Windows Log

(Windows Event Log)

**I. Tổng quát:**

+ Gồm các sự kiện liên quan đến: OS, software, hardware, security

**II. Vị trí**

+ Phiên bản cũ (trước Windows Vista): systemroot%\System32\config, phần mở rộng .evt

+ Từ Win Server 2008: %systemroot%\System32\winevt\logs (Event Log được lưu dưới dạng file XML, phần mở rộng .evtx)

A screenshot of a computer

Description automatically generated

Trên registry xem ở: HKLM\System\ControlSet001\Services\EventLog

A screenshot of a computer

Description automatically generated

**III. Format Log:**

+ Trước Win2008:

- Toàn bộ tệp log được ánh xạ vào bộ nhớ (máy dùng tối đa 300MB cấp phát cho Event Log)

+ Sau:

- service Windows Event Log quản lý các event và event logs (logging events, querying events, subscribing to events, archiving event logs, and managing event metadata)

- Bộ nhớ sẽ chứa các header nhỏ với đoạn mã 64KB trong bộ nhớ

- Cấu trúc dễ xem hơn (vào %systemroot%\System32\winevt\logs, chọn 1 file xml, dễ dàng xem được)

**IV. Event Types:**

+ Có 5 loại sự kiện có thể được ghi lại:

A screenshot of a computer error

Description automatically generated

Error: Vấn đề nghiêm trọng: mất dữ liệu hoặc mất chức năng (VD: 1 dịch vụ không tải được trong khởi động)

Warning: sự kiện không nhất thiết quan trọng nhưng có thể xảy ra trong tương lai (ổ đĩa sắp hết,…)

Information: Hoạt động thành công của 1 dịch vụ

Success: Hoạt động truy cập bảo mật thành công (đăng nhập thành công vào hệ thống)

Failure: Ngược lại với Success

V. Log Types:

A screenshot of a computer

Description automatically generated

+ Một số loại phổ biến:

* System: Sự kiện ghi lại bởi OS hoặc các thành phần của nó (VD: dịch vụ không thể khởi chạy trong quá trình khởi động)
* Application: Sự kiện sinh ra bởi ứng dụng (VD: Lỗi khởi động ứng dụng)
* Security: Ghi lại thông tin về kiểm soát truy cập: các lần login fail,… (theo tiêu chí trong local hay global group policies)
* Setup: Xác định bản cập nhật Windows, các bản vá lỗi, các hostfix được thêm vào hệ thống
* Forwarded Events (mới): Chứa event log được chuyển tiếp từ các máy tính khác nhau trong cùng mạng

VI. Phát hiện tấn công, tìm kiếm thông tin thông qua phân tích Windows event logs

1. Brute-force Password:

+ Hình thức: Người tấn công thử nhiều lần với các mật khẩu khác nhau

+ Dấu hiệu: Mỗi lần đăng nhập thất bại sẽ tạo ra event trong Security Logs (Event ID 4625), các event xuất hiện trong 1 thời gian ngắn nhất định

A screenshot of a computer

Description automatically generated

+ Xem chi tiết hơn:

A screenshot of a computer

Description automatically generated

* Tài khoản truy cập không thành công administrator
* Logon type 3 ⬄ Người dùng đăng nhập từ xa vào máy tính

A screenshot of a computer

Description automatically generated

Event 4625(Đăng nhập fail)

A screenshot of a computer

Description automatically generated

Event 4624(Đăng nhập thành công)

(4624 chứa IP và timestamp)

2. Remote Desktop Protocol (rdp)

+ Dấu hiệu: 2 Event ID: 4778, 4779

* 4778 cho biết 1 phiên kết nối được mở
* 4779 khi kết thúc 1 phiên

Event ID 4624 đồng thời với 4778 nghĩa là một session remote được thiết lập thành công

Với Event ID 4779 và 4647 (đăng xuất thành công)

A screenshot of a computer

Description automatically generated

VD (hình trên): ta thấy Event ID 4624, sau đó là 4778 ⬄ Có một event đăng nhập thành công, sau đó

A screenshot of a computer

Description automatically generated

Logon type: 10: Người dùng truy cập từ xa vào máy tính thông qua RDP

Sau đó là Event ID 4778:

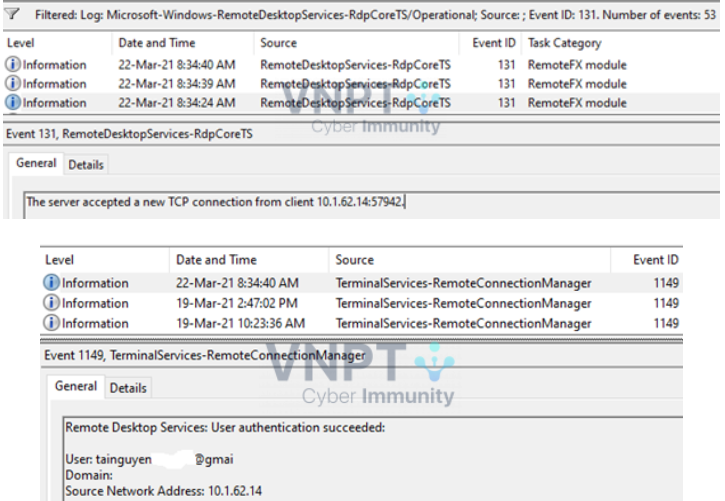
A screenshot of a computer

Description automatically generated

Phiên RDP được mở

+ Ngoài ra, check thêm log Remote Desktop Services:

Event ID 131 trong log RDPCoreTS và Event ID 1149 trong log TerminalServices-RemoteConnectionManager ghi lại địa chỉ IP remote, user và ngày/giờ kết nối thành công



\*\* Chú ý: Một số loại Logon Type:

+ 2 (Interactive): Người dùng đăng nhập vào máy tính

+ 3(Network): Khi người dùng hoặc máy tính đăng nhập vào máy tính từ mạng

+ 4 (Batch): sử dụng bởi các máy chủ hàng loạt. Các tác vụ theo lịch trình được thực hiện thay mặt người dùng mà không cần sự can thiệp của con người

+ 5 (Service): sử dụng cho các dịch vụ và tài khoản dịch vụ đăng nhập để chạy một dịch vụ.

+ 7 (Unlock): khi người dùng mở khóa máy của họ.

+ 8 (Network Cleartext): người dùng hoặc máy tính đăng nhập vào máy tính từ mạng và mật khẩu được gửi ở dạng văn bản rõ ràng.

+ 9 (NewCredentials): Người dùng sử dụng ‘RunAs’ command để chạy ứng dụng

+ 10 (RemoteInteractive): Người dùng truy cập từ xa vào máy tính thông qua RDP

+ 11(CacheInteractive): người dùng đăng nhập vào máy tính mà không cần phải liên hệ với bộ điều khiển miền vì thông tin xác thực mạng được lưu trữ cục bộ trên máy tính.

\*\* Xem thêm về Event ID: <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor>

\*\* Nguồn:

[[Windows Forensic] [Part1] Windows Event Logs - VNPT Cyber Immunity](https://sec.vnpt.vn/2022/03/windows-event-logs-1/)

[[Windows Forensic][Part3] Windows Event Logs - VNPT Cyber Immunity](https://sec.vnpt.vn/2023/02/windows-forensicpart3-windows-event-logs/)

Phân tích Event của Windows Log:

VD:

A screenshot of a computer

Description automatically generated

+ Subject User Sid: