Windows Logging for SOC

TryHackMe Lab Report — Log Analysis Project

Analyst: _____

Date: July 19, 2026

Room Status: Completed — 128 points, 8/8 tasks

1. Overview

This report documents a hands-on log analysis exercise completed as part of the TryHackMe "Windows Logging for SOC" room. The objective was to use Windows Event Viewer and Sysmon logs to reconstruct a simulated intrusion: a brute-force RDP compromise, backdoor account creation, privilege escalation, malware delivery via a browser download, persistence, and command-and-control (C2) communication.

Two saved event log files were analyzed: Practice-Security.evtx (Windows Security log) and Practice-Sysmon.evtx (Sysmon operational log). Investigation was performed directly in the Windows Event Viewer GUI on the provided lab VM.

2. Task 2 — What Is Logged

Question: Looking at the last screenshot, which event ID describes a successful login?

ANSWER	Security / 4624

Event ID 4624 is logged whenever any account — interactive, network, service, or RDP — successfully authenticates on a Windows host. Its counterpart, Event ID 4625, logs failed logon attempts and is used later in this investigation to identify the brute-force attack.

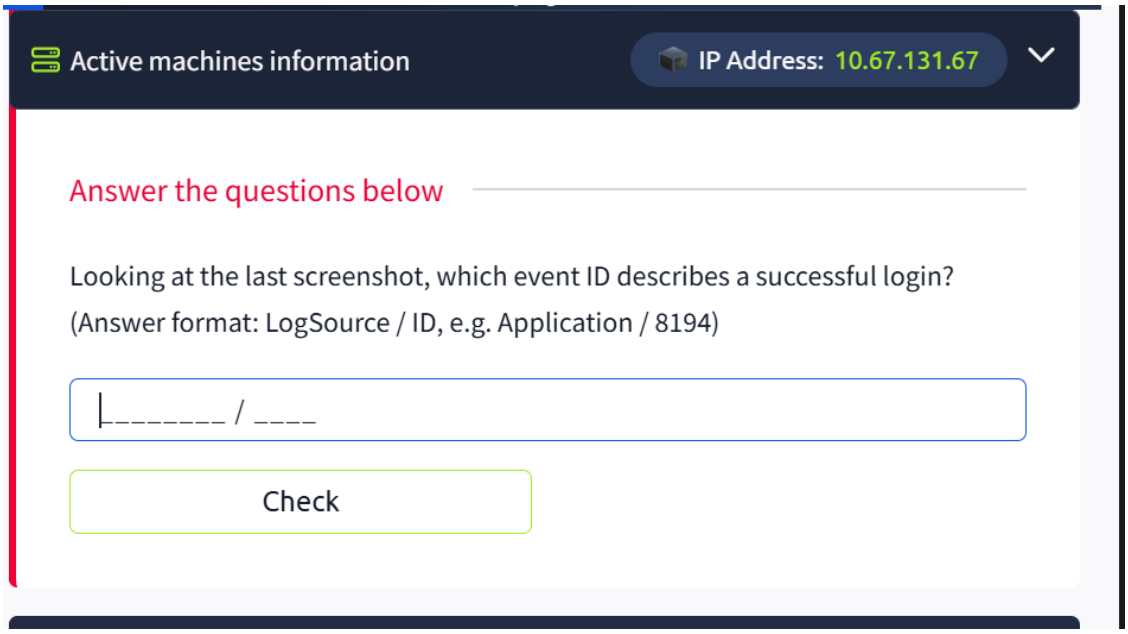

Figure 2.1 — Task question interface confirming the successful-logon event ID.

3. Task 3 — Security Log: Authentication

File used: Practice-Security.evtx

3.1 Locating and Opening the Practice Log

The practice file first had to be opened via Action -> Open Saved Log... and browsed to from the VM Desktop. Several initial attempts filtered the wrong log (the live local Security log) or entered the

Event ID into the wrong filter field, producing 0 results before the correct log and field were identified.

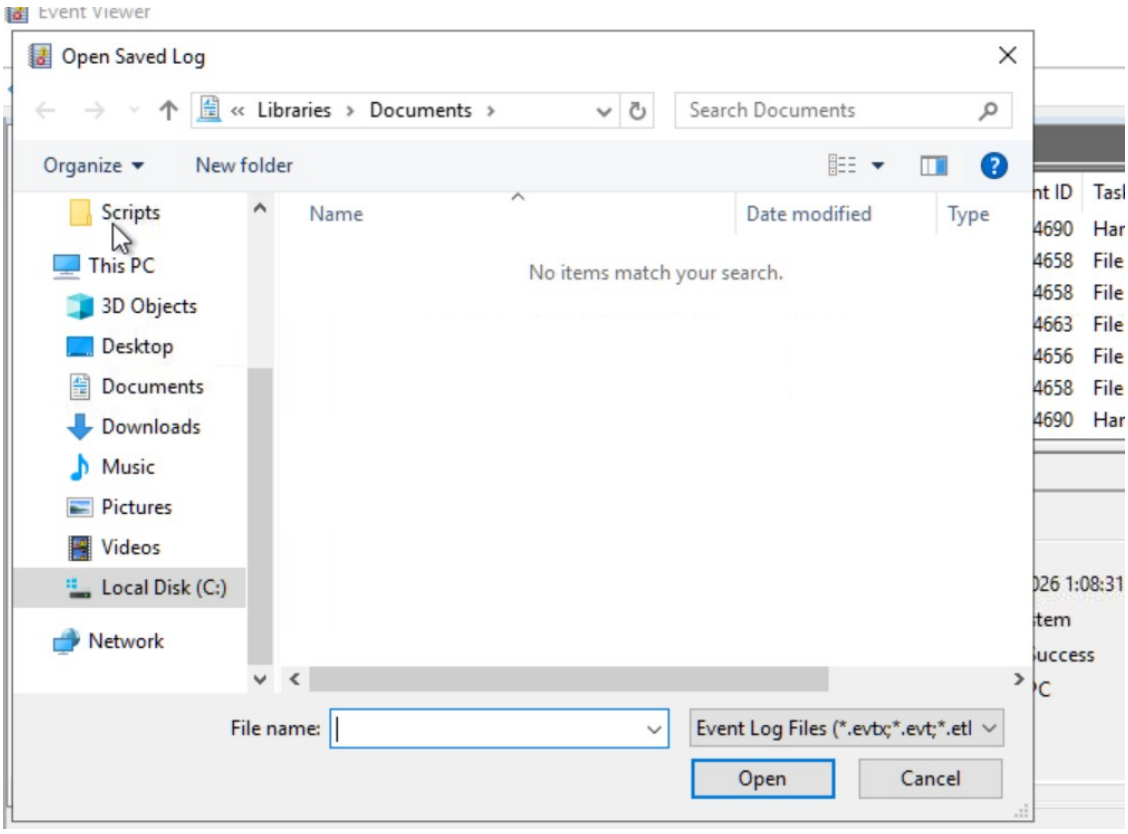

Figure 3.1 — Open Saved Log dialog, browsing to the Desktop.

