Ôn tập Pháp chứng kỹ thuật số

1. Các loại tội phạm máy tính

Tội phạm máy tính là một tội phạm xâm phạm trật tự an toàn xã hội được thực hiện trong lĩnh vực công nghệ thông tin, có hành vị khách quan liên quan đến sử dụng máy tính và các tính năng của nó gây rối loạn hoạt động[21]. Tội phạm này đòi hỏi về kiến thức công nghệ máy tính chẳng hạn như phá hoại hoặc ăn cắp dữ liệu máy tính hay sử dụng máy tính để thực hiện một số tội phạm khác[1].

Tội phạm mạng - cyber crime, là những hành động phạm pháp trong đó máy tính hoặc mạng là công cụ, mục tiêu hoạc nơi diễn ra hành vi. Bao gồm các loại

- Đánh cắp định danh (identity), sỡ hữu trí tuệ

- Hacking

- Malware

- Theo dõi mạng

- Phising/spoofing

- Spam

- Tấn công từ chối dịch vụ

- Tổn hại tài sản nạn nhân

- Tống tiền

- Tian lận tài sản số

- Bắt nạt mạng

- Vi phạm bản quyền phần mềm

Đối tượng phạm tội - cyber criminals, bao gồm

- Liên kết tới các tập đoàn tội phạm có tổ chức nhằm tận dụng các kĩ thuật tinh vi

- Nhóm có tổ chức, hoạt động theo cơ chế phân cấp với mô hình chia sẻ doanh thu đã định trước, giống như một tập đoàn lớp cung cấp dịch vụ tội phạm

- Nhóm có tổ chức, tạo và thuê botnet, cung cấp nhiều dịch vụ như viết malware, hack tài khoản cá nhân, tấn công DoS theo yêu cầuCác bước chính của Forensics Investigations

2. Các bước chính trong điều tra pháp y, gồm 14 bước như sau

1. Xác định tội phạm máy tính
2. Thu thập chứng cứ sơ bộ
3. Xin lệnh thu giữ của tòa án (nếu cần)
4. Thực hiện các thủ tục phản ứng đầu tiên
5. Thu giữ bằng chứng tại hiện trường
6. Vận chuyển bằng chứng đến phòng thí nghiệm pháp y
7. Tạo 2 bản sao luồng bit của bằng chứng
8. Tạo MD5 checksum trên hình ảnh
9. Duy trì chuỗi hành trình
10. Lưu trữ bằng chứng gốc ở nơi an toàn
11. Phân tích bản sao hình ảnh cho bằng chứng
12. Chuẩn bị báo cáo pháp y
13. Gửi báo cáo cho client
14. Tham dự phiên tòa và làm nhân chứng chuyên gia (nếu cần)

3. Các role của investigator and digital element

Vai trò của điều tra viên pháp y:

1. Bảo vệ máy tính của nạn nhân khỏi thiệt hại và viruses
2. Xác định mức độ thiệt hại
3. Thu thập bằng chứng theo cách hợp pháp

4. Phân tích và bảo vệ dữ liệu bằng chứng được tìm thấy

5. Chuẩn bị báo cáo phân tích

6. Trình bày bằng chứng được chấp nhận trước tòa

Vai trò của yếu tố kĩ thuật số:

- Các bằng chứng số có thể hỗ trợ điều tra viên pháp y trong việc truy tố hoặc bào chữa nghi phạm

- Thực hiện hỗ trợ cho vài trò phân tích dữ liệu

- Thực hiện xác định trách nhiệm pháp lý và hình sự số

- Thực hiện hỗ trợ việc theo dõi và truy tìm tội phạm

- Thực hiện mã hoá và giám sát an ninh mạng nhằm thực hiện bảo vệ dữ liệu và ngăn chặn các hoạt động phạm tội

4. Các role của digital evidence

Digital forensics investigation methodology

Phương pháp điều tra pháp y kỹ thuật số:

1) Xin lệnh khám xét của tòa án để tiến hành điều tra (có thể khám xét toàn bộ công ty, một tầng, một phòng, một thiết bị, một ngôi nhà hoặc bất kì tài sản nào khác)

2) Đánh giá và bảo vệ hiện trường

Thu thập thông tin sơ bộ tại hiện trường như

- Ngày giờ

- Địa điểm xảy ra

- Bằng chứng từ hệ thống biến động và không biến động

- Thông tin chi tiết của (những) người có mặt tại hiện trường

- Tên và nhận của (những) người có thể làm nhân chứng

Với người phản ứng (responder) đầu tiên tại hiện trường

- Thu thập và bảo quản càng nhiều bằng chứng càng tốt

- Thu thập bằng chứng của tất cả các thiết bị có mặt tại hiện trường

- Tuân thủ luật khi thu thập và liên hệ sớm với giám định pháp y máy tính

Chụp ảnh pháp y: tất cả bằng chứng hoặc có liên quan tới bằng chứng và dán nhãn chúng

3) Thu thập bằng chứng

1. Bằng chứng vật lí

- Phương tiện di dộng, cáp, thiết bị máy tính, vật phẩm từ thùng rác

2. Bằng chứng điện tử

- Data files: các máy tính và dữ liệu bên trong

- Các bản sao lưu: toàn hệ thống, phục hồi sự cố (được lưu ở bên ngoài), cá nhân và đặc biệt khác (đĩa mềm hoặc phương tiện di động)

- Nguồn khác: băng, ổ đĩa thay thế/loại bỏ, đĩa mềm hoặc phương tiện di động

4) Bảo vệ bằng chứng

- Không tổn hại tới integrity

- Ở nơi an toàn

- Duy trì chain of custody

- Log lại thời điểm và người

- Hệ thống cảnh báo

5) Nhận dữ liệu

- Không phân tích trên bằng chứng gốc

- Tạo bản sao hình ảnh của dữ liệu bit by bit

- Xác minh tính toàn vẹn của bản sao: tính và so sánh mã hash MD5 của bằng chứng gốc với hình ảnh pháp chứng

5. Chain of custody: What? How?

Chain of custody (danh sách truy nguồn) là một khái niệm quan trọng trong lĩnh vực pháp chứng kỹ thuật số. Nó đề cập đến việc ghi lại và bảo vệ sự truy nguồn của các bằng chứng kỹ thuật số từ khi nó được tạo ra cho đến khi nó được sử dụng trong một vụ việc pháp lý.

Trong một vụ việc pháp lý, chain of custody là quá trình theo dõi và ghi lại lịch sử di chuyển và xử lý của các bằng chứng kỹ thuật số từ nguồn gốc của nó cho đến khi nó được trình diện trong phòng tòa. Mục đích của chain of custody là đảm bảo tính toàn vẹn và đáng tin cậy của bằng chứng kỹ thuật số và ngăn chặn bất kỳ sự thay đổi, mất mát hoặc nhiễu loạn nào có thể ảnh hưởng đến giá trị chứng cứ.

Quá trình chain of custody bao gồm việc đánh dấu, bảo vệ, ghi lại và kiểm soát các bằng chứng kỹ thuật số. Các bước quan trọng trong quá trình này bao gồm:

1) Thu thập: Các bằng chứng kỹ thuật số được thu thập từ nguồn gốc của chúng, chẳng hạn như máy tính, thiết bị lưu trữ hoặc hệ thống mạng.
2) Đánh dấu: Các bằng chứng kỹ thuật số được đánh dấu bằng các thông tin như thời gian, địa điểm và người thu thập. Điều này giúp xác định rõ ràng về nguồn gốc và lịch sử của chúng.
3) Bảo vệ: Các bằng chứng kỹ thuật số phải được bảo vệ khỏi sự thay đổi, mất mát hoặc tác động bên ngoài. Điều này có thể bao gồm việc sử dụng mã hóa, chữ ký số và các biện pháp bảo mật khác.
4) Ghi lại: Mọi hoạt động liên quan đến bằng chứng kỹ thuật số phải được ghi lại chi tiết. Điều này bao gồm thông tin về việc chuyển giao, vận chuyển, lưu trữ và truy cập.
5) Kiểm soát: Quá trình kiểm soát được áp dụng để đảm bảo rằng chỉ những người được ủy quyền mới có thể truy cập và xử lý các bằng chứng kỹ thuật số. Việc giới hạn quyền truy cập này giúp duy trì tính toàn vẹn của dữ liệu.

Quá trình chain of custody là quan trọng để đảm bảo tính hợp pháp và đáng tin cậy của bằng chứng kỹ thuật số trong hệ thống pháp lý. Nó cung cấp một hệ thống đáng tin cậy để xác định nguồn gốc và lịch sử của các bằng chứng kỹ thuật số, giúp bảo

vệ quyền lợi của các bên liên quan và đảm bảo rằng quy trình pháp lý được thực hiện một cách công bằng và minh bạch.

6. Steganography: định nghĩa, các loại, các công cụ, cấu trúc file -> hỏi file gì?

Steganography là một phương pháp ẩn tin trong pháp chứng kỹ thuật số, mà trong đó thông tin được che giấu trong một đối tượng không liên quan mà người khác không thể nhận biết được. Nó là một kỹ thuật phổ biến được sử dụng để ẩn dữ liệu hoặc tin nhắn bên trong các tập tin kỹ thuật số như hình ảnh, âm thanh hoặc video mà không gây nghi ngờ cho người khác.

Steganography hoạt động bằng cách thay đổi các bit thấp nhất của tập tin gốc để nhúng thông tin bên trong. Các bit thấp nhất thường không gây sự thay đổi đáng kể đối với tập tin gốc, do đó, việc ẩn thông tin trong các bit này không dễ bị phát hiện. Phương pháp này cho phép thông tin được truyền đi một cách ẩn danh và bảo mật, nhằm tránh việc thu thập dữ liệu bởi những người không được ủy quyền.

Tuy nhiên, steganography cũng có thể được sử dụng với mục đích xấu. Các cá nhân hoặc tổ chức có thể sử dụng steganography để che giấu thông tin bất hợp pháp hoặc độc hại trong các tập tin kỹ thuật số, chẳng hạn như virus, mã độc hoặc thông tin nhạy cảm. Do đó, steganography cũng đặt ra một thách thức cho lĩnh vực pháp chứng kỹ thuật số khi cần xác định và trích xuất thông tin ẩn trong các tập tin kỹ thuật số.

Các loại:

- Steganography hình ảnh: Thông tin được che giấu trong các tập tin hình ảnh. Phương pháp phổ biến bao gồm thay đổi các bit thấp nhất của các pixel hoặc sử dụng kỹ thuật mã hóa thông tin vào các vùng không đáng kể của hình ảnh.
- Steganography âm thanh: Thông tin được che giấu trong các tập tin âm thanh. Các phương pháp thường sử dụng là thay đổi các bit thấp nhất của mẫu âm thanh hoặc nhúng thông tin vào tần số không nghe được.
- Steganography video: Thông tin được che giấu trong các tập tin video. Các phương pháp thường sử dụng là thay đổi các khung hình hoặc khung thời gian của video để chứa thông tin ẩn.
- Steganography văn bản: Thông tin được che giấu trong các tập tin văn bản hoặc tài liệu. Các phương pháp bao gồm việc sử dụng các kỹ thuật mã hóa,

thay thế ký tự hoặc sử dụng các vùng không đáng kể của văn bản để chứa thông tin ẩn.

- Steganography mạng: Thông tin được che giấu trong dữ liệu truyền qua mạng. Các phương pháp này thường liên quan đến việc thay đổi các giao thức truyền dẫn hoặc thêm thông tin ẩn vào các gói tin.
- Steganography file: Thông tin được che giấu trong cấu trúc của tập tin. Các phương pháp này thường sử dụng việc thay đổi metadata hoặc sử dụng các vùng không đáng kể của tập tin để chứa thông tin ẩn.

Các công cụ:

Steghide (hình ảnh, âm thanh), stegosuite (hình ảnh, file mã hoá), OpenStego (hình ảnh, âm thanh, video), Steganography Toolkit (hình ảnh, âm thanh, video, văn bản), Stegdetect (detect thông tin ẩn), WireShark (mạng)

7. Quá trình điều tra cụ thê: memory forensic, email forensic (học lệnh!!!!)

Memory forensics

Quá trình điều tra memory forensics là quá trình thu thập, phân tích và phục hồi thông tin từ bộ nhớ của một hệ thống máy tính. Nó thường được thực hiện trong các tình huống điều tra vi phạm an ninh mạng hoặc tìm kiếm dấu vết của các hoạt động độc hại trên hệ thống.

Dưới đây là quá trình chung để thực hiện điều tra memory forensics:

1) Thu thập bộ nhớ: Quá trình bắt đầu bằng việc thu thập toàn bộ hoặc một phần của bộ nhớ từ hệ thống đang được điều tra. Có nhiều công cụ phổ biến được sử dụng để thực hiện việc này, chẳng hạn như Volatility Framework hoặc Rekall.
2) Phân tích bộ nhớ: Sau khi thu thập bộ nhớ, các chuyên gia điều tra sẽ phân tích dữ liệu thu được để tìm kiếm các thông tin quan trọng. Điều này có thể bao gồm việc tìm kiếm các quy trình đang chạy, tiến trình bị tắt, đối tượng đã được tải vào bộ nhớ, địa chỉ bộ nhớ quan trọng và thông tin khác có thể cung cấp dấu vết về hoạt động độc hại.
3) Khôi phục dữ liệu: Khi các thông tin quan trọng đã được xác định, quá trình khôi phục dữ liệu bắt đầu. Điều này có thể bao gồm việc khôi phục các tập

tin đã bị xóa, truy xuất các trình duyệt web hoặc email lịch sử, trích xuất các khóa mã hóa hoặc các thông tin xác thực khác.

4) Phân tích và tìm kiếm dấu vết: Khi dữ liệu đã được khôi phục, các chuyên gia sẽ tiến hành phân tích sâu hơn để tìm kiếm các dấu vết của các hoạt động độc hại hoặc vi phạm an ninh. Điều này có thể bao gồm việc xem xét lịch sử truy cập, tìm kiếm các mẫu mã độc hại, phân tích tệp tin, tìm kiếm tác vụ lịch trình và các hoạt động khác có thể cung cấp thông tin quan trọng.
5) Bảo tồn dữ liệu: Sau khi hoàn thành quá trình điều tra, việc bảo tồn dữ liệu rất quan trọng để đảm bảo tính toàn vẹn của chứng cứ. Dữ liệu thu thập và thông tin liên quan sẽ được sao lưu và bảo mật để đảm bảo không có sự thay đổi hoặc mất mát.

Quá trình điều tra memory forensics đòi hỏi kỹ năng chuyên môn và sử dụng các công cụ phân tích mạnh mẽ để phục hồi thông tin từ bộ nhớ. Nó có thể cung cấp cái nhìn sâu sắc về hoạt động của hệ thống và giúp điều tra viên tìm ra nguyên nhân và tác nhân gây ra sự vi phạm an ninh hoặc tấn công mạng.

Xem imageinfo -> Xem hàng loạt (hive, cmdscan, consoles) -> dump hash file -> xem netscan -> dump tiến trình -> Sử dụng các công cụ để xem (strings, gimp) -> xem clipboard -> xem file scan ->

Volatility –help:

Hivelist: xem file hive

Cmdscan: scan cmd

Consoles: xem thông tin console

Pstree: liệt kê các tiến trình

Pslist: danh sách tiến trình

Lsadump: dịch ngược hash

-f <tên file>

--profile <hệ điều hành>

memdump -p <id tiến trình> -D.

Một số cú pháp chú ý

./volatility_2.6_lin64_standalone -f find-me.bin --profile=Win7SP1x86 hivelist

./volatility_2.6_lin64_standalone -f find-me.bin --profile=Win7SP1x86 memdump -D ./ -p <id tiến trình>

./volatility_2.6_lin64_standalone -f find-me.bin --profile=Win7SP1x86 hashdump -y <virtual addr> -s <physical addr> > hash.txt

./volatility_2.6_lin64_standalone -f Kb05-dp-E81.vmem --profile=Win2008R2SP1x64 dumpfiles -Q 0x000000007d8813c0 -D .

Email forensics

Quá trình điều tra email forensics là quá trình thu thập, phân tích và phục hồi thông tin từ các hệ thống email để tìm kiếm dấu vết và thu thập chứng cứ trong một tình huống điều tra hoặc pháp lý. Nó được sử dụng để khám phá và xác định hoạt động gian lận, vi phạm an ninh hoặc bất kỳ hành vi đáng ngờ nào trong liên lạc qua email.

Dưới đây là quá trình chung để thực hiện điều tra email forensics:

1) Thu thập dữ liệu email: Quá trình bắt đầu bằng việc thu thập dữ liệu email từ các nguồn khác nhau, chẳng hạn như máy chủ email, các tệp tin sao lưu, thiết bị di động hoặc dịch vụ lưu trữ đám mây. Việc thu thập này có thể được thực hiện bằng cách truy cập trực tiếp vào hệ thống hoặc thông qua các công cụ hỗ trợ.
2) Phân tích dữ liệu email: Sau khi thu thập dữ liệu, các chuyên gia điều tra sẽ phân tích các thông tin email để tìm kiếm các tín hiệu và dấu vết quan trọng. Các hoạt động phân tích có thể bao gồm xác định danh tính và địa chỉ email của người gửi và người nhận, xem xét nội dung và đính kèm email, tìm kiếm từ khóa quan trọng, xác định thời gian và ngày gửi/nhận, xem xét các tiêu đề và thông tin nhận diện khác.
3) Phục hồi dữ liệu bị xóa: Trong một số trường hợp, điều tra viên có thể phải phục hồi dữ liệu email đã bị xóa hoặc bị ẩn. Điều này có thể được thực hiện bằng cách sử dụng công cụ phục hồi dữ liệu hoặc khôi phục từ các tệp tin sao lưu hoặc dữ liệu gốc.
4) Phân tích metadata: Metadata trong email cung cấp thông tin quan trọng về các yếu tố như ngày gửi, ngày nhận, địa chỉ IP, địa chỉ MAC và các thông tin

khác liên quan đến quá trình gửi và nhận email. Phân tích metadata có thể giúp xác định tính xác thực của email, đối tượng liên quan và quá trình truyền thông.

5) Phân tích đường dẫn mạng: Trong trường hợp email chứa các đường dẫn đến tài liệu, hình ảnh hoặc trang web, phân tích các URL và địa chỉ IP có thể cung cấp thông tin về các tài nguyên mạng liên quan và tương tác với email.
6) Bảo tồn dữ liệu: Khi quá trình điều tra hoàn tất, việc bảo tồn dữ liệu là rất quan trọng. Các dữ liệu đã thu thập và thông tin liên quan sẽ được sao lưu và bảo mật để đảm bảo tính toàn vẹn của chứng cứ.

Quá trình điều tra email forensics đòi hỏi kỹ năng chuyên môn và sử dụng các công cụ phân tích mạnh mẽ để phục hồi và phân tích dữ liệu email. Nó giúp điều tra viên tìm ra các thông tin quan trọng, xác định nguyên nhân và tìm kiếm chứng cứ trong các tình huống pháp lý hoặc điều tra.

8. **Propose: đề xuất vấn đề -> giải quyết (vấn đề thách thức, giải pháp hợp lý) (trình bày đồ án)**

Đồ án blockchain

Nguyên nhân: cần blockchain đảm bảo tính toàn vẹn, cross chain chuyển đổi dữ liệu, phân quyền và thu hồi quyền truy cập.

Quá trình chuyển đổi dữ liệu

1) Bệnh nhân request -> dapp -> private blockchain
2) Tạo smart contract
3) Yêu cầu data -> process oracle contract -> get audit proof -> send data -> respone smart contract
4) Kiểm tra
5) Thông báo

Quá trình tạo khoá thời hạn

1) Người dùng quyền thấp yêu cầu truy cập
2) Gửi yêu cầu đến người dùng quyền cao

3) Request và thực hiện lấy data
4) Tạo khoá có thời hạn
5) Gửi cho người dùng quyền truy cập cùng khoá thời hạn

Demo

3 máy: Ubuntu 22.04 16/8/8 ram 60gb HDD NAT 4 core CPU

Performance ở mức 62% store, 66% đăng ký, cấp/thu hồi quyền, 76% chuyển đổi data

Thời gian giao động ở mức 3 đến 5s còn lại 10s ở register và 20s ở chuyển đổi

Chi phí 4.45 đô đăng ký, lưu 9, cấp 15 đô, thu hồi 3 đô, chuyển đổi 22 đô

Đồ án EDR/Registry Spy

Nguyên nhân: nhiễm mal…

EDR Detect và Response về hệ thống từ endpoint, tool scan, malware (không phân tích được top10 OWASP)

Registry Spy: tạo hiren boot -> dump máy -> get file USER SOFTWARE SYSTEM định dạng .DAT để phân tích (phải dump máy)