

Chương 9
KỸ THUẬT VIẾT BÁO CÁO VÀ MỘT SỐ DẠNG
ĐIỀU TRA KHÁC

Nội dung chính

1. Khái niệm cơ bản
2. Chuẩn bị báo cáo
3. Khai báo sử dụng FTK&Encase
4. Điều tra thư điện tử
5. Điều tra tấn công web
6. Điều tra cơ sở dữ liệu
7. Điều tra tấn công mạng không dây

I. Báo cáo điều tra

Báo cáo điều tra

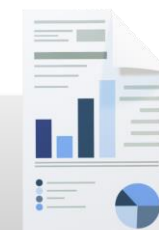
- ❑ Một báo cáo điều tra cung cấp thông tin chi tiết về **quá trình hoàn thành điều tra**



- ❑ Nó bao gồm **phạm vi điều tra, các công cụ** được sử dụng để thu thập và phân tích dữ liệu, **bằng chứng thu thập được, thông tin chi tiết về điều tra viên,...**



- ❑ Báo cáo **trình bày lời khai** về vụ xét xử với bằng chứng liên quan để hỗ trợ lập luận trong tố tụng hình sự và dân sự



Các khía cạnh quan trọng của một báo cáo điều tra tốt

- ☐ Xác định chính xác chi tiết vụ việc
- ☐ Truyền tải tất cả những thông tin cần thiết một cách ngắn gọn
- ☐ Phát âm chuẩn và nói sao cho dễ hiểu đối với người nghe
- ☐ Rõ ràng và không được nhầm lẫn
- ☐ Được cấu trúc một cách hợp lý giúp cho thông tin dễ dàng tìm kiếm
- ☐ Tạo ra kịp thời đúng thời điểm

- ☐ Có khả năng chịu sự điều tra của pháp luật
- ☐ Nội dung chứa kết quả có thể rút gọn hoàn toàn
- ☐ Giúp trả lời các câu hỏi được nêu ra tại phiên tòa xét xử
- ☐ Kết quả đưa ra hợp lệ, ý kiến, khuyến nghị được hỗ trợ bởi số liệu và thực tế
- ☐ Phải tuân thủ luật pháp địa phương để được chấp nhận tại tòa

Mẫu báo cáo điều tra

1. Tóm tắt	5. Thông tin bằng chứng
<ul style="list-style-type: none">Số hồ sơTên và số căn cước công dân của người viết, điều tra viên, và giám địnhMục đích điều traPhân tích chữ ký điện tử	<ul style="list-style-type: none">Vị trí của bằng chứngDanh sách các bằng chứng đã thu thậpCác công cụ liên quan đến việc thu thập bằng chứngBảo quản bằng chứng
2. Mục tiêu điều tra	
3. Thông tin chi tiết về vụ việc	6. Quy trình đánh giá và phân tích
<ul style="list-style-type: none">Ngày và thời gian sự cố được cho là xảy raNgày và thời gian vụ việc được báo cáo cho cơ quan điều traChi tiết về người và hoặc những người báo cáo sự cố	<ul style="list-style-type: none">Đánh giá ban đầu về bằng chứngKỹ thuật điều traPhân tích bằng chứng điện tử (Bảng các công cụ liên quan)
4. Quy trình điều tra	7. Những phát hiện có liên quan
<ul style="list-style-type: none">Ngày và thời gian cuộc điều tra đã được chỉ địnhCác điều tra viên được phân bổBản chất của yêu cầu và thông tin được cung cấp cho điều tra viên	8. Tập hỗ trợ
	<ul style="list-style-type: none">Tập đính kèm và phụ lụcĐường dẫn đầy đủ của các tập quan trọngĐánh giá và ý kiến của chuyên gia
	9. Các chi tiết hỗ trợ khác
	<ul style="list-style-type: none">Phương thức lý luận của kẻ tấn côngỨng dụng của người dùng và hoạt động trên mạngKhuyến nghị

Phân loại báo cáo

01. Báo cáo chính thức bằng lời nói



Báo cáo bằng lời nói được gửi tới hội đồng quản trị / Các nhà quản lý/Ban bồi thẩm

02. Báo cáo chưa chính thức bằng văn bản



Báo cáo không chính thức hoặc sơ bộ dưới dạng văn bản

03. Báo cáo chính thức bằng văn bản



Báo cáo bằng văn bản tuyên thệ ,ví dụ như bản khai có cam kết hoặc tờ khai

04. Báo cáo chưa chính thức bằng lời nói



Báo cáo bằng lời nói có cấu trúc ngắn hơn báo cáo chính thức và thường được nói tại văn phòng luật sư hoặc đồn cảnh sát



Hướng dẫn viết báo cáo

1

Ghi lại từng bước được thực hiện trong quá trình điều tra nhanh chóng, rõ ràng và ngắn gọn. Điều này giúp tiết kiệm thời gian và nâng cao độ chính xác.

2

Biết rõ mục đích thẩm vấn của bạn trước khi bắt đầu phân tích. Giúp cho bài báo cáo đạt kết quả tốt, đúng trọng tâm hơn.

3

Tổ chức báo cáo theo cách tăng dần độ phức tạp. Điều đó cho phép giám đốc điều hành cấp cao nắm bắt được bản chất của nó ngay khi đọc những trang đầu

4

Tạo và sử dụng mẫu báo cáo tiêu chuẩn với tất cả những yếu tố cần thiết để tiết kiệm thời gian

5

Sử dụng mã định danh duy nhất hoặc thẻ cho từng người, đồ vật và địa điểm được đề cập nhiều lần trong báo cáo của bạn. Điều này giúp tránh không rõ ràng hoặc nhầm lẫn

Hướng dẫn viết báo cáo (tiếp)

6

Viết báo cáo bạn nên cân nhắc xem xét về khả năng kỹ thuật và hiểu biết của bạn về người đọc. Ngoài ra nên cho người khác đọc lại báo cáo để biết báo cáo của bạn có dễ hiểu và đúng chính tả chưa

7

Sử dụng tệp đính kèm hoặc phụ lục để duy trì luồng báo cáo. Cung cấp thêm chi tiết về bất kỳ thuật ngữ hoặc trích dẫn trong báo cáo. Ngoài ra hãy thêm các tham chiếu đến các phụ lục trong báo cáo

8

Ghi lại hàm băm MD5 trong báo cáo cho tất cả các bằng chứng được khôi phục (trong đĩa cứng, USB,...) trong quá trình thu thập và xác minh hình ảnh. Điều này cho thấy bạn đang xử lý dữ liệu theo một cách thích hợp và nó có thể được chấp nhận trước tòa

9

Thêm vào siêu dữ liệu (vị trí tệp, kích thước tệp, dấu thời gian/ngày tháng, tác giả,...) cho mọi tệp trong báo cáo. Điều này giúp loại bỏ sự nhầm lẫn và tăng niềm tin của khách hàng

Hướng dẫn viết báo cáo (tiếp)

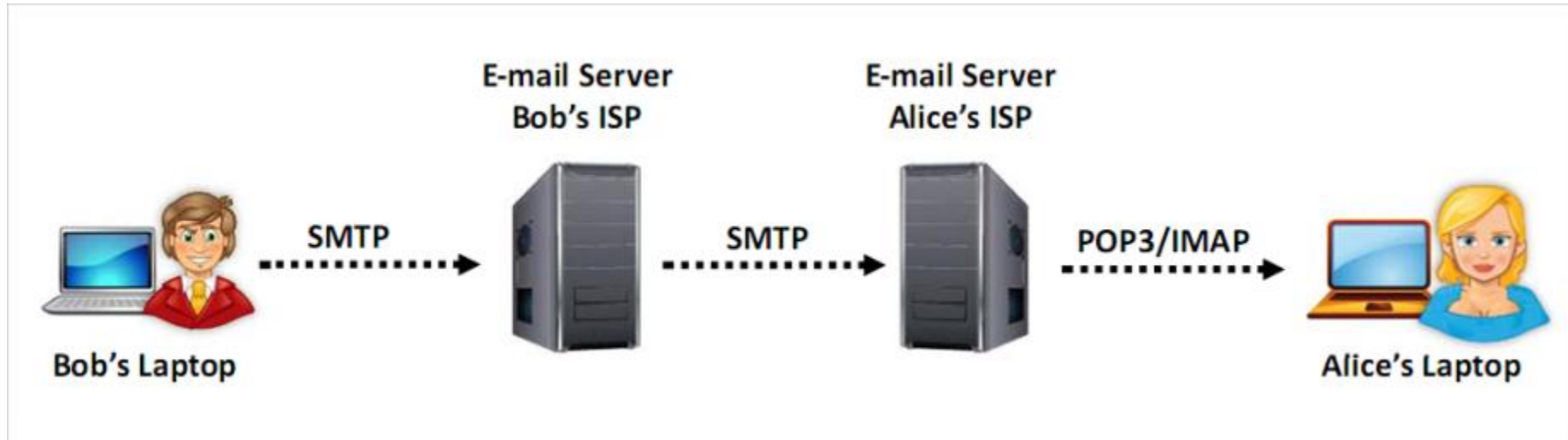
- ❑ Viết ý kiến dựa trên kiến thức và kinh nghiệm của bản thân
- ❑ Tạo một cấu trúc logic từ đầu đến cuối
- ❑ Duy trì phong chữ và khoảng cách nhất quán trong toàn bộ báo cáo
- ❑ Sử dụng dấu đầu dòng hoặc số thứ tự nếu có để làm thông tin dễ đọc hơn
- ❑ Cố gắng tránh những câu hỏi giả định
- ❑ Sử dụng các câu hỏi lý thuyết để hướng dẫn và hỗ trợ các ý kiến dựa trên bằng chứng thực tế
- ❑ Tránh sử dụng từ ngữ lặp lại và mơ hồ

- ❑ Nhóm các ý tưởng và câu liên quan thành đoạn văn sau đó chia thành các phần
- ❑ Không sử dụng từ lóng, ngôn ngữ chuyên môn
- ❑ Giải thích một cách chi tiết bất kỳ một từ viết tắt nào
- ❑ Sau khi hoàn thành báo cáo, hãy kiểm tra ngữ pháp, từ vựng, dấu câu và chính tả
- ❑ Viết báo cáo một cách súc tích sao cho dễ hiểu và gây hứng thú cho mọi đối tượng
- ❑ Tránh đề cập quá nhiều chi tiết và ý kiến cá nhân trong báo cáo

II. Điều tra thư điện tử

Cơ chế hoạt động của hệ thống thư điện tử

- Hệ thống thư điện tử bao gồm các máy chủ gửi và nhận thư trên mạng, cùng với phần mềm thư tại máy trạm cho phép người dùng xem và soạn thư.
- Hệ thống thư điện tử hoạt động dựa vào kiến trúc Client-Server
- Thư được gửi từ máy trạm tới máy chủ thư gần nhất, máy chủ thư nhận và xử lý thư và gửi tới người nhận thư



Tội phạm thư điện tử

- Thư điện tử trở thành phương tiện truyền thông phổ biến bởi vì nó dễ sử dụng và truyền tin nhanh. Cũng vì vậy mà nó trở thành công cụ hoạt động của tội phạm mạng.
- Tội phạm thư điện tử có thể chia theo 2 cách:

Phạm tội bằng cách gửi thư	Lợi dụng thư để thực hiện hành vi
Gửi thư hàng loạt (Spamming)	Giả mạo (Identity Fraud)
Gửi thư lừa đảo (Phishing)	Trao đổi thông tin qua thư
Mail bombing	Child pornography
Mail storms	Bắt cóc trẻ em

Các bước điều tra trên thư điện tử

- Hệ thống thư tín và ứng dụng chat cho phép tội phạm lợi dụng để thực hiện các hành vi phạm pháp. Do vậy có thể là đầu mối để điều tra và là các bằng chứng quan trọng.