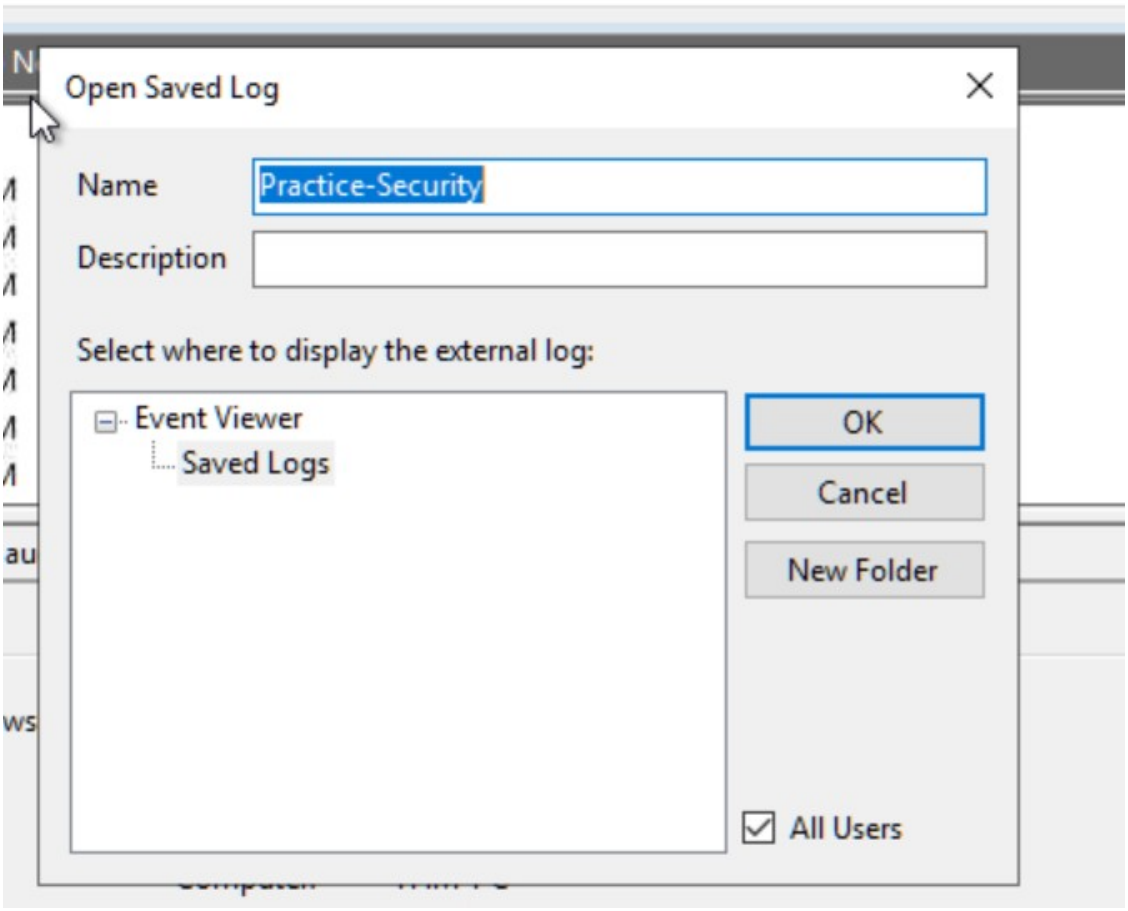

Figure 3.2 — Confirming import of Practice-Security.evtx into Saved Logs.

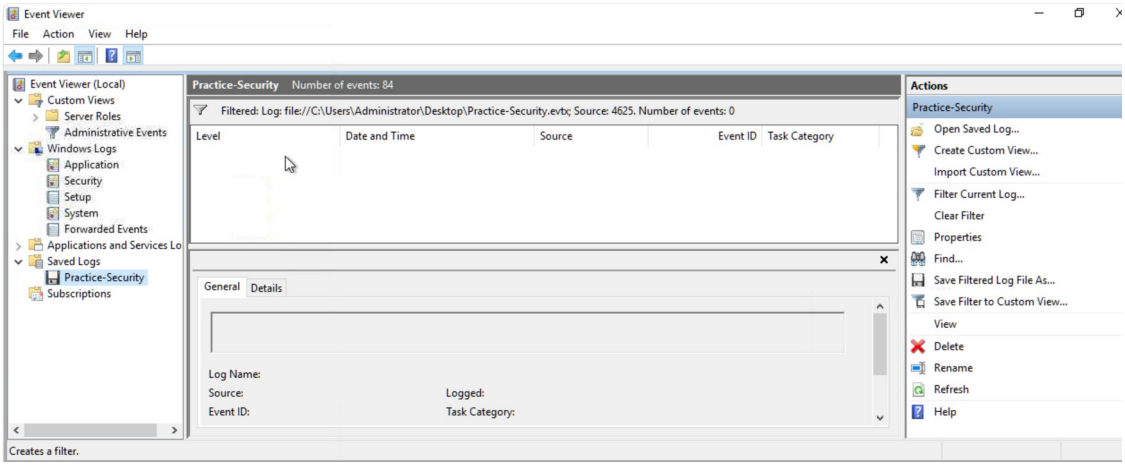

Figure 3.3 — Practice-Security.evtx loaded (84 total events).

3.2 Brute Force Source IP

Method: Filter Current Log -> Event ID 4625 (failed logon).

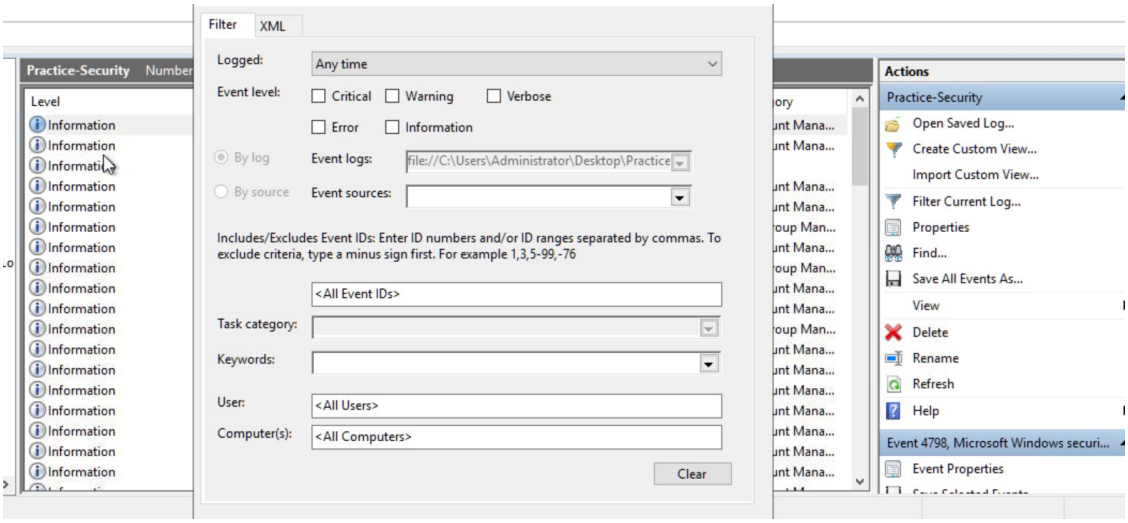

Figure 3.4 — Filter Current Log dialog, entering 4625 in the correct Event ID field.

