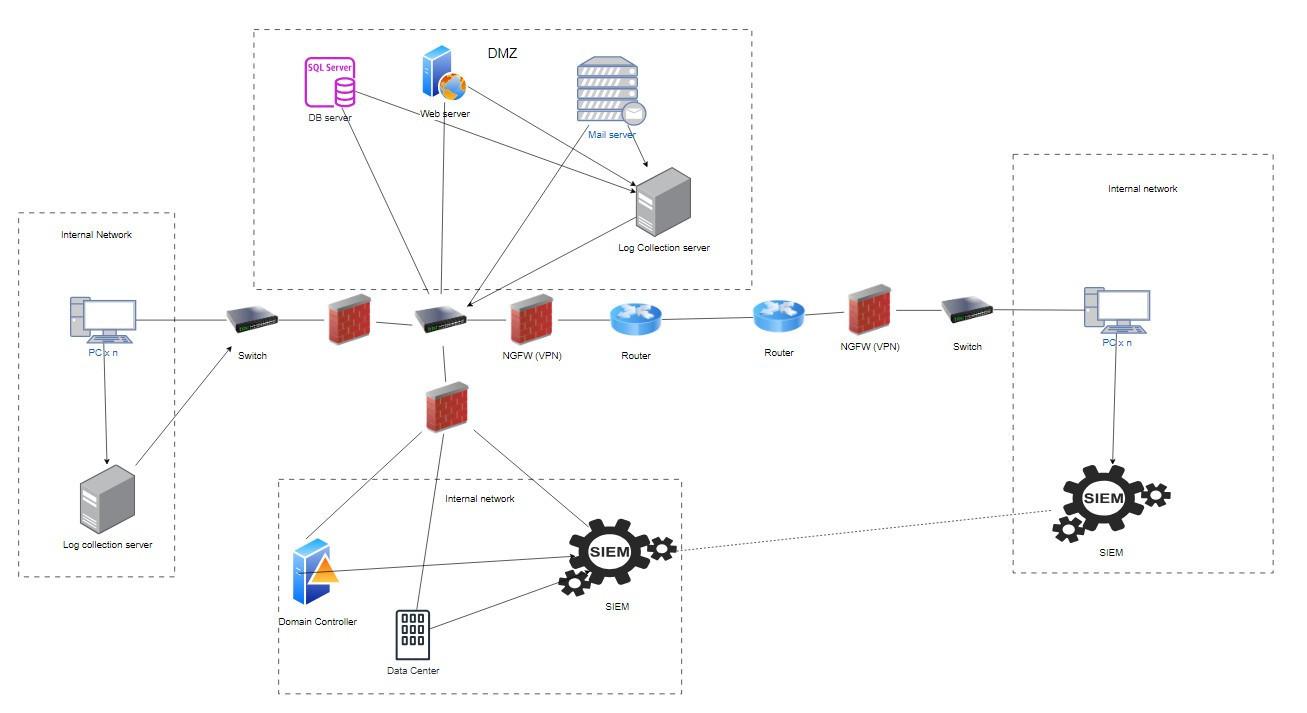
**\* Đề 2:**

Câu 2:



* Trước tiên, chi nhánh TP.HCM muốn truy cập vào dữ liệu tại trụ sở chính thì bắt buộc phải thông qua VPN để vào được mạng nội bộ công ty (Có thể dùng Cisco)
* Trên các client, server phải được cài đặt Agent monitoring, và các giải phảp Endpoint như EDR,.. để phục vụ cho công việc giám sát.
* Yêu cầu phải có tường lửa ở phía bên ngoài router để lọc những gói tin độc hại.
* Yêu cầu phải có những giải pháp load balancing, Content Delivery Network (CDN) và tường lửa để giám sát các traffic mạng đối với Webserver. Đặc biệt chú ý các port 80, 443,.. đối với máy chủ web.
* Domain controller, Data Center, chỉ mở cổng kết nối mạng đối với các máy trong nội bộ, không thông mạng ra Internet.
* Mail server được phép mở port ra bên ngoài để gửi mail, tuy nhiên nên được cài đặt giải pháp Anti-APT để tránh những email phishing được gửi đến client bên trong mạng nội bộ.
* Đối với doanh nghiệp 200 người, có thể sử dụng giải pháp SIEM của splunk, Qradar để thực hiện giám sát, bộ luật cần được tối ưu và có độ bao phủ rộng để giảm thiếu những trường hợp dương tính giả, đồng thời tránh lộ lọt tấn công.
* Truy cập vào các giải pháp cần thông qua PAM, JUMP server.

Câu 3:

Phương pháp ứng cúu sự cố DdoS:

* Hệ thống monitor và tường lửa sẽ phát hiện ra rằng traffic đột ngột tăng cao vượt quá ngưỡng được thiết lập và quá khả năng tải của server.
* Sau khi nhận diện ra đó là sự cố DdoS, quan trọng nhất là cần phải khôi phục lại trang web hoạt động một cách bình thường, để không gây ảnh hưởng đến với hoạt động của doanh nghiệp.
* Load balancing và CDN sẽ giúp giảm tải cho server một phần, tuy nhiên vẫn cần thực hiện xử lý sự cố.
* Thông thường DdoS sẽ sử dụng botnet để tấn công, và nó mang theo rất nhiều IP, các request thường chỉ access vào trang chủ và không tải các static resource (js, css, image,..) điều này cho thấy đây không phải là các client bình thường và không được truy cập bằng browser.
* Sử dụng rule limit để đưa website trở về hoạt động bình thường, nếu IP vượt quá số lần request quy định thì sẽ được đưa vào blacklist và bị block 3 ngày.
* Nếu như request mang theo X-forwarder-For: thì http header chứa X-forwarder-for sẽ mang theo IP của máy chạy tool DdoS. Lúc đấy sẽ thực hiện cấu hình rule để block IP tấn công.
* Ngoài ra, giới hạn số lần truy cập mỗi giây cho từng IP đến từ các quốc gia khác nhau (ví dụ 2 lần /s đối với nước ngoài, 5 lần /s đối với Việt Nam) để tránh việc block nhầm IP của khách hàng.

**\* Đề 1:**

Câu 2:

Các dấu hiệu xâm nhập:

* Có kết nối đến trang web trafficconverter.biz với IP 104.244.14.253.
* Tự động tải tệp tin loadadv.exe MD5: 58A347C5DA60FE449F7BB6F0BEE3FA44
* Các tệp tin dll lạ được tải vào thư mục hệ thống, trong đó tên các tệp dll là những ký tự ngẫu nhiên
* Add registry, tạo persistence, cho phép dll tự động tải ngay khi máy tính được bật lên. Cụ thể ở đây là được tải cùng với svchost, một tiến trình được verified bới Microsoft.
* Lỗ hổng MS08-067 đang được sử dụng để leo thang chiều ngang.
* Đăng nhập vào share folder $ADMIN.
* Vô hiệu hoá Automatic Update, System Restore.

Câu 3:

Như trong sự cố trên, dễ dàng nhận thấy đây là sự cố tấn công bằng mã độc, và máy tính tải phần mềm độc hại về đã bị Compromise do đã xuất hiện các hành vi tải các dll vào hệ thống, thêm registry, đồng thời xuất hiện hành vi leo thang chiều ngang qua các máy khác bằng lỗ hổng MS08-067.

Trước tiên, ngay khi xuất hiện cảnh báo trên hệ thống giám sát, đội ngũ Tier 1 cần ngay lập tức escalate lên Tier 2, 3 để thực hiện các biện pháp ứng phó sự cố.

Đội ngũ ứng phó sự cố (Incident Response) thực hiện cách ly tất cả các máy có dấu hiệu bị lây nhiễm ra khỏi mạng nội bộ của công ty.

Lúc này, bắt đầu thực hiện điều tra sự cố, loại bỏ mã độc.

* Forensic máy, kiểm tra những hành vi của mã độc (Kết nối tới C2, tạo persistence, clear log,….). Trong trường hợp này là mã độc trên windows, có thể sử dụng bộ công cụ của Hayabusa Security hoặc Eric Zimmerman để thực hiện kiểm tra Event Viewer.
* Scan máy (thor, krvt, tdsskiller,..) để kiểm tra những file có dấu hiệu khả nghi đang nằm trên máy.
* Sử dụng bộ công cụ Sysinternal để thực hiện rà quét, loại bỏ mã độc. Kiểm tra các process, dll lạ, sử dụng Autorun để kiểm tra những entry lạ đang được khởi động cùng hệ thống, hoặc được lập lịch chạy thường xuyên.
* Sau khi đã xác định được những file, dll, lạ, thực hiện xoá bỏ khỏi máy. Chặn connect tới C2 server
* Sau khi đã hoàn toàn loại bỏ mã độc ra khỏi máy, thực hiện khôi phục lại hoạt động bình thường.