Các bước điều tra tội phạm thư tín:

1. Lệnh khám xét
2. Kiểm tra thư
3. Tạo bản sao và in thư ra giấy
4. Xem phần header của thư
5. Phân tích header của thư
6. Truy dấu vết thư
7. Lấy thư có liên quan từ hòm thư
8. Kiểm tra nhật ký thư



Lệnh khám xét và tịch thu bằng chứng

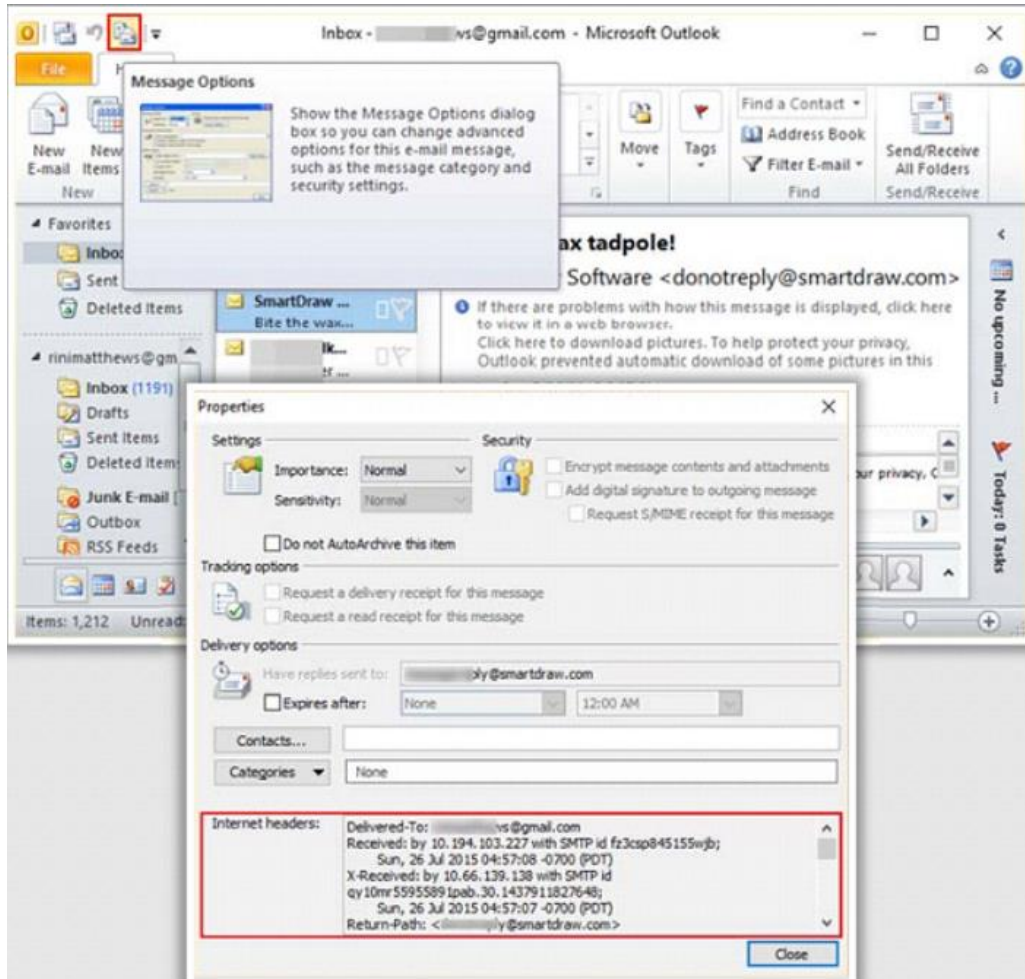
- Lệnh khám xét nên bao gồm ngôn ngữ thích hợp để thực hiện kiểm tra trên máy tính nghi ngờ và máy chủ thư đã sử dụng trong quá trình điều tra.
- Tịch thu tất cả máy tính và tài khoản thư nghi ngờ liên quan tới tội phạm
- Tịch thu tài khoản thư với mật khẩu đã biết (có thể hỏi người bị tình nghi hoặc lấy từ máy chủ thư)

Copy và Print thư điện tử

- Điều tra thư có thể được bắt đầu với thư đã được sao chép và từ bản in
- Một số ứng dụng thư cho phép Điều tra viên tạo bản sao của thư tới ổ cứng di động
- Các bước tạo bản sao thư với ứng dụng Microsoft Outlook:
 1. Cắm USB vào máy tính
 2. Mở USB từ máy tính
 3. Mở Microsoft Outlook
 4. Mở hòm thư
 5. Lựa chọn thư cần sao chép và mở thư
 6. Thay đổi kích thước cửa sổ ứng dụng Outlook sao cho nhìn được cả thư mục USB
 7. Kéo thả thư từ Outlook tới USB
 8. In thư từ ứng dụng
 9. Trong báo cáo có thể bao gồm cả thư đã được in

Xem phần header của thư

- Header của thư điện tử chứa thông tin quan trọng trong quá trình điều tra bởi ví nó chứa thông tin chi tiết thư gốc. Vì vậy điều tra viên cần chụp ảnh phần header của thư
- Sau khi tạo bản sao thư điện tử thì đã bao gồm phần header thư.



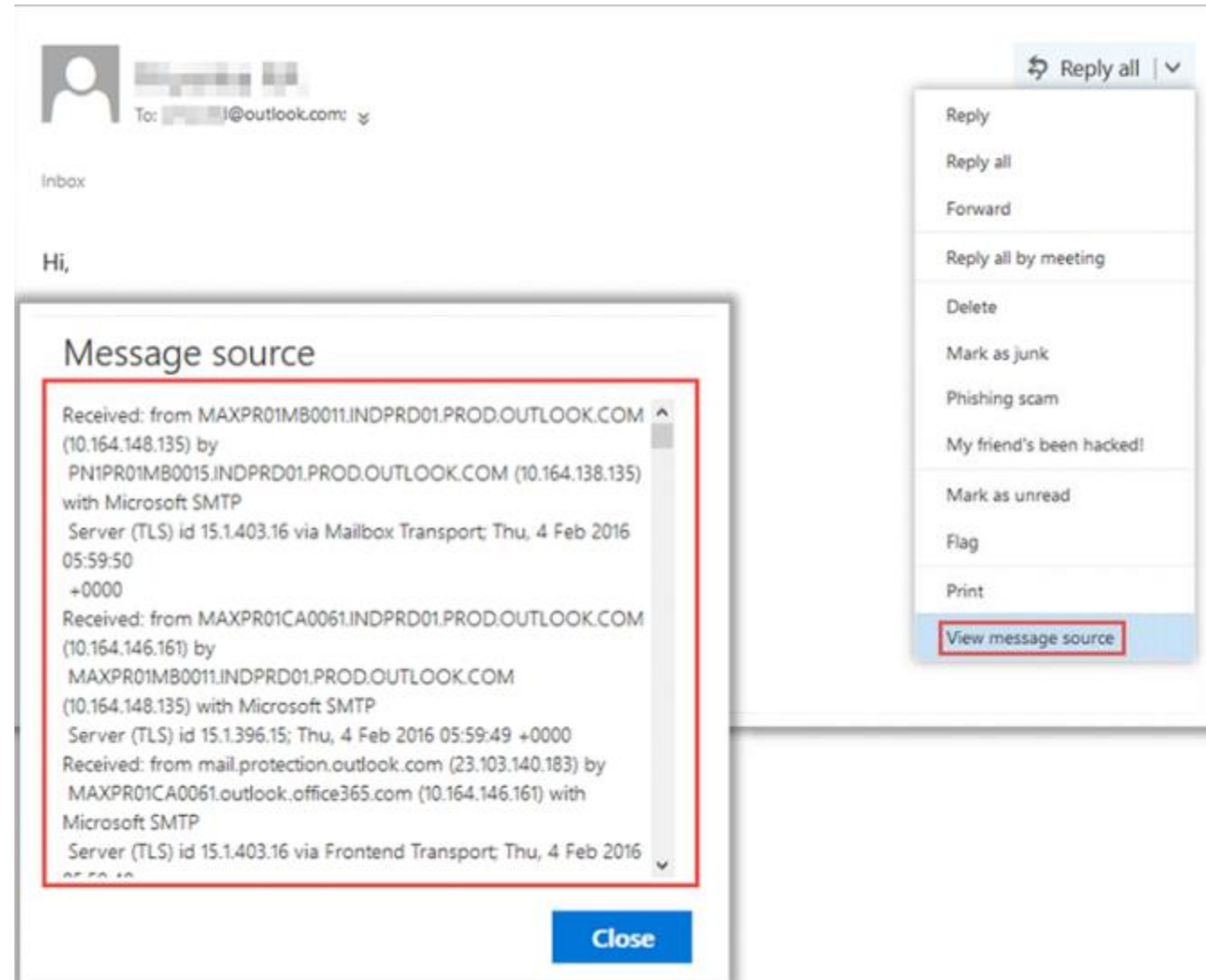
Các bước thu thập header với **Microsoft Outlook 2010**:

- Chạy chương trình **Outlook** và mở thư từ bản sao
- Kích vào phần **Message Options**
- Trong cửa sổ thuộc tính, lựa chọn phần **header**: sao chép phần thông tin của **header** và lưu vào chương trình soạn thảo bất kỳ để lưu trữ.

Xem phần header của thư

Các bước thu thập header với **Microsoft Outlook.com**:

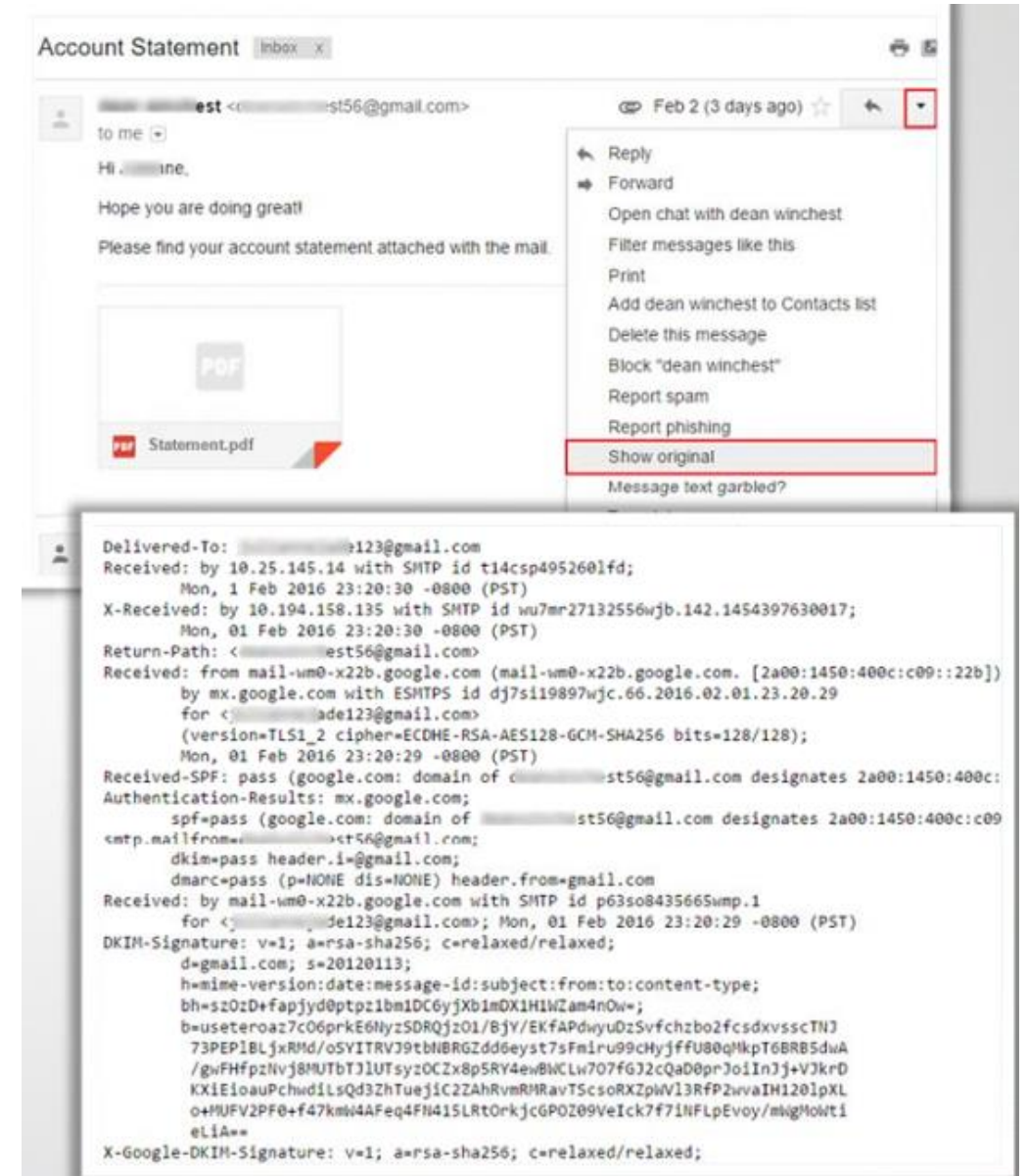
- Đăng nhập vào Microsoft Outlook.com và truy cập tới thư muốn lấy header
- Kích vào phần **View Message source**
- Lựa chọn phần **header**: sao chép phần thông tin của **header** và lưu vào chương trình soạn thảo bất kỳ để lưu trữ.