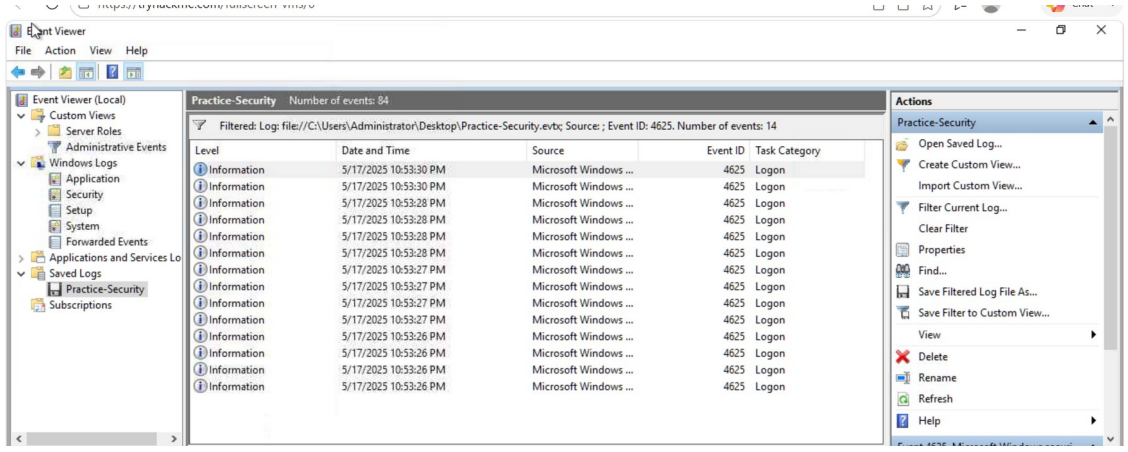

Figure 3.5 — Filtered results: 14 failed logon events (4625) within ~4 seconds.

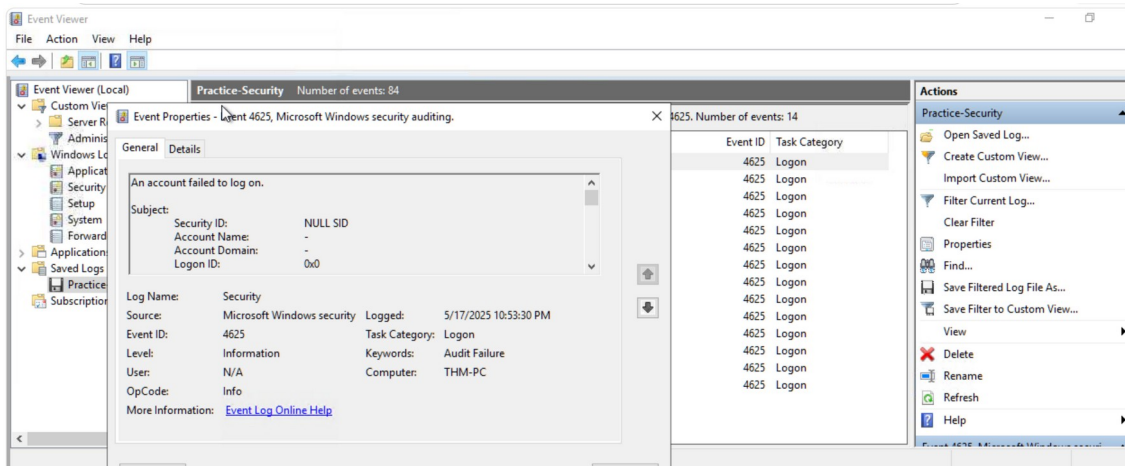

Figure 3.6 — Event 4625 detail: NULL SID subject, typical of a pre-authentication failed remote logon.

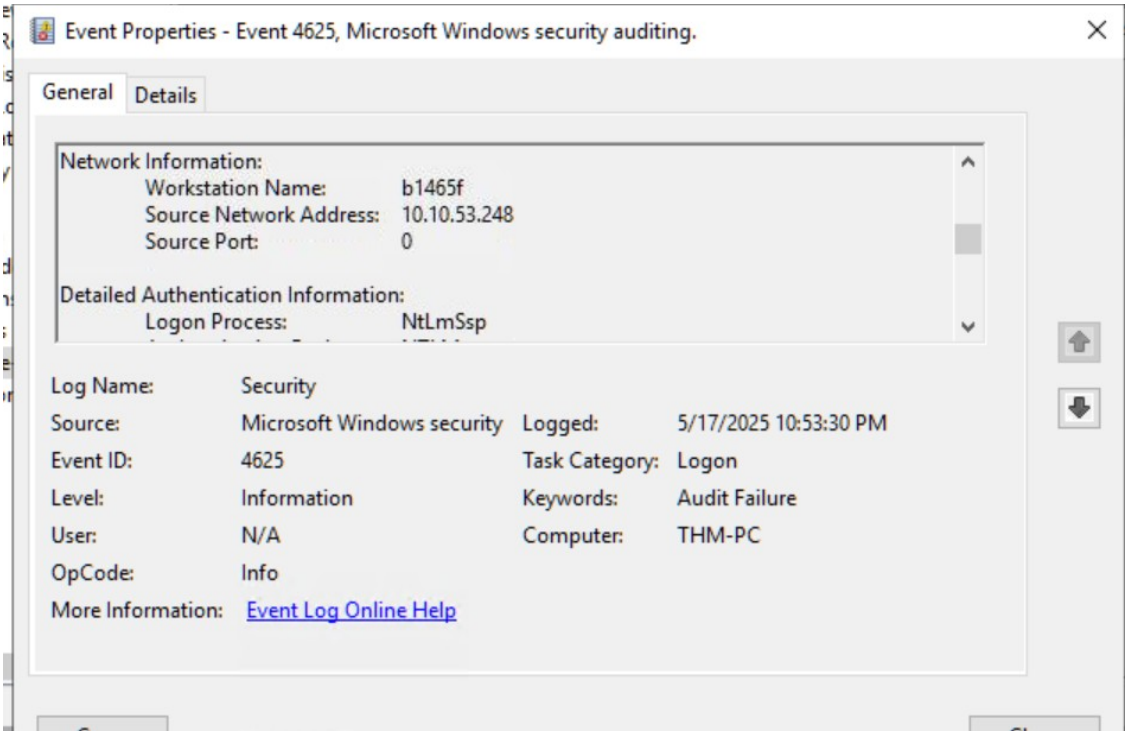

Figure 3.7 — Network Information section revealing the Source Network Address.

Brute-force IP	**10.10.53.248**
Failed attempts observed	**14 attempts in ~4 seconds (10:53:26–10:53:30 PM)**
Logon Process	**NtLmSsp (network/NTLM authentication)**

3.3 Breached User Account

ANSWER	**Administrator**

3.4 Malicious RDP Login

Method: Filter Event ID 4624 (successful logon), then check the Logon Type field. RDP sessions are logged as Logon Type 10 (RemoteInteractive).