Thực hiện vá lỗi (lỗ hổng MS08-067), thực hiện VA (Vulnerable Assessment) để đánh giá các lỗ hổng bảo mật đang tồn tại trên máy.

Blacklist domain và IP.

# C. Đề ôn tập

# Dạng 1:

- Quản trị viên nhận được thông báo của người dùng rằng máy của họ gần

đây hay bị treo máy, nghẽn mạng, một số website bảo mật không truy cập

được.

- Trước đó người dùng này đã truy cập vào đường liên kết được từ email:

ddarkmaster@gmail.com có tên Daniel Adams. Liên kết dẫn người dùng

truy cập vào website trafficconverter.biz, IP máy chủ: 104.244.14.253,

sau khi truy cập máy tính tự động tải về và thực thi tệp tin loadadv.exe có

mã băm MD5: 58A347C5DA60FE449F7BB6F0BEE3FA44.

Quản trị viên tiếp cận, phân tích, điều tra và phát hiện thấy một số tệp tin

DLL bất thường trong thư mục hệ thống:

%System%\<rnd>dir.dll

%Program Files%\Internet Explorer\<rnd>.dll

%Program Files%\Movie Maker\<rnd>.dll

%All Users Application Data%\<rnd>.dll

%Temp%\<rnd>.dll

%System%\<rnd>tmp

55

%Temp%\<rnd>.tmp

- Trong đó <rnd> là một chuỗi ngẫu nhiên những kí hiệu.

- Kiểm tra Registry Quản trị viên thấy một số khóa sau được tạo ra:

HKLM\SYSTEM\CurrentControlSet\Services\netsvcs]

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SvcHost]

"netsvcs" = "<original

value> %System%\<rnd>.dll”

- Máy bị nhiễm đang chạy dịch vụ HTTP server trên một cổng TCP 8081.

Thực hiện nhiều kết nối tới các máy tính khác trong mạng thông qua

cổng TCP 445 hoặc 139, sử dụng lỗ hổng MS08-067. Một số kết nối cố

gắng đăng nhập vào thư mục chia sẻ ADMIN$. Kiểm tra một số cấu hình

trên máy thấy dịch vụ WindowsAutomatic Update bị tắt, System Restore

bị vô hiệu hóa.

- Bạn hãy tìm các dấu hiệu xâm nhập cho các hệ thống IDS, SIEM phát

hiện các tấn công tương ứng.

- Ứng cứu sự cố trên.

# Giải :

- Các dấu hiệu xâm nhập:

- Phân tích các dấu hiệu thành các IOC hành vi (Behavior) như sau:

- B-1: Người dùng nhận được một email từ ddarkmaster@gmail.com có

tên Daniel Adams và một liên kết trong email.

- B-2: Người dùng truy cập liên kết trong email. Liên kết dẫn người dùng

đến trang web trafficonverter.biz có IP 104.244.14.253

- B-3: File loadadv.exe được tải về từ trafficonverter.biz. File này có giá trị

md5 hash là 58A…

- B-4: Máy nạn nhân có một số tệp tin dll bất thường:

- %System\<rnd>dir.dll

- %Program Files%\Internet Explorer\<rnd>.dll

- %Program Files%\Movie Maker\<rnd>.dll

- %All Users Application Data%\<rnd>.dll

- %Temp%\<rnd>.dll

- %System%\<rnd>.tmp

- %Temp%\<rnd>.tmp

56

- B-5: Máy nạn nhân có một số registry key bất thường:

- HKLM\SYSTEM\CurrentControlSet/Services/netsvcs

- HKLM\SOFTWARE\Microsoft\Windows

NT\CurrentVersion\SvcHost

- Thay đổi giá trị của dịch vụ netsvcs để bao gồm file dll độc hại

(<rnd>.dll)

- B-5: Máy nạn nhân đang chạy dịch vụ HTTP server trên cổng TCP 8081.

Thực hiện kết nối tới các máy tính trong mạng thông qua cổng TCP 445

hoặc 139 sử dụng lỗ hổng MS08-067. Một số kết nối cố gắng đăng nhập

vào thư mục chia sẻ ADMIN$

- B-6: Dịch vụ Windows automatic update bị tắt, System restore bị vô hiệu

hóa trên máy nạn nhân.

- Tiếp tục phân tích IOC hành vi thành các IOC đơn vị (Atomic) và IOC

được tính toán (Computed):

- C-1: MD5 hash 58A…

- A-1: Địa chỉ email: ddarkmaster@gmail.com

- A-2: Tên thư: Daniel Adams

- A-3: Tên miền nguy hiểm: trafficconverter.biz

- A-4: IP nguy hiểm: 104.244.14.253

- A-5: Tên file được tải xuống: loadadv.exe

- A-6: Tên file <rnd>dir.dll

- A-7: Tên file <rnd>.dll

- A-8: Tên file <rnd>.tmp

- A-9: Đường dẫn %System\

- A-10: Đường dẫn %Program Files%\Internet Explorer\

- A-11: Đường dẫn %Program Files%\Movie Maker\

- A-12: Đường dẫn %Temp%\

- A-13: Đường dẫn %System%\

- A-14: Registry key

HKLM\SYSTEM\CurrentControlSet/Services/netsvcs

57

- A-15: Registry key HKLM\SOFTWARE\Microsoft\Windows

NT\CurrentVersion\SvcHost

- A-16: Giao thức TCP

- A-17: Port 8081

- A-18: Giao thức kết nối tới máy khác: TCP

- A-19: Port máy khác: 445 hoặc 139

- A-20: Mã lỗ hổng: MS08-067

- A-21: Thư mục ADMIN$

- A-22: Trạng thái dịch vụ Windows automatic update

- A-23: Trạng thái dịch vụ System Restore

- IOC được chuyển đổi thành các dấu hiệu để sử dụng trong một loạt các

hệ thống IDS, SIEM:

- C-1: Chữ ký antivirus để phát hiện sự tồn tại các giá trị băm

- A-1: Chữ ký snort để phát hiện thư nhận từ email nguy hiểm

- A-2: Bro script để phát hiện dòng tên thư

- A-3: Chữ ký Snort để phát hiện kết nối với tên miền nguy hiểm

- A-4: Chữ ký Snort để phát hiện kết nối với IP nguy hiểm

- A-5/C-1: Bro script để dò tìm tệp tin có tên là loadadv.exe hoặc tệp tin

với giá trị băm MD5 truyền qua mạng

- A-6/A-7/A-8: Bro script để dò tìm tệp tin có tên chứa chuỗi <rnd> hoặc

tệp tin với giá trị băm MD5 tương tự truyền qua mạng

- A-9/A-10/A-11/A-12/A-13: HIDS để phát hiện sự thay đổi của những thư

mục này có chứa file dll với MD5 nguy hiểm hay không

- A-14/A-15: Luật HIDS để phát hiện những sự thay đổi trong registry

- A-16/A-17: Chữ ký snort để phát hiện những kết nối TCP từ cổng 8081

- A-18/A-19: Chữ ký snort để phát hiện những kết nối TCP đến máy khác

cổng 445 hoặc 139

- A-20: Chữ ký snort để phát hiện dữ liệu truyền tiềm ẩn lỗ hổng MS08-

067

- A-21: Luật HIDS để phát hiện số lần đăng nhập bất thường vào thư mục

ADMIN$

58

- A-22/A-23: Luật HIDS để đảm bảo trạng thái dịch vụ windows automatic

update, system restore luôn bật..

- Ứng cứu sự cố:

o Như trong sự cố trên, dễ dàng nhận thấy đây là sự cố tấn công

bằng mã độc, và máy tính tải phần mềm độc hại về đã bị

Compromise do đã xuất hiện các hành vi tải các dll vào hệ thống,

thêm registry, đồng thời xuất hiện hành vi leo thang chiều ngang

qua các máy khác bằng lỗ hổng MS08-067.

o Trước tiên, ngay khi xuất hiện cảnh báo trên hệ thống giám sát, đội

ngũ Tier 1 cần ngay lập tức chuyển lên Tier 2, 3 để thực hiện các

biện pháp ứng phó sự cố.

o Đội ngũ ứng phó sự cố (Incident Response) thực hiện cách ly tất cả

các máy có dấu hiệu bị lây nhiễm ra khỏi mạng nội bộ của công ty.

o Lúc này, bắt đầu thực hiện điều tra sự cố, loại bỏ mã độc.

o Forensic máy, kiểm tra những hành vi của mã độc (Kết nối tới C2,

tạo persistence, clear log,….). Trong trường hợp này là mã độc trên

windows, có thể sử dụng bộ công cụ của Hayabusa Security hoặc

Eric Zimmerman để thực hiện kiểm tra Event Viewer.

o Scan máy (thor, krvt, tdsskiller,..) để kiểm tra những file có dấu

hiệu khả nghi đang nằm trên máy.

o Sử dụng bộ công cụ Sysinternal để thực hiện rà quét, loại bỏ mã

độc. Kiểm tra các process, dll lạ, sử dụngAutorun để kiểm tra

những entry lạ đang được khởi động cùng hệ thống, hoặc được lập

lịch chạy thường xuyên.

o Sau khi đã xác định được những file, dll, lạ, thực hiện xoá bỏ khỏi

máy. Chặn connect tới C2 server

o Sau khi đã hoàn toàn loại bỏ mã độc ra khỏi máy, thực hiện khôi

phục lại hoạt động bình thường.

o Thực hiện vá lỗi (lỗ hổng MS08-067), thực hiện VA(Vulnerable

Assessment) để đánh giá các lỗ hổng bảo mật đang tồn tại trên

máy.

o Blacklist domain và IP.