Xem phần header của thư

Các bước thu thập header với **Google mail**:

- Đăng nhập vào Gmail và truy cập tới thư muốn lấy header
- Kích vào phần **Show original**
- Lựa chọn phần **header**: sao chép phần thông tin của **header** và lưu vào chương trình soạn thảo bất kỳ để lưu trữ.



Received Headers

01

- Received cho biết nhật ký chi tiết về lịch sử của một thư điện tử
- Những header này giúp rút ra kết luận về nguồn gốc của thư.
- Nó cũng cung cấp thông tin thư có bị giả mạo hay không

02

- Ví dụ:

Một máy với tên miền xsecurity.com, có địa chỉ IP là 104.128.23.115 đã gửi thư tới mail.target.com, nhưng giả mạo HELO example.org, kết quả "Received" có thể bắt đầu như sau:

```
Received: from example.org  
([104.128.23.115]) by mail.target.com  
(8.8.5)...
```



Phân tích header của thư

Thu thập các bằng chứng chứa thông tin như bảng dưới đây, từ các email header và theo dõi nghi phạm:

Đường dẫn trả về (Return path)	Địa chỉ IP của máy chủ gửi thư
Địa chỉ người nhận	Số định danh duy nhất của thư
Tên máy chủ thư	Thời gian nhận thư
Loại máy chủ gửi thư đi	Thông tin tệp tin đính kèm

Phân tích header của thư

Xét ví dụ: Rudy gửi thư tới Timmy

From: rudy@bieberdorf.edu (Rudy)

To: timmy@immense-isp.com

Date: Tue, Jan 26 2016 14:36:14 PST

X-Mailer: Loris v2.32

Subject: Lunch today?

Received: from mail.bieberdorf.edu
(mail.bieberdorf.edu [124.211.3.78]) by
mailhost.immense-isp.com (8.8.5/8.7.2)
with ESMTP id LAA20869 for
<timmy@immense-isp.com>; Tue, Jan
26 2016 14:39:24 -0800 (PST)

Received: from alpha.bieberdorf.edu
(alpha.bieberdorf.edu
[124.211.3.11]) by

mail.bieberdorf.edu (8.8.5) id
004A21; Tue, Jan 26 2016 14:36:17 -
0800 (PST)

From: rudy@bieberdorf.edu (R.T.
Hood)

To: timmy@immense-isp.com

Date: Tue, Jan 26 2016 14:36:14 PST

Message-Id: <rth031897143614-
00000298@mail.bieberdorf.edu>

X-Mailer: Loris v2.32

Subject: Lunch today?

Kiểm tra tệp tin đính kèm

- Lưu trữ thư phụ thuộc vào trạng thái của máy trạm và máy chủ
- Một số chương trình thư điện tử cho phép người dùng lưu trữ thư trên máy chủ, một số lưu trữ trên máy tính



Kiểm tra tính hợp lệ của thư

- Công cụ Dossier là một phần của CentralOps.net cung cấp các tính năng mạng trực tuyến
- Nó là một công cụ dò quét giúp Điều tra viên xác nhận tình trạng của địa chỉ thư
- Nó cung cấp thông tin về địa chỉ thư, bao gồm cả bản ghi MX
- Công cụ này khởi tạo một phiên SMTP, để kiểm tra sự hợp lệ của thư, nhưng nó không gửi thư

Email Dossier Investigate email addresses

email address

user: anonymous [183.82.41.51]
balance: 49 units
[log in](#) | [account info](#) **CentralOps.net**

Validating ...

Validation results

confidence rating: **3 - SMTP**
The email address passed this level of validation without an error. However, it is not guaranteed to be a good address. [more info](#)

canonical address: <>

MX records

preference	exchange	IP address (if included)
5	gmail-smtp-in.l.google.com	[108.177.9.27]
10	alt1.gmail-smtp-in.l.google.com	[64.233.185.26]
20	alt2.gmail-smtp-in.l.google.com	[173.194.205.27]
30	alt3.gmail-smtp-in.l.google.com	[74.125.141.26]
40	alt4.gmail-smtp-in.l.google.com	[64.233.186.26]

SMTP session

```
[Contacting gmail-smtp-in.l.google.com [108.177.9.27]...]
[Connected]
```


Kiểm tra nguồn gốc địa chỉ IP của thư

Các bước sau đây có liên quan tới kiểm tra địa chỉ IP gốc của thư điện tử:

- Thu thập địa chỉ IP của người gửi từ mail header từ người nhận
- Tìm kiếm thông tin về địa chỉ IP từ cơ sở dữ liệu trong WHOIS
- Tìm kiếm vị trí địa lý của người gửi từ cơ sở dữ liệu trong WHOIS

Smart Whois lookup completed successfully.	
Smart Whois: formatted	
NetRange	66.220.144.0 - 66.220.159.255
CIDR	66.220.144.0/20
NetName	TFBNET3
NetHandle	NET-66-220-144-0-1
Parent	NET66 (NET-66-0-0-0-0)
NetType	Direct Assignment
OriginAS	AS32934
Organization	Facebook, Inc. (THEFA-3)
RegDate	2009-02-13
Updated	2012-02-24
Ref	http://whois.arin.net/rest/net/NET-66-220-144-0-1
OrgName	Facebook, Inc.
OrgId	THEFA-3
Address	1601 Willow Rd.
City	Menlo Park
StateProv	CA
PostalCode	94025
Country	US
RegDate	2004-08-11
Updated	2012-04-17
Ref	http://whois.arin.net/rest/org/THEFA-3
OrgAbuseHandle	OPERA82-ARIN
OrgAbuseName	Operations
OrgAbusePhone	+1-650-543-4800
OrgAbuseEmail	domain@facebook.com
OrgAbuseRef	http://whois.arin.net/rest/poc/OPERA82-ARIN
OrgTechHandle	OPERA82-ARIN
OrgTechName	Operations
OrgTechPhone	+1-650-543-4800
OrgTechEmail	domain@facebook.com
OrgTechRef	http://whois.arin.net/rest/poc/OPERA82-ARIN
RNOCHandle	OPERA82-ARIN
RNOCHandle	Operations
RNOCHandle	+1-650-543-4800
RNOCHandle	domain@facebook.com
RNOCHandle	http://whois.arin.net/rest/poc/OPERA82-ARIN
RTechHandle	OPERA82-ARIN
RTechName	Operations
RTechPhone	+1-650-543-4800
RTechEmail	domain@facebook.com
RTechRef	http://whois.arin.net/rest/poc/OPERA82-ARIN
RABuseHandle	OPERA82-ARIN
RABuseName	Operations
RABusePhone	+1-650-543-4800
RABuseEmail	domain@facebook.com
RABuseRef	http://whois.arin.net/rest/poc/OPERA82-ARIN

Điều tra thư trên ứng dụng web

1. Thư điện tử dựa trên nền web (Gmail, Yahoo, AOL...) thường khó khăn trong việc điều tra người gửi
2. Người dùng có thể đọc và gửi thư dựa trên web ở nhiều máy tính khác nhau
3. Tài khoản miễn phí, không xác thực thông tin trong quá trình mở dịch vụ thư
4. Tội phạm lợi dụng thuận lợi này để tạo ra các địa chỉ thư giả mạo
5. Trong trường hợp tài khoản sử dụng web mail để gửi thư, Điều tra viên có thể liên hệ với nhà cung cấp dịch vụ thư để tìm kiếm địa chỉ IP của người dùng đã sử dụng web mail.
6. Sau khi xác thực địa chỉ IP, Điều tra viên có thể thu thập thông tin người gửi



Xác định nơi lưu trữ thư

- Lưu trữ thư là một cách để đảm bảo an toàn
- Lý do lưu trữ thư: Sự tuân thủ chính sách, hỗ trợ điều tra, lưu trữ, quản lý

Lưu trữ cục bộ

- 👉 Mỗi ứng dụng khác nhau có định dạng lưu trữ khác nhau:

Ex: Microsoft Outlook (Index + Messages: *.pst), FoxMail (Index + Messages: *.box), etc.


Máy chủ lưu trữ

- 👉 Mỗi ứng dụng khác nhau có lưu trữ hỗn hợp cho tất cả các máy khách tồn tại trên máy chủ

Ex: MS Exchange (.STM, .EDB), IBM Notes (.NSF, .ID), GroupWise (.DB), etc.