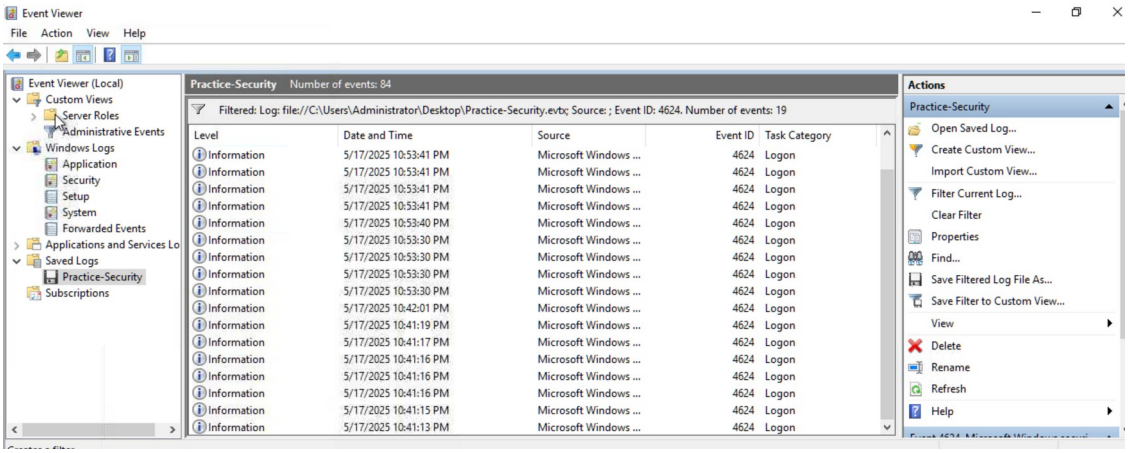

Figure 3.8 — Filtered results: 19 successful logon events (4624).

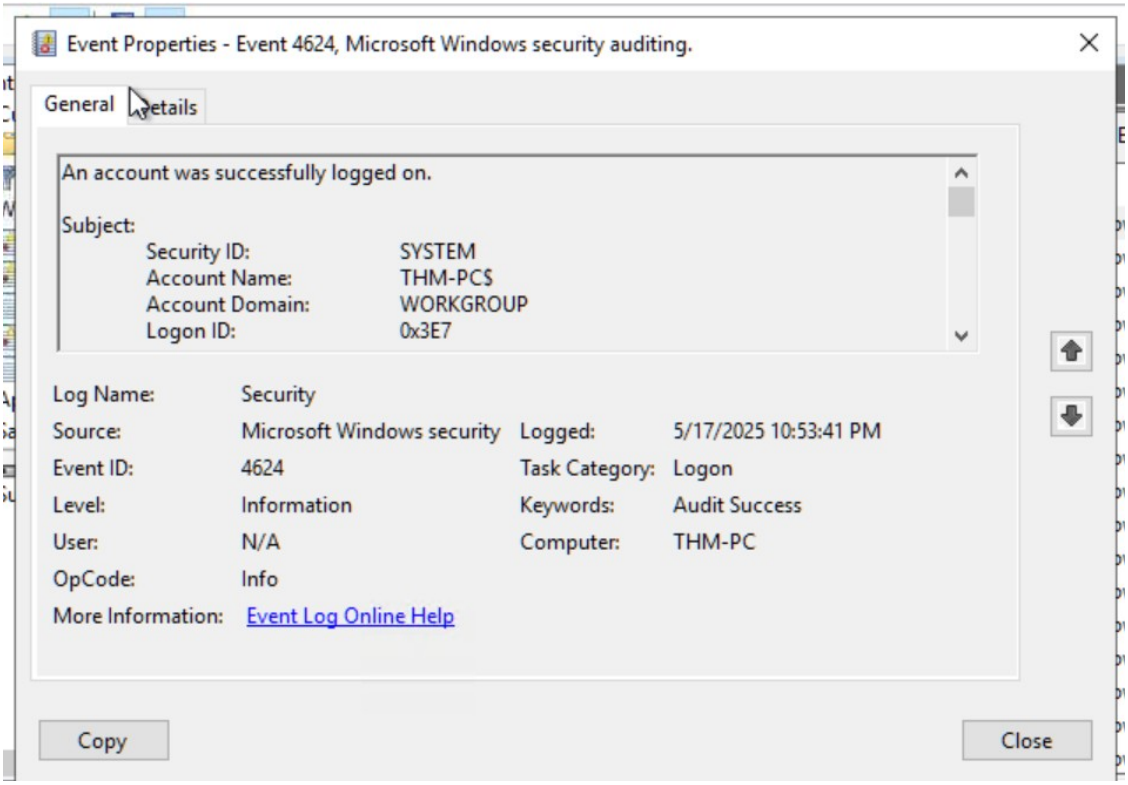

Figure 3.9 — First candidate event was a SYSTEM/THM-PC$ machine account logon, not the RDP session.

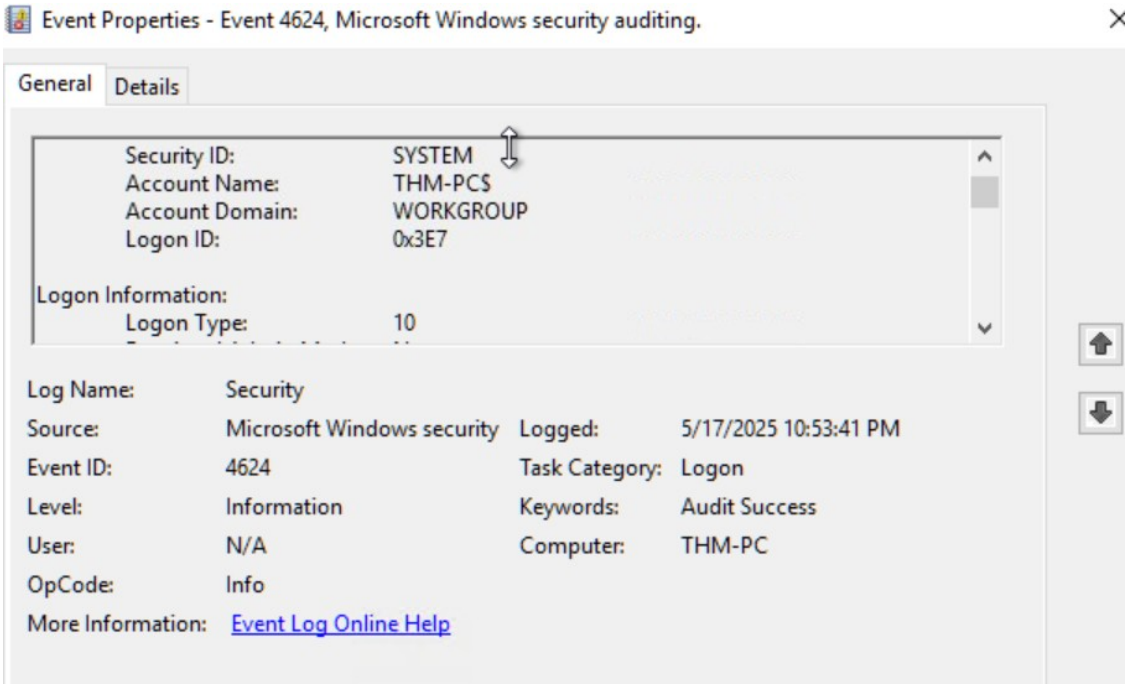

Figure 3.10 — Logon Type: 10 confirmed on the correct event, timestamped 10:53:41 PM.

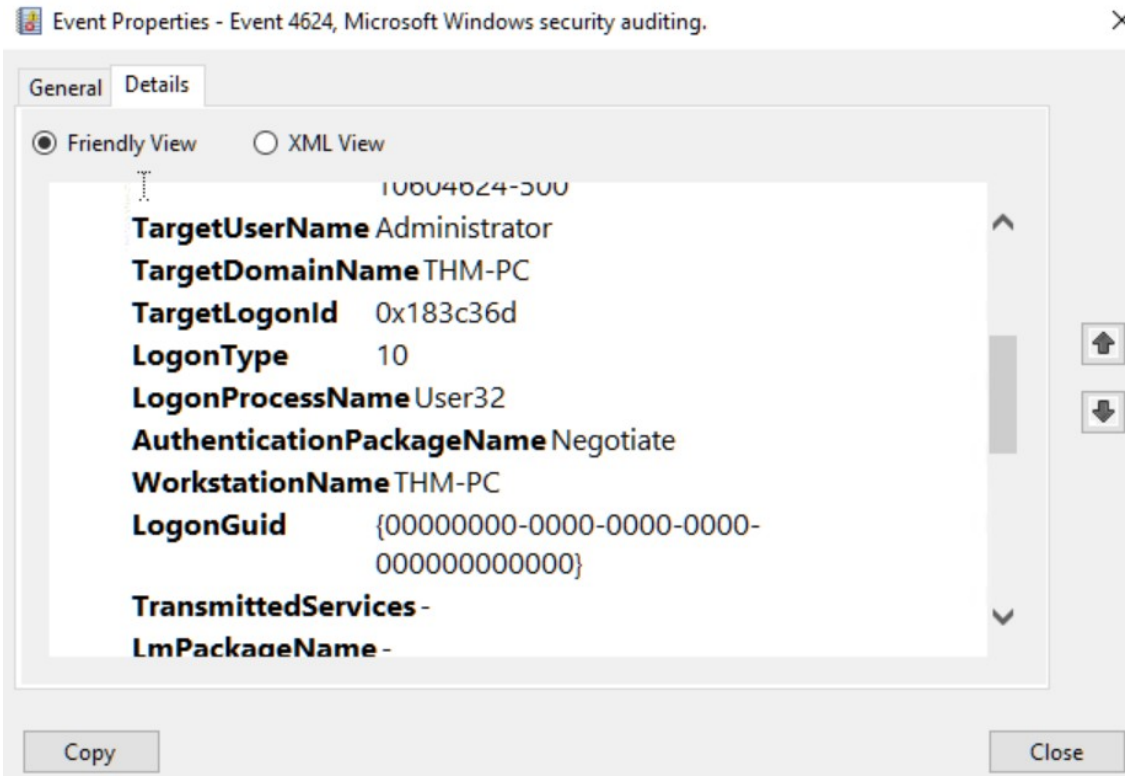

Figure 3.11 — Details (XML/Friendly view) showing TargetUserName: Administrator and TargetLogonId: 0x183c36d.

Logon ID of malicious RDP login	**0x183c36d**

4. Task 4 — Account Creation and Privilege Escalation

File used: Practice-Security.evtx (continued)

4.1 Backdoor Account Created

Method: Filter Event ID 4720 (a user account was created).

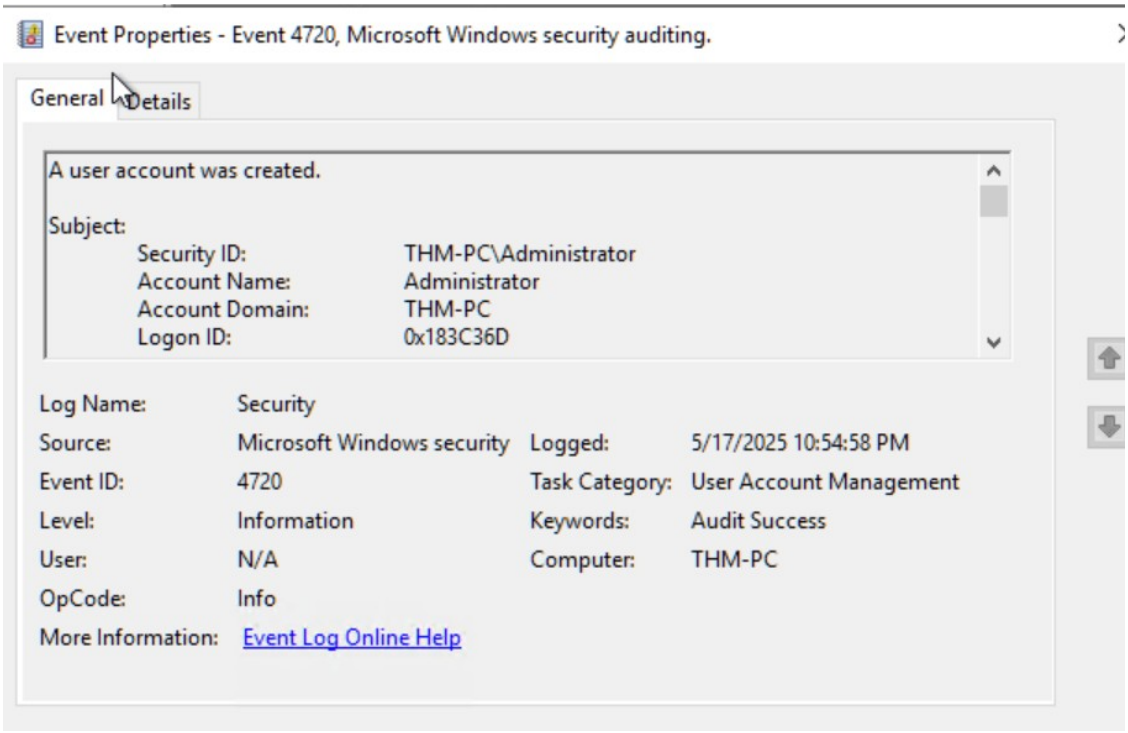

Figure 4.1 — Event 4720: account created under Logon ID 0x183C36D, matching the RDP session.