- Trả lời cách 2:

Giai đoạn 1: Nhận dạng

- Nhân viên báo cáo hoạt động đáng ngờ, chẳng hạn như máy bị treo, nghẽn mạng,

một số website bảo mật không truy cập được.

59

- Kiểm tra log, cảnh báo bất thường từ hệ thống SIEM, IDS, email đang có chẳng

hạn như thông tin đăng nhập từ các vị trí bất thường, băng thông ra từ máy cao, các

nỗ lực kết nối đến các máy lạ

Giai đoạn 2: Ghi lại sự cố

• Ghi lại thời gian nhân viên báo cáo sự cố

• Ghi lại thông tin nhân viên báo cáo sự cố

• Mô tả sơ bộ về sự cố

Giai đoạn 3: Phản hồi ban đầu

• Thu thập thông tin chi tiết, độ nghiệm trọng về sự cố

• Thông báo cho toàn bộ nhân viên xem có ai nhận được email tương tự

không

• Tạo nhóm ứng phó

Giai đoạn 4: Thiết lập liên lạc

• Liên lạc với nhóm báo cáo sự cố và mô tả về sự cố

• Liên lạc với đại diện pháp lý nếu cần cần nộp đơn kiện thủ phạm

Giai đoạn 5: Ngăn chặn

- Ngắt kết nối máy đang bị xâm nhập khỏi mạng để tạm dừng mọi hoạt động trái

phép đang diễn ra.

- Sao lưu các dữ liệu ở máy bị xâm nhập

- Thiết lập các luật Firewall, IDS để chặn các email tương tự từ kẻ tấn công và các

lưu lượng truy cập các IP, PORT liên quan trong cuộc tấn công.

- Thiết lập các luật HIDS cho máy bị xâm phạm dựa trên các yếu tố như đầu bài

nêu.

Giai đoạn 6: Loại bỏ

- Quét hệ thống bị ảnh hưởng để tìm phần mềm độc hại hoặc các dấu hiệu xâm

phạm bằng cách sử dụng các công cụ antivirus.

- Kiểm tra lại máy bị xâm nhập xem có bất kỳ thay đổi trái phép nào trong thư mục

hệ thống, registry, các file cấu hình do kẻ tấn công thực hiện hay không. Nếu cần

thiết có thể cài lại hệ điều hành.

- Loại bỏ các tệp tin DLL bất thường đã phát hiện được

- Tắt dịch vụ tồn tại lỗ hổng MS08-067

Giai đoạn 7: Phục hồi

60

- Khôi phục cây thư mục, registry ban đầu của máy bị xâm phạm. Khởi động lại

dịch vụ windows automatic update và windows restore

- Giám sát tài khoản email của nhân viên để phát hiện các dấu hiệu bị tấn công

tương tự hay không.

- Liên lạc với tất cả các bên có thể đã nhận được email lừa đảo từ tài khoản bị xâm

nhập.

- Kiểm tra xem còn nhân viên nào khác nhận được email tương tự không.

Giai đoạn 8: Tài liệu hóa sự cố

• Ghi lại các dấu hiệu của sự cố.

• Ghi lại các luật IDS, Firewall, HIDS đã dùng để ngăn chặn, phát hiện sự cố.

• Ghi lại thông tin nhóm đã ứng cứu sự cố

• Ghi lại lý do đằng sau sự cố

Giai đoạn 9: Xem lại và cập nhật ứng phó sự cố

• Xem lại quy trình sau khi hoàn thành tài liệu và các bước khôi phục

• Thảo luận với các thành viên trong nhóm của bạn về các bước được triển

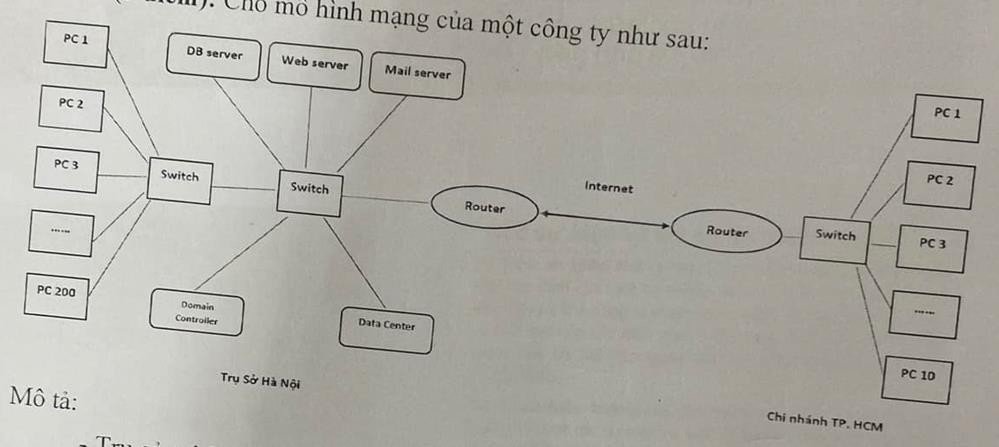
khai thành công và những sai lầm đã phạm

• Xem xét phản hồi và cập nhật chính sách sẽ làm giảm tác động của sự cố và

giúp xử lý các sự cố trong tương lai

# Dạng 2:

- Mô tả:



o Trụ sở tại Hà Nội có 200 người dùng tại các phòng. Kinh doanh,

nhân sự, tài chính, điều hành, công nghệ thông tin

o Máy chủ cung cấp dịch vụ web và mail cho người dùng bên trong

và bên ngoài truy cập. Máy chủ điều khiển miền (DC) và máy chủ

lưu trữ tập trung dữ liệu nội bộ

o Chi nhánh tại TP. HCM có nhu cầu truy cập vào dữ liệu tại trụ sở

chính

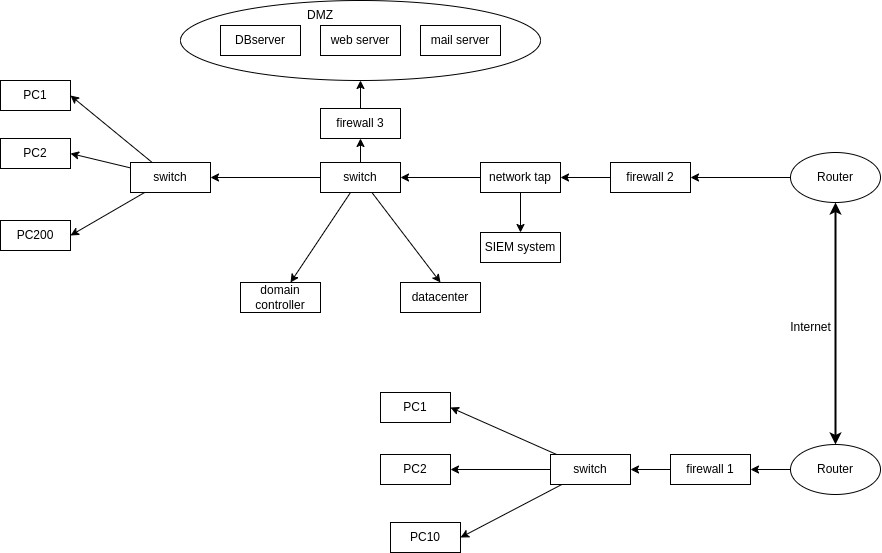
- Hãy đảm bảo an toàn cho mô hình mạng ở trên sử dụng firewall và SIEM

có chọn lọc dữ liệu

- Sử dụng mô hình trên, trình bày phương pháp ứng cứu sự cố khi máy chủ

web bị tấn công từ chối dịch vụ phân tán.

# Giải:



- Firewall:

- Đặt tường lửa Firewall 1 và Firewall 2 sau các router kết nối với internet

mỗi khu vực để bảo vệ mạng nội bộ khỏi các mối đe dọa bên ngoài.

- Đặt một tường lửa Firewall 3 khác giữa vùng DMZ và mạng nội bộ ở khu

vực Hà Nội để bổ sung thêm một lớp bảo vệ cho mạng nội bộ, đảm bảo

rằng ngay cả khi DMZ bị xâm phạm, kẻ tấn công không thể dễ dàng truy

cập vào mạng nội bộ.