Điều tra nhật ký thư

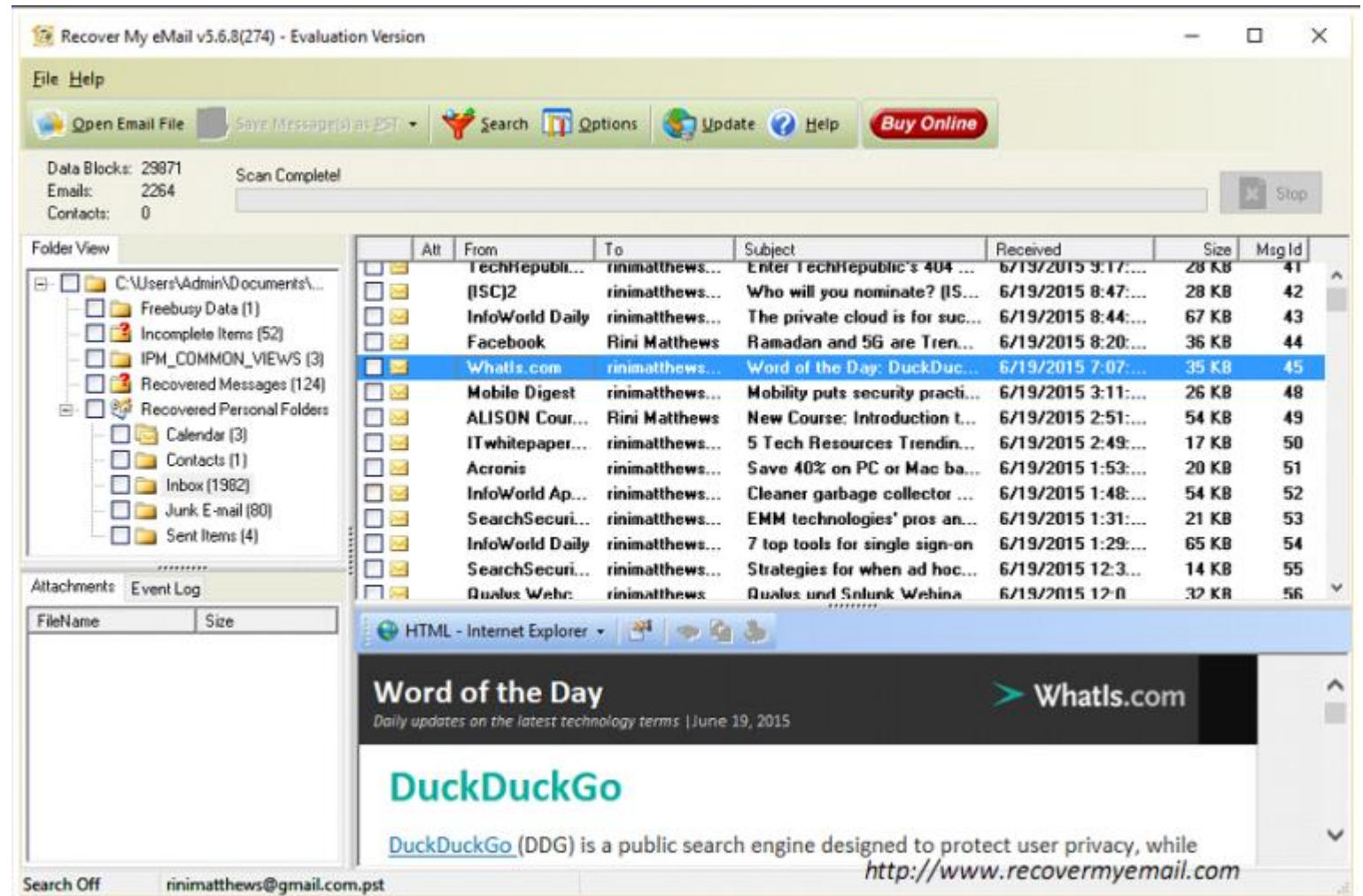
- Trong điều tra thư tín điện tử, một điều quan trọng là phải xác minh địa chỉ thư, nguồn, đường dẫn, liên quan tới thư nghi ngờ.
- Kiểm tra nhật ký là điều quan trọng để tìm ra thủ phạm nếu mail header có sự giả mạo sau sự cố

Kiểm tra Logs hệ thống	Kiểm tra Logs thiết bị mạng
<p>Kiểm tra Logs hệ thống, điều tra viên có thể xác định đường dẫn thư đã thực hiện</p> 	<ul style="list-style-type: none">• Kiểm tra Logs của Router và Firewall, giúp điều tra viên xác định thời gian và địa chỉ IP liên quan tới thư• Những Logs này cung cấp thông tin về định danh thông điệp thư, địa chỉ nguồn, đích của máy chủ sử dụng gửi thư.

Công cụ sử dụng trong điều tra

Recovery My Email

- Recovery My Email là một phần mềm khôi phục thư đã bị xóa từ các tệp Microsoft Outlook PST, Microsoft Outlook Express DBX



Công cụ sử dụng trong điều tra



Stellar Phoenix Deleted Email Recovery

<http://www.stellarinfo.com>



Wise Data Recovery

<http://www.wisecleaner.com>



Forensic Toolkit (FTK)

<http://accessdata.com>



EaseUS Email Recovery Wizard

<http://www.easeus.com>



Paraben's Email Examiner

<https://www.paraben.com>



DiskInternals Mail Recovery

<http://www.diskinternals.com>



Kernel for PST Recovery

<http://www.pstrecoverytools.com>



Aid4Mail Email Forensic software

<http://www.aid4mail.com>



MxToolBox Email Header Analyzer

<http://mxtoolbox.com>



Paraben's Network E-mail Examiner

<https://www.paraben.com>

III. Điều tra tấn công web

Giới thiệu về ứng dụng web

1

Ứng dụng web **cung cấp giao diện giữa người dùng và máy chủ web** thông qua một tập hợp các trang web được tạo ở cuối máy chủ hoặc chứa mã tập lệnh, được trình duyệt web của người dùng.

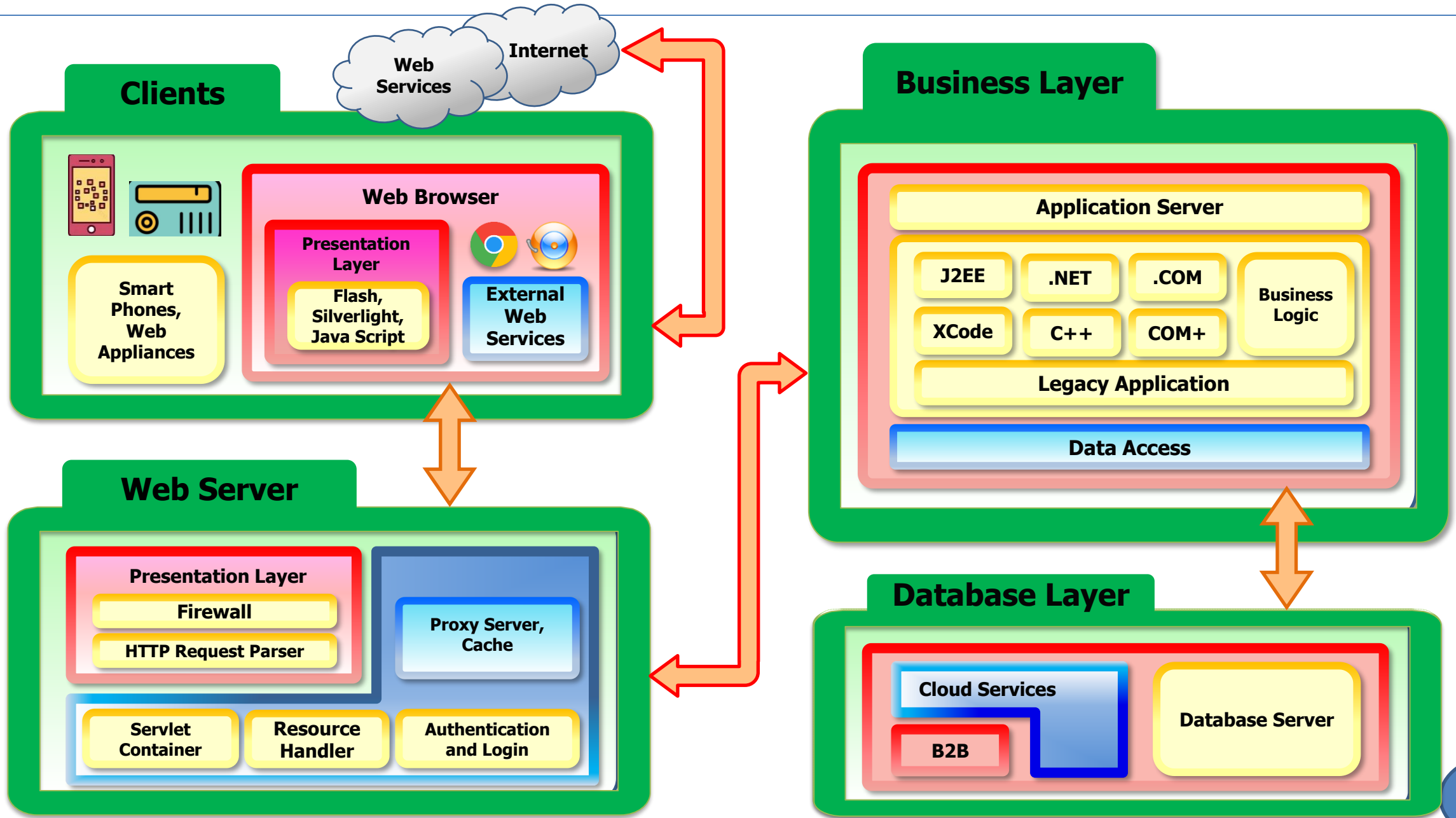


2

Điều tra ứng dụng web liên quan đến việc **thu thập và phân tích nhật ký** và các chứng cứ khác dọc theo đường dẫn hoàn chỉnh theo yêu cầu web. Nó bao gồm máy chủ web, máy chủ ứng dụng, máy chủ cơ sở dữ liệu, các sự kiện hệ thống, v.v., để xác định nguyên nhân, bản chất và thủ phạm khai thác ứng dụng web.



Kiến trúc ứng dụng web



Thách thức trong điều tra web

01

Các ứng dụng web thường được **phân phối tự nhiên**

02

Dấu vết của các hoạt động được **ghi lại trên một số** của phần cứng và phần mềm của cơ sở hạ tầng

03

Rất hạn chế hoặc không có nhiều phép thời gian để điều tra

04

Khối lượng nhật ký khổng lồ từ các nguồn khác nhau được phân tích và tương quan

05

Cơ sở dữ liệu lớn được phân tích

06

Yêu cầu kiến thức đầy đủ về các máy chủ web, máy chủ ứng dụng, cơ sở dữ liệu và các ứng dụng cơ bản khác nhau

07

Khó truy tìm trong trường hợp proxy ngược và trình ẩn danh

Dấu hiệu của các cuộc tấn công web

➤ Khách hàng không thể truy cập dịch vụ

➤ Các hoạt động đáng ngờ trong tài khoản người dùng

➤ Rò rỉ dữ liệu nhạy cảm

➤ URL chính xác chuyển hướng đến các trang web không an toàn

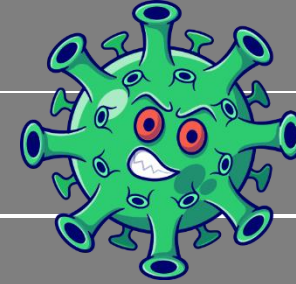
➤ Trang web không lành mạnh

➤ Hiệu suất mạng chậm bất thường

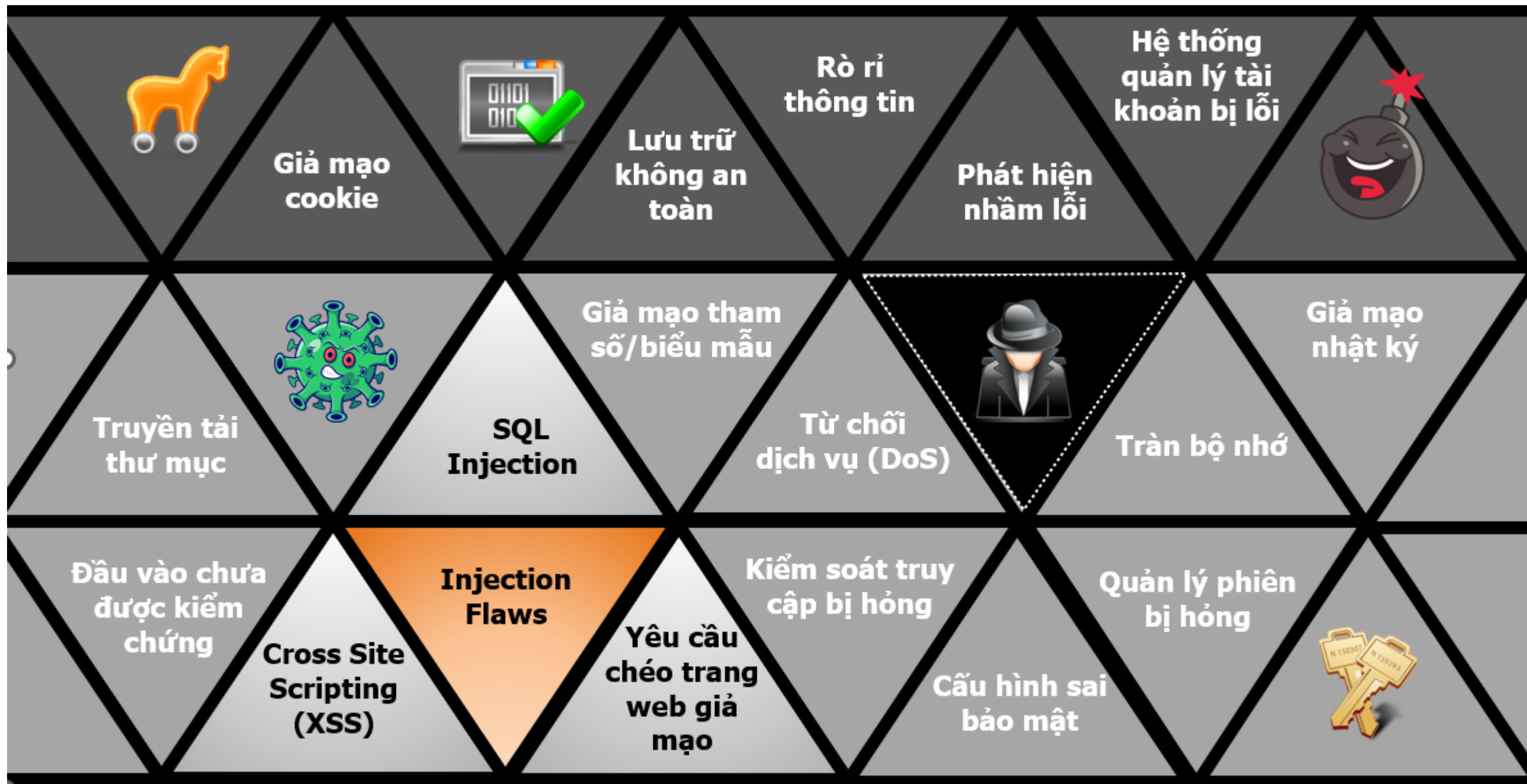
➤ Thường xuyên khởi động lại máy chủ

➤ Sự bất thường trong tệp nhật ký

➤ Các thông báo lỗi như lỗi 500, "lỗi máy chủ nội bộ" và "sự cố khi xử lý yêu cầu của bạn"



Các hiểm họa với ứng dụng web (1)



Các hiểm họa với ứng dụng web (2)



Điều tra trên máy chủ web Windows

Điều tra các cuộc tấn công web trong máy chủ Windows



Chạy **Event Viewer** để xem nhật ký:

C: \> eventvwr.msc



Kiểm tra xem các **sự kiện đáng ngờ** sau đã xảy ra chưa:

- Dịch vụ nhật ký sự kiện đã kết thúc
- Windows File Protection không hoạt động trên hệ thống
- Dịch vụ MS Telnet đang chạy



Tìm xem hệ thống có **đăng nhập không thành công** hoặc **tài khoản bị khóa**

Điều tra các cuộc tấn công web trong máy chủ Windows(Tiếp)



- Xem lại các lượt chia sẻ tệp để đảm bảo mục đích của chúng

C:\> net view <IP Address>



- Xác minh người dùng bằng các phiên mở

C:\> net session



- Kiểm tra xem các phiên đã được mở bằng các hệ thống khác chưa

C:\> net use



- Phân tích tại NetBIOS qua hoạt động TCP/IP

C:\> netstat -S



- Tìm xem các cổng TCP và UDP có lắng nghe bất thường không

C:\> netstat -na

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19044.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>net session

Computer            User name            Client Type          Open Idle time
-----
\\[::1]              Admin                0 00:12:30
\\[fe80:7462:70a6:8...Admin  0 00:12:30
The command completed successfully.

C:\Windows\system32>
```

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19044.1949]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>netstat -na

Active Connections

Proto Local Address           Foreign Address         State
TCP 0.0.0.0:135              0.0.0.0:0               LISTENING
TCP 0.0.0.0:445              0.0.0.0:0               LISTENING
TCP 0.0.0.0:902              0.0.0.0:0               LISTENING
TCP 0.0.0.0:912              0.0.0.0:0               LISTENING
TCP 0.0.0.0:5040             0.0.0.0:0               LISTENING
TCP 0.0.0.0:5357             0.0.0.0:0               LISTENING
TCP 0.0.0.0:7680             0.0.0.0:0               LISTENING
TCP 0.0.0.0:49664            0.0.0.0:0               LISTENING
TCP 0.0.0.0:49665            0.0.0.0:0               LISTENING
TCP 0.0.0.0:49666            0.0.0.0:0               LISTENING
TCP 0.0.0.0:49667            0.0.0.0:0               LISTENING
TCP 0.0.0.0:49668            0.0.0.0:0               LISTENING
TCP 0.0.0.0:49670            0.0.0.0:0               LISTENING
TCP 127.0.0.1:8884           0.0.0.0:0               LISTENING
TCP 127.0.0.1:49671          0.0.0.0:0               LISTENING
TCP 192.168.18.1:139         0.0.0.0:0               LISTENING
TCP 192.168.20.161:139       0.0.0.0:0               LISTENING
TCP 192.168.20.161:52448     23.98.104.196:8883      ESTABLISHED
TCP 192.168.20.161:52449     20.198.119.84:443       ESTABLISHED
TCP 192.168.20.161:52451     31.13.75.1:443          ESTABLISHED
TCP 192.168.20.161:52452     31.13.75.17:443         ESTABLISHED
TCP 192.168.20.161:52457     31.13.75.1:443          ESTABLISHED
```


Điều tra các cuộc tấn công web trong máy chủ Windows(Tiếp)

Administrator: Command Prompt

```
C:\Windows\system32> net start
These Windows services are started:

AarSvc_3095a
Adobe Acrobat Update Service
Application Information
AppX Deployment Service (AppXSVC)
AtherosSvc
AVCTP service
Background Tasks Infrastructure Service
Base Filtering Engine
Capability Access Manager Service
cbdhsvc_3095a
CDPUserSvc_3095a
Client License Service (ClipSVC)
CNG Key Isolation
COM+ Event System
Connected Devices Platform Service
Connected User Experiences and Telemetry
CoreMessaging
Credential Manager
Cryptographic Services
Data Usage
DCOM Server Process Launcher
Delivery Optimization
Dell Client Management Service
Dell Data Vault Collector
Dell Data Vault Processor
Dell Data Vault Service API
Dell Digital Delivery Services
```

Tìm các công việc đã lên lịch và chưa được lên lịch trên máy chủ cục bộ

C:\> schtasks.exe

Kiểm tra việc tạo tài khoản mới trong nhóm quản trị viên

C:\> lusrmgr.msc

Xem có bất kỳ quy trình không mong muốn nào đang chạy trong Trình quản lý tác vụ không