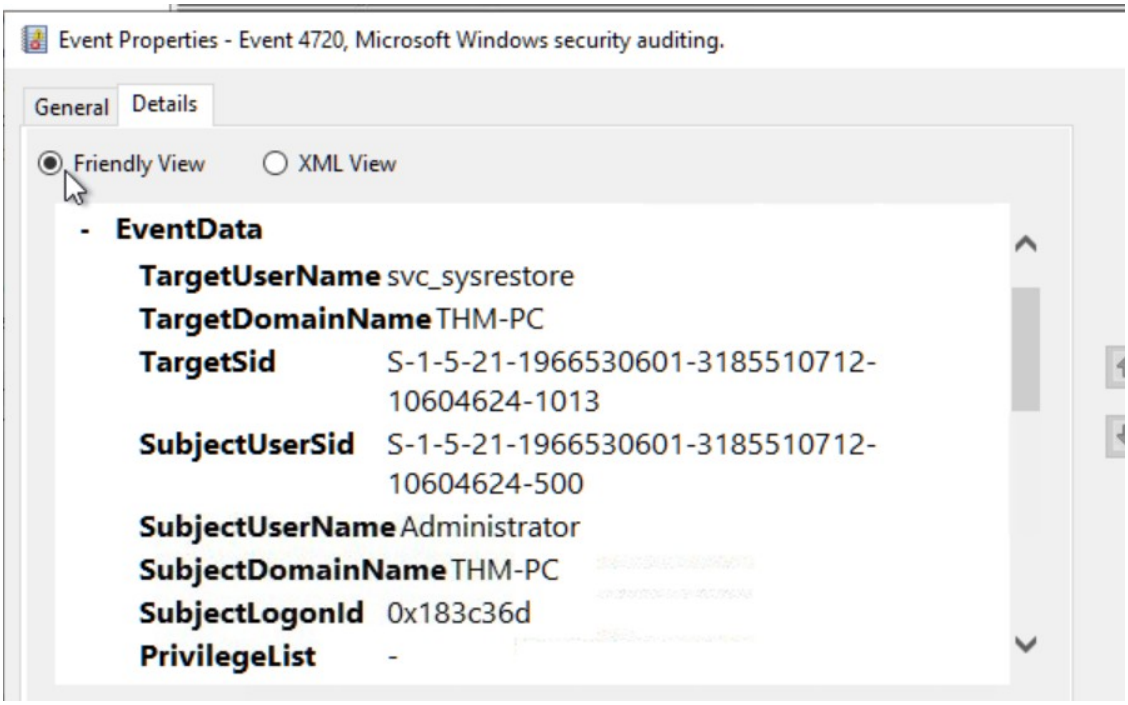

Figure 4.2 — Details tab: TargetUserName svc_sysrestore, created by Administrator.

Backdoor account created	svc_sysrestore

The account name svc_sysrestore was deliberately chosen to resemble a legitimate Windows service account, a common attacker tactic to avoid drawing attention during casual review.

4.2 Privileged Groups Added

Method: Filter Event ID 4732 (member added to a security-enabled local group), then match the MemberSid against the backdoor account's SID.

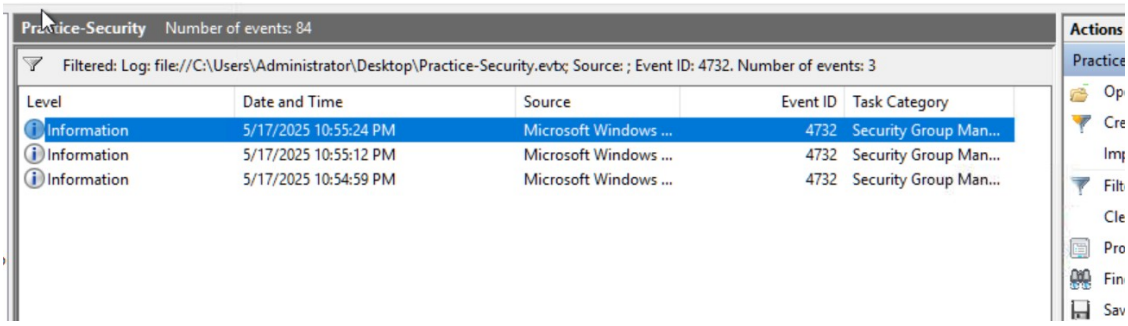

Figure 4.3 — Three 4732 events found for the same MemberSid.

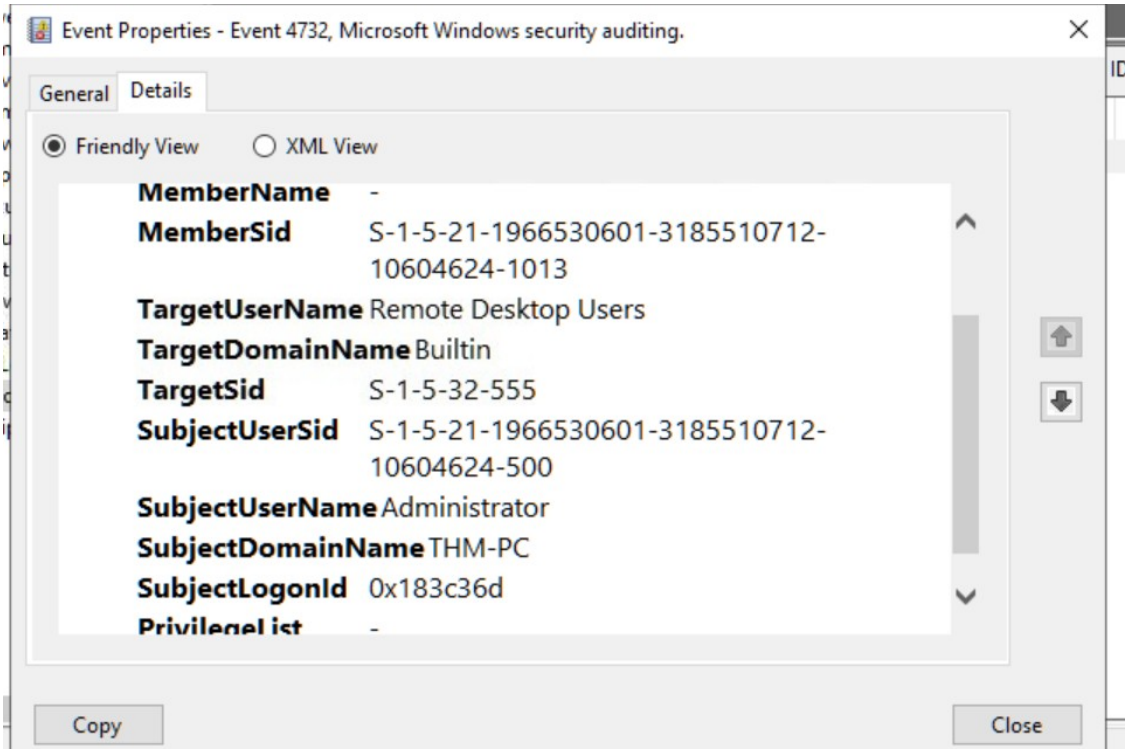

Figure 4.4 — First group membership: Remote Desktop Users.

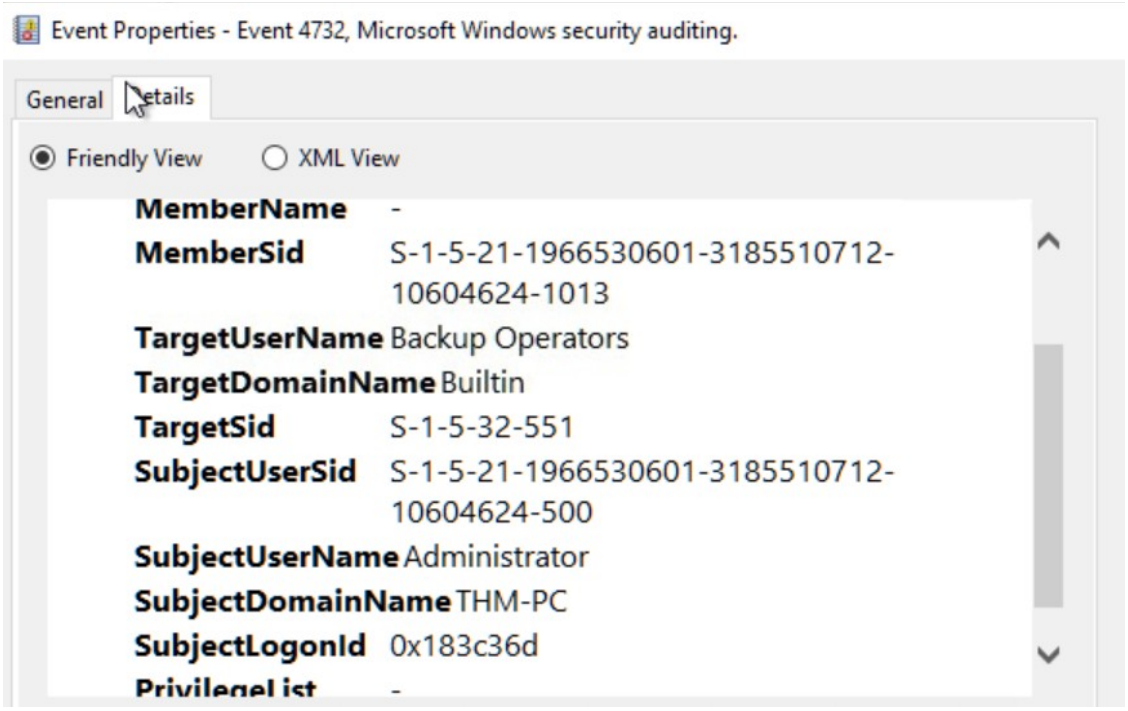

Figure 4.5 — Second group membership: Backup Operators (a known privilege-escalation vector).

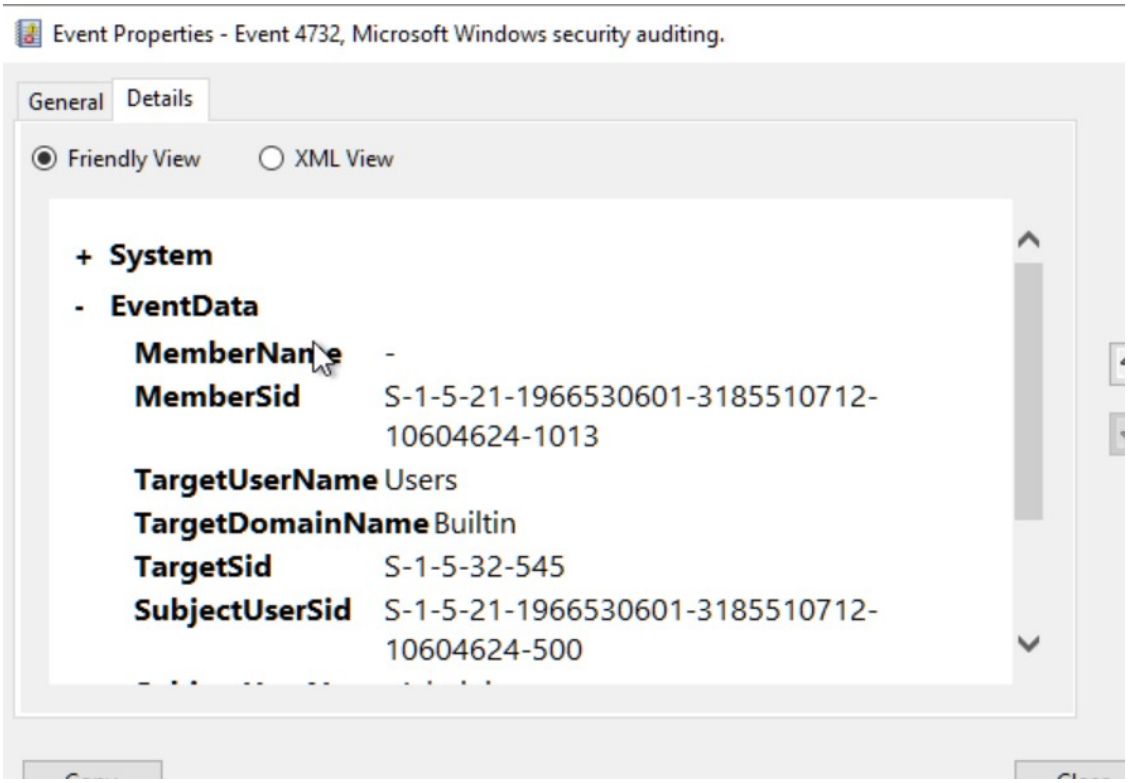

Figure 4.6 — Third event was membership in the default "Users" group — not privileged, excluded from the answer.

Privileged groups (alphabetical)	**Backup Operators, Remote Desktop Users**

4.3 Logon ID Correlation

Question: Does the Logon ID field match what you saw in the previous task?

ANSWER	Yea

The account-creation event (4720) and both group-membership events (4732) all share Logon ID 0x183c36d — the same session used for the malicious RDP login — confirming a single continuous attacker session performed the login, account creation, and privilege escalation.

5. Task 5 — Sysmon: Process Tracking

File used: Practice-Sysmon.evtx

Figure 5.1 — Windows VM desktop showing the Practice-Sysmon.evtx file.

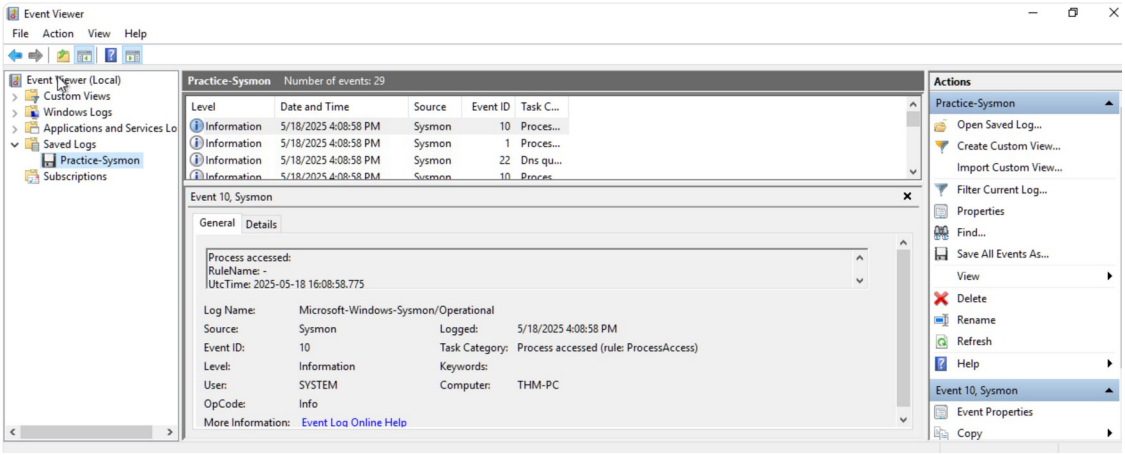

Figure 5.2 — Practice-Sysmon.evtx loaded (29 total events).

5.1 Browser Identification

Method: Filter Event ID 1 (Process Create) and inspect the Image field of each result.

