

Câu 1:

Hệ thống giám sát an toàn thông tin (SIEM – Security information and event maagement) là hệ thống được thiết kế nhằm thu thập thông tin nhật ký sự kiện từ các thiết bị đầu cuối và phân tích chúng với mục đích phát hiện và kịp thời ứng phó, cho phép cơ quan/tổ chức hạn chế được các rủi ro, tiết kiệm thời gian và nhân lực.

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.

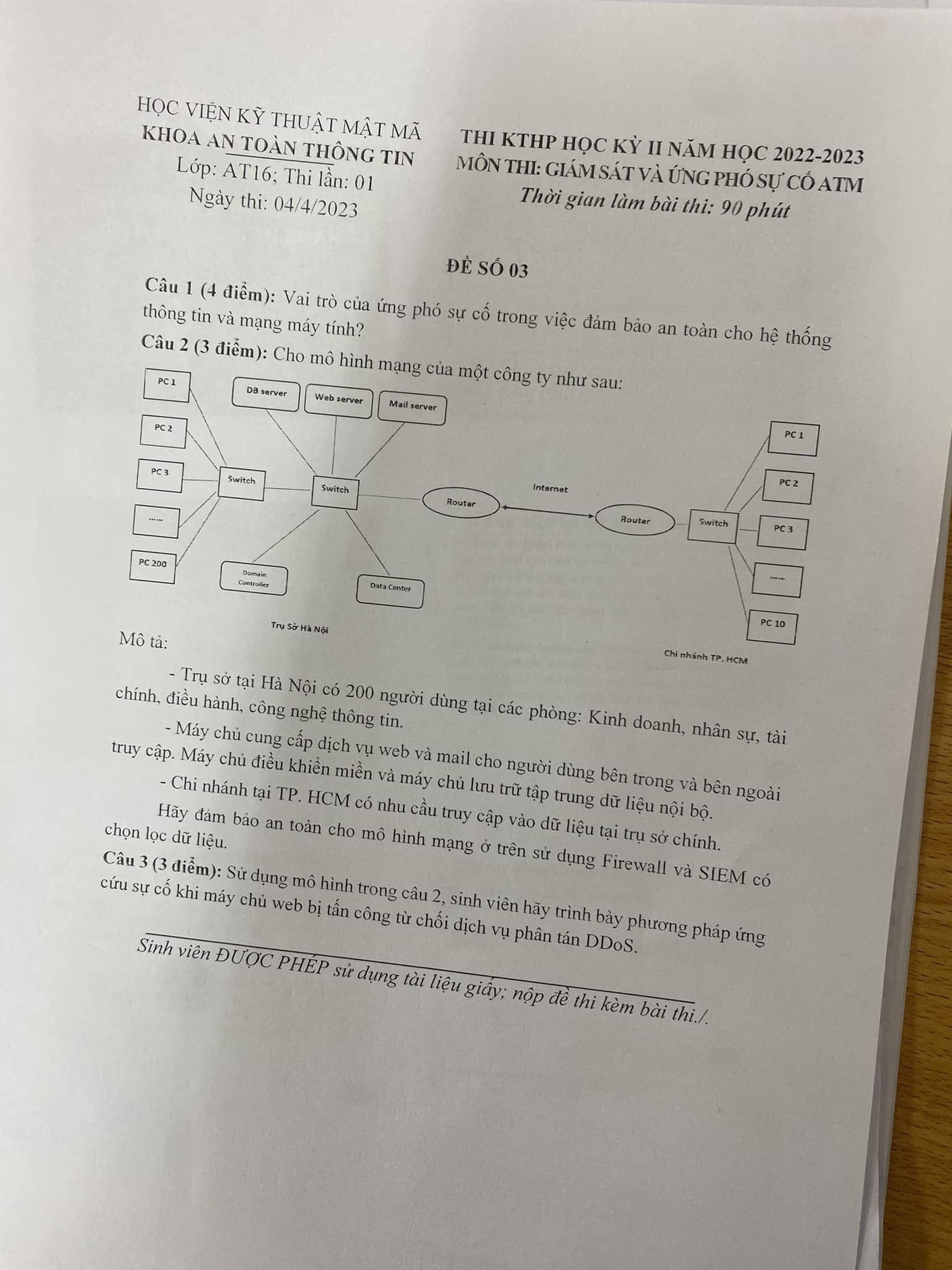
Đội ngũ ứng phó sự cố (Incident Response) thực hiện cách ly tất cả các máy có dấu hiệu bị lây nhiễm ra khỏi mạng nội bộ của công ty.

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.



**Câu 1: Vai trò của ứng phó sự cố**

Là một phần chính trong chiến lược an toàn thông tin tổng thể.

Ứng phó sự cố giúp giảm thiểu mất mát hoặc đánh cắp thông tin và gián đoạn dịch vụ do sự cố gây ra.

Hỗ trợ ứng phó với các sự cố một cách có hệ thống (tuân theo một phương pháp xử lý sự cố nhất quán) để thực hiện các hành động thích hợp.

Sử dụng thông tin thu được trong quá trình xử lý sựcố để chuẩn bị tốt hơn cho việc xử lý các sự cố trong tương lai và tăng cường khả năng bảo vệ cho hệ thống và dữ liệu

• Mục đích của ứng phó sự cố là hỗ trợ nhân viên khắc phục nhanh chóng và hiệu quả sau sự cố.

• Phản ứng sự cố được yêu cầu để xác định các cuộc tấn công đã xâm phạm thông tin hoặc dữ liệu cá nhân và doanh nghiệp.

• Phản ứng sự cố được yêu cầu nhằm mục đích

• Bảo vệ hệ thống

• Bảo vệ nhân viên

• Sử dụng hiệu quả các nguồn lực

• Giải quyết các vấn đề pháp lý

Kiểm tra sự cố

Giảm thiểu tác động của sự cố lên các cá nhân, tổ chức

Ngăn chặn các cuộc tấn công, sự cố trong tương lai

Tăng cường bảo mật hệ thống máy tính

Đảm bảo các quyền riêng tư được thiết lập bởi luật pháp và chính sách

Cung cấp các báo cáo chính xác và các khuyến nghị hữu ích

Hỗ trợ cơ quan thực thi pháp luật trong việc truy tố tội phạm kỹ thuật số

Bảo vệ danh tiếng và tài sản của tổ chức

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 (CND) 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.