Start -> Run -> taskmgr -> OK

Tìm kiếm các dịch vụ mạng bất thường

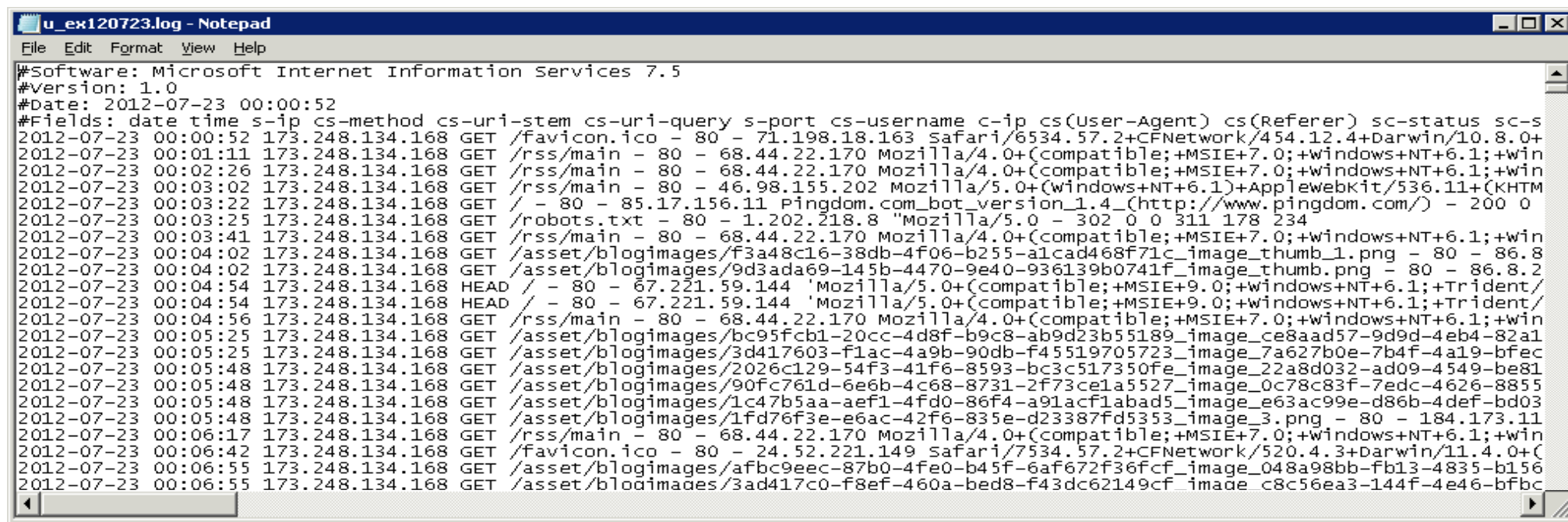
C: \> net start

Kiểm tra việc sử dụng dung lượng tệp để tìm sự giảm đột ngột về dung lượng trống

C: \> dir

Nhật Ký IIS

- IIS ghi lại **tất cả các lượt truy cập** máy chủ trong các tệp nhật ký
- Nhật ký IIS** cung cấp thông tin hữu ích về hoạt động của các ứng dụng Web khác nhau, chẳng hạn như thời gian kết nối, địa chỉ IP, tài khoản người dùng, URL của trang và các hành động
- Máy chủ IIS tạo tệp nhật ký dựa trên **văn bản ASCII**
- Trên Windows Server 2012, các tệp nhật ký được lưu trữ theo mặc định trong **% SystemDrive% \ inetpub \ logs \ LogFiles**



```
u_ex120723.log - Notepad
File Edit Format View Help
#Software: Microsoft Internet Information Services 7.5
#Version: 1.0
#Date: 2012-07-23 00:00:52
#Fields: date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(User-Agent) cs(Referer) sc-status sc-s
2012-07-23 00:00:52 173.248.134.168 GET /favicon.ico - 80 - 71.198.18.163 Safari/6534.57.2+CFNetwork/454.12.4+Darwin/10.8.0+
2012-07-23 00:01:11 173.248.134.168 GET /rss/main - 80 - 68.44.22.170 Mozilla/4.0+(compatible;+MSIE+7.0;+windows+NT+6.1;+win
2012-07-23 00:02:26 173.248.134.168 GET /rss/main - 80 - 68.44.22.170 Mozilla/4.0+(compatible;+MSIE+7.0;+windows+NT+6.1;+win
2012-07-23 00:03:02 173.248.134.168 GET /rss/main - 80 - 46.98.155.202 Mozilla/5.0+(Windows+NT+6.1)+AppleWebKit/536.11+(KHTML
2012-07-23 00:03:22 173.248.134.168 GET / - 80 - 85.17.156.11 Pingdom.com_bot_version_1.4_(http://www.pingdom.com/) - 200 0
2012-07-23 00:03:25 173.248.134.168 GET /robots.txt - 80 - 1.202.218.8 "Mozilla/5.0 - 302 0 0 311 178 234
2012-07-23 00:03:41 173.248.134.168 GET /rss/main - 80 - 68.44.22.170 Mozilla/4.0+(compatible;+MSIE+7.0;+windows+NT+6.1;+win
2012-07-23 00:04:02 173.248.134.168 GET /asset/blogimages/f3a48c16-38db-4f06-b255-a1cad468f71c_image_thumb_1.png - 80 - 86.8
2012-07-23 00:04:02 173.248.134.168 GET /asset/blogimages/9d3ada69-145b-4470-9e40-936139b0741f_image_thumb.png - 80 - 86.8.2
2012-07-23 00:04:54 173.248.134.168 HEAD / - 80 - 67.221.59.144 'Mozilla/5.0+(compatible;+MSIE+9.0;+windows+NT+6.1;+Trident/
2012-07-23 00:04:54 173.248.134.168 HEAD / - 80 - 67.221.59.144 'Mozilla/5.0+(compatible;+MSIE+9.0;+windows+NT+6.1;+Trident/
2012-07-23 00:04:56 173.248.134.168 GET /rss/main - 80 - 68.44.22.170 Mozilla/4.0+(compatible;+MSIE+7.0;+windows+NT+6.1;+win
2012-07-23 00:05:25 173.248.134.168 GET /asset/blogimages/bc95fcb1-20cc-4d8f-b9c8-ab9d23b55189_image_ce8aad57-9d9d-4eb4-82a1
2012-07-23 00:05:25 173.248.134.168 GET /asset/blogimages/3d417603-f1ac-4a9b-90db-f45519705723_image_7a627b0e-7b4f-4a19-bfec
2012-07-23 00:05:48 173.248.134.168 GET /asset/blogimages/2026c129-54f3-41f6-8593-bc3c517350fe_image_22a8d032-ad09-4549-be81
2012-07-23 00:05:48 173.248.134.168 GET /asset/blogimages/90fc761d-6e6b-4c68-8731-2f73ce1a5527_image_0c78c83f-7edc-4626-8855
2012-07-23 00:05:48 173.248.134.168 GET /asset/blogimages/1c47b5aa-aef1-4fd0-86f4-a91acflabad5_image_e63ac99e-d86b-4def-bd03
2012-07-23 00:05:48 173.248.134.168 GET /asset/blogimages/1fd76f3e-e6ac-42f6-835e-d23387fd5353_image_3.png - 80 - 184.173.11
2012-07-23 00:06:17 173.248.134.168 GET /rss/main - 80 - 68.44.22.170 Mozilla/4.0+(compatible;+MSIE+7.0;+windows+NT+6.1;+win
2012-07-23 00:06:42 173.248.134.168 GET /favicon.ico - 80 - 24.52.221.149 Safari/7534.57.2+CFNetwork/520.4.3+Darwin/11.4.0+
2012-07-23 00:06:55 173.248.134.168 GET /asset/blogimages/afbc9eec-87b0-4fe0-b45f-6af672f36fcf_image_048a98bb-fb13-4835-b156
2012-07-23 00:06:55 173.248.134.168 GET /asset/blogimages/3ad417c0-f8ef-460a-bed8-f43dc62149cf_image_c8c56ea3-144f-4e46-bfbc
```

Điều tra IIS Logs

■ Ví dụ về IIS log file:

2016-02-10 06:11:41
192.168.0.10
GET/images/content/bg_body_1.jpg - 80-192.168.0.27
Mozilla/5.0+(Windows+NT+6.3;+WOW64)+AppleWebKit/537.36+ (KHTML,+like+Gecko)+Chrome/48.0.2564.103+Safari/537.36
http://www.moviescope.com/css/style.css 200 0 0 365

Chủ đề	Cụm từ	Mô tả
Date	03/06/2015	Log file được thực hiện vào ngày 03 tháng 6 năm 2015
Time	8:45:30	Log file được ghi lại lúc 8:45 sáng
Server IP	172.15.10.30	Địa chỉ IP của máy chủ
Client IP address	192.168.100.150	Địa chỉ IP của khách hàng
cs-method	GET	Người dùng đã đưa ra lệnh GET hoặc tải xuống
cs-uri-stem	/images/content/bg_body_1.jpg	Người dùng muốn tải xuống tệp bg_body_1.jpg từ thư mục Hình ảnh
cs-uri-query	-	Truy vấn URI không xảy ra (các truy URI chỉ cần thiết cho các trang động, chẳng hạn như các trang ASP, vì vậy trường này thường chứa dấu gạch ngang cho các trang tĩnh.)

Điều tra IIS Logs

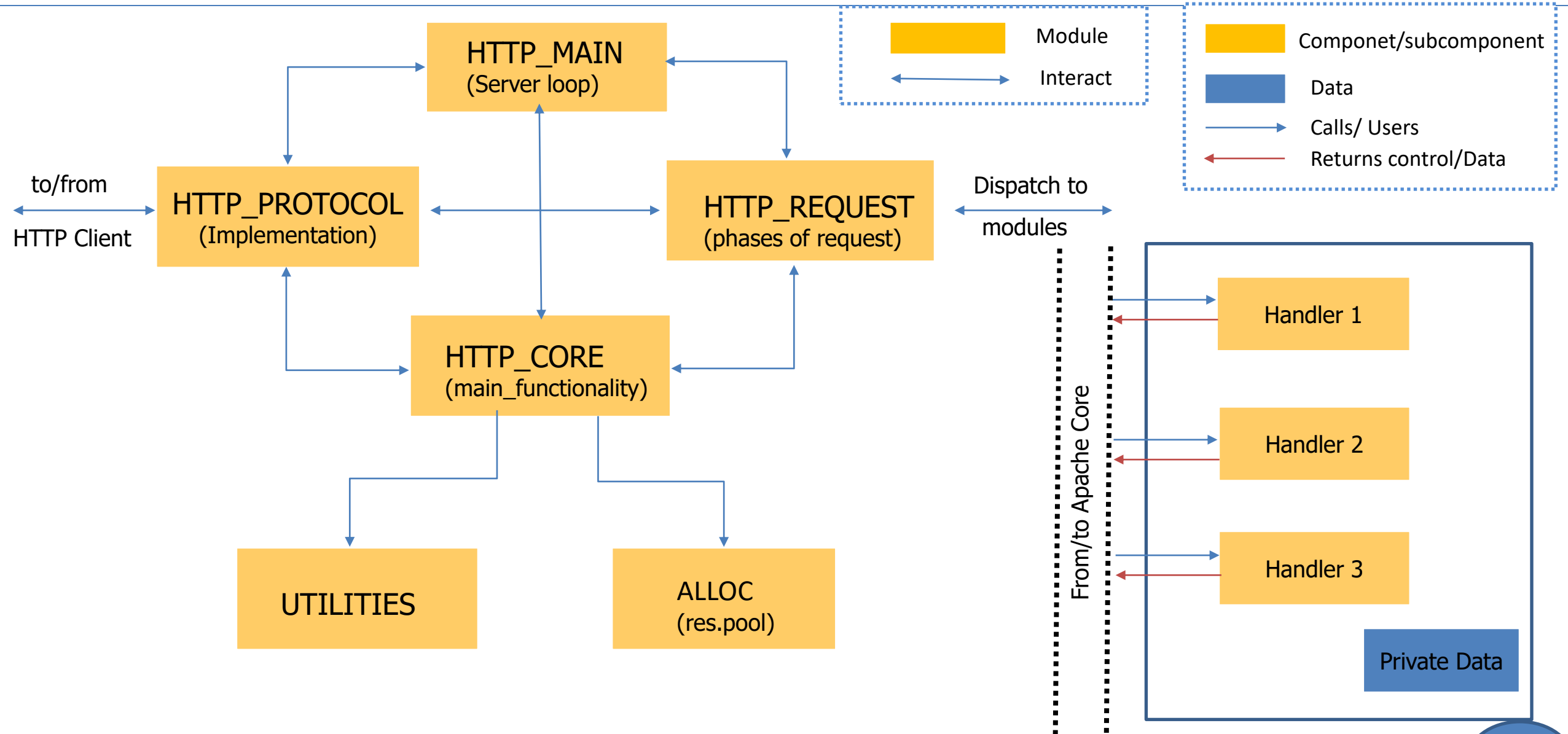
■ Ví dụ về IIS log file:

2016-02-10 06:11:41
192.168.0.10
GET/images/content/bg_body_
1.jpg - 80-192.168.0.27
Mozilla/5.0+(Windows+NT+
6.3;+WOW64)+AppleWebKi
t/537.36+ (KHTML,+like+Gec
ko)+Chrome/48.0.2564.103
+Safari/537.36
http://www.moviescope.co
m/css/style.css 200 0 0 365

Chủ đề	Cụm từ	Mô tả
s-port	80	Số hiệu cổng port của Server
cs-username	-	Người dùng đã được ẩn danh
c-ip	192.168.0.27	Địa chỉ IP của Client
cs(User-Agent)	Mozilla/5.0+(Windows+NT+6.3;+WOW64)+AppleWebKit/537.36+ (KHTML,+like+Gecko)+Chrome/48.0.2564.103 +Sa/537.36 <u>http://www.moviescope.com/css/style.css</u>	Loại trình duyệt mà khách hàng đã sử dụng như trình duyệt đại diện
cs(Referer)		Trang Web cung cấp liên kết đến Web site
sc-status	200	Yêu cầu đã được thực hiện mà không có lỗi
time-taken	365	Hành động được hoàn thành trong 365 mili giây

Điều tra trên máy chủ web Linux

Kiến trúc máy chủ web Apache



Nhật ký máy chủ web Apache

Máy chủ Apache HTTP

- ❑ Apache HTTP Server là một web server hỗ trợ nhiều hệ thống như Unix, GNU, FreeBSD, Linux, Solaris, Novell Netware, Amiga OS, Mac OS X, Microsoft windows, OS/2 và TPF

Thông tin nhật ký Apache

- ❑ Apache log cung cấp **thông tin về ứng dụng web** ví dụ như :
 - Địa chỉ IP của máy khách
 - ID của máy khách
 - Thời gian
 - Request từ phía Client
 - Mã trạng thái
 - Kích thước của đối tượng trả về phía máy khách

Định dạng của nhật ký Apache

- ❑ Định dạng của nhật ký Apache có dạng sau:
 - Thông thường Apache Log có định dạng
 - logFormat "%h %l %u %t \"%r\" %>s %b"
 - Log tùy biến
 - "logs/access_log" common

Điều tra nhật ký Apache

Nhật ký lỗi	Nhật ký truy cập
<ul style="list-style-type: none">❑ Máy chủ Apache (Apache Server) lưu các thông tin chẩn đoán và thông báo lỗi gặp phải trong khi gửi hoặc nhận request vào các error logs❑ Đây là một bằng chứng quan trọng khi tiến hành điều tra❑ Log mặc định<ul style="list-style-type: none">• RHEL/Red Hat/Centos/ Fedora Linux:<ul style="list-style-type: none">• /var/log/httpd/error_log• Debian/Ubuntu Linux<ul style="list-style-type: none">• /var/log/apache2/error.log• Free BDS<ul style="list-style-type: none">• /var/log/httpd-error.log	<ul style="list-style-type: none">❑ Bao gồm các quá trình gửi nhận request của máy chủ Apache❑ Đường dẫn mặc định của các log lỗi:<ul style="list-style-type: none">• RHEL/Red Hat/ Centos OS/Fedora Linux• Debian/ Ubuntu Linux<ul style="list-style-type: none">• /var/log/apache2/access.log• FreeBSD Linux:<ul style="list-style-type: none">• /var/log/httpd-access.log

Điều tra nhật ký Apache (Tiếp)

Access Log, định dạng thông thường

"%h %l %u %t \"%r\" %>s %b"

Xem trên text editor

10.10.10.10 - jason (17/Aug/2016:00:12:34 +0300] "GET /images/content/bg_body_1.jpg HTTP/1.0" 500 1458

