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)

+ Một số trường phổ biến:

* Log Name: Tên của Event log mà sự kiện được lưu
* Source: Dịch vụ, thành phần Microsoft hoặc ứng dụng có liên quan đến sự kiện
* Event ID: Mã được gán cho mỗi audited activity
* Level: Mức độ được gán cho sự kiện trong câu hỏi (question)
* User: Tài khoản người dùng liên quan đến kích hoạt hoạt động hoặc ngữ cảnh người dùng mà nguồn đang chạy khi sự kiện được ghi lại. Trường này thường hiển thị là “System” hoặc một người dùng không phải là nguyên nhân của sự kiện được ghi nhận
* OpCode: Được gán bởi nguồn liên quan đến log
* Logged: Ngày giờ trên local system khi mà sự kiện được ghi
* Task Category: Giống OpCode
* Keywords: Được gán bởi nguồn và sử dụng để nhóm hoặc sắp xếp sự kiện
* Computer: Máy tính mà sự kiện được ghi. Hữu ích cho thu thập từ nhiều hệ thống, không được coi là thiết bị dẫn đến sự kiện (VD: khi remote logon được khởi tạo, trường máy tính sẽ vẫn để tên của hệ thống ghi event, không phải nguồn kết nối)
* Description: Là khối văn bản thêm vào các thông tin chi tiết liên quan đến event được ghi lại được ghi vào. Là trường quan trọng cho phân tích

Account Management Events:

|  |  |
| --- | --- |
| Event ID | Description |
| 4720 | Tài khoản người dùng được tạo |
| 4722 | Tài khoản người dùng được kích hoạt |
| 4723 | Nỗ lực thay đổi mật khẩu tài khoản người dùng |
| 4724 | Nỗ lực reset mật khẩu tài khoản của người dùng |
| 4725 | Vô hiệu hóa một tài khoản người dùng |
| 4726 | Xóa 1 tài khoản người dùng |
| 4727 | Tạo 1 nhóm security-enabled Global |
| 4728 | Thêm một thành viên vào nhóm security-enabled Global |
| 4729 | Xóa một thành viên khỏi nhóm security-enabled global |
| 4730 | Xóa một nhóm security-enabled global |
| 4731 | Tạo một nhóm security-enabled local |
| 4732 | Thêm một thành viên khỏi nhóm security-enabled local |
| 4733 | Xóa một thành viên khỏi nhóm security-enabled local |
| 4734 | Xóa một nhóm security-enabled local |
| 4735 | Thay đổi một nhóm security-enabled local |
| 4737 | Thay đổi một nhóm security-enabled global |
| 4738 | Thay đổi một tài khoản người dùng |
| 4741 | Tạo mới một tài khoản máy tính |
| 4742 | Thay đổi một tài khoản máy tính |
| 4743 | Xóa một tài khoản máy tính |
| 4754 | Tạo một nhóm security-enabled universal |
| 4755 | Thay đổi một nhóm security enabled universal |
| 4756 | Thêm một thành viên vào nhóm security enabled universal |
| 4757 | Xóa một thành viên khỏi nhóm security enabled universal |
| 4758 | Xóa một nhóm security-enabled universal |
| 4798 | Liệt kê thông tin các thành viên trong nhóm người dùng cục bộ -> Tìm kiếm thông tin |
| 4799 | Liệt kê thông tin các thành viên trong nhóm security-enabled cục bộ -> Tìm kiếm thông tin |

Nhóm security-enabled local: nhóm tài khoản người dùng và tài khoản máy tính được tổ chức thành một đơn vị có thể quản lý và được cấp quyền cụ thể

Nhóm security-enabled global:

Nhóm security-enabled universal:

=> Các nhóm security được sử dụng để kiểm soát lưu lượng truy cập vào tài nguyên và cũng có thể được sử dụng để cấp quyền cho người dùng

Account Logon và Logon Events

* Đăng nhập tài khoản (Account Logon) chỉ việc xác thực. Đăng nhập (Logon) chỉ ra tài khoản có quyền truy cập
* Authentication (account logon) của domain account được thực hiện bởi domain controller, Local account (nằm trong file SAM hơn là 1 phần của AD) được xác thực bởi local system nơi chúng tồn tại => Các hệ thống thưc hiện xác thực sẽ ghi lại sự kiện này
* Có thể thiết lập nhật ký đăng nhập tài khoản/Đăng nhập với chính sách nhóm GPO. Việc ghi nhật ký từ xa, qua SIEM,… giúp bảo vệ nhật ký bị sửa đổi trái phép

Các Event ID trên Domain Controller liên quan đến xác thưc người dùng trong domain

|  |  |
| --- | --- |
| Event ID | Ý nghĩa |
| 4768 | * TGT được cấp phát thành công cho biết tài khoản người dùng đã được Domain Controller xác thực. Phần “Network Information” có thể chứa thông tin bổ sung về máy chủ từ xa đã cố gắng đăng nhập * Trường “Keyword” cho biết kết quả xác thực thành công/thất bại, mã lỗi trả về mô tả trong RFC 4120 |
| 4769 | * Một ticket được yêu cầu bởi một người dùng cho một tài nguyên cụ thể. Chứa thông tin:   + IP nguồn yêu cầu  + Tài khoản dịch vụ người dùng  + Dịch vụ cần truy cập   * Cho phép theo dõi quyền truy cập của người dùng đã được xác thực qua mạng * Trường keywords cho biết yêu cầu cho dịch vụ ticket thành công hay thất bại và chứa mã lỗi * Ghi lại “TicketEncryptionType” để phát hiện tấn công vào giao thức Keberos |
| 4770 | Ticket được gia hạn. Chứa thông tin:  + Tên tài khoản và tên dịch vụ  + Địa chỉ IP của máy khách và “TicketEncryptionType” |
| 4771 | * Dựa vào kết quả đăng nhập Keberos thất bại. Trường “Additional Information/Result code ” bổ sung thông tin về lỗi |
| 4776 | * Ghi lại cho các lần xác thực với NTLM   + Network Information -> thông tin về máy chủ cố gắng đăng nhập từ xa  + Keywords -> kết quả xác thực thành công/thất bại, cho biết mã lỗi   * Nhiều sự kiện 4776 với lỗi C000006A (mật khẩu không đúng) sau đó tới mã C0000234 (tài khoản bị khóa) * Dấu hiệu tấn công dò đoán mật khẩu / người dùng quên mật khẩu * Nhiều sự kiện 4776 lỗi, sau đó thành công -> có thể mật khẩu đã bị lộ |
| 4624 |  |
| 4625 | Đăng nhập thất bại. Số lượng lớn sự kiện 4625 -> Tấn công dò đoán mật khẩu. Phần Network Info chứa thông tin máy chủ từ xa đang cố gắng đăng nhập. Chú ý đăng nhập không thành công với RDP có thể ghi “Type=3” thay vì “Type=10”, phụ thuộc vào hệ thống |
| 4634/4647 | Ghi lại sự kiện đăng xuất (có thể không được ghi lại). Giá trị LogonID sẽ giống với giá trị trong sự kiện đăng nhập có EventID = 4624:   * Giá trị “Logon Type=3” thường ngắt kết nối sau khi yêu cầu hoàn tất, không cho biết thời gian thực tế mà người dùng tham gia vào bất kỳ hoạt động cụ thể nào * Giá trị “Logon Type=2,10,11” cung cấp cảm nhận tốt hơn về thời lượng phiên. Tuy nhiên, Windows có thể ngắt kết nối phiên do người dùng ngừng tương tác trong một khoảng thời gian |
| 4768 |  |
| 4768 |  |
| 4768 |  |
| 4768 |  |

**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:

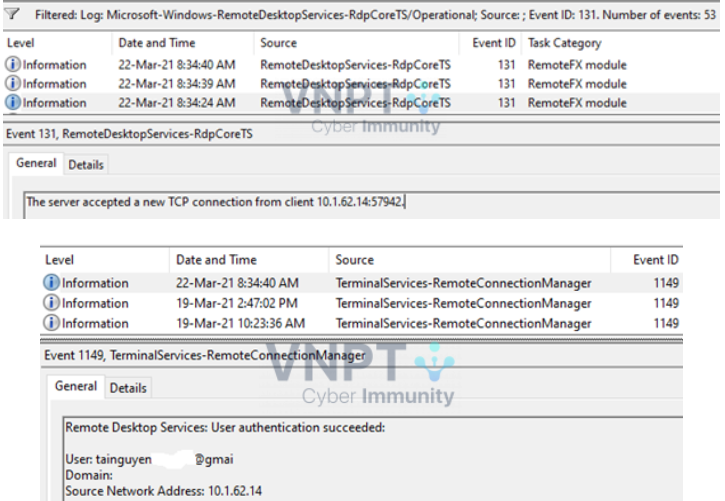
A screenshot of a computer

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: