn nén hoặc không nén tệp hình ảnh của ổ nguồn để tiết kiệm dung lượng trên ổ đích.  - Khả năng chia hình ảnh thành các tệp được phân đoạn nhỏ hơn để lưu trữ, chẳng hạn như CD hoặc DVD với kiểm tra tính toàn vẹn của dữ liệu được tích hợp vào từng phân đoạn  - Khả năng tích hợp siêu dữ liệu vào tệp hình ảnh như ngày và thời gian thu thập, giá trị băm của ổ nghi ngờ, tên điều tra viên, nhận xét, chi tiết vụ án,... | - Không có khả năng chia sẻ hình ảnh giữa các công cụ phân tích điều tra máy tính khác nhau  - Giới hạn kích thước tệp cho mỗi ổ đĩa được phân đoạn |

**+ Định dạng nâng cao (AFF):**

Định dạng điều tra nâng cao là một định dạng chuyển đổi mà mã nguồn mở với những mục thiết kế sau

|  |  |
| --- | --- |
| Ưu điểm | Nhược điểm |
| - Không giới hạn kích thước cho các tập tin disk-to-image  - Tạo tệp hình ảnh nén hoặc không nén  - Cung cấp không gian cho siêu dữ liệu trong tệp hình ảnh hoặc tệp được phân đoạn | - Thiết kế đơn giản với khả năng mở rộng  - Mã nguồn mở cho nhiều nền tảng máy tính và OSs  - Kiểm tra tính nhất quán nội bộ để xác thực |

Phần mở rộng tệp bao gồm .afm cho siêu dữ liệu AFF và .afd cho tệp hình ảnh được phân đoạn.

**Advanced Forensic Framework 4 (AFF4):**

* Thiết kế lại và sửa đổi AFF để quản lý và sử dụng số lượng lớn ảnh đĩa, giảm cả thời gian thu thập và yêu cầu lưu trữ
* Được những người tạo ra nó đặt tên là object-oriented framework (Michael Cohen, Simson Garfinkel, and Bradly Schatz)
* Các kiểu cơ bản của đối tượng AFF4: Khối lượng, luồng và đồ thị. Chúng phổ biến được tham chiếu qua một URL duy nhất
* Mô hình thông tin trừu tượng cho phép lưu trữ dữ liệu hình ảnh đĩa ở một hoặc nhiều nơi trong khi thông tin về dữ liệu được lưu trữ ở nơi khác
* Lưu trữ nhiều loại thông tin có tổ chức hơn trong hồ sơ bằng chứng
* Cung cấp mô hình dữ liệu thống nhất và lược đồ đặt tên

**4. Các định dạng sao lưu phổ biến, ưu và nhược điểm từng định dạng.**

**Sao chép dạng bit** (còn được gọi là hình ảnh phản chiếu/sao lưu cấp bằng chứng) liên quan đến sao chép từng bit của ổ cứng vật lý hoặc bất kỳ phương tiện lưu trữ nào khác.

* Nó sao chép chính xác tất cả các khu vực trên một thiết bị lưu trữ nhất định.
* Điều này bao gồm dữ liệu ẩn và dữ liệu còn lại (trùng, không gian, hoán đổi, không gian chưa sử dụng, phần còn lại và các tệp đã xóa).
* Các chương trình dạng bit dựa trên các tính toán kiểm tra dự phòng theo chu kỳ (CRC) trong quá trình xác nhận.

**Sao chép dạng sao lưu**

* Hầu hết các hệ điều hành chỉ chú ý đến cấu trúc hệ thống tệp trực tiếp.
* Slack, dung lượng trống, các tệp đã xoá… không được lập chỉ mục.
* Các bản sao lưu thường không nắm bắt được dữ liệu này và sửa đổi dấu thời gian của dữ liệu, làm mất chính xác thời gian.

**5. Trình bày phương pháp và các công cụ thu thập bộ nhớ Volatile và Non-Volatile trên Hệ điều hành Windows?**

1. Thu thập dữ liệu động (Volatile)

Dữ liệu động là dữ liệu có thể bị mất khi hệ thống tắt hoặc khởi động lại, ví dụ như dữ liệu trong RAM. Dưới đây là các phương pháp và công cụ để thu thập dữ liệu này:

# a. Thu thập dữ liệu động:

- Thời gian hệ thống: Sử dụng lệnh `System Time` để thu thập thông tin về thời gian hoạt động của hệ thống.

- Người dùng đã đăng nhập: Sử dụng các công cụ như `PsLoggedOn`, `Net Sessions`, và `LogonSessions` để xác định người dùng đã đăng nhập vào hệ thống.

- Thông tin mạng: Sử dụng lệnh `nbtstat -c` để xem bộ đệm bảng tên NetBIOS.

- Kết nối mạng: Dùng lệnh `netstat -ano` để hiển thị chi tiết về kết nối mạng TCP và UDP.

- Thông tin tiến trình: Sử dụng các công cụ như `Tasklist`, `Task Manager`, và `Pslist` để hiển thị thông tin chi tiết về các tiến trình đang chạy.

- Bộ nhớ tiến trình: Sử dụng `Process Explorer` để kiểm tra và thu thập thông tin bộ nhớ của các tiến trình.

- Nội dung khay nhớ tạm: Khai thác nội dung khay nhớ tạm để lấy dữ liệu quan trọng có thể lưu trữ tạm thời.

- Dịch vụ và driver: Kiểm tra thông tin về các dịch vụ và driver đang chạy trên hệ thống.

2. Thu thập dữ liệu tĩnh (Non-Volatile)

Dữ liệu tĩnh là dữ liệu không bị mất khi hệ thống tắt hoặc không có nguồn điện, ví dụ như dữ liệu trên ổ cứng.

# a. Thu thập dữ liệu tĩnh:

- Email, tài liệu, bảng tính: Thu thập các tệp tin lưu trữ trên ổ cứng, bao gồm cả các tệp tin đã xóa.

- File hệ thống: Sử dụng lệnh `dir /o:d` để kiểm tra ngày và giờ cài đặt hệ điều hành, các bản vá lỗi và thư mục con.

- Registry Settings: Truy cập và quản lý Registry bằng tiện ích `Registry Editor`.

- Event Logs: Sử dụng các công cụ như `psloglist.exe` để truy xuất các bản ghi sự kiện.

- Print Spool Files: Kiểm tra các tệp `.SPL` và `.SHD` để lấy thông tin chi tiết về các lệnh in.

- Slack Space: Sử dụng công cụ `DriveSpy` để thu thập không gian trống trên ổ đĩa.

- Virtual Memory: Sử dụng công cụ `X-Ways Forensics` để quét bộ nhớ ảo.

- Hibernate Files: Khai thác tệp `hiberfil.sys` để theo dõi các ứng dụng và chi tiết xác thực.

- Page File: Sử dụng các công cụ như `rekallmaster` để thu thập thông tin từ tệp `pagefile.sys`.

- Windows Search Index: Sử dụng `Passware Search Index Examiner` để truy cập dữ liệu được lập chỉ mục bởi Windows Search.

**1. Phương pháp thu thập bộ nhớ Volatile (RAM)**

**a. Chuẩn bị:**

* **Bước 1:** Xác định thời điểm thích hợp để thu thập dữ liệu, thường là ngay sau khi phát hiện sự cố hoặc trước khi tắt máy.
* **Bước 2:** Chuẩn bị các công cụ thu thập dữ liệu như USB chứa phần mềm cần thiết.

**b. Tiến hành thu thập:**

* **Bước 1:** Cắm USB chứa công cụ vào máy tính mục tiêu.
* **Bước 2:** Sử dụng các công cụ như Volatility, FTK Imager hoặc DumpIt để thu thập ảnh bộ nhớ RAM.
* **Bước 3:** Lưu lại ảnh bộ nhớ vào một thiết bị lưu trữ an toàn để phân tích sau này.

**c. Phân tích dữ liệu:**

* **Bước 1:** Sử dụng Volatility Framework để phân tích ảnh bộ nhớ, trích xuất các tiến trình, kết nối mạng, và các thông tin liên quan khác.
* **Bước 2:** Kiểm tra nội dung khay nhớ tạm, trạng thái tiến trình và thông tin mạng để tìm kiếm các dấu hiệu bất thường.

**2. Phương pháp thu thập bộ nhớ Non-Volatile (ổ cứng)**

**a. Chuẩn bị:**

* **Bước 1:** Xác định các phân vùng và ổ đĩa cần thu thập dữ liệu.
* **Bước 2:** Chuẩn bị các công cụ pháp y số như FTK Imager, Autopsy, hoặc EnCase.

**b. Tiến hành thu thập:**

* **Bước 1:** Khởi động hệ thống bằng USB hoặc CD chứa công cụ pháp y để tránh làm thay đổi dữ liệu.
* **Bước 2:** Tạo ảnh của ổ cứng bằng FTK Imager hoặc các công cụ tương tự, đảm bảo ghi lại toàn bộ dữ liệu, bao gồm cả slack space và unallocated space.
* **Bước 3:** Lưu ảnh ổ cứng vào một thiết bị lưu trữ an toàn để phân tích sau này.

**c. Phân tích dữ liệu:**

* **Bước 1:** Sử dụng Autopsy hoặc EnCase để phân tích hệ thống tệp, khôi phục các tệp đã xóa và kiểm tra các dấu vết trong registry.
* **Bước 2:** Kiểm tra các file hệ thống, nhật ký sự kiện, và các thiết lập registry để xác định các hoạt động đáng ngờ.
* **Bước 3:** Phân tích các file tạm, cache, cookies và lịch sử trình duyệt để tìm kiếm các dấu hiệu của hoạt động bất thường.

**Các công cụ phổ biến:**

- Volatile Memory:

- Volatility Framework: Phân tích hình ảnh bộ nhớ, trích xuất và phân tích dữ liệu từ bộ nhớ RAM.

- FTK Imager: Tạo ảnh của bộ nhớ và ổ cứng.

- DumpIt: Tạo ảnh của bộ nhớ RAM.

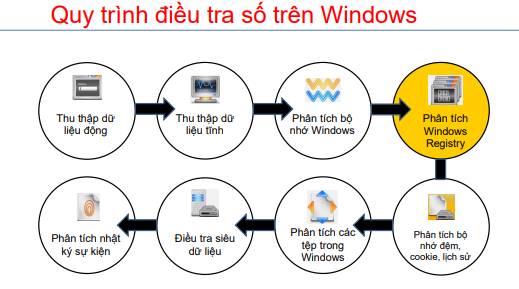
- Non-Volatile Memory:

- FTK Imager: Tạo và phân tích ảnh của ổ cứng.

- Autopsy: Phân tích hệ thống tệp và khôi phục dữ liệu.

- EnCase: Công cụ pháp y số để phân tích dữ liệu trên ổ cứng.

**6. Tìm hiểu về quy trình, công cụ, các công việc cần thực hiện khi thực hiện công việc điều tra số trên Windows.**

****

1. **Thu thập dữ liệu động**

Dữ liệu động là loại dữ liệu có thể dễ dàng bị sửa đổi hoặc bị mất khi hệ thống tắt hoặc khởi động lại. Thu thập dữ liệu động giúp xác định mốc thời gian của sự cố máy tính và những người dùng có trách nhiệm. Dữ liệu động nằm trong thanh ghi, bộ nhớ cache và RAM, dựa vào các dữ liệu động thu thập được, nhà điều tra có thể xác định những người dùng đã đăng nhập, dòng thời gian xảy ra sự cố, các chương trình và thư viện liên quan, các tệp được truy cập và chia sử trong một cuộc tấn công đáng ngờ như thông tin mạng, mã mở tệp, ánh xạ quy trình tới cổng, ổ đĩa được ánh xạ, lịch sử lệnh, thông tin quy trình, chia sẻ, ...

Dữ liệu động bao gồm:

* Thời gian hệ thống
* Người dùng đã đăng nhập
* Thông tin mạng
* Tập tin đang mở
* Kết nối mạng
* Trạng thái mạng
* Trạng thái cổng dịch vụ
* Thông tin tiến trình
* Bộ nhớ tiến trình
* Các ổ đĩa được ánh xạ
* Dữ liệu chia sẻ
* Nội dung trong khay nhớ tạm
* Thông tin services/driver
* Lịch sử lệnh

**2. Thu thập dữ liệu tĩnh**

Dữ liệu tĩnh không thay đổi khi hệ thống bị tắt hoặc mất điện. Ví dụ về dữ liệu bất biến bao gồm email, tài liệu xử lý văn bản, bảng tính và các tệp "đã xóa" khác nhau. Điều tra viên có thể quyết định thông tin nào cần được trích xuất từ ​​sổ đăng ký hoặc thông tin nào về (hoặc từ) tệp cần được thu thập để phân tích thêm. Ngoài ra, kẻ tấn công có thể đăng nhập vào hệ thống và truy cập dữ liệu. Trong những trường hợp như vậy, điều tra viên có thể quyết định theo dõi kẻ tấn công. Điều quan trọng là điều tra viên phải giữ nguyên một số thông tin quan trọng mà không có bất kỳ sửa đổi hoặc xóa nào.

