Phạm Hồ Bình An\_1050080127\_10DH\_CNPM2

BÀI TẬP 6:

B. THỰC HÀNH

1. Tổng quan về xây dựng chính sách kiểm soát ứng dụng

Trong Sophos UTM, việc xây dựng các quy tắc kiểm soát các ứng dụng mạng được

thực hiện trong Web Protection > Application Control

Kiểm soát ứng dụng mạng

Để tiến hành thiết lập các quy tắc, cần bật Network visibility.

Tại đây còn cung cấp chức năng Flow Monitor cho phép theo dõi lưu lượng mạng

(network traffic) của các ứng dụng thông qua các card mạng theo thời gian thực.

Ảnh có chứa văn bản, ảnh chụp màn hình, số, Song song

Nội dung do AI tạo ra có thể không chính xác.

Theo dõi network traffic và chặn theo thời gian thực

Để thiết lập các quy tắc, ta thực hiện ở tab Application Control Rules.

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Trang web

Nội dung do AI tạo ra có thể không chính xác.

Xây dựng các chính sách cho các ứng dụng mạng

Khi xây dựng chính sách, có thể thực hiện chính sách kiểm soát (Control by) theo loại

ứng dụng (Applications) hoặc theo bộ lọc động (Dynamic filter) dựa theo đánh giá từ

Sophos về năng suất (Productivity) và độ nguy hiểm (Risk) của loại ứng dụng đó.

Ảnh có chứa văn bản, ảnh chụp màn hình, số, phần mềm

Nội dung do AI tạo ra có thể không chính xác.

Chọn loại danh mục và đánh giá ứng dụng để xây dựng quy tắc

Việc xây dựng các quy tắc tương tự các Web Filter Profiles.

2. Xây dựng bộ chính sách kiểm soát ứng dụng và triển khai CA (HTTPS)

Thiết lập các chính sách đảm bảo các yêu cầu sau:

Môi trường giả định:

Hệ thống mạng nội bộ xây dựng theo mô hình domain như đã xây dựng gồm 3 user:

Administrator (Quản trị), user a và b (tương ứng 2 user trong nhóm sinh viên đã tạo).

Máy người dùng sử dụng trình duyệt Chrome version 49.0 để truy cập Internet.

Thiết lập bộ Chính sách kiểm soát ứng dụng & giải quyết các vấn đề:

1. Khắc phục lỗi HTTPS khi truy cập web tại máy DC.

Gợi ý: Vào Web Protection > Filtering Options > tab HTTPS Cas > Tải Signing

CA và cài đặt vào Trusted Root Certification Authorities của máy DC.

Ảnh có chứa văn bản, Phông chữ, phần mềm, Trang web

Nội dung do AI tạo ra có thể không chính xác.

Tải về Signing CA và import vào máy DC

2. Cấm tất cả người dùng sử dụng các phương thức truyền tập tin qua Internet

bằng các website chia sẻ file (File transfer) như Mediafire.com, box.net

3. Cấm tất cả người dùng sử dụng giao thức truyền tập tin FTP, không cho

download Torrent.

4. Hạn chế người dùng sử dụng mạng xã hội: Cấm sử dụng Twitter, Google+.

Đối với Facebook cho truy cập nhưng cấm đăng status trên tường và nhắn tin trên

Facebook (nếu không thực hiện được thì cấm hẳn sử dụng Facebook).

5. Cấm sử dụng các chương trình thay đổi Proxy như Tor hay Ultrasuft

6. Cấm không cho sử dụng các email server (gmail, yahoo,...), ngoại trừ email

server của công ty, trong ví dụ này giả sử cho phép http://ctmail.vnu.edu.vn

(WebMail ĐH Công nghệ - ĐHQG-HN).

3. Kiểm tra kết quả & ứng dụng

Kiểm tra kết quả sau khi đã xây dựng bộ chính sách ở bước 2 với từng trường hợp

trong kịch bản kiểm tra tương ứng với các quy tắc ở phần 2 như sau, nếu chưa đúng

yêu cầu cần điều chỉnh lại chính sách:

1. Khi vào các website có https trên Chrome không còn xảy ra tình trạng bị cảnh

báo HTTPS

Ảnh có chứa văn bản, đồ điện tử, Trang web, Website

Nội dung do AI tạo ra có thể không chính xác.

Truy cập các website HTTPS bình thường

2. Không thể truy cập các website chia sẻ file như Mediafire, Dropbox, ...

Ảnh có chứa văn bản, phần mềm, Trang web, Website

Nội dung do AI tạo ra có thể không chính xác.

Không thể truy cập các website Dropbox, Mediafire, ...

3. Kiểm tra sử dụng giao thức FTP trước và sau khi áp dụng Rule.

Có thể sử dụng FileZilla đăng nhập qua FTP đến 1 FTP server free nào đó, sinh

viên cũng có thể sử dụng tài khoản mẫu sau đây để thử nghiệm:

FTP Server: ftp.iselab.16mb.com

User: u971091963.isedemo

Password: ise2016

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, hàng

Nội dung do AI tạo ra có thể không chính xác.

Kiểm tra giao thức FTP khi thực hiện Rule

Kiểm tra sử dụng uTorrent hay BitTorrent và download thông qua một tập tin

.torrent nào đó để kiểm tra kết quả.

4. Thử nghiệm khi truy cập và sử dụng với các Mạng xã hội phổ biến.

5. Thử nghiệm với Ultrasuft hay Tor và kiểm tra kết quả

Ảnh có chứa văn bản, ảnh chụp màn hình, màn hình, phần mềm

Nội dung do AI tạo ra có thể không chính xác.

Sử dụng Ultrasurf trước và sau khi thiết lập chính sách và kiểm tra kết quả

6. Kiểm tra kết quả khi truy cập gmail.com; mail.uit.edu.vn; ctmail.vnu.edu.vn