**Lab 1 - Phát hiện tấn công Brute-Force RDP Windows với Sysmon và Splunk**

**1. Mục tiêu**

* Mục tiêu của lab này là phát hiện, điều tra và phản ứng với các cuộc tấn công brute-force nhắm vào dịch vụ RDP trên máy Windows.
* Lab này sử dụng Sysmon và Splunk để giám sát các nỗ lực đăng nhập thất bại và thành công, đồng thời xác định các mẫu đáng ngờ cho thấy có cuộc tấn công.

**2. Sơ đồ mạng**

Ubuntu Server (Splunk Server): 192.168.56.105/24

Windows 10 (SplunkUniversalForwarder): 192.168.56.106/24

Kali (Attacker): 192.168.56.101/24

**3. Kiến thức nền**

* **RDP (Remote Desktop Protocol)**: Là giao thức độc quyền của Microsoft cho phép người dùng kết nối và điều khiển máy tính Windows từ xa qua mạng. Giao thức này sử dụng cổng TCP 3389 và hỗ trợ giao diện đồ họa, truyền clipboard, chia sẻ ổ đĩa,... Do tính chất truy cập từ xa, RDP thường là mục tiêu của các cuộc tấn công brute-force, khai thác lỗ hổng, hoặc tấn công dịch vụ nếu không được bảo vệ đúng cách.
* **Sysmon:** Là công cụ giám sát hệ thống nâng cao do Microsoft phát hành trong bộ Sysinternals, giúp ghi lại các sự kiện bảo mật chi tiết như tạo tiến trình, thay đổi file, kết nối mạng, và đặc biệt là các hành động liên quan đến Scheduled Tasks như tạo hoặc thực thi tác vụ. Với cấu hình phù hợp, Sysmon giúp phát hiện hành vi đáng ngờ mà các log mặc định của Windows có thể bỏ sót.
* **Splunk Universal Forwarder:** Là một lightweight agent được cài trên máy Windows (hoặc các hệ điều hành khác) để thu thập log theo thời gian thực và gửi về máy chủ Splunk. Trong môi trường giám sát bảo mật, nó thường được cấu hình để gửi log của Windows Event Log, Sysmon hoặc các file log tùy chỉnh về Splunk nhằm phục vụ việc phân tích tập trung.
* **Splunk:** Là một nền tảng SIEM mạnh mẽ hỗ trợ thu thập, tìm kiếm, phân tích, cảnh báo và trực quan hóa dữ liệu log từ nhiều nguồn. Với khả năng truy vấn linh hoạt bằng SPL (Search Processing Language), Splunk giúp các analyst nhanh chóng phát hiện các hành vi đáng ngờ, như việc tạo Scheduled Task bất thường hoặc hoạt động lateral movement, từ các log được gửi về.

**4. Các bước tiến hành**

**Bước 1: Chuẩn bị môi trường**

* Tải và cài đặt máy ảo Ubuntu Server 22.04 VMware Player.
  + Ubuntu Server: <https://releases.ubuntu.com/jammy/ubuntu-22.04.5-live-server-amd64.iso>
  + Kali Linux: <https://cdimage.kali.org/kali-2025.1a/kali-linux-2025.1a-vmware-amd64.7z>
* Thực hiện cài đặt, cấu hình Splunk Server trên Ubuntu Server và Splunk Universal Forwarder trên Windows theo hướng dẫn tại: <https://github.com/0xrajneesh/90-days-security-challenge/blob/main/Challenge%232/Lab%20Set%20up%20.md>

**Bước 2: Cài đặt Sysmon trên máy Windows**

1. **Tải Sysmon**

* Truy cập: <https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon>
* Tải file .zip về và giải nén (thường sẽ có Sysmon.exe và Sysmon64.exe)

1. **Tải file cấu hình Sysmon**

* Dùng mẫu cấu hình từ SwiftOnSecurity (rất phổ biến): <https://github.com/SwiftOnSecurity/sysmon-config>

-> Tải file sysmonconfig-export.xml.