Sau khi người dùng khởi động hệ thống, một số dữ liệu có thể bị thay đổi, chẳng hạn như các ổ đĩa được ánh xạ đến hoặc từ hệ thống, các dịch vụ đã khởi động hoặc các ứng dụng đã cài đặt. Những thay đổi này có thể không tồn tại lâu dài trong quá trình khởi động lại, do đó, điều tra viên nên ghi lại chúng.

Dữ liệu bất biến thường nằm trong ổ cứng; ngoài ra cũng tồn tại trong các tệp hoán đổi, dung lượng trống và dung lượng ổ đĩa chưa được phân bổ. Các nguồn dữ liệu bất biến khác bao gồm CD-ROM, ổ lưu trữ USB và điện thoại thông minh.

**3. Phân tích bộ nhớ Windows**

Phân tích bộ nhớ Windows là một phần quan trọng trong quy trình điều tra, bao gồm việc thu thập bộ nhớ vật lý hoặc kết xuất RAM của máy Windows. Việc kiểm tra các kết xuất bộ nhớ này cho phép các nhà điều tra phát hiện rootkit ẩn, tìm các đối tượng bị che giấu, xác định các quy trình đáng ngờ, và nhiều hơn nữa.

Phân tích bộ nhớ Windows:

* Vai trò quan trọng: Bộ nhớ Windows chứa nhiều thông tin quan trọng có thể giúp phát hiện các hoạt động độc hại.
* Thu thập bộ nhớ: Điều tra viên cần có kỹ thuật và công cụ phù hợp để thu thập bộ nhớ vật lý hoặc kết xuất RAM chính xác.

Kết xuất bộ nhớ:

* Kết xuất bộ nhớ (Memory Dump): Đây là bản sao toàn bộ hoặc một phần bộ nhớ của hệ thống tại một thời điểm cụ thể.
* Kiểm tra kết xuất bộ nhớ: Quá trình này có thể tiết lộ nhiều thông tin quan trọng như rootkit ẩn, đối tượng ẩn, và quy trình đáng ngờ.

Phát hiện rootkit ẩn:

* Rootkit: Phần mềm độc hại được thiết kế để ẩn sự hiện diện của chính nó và các hoạt động của kẻ tấn công.
* Tìm kiếm rootkit: Phân tích bộ nhớ có thể phát hiện các rootkit mà các phương pháp bảo mật khác có thể bỏ sót.

Xác định quy trình đáng ngờ:

* Quy trình đáng ngờ: Các quy trình không bình thường hoặc không mong muốn chạy trên hệ thống.

Xác định quy trình đáng ngờ: Kiểm tra kết xuất bộ nhớ giúp xác định và phân tích các quy trình này, hỗ trợ trong việc phát hiện và loại bỏ mối đe dọa.

**4. Phân tích Windows Registry**

Windows Registry là cơ sở dữ liệu phân cấp chứa các cài đặt cấp thấp cho hệ điều hành Microsoft Windows và cho các ứng dụng sử dụng registry. Việc điều tra các dữ liệu có trong registry giúp nhà điều tra có thông tin về cài đặt cấu hình trình điều khiển phần cứng và cài đặt phần mềm, theo dõi hoạt động đáng ngờ của người dùng, xác định thông tin thiết bị được kết nối, ... từ đó giúp xây dựng phân tích luồng thời gian về sự cố.

Quản trị viên có thể tương tác trực tiếp với registry thông qua bất kỳ ứng dụng trung gian nào, phổ biến nhất là trình chỉnh sửa registry GUI đi kèm với Windows-regedit và regedit 32

Có 5 thư mục gốc trong trình chỉnh sửa Registry:

- HKEY\_USERS: Thư mục này chứa tất cả các hồ sơ người dùng được tải cho hệ thống đó

- HKEY\_CLASSES\_ROOT: Thư mục này chứa thông tin cấu hình liên quan đến ứng dụng nào được sử dụng để mở các tệp khác nhau trên hệ thống

- HKEY\_CURRENT\_CONFIG: Thư mục này chứa cấu hình phần cứng mà hệ thống sử dụng khi khởi động

- HKEY\_LOCAL\_MACHINE: Thư mục này chứa một loạt các thông tin cấu hình cho hệ thống bao gồm cài đặt phần cứng và cài đặt phần mềm

- HKEY\_CURRENT\_USER: Thư mục này là hồ sơ người dùng đang hoạt động, được tải cho người dùng hiện đang đăng nhập

Cấu trúc của Registry: Các thành phần khác nhau của Registry được gọi là "ô" có cấu trúc cụ thể và chứa loại thông tin cụ thể, bao gồm:

- Ô khoá chính: chứa thông tin khóa registry và bao gồm các nhánh đối với các ô khác cũng như thời gian ghi cuối cùng cho khóa

- Ô giá trị: lưu giữ một giá trị và dữ liệu

- Ô danh sách khóa con: được tạo thành từ một loạt các chỉ mục trỏ đến các ô khóa chính, tất cả đều là các khóa phụ của ô khóa chính

- Ô danh sách giá trị: được tạo thành từ một loạt các chỉ mục trỏ đến các ô giá trị, tất cả đều là giá trị của một ô khóa chung

- Ô mô tả bảo mật: chứa thông tin mô tả bảo mật cho một ô khóa chính

Registry dưới dạng một tệp nhật ký:

- Registry được so sánh với tệp nhật ký vì nó có một số hành động hoặc sự kiện liên quan đến thời gian

- Thời gian ghi cuối là thuộc tính được liên kết với các khóa registry tương tự như thời gian sửa đổi cuối cùng được liên kết với các tệp và thư mục

- Thông tin này cung cấp khung thời gian tham chiếu cho các hoạt động nhất định của người dùng trên hệ thống và nó cũng cho biết khi nào một giá trị cụ thể được thêm vào khóa hoặc sửa đổi

**5. Phân tích bộ nhớ đệm, cookie, lịch sử**

Cache: Cho phép người dùng lưu vào bộ đệm cục bộ nội dung của các trang web để tăng tốc độ truy cập trong tương lai vào các trang được truy cập thường xuyên. Nội dung đã tải xuống vẫn còn trên ổ cứng cho đến khi bị xóa. Dữ liệu vẫn còn trong không gian chưa được phân bổ của ổ cứng ngay cả sau khi bộ nhớ cache bị xóa.

Cookie: Cookie là các gói dữ liệu nhỏ để theo dõi, xác thực và duy trì thông tin người dùng cụ thể Cookie hết hạn tại đó trình duyệt sẽ xóa; cookie không có ngày hết hạn sẽ xóa cuối phiên người dùng. Người dùng có thể xóa dữ liệu cookie. Ngay cả sau khi xóa cookie, dữ liệu có thể vẫn còn trong không gian chưa được phân bổ của ổ cứng

Lịch sử: Lịch sử duyệt web là dấu vết do người dùng để lại khi họ thực hiện các hoạt động kết nối Internet qua trình duyệt web.

Việc kiểm tra các trình duyệt web như Microsoft Edge, Google Chrome, Mozilla Firefox, ... cung cấp các bằng chứng quan trọng như lịch sử web, thông tin cookie và bộ đệm liên quan đến hoạt động duyệt web của người dùng

**6. Phân tích các tệp trong Windows**

Trong khi điều tra hệ thống Windows, thường cần phát hiện bất kỳ thay đổi nào mà kẻ tấn công có thể thực hiện đối với các tệp trên hệ thống

Để phát hiện những thay đổi, cần kiểm tra những điều sau:

- Restore Point Directories: Thư mục này lưu trữ thông tiên liên quan đến cài đặt xóa các tệp ứng dụng và bất kỳ thay đổi nào được thực hiện với chúng

- Prefetch File: Kiểm tra các thư mục tìm nạp trước giúp xác định các ứng dụng đã được chạy trên hệ thống

- Metadata: Siêu dữ liệu được liên kết với bất kỳ tệp nào sẽ tiết lộ các đặc điểm khác nhau và chi tiết hơn liên quan đến việc tạo truy cập sửa đổi tệp

- Tệp hình ảnh và dữ liệu exif: Kiểm tra ảnh Jpeg và dữ liệu exif được lưu trữ trong đó giúp xác định các siêu dữ liệu được liên kết với hình ảnh đó

**7. Điều tra siêu dữ liệu**

Mỗi tệp tin được lưu trữ trên máy tính đều sẽ có liên kết với một bộ siêu dữ liệu Metadata mà cung cấp đầy đủ thông tin về xuất xứ nguồn gốc, tác giả tệp tin và các thông tin liên quan khác. Có thể nói, Metadata trong tệp tin là phần thông tin lưu trữ ở trong tệp, bao gồm các thông tin cơ bản:

- Thời gian và ngày tạo

- Chương trình hoặc quy trình được sử dụng để tạo dữ liệu

- Mục đích của dữ liệu

- Người tạo hoặc tác giả của dữ liệu

- Vị trí trên thiết bị nơi dữ liệu được tạo

- Tiêu chuẩn kỹ thuật được sử dụng

- Các sửa đổi hoặc chương trình được sử dụng để sửa đổi tệp

Một số thông tin hữu ích đối với các nhà điều tra như:

- Khôi phục tên tệp, phần mở rộng của chúng, ngày tạo, sửa đổi và truy cập tương ứng của chúng

- Lịch sử thực thi, lỗi, số lần ghi và đọc bản ghi

- Thông tin tạo, sửa đổi và truy cập tập tin

- Truy cập tất cả thông tin được lưu trữ trong một tài liệu

- Truy cập thông tin tài liệu ẩn

Mặc dù có nhiều loại siêu dữ liệu nhưng những loại siêu dữ liệu quan trọng nhất đối với các trường hợp nhà điều tra là thông tin liên quan đến ngày tạo, sửa đổi và truy cập tệp. Những loại siêu dữ liệu này có thể được sử dụng để xác định thời điểm tệp được tạo và sửa đổi bởi kẻ tấn công cũng như xác định thời điểm chúng được truy cập bởi các cá nhân khác trên mạng hoặc hệ thống.

Siêu dữ liệu được biết đến phổ biến nhất về các tệp trên hệ thống Windows là thời gian MAC (modified, accessed and created) của tệp. Thời gian MAC là dấu thời gian đề cập đến thời điểm teeoj được sửa đổi lần cuối, thời điểm tệp được truy cập lần cuối và thời điểm tập tin được tạo ban đầu. Trên hệ thống tệp FAT, những khoảng thời gian này được ghi lại trên giờ địa phương của hệ thống trong khi hệ thống tệp NTFS lưu thời gian MAC ở định dạng giờ quốc tế UTC

Siêu dữ liệu trên PDF

- Các tệp định dạng tài liệu di động (PDF) có thể chứa siêu dữ liệu như tên tác giả, ngày tạo ứng dụng sử dụng để tạo.

- Siêu dữ liệu cho thấy tệp PDF được tạo trên MAC hoặc được tạo bằng cách chuyển Word sang pdf.

- Các tập lệnh pdfmeta.pf và pdfdmp có thể sử dụng để trích xuất dữ liệu từ các tệp pdf

- Ngoài ra các thể truy xuất siêu dữ liệu thông qua Adobe Reader

Siêu dữ liệu trên Word:

- Tài liệu Word là phức hợp hơn dựa trên công nghệ OLE để xác định cấu trúc tệp trong một tệp

- Bên cạnh thông tin định dạng tài liệu Word có thể chứ khá nhiều thông tin bổ sung mà người dùng không nhìn thấy được hoặc tùy vào cách nhìn của người dùng đối với tài liệu.

- Tài liệu Word không chỉ có thể lưu giữ các bản sửa đổi trước đây mà còn danh sách tối đa 10 người dùng đã chỉnh sửa tệp gần đây nhất. Điều này gây ra rủi ro rò rỉ thông tin cho các cá nhân tổ chức

- Các tập lệnh Perl wmd.pl và olemp.pl được sử dụng để liệt kê các luồng OLE và thùng rác được nhúng trong tài liệu

**8. Phân tích nhật ký sự kiện**

Windows Event Logs gồm những sự kiện liên quan đến software, hardware, OS, security. Service Windows Event Log chịu trách nhiệm quản lý các sự kiện, nhật ký sự kiện; nó thu thập các sự kiện từ nhiều nguồn khác nhau và lưu trữ tập chung tại một thư mục. Các sự kiện này có thể giúp người điều tra biết những gì xảy ra trên hệ thống, xảy ra vào thời gian nào, tham chiếu đến người dùng cụ thể liên quan đến những hành vi đó hay các thông tin của các hệ thống, tài nguyên truy cập từ xa.

Có 3 loại nhật ký sự kiện chính của Windows:

- Application Log (Nhật ký ứng dụng): Ghi lại những sự kiện liên quan đến các chương trình được cài đặt trong hệ thống. Điều này ghi lại các lỗi xảy ra trong ứng dụng, các sự kiện thông tin và cảnh báo từ các ứng dụng phần mềm. Bằng cách sử dụng nhật ký ứng dụng, có thể khắc phục mọi sự cố phần mềm ngăn phần mềm đăng nhập hoặc hoạt động bình thường.

- Security Log (Nhật ký bảo mật): Ghi lại các thông tin chi tiết về sự kiện dựa liên quan đến bảo mật như nỗ lực truy đăng nhập, truy cập tài nguyên. Các thông tin này có thể giúp nhà điều tra xác định hoạt động trái phép trên hệ thống

- System Log (Nhật ký hệ thống): Các sự kiện được ghi lại liên quan đến các thành phần hệ thống Window chẳng hạn như thành phần giao diện và trình điều khiển tích hợp sẵn. Những sự kiện này thường được thiết lập trước bởi chính hệ điều hành đang hoạt động. Tệp nhật ký hệ thống có thể chứa dữ liệu về những thay đổi phần cứng, trình điều khiển thiết bị, thay đổi hệ thống và tất cả các hoạt động liên quan đến máy.

**Liệt kê các thư mục quan trọng khi thực hiện công việc điều tra số trên Windows**

Khi cài đặt Windows, trình cài đặt có thể chọn vị trí bất kỳ. Tuy nhiên trên hầu hết các máy, có thể tìm thấy vị trí mặc định. Ví dụ C:\thư mục người dùng, chỉ truy cập được nếu người dùng có quyền quản trị.

− C:\Program Files. Đây là nơi hầu hết các chương trình được cài đặt. Là nơi tốt để tìm các phần mềm gián điệp, công cụ hack, và phần mềm khác có thể liên quan đến tội phạm máy tính.

− C:\Windows. Đây là nơi mà các hệ điều hành được lưu trữ. Kiểm tra các thư mục tạm thời có thể mang lại những bằng chứng hữu ích. Cũng là một ý hay để tìm kiếm bất cứ file mới trong thư mục này, vì chúng có thể là dấu hiệu của phần mềm gián điệp hay virus.

− C:\Windows\System32. Thư mục này chứa các file hệ thống quan trọng DLLs. Nếu thấy có bổ sung mới có nghĩa là phần mềm mới được cài đặt. Phần mềm mới có thể bao gồm các chương trình chat, phần mềm gián điệp hoặc virus.

− C:\Users\username\Documents. Đây là vị trí mặc định của các tài liệu, và là một nơi tốt để kiểm tra. Khi đăng nhập vào Windows và vào C:\Users \username\Documents – thư mục cho người sử dụng hiện đang đăng nhập.

− C:\Users\username\Pictures. Đây là nơi lưu trữ hình ảnh mặc định của Windows, cũng như tài liệu là thư mục tài liệu mặc định.

− C:\Users\username\Favorites. Đây là nơi Internet Explorer lưu trữ thư mục yêu thích của mỗi người dùng. Là nơi có thể tìm ra những trang web mà tội phạm có thể đánh dấu.

− C:\Users\username\Desktop. Cho thấy màn hình máy tính người dùng.

− C:\Users\username\Downloads. Thư mục này quan trọng. Đây là vị trí mặc định cho bất kỳ chương trình tải về từ Internet.

**7.Trình bày phương pháp và các công cụ thu thập bộ nhớ Volatile và Non-Volatile trên Hệ điều hành Linux ?**

### 1. Phương pháp thu thập bộ nhớ Volatile (RAM)

a. Chuẩn bị:

- Bước 1: Xác định thời điểm thu thập dữ liệu, thường là ngay sau khi phát hiện sự cố hoặc trước khi tắt máy.

- Bước 2: Chuẩn bị các công cụ thu thập dữ liệu như USB chứa phần mềm cần thiết.

b. Tiến hành thu thập:

- Bước 1: Cắm USB chứa công cụ vào máy tính mục tiêu.

- Bước 2: Sử dụng các lệnh shell để thu thập thông tin hệ thống.

- Bước 3: Lưu dữ liệu thu thập được vào một thiết bị lưu trữ an toàn để phân tích sau này.

c. Công cụ và lệnh:

- dmesg`: Hiển thị bộ đệm vòng kernel và thông tin về trình điều khiển thiết bị.

- stat`: Hiển thị trạng thái file hoặc các trạng thái hệ thống file.

- history`: Liệt kê nhật ký của Bash về các lệnh đã nhập.

- fsck`: Kiểm tra và sửa chữa hệ thống tệp.

- ps`: Báo cáo trạng thái của tiến trình hiện tại.

- netstat`: Hiển thị các kết nối mạng, bảng định tuyến và giao diện mạng.

- last`: Hiển thị thời gian và ngày đăng nhập và đăng xuất của người dùng.

- ifconfig`: Hiển thị cấu hình của các giao diện mạng.

- lsof`: Liệt kê các tệp đang mở và các tiến trình đang hoạt động đã mở chúng.

- xclip`: Xuất nội dung của khay nhớ tạm.

- aureport`: Xem báo cáo tóm tắt nhật ký daemon kiểm tra.

- ps`: Kiểm tra cây tiến trình để xác định quy trình con và phụ thuộc đáng ngờ.

- ss`: Kiểm tra các kết nối mạng hiện tại và trạng thái của chúng.

- arp`: Giải nén bộ nhớ cache ARP.

- readelf`: Phân tích tiêu đề và các phần của tệp ELF.

- cat /proc/`: Các lệnh như `cat /proc/cpuinfo`, `cat /proc/partitions`, `cat /proc/swaps` để thu thập thông tin về hệ thống.

### 2. Phương pháp thu thập bộ nhớ Non-Volatile (ổ cứng)

a. Chuẩn bị:

- Bước 1: Xác định các phân vùng và ổ đĩa cần thu thập dữ liệu.

- Bước 2: Chuẩn bị các công cụ pháp y số như `dd`, `Autopsy`, hoặc `EnCase`.

b. Tiến hành thu thập:

- Bước 1: Khởi động hệ thống bằng USB hoặc CD chứa công cụ pháp y để tránh làm thay đổi dữ liệu.

- Bước 2: Tạo ảnh của ổ cứng bằng `dd` hoặc các công cụ tương tự, đảm bảo ghi lại toàn bộ dữ liệu, bao gồm cả slack space và unallocated space.

- Bước 3: Lưu ảnh ổ cứng vào một thiết bị lưu trữ an toàn để phân tích sau này.

c. Công cụ và lệnh:

- dd`: Sao chép tệp, chuyển đổi và định dạng tệp.

- mount`: Gắn kết một hệ thống tệp.

- lsmod`: Hiển thị các mô-đun đã tải.

- lsof`: Liệt kê các tệp đang mở.

- top`: Hiển thị thông tin tóm tắt hệ thống và danh sách tiến trình.

- swapon`: Kiểm tra không gian swap.

- file`: Hiển thị loại dữ liệu có trong tệp máy tính.

- find`: Tìm kiếm các tệp trong cây thư mục.

- grep`: Tìm kiếm mẫu trong tệp.

- log files`: Kiểm tra các nhật ký hệ thống tại `/var/log/`.

**8. Tìm hiểu về quy trình, công cụ, các công việc cần thực hiện khi thực hiện công việc điều tra số trên Linux, liệt kê các thư mục quan trọng khi thực hiện công việc điều tra số trên Linux.**

**1. Shell Commands**

Các điều tra viên sử dụng các lệnh shell trong Linux để thu thập thông tin từ hệ thống, một số lệnh thường dùng bao gồm:

DMESG

Lệnh “dmesg” là viết tắt của các thông báo hiển thị hoặc “thông báo trình điều khiển”, lệnh hiển thị bộ đệm Dmesg chứa thông tin về trình điều khiển được tải vào nhân trong quá trình khởi động và thông báo lỗi đượC tạo ra tại thời điểm tải trình điều khiển vào nhân.

Lệnh dmesg –S: xem nhật ký hệ thống

Lệnh dmesg --level=err,warn: xem các lỗi và cảnh báo

FSCK

Lệnh “fsck” dành cho kiểm tra tính nhất quán của hệ thống tệp. Nó là một công cụ để kiểm tra tính nhất quán của hệ thống Linux và sửa chữa tương tác trên một hoặc nhiều hệ thống tệp Linux.

Lệnh fsck –A: kiểm tra tất cả các hệ thống tệp được cấu hình

STAT

Lệnh “stat” dùng để hiển thị thông tin về một tập tin hoặc thư mục cụ thể, bao gồm các thông tin về quyền truy cập, thời gian tạo, thời gian sửa đổi và kích thước của tập tin hoặc thư mục.

Cú pháp: stat + tên file: để xem cái thông tin về file

File: Tên của file.

Size: Dung lượng của file tính theo byte.

Uid: ID người dùng và tên tài khoản của chủ sở hữu.

Access: Đánh dấu thời gian truy cập.

Change: Đánh dấu thời gian thay đổi. Đây là thời gian các thuộc tính hoặc nội dung của file được thay đổi lần gần nhất.

HISTORY: Lệnh history liệt kê tất cả các lệnh đã được chạy trên Shell Commands trước đó.

MOUNT

PS: hiển thị thông tin về các tiến trình đang chạy trên hệ thống.

Cú pháp: ps [tùy chọn]

4 tham số được hiển thị về các process đang chạy:

PID: process ID.

TTY: Loại terminal.

TIME: Tổng thời gian process đã chạy.

CMD: tên của lệnh khởi chạy process.

Ví dụ: Lệnh ps trong Linux có thể được sử dụng với tùy chọn -u để hiển thị thêm thông tin về các quy trình.

%CPU: thể hiện cho sức mạnh tính toán mà tiến trình đang sử dụng.

%MEM: thể hiện cho dung lượng bộ nhớ mà tiến trình đang sử dụng.

STAT: thể hiện cho trạng thái tiến trình.

PSTREE: Lệnh "pstree" trong Linux là một công cụ hiển thị cấu trúc cây của tất cả các tiến trình đang chạy trên hệ thống.

Cú pháp:

pstree [tùy chọn] [Pid]

Các tùy chọn phổ biến của lệnh "pstree" bao gồm:

-p: Hiển thị các ID tiến trình của các tiến trình con.

-u: Hiển thị tên người dùng của các tiến trình.

-a: Hiển thị tên của tất cả các tiến trình, thay vì chỉ hiển thị tên của các tiến trình cha.

Cây tiến trình được sắp xếp theo thứ tự cha con,từ đó dễ dàng hiểu được mối quan hệ giữa các tiến trình và quá trình khởi động hệ thống.

GREP: Lệnh grep trong linux thường được sử dụng để tìm kiếm văn bản hoặc tìm kiếm tệp file có chứa nội dung khớp với các chuỗi hoặc từ cần tìm kiếm.

Cú pháp: grep [tùy chọn] pattern [FILE]

KILL:Lệnh "kill" trong Linux được sử dụng để gửi một tín hiệu (signal) đến một tiến trình để yêu cầu nó dừng hoạt động. Tuy nhiên, không nên sử dụng lệnh "kill" một cách ngẫu nhiên vì nó có thể gây ra các vấn đề về ổn định hệ thống hoặc mất dữ liệu.

Lưu ý: nếu muốn dừng một tiến trình bằng cách sử dụng lệnh "kill", cần biết ID của tiến trình đó.

Ví dụ: Có thể sử dụng lệnh "ps" để xem danh sách các tiến trình đang chạy trên hệ thống và tìm ID của tiến trình muốn dừng. Sau đó, có thể sử dụng lệnh kill theo cú pháp "kill <ID tiến trình>" để dừng tiến trình đó.

TOP: Lệnh top trong Linux được sử dụng để hiển thị tất cả các tiến trình đang chạy trong môi trường linux.

**2. Linux Log Files**

Cách sử dụng các tệp nhật ký Linux phổ biến

/var/log/messages: thông báo chung và những thứ liên quan đến hệ thống

/var/log/auth.log: nhật ký xác thực (/var/log/secure)

/var/log/kern.log: nhật ký kernel

/var/log/cron.log: nhật ký crond

/var/log/maillog: nhật ký máy chủ mail

/var/log/qmail: thư mục nhật ký qmail (nhiều file hơn ở trong thư mục này)

/var/log/httpd: thư mục nhật ký lỗi và truy cập apache

/var/log/lighttpd: thự mục nhật ký lỗi và quyền truy cập lighttpd

/var/log/nginx: thư mục nhật lý lỗi và truy cập nginx

/var/log/apt: lịch sử lệnh apt/apt-get và thư mục nhật ký

/var/log/boot.log: nhật ký khởi động hệ thống

/var/log/mysqld.log: tệp nhật ký máy chủ cơ sở dữ liệu MySQL

/var/log/utmp or /var/log/wtmp: tệp bản ghi đăng nhập

/var/log/yum.log or /var/log/dnf.log: tệp nhật ký lệnh yum/dnf

/var/log/daemon.log: nhật ký daemon

/var/log/debug: Nhật ký gỡ lỗi (nhật ký gỡ lỗi lưu trữ các thông báo chi tiết liên quan đến gỡ lỗi và rất hữu ích để khắc phục sự cố các hoạt động hệ thống cụ thể)

**3. Collecting Volatile Data**

Chạy lệnh netstat để hiển thị danh sách các kết nối mạng đang được sử dụng trên hệ thống, bao gồm các số như địa chỉ IP và số cổng. Nó cũng sẽ hiển thị ID của tiến trình đang sử dụng kết nối, giúp bạn xác định các tiến trình đang hoạt động trên hệ thống và các kết nối mạng mà chúng đang sử dụng.

Chạy lệnh last –F để xem thời gian người dùng đăng nhập và đăng xuất

Chạy lệnh hostname để xem tên máy chủ hệ thống

Chạy lệnh ifconfig –a để xem cấu hình của tất cả các mạng trên hệ thống

Chạy lệnh lsof để cho phép bạn xem các tệp tin và socket được mở trên hệ thống và thông tin về các tiến trình đang sử dụng chúng. Công cụ này có thể cung cấp các số như ID của tiến trình và địa chỉ inode của tệp tin.

Chạy lệnh lsmod để hiển thị các module đã tải

Xclip là một giao diện dòng lệnh cho X clipboard

Chạy xclip –o để xuất nội dung của bộ nhớ tạm

Chạy lệnh aureport để xem báo cáo tóm tắt nhật kí

Chạy lệnh id để xác định id cho tên người dùng được chỉ định.

Sau đó, chạy lệnh ausearch để theo dõi tất cả các sự kiện liên quan đến người dùng này.

Định dạng thực thi và liên kết (ELF) là định dạng tệp thực thi chính.

Hệ thống lưu trữ các thư viện được chia sẻ , nhân module và nhân ở dạng ELF.

Chạy lệnh readelf để phân tích tiêu đề và các phần của tệp ELF.

Xác minh nội dung của đường dẫn /var/spool/cron/ và /etc/cron.daily để thu thậtp thông tin về các nhiệm vụ đã được lên lịch

Nhận về lịch sử các dòng lệnh từ tệp .bash\_history

Thu thập dữ liệu trạng thái hiện tại của một hệ thống linux từ thư mục “/proc”

1. Chạy lệnh ps để xem các tiến trình đang chạy trên hệ thống

2. Nó cung cấp bản ghi nhanh của các quy trình hiện tại cùng với thông tin chi tiết như id người dùng , mức sử dụng cpu , mức sử dụng bộ nhớ , tên lệnh , ...

3. Kiểm tra cây quy trình để xác định bất kì quy trình con và phụ thuộc đáng ngờ nào

Chạy lệnh arp để giải nén bộ nhớ cache ARP

Chạy lệnh ss –l –p –n | grep <PID> để xem liệu một quá trình chạy trên hệ thống có đáng nghi ngờ

Chạy lệnh cat /proc/version để cho biết phiên bản nhân linux được sử dụng trong hệ điều hành.

Chạy lệnh cat /proc/sys/kernel/ domainname để biết tên miền.

Chạy lệnh cat /proc/swaps để xem tổng số và kích thước hoán đổi đã sử dụng.

Chạy lệnh cat /proc/partitions để xem danh sách các phân vùng ổ đĩa.

Chạy lệnh cat /proc/cpuinfo để hiển thị thông tin về CPU trong hệ thống.

Chạy lệnh cat /proc/self/mounts để xem bộ đếm điểm và gọi các thiết bị gắn ngoài.

**4. Collecting Non-Volatile Data**

Xem các kết nối và tệp được chia sẻ

Kiểm tra các dịch vụ tự động khởi chạy

Xem xét các tệp mới được chỉnh sửa

Thu thập thông tin đăng nhập và thông tin hệ thống

Tìm kiếm tệp có tên lạ trong thư mục /dev

Kiểm tra cài đặt bảo mật của hệ thống

Tìm các tệp đã xóa và liên kết dữ liệu

Sử dụng LVM để tìm kiếm các phân vùng chưa được định dạng và các tệp tin

**5. Swap Space**

Không gian lưu trữ hoán đổi

Là không gian lưu trữ trên ổ cứng được sử dụng làm bộ nhớ ảo (RAM ảo).

Khi các máy linux chạy hết RAM , các trang không hoạt động sẽ được di chuyển đến không gian lưu trữ hoán đổi để giải phóng bộ nhớ.

Dung lượng slack trên đĩa cứng phải gấp đôi RAM , nếu dung lượng ram <= 2gb.

Trong trường hợp RAM > 2gb , ví dụ 5gb , thì dung lượng slack phải nhiều hơn 2gb so với RAM, tức là 7gb.

Lệnh swapon –s để xem không gian lưu trữ hoán đổi.

**Các thư mục quan trọng khi thực hiện công việc điều tra số trên Linux.**

* /home: Thư mục này là thư mục của mỗi người dùng. Nó tương tự như C:\Users trong Windows.
* /root: Đây là thư mục cho người quản trị có quyền root. Hacker luôn muốn hack được tài khoản root trên bất kỳ hệ thống Unix.
* /var: Thư mục này có chứa các mục quản trị như các bản ghi, cần kiểm tra thư mục này triệt để.
* /temp: Nơi đây chứa các tập tin tạm thời.
* /etc: Chứa các tập tin cấu hình, khi điều tra sự xâm nhập, thường thì thủ phạm thay đổi file cấu hình. Vì vậy so sánh các tập tin cấu hình trên máy tính bị nghi ngờ với các phiên bản sao lưu có thể rất hữu ích.

**9. Trình bày các kỹ thuật Anti-forensic trên hệ điều hành Windows và đưa ra một ví dụ cụ thể?**

Các kỹ thuật Anti-forensic trên hệ điều hành Windows

Anti Forensics - chống điều tra kỹ thuật số là các kỹ thuật được sử dụng để đối phó để việc tìm kiếm và thu thập các chứng cứ số trong điều tra.

Sử dụng các kỹ thuật làm ảnh hưởng đến sự tồn tại, số lượng và chất lượng của chứng cứ số thu được tại hiện trường vụ án, điều này làm cho việc phân tích và kiểm tra chứng cứ gặp khó khăn hoặc không thể thực hiện được.

Các kỹ thuật Anti-forensic

- Che giấu các dữ liệu có chứng cứ số

+ Ẩn các dữ liệu có chứng cớ là quá trình làm cho dữ liệu khó tìm với người lạ trong khi cũng giữ nó dễ tiếp cận với người chủ để còn sử dụng trong tương lai.

+ Mã hóa dữ liệu là một cách giấu dữ liệu thông dụng. Khi dữ liệu được mã hóa, người ta có thể sử dụng các thuật toán phức tạp để khiến dữ liệu khó có thể đọc được.

++Mã hóa có hai quá trình ngược chiều nhau là mã hóa và giải mã dựa vào một chìa khóa bí mật. Các thuật toán mã hóa càng phức tạp, càng mất thời gian giải mã nó mà không có mã số. Các thuật toán mã hóa càng phức tạp, càng mất thời gian giải mã nó mà không có mã số. Các thuật toán mã hóa có thể bị phá nhưng phải tốn nhiều thời gian và công sức.

++Kỹ thuật mã hóa dữ liệu

           Thông thường khi mã hóa, người ta thiết lập mật khẩu cho tập tin hoặc thư mục, đây là cách an toàn nhất cho việc mã hóa và bảo vệ dữ liệu. Tập tin hoặc thư mục sẽ được mã hóa và chỉ có thể mở hoặc sử dụng bằng cách khai báo mật khẩu. Người ta hay dùng mã hóa các file bằng các phần mềm nén file có dùng mật khẩu. Nếu không có mã số, điều tra viên sẽ phải sử dụng đến các chương trình chuyên dụng để có thể bẻ khóa.

+Kỹ thuật giấu dữ liệu

Steganography - việc viết và chuyển tải các thông điệp một cách bí mật, sao cho ngoại trừ người gửi và người nhận, không ai biết đến sự tồn tại của các thông điệp này, là một dạng của bảo mật như là che giấu file chứa dữ liệu.

• Trong kỹ thuật ẩn giấu thông thường, thông điệp xuất hiện dưới một dạng khác trong quá trình truyền tải: hình ảnh, bài báo hoặc thông điệp ẩn có thể được viết bằng mực vô hình giữa các khoảng trống trong một lá thư bình thường.

Kỹ thuật che giấu này còn được dùng trong công nghiệp giải trí và phần mềm như một kỹ thuật đánh dấu (watermarking) trên các hình ảnh, âm nhạc hay phần mềm để:

* Bảo vệ bản quyền tác giả
* Ngăn chặn mạo nhận, chống sao chép
* Xác thực nội dung
* Cho phép giám sát hay lần ngược dấu vết các bản sao bất hợp pháp

+Ẩn dấu các file dữ liệu: Giấu dữ liệu trong file hình ảnh

* Thay đổi các bit dữ liệu của hình ảnh bằng các bit của thông điệp bí mật sao cho mắt thường khó nhận ra sự thay đổi trên hình ảnh chứa thông điệp.
* Thuật toán cơ bản nhất là LSB (Least Significant Bit) để ẩn một thông điệp vào một tập tin ảnh bằng cách thay đổi bit cuối cùng của các giá trị màu RGB trong bức ảnh bằng bit của thông điệp bí mật.
* Các phần mềm dấu dữ liệu: QuickStego, Steganography, OpenPuff.

- Xóa các chứng cứ số

+Sử dụng các phần mềm xóa sạch chứng cứ số qua đó loại bỏ vĩnh viễn các tập tin cụ thể hoặc toàn bộ File System

+Việc xóa các chứng cứ số có thể được thực hiện thông qua việc sử dụng các phần mềm như: phần mềm xóa sạch tập tin, phần mềm làm sạch đĩa, công nghệ khử từ, xóa sạch ổ đĩa.

+phần mềm xóa sạch tập tin được sử dụng để xóa các tập tin cá nhân từ một hệ điều hành. Ưu điểm của phần mềm xóa sạch tập tin có thể hoàn thành công việc nhanh chóng. Một số phần mềm: BCWipe, R-Wipe & Clean, Eraser, Aevita Wipe & Delete, PrivacySuite.

+phần mềm làm sạch đĩa: sử dụng nhiều phương pháp để ghi đè lên dữ liệu hiện có trên đĩa. Phần mềm này sẽ vĩnh viễn xóa sạch các file bị xóa và đảm bảo không thể đọc lại các thông tin. Một số phần mềm: TuneUp Disk, Cleaner, DBAN, BCWipe, KillDisk, PC Inspector.

- Làm sai lạc các dấu vết

+mục đích của làm sai lạc các dấu vệt là để gây nhầm lẫn, nghi ngờ và làm chuyển hướng quá trình điều tra số.

+ làm sai lạc các dấu vết bao gồm một loạt các kỹ thuật và các công cụ như làm thay đổi thông tin đăng nhập, làm giả mạo và tạo thông tin sai lạc.

+ Dùng phần mềm thay đổi Metadata được đính kèm với file. Nếu Metadata đã bị hủy hoại, việc chứng minh bằng chứng trở nên khó khăn hơn.

- Dùng phần mềm chống các quy trình và các công cụ điều tra kỹ thuật số

Phần mềm thay đổi Header của file

+Dùng phần mềm đánh lừa bằng cách thay đổi thông tin trong header của file

+Header thường được ẩn với mọi người nhưng nó thực sự quan trọng khi nó thông báo cho máy tính loại file mà nó đang được gắn với.

+Điều tra viên đang tìm kiếm một định dạng file cụ thể mà có thể bỏ qua thông tin quan trọng bởi header của file đã vị thay đổi như không liên quan tới thông tin cần tìm kiếm.

+phần mềm: Transmogrify

Sử dụng các phần mềm bảo vệ hệ thống

+Nghi phạm có thể dùng phần mềm cài trên máy chống cac quy trình và các công cụ điều tra kỹ thuật số

+Sử dụng ứng dụng tự động xóa dữ liệu khi có người không được quyền truy cập hệ thống vào

Phần mềm tự xóa dữ liệu

+Các phần mềm giúp người chủ máy tính, laptop hay thiết bị di động có thể hủy dữ liệu khi máy bị mất hoặc bị thu giữ

+Chức năng tự xóa có thể là một chức năng của các phần mềm chống mất cắp thiết bị

+Các phần mềm có thể dùng: Prey, LaptopLock, LoJack, McAfee,....

**10. Trình bày các kỹ thuật Anti-forensic trên hệ điều hành Linux và đưa ra một ví dụ cụ thể? (như câu 9)**

**11. Quy trình điều tra số mạng ( Network forensics)**

*Giai đoạn 1: Chuẩn bị và ủy quyền*

Trước khi bắt đầu một cuộc điều tra mạng, cần tiến hành khảo sát cơ sở hạ tầng mạng nơi xảy ra sự cố về an toàn. Điều tra mạng chỉ có thể áp dụng cho các môi trường mà ở đó những công cụ an toàn mạng như hệ thống phát hiện xâm nhập, hệ thống phân tích gói tin, tường lửa, phần mềm đo đạc lưu lượng đã được triển khai tại những điểm chiến lược. Các hệ thống như Honeynets, network telescope... cũng có thể được xây dựng để thu hút kẻ tấn công, nhằm nghiên cứu các hành vi và tìm hiểu chiến thuật của chúng. Đội ngũ chuyên gia quản lý những công cụ và hệ thống này cần phải được đào tạo, huấn luyện để có thể thu thập số bằng chứng tối đa và chất lượng nhất, nhằm tạo điều kiện thuận lợi cho việc điều tra, quy kết hành vi phạm tội. Giai đoạn này còn đòi hỏi một sự ủy quyền từ các bên liên quan nhằm hạn chế những vi phạm liên quan đến quyền bảo mật thông tin hay các chính sách an toàn của cá nhân hay tổ chức bên trong hệ thống.