Apache Log Fields		
%a-RemoteIPOrHost	%r - Request	%X - ConnectionStatus
%A-LocalIPOrHost	%>s - HttpStatusCode	%(Referer)i - Referer
%b or %B- Size	%t - eventTime	%{User-agent}i – UserAgent
%D-RequestTimeUs(microsecond)	%T- RequestTimeSeconds	%{UNIQUE_ID}e - Uniqueld
%h- RemoteIPOrHost	%u - RemoteUser	%{X – Forwarded-For}i - XForwardedFor
%k- KeepAliveRequests	%U- UrlPath	%{Host}i - Host
%l- RemoteLogname	%v- VirtualHost	

Điều tra nhật ký Apache (Tiếp)

Ví dụ tệp nhật ký lỗi xem trong trình biên dịch văn bản

```
[Mon Sep 16 14:25:33.812856 2016] [core: error] [pid 12485:tid 858 9745621] [client 10.10.255.14] File does not exist: /images/content/bg_body_1.jpg
```

Thành phần đầu tiên: Ngày, tháng, năm của log

Thành phần thứ hai: Mức độ nghiêm trọng của lỗi

Thành phần thứ ba: ID của tiến trình và thread tương ứng

Thành phần thứ tư : Địa chỉ IP của khách tạo ra lỗi

Thành phần thứ năm : Thông điệp lỗi (ví dụ ở đây "File does not exist")

Severity	Description	Example
emerg	Emergencies — system is unusable	"Child cannot open lock file. Exiting"
alert	Immediate action required	"getpwuid: couldn't determine user name from uid"
crit	Critical conditions	"socket: Failed to get a socket, exiting child"
error	Error conditions	"Premature end of script headers"
warn	Warning conditions	"child process 1234 did not exit, sending another SIGHUP"
notice	Normal but significant condition	"httpd: caught SIGBUS, attempting to dump core in ..."
info	Informational	"Server seems busy..."
debug	Debug-level messages	"opening config file ..."
trace1-8	Trace messages	"proxy: FTP: ... "

Điều tra Cross-site Scripting(XSS)

❑ Thông thường tấn công XSS sử dụng các thẻ HTML ví dụ <script></script>, ,<INPUT>,<BODY>, <etc>

❑ Kẻ tấn công sử dụng các công nghệ xáo trộn để tránh sự phát hiện của hệ thống IDS/IPS

Hex coding

In-line comment

Char Encoding

Toggle Case

Replace Keywords

White Space manipulation

❑ Ví dụ , tất cả các dòng lệnh dưới đây đều tương đương nhau

<script>alert("XSS")</script>

<sCRipT>alert("XSS")</ScRiPt>

%3cscript%3ealert("XSS")%3c/script%3e>

%253cscript%253ealert(1)%253c/script%253e

(Toggle Case)

(Hex Encoding)

(Double encoding)

❑ Điều tra viên có thể sử dụng regex để tìm kiếm HTML tags, các chữ ký XSS và các từ tương đương trong nhật ký truy cập web để kiểm tra tấn công XSS

Điều tra XSS: sử dụng Regex để tìm kiếm XSS Strings

1

- ❑ Biểu thức chính quy dưới đây kiểm tra tấn công bao gồm thẻ HTML đóng và mở (<>). Với các văn bản bên trong, theo đó là hex và mã hoá kép tương đương



2

- ❑ `/((\\%3C)|(\\%253C)|<)((\\%2F)|(\\%252F)|\\/*)[a-zA-Z0-9\\%]+((\\%3E)|(\\%253E)|>)/ix`
 - `/((\\%3C)|(\\%253C)|<)` - Kiểm tra dấu ngoặc nhọn mở, mã hex hoặc mã double hex tương đương
 - `/((\\%2F)|(\\%252F)|\\/*)` - Kiểm tra dấu gạch chéo, mã hex hoặc mã double hex tương đương
 - `[a-zA-Z0-9\\%]` - Kiểm tra kí tự viết hoa và kí tự viết thường ở bảng chữ cái alphabet trong các thẻ hoặc trong hex tương đương
 - `/((\\%2F)|(\\%252F)|\\/*)` - Kiểm tra dấu ngoặc nhọn đóng, mã hex hoặc mã double hex tương đương

Điều tra tấn công SQL Injection

❑ Tìm kiếm tấn công SQL injection trong các đường dẫn sau:

- IDS log files
- Log file của Database Server
- Web server log files



❑ Tấn công SQL injection ở file log của máy chủ web

```
12:34:35 192.2.3.4 HEAD GET  
/login.asp?username=blah' or  
1=1 - 12:34:35 192.2.3.4  
HEAD GET  
/login.asp?username=blah' or  
) 1=1 (-- 12:34:35 192.2.3.4  
HEAD GET  
/login.asp?username=blah' or  
exec master..xp_cmdshell 'net  
user test testpass --
```

Điều tra tấn công SQL injection(Tiếp)

Biểu thức chính quy dưới đây kiểm tra các tấn công có thể bao gồm siêu kí tự (meta-characters) ví dụ như dấu nháy đơn, nháy kép và văn bản bên trong hoặc mã hex tương đương

Biểu thức chính quy phát hiện siêu kí tự SQL

```
/(\%27 | (\') | (\- \-) | (\%23) | (#) /ix
```

Snort signature

```
alert tcp $EXTERNAL_NET  
any -> $HTTP_SERVERS  
$HTTP_PORTS (msg: "SQL  
Injection - Paranoid" ;  
flow:to_server,  
established; uricontent:  
".pl"; pcre: "/ (\%27) | (\'  
(\-\-) (%23) | (#) /i";  
classtype: Webapplication-  
attack; sid: 9099; rev:5;)
```

Biểu thức chính quy tùy biến để phát hiện siêu kí tự SQL

```
/((\%3D) | (=) ) [^\n] *((\%27)|(\')|(\-|) |(\%3B) (;))/i
```

Biểu thức chính quy cho việc kiểm tra tấn công SQL injection đặc thù

```
/\w* ((\%27) | (\')) ((\%6F) | 0 | (\%4F))  
((\%72) | r | (\%52)) /ix
```

Biểu thức chính quy cho việc kiểm tra tấn công SQL injection với từ khoá union

```
/((\%27) | (\') ) union /ix
```


Pentesting CSRF Validation Fields

Test 1

Xác nhận rằng các trường xác thực là bắt buộc cho mỗi người dùng

Test 2

Đảm bảo rằng người dùng khác không thể phát hiện các trường xác thực
Nếu kẻ tấn công có thể tạo trường xác thực giống nhau cho các người dùng khác thì việc tạo một trường xác thực mới là vô ích
Trường xác thực bắt buộc cho mỗi site

Test 3

Đảm bảo trường xác thực không bao giờ gửi các câu truy vấn bởi vì dữ liệu này có thể bị tiết lộ tới kẻ tấn công ở những trường hợp như HTTP referer

Test 4

Đảm bảo request sẽ thất bại nếu trường xác thực bị thiếu

Điều tra tấn công Code Injection

01

IDS và sandbox execution environment của hệ điều hành giúp phát hiện ra tấn công Code Injection

02

Khi hệ thống IDS tìm kiếm **một loạt các hướng dẫn thực thi trong lưu lượng mạng**, nó sẽ chuyển payload của các gói tin đáng ngờ tới môi trường thực thi khớp với đích của gói tin

03

Môi trường thực thi đúng là xác định với sự trợ giúp của **địa chỉ IP đích** của gói tin đến

04

Payload của gói tin sau đó thực thi ở môi trường theo dõi tương ứng, và thông báo của payload **tài nguyên hệ điều hành** sử dụng chuyển đến IDS

05

Nếu thông báo bao gồm bằng chứng của tài nguyên OS sử dụng, **IDS sẽ cảnh báo người dùng rằng gói tin bao gồm dữ liệu độc hại**

Điều tra tấn công Cookie Poisoning

01

Các phần mềm giúp phòng ngừa **giúp phát hiện tấn công Cookie Poisoning**

02

Các phần mềm **truy vết các lệnh đặt cookie** của máy chủ web

03

Với mỗi dòng lệnh thông tin như **tên cookie, giá trị cookie**, địa chỉ IP, thời gian và phiên nơi cookie được khởi tạo được lưu trữ lại

04

Sau đó , sản phẩm phòng ngừa sẽ bắt các HTTP request **gửi tới máy chủ** và so sánh với các thông tin cookie bất kì đã được lưu trữ

05

Nếu **kẻ tấn công** thay đổi **nội dung cookie** , chúng sẽ không giống với cookie được lưu trữ và sản phẩm phòng ngừa sẽ xác định được tấn công

Web Log Viewer

Deep log Analyzer

Đó là một giải pháp xử lý web có thể giúp bạn phân tích logs từ máy chủ web, ví dụ IIS trên Windows, Apache hoặc Nginx ở Unix/Linux

Sample Project - Deep Log Analyzer Pro Unregistered / 25 trial day(s) left - [General Statistics]

File Report View Tools Help

Open Import Back Next Dates Reports

[1 Projects] - Project: Sample Project (53 Reports) > General Statistics 11/12/05 - 11/25/05 / 14 day(s)

Reports

- General Statistics
- Accessed Resources
- Top Pages by Pageviews
- Top Pages by Visits
- All Accessed Files
- Top Downloads
- Accessed Graphics
- Entry Pages
- Visitors Bouncing Rate
- Exit Pages
- Entry Files

Calendar

All Dates

November 2005

S	M	T	W	T	F	S
30	31	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	1	2	3
4	5	6	7	8	9	10

General Statistics

Project: Sample Project Deep Log Analyzer

Report for website: <http://www.interactivevegt.com>
Web server logs imported: 11/12/05 12:01:21 AM - 11/25/05 11:59:50 PM
Report Date Interval: All Dates (14 Days) [Change...]

General Information for selected dates

Hits Summary [Details...]		Total	Per Day	Visits Summary	
Number of Hits:	82,226		5,873	Number of Unique Visitors:	4,836
Number of Successful Hits:	78,362 (95%)		5,597	Visitors who visited once:	4,082 (84%)
Outgoing Traffic:	6.87 Gb		498.30 Mb	Repeat visitors:	754 (16%)
Incoming Traffic:	161 Kb		11 Kb	Average Visits per visitor:	1.80

Visitors Summary

Visitors Summary		Total	Page Views	
Number of Unique visitors:	4,836		Total Page Views	957
Visitors who visited once:	4,082 (84%)		Average Page Views per Day	119
Repeat visitors:	754 (16%)		Average Page Views per Visitor	1.96
Average Visits per visitor:	1.80			

Open a Project

- Sample Project
- More Projects...

Analyze Website

- Create New Project...
- Import Log Files...
- Edit Project Settings...
- Filter Report by Date...
- Close Project
- Delete Imported Logs from D...

Reports

- View Report Properties...
- Refresh Report
- Export report to html...
- Add to Export list...
- Export list of reports...
- Create Custom Report...
- Load Custom Reports...