1. **Cài đặt Sysmon**

* Mở **Command Prompt với quyền Administrator**, điều hướng đến thư mục chứa Sysmon, rồi chạy:

sysmon64.exe -i sysmonconfig-export.xml

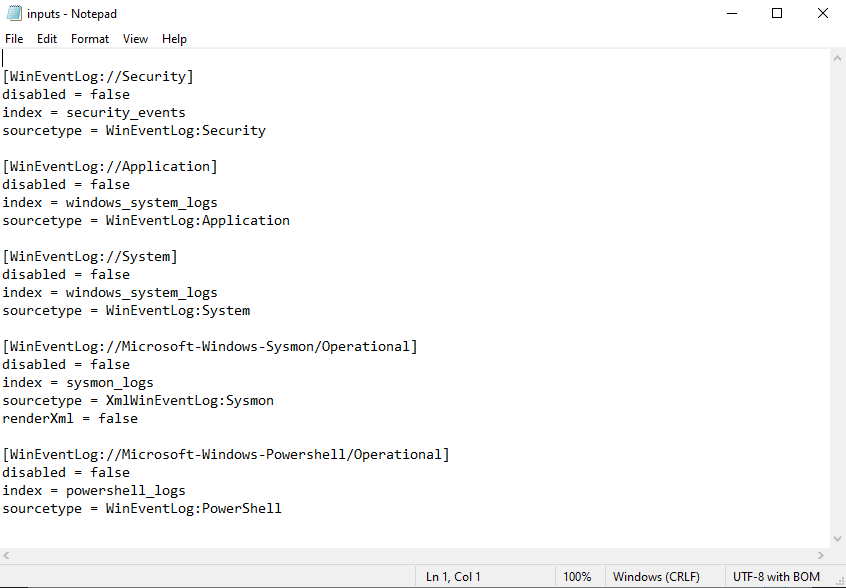
* Nếu thành công, Sysmon sẽ bắt đầu ghi lại các sự kiện vào Windows Event Log, mục **"Microsoft-Windows-Sysmon/Operational"**.
* **Kiểm tra:** Mở Event Viewer > Applications and Services Logs > Microsoft > Windows > Sysmon > Operational.