*Giai đoạn 2. Phát hiện sự cố hoặc hành vi phạm tội*

Sau khi có được sự ủy quyền, điều tra viên cần tiến hành nghiên cứu các cảnh báo được tạo ra bởi các công cụ an toàn đã được triển khai. Thông thường, những cảnh báo này sẽ chỉ ra các hành vi vi phạm chính sách an toàn được thiết lập bởi tổ chức. Mọi hành động bất thường xuất hiện trong các cảnh báo đều sẽ được phân tích dựa trên những kiến thức về mạng máy tính hay kinh nghiệm nhận dạng các tấn công mạng thường gặp của điều tra viên. Sự hiện diện và tính chất của cuộc tấn công được xác định một cách sơ bộ dựa vào các thông số khác nhau như: lưu lượng mạng, thời gian hay tần suất xuất hiện các dấu hiệu bất thường. Lúc này cần nhanh chóng đưa ra nhận định về hình thức tấn công khả nghi. Đây là căn cứ cho việc quyết định tiếp tục điều tra hay bỏ qua các cảnh báo (cảnh báo sai). Cần thực hiện các biện pháp đề phòng như: sao lưu, ghi lại nội dung cảnh báo để đảm bảo chứng cứ số không bị sửa đổi trong toàn bộ quá trình, có hai hướng để tiếp cận vụ việc là ứng phó với sự cố hoặc thu thập các dấu vết mạng.

*Giai đoạn 3. Ứng phó sự cố*

Việc ứng phó sẽ dựa trên các thông tin được thu thập từ giai đoạn trước. Cần phải xây dựng quy trình ứng phó sự cố nhằm ngăn chặn các cuộc tấn công trong tương lai và phục hồi các tổn thất do tấn công gây ra. Trong cùng thời điểm ứng phó sự cố, điều tra viên cần quyết định ngay việc có tiếp tục điều tra và thu thập thêm thông tin hay không. Việc này được áp dụng đối với những trường hợp mà cuộc điều tra được triển khai trong khi tấn công đang xảy ra và vẫn chưa có thông tin về tội phạm.

*Giai đoạn 4. Thu thập các dấu vết mạng*

Dữ liệu tiếp tục được thu thập từ những công cụ an toàn mạng được sử dụng bổ sung. Các công cụ được sử dụng phải an toàn, có khả năng chịu lỗi, giới hạn quyền truy cập và phải có khả năng tránh sự thỏa hiệp. Các công cụ phải đảm bảo thu thập được lượng chứng cứ tối đa mà chỉ gây ra tác động tối thiểu đến nạn nhân. Một số công cụ có thể kể đến như Wireshark, tcpdump, Snort, Tcpxtract, Foremost.... Hệ thống mạng cũng cần được giám sát để xác định các tấn công trong tương lai. Tính toàn vẹn của dữ liệu được ghi lại và các bản ghi sự kiện mạng phải được đảm bảo, vì dữ liệu mạng thay đổi một cách liên tục và ít có khả năng tạo ra cùng một dạng dấu vết trong những lần sau. Không những vậy, số lượng dữ liệu lớn cần yêu cầu một không gian bộ nhớ tương đương và hệ thống phải đủ khả năng để xử lý các định dạng khác nhau một cách thích hợp.

*Giai đoạn 5. Duy trì và bảo vệ*

Các dữ liệu thu được từ giai đoạn trước sẽ được lưu trữ trên một thiết bị sao lưu. Việc “băm” giá trị của dữ liệu thu được sẽ đảm bảo tính chính xác và độ tin cậy trong quá trình điều tra. Một bản sao lưu khác của dữ liệu sẽ được sử dụng cho việc phân tích và lưu lượng mạng ban đầu thu được cũng sẽ được bảo vệ. Giai đoạn này được thực hiện để đảm bảo quá trình điều tra có thể được chứng minh ngay trên dữ liệu gốc (đã được bảo vệ) để đáp ứng các yêu cầu pháp lý.

*Giai đoạn 6. Kiểm tra*

Các dấu vết thu được từ các công cụ an ninh sẽ được tổng hợp, sắp xếp và chuyển đổi thành các dữ liệu theo thời gian. Điều này nhằm đảm bảo thông tin quan trọng không bị mất hoặc lẫn lộn. Những vết tích ẩn hoặc ngụy trang của kẻ tấn công cần phải được khai phá. Các thông tin dự phòng và dữ liệu không liên quan bị loại bỏ nhằm tập trung phân tích các bằng chứng có khả năng nhất.

*Giai đoạn 7. Phân tích*

Các vết tích sau khi được xác định sẽ được coi là chứng cứ số cơ sở và được tiếp tục phân tích để khai thác những dấu hiệu đặc biệt của tội phạm; Có thể sử dụng phương pháp thống kê và khai phá dữ liệu để tìm kiếm những dữ liệu phù hợp với các mẫu tấn công nghi ngờ. Một vài thông số quan trọng liên quan đến việc phân tích điều tra mạng như: sự thiết lập các kết nối mạng, truy vấn DNS, phân mảnh gói tin, kỹ thuật in dấu giao thức và hệ điều hành, các tiến trình giả mạo, phần mềm hay rootkit được cài đặt. Những công cụ được sử dụng trong giai đoạn này là NetworkMiner, Splunk, OllyDbg, Scapy.... Các mẫu tấn công được xâu chuỗi với nhau và tấn công sẽ được xây dựng và tái hiện lại giúp các điều tra viên nắm được ý định và phương thức hành động của kẻ tấn công. Kết quả của giai đoạn này là sự xác nhận các hành động khả nghi.

*Giai đoạn 8. Điều tra, quy kết trách nhiệm*

Các thông tin có từ giai đoạn Phân tích sẽ được dùng để xác định ai? Cái gì? Ở đâu? Khi nào? Như thế nào? Tại sao gây ra sự cố? Việc này sẽ giúp cho việc xây dựng lại kịch bản tấn công và quy kết trách nhiệm. Phần khó khăn nhất của việc phân tích điều tra mạng là xác định danh tính kẻ tấn công. Có hai cách thức mà kẻ tấn công sử dụng để che giấu danh tính là giả mạo IP và thực hiện tấn công bàn đạp.

*Giai đoạn 9. Báo cáo tổng kết*

Phần hoàn tất quá trình điều tra mạng là xây dựng báo cáo tổng kết. Nội dung báo cáo tổng kết trình bày cho người quản lý tổ chức và cán bộ pháp chế về các chứng cứ số thu thập được trong quá trình điều tra và một số tài liệu hệ thống liên quan. Bên cạnh đó, một báo cáo điều tra toàn diện của vụ việc sẽ được trình bày cùng các biện pháp được khuyến nghị để ngăn ngừa những sự cố tương tự xảy ra trong tương lai. Các kết quả được tài liệu hóa để sử dụng trong những cuộc điều tra sau này, cũng như cải thiện chất lượng các sản phẩm bảo mật.

**12. Các kiến thức về ổ đĩa NTFS, FAT32, Ext4.**

**\*Kiến thức về ổ đĩa NTFS:**

New Technology File System (NTFS) - hệ thống tập tin công nghệ mới: là một trong những hệ thống tập tin mới nhất được Windows hỗ trợ. Nó là một hệ thống tập tin hiệu suất cao có khả năng tự sửa chữa, hỗ trợ một số tính năng nâng cao như bảo mật, nén và kiểm tra ở cấp độ tập tin. Nó cũng hỗ trợ các giải pháp lưu trữ có dung lượng lớn và mạnh mẽ như đĩa tự phục hồi.

NTFS cung cấp bảo mật dữ liệu vì nó có khả năng mã hóa và giải mã dữ liệu, files, hoặc folders. Nó sử dụng 16-bít Unicode characters để đặt tên file và folders. Thuộc tính này của NTFS cho phép người dùng toàn thế giới quản lý files của họ với ngôn ngữ bản địa. Hơn nữa, nó còn có khả năng chịa lỗi cho hệ thống file. Nếu người dùng tạo bất cứ thay đổi nào đối với files, NTFS sẽ lưu lại tất cả những thay đổi vào một tệp log đặc biệt. Nếu hệ thống bị crash, NTFS sử dụng những files log đó để khôi phục lại ổ cứng trong một tình trạng đáng tin cậy và tối thiểu hóa mất mát dữ liệu. NTFS cũng tận dụng những khái niệm về siêu dữ liệu và master file tables. Metadata chứa những thông tin về data được lưu trữ trên máy tính. Master file table cũng có chứa những thông tin tương tự dạng bảng, nhưng so với metadata, bảng này có khả năng lưu dữ liệu ít hơn.

Các đặc điểm của NTFS bao gồm:

* NTFS dùng thư mục dạng b-tree để lưu trữ file clusters.
* NTFS lưu thông tin về file’s clusters và những thông tin khác về cluster.
* NTFS hỗ trợ files lên đến xấp xỉ 16 tỷ bytes.
* Một access-control list (ACL) cho phép admin server truy cập vào những file cụ thể
* NTFS có tính năng nén tập tin tích hợp
* NTFS cung cấp bảo mật dữ liệu trên cả đĩa di động và cố định

Kiến trúc của NTFS

Vào thời điểm định dạng ổ đĩa của file hệ thống, hệ thống tạo ra Master Boot Record. Nó chứa các câu lệnh thực thi gọi lệnh master boot và thông tin về bảng phân vùng cho ổ cứng. Khi một ổ đĩa với được gắn vào, Master Boot Record chạy những lệnh master boot. Trong NTFS, tất cả files được lưu trên clusters và chúng có những thuộc tính riêng biệt. Các thành phần như tên, size, hoặc dữ liệu lưu trữ trong một file được xem như là thuộc tính. Do đó, cấu trúc bên trong của NTFS đó giống như một cơ sở dữ liệu nơi mà tất cả các files được coi như một phần của hệ điều hành.

Các thành phần của kiến trúc NTFS gồm:

* Hard disk: nó bao gồm ít nhất một phân vùng.
* Master boot record: Nó chứa các lệnh thực thi master boot, cái mà hệ thống BIOS nạp vào bộ nhớ, những lệnh này được tìm những Master Boot Record được lưu trên bảng phân vùng để tìm ra phân phùng nào có thể kích hoạt hoặc boot vào.
* Boot sector: Được biết đến là volume boot record (VBR), nó là sector đầu được tìm thấy trong hệ thống file NTFS, nó lưu trữ lệnh boot và những thông tin khác, như định dạng, vị trí, kích cỡ dữ liệu được lưu trên hệ thống file NTFS.
* Ntldlr.dll: Bộ nạp khởi động, nó truy cập hệ thống file NTFS và nạp nội dung của file boot.ini.
* Ntfs.sys: File driver của hệ thống máy tính cho NTFS.
* Kernel mode: Nó là chế độ xử lý phép thực thi lệnh để có truy cập trực tiếp tới những thành phần hệ thống.
* User mode: Đây là chế độ xử lý trong đó một chương trình hoặc đoạn mã chạy.

**File Allocation Table (FAT),** được thiết kế vào năm 1976, là một hệ thống file cho rất nhiều hệ điều hành như DOS, Windows, và OpenDOS. Được thiết kế cho ổ cứng có dung lượng nhỏ và cấu trúc folder đơn giản, hệ thống file FAT được đặt tên theo cách nó tổ chức thư mục và bảng phân bổ file, chúng lưu tất cả các files và nằm ở ngay đầu ổ đĩa.

FAT tạo ra 2 bản copy của bảng phân bố file để bảo vệ ổ đĩa khỏi thiệt hại. Bảng phân bố file và thư mục gốc được lưu trữ trong một vị trí vĩnh viễn cố định. Ổ đĩa được định dạng sử dụng hệ thống file FAT tạo thành một cluster data, và kích thước của một khối được định dạng trên ổ đĩa sẽ xác định kích thước cluster dữ liệu.

Hệ thống này khớp số cluster cho hệ thống tệp FAT theo 16 bit và số cluster nằm trong lũy thừa của 2. Những thiết bị thực hiện FAT bao gồm bộ nhớ flash, camera số và những thành phần khác. Hầu hết tất cả các hệ điều hành được cài đặt trên máy tính cá nhân đều dùng hệ thống file FAT.

FAT File System Layout

Loại file hệ thống FAT32 bao gồm những thành phần sau:

* Reserved area: Sector đầu tiên được dành cho việc khởi động (Volume boot record - VBR), bao gồm tham số BIOS Parameter block (BPB) chứa thông tin cơ bản của file hệ thống, như là hệ thống tệp với các con trỏ chỉ vị trí của các phần khác cũng như mã khởi động của hệ điều hành.
* FAT area: Khu vực này lưu trữ hai bản sao (có thể thay đổi) của bản phân bổ file để giúp hệ thống kiểm tra khoảng trống hoặc không gian free của ổ cứng. Ở đây chứa các thông tin chi tiết về cluster và nội dung của chúng bao gồm files và đường dẫn. Các bản sao bổ sung trong hệ thống này được đồng bộ hoàn hảo với quá trình ghi, đọc, và chúng thay thế cho bảng cấp phát tệp chính FAT khi nó có vẻ như bị lỗi và hư hỏng.
* Data area: Trong khu vực này, nơi chiếm nhiều phần nhất của phân vùng, lưu các dữ liệu tập tin và thư mục thực tế. File hệ thống FAT làm đầy những phần trống hoặc không gian với filler (làm đầy) ước tính bởi 0xF6 dựa trên INT 1Eh’s Disk Parameter Table (DPT). FAT hỗ trợ read-only, phân vùng ẩn, hệ thống, và các thuộc tính lưu trữ.