- Hệ thống SIEM:

62

- SIEM cần đặt sau Firewall 2 vì đây là vị trí vừa có thể đảm bảo an toàn

cho SIEM khỏi các tấn công trực tiếp vừa dễ dàng thu thập dữ liệu từ tất

cả các thiết bị từ cả 2 khu vực.

- Sử dụng thêm cơ chế thu thập bằng network tap để SIEM có thể thu thập

thông tin từ các thiết bị mà không gây nghẽn mạng.

- Ứng cứu sự cố:

o Hệ thống monitor và tường lửa sẽ phát hiện ra rằng traffic đột ngột

tăng cao vượt quá ngưỡng được thiết lập và quá khả năng tải của

server.

o Sau khi nhận diện ra đó là sự cố DdoS, quan trọng nhất là cần phải

khôi phục lại trang web hoạt động một cách bình thường, để không

gây ảnh hưởng đến với hoạt động của doanh nghiệp.

o Load balancing và CDN sẽ giúp giảm tải cho server một phần, tuy

nhiên vẫn cần thực hiện xử lý sự cố.

o Thông thường DdoS sẽ sử dụng botnet để tấn công, và nó mang

theo rất nhiều IP, các request thường chỉ access vào trang chủ và

không tải các static resource (js, css, image,..) điều này cho thấy

đây không phải là các client bình thường và không được truy cập

bằng browser.

o Sử dụng rule limit để đưa website trở về hoạt động bình thường,

nếu IP vượt quá số lần request quy định thì sẽ được đưa vào

blacklist và bị block 3 ngày.

o Nếu như request mang theo X-forwarder-For: thì http header chứa

X-forwarder-for sẽ mang theo IP của máy chạy tool DdoS. Lúc đấy

sẽ thực hiện cấu hình rule để block IP tấn công.

o Ngoài ra, giới hạn số lần truy cập mỗi giây cho từng IP đến từ các

quốc gia khác nhau (ví dụ 2 lần /s đối với nước ngoài, 5 lần /s đối

với Việt Nam) để tránh việc block nhầm IP của khách hàng.

Giai đoạn 1: Nhận dạng

- Nhân viên báo cáo hoạt động đáng ngờ, chẳng hạn như web bị chậm, truy cập lúc

được lúc không…

- Kiểm tra log, cảnh báo bất thường từ hệ thống SIEM, IDS, web server đang có để

xác nhận rằng web server đang bị tấn công DDoS. Các dấu hiệu ddos tiêu biểu như

lưu lượng băng thông truy cập tăng đột ngột, nhiều request từ một hoặc nhiều địa

chỉ IP hoặc số phản hồi lỗi từ máy chủ tăng lên.

Giai đoạn 2: Ghi lại sự cố

• Ghi lại thời gian nhân viên báo cáo sự cố

63

• Ghi lại thông tin nhân viên báo cáo sự cố

• Mô tả sơ bộ về sự cố

Giai đoạn 3: Phản hồi ban đầu

• Thu thập thông tin chi tiết, độ nghiệm trọng về sự cố

• Thông báo cho toàn bộ các bên liên quan về sự cố, có thể bao gồm nhóm

phát triển web, đội ứng phó sự cố, ban quản lý, khách hàng ,...

• Tạo nhóm ứng phó

Giai đoạn 4: Thiết lập liên lạc

• Liên lạc với nhóm báo cáo sự cố và mô tả về sự cố

• Liên lạc với đại diện pháp lý nếu cần cần nộp đơn kiện thủ phạm

Giai đoạn 5: Ngăn chặn

• Lọc lưu lượng truy cập: Cấu hình firewall để chặn hoặc giới hạn lưu lượng

truy cập từ các địa chỉ IP đang tạo ra nhiều request nhất.Tuy nhiên cũng cần

kiểm tra kỹ để không chặn nhầm lưu lượng truy cập hợp pháp.

• Xác định endpoint gây tốn mà cuộc tấn công ddos khai thác, có thể tắt

endpoint này tạm thời cho đến khi cuộc tấn công lắng xuống.

• Backup dữ liệu webserver tránh trường hợp hacker thực hiện tấn công lấy

cắp dữ liệu sau khi ddos thành công.

• Nếu các phương pháp trên vẫn không thể ngăn chặn cuộc tấn công có thể

cần tắt web server đến khi tần suất tấn công giảm xuống

Giai đoạn 6: Loại bỏ

• Tăng khả năng xử lý của website như tăng tài nguyên vật lý của web server.

Mở rộng theo chiều ngang thêm nhiều máy chủ hơn, tích hợp khả năng auto

scale,...

• Tích hợp thêm các công cụ chống ddos tự động cho web server.

• Thêm tính năng ratelimit cho các IP truy cập

• Tìm hiểu thêm xem cách thức cuộc tấn công ddos xảy ra xem có thể giải

quyết triệt để hơn không

Giai đoạn 7: Phục hồi

- Khôi phục lại web trạng thái web server như ban đầu (có thể kèm theo các tính

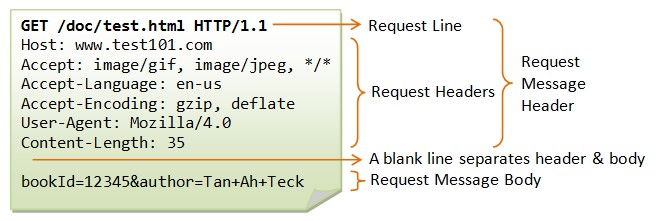
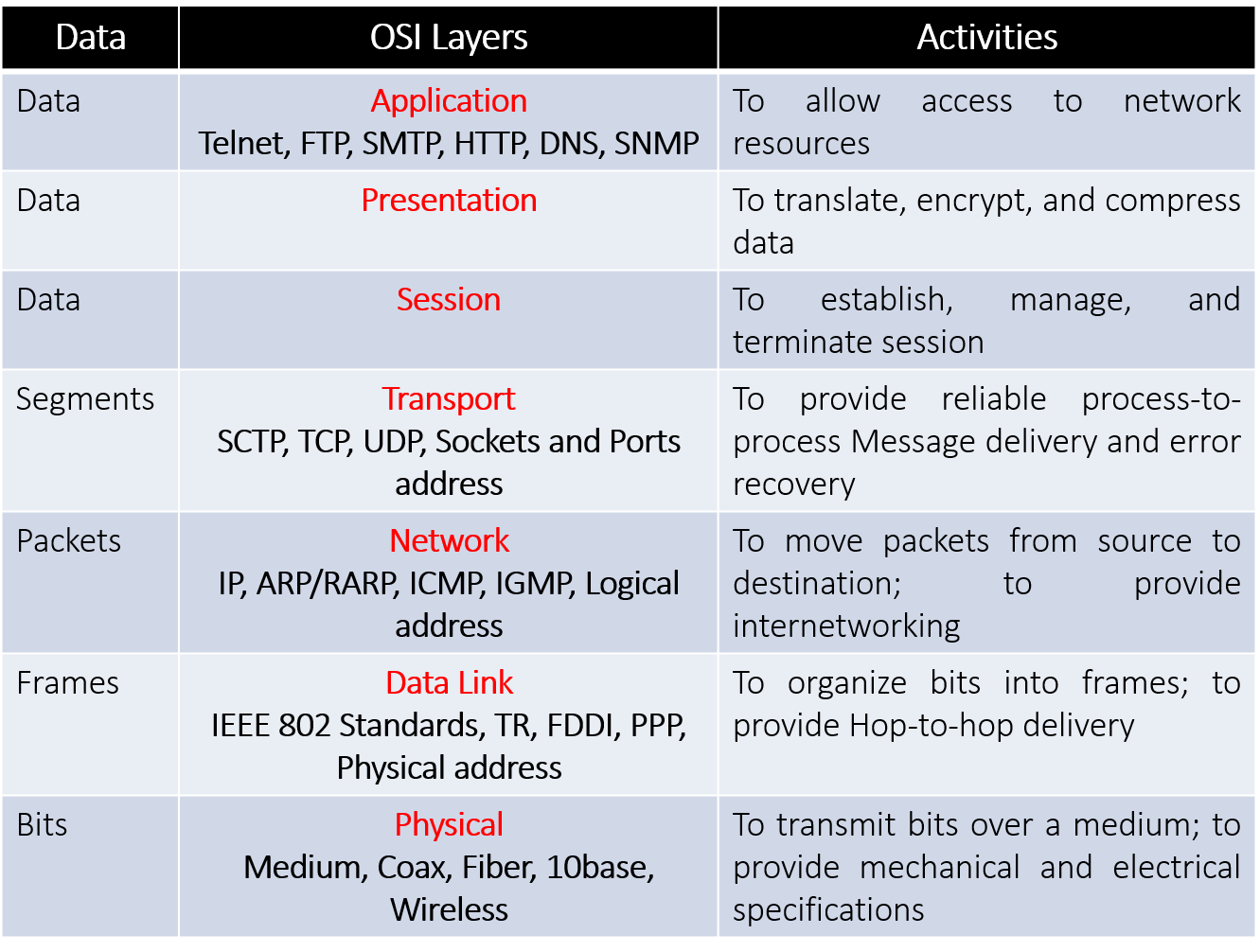
năng đã được cải tiến)

- Thông báo lại các bên ảnh hưởng bởi cuộc tấn công

Giai đoạn 8: Tài liệu hóa sự cố

• Ghi lại các dấu hiệu của sự cố.