**Bước 3: Cấu hình Splunk Forwarder theo dõi và gửi log của Sysmon**

1. **Mở file inputs.conf của Splunk Forwarder**

C:\\Program Files\\SplunkUniversalForwarder\\etc\\system\\local\\inputs.conf

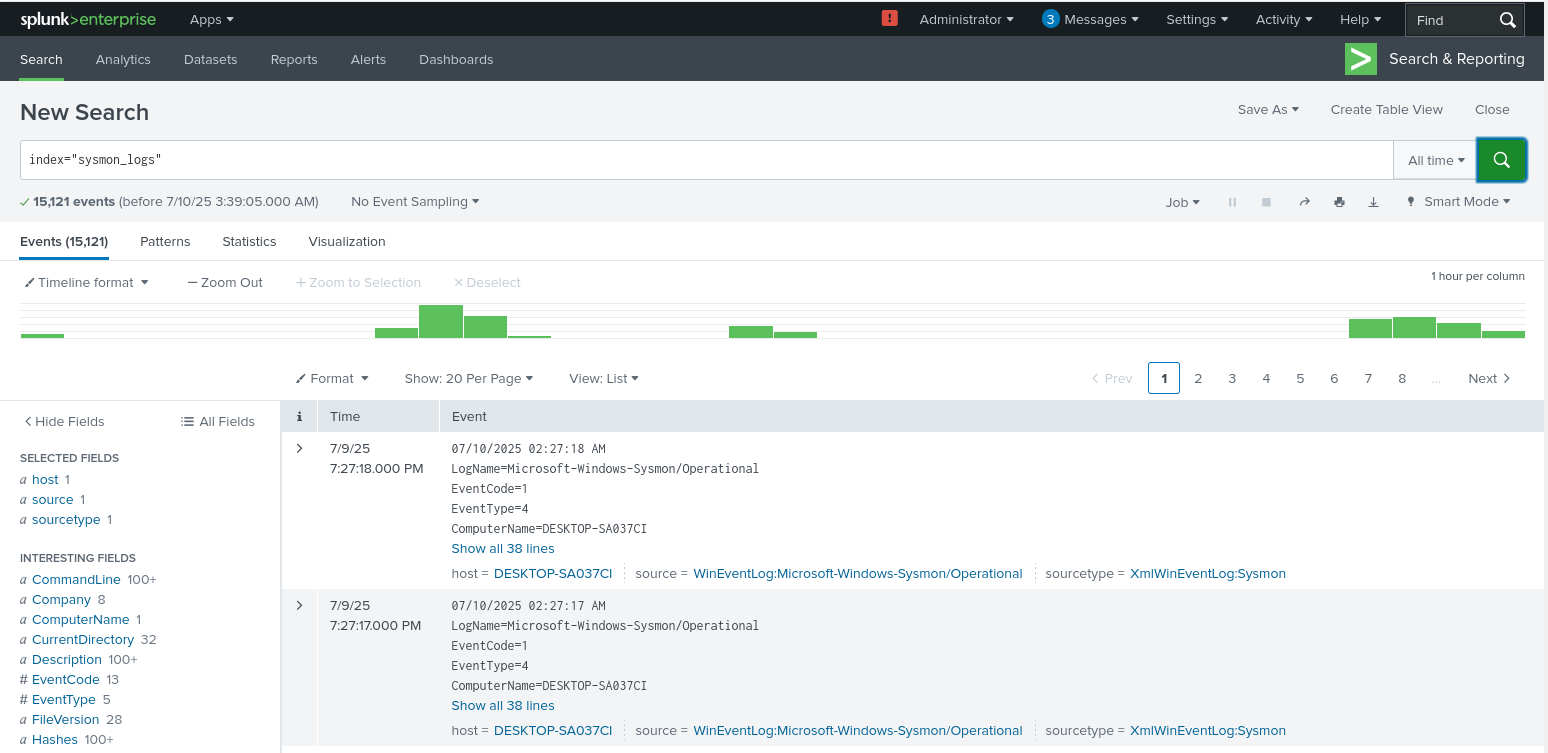
**Thêm dòng sau**



1. **Khởi động lại Splunk Forwarder**

C:\\WINDOWS\\system32>"C:\\Program Files\\SplunkUniversalForwarder\\bin\\splunk.exe" restart

1. **Kiểm tra xem Splunk nhận được log của Sysmon**



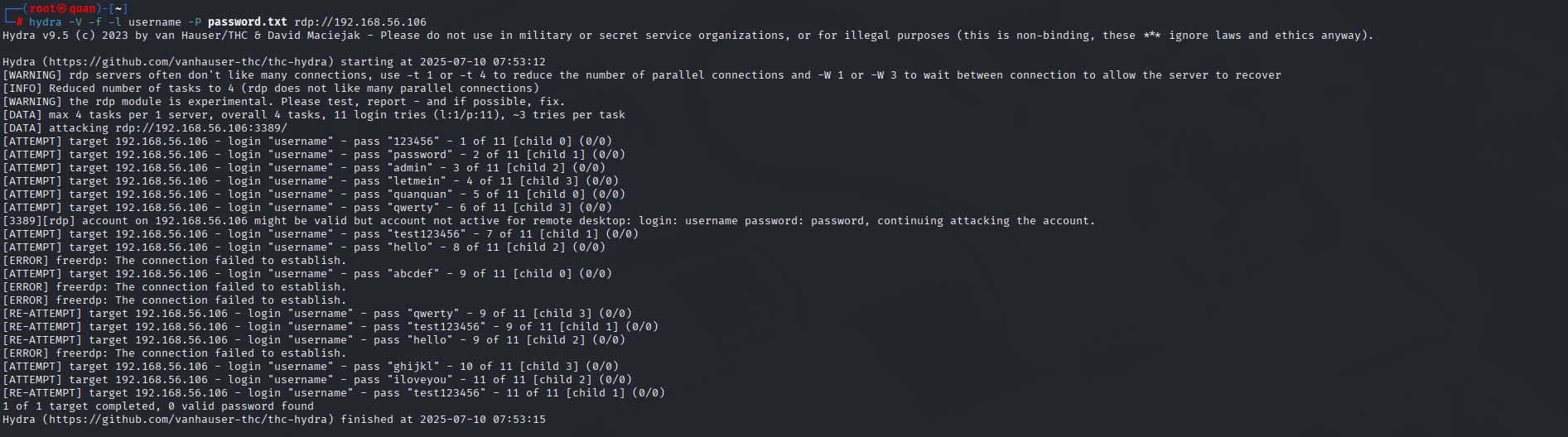
* **Lưu ý:** Nếu Splunk không nhận được log của **Sysmon** mà xem thủ công log của **Sysmon** trên máy Windows vẫn có thì khả năng là do Splunk Forwarder **không chạy bằng Local System Account** nên không đủ quyền đọc log Event Viewer ở Microsoft-Windows-Sysmon/Operational
* **Cách khắc phục:**
  + Kiểm tra lại account đang chạy Splunk Forwarder:
* Get-WmiObject win32\_service | Where-Object { $\_.Name -eq "SplunkForwarder" } | Select-Object StartName
* Nếu không thấy LocalSystem, bạn cần sửa:
  + - Nhấn Win + R, nhập: services.msc
    - Tìm dịch vụ **"SplunkForwarder"**
    - Chuột phải → Properties
    - Chuyển sang tab **Log On**
    - Chọn: Local System account
    - Khởi động lại Splunk Forwarder

**Bước 4: Mô phỏng cuộc tấn công Brute-Force SSH**

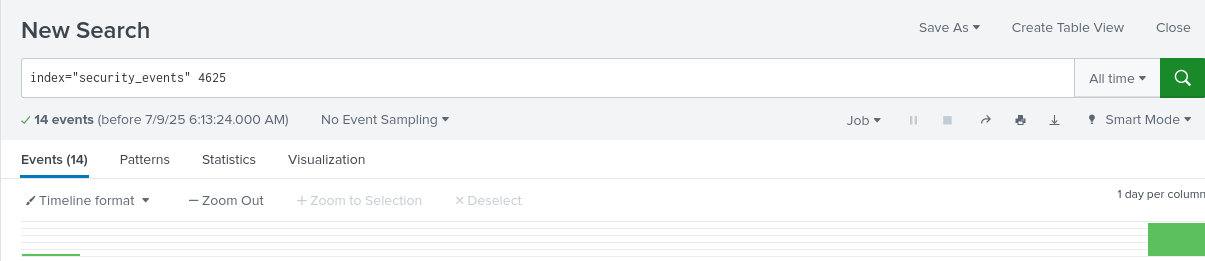
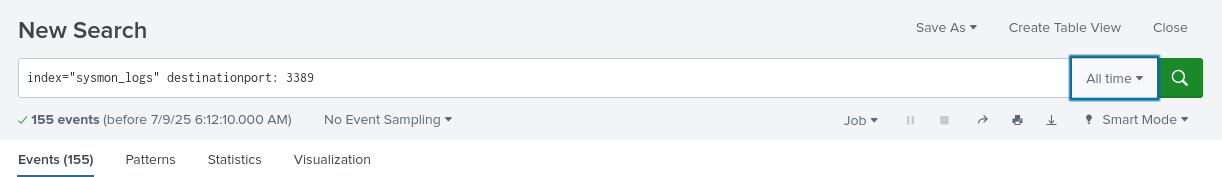
1. **Trên máy tính Kali**

* Chạy lệnh

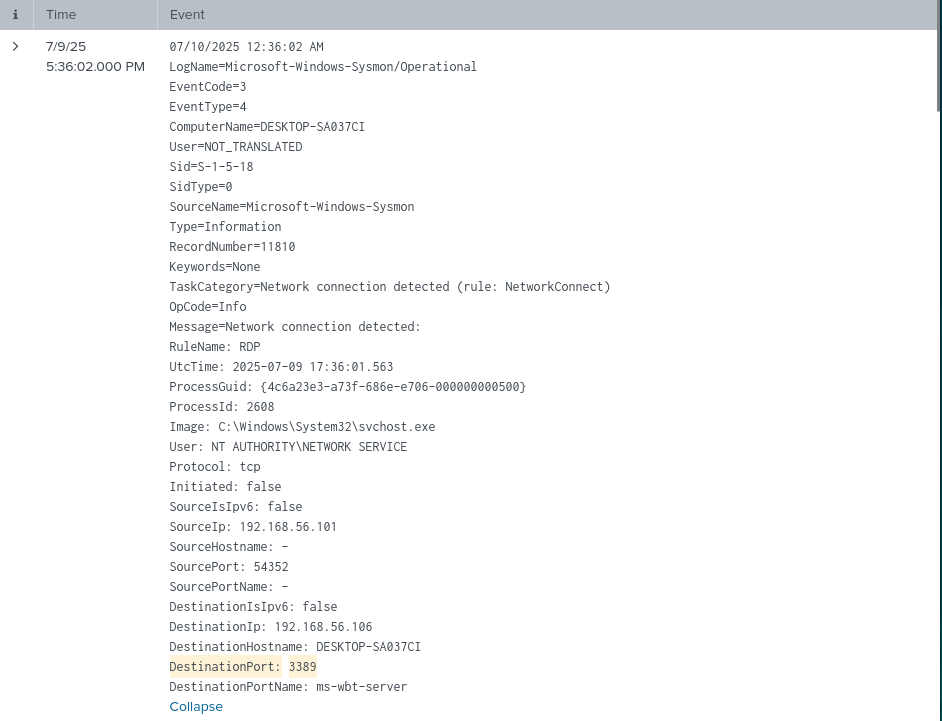
hydra -V -f -l username -P passwords.txt rdp://192.168.56.106



1. **Kiểm tra log của Sysmon và Windows Security trên Splunk**



**Bước 5: Phân tích Log trên Splunk**

****

****

**🛡️ BÁO CÁO PHÂN TÍCH SỰ CỐ - RDP BRUTE-FORCE ATTACK**

**🔍 1. Tóm tắt sự cố**

* **Tên sự cố**: Phát hiện brute-force tấn công vào dịch vụ Remote Desktop Protocol (RDP).
* **Mục tiêu**: Máy tính Windows DESKTOP-Lab tại địa chỉ IP 192.168.100.100.
* **Thời gian phát hiện**: 10/7/2025, từ 12:33:14 đến 12:36:02
* **Nguồn tấn công**: 192.168.56.101 (Kali giả lập hành vi attacker).
* **Mục tiêu tài khoản**: quan.
* **Kết quả**: Tất cả các lần đăng nhập đều thất bại (Event ID 4625), cho thấy đây là brute-force không thành công.

**📁 2. Chi tiết log phát hiện**

**✅ Log kết nối mạng từ Sysmon (Event ID 3)**

UtcTime: 09/7/2025 17:36:01.563

SourceIp: 192.168.56.101

DestinationIp: 192.168.56.106

DestinationPort: 3389 (RDP)

Image: C:\\Windows\\System32\\svchost.exe

ProcessId: 2608

User: NT AUTHORITY\\NETWORK SERVICE

RuleName: RDP

🔸 **Nhận định**: Một kết nối đến cổng **3389 (RDP)** đã được phát hiện từ IP 192.168.56.101, thực hiện bởi tiến trình hệ thống svchost.exe.

**❌ Log thất bại đăng nhập từ Windows Security Log (Event ID 4625)**

EventCode: 4625 - An account failed to log on

Logon Type: 3 (Network logon)

Account Name: lab

Failure Reason: Unknown user name or bad password

Source Network Address: 192.168.56.101

Workstation Name: quan (Kali)

Authentication Package: NTLM

🔸 **Nhận định**: Đây là log thất bại đăng nhập từ xa (logon type 3), cho biết kẻ tấn công đã cố gắng sử dụng tài khoản lab để truy cập nhưng bị từ chối do **tên người dùng sai hoặc mật khẩu không đúng**.

**🔗 3. Tương quan sự kiện**

* Địa chỉ IP 192.168.56.101 xuất hiện trong cả hai log (Sysmon và Security).
* Các sự kiện 4625 lặp lại liên tục trong thời gian ngắn, kết hợp với kết nối đến cổng 3389 ⇒ **Brute-force RDP attack**.

**📌 4. Đánh giá mức độ nghiêm trọng**

| **Tiêu chí** | **Mức độ** |
| --- | --- |
| Mục tiêu dịch vụ quan trọng | Cao |
| Mức độ thành công | Thất bại |
| Tần suất và hành vi | Rõ ràng là brute-force |
| Nguồn nội bộ hay bên ngoài | Nội bộ (lab) |

**→ Mức độ nghiêm trọng: Trung bình - Cao** (Nếu tấn công thành công, có thể chiếm quyền điều khiển máy từ xa.)

**🧯 5. Hành động đề xuất / Ứng phó**

1. **Chặn tạm thời IP 192.168.56.101** trên firewall nội bộ.
2. **Kiểm tra tài khoản lab** xem có dấu hiệu bị thay đổi thông tin hay đăng nhập thành công.
3. **Kích hoạt cơ chế giới hạn đăng nhập** (Account Lockout Policy) sau nhiều lần thất bại.
4. **Tắt RDP nếu không cần thiết**, hoặc chuyển sang giải pháp bảo mật khác như VPN + MFA.
5. **Tạo alert Splunk tự động** cho pattern brute-force RDP:

index=sysmon\_logs DestinationPort=3389

| stats count by SourceIp, DestinationIp, \_time

| where count > 10