Cấu trúc Folder FAT

Hệ thống file FAT set đầu vào thư mục 32-bytes cho tất cả các thư mục. Thư mục của hệ thống FAT tuân thủ theo quy tắc sau:

* Tên (eight-plus-threes characters): Tên file tối đa 8 kí tự và 3 kí tự đối với file mở rộng.
* Attribute byte (8 bits): thuộc tính
* Create time (24 bits)
* Create date (16 bits)
* Last access date (16 bits)
* Last modified date (16 bits)
* Starting cluster number in the file allocation table (16 bits)
* File size (32 bits)
* Tất cả hệ điều hành hỗ trợ hệ thống file FAT sử dụng thông tin hiện tại trong thư mục FAT

FAT32

FAT32 là một phiên bản của FAT thay thế FAT16, và nó xuất hiện trên Windows 95 OSR 2 và Windows 98. So với FAT16, FAT32 sử dụng các cluster nhỏ hơn với nhiều địa chỉ bits để hỗ trợ những ổ cứng có kích cỡ lớn hơn và lưu   trữ tốt hơn. Nó luôn tạo ra một backup cho bảng phân bổ file thay vì chỉ duy trì bản copy mặc định.

FAT32 Features

* Khả năng tận dụng không gian hiệu quả trên FAT32 là khoảng 10%-15%, cao hơn FAT16. Lý do là sử dụng các cluster nhỏ hơn.
* FAT32 rất mạnh mẽ vì nó có thể đối đích đến của thư mục gốc và tận dụng bản backup của bảng phân bố file.
* FAT32 bao gồm bản ghi mở rộng boot record để kết hợp bản backup các thông tin cơ bản.
* Tỷ lệ lỗi của FAT32 thấp hơn so với FAT16.
* FAT32 có khả năng tương thích tốt hơn FAT16.
* Thư mục gốc trên FAT32 là một chuỗi cluster thông thường, do đó có thể lưu trữ bất cứ nơi nào trên ổ cứng.
* FAT32 không áp đặt bất kì hạn chế nào đối với số lượng thư mục gốc.
* FAT32 cho phép người dùng vô hiệu hóa việc lặp lại bảng phân bổ tệp.

**Extended File System (ext)**

Hệ thống tập tin mở rộng (ext), hoặc hệ thống tập tin mở rộng đầu tiên, được phát hành vào tháng 4 năm 1992, là hệ thống tập tin đầu tiên vượt qua các hạn chế của hệ thống tập tin Minix. Ban đầu, nó được phát triển như một phần mở rộng của hệ thống tập tin Minix để vượt qua một số hạn chế của nó như kích thước phân vùng tối đa là 64 MB và tên tập tin ngắn. Hệ thống tập tin ext cung cấp kích thước phân vùng tối đa là 2 GB và độ dài tên tập tin tối đa là 255 ký tự. Hạn chế chính của hệ thống tập tin này là nó không cung cấp hỗ trợ cho các timestamp riêng biệt cho truy cập, sửa đổi inode và dữ liệu. Nó giữ một danh sách chưa được sắp xếp của các khối và inode trống, và nó làm phân mảnh hệ thống tập tin.

Hệ thống tập tin ext có cấu trúc dữ liệu siêu dữ liệu được lấy cảm hứng từ Hệ thống Tập tin UNIX (UFS). Nhược điểm khác của hệ thống tập tin này bao gồm sự hiện diện chỉ một timestamp và các danh sách liên kết cho không gian trống, dẫn đến sự phân mảnh và hiệu suất kém. Nó đã được thay thế bởi hệ thống tập tin mở rộng thứ hai (ext2).

**Second Extended File System (ext2)**

Remy Card phát triển hệ thống tập tin mở rộng thứ hai (ext2) như là một hệ thống tập tin mở rộng và mạnh mẽ cho Linux. Là hệ thống tập tin thành công nhất cho đến nay trong cộng đồng Linux, Ext2 là cơ sở cho tất cả các bản phân phối Linux hiện đang được sử dụng.

Hệ thống tập tin ext2 được phát triển dựa trên nguyên tắc lưu trữ dữ liệu dưới dạng các khối dữ liệu cùng độ dài. Mặc dù độ dài có thể thay đổi giữa các hệ thống tập tin ext2 khác nhau, kích thước khối của một hệ thống tập tin ext2 được thiết lập trong quá trình tạo ra nó.

Hệ thống làm tròn mỗi kích thước tập tin lên thành một số nguyên khối. Nếu kích thước khối là 1024 byte, thì một tập tin có kích thước 1025 byte sẽ chiếm hai khối 1024 byte. Không phải tất cả các khối trong hệ thống tập tin đều chứa dữ liệu; một số khối phải chứa thông tin mô tả cấu trúc của hệ thống tập tin. Hệ thống tập tin ext2 xác định topologia của hệ thống tập tin bằng cách mô tả mỗi tập tin trong hệ thống bằng một cấu trúc dữ liệu inode.

Một inode mô tả các khối dữ liệu mà một tập tin chiếm, cũng như quyền truy cập của tập tin, thời gian sửa đổi của tập tin và loại tập tin. Mỗi inode mô tả một tập tin duy nhất trong hệ thống tập tin ext2, và mỗi inode có một số duy nhất định danh nó.

Bảng inode lưu trữ tất cả các inode cho hệ thống tập tin. Hơn nữa, các thư mục ext2 đơn giản chỉ là các tập tin đặc biệt (được mô tả bởi các inode) chứa các con trỏ đến các inode của các mục thư mục của chúng.

**Third Extended File System (ext3)**

Được phát triển bởi Stephen Tweedie vào năm 2001, hệ thống file mở rộng thứ 3 (ext3) là bản file hệ thống sử dụng trên GNU/Linux OS. Đây là phiên bản nâng cấp của hệ thống file ext2. Lợi ích chính của hệ thống file này đó là ghi nhật ký giúp cái thiện tính ổn định của hệ thống máy tính. Nó có thể được gắn kết và sử dụng như một hệ thống tệp ext2 và có thể sử dụng tất cả các chương trình được phát triển cho hệ thống tệp ext2.

Kích thước tối đa của một file ext3 đơn lẻ dao động từ 16 GB đến 2 TB, và kích thước tối đa của toàn bộ hệ thống file ext3 dao động từ 2 TB đến 32 TB. Hệ thống file ext3 cũng cung cấp tính toàn vẹn dữ liệu tốt hơn. Nó đảm bảo rằng dữ liệu phù hợp với trạng thái của hệ thống tệp. Hơn nữa, ext3 nhanh hơn ext2 vì tính năng ghi nhật ký tối ưu hóa chuyển động đầu của ổ cứng HDD. Nó cũng cung cấp ba chế độ ghi nhật ký khác nhau, cung cấp sự đánh đổi giữa việc tối đa hóa tính toàn vẹn dữ liệu và tối ưu hóa tốc độ. Hệ thống file ext3 cũng rất đáng tin cậy và có khả năng chuyển đổi các phân vùng ext2 sang ext3 và ngược lại mà không cần phải phân vùng lại và sao lưu dữ liệu.

Các tính năng của Ext3

Tính toàn vẹn dữ liệu: Nó cung cấp tính toàn vẹn dữ liệu cho những sự kiện xảy ra bởi vì hệ thống máy tính tắt nguồn. Nó cho phép người dùng chọn loại và mức độ bảo vệ cho những dữ liệu nhận được.

Tốc độ: Vì hệ thống tệp ext3 là một hệ thống tệp có tính năng ghi nhật ký, nó thường có hiệu suất thông qua cao hơn ext2 trong hầu hết các trường hợp. Người dùng có thể lựa chọn tốc độ tối ưu từ ba chế độ ghi nhật ký khác nhau.

Dễ dàng chuyển đổi: Người dùng có thể chuyển đổi dễ dàng hệ thống file ext2 sang ext3 và tăng hiệu suất của hệ thống bằng cách sử dụng hệ thống file ghi nhật cứ mà không cần định dạng lại.

**Fourth Extended File System (ext4)**

Hệ thống tập tin mở rộng thứ tư (ext4) là một hệ thống tập tin nhật ký được phát triển như một bản kế nhiệm của hệ thống tập tin ext3 phổ biến. Nó cung cấp tính mở rộng và đáng tin cậy tốt hơn so với ext3 để hỗ trợ các hệ thống tập tin lớn của các máy tính 64 bit để đáp ứng nhu cầu tăng về dung lượng đĩa ngày càng tăng.

Hệ thống tập tin ext4 mặc định kích hoạt rào cản ghi và cho phép người dùng gắn một hệ thống tập tin ext3 như là một hệ thống tập tin ext4. Hệ thống tập tin này hỗ trợ Linux Kernel từ phiên bản 2.6.19 trở đi.

Các tính năng chính của ext4:

File System File: Ext4 hỗ trợ tối đa mỗi file cá nhân lên tới 16 TB và các phân vùng khoảng 1EiB(exbibyte)

Extents: Nó thay thế lược đồ ánh xạ khối được tìm thấy trong ext2 và ext3 để tăng hiệu suất và giảm phân mảnh

Delay allocation: Điều này cải thiện hiệu suất và giảm phân mảnh bằng cách phân bổ một lượng lớn dữ liệu một cách hiệu quả bằng cách trì hoãn việc phân bổ cho đến khi hệ thống đẩy dữ liệu vào đĩa.

Multiblock allocation: Nó phân bổ nhiều tập tin liên tục trên đĩa, từ đó giảm công việc gọi bộ phân bổ khối và tối ưu hóa phân bổ bộ nhớ

Increased file system checking (fsck) speed: Nó đánh dấu các nhóm khối và phần không được phân bổ và bỏ qua các phần đã được đánh dấu khi thực hiện kiểm tra. Do đó, nó hỗ trợ việc kiểm tra hệ thống tập tin nhanh hơn

Journal check summing: Nó sử dụng các checksum trong nhật ký để cải thiện độ tin cậy

Persistent pre-allocation: Hệ thống tập tin có thể phân bổ trước không gian trên đĩa cho một tập tin bằng cách ghi các giá trị zero vào nó trong quá trình tạo

Improved timestamps: Nó cung cấp dấu thời gian được đo bằng nanogió và có hỗ trợ cho dấu thời gian ngày tạo

Backwards compatibility: Hệ thống tập tin này tương thích ngược và cho phép người dùng gắn kết ext3 và ext2 như là ext4

**13. Các kiến thức thu thập, tạo bảo sao, phân tích bằng chứng số.**

Thu thập dữ liệu là việc sử dụng các phương pháp đã được thiết lập để trích xuất

Thông tin được lưu trữ điện tử (ESI) từ máy tính hoặc phương tiện lưu trữ bị nghi ngờ

để có được cái nhìn sâu sắc về tội phạm hoặc sự cố

• Đây là một trong những bước quan trọng nhất của điều tra số vì việc thu thập không

đúng cách có thể làm thay đổi dữ liệu trong chứng cứ điện tử và khiến nó không được

chấp nhận trước tòa án, pháp luật

• Các điều tra viên phải xác minh được tính chính xác của dữ liệu thu được. Quá trình

hoàn chỉnh phải được kiểm tra và tòa án chấp nhận

Có 2 loại phương pháp thu thập dữ liệu:

* **Thu thập dữ liệu động:** Liên quan đến việc thu thập thông tin khả biến nằm trong thanh ghi, cache và RAM
* **Thu thập dữ liệu tĩnh:** Thu thập dữ liệu không thay đổi ngay cả khi hệ thống đã tắt nguồn

**Thu thập dữ liệu động**

* Vì RAM và các dữ liệu khả biến khác là động, nên việc thu thập thông tin này sẽ diễn ra trong thời gian thực
* Bằng chứng quan trọng có thể bị mất hoặc bị phá huỷ nếu chỉ nhìn các chương trình đang chạy hoặc khởi động lại máy tính
* Trong quá trình thu thập dữ liệu động, tính toàn vẹn khó kiểm soát hơn vì các công cụ và lệnh có thể thay đổi thời gian truy cập tệp tin
* Dữ liệu động hỗ trợ và bằng chứng xác định thời gian của sự cố và những người dùng có liên quan
* Các loại dữ liệu động:
  + **Thông tin hệ thống**
    - Thu thập thông tin về cấu hình hiện tại và trạng thái chạy của máy tính nghi ngờ.
    - Thông tin hệ thống khả biến gồm hồ sơ hệ thống (chi tiết về cấu hình), ngày giờ hệ thống hiện tại, lịch sử lệnh, thời gian hoạt động của hệ thống hiện tại, các tiến trình đang chạy, file mở, file khởi động, dữ liệu tạm, người dùng đã đăng nhập, DLL hoặc thư viện được chia sẻ
  + **Thông tin mạng**
    - Thu thập thông tin về trạng thái mạng của máy tính nghi ngờ
    - Thông tin mạng dễ thay đổi bao gồm các kết nối và cổng đang mở, thông tin định tuyến và cấu hình, và bộ nhớ cache ARP.