64



• Ghi lại các luật IDS, Firewall, HIDS đã dùng để ngăn chặn, phát hiện sự cố.

• Ghi lại thông tin nhóm đã ứng cứu sự cố

• Ghi lại lý do đằng sau sự cố

Giai đoạn 9: Xem lại và cập nhật ứng phó sự cố

• Xem lại quy trình sau khi hoàn thành tài liệu và các bước khôi phục

• Thảo luận với các thành viên trong nhóm của bạn về các bước được triển

khai thành công và những sai lầm đã phạm

• Xem xét phản hồi và cập nhật chính sách sẽ làm giảm tác động của sự cố và

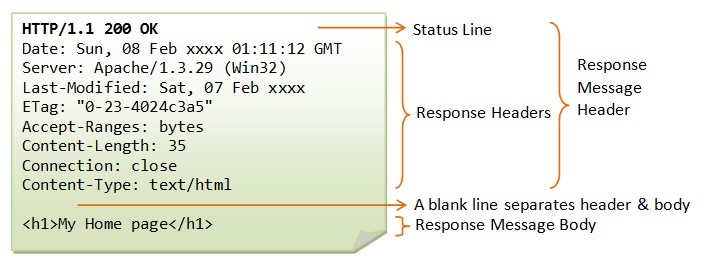
giúp xử lý các sự cố trong tương lai

# D. Bổ sung

- OSI Model:

- HTTP Request:

65



o Request-line = Phương thức+ URI request + HTTP version

o Phương thức: GET/POST/HEAD/PUT/DELETE/PATCH… -

- HTTP Response:

o Status-line = HTTP version + Mã trạng thái + trạng thái

o Mã trạng thái: 1xx: Thông tin; 2xx: Thành công ; 3xx: Sự điều

hướng lại ; 4xx: Lỗi phía Client ; 5xx: Lỗi phía Server.

- Test access point (TAP hay Inline TAP)

o Là 1 thiết bị phần cứng giúp sao chép chính xác và đầy đủ 100%

dữ liệu mạng đi qua Tap (liên tục 24/7) mà không không làm gián

đoạn hệ thống mạng.

o Các bản sao này có thể được dùng để “monitoring”, “security”

hoặc “analysis”. Taps có thể được đặt ở bất kỳ đâu trong hệ thống

mạng nơi mà bạn muốn sao chép dữ liệu mà không làm ảnh hưởng

đến cấu trúc hệ thống của bạn.

Ứng Phó sự cố gồm 4 bước:

1. Tiếp nhận sự cố (người dùng/khách hàng k truy cập được sẽ liên hệ đến đội

bảo mật)

- Người dùng phản ánh

- Cảnh bảo từ chương trình bảo mật (SIEM, IDS)

- Kiểm tra mạng

2. Phân tích sự cố

- Quy mô mức độ, nguồn gốc, cách thức thực hiện

- Địa chỉ IP

3. Xử lí sự cố

- Cách ly, ngăn chặn, khôi phục

4. Tổng kết

TH1: UPSC PC bị nhiễm mã độc tống tiền

66

B1: Dấu hiệu dữ liệu bị mã hóa, mất quyền điều khiển, giao diện hiển thị, nghẽn

mạng

B2: Phân tích xác định được mã độc

- Quy mô: Toàn bộ (xem xét)

- Mức độ: DL, CSDL, Source code

- Cách thức hoạt động : loại mã độc

- Phân tích IP nguồn đích

B3: Xử lí

- Cách ly, phân vùng, khôi phục lại DL, xóa bỏ( backup)

B4: Tổng kết:

- Nguyên nhân

- Kinh nghiệm: Tăng cường bảo mật, giám sát HT, nâng cao nhận thức

người dùng, quy trình sao lưu,

- Dữ liệu sao lưu: Local server, remote server, cloud, SAN( StogareArea

Nẻtwork)

TH2: UPSC khi web server bị tấn công DDOS

B1: Dấu hiệu : Người dung truy cập thất bại

- Cảnh báo từ HT bảo mật, nghẽn mạng

B2: Phân tích

- Quy mô: Số MT tấn công

- Mức độ nghiêm trọng

- Phân tích nguồn và đích tấn công giao thức sử dụng ICMP, UDP,

SYN(TCP), HTTP

- Thời gian: từ log sự kiện

B3: Xử lý

- Liện hệ ISP, kiểm soát băng thông

- Liên hệ tổ chức VNCERT

- Cấu hình mạng ngăn chặn (1 phần)

- Giám sát băng thông mạng, tốc độ internet ổn định không nhanh hay

chậm, có chập chờn không

B4: Tổng kết:

- Nguyên nhân

67

- Chiến lược ứng phó, hấp thụ (cân bằng tải)

- Tắt các dịch vụ không cần thiết

# Kịch bản trong NIST SP – 800:

- Preparation (Chuẩn bị) -> Phát hiện và phân tích -> Ngăn chặn, Loại bỏ

và phục hồi -> Hoạt động sau sự cố

# Scenario 1: Domain Name System (DNS) Server Denial of Service (DoS)

Kịch bản này mô tả một cuộc tấn công từ chối dịch vụ (DoS) nhắm vào máy chủ

DNS của tổ chức. Cuộc tấn công bắt đầu vào một buổi chiều thứ Bảy khi người

dùng bên ngoài gặp sự cố khi truy cập các trang web công cộng của tổ chức. Trong

vòng một giờ tiếp theo, tình trạng trở nên tồi tệ đến mức gần như mọi yêu cầu truy

cập đều thất bại. Trong khi đó, một thành viên của nhóm mạng của tổ chức phản

ứng lại các cảnh báo từ router biên Internet và xác định rằng băng thông Internet

của tổ chức đang bị tiêu thụ bởi một lượng lớn các gói tin User Datagram Protocol

(UDP) đi và đến từ cả hai máy chủ DNS công cộng của tổ chức. Phân tích lưu

lượng cho thấy rằng các máy chủ DNS đang nhận được số lượng lớn các yêu cầu

từ một địa chỉ IP bên ngoài duy nhất. Ngoài ra, tất cả các yêu cầu DNS từ địa chỉ

đó đều đến từ cổng nguồn giống nhau.

1. Tổ chức nên liên hệ với nhà cung cấp dịch vụ Internet (ISP) để báo cáo về

địa chỉ IP bên ngoài gây ra vấn đề. ISP có thể hỗ trợ trong việc phát hiện và

chặn lưu lượng độc hại từ nguồn này.

2. Nếu sau khi các biện pháp kiểm soát ban đầu được áp dụng, các quản trị

mạng phát hiện ra rằng có chín máy chủ nội bộ cũng đang cố gắng thực hiện

các yêu cầu không bình thường đến máy chủ DNS, điều này sẽ ảnh hưởng

đến việc xử lý sự cố. Sự hiện diện của các máy chủ nội bộ này có thể chỉ ra

rằng tổ chức đang chịu tác động của một cuộc tấn công từ bên trong, có thể

là do một máy tính trong mạng bị nhiễm malware hoặc bị chiếm đoạt.

3. Nếu hai trong số chín máy chủ nội bộ này đã ngắt kết nối khỏi mạng trước

khi chủ sở hữu hệ thống của họ được xác định, việc xác định chủ sở hữu hệ

thống sẽ phụ thuộc vào việc xem xét các dấu vết và thông tin liên quan,

chẳng hạn như log hệ thống, các yêu cầu địa chỉ IP từ DHCP server, hoặc sử

dụng công cụ quản lý mạng để xác định các thiết bị đã được kết nối vào

mạng trong khoảng thời gian tấn công.

# Scenario 2: Worm and Distributed Denial of Service (DDoS) Agent Infestation

Kịch bản này mô tả về sự lan truyền của một loại worm mới thông qua các phương

tiện di động và có khả năng sao chép chính nó vào các Windows shares mở. Khi

worm xâm nhập vào một máy chủ, nó cài đặt một đại lý DDoS. Tổ chức đã phải

chịu sự lan truyền rộng rãi của các lây nhiễm trước khi các chữ ký antivirus trở nên

68

khả dụng vài giờ sau khi worm bắt đầu lan truyền.

1. Đội phản ứng sự cố sẽ có thể xác định tất cả các máy chủ bị nhiễm bằng

cách sử dụng các công cụ giám sát mạng và hệ thống, phân tích các log, và

triển khai các công cụ quét và diệt malware trên toàn bộ hạ tầng mạng của tổ

chức.

2. Tổ chức có thể cố gắng ngăn chặn sự lan truyền của worm vào tổ chức trước

khi các chữ ký antivirus được phát hành bằng cách tăng cường biện pháp an

ninh mạng như cập nhật các tường lửa và hệ thống phát hiện xâm nhập

(IDS/IPS), hạn chế quyền truy cập vào các Windows shares, và triển khai

các biện pháp an ninh cứng rắn như firewall.

3. Tổ chức có thể cố gắng ngăn chặn sự lan truyền của worm bằng cách tăng

cường biện pháp an ninh mạng như cắt kết nối mạng của các máy nhiễm,

hạn chế quyền truy cập vào các tài nguyên mạng chia sẻ, và cảnh báo nhân

viên về nguy cơ và các biện pháp phòng ngừa.

4. Tổ chức có thể cố gắng vá lỗ hổng trên tất cả các máy chủ có thể bị tổn

thương bằng cách triển khai các bản vá và cập nhật bảo mật từ các nhà cung

cấp phần mềm.

5. Nếu các máy chủ nhiễm phải nhận được đại lý DDoS và được cấu hình để

tấn công một trang web của tổ chức khác vào sáng hôm sau, xử lý của sự cố

sẽ phải tập trung vào ngăn chặn tấn công này, bao gồm cả việc liên hệ với tổ

chức bị tấn công để cảnh báo và hợp tác trong việc ngăn chặn tấn công.

6. Nếu một hoặc nhiều trong số các máy chủ nhiễm chứa thông tin nhạy cảm

về nhân viên của tổ chức, xử lý của sự cố sẽ phải tập trung vào việc ngăn

chặn việc tiếp cận và lợi dụng thông tin này bằng cách cập nhật các biện

pháp an ninh mạng và thông tin, cũng như báo cáo vụ việc cho cơ quan quản

lý dữ liệu.

7. Đội phản ứng sự cố sẽ thông báo cho người dùng trong tổ chức về tình trạng

của sự cố thông qua các kênh liên lạc như email, tin nhắn nội bộ, và thông

báo trên trang web hoặc intranet của tổ chức.

8. Đối với các máy chủ không kết nối mạng vào thời điểm sự cố xảy ra, đội

phản ứng sự cố có thể cập nhật và triển khai các biện pháp bảo mật khi nhân

viên kết nối lại với mạng, hoặc thông qua các cập nhật từ xa nếu có khả

năng.

# Scenario 3: Stolen Documents

Kịch bản này mô tả về một cuộc gọi từ Cục Điều tra Liên bang (FBI) với phòng

pháp lý của tổ chức vào một buổi sáng thứ Hai, thông báo về một số hoạt động

đáng ngờ liên quan đến hệ thống của tổ chức. Sau đó trong ngày, một đặc vụ của

FBI gặp gỡ các thành viên của ban quản lý và phòng pháp lý để thảo luận về hoạt

động đó. FBI đã đang điều tra về việc đăng công khai các tài liệu chính phủ nhạy

cảm, và một số tài liệu được cho là thuộc sở hữu của tổ chức. Đặc vụ yêu cầu sự hỗ

69

trợ của tổ chức, và ban quản lý yêu cầu sự hỗ trợ của đội phản ứng sự cố để thu

thập bằng chứng cần thiết để xác định xem các tài liệu này có hợp lệ hay không và

chúng có thể đã bị rò rỉ như thế nào.

1. Đội phản ứng sự cố có thể thu thập bằng chứng từ nhiều nguồn khác nhau,

bao gồm log hệ thống, log mạng, các tập tin và thư mục trên hệ thống, cũng

như các ghi chú, email và tài liệu nội bộ của tổ chức.

2. Để giữ cho cuộc điều tra được giữ bí mật, đội phản ứng sự cố sẽ thực hiện

các biện pháp an ninh như mã hóa các tập tin, hạn chế quyền truy cập vào

thông tin liên quan chỉ đến những người cần biết và thông báo nghiêm túc về

việc giữ bí mật cho tất cả các thành viên tham gia trong cuộc điều tra.

3. Nếu đội phát hiện ra một máy chủ nội bộ có trách nhiệm cho việc rò rỉ thông

tin, xử lý của cuộc điều tra sẽ chuyển sang tập trung vào việc xác định

nguyên nhân và xử lý vấn đề tại nguồn gốc của rò rỉ thông tin, bao gồm cả

việc đưa ra biện pháp phòng ngừa để ngăn chặn việc tương tự xảy ra trong

tương lai.

4. Nếu đội phát hiện một rootkit được cài đặt trên máy chủ nội bộ có trách

nhiệm cho việc rò rỉ thông tin, xử lý của cuộc điều tra sẽ phải mở rộng để

loại bỏ rootkit, xác định thiệt hại đã gây ra, và thực hiện các biện pháp khôi

phục và tăng cường bảo mật để ngăn chặn việc tương tự xảy ra trong tương

lai.

# Scenario 4: Compromised Database Server

Kịch bản này mô tả về việc một quản trị cơ sở dữ liệu thực hiện bảo dưỡng ngoài

giờ trên một số máy chủ cơ sở dữ liệu sản xuất vào một đêm thứ Ba. Quản trị viên

nhận thấy một số tên thư mục không quen thuộc và bất thường trên một trong các

máy chủ. Sau khi xem xét danh sách thư mục và xem một số tệp, quản trị viên kết

luận rằng máy chủ đã bị tấn công và gọi đội phản ứng sự cố để được hỗ trợ. Cuộc

điều tra của đội phản ứng sự cố xác định rằng kẻ tấn công đã thành công trong việc

có quyền truy cập root vào máy chủ sáu tuần trước.

1. Đội phản ứng sự cố có thể sử dụng nhiều nguồn thông tin để xác định thời

điểm xâm nhập đã xảy ra, bao gồm log hệ thống, log mạng, và thông tin về

các hoạt động của quản trị viên trên máy chủ cũng như các tập tin và thư

mục mới được tạo hoặc sửa đổi.

2. Nếu đội phát hiện ra rằng máy chủ cơ sở dữ liệu đã chạy một chương trình

bắt gói và ghi lại mật khẩu từ mạng, xử lý của cuộc điều tra sẽ cần tập trung

vào việc đánh giá và xử lý hậu quả của việc này, bao gồm cả việc đổi mật

khẩu và triển khai các biện pháp bảo mật mạng để ngăn chặn việc tiếp tục

mất mát dữ liệu.

3. Nếu đội phát hiện ra rằng máy chủ đang chạy một tiến trình sẽ sao chép một

cơ sở dữ liệu chứa thông tin khách hàng nhạy cảm (bao gồm thông tin cá

70

nhân có thể xác định được) hàng đêm và chuyển nó đến một địa chỉ bên

ngoài, xử lý của cuộc điều tra sẽ phải tập trung vào việc ngăn chặn và kiểm

soát việc tiếp tục rò rỉ thông tin, bao gồm cả việc báo cáo vụ việc cho cơ

quan quản lý dữ liệu và các cơ quan pháp luật.

4. Nếu đội phát hiện ra một rootkit trên máy chủ, xử lý của cuộc điều tra sẽ

phải mở rộng để loại bỏ rootkit, xác định thiệt hại đã gây ra, và triển khai

các biện pháp phục hồi và củng cố bảo mật để ngăn chặn việc tương tự xảy

ra trong tương lai.

# Scenario 5: Unknown Exfiltration

Kịch bản này mô tả về việc một trong các cảm biến phát hiện xâm nhập mạng của

tổ chức phát hiện ra hoạt động mạng ra lạ và không bình thường liên quan đến việc

truyền tải tập tin lớn. Một nhà phân tích xâm nhập xem xét các cảnh báo; có vẻ như

hàng nghìn tệp .RAR đang được sao chép từ một máy chủ nội bộ đến một máy chủ

bên ngoài, và máy chủ bên ngoài này nằm ở một quốc gia khác. Nhà phân tích liên

lạc với đội phản ứng sự cố để họ có thể điều tra thêm về hoạt động này. Tuy nhiên,

đội không thể xem nội dung của các tệp .RAR vì chúng được mã hóa. Phân tích

máy chủ nội bộ chứa các tệp .RAR cho thấy có dấu hiệu của việc cài đặt bot.

1. Đội phản ứng sự cố có thể sử dụng các kỹ thuật phân tích tệp để đoán đoán

những gì có thể nằm bên trong các tệp .RAR, bao gồm việc xem xét các tiêu

đề, tìm kiếm các tập tin metadata và xác định các dấu hiệu của loại tệp. Đội

cũng có thể nhờ sự hỗ trợ của các nhóm an ninh mạng, các chuyên gia mã

hóa, hoặc các đơn vị phân tích malware để giúp giải mã và phân tích nội

dung của các tệp .RAR.