Web log expert

Đây là trình phân tích access logs có thể giúp phân tích logs của Apache, IIS và Nginx web Servers

Report for Sample - HTML

File | C:/ProgramData/WebLog%20Expert/Report/index.htm

Contents

- General Statistics
- Activity Statistics
- Access Statistics
- Visitors
- Referrers
- Browsers
- Errors
- Tracked Files

Report for Sample - HTML: General Statistics

Powered by WebLog Expert

Time range: 4/9/18 15:05:54 - 4/16/18 14:15:48 Generated on Fri Sep 30, 2022 - 19:22:28

Summary

Summary	
Hits	
Total Hits	3,135
Visitor Hits	3,059
Spider Hits	76
Average Hits per Day	391
Average Hits per Visitor	6.26
Cached Requests	0
Failed Requests	28
Page Views	
Total Page Views	957
Average Page Views per Day	119
Average Page Views per Visitor	1.96
Visitors	
Total Visitors	489
Average Visitors per Day	61

Web log viewers (Tiếp)



Apache WebLog Viewer
<https://apacheviewer.com>



Log Cruncher
<https://logentries.com>



AWStats
<http://awstats.org>



Go Access
<https://goaccess.io>



Nagios Log Server
<https://apacheviewer.com>



HTTP-ANALYZE
<https://http-analyze.com>



Splunk
<https://splunk.com>



Active LogView
<https://softcab.com>



Web Log Storming
<https://weblogstorming.com>

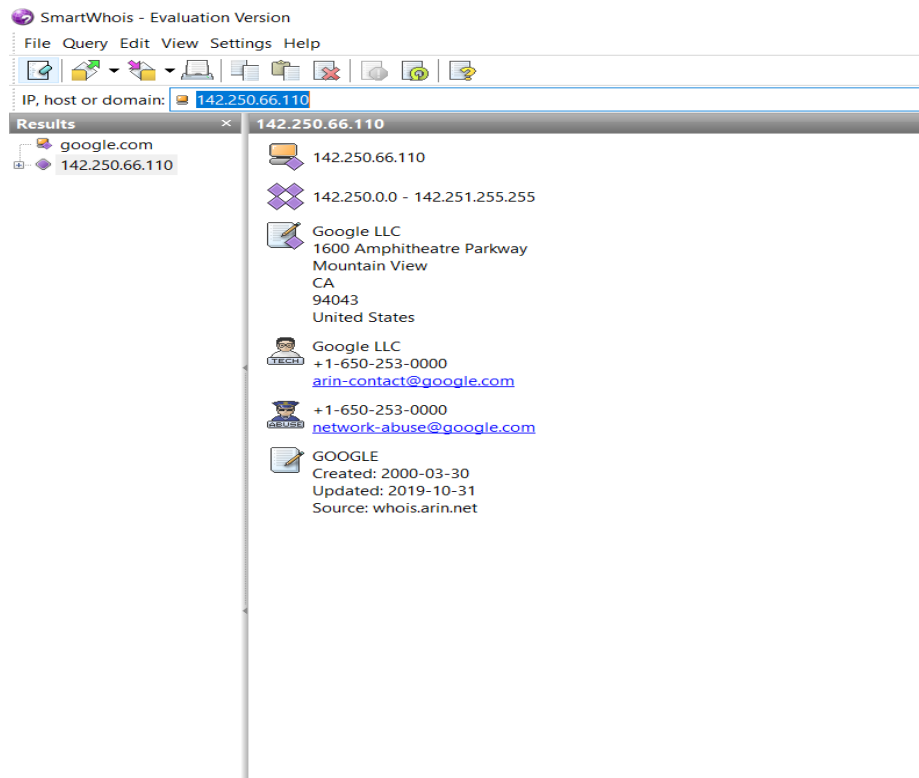


Webalizer
<https://apacheviewer.com>

Công cụ xác định địa chỉ IP

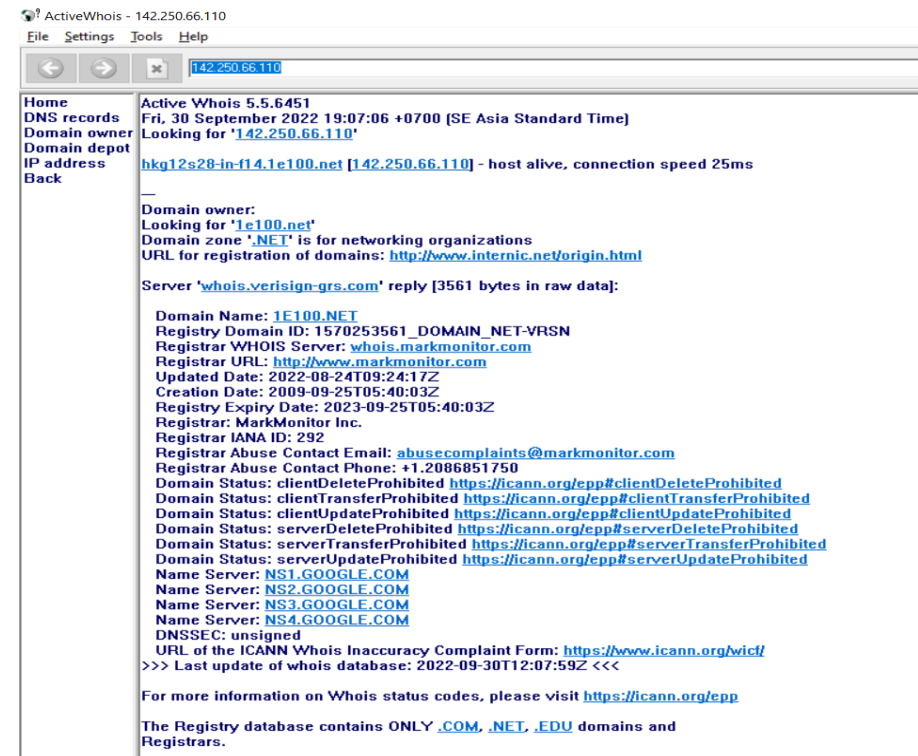
SmartWhois:

Các thông tin của network cho phép tìm kiếm tất cả các thông tin về địa chỉ IP ví dụ như tên host (hostname), tên miền bao gồm quốc gia, bang hoặc tỉnh, thành phố tên của nhà cung cấp dịch vụ mạng, quản trị và thông tin của hỗ trợ viên



ActiveWhois:

Công cụ mạng tìm bất kì thông tin về chủ sở hữu của địa chỉ IP hoặc tên miền
Có thể xác định quốc gia, thông tin cá nhân của đối tượng



Các công cụ Whois Lookup



LanWhoIs

lizardsystems.com/lanwhois/



HotWhois

<https://tialsoft.com>



Batch IP Converter

<https://networkmost.com>



ActiveWhois

<https://johnru.com>



CallerIP

<https://callerippro.com>



WhoisThisDomain

<https://nirsoft.net>



Sopolsoft

<https://sopolsoft.com>



SoftFuse Whois

<https://softfuse.com>



WhoIs Anylyzer Pro

<https://whoisanalyzer.com>



Whois

<https://technet.microsoft.com>

IV. Điều tra tần công mạng không dây

Nhu cầu điều tra số với mạng không dây

- Ngày nay, các thiết bị mạng và sử dụng mạng không dây có sự bùng nổ trong các thập niên vừa qua. Điển hình là các thiết bị di động, iPad, Laptop, các thiết bị GPS...
- Điều tra việc sử dụng các thiết bị không dây đang được chú trọng do việc dễ dàng sử dụng chúng của các nghi phạm
- Các thiết bị mạng không dây phổ biến bao gồm:
 - Thiết bị WiFi, Wi-Max
 - Điện thoại không dây, di động
 - Tai nghe Bluetooth
 - Các thiết bị hồng ngoại (TV remotes ...)



Lý do điều tra mạng không dây

- Tìm kiếm một máy tính xách tay bị đánh cắp bằng cách theo dõi nó trên mạng không dây.
- Xác định các điểm truy cập giả mạo
- Điều tra các hoạt động nguy hiểm hoặc trái phép xảy ra khi nghi phạm sử dụng mạng không dây.
- Điều tra các cuộc tấn công trên mạng không dây, bao gồm tấn công từ chối dịch vụ (DoS), tấn công mã hóa, chứng thực...



Các thiết bị không dây thông dụng



Tấn công mạng không dây

- *Wireless sniffing*: đây là một trong những cuộc tấn công nguy hiểm nhất trên mạng không dây như là kẻ tấn công có thể bắt được các gói tin trong quá trình truyền và nhìn thấy chi tiết các hoạt động của mạng không dây. Nếu gói tin không mã hóa trong khi truyền, kẻ tấn công có thể có được đầy đủ thông tin chi tiết của gói tin.
- *Mirror image access point*: đây là một điểm truy cập giả mạo được tạo ra sau khi nhận được thông tin của một điểm truy cập công cộng. khi một kẻ tấn công tạo ra một điểm truy cập với một tín hiệu mạnh hơn so với điểm truy cập thực tế và phát sóng. người dùng sẽ kết nối tín hiệu mạnh nhất và do đó trở thành nạn nhân.

Tấn công mạng không dây

- Ad-hoc network: đây là cuộc tấn công mạng không dây đơn giản nhất để thực hiện. một kẻ tấn công có thể kết nối với mạng ad-hoc của tổ chức và có thể truy cập vào các file nhạy cảm.
- Buffer overflow: đây là cuộc tấn công mạng không dây cho phép một kẻ tấn công sử dụng mã độc để khai thác lỗ hổng trong mã phần mềm của nhiều hệ điều hành và ứng dụng.
- Remote control software: đây là cuộc tấn công mạng không dây cho phép một kẻ tấn công cài đặt phần mềm điều khiển từ xa các máy tính.

Tấn công mạng không dây

- Virus/worm/spyware: đây là cuộc tấn công mạng không dây cho phép một kẻ tấn công cài đặt mã độc khai thác lỗ hổng hệ thống để đạt được đặc quyền truy cập hoặc để thao tác dữ liệu.
- Arp redirection/spoofing: đây là cuộc tấn công mạng không dây sử dụng là địa chỉ MAC giả mạo mà cho phép một kẻ tấn công chuyển hướng lưu lượng mạng đến máy tính của mình.
- Denial of service attack: đây là cuộc tấn công mạng không dây phá bỏ chứng thực vì nó sẽ ngắt kết nối một người dùng từ các điểm truy cập không dây đến hết thời hạn gói tin gửi. cuộc tấn công này sẽ ngắt kết nối các dịch vụ không dây.

Ăn cắp thông tin trên mạng không dây

- Sniffing là loại tấn công nghe trộm thông tin trên mạng không dây phổ biến nhất bởi vì nó dễ dàng thực hiện, khó phát hiện nhưng thông tin thu được lại có giá trị.
- Kẻ tấn công có thể truy cập vào mạng, giám sát các lưu lượng mạng từ khoảng cách lớn hơn nhiều so với khoảng cách được quy định trong chuẩn 802.11 là 61m.

Điều tra tấn công mạng không dây

- Điều tra viên cần kiểm tra xem các điểm truy cập không dây sử dụng giao thức bảo mật mạng không dây nào để qua đó xác định khả năng có các lỗ hổng.
- Thiết lập các thử nghiệm để kiểm tra quá trình xâm nhập: Điều tra viên có thể sử dụng các công cụ Backtrack để kiểm tra với các mật khẩu được cung cấp để kiểm tra việc mã hóa bảo mật cho mạng không dây.
- Dùng công cụ để kiểm tra pháp chứng: Điều tra viên có thể sử dụng các công cụ tìm kiếm phát hiện mạng không dây: daerosol, airfart, aphopper, apradar, karma, kismet, ministumbler, netstumbler, wellenreiter, wifi hopper, wirelessmon.

Điều tra mạng không dây của doanh nghiệp

- Một số điểm truy cập mạng không dây của tổ chức, doanh nghiệp chọn giao thức mã hóa không được an toàn dành cho mạng không dây, rất đơn giản để có thể cài đặt cho hầu hết những thiết bị nhỏ, giúp cho mạng không dây liên kết nhanh hơn và giảm chi phí của người dùng.
- Trước khi kiểm tra giao tiếp mạng không dây của doanh nghiệp, Điều tra viên phải biết được làm thế nào điểm truy cập và máy tính tương tác với nhau.
- Điều tra viên cần kiểm tra xem có điểm truy cập không dây nào cung cấp cho kẻ tấn công truy cập vào một cách đơn giản, Điều tra viên có thể sử dụng các công cụ Fern-Wifi-cracker – GUI để kiểm tra mã hóa.