**Thu thập dữ liệu tĩnh**

* Thu thập dữ liệu tĩnh được định nghĩa là thu thập dữ liệu không bị thay đổi khi hệ thống tắt hoặc tắt máy
* Loại dữ liệu này được gọi là bất biến và thường được phục hồi từ ổ cứng. Nó cũng có thể tồn tại trong vùng dung lượng trống, file swap và không gian ổ đĩa chưa kịp phân bổ
* Các nguồn dữ liệu bất biến khác bao gồm DVD-ROM, ổ USB, thẻ flash, điện thoại thông minh và ổ cứng ngoài
* Ví dụ về dữ liệu tĩnh: email, tài liệu văn bản, lịch sử web, bảng tính, phần mềm, file swap, dung lượng ổ đĩa chưa được phân bổ và các tệp đã bị xoá

**Tạo bản sao:**

❑ Không làm việc trên chứng cứ điện tử ban đầu. Làm việc trên bản sao của một ổ đĩa/tệp đáng ngờ để điều tra dữ liệu

❑ Tạo ra hai bản sao từ phương tiện gốc :

• Bản sao thứ nhất là bản sao đang làm việc được sử dụng để phân tích

• Bản sao thứ hai là thư viện/bản sao kiểm soát được lưu trữ cho mục đích tiết lộ hoặc trong trường hợp bản sao đang hoạt động hỏng

❑ Nếu thực hiện tạo ảnh đĩa, hãy sử dụng phương tiện sạch để sao chép vào các ổ đĩa mới được bọc gọn

❑ Sau khi sao chép phương tiện gốc được thực hiện, hãy xác minh tính toàn vẹn của các bản sao so với bản gốc

**Tại sao phải tạo một bản sao?**

Máy tính/phương tiện truyền thông là hiện trường vụ án và nó cần được bảo vệ để đảm bảo rằng bằng chứng không bị hư hỏng

• Nhân bản cho phép những điều sau:

Bảo tồn bằng chứng ban đầu

• Ngăn chặn việc vô tình thay đổi bằng chứng gốc trong quá trình kiểm tra

• Cho phép tái tạo bản sao nếu cần thiết

• Bằng chứng có thể được sao chép mà không bị giảm chất lượng từ bản sao này sang bản sao khác

**14. Một số các thuật ngữ như chain-of-custody, digital eviden.**

**Chain-of-custody:**

Chain-of-custody là một tài liệu pháp lý thể hiện quá trình di chuyển của bằng chứng khi nó được di chuyển từ vị trí bằng chứng ban đầu đến phòng thí nghiệm pháp y. Đây là một lộ trình cho thấy cách các nhân viên ứng cứu đầu tiên và điều tra viên thu thập, phân tích và bảo quản chứng cứ. Các nhân viên ứng cứu đầu tiên/điều tra viên cần trình bày tài liệu này. Điều này đảm bảo việc kiểm tra chính xác dữ liệu bằng chứng gốc, hình ảnh phương tiện nguồn, theo dõi nhật ký,...

Chain-of-custody quản lý việc thu thập, lưu trữ, kiểm tra và xử lý bằng chứng. Nó đảm bảo bảo vệ bằng chứng chống lại việc giả mạo hoặc thay thế bằng chứng.

Tài liệu chain-of-custody liệt kê tất cả những người tham gia vào việc thu thập và bảo quản bằng chứng, hành động của họ với một con dấu cho mỗi hoạt động.

Biểu mẫu chain-of-custody phải xác định các thông tin sau:

* Người thu thập mẫu
* Mô tả mẫu, loại và số lượng
* Dữ liệu và địa điểm lấy mẫu
* Bất kỳ người nào giữ mẫu

Việc nộp bằng chứng số yêu cầu một cách tiếp cận đa chiều. Theo quan điểm này, chain-of-custody mang ý nghĩa quan trọng. Nhân viên ứng cứu đầu tiên cần ghi lại từng bước thực hiện trong quá trình thu thập bằng chứng. Tài liệu cũng nên bao gồm các ghi chú chi tiết về các thủ tục được thực hiện trên bằng chứng. Điều quan trọng là nhân viên ứng cứu đầu tiên phải làm rõ nguồn gốc, ngày thu hồi, phương pháp thu hồi và bản chất của bằng chứng kỹ thuật số.

Những cá nhân sở hữu một bằng chứng phải xử lý nó theo cách để họ có thể chịu sự giám sát pháp lý trước bất kỳ cáo buộc giả mạo bằng chứng nào.

Tài liệu chain-of-custody chứa tất cả thông tin về bằng chứng đã thu được. Điều này bao gồm các thông tin sau:

* Số vụ án: Số vụ án là một số duy nhất được phân bổ bởi phòng thí nghiệm pháp y hoặc cơ quan điều tra cho các vụ án hình sự.
* Tên và chức danh của người nhận: Trường này chứa thông tin về cá nhân phát hành hoặc chuyển tiếp vật chứng cho nhân viên điều tra.
* Địa chỉ và số điện thoại: Trường này chứa địa chỉ và số điện thoại đầy đủ của những cá nhân đã xử lý bằng chứng điện tử.
* Vị trí của bằng chứng: Trường này chứa thông tin về vị trí vậy lý của bằng chứng trong quá trình trích xuất hoặc thu thập.
* Ngày/giờ của bằng chứng: Trường này chứa thông tin về ngày và giờ thu thập bằng chứng.
* Lý do và quy trình thu thập bằng chứng: Trường này chứa thông tin về lý do nhân viên ứng cứu đầu tiên đã thu thập vật chứng và quy trình họ đã theo để thu thập nó.
* Số vật chứng/số lượng/mô tả vật chứng: Trường này chứa thông tin đầy đủ về bằng chứng đã thu được, chẳng hạn như:
  + Tên của bằng chứng
  + Màu sắc
  + Tên công ty sản xuất
  + Thông tin đánh dấu
  + Thông tin bao bì

**Digital Evidence**

Bằng chứng số đề cập đến thông tin có giá trị pháp lý được lưu trữ trên hoặc truyền qua thiết bị điện tử. Các thiết bị kỹ thuật số được sử dụng trong các cuộc tấn công mạng có thể lưu trữ một số dữ liệu về phiên làm việc, chẳng hạn như người dùng đăng nhập, thời gian, loại kết nối và địa chỉ IP, những thông tin này có thể cung cấp bằng chứng để truy tố kẻ tấn công. Bằng chứng số bao gồm tất cả các thông tin như vậy được lưu trữ hoặc truyền dưới dạng kỹ thuật số và có giá trị pháp lý, do đó giúp các nhà điều tra tìm ra thủ phạm.

Bằng chứng số có thể được tìm thấy trên các thiết bị máy tính, máy chủ, bộ định tuyến… Nó được tiết lộ trong quá trình điều tra pháp y khi kiểm tra phương tiện lưu trữ kỹ thuật số, giám sát lưu lượng mạng hoặc tạo bản sao dữ liệu kỹ thuật số. Các nhà điều tra cẩn thận khi thu thập và trích xuất bằng chứng số vì bằng chứng này rất dễ bị hỏng. Điều này làm cho việc theo dõi các hoạt động tội phạm trở nên khó khăn đối với nhà điều tra pháp y.

Theo nguyên tắc trao đổi của Locard, “bất kỳ ai hoặc bất kỳ thứ gì khi bước vào hiện trường vụ án đều mang một thứ gì đó từ hiện trường và để lại một thứ gì đó của chính mình khi họ rời đi”. Ví dụ, nếu thông tin từ máy tính của nạn nhân được lưu trữ trên máy chủ hoặc hệ thống tại thời điểm xảy ra tội phạm, nhà điều tra có thể dễ dàng thu thập thông tin này bằng cách kiểm tra các tệp nhật ký, lịch sử duyệt web… Tương tự, nếu một cá nhân gửi một tin nhắn đe dọa qua dịch vụ email dựa trên Internet như Hotmail, Gmail hoặc Yahoo Mail, cả hệ thống của nạn nhân và hệ thống của người gửi đều có thể lưu trữ các tệp, liên kết và thông tin khác mà các nhà điều tra pháp y có thể trích xuất và phân tích.

Hầu hết các bằng chứng nằm trên các thiết bị mà kẻ tấn công sử dụng để kết nối với mạng hoặc các thiết bị máy tính của nạn nhân. Bằng chứng số có thể là bất kỳ loại tệp nào được lưu trữ trên thiết bị, bao gồm tệp văn bản, hình ảnh, tài liệu, tệp thực thi và dữ liệu ứng dụng. Dựa trên kiểu lưu trữ và thời gian tồn tại, bằng chứng số được chia thành hai loại: volatile data và non-volatile data.

* Volatile data: Dữ liệu bị mất ngay khi thiết bị tắt nguồn; ví dụ bao gồm thời gian hệ thống, người dùng đăng nhập, các tệp mở, thông tin mạng, thông tin tiến trình, bộ nhớ tiến trình, nội dung clipboard, lịch sử lệnh…
* Non-volatile data: Đây là dữ liệu cố định được lưu trữ trên các thiết bị lưu trữ thứ cấp như ổ cứng và thẻ nhớ. Dữ liệu không dễ mất khi thiết bị tắt ví dụ bao gồm các tệp ẩn, không gian trống, tệp hoán đổi, thiết lập registry và nhật lý sự kiện…

**Vai trò của bằng chứng số có thể hỗ trợ nhà điều tra trong việc truy tố hoặc bào chữa cho nghi phạm:**

* Ăn cắp danh tính
* Tấn công độc hại vào các hệ thống máy tính
* Rò rỉ thông tin
* Truyền thông tin trái phép
* Ăn cắp bí mật thương mại
* Sử dụng/lạm dụng Internet
* Sản xuất tài liệu và tài khoản giả
* Mã hoá trái phép/bảo vệ bằng mật khẩu các tài liệu
* Lạm dụng hệ thống
* Giao tiếp qua email giữa các nghi phạm/kẻ âm mưu

**15. Các nơi chứa nhật ký của các hệ điều hành Linux, Windows ( eventlog, security log…) Và hiểu về các định dạng nhật ký**.

Trong tất cả các phiên bản của Windows, ta có thể xem bản ghi log và các sự kiện sau:

* Bản ghi log ứng dụng : ghi lại nhiều sự kiện đăng nhập bởi các ứng dụng. Nhiều ứng dụng sẽ ghi lại lỗi của chúng ở đây trong bản ghi log ứng dụng. Điều này có thể hữu ích đặc biệt là nếu đăng nhập trên một máy chủ mà có cơ sở dữ liệu.
* Bản ghi log bảo mật : Điều quan trọng nhất có thể tìm thấy trong bản ghi log bảo mật là lần đăng nhập thành công và lỗi. Bản ghi này cũng ghi lại các sự kiện liên quan đến sử dụng tài nguyên, như tạo, mở, hoặc xóa các tập tin hoặc đối tượng khác. Các quản trị viên có thể xác định những sự kiện được ghi lại trong bản ghi log bảo mật. Một số hacker/cracker tắt bản ghi log bảo mật để hoạt động của chúng không được ghi lại.
* Bản ghi log Setup : chứa các sự kiện liên quan đến cài đặt ứng dụng. Nơi này sẽ hiển thị các ứng dụng mới được cài đặt trên máy. Rõ ràng, hầu hết các virus và phần mềm gián điệp sẽ không ghi tới bản ghi log ứng dụng. Tuy nhiên, bản ghi này có thể cho biết các ứng dụng mới đã được cài đặt mà có thể là một lỗ hổng bảo mật hoặc là trojan
* Bản ghi log hệ thống: Có chứa các sự kiện đăng nhập bởi các thành phần hệ thống Windows. Điều này bao gồm các sự kiện như lỗi driver.
* Bản ghi sự kiện chuyển tiếp: Được sử dụng để lưu trữ các sự kiện thu thập được từ máy tính từ xa. Nhật ký này rất quan trọng trong một môi trường mạng. Tuy nhiên, các hệ thống khác nhau phải được cấu hình để có được bản ghi này.
* Bản ghi các ứng dụng và dịch vụ: Là một loại bản ghi mới của bản ghi log sự kiện. Những sự kiện này lưu trữ các bản ghi từ một ứng dụng hoặc thành phần chứ không phải là sự kiện có tác động lên toàn hệ thống. Điều này có tiết lộ các vấn đề với một ứng dụng cụ thể hoặc thành phần Windows.