2. Nếu đội phản ứng sự cố xác định rằng sự tấn công ban đầu đã được thực

hiện thông qua một thẻ mạng không dây trên máy chủ nội bộ, đội sẽ tiếp tục

điều tra bằng cách kiểm tra lịch sử kết nối mạng của thiết bị, kiểm tra cấu

hình mạng và kiểm tra các lỗ hổng bảo mật trong hạ tầng mạng của tổ chức.

Nếu đội phản ứng sự cố xác định rằng máy chủ nội bộ đang được sử dụng để chuẩn

bị các tệp nhạy cảm từ các máy chủ khác trong doanh nghiệp, đội sẽ tiếp tục điều

tra bằng cách kiểm tra quyền truy cập và hoạt động của người dùng trên máy chủ,

xem xét các kết nối mạng đến và từ máy chủ, và kiểm tra các hoạt động không

bình thường hoặc đáng ngờ trên máy chủ.

# Scenario 6: Unauthorized Access to Payroll Records

Kịch bản này mô tả về việc một nhân viên quản lý lương nhận được một cuộc gọi

từ nhóm an ninh vật lý của tổ chức vào một tối thứ Tư. Người quản lý lương thấy

một người lạ rời khỏi văn phòng của mình, chạy xuống hành lang và rời khỏi tòa

nhà. Người quản lý lương đã để lại máy tính của mình mở và không có người trông

coi chỉ trong vài phút. Chương trình lương vẫn đăng nhập và hiển thị trên menu

chính, như khi cô rời đi, nhưng người quản lý lương nhận thấy con chuột dường

71

như đã được di chuyển. Đội phản ứng sự cố đã được yêu cầu thu thập bằng chứng

liên quan đến sự việc và xác định những hành động đã được thực hiện.

1. Đội phản ứng sự cố có thể xác định các hành động đã được thực hiện bằng

cách kiểm tra lịch sử hoạt động trên máy tính của người quản lý lương, kiểm

tra các tệp đã được mở hoặc sửa đổi, kiểm tra các hoạt động mạng như truy

cập vào hệ thống hay chuyển tệp, và phân tích các thông tin từ các cảm biến

an ninh vật lý.

2. Nếu người quản lý lương nhận ra người rời khỏi văn phòng của mình là một

cựu nhân viên của bộ phận lương, xử lý của sự cố có thể tập trung vào việc

xác định mục đích và động cơ của cựu nhân viên, cũng như xác định xem

liệu có dấu hiệu của hoạt động bất thường nào từ trước đó hay không.

3. Nếu đội có lý do để tin rằng người đó là một nhân viên hiện tại, xử lý của sự

cố có thể tập trung vào việc xác định nguyên nhân và xử lý nội bộ, cũng như

thực hiện các biện pháp bảo mật để ngăn chặn việc tái diễn.

4. Nếu nhóm an ninh vật lý xác định rằng người đó đã sử dụng kỹ thuật kỹ

nghệ xã hội để có quyền truy cập vật lý vào tòa nhà, xử lý của sự cố sẽ tập

trung vào việc cải thiện và mở rộng biện pháp bảo mật vật lý và huấn luyện

nhân viên về an ninh.

5. Nếu các log từ tuần trước cho thấy một số lượng lớn các lần đăng nhập từ xa

không thành công sử dụng ID người quản lý lương, xử lý của sự cố có thể

tập trung vào việc kiểm tra và bảo vệ hệ thống đăng nhập từ xa, bao gồm cả

việc cập nhật mật khẩu và triển khai các biện pháp an ninh mạng.

6. Nếu đội phát hiện ra rằng một keystroke logger đã được cài đặt trên máy

tính hai tuần trước, xử lý của sự cố sẽ phải tập trung vào việc xác định và

loại bỏ phần mềm độc hại, kiểm tra và cải thiện an ninh của hệ thống và dữ

liệu, cũng như cập nhật quy trình và biện pháp bảo mật để ngăn chặn việc

tương tự xảy ra trong tương lai.

# Scenario 7: Disappearing Host

Vào một buổi chiều thứ Năm, một cảm biến phát hiện xâm nhập mạng ghi lại hoạt

động quét lỗ hổng được thực hiện đối với các máy chủ nội bộ, được tạo ra bởi một

địa chỉ IP nội bộ. Do nhà phân tích phát hiện xâm nhập không biết về bất kỳ hoạt

động quét lỗ hổng được ủy quyền hoặc lên lịch trình nào, cô ấy báo cáo hoạt động

này cho đội phản ứng sự cố. Khi đội bắt đầu phân tích, họ phát hiện rằng hoạt động

đã dừng lại và không còn một máy chủ nào sử dụng địa chỉ IP nữa.

1. Các nguồn dữ liệu có thể chứa thông tin về danh tính của máy chủ thực hiện

hoạt động quét lỗ hổng có thể bao gồm các log của cảm biến phát hiện xâm

nhập mạng, log của máy chủ mạng, và log của các thiết bị bảo mật khác như

tường lửa hoặc hệ thống giám sát mạng.

2. Đội có thể xác định ai đã thực hiện các quét lỗ hổng bằng cách kiểm tra các

tài khoản được sử dụng để đăng nhập vào hệ thống hoặc kiểm tra bất kỳ máy

72

tính hoặc thiết bị nào có dấu vết của các công cụ quét lỗ hổng.

3. Nếu hoạt động quét lỗ hổng được hướng vào các máy chủ quan trọng nhất

của tổ chức, xử lý sự cố có thể trở nên ưu tiên hơn, với việc tăng cường giám

sát và phân tích chi tiết để đảm bảo rằng không có lỗ hổng nào được tận

dụng.

4. Nếu hoạt động quét lỗ hổng được hướng vào các máy chủ bên ngoài, đội

phản ứng sự cố có thể cần hợp tác với các bên liên quan bên ngoài tổ chức

để giải quyết vấn đề và định rõ nguồn gốc và mục tiêu của hoạt động này.

5. Nếu địa chỉ IP nội bộ được liên kết với mạng khách không dây của tổ chức,

việc xử lý sự cố có thể đòi hỏi kiểm tra và tăng cường bảo mật của mạng

không dây, cũng như kiểm tra quy trình xác thực và phân quyền truy cập.

6. Nếu nhân viên an ninh vật lý phát hiện ra rằng có người đã đột nhập vào cơ

sở vật chất nửa giờ trước khi hoạt động quét lỗ hổng xảy ra, đội phản ứng sự

cố sẽ phải tập trung vào việc điều tra và giải quyết cả hai sự kiện, có thể kết

hợp thông tin từ cả hai nguồn để xác định mối liên kết và tác động của

chúng.

# Scenario 8: T elecommuting Compromise

Vào một buổi tối thứ Bảy, phần mềm phát hiện xâm nhập mạng ghi lại một kết nối

đến từ một địa chỉ IP nằm trong danh sách theo dõi. Nhà phân tích phát hiện xâm

nhập xác định rằng kết nối đang được thực hiện đến máy chủ VPN của tổ chức và

liên hệ với đội phản ứng sự cố. Đội xem lại các log phát hiện xâm nhập, tường lửa

và máy chủ VPN và xác định ID người dùng đã được xác thực cho phiên và tên

của người dùng được liên kết với ID người dùng đó.

1. Bước tiếp theo của đội nên là gì (ví dụ: gọi người dùng tại nhà, vô hiệu hóa

ID người dùng, ngắt kết nối phiên VPN)? Tại sao bước này nên được thực

hiện đầu tiên? Bước tiếp theo nào nên được thực hiện sau đó?

● Bước tiếp theo của đội nên là ngắt kết nối phiên VPN và vô hiệu hóa

ID người dùng. Điều này cần được thực hiện đầu tiên để ngăn chặn

tiếp tục truy cập trái phép vào hệ thống. Bước tiếp theo sẽ là liên hệ

với người dùng để xác nhận xem liệu kết nối này có được thực hiện

một cách hợp lệ hay không và để thông báo về việc xảy ra sự cố.

2. Xử lý của sự cố sẽ khác đi nếu địa chỉ IP bên ngoài thuộc về một proxy mở.

Trong trường hợp này, việc xác định người dùng thực sự đứng sau kết nối sẽ

trở nên phức tạp hơn vì dữ liệu IP đầu vào sẽ được giấu đi thông qua proxy.

3. Nếu ID đã được sử dụng để khởi tạo các kết nối VPN từ một số địa chỉ IP

bên ngoài mà không có sự chấp nhận từ phía người dùng, đội phản ứng sự

cố sẽ cần tăng cường giám sát và kiểm soát truy cập vào hệ thống, và cần

phải kiểm tra xem liệu ID đã bị chiếm đoạt hay không.

4. Nếu máy tính của người dùng đã bị chiếm đoạt bởi một trò chơi chứa mã

độc Trojan được tải xuống bởi một thành viên trong gia đình, điều này sẽ

ảnh hưởng đến phân tích của đội về sự cố. Họ sẽ cần kiểm tra xem liệu có

73

dấu hiệu của một cuộc tấn công mục tiêu hoặc là một vụ việc ngẫu nhiên.

Trong việc thu thập và xử lý bằng chứng, họ sẽ cần phải tìm kiếm dấu vết

của mã độc Trojan và xác định cách thức chiếm quyền kiểm soát của nó. Đối

với việc loại bỏ sự cố từ máy tính của người dùng, đội cần phải loại bỏ hoàn

toàn mã độc Trojan và triển khai biện pháp bảo mật bổ sung để ngăn chặn sự

truy cập trái phép vào máy tính.

5. Nếu người dùng cài đặt phần mềm diệt virus và xác định rằng mã độc Trojan

đã bao gồm một bộ ghi lại phím, điều này sẽ ảnh hưởng đến việc xử lý sự

cố. Nếu người dùng là một quản trị hệ thống, việc này có thể yêu cầu các

biện pháp bổ sung để xác minh tính toàn vẹn của hệ thống và dữ liệu. Nếu

người dùng là một cấp cao trong tổ chức, việc này có thể dẫn đến một cuộc

điều tra sâu sắc hơn và một số biện pháp bảo mật cao cấp được triển khai để

đảm bảo an ninh của thông tin quan trọng.

# Scenario 9: Anonymous Threat

Vào một buổi chiều thứ Năm, nhóm an ninh vật lý của tổ chức nhận được một cuộc

gọi từ một quản lý IT, báo cáo rằng hai nhân viên của cô vừa nhận được các mối đe

dọa ẩn danh đối với hệ thống của tổ chức. Dựa trên cuộc điều tra, nhóm an ninh vật

lý tin rằng các mối đe dọa nên được đối phó một cách nghiêm túc và thông báo cho

các nhóm nội bộ phù hợp, bao gồm cả đội phản ứng sự cố, về những mối đe dọa

này.

1. Đội phản ứng sự cố có thể cần thực hiện một số biện pháp khác biệt trong

phản ứng với thông báo về các mối đe dọa. Đầu tiên, họ có thể cần tiến hành

một cuộc phân tích sâu hơn về nguồn gốc và tính nghiêm trọng của các đe

dọa này. Sau đó, họ cần tăng cường giám sát và bảo mật hệ thống để đảm

bảo rằng không có hành động xâm nhập nào được thực hiện và hệ thống

được bảo vệ tốt hơn trước nguy cơ.

2. Việc tăng cường các biện pháp an ninh vật lý có thể ảnh hưởng đến cách

thức đội phản ứng sự cố xử lý các sự cố. Các biện pháp an ninh vật lý có thể

làm giảm khả năng của kẻ tấn công tiếp cận vật lý vào hệ thống, nhưng cũng

có thể làm giảm khả năng của nhóm phản ứng sự cố trong việc thu thập bằng

chứng hoặc tiến hành các cuộc điều tra trực tiếp. Do đó, đội phản ứng sự cố

có thể cần phải điều chỉnh kế hoạch và phương pháp làm việc của họ để đảm

bảo rằng họ vẫn có thể hoạt động hiệu quả trong một môi trường với các

biện pháp an ninh vật lý được tăng cường.

# Scenario 10: Peer-to-Peer File Sharing

Tổ chức đã cấm việc sử dụng các dịch vụ chia sẻ file ngang hàng. Các cảm biến

phát hiện xâm nhập mạng của tổ chức đã được kích hoạt chữ ký có thể phát hiện

việc sử dụng một số dịch vụ chia sẻ file ngang hàng phổ biến. Vào một buổi tối thứ

Hai, một nhà phân tích phát hiện xâm nhập nhận thấy rằng một số cảnh báo chia sẻ

file đã xảy ra trong vòng ba giờ qua, tất cả đều liên quan đến cùng một địa chỉ IP

74

nội bộ.

1. Các yếu tố sau đây nên được sử dụng để ưu tiên xử lý sự cố này:

● Nội dung rõ ràng của các tập tin đang được chia sẻ: Nếu nội dung của

các tập tin có vẻ như là thông tin nhạy cảm hoặc bí mật, sự cố có thể

được ưu tiên xử lý để ngăn chặn sự tiếp tục phát tán thông tin không

được ủy quyền.

● Quy mô và tần suất của các hoạt động chia sẻ file: Nếu có nhiều cảnh

báo và các hoạt động chia sẻ file diễn ra ở quy mô lớn, sự cố có thể

được coi là nghiêm trọng hơn và cần được xử lý ngay lập tức để ngăn

chặn việc tiếp tục sử dụng dịch vụ chia sẻ file ngang hàng.

2. Các yếu tố về quyền riêng tư có thể ảnh hưởng đến cách xử lý sự cố:

● Quyền riêng tư của người sử dụng: Việc thu thập và xử lý dữ liệu về

các hoạt động mạng của người sử dụng có thể vi phạm quyền riêng tư

của họ. Cần phải cân nhắc cẩn thận để đảm bảo tuân thủ các quy định

về quyền riêng tư và bảo vệ dữ liệu cá nhân.

● Sự cân nhắc giữa quyền riêng tư và bảo mật: Cần phải cân nhắc kỹ

lưỡng giữa việc thu thập thông tin để bảo vệ hệ thống và việc bảo vệ

quyền riêng tư của cá nhân.

3. Xử lý sự cố sẽ khác nhau nếu máy tính thực hiện chia sẻ file ngang hàng

cũng chứa thông tin nhạy cảm về cá nhân. Trong trường hợp này, sự cố sẽ

cần được xử lý một cách cẩn thận hơn để đảm bảo rằng thông tin nhạy cảm

không bị rò rỉ hoặc bị truy cập trái phép. Cần triển khai các biện pháp bảo

mật bổ sung để bảo vệ thông tin nhạy cảm và cân nhắc kỹ lưỡng hơn về

quyền riêng tư của người dùng trong quá trình xử lý sự cố.

# Scenario 11: Unknown Wireless Access Point

Vào một buổi sáng thứ Hai, bộ phận hỗ trợ kỹ thuật của tổ chức nhận được cuộc

gọi từ ba người dùng trên cùng một tầng của một tòa nhà cho biết họ đang gặp vấn

đề với kết nối không dây của họ. Một quản trị mạng được yêu cầu hỗ trợ trong việc

giải quyết vấn đề mang theo một laptop có kết nối không dây đến tầng của người

dùng. Khi anh ấy kiểm tra cấu hình mạng không dây của mình, anh ấy nhận thấy

có một điểm truy cập mới được liệt kê là có sẵn.Anh ấy kiểm tra với đồng đội của

mình và kết luận rằng điểm truy cập này không được triển khai bởi nhóm của anh

ấy, vì vậy nó có thể là một điểm truy cập giả mạo được thiết lập mà không có sự

cho phép.

1. Bước quan trọng đầu tiên trong việc xử lý sự cố này là xác định vị trí của

điểm truy cập giả mạo. Điều này có thể được thực hiện bằng cách tìm vị trí

vật lý của điểm truy cập hoặc kết nối logic đến điểm truy cập.

2. Cách nhanh nhất để định vị điểm truy cập là sử dụng các công cụ quét mạng

không dây hoặc phần mềm quét để xác định vị trí cụ thể của nó trên mạng.

Cách tiếp cận tinh vi nhất là theo dõi tín hiệu từ điểm truy cập và điều tra

75

các yếu tố gần nó để xác định vị trí một cách chính xác.

3. Xử lý sự cố sẽ khác nhau nếu điểm truy cập đã được triển khai bởi một bên

bên ngoài (ví dụ: nhà thầu) tạm thời làm việc tại văn phòng của tổ chức.

Trong trường hợp này, quá trình xác minh và giao tiếp với bên triển khai sẽ

là bước quan trọng để hiểu rõ hơn về mục đích và cơ sở pháp lý của điểm

truy cập.

4. Xử lý sự cố sẽ khác biệt nếu một nhà phân tích phát hiện dấu hiệu của hoạt

động đáng ngờ liên quan đến một số máy trạm trên cùng một tầng của tòa

nhà. Trong trường hợp này, điều tra sẽ mở rộng để kiểm tra xem liệu có sự

kết nối giữa điểm truy cập giả mạo và các hoạt động đáng ngờ trên máy trạm

hay không.

5. Xử lý sự cố sẽ khác biệt nếu điểm truy cập đã bị gỡ bỏ trong khi nhóm vẫn

cố gắng định vị nó vật lý. Trong trường hợp này, quan trọng là ghi lại mọi

thông tin có thể về sự kiện và tiếp tục thực hiện các biện pháp bảo mật bổ

sung để ngăn chặn việc tái xảy ra và bảo vệ hệ thống.

chữ chân tình Coi nhau là anh em, đừng lúc vơi lúc đầy