Hai bản ghi log quan trọng là bảo mật và đăng nhập hệ thống. Các hạng mục quan trọng nhất trong bản ghi log bảo mật là bản ghi của tất cả các đăng nhập hoặc đăng xuất dù là thành công hay không thành công. Đây là dấu hiệu đầu tiên của một nỗ lực xâm nhập vào máy chủ. Nếu thấy rất nhiều lần đăng nhập thất bại, hoặc nếu thấy thông tin đăng nhập tài khoản vào các giờ lẻ, mà có thể là một dấu hiệu cho thấy hoạt động bất hợp pháp đang diễn ra. Đây là một trong những điều đơn giản nhất để kiểm tra, vì vậy chắc chắn không nên bỏ qua phần này.

**Windows 10 lưu trữ event logs theo định dạng tệp EVTX và dựa trên ngôn ngữ XML.**

Các nơi chứa nhật ký của hệ điều hành Linux:

Hệ điều hành Linux cũng ghi lại nhật ký hoạt động.Tất cả các bản ghi log hệ thống điều hành có thể tìm được trong mục /var/log subdirectory. Có một số bản ghi log có thể tìm thấy trong thư mục này. Một vài trong số này không có mặt trong tất cả các bản của Linux, vậy cần tìm trong thư mục đó và xem các bản ghi log có mặt:

- /var/log/faillog: tập tin đăng nhập này có chứa thông tin đăng nhập người dùng không thành công. Điều này có thể rất quan trọng khi theo dõi cracker.

- /var/log/kern.log: tập tin đăng nhập này được sử dụng cho tất cả các tin nhắn từ nhân của hệ điều hành. Điều này không có khả năng thích hợp với hầu hết các máy tính của tội phạm.

- /var/log/lpr.log: đây là nhật ký log máy in có thể cung cấp một bản ghi bất kỳ được in ra từ máy này. Điều này có thể hữu ích cho doanh nghiệp cạnh tranh.

- /var/log/mail.\*: đây là nhật ký máy chủ email và có thể hữu ích trong việc điều tra tội phạm máy tính. Email có thể là một phần cần thiết của bất kỳ tội phạm máy tính nào .

- /var/log/mysql.\*: bản ghi log này liên quan đến hồ sơ máy chủ cơ sở dữ liệu MySql .

- /var/log/apache2/\*: nếu máy tính này đang chạy máy chủ web Apache, sau đó bản ghi log sẽ hiển thị các hoạt động liên quan. Điều này hữu ích khi theo dõi hacker.

- /var/log/lighttpd/\*: nếu máy này đang chạy máy chủ web Lighttpd, sau đó bản ghi log sẽ hiển thị các hoạt động liên quan. Điều này có thể hữu ích khi theo dõi hacker cố gắng hack máy chủ web.

- /var/log/apport.log: Đây là hồ sơ ứng dụng bị treo. Đôi khi, nó cho thấy sự hiện diện của virus hoặc phần mềm gián điệp.

- /var/log/user.log: Chứa bản ghi hoạt động của người dùng và có thể rất quan trọng với một cuộc điều tra hình sự

**Nhật ký trong Linux thường ở dạng văn bản thuần túy và có thể đọc bằng bất kỳ trình soạn thảo văn bản nào.**

**16. Phân tích sự khác nhau về điều tra số bộ nhớ Volatile và Non-Volatile trên Hệ điều hành Linux?**

Bộ nhớ volatile là loại bộ nhớ sẽ bị mất dữ liệu khi máy tính tắt nguồn.

Thông tin volatile bao gồm:

* Hostname, date&time, và múi giờ
* Thời gian hoạt động (uptime)
* Thông tin mạng
* Các cổng mở
* Các tập tin đang mở
* Thông tin hệ thống tập tin đã gắn kết
* Các module kernel đã tải
* User events
* Các tiến trình đang chạy
* Vùng swap và thông tin phân vùng đĩa
* Kernel message

Phương pháp điều tra:

* Thu thập dữ liệu bộ nhớ: Sử dụng các công cụ như LiME (Linux Memory Extractor) để trích xuất ảnh bộ nhớ trực tiếp từ RAM.
* Phân tích bộ nhớ: Sử dụng các công cụ như Volatility hoặc Rekall để phân tích ảnh bộ nhớ và trích xuất thông tin hữu ích như danh sách tiến trình, kết nối mạng, và các hoạt động hệ thống.
* Chụp ảnh bộ nhớ nhanh chóng: Thực hiện chụp ảnh bộ nhớ nhanh chóng trước khi hệ thống bị tắt hoặc thay đổi trạng thái để đảm bảo dữ liệu không bị mất.

Bộ nhớ non-volatile là loại bộ nhớ dữ liệu không thay đổi khi máy tính được tắt.

Trong quá trình điều tra pháp y, các nhà điều tra nên thu thập thông tin non-volatile như thông tin hệ thống, lịch sử đăng nhập của người dùng, nhật ký hệ thống và các tệp tin ẩn để xây dựng phân tích dòng thời gian của sự cố đã xảy ra.

Dữ liệu non-volatile bao gồm các mục sau:

- Thông tin hệ thống

- Thông tin kernel

- Tài khoản người dùng

- Người dùng hiện đang đăng nhập và lịch sử đăng nhập

- Nhật ký hệ thống

- Các tệp nhật ký của Linux

- Tệp lịch sử của người dùng

- Các tệp và thư mục ẩn

- Thông tin đáng ngờ

- Chữ ký tệp

- Thông tin tệp được lấy từ các lệnh `file` và `strings`

- Các tệp có thể ghi được lấy bằng lệnh `find`

Phương pháp điều tra:

* Sao chép và bảo toàn dữ liệu: Sử dụng các công cụ như dd hoặc dcfldd để tạo bản sao dữ liệu từ các thiết bị lưu trữ Non-Volatile.
* Phân tích hệ thống tệp: Sử dụng các công cụ như The Sleuth Kit hoặc Autopsy để phân tích cấu trúc hệ thống tệp và tìm kiếm các tệp tin bị xóa, nhật ký hệ thống, và các thông tin ẩn.
* Khôi phục dữ liệu: Sử dụng các công cụ khôi phục dữ liệu như TestDisk hoặc Photorec để khôi phục các tệp tin bị xóa hoặc bị hỏng.

**17. Sinh viên phân tích sự khác nhau về điều tra số bộ nhớ Volatile và Non-Volatile trên Hệ điều hành Windows?**

| **Tiêu chí** | **Bộ nhớ Volatile** | **Bộ nhớ Non-Volatile** |
| --- | --- | --- |
| **Khái niệm** | Mất dữ liệu khi tắt hệ thống | Không mất dữ liệu khi tắt hệ thống |
| **Mục tiêu điều tra** | Thông tin thời gian thực, dữ liệu tạm thời | Dữ liệu lâu dài, bằng chứng tĩnh |
| **Công cụ** | Volatility, FTK Imager, DumpIt, Process Explorer | FTK Imager, Autopsy, EnCase, Registry Editor |
| **Phương pháp** | Chụp ảnh bộ nhớ RAM, phân tích tiến trình và kết nối | Tạo ảnh ổ cứng, phân tích hệ thống tệp và nhật ký |
| **Thách thức** | Thời gian nhạy cảm, cần công cụ đặc biệt | Dung lượng lớn, dữ liệu ẩn |
| **Ví dụ thực tế** | Điều tra tiến trình, kết nối mạng hiện tại | Phân tích tệp tin, nhật ký hệ thống |

**18. Phương pháp tạo bản sao cho dữ liệu tĩnh trên hệ điều hành và ví dụ cụ thể?**

* Thu thập dữ liệu tĩnh được định nghĩa là thu thập dữ liệu không bị thay đổi khi hệ thống tắt hoặc tắt máy
* Loại dữ liệu này được gọi là bất biến và thường được phục hồi từ ổ cứng. Nó cũng có thể tồn tại trong vùng dung lượng trống, file swap và không gian ổ đĩa chưa kịp phân bổ
* Các nguồn dữ liệu bất biến khác bao gồm DVD-ROM, ổ USB, thẻ flash, điện thoại thông minh và ổ cứng ngoài
* Ví dụ về dữ liệu tĩnh: email, tài liệu văn bản, lịch sử web, bảng tin, phần mềm, file swap, dung lượng ổ đĩa chưa được phân bổ và các tệp đã bị xoá

**Phương pháp thu thập và sao chép dữ liệu:**

* Chuẩn bị tài liệu liên quan
* Phương tiện chống ghi đè
* Tìm kiếm phương tiện mục tiêu
* Xác định định dạng dữ liệu thu thập
* Xác định phương pháp thu thập tốt nhất
* Chọn công cụ thu thập dữ liệu
* Thu thập dữ liệu
* Lập kế hoạch dự phòng
* Xác nhận dữ liệu đã thu thập

**Tạo bản sao bằng dd trên Linux**

**Bước 1**: Kết nối ổ cứng cần sao chép vào máy tính thông qua cổng USB.

**Bước 2**: Mở terminal và xác định tên thiết bị của ổ cứng (ví dụ: /dev/sdX).

**Bước 3**: Sử dụng lệnh dd để tạo bản sao:

bash

Copy code

dd if=/dev/sdX of=/path/to/output.img bs=4M

**Bước 4**: Sau khi hoàn tất, sử dụng hàm băm để kiểm tra tính toàn vẹn của bản sao:

bash

Copy code

md5sum /dev/sdX

md5sum /path/to/output.img

**Tạo bản sao bằng FTK Imager**

**Bước 1**: Kết nối ổ cứng cần sao chép vào máy tính thông qua cổng USB.

**Bước 2**: Khởi động FTK Imager.

**Bước 3**: Chọn "File" -> "Create Disk Image".

**Bước 4**: Chọn "Physical Drive" và chọn ổ cứng cần sao chép.

**Bước 5**: Chọn định dạng (E01 hoặc raw) và vị trí lưu trữ bản sao.

**Bước 6**: Bắt đầu quá trình sao chép và theo dõi tiến trình.

**Bước 7**: Sau khi hoàn tất, sử dụng hàm băm để kiểm tra tính toàn vẹn của bản sao:

md5sum /dev/sdX

md5sum /path/to/output.img

**19. Sinh viên trình bày khi tiếp cận để điều tra một máy tính đang bật sử dụng hệ điều hành Linux thì sẽ cần thu thập dữ liệu động nào? Nêu ví dụ cụ thể và các công cụ cần sử dụng.**

Thu thập dữ liệu động bao gồm:

- Chạy lệnh netsat để trích xuất thông tin mạng. Nó hiển thị các kết nối mạng, bảng định tuyến và một số giao diện mạng (bộ điều khiển giao diện mạng hoặc giao mạng do phần mềm xác định) và thống kê giao thức mạng

- Chạy lệnh last -F để xem thời gian và ngày đăng nhập và đăng xuất đầy đủ của người dùng vào hệ thống.

- Chạy lệnh hostname để xem tên máy chủ hệ thống.

- Chạy lệnh ifconfig -a để xem cấu hình của tất cả các giao diện mạng trên hệ thống

- Chạy lệnh lsof để liệt kê tất cả các tệp đang mở và các tiến trình đang hoạt động đã mở chúng

- Chạy lệnh lsmod hiển thị các mô-đun đã tải

- Xclip là một giao diện dòng lênh cho X clipboard. Chạy xclip –o để xuất nội dung của khay nhớ tạm

- Chạy lệnh aureport để xem báo cáo tóm tắt nhật ký daemon kiểm tra

- Chạy lệnh id để xác định ID người dùng cho tên người dùng được chỉ định

- Sau đó, chạy lệnh ausearch để theo dõi tất cả các sự kiện người dùng liên quan đến ID người dùng đó

- Định dạng Thực thi và liên kết (ELF) là định dạng tệp thực thi chính

- Hệ thống lưu trữ các thư viện được chia sẻ, mô-đun kernel và kernel ở định dạng ELF

- Chạy lệnh readelf để phân tích tiêu đề và các phần của tệp ELF

- Xác minh nội dung của /var/spool/cron và /etc/cron.daily để thu thập thông tin về bất kỳ tác vụ lên lịch nào

- Nhận lịch sử lệnh từ tệp .bash\_history

- Thu thập dữ liệu trạng thái hiện tại của hệ thống Linux từ thư mục “/proc”

- Chạy lệnh ps để xem các tiến trình đang chạy trên hệ thống

- Nó cung cấp ảnh chụp nhanh các quy trình hiện tại cùng với thông tin chi tiết như id người dùng, mức sử dụng CPU, mức sử dụng bộ nhớ, tên lệnh…

- Kiểm tra cây tiến trình để xác định bất cứ quy trình con và phụ thuộc đáng ngờ không

- Các lệnh khác để thu thập thông tin hữu ích về hệ thống bị xâm nhập:

* Chạy lệnh cat/proc/version để biết phiên bản kernel Linux được sử dụng trong hệ điều hành
* Chạy lệnh cat/proc/kernel/domainname để biết tên miền
* Chạy lệnh cat/proc/swaps để xem tổng kích thước hoán đổi đã sử dụng
* Lệnh cat/proc/partitions phân vùng để xem danh sách các phân vùng đĩa
* Lệnh cat /proc/cpuinfo để xem chi tiết về CPU trên máy
* Chạy lệnh cat/proc/self/mounts để xem các điểm đến và các thiết bị bên ngoài được gắn kết
* Chạy lệnh cat/proc/uptime để đo thời gian làm việc của máy tính