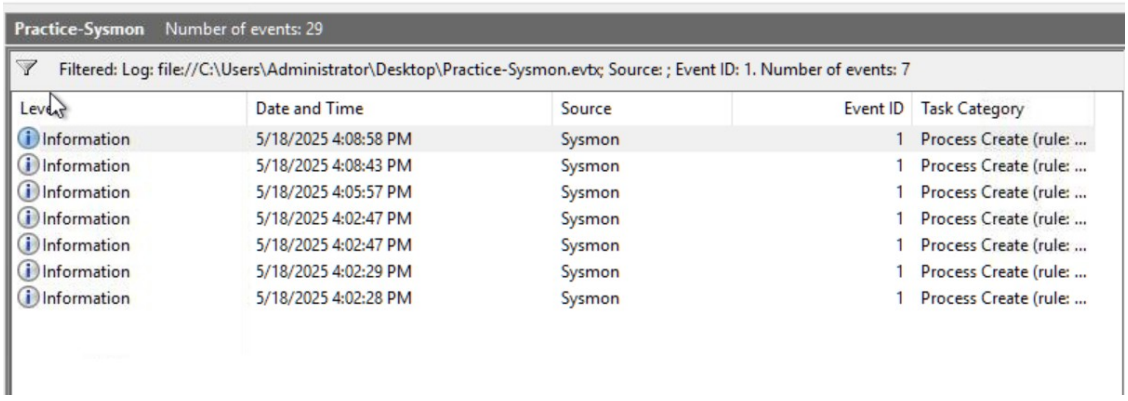

Figure 5.3 — Filtered results: 7 process-creation events.

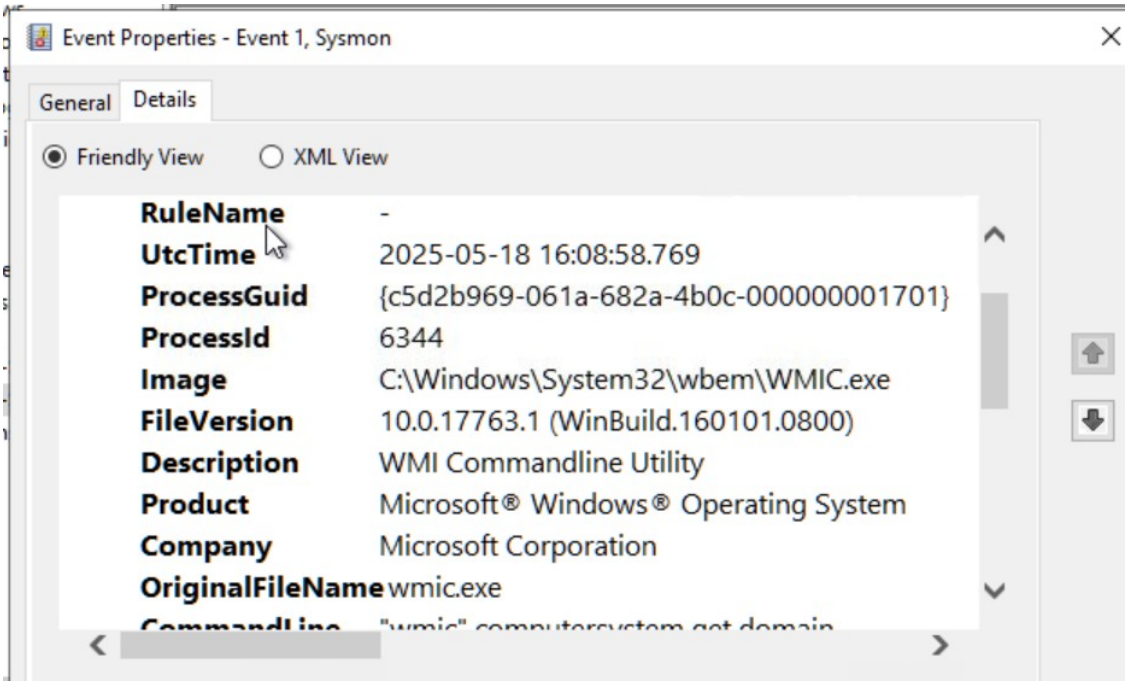

Figure 5.4 — First process checked: WMIC.exe, run by user sarah.miller.

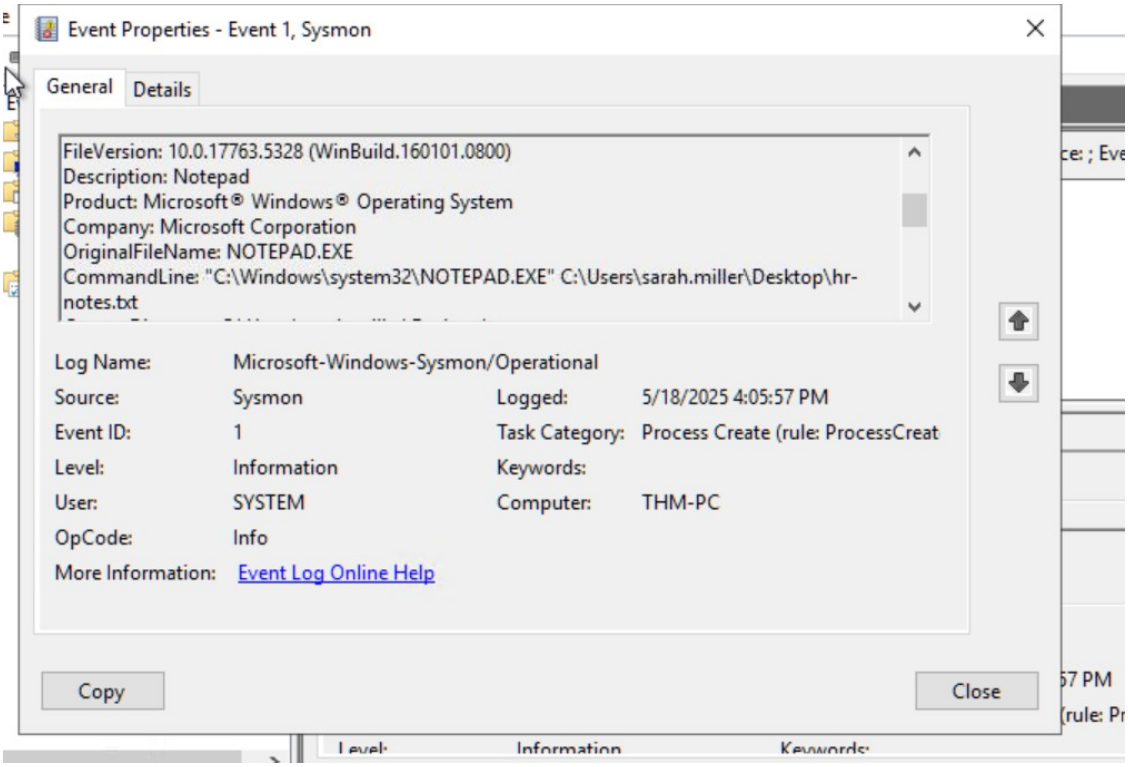

Figure 5.5 — Notepad opening hr-notes.txt — not the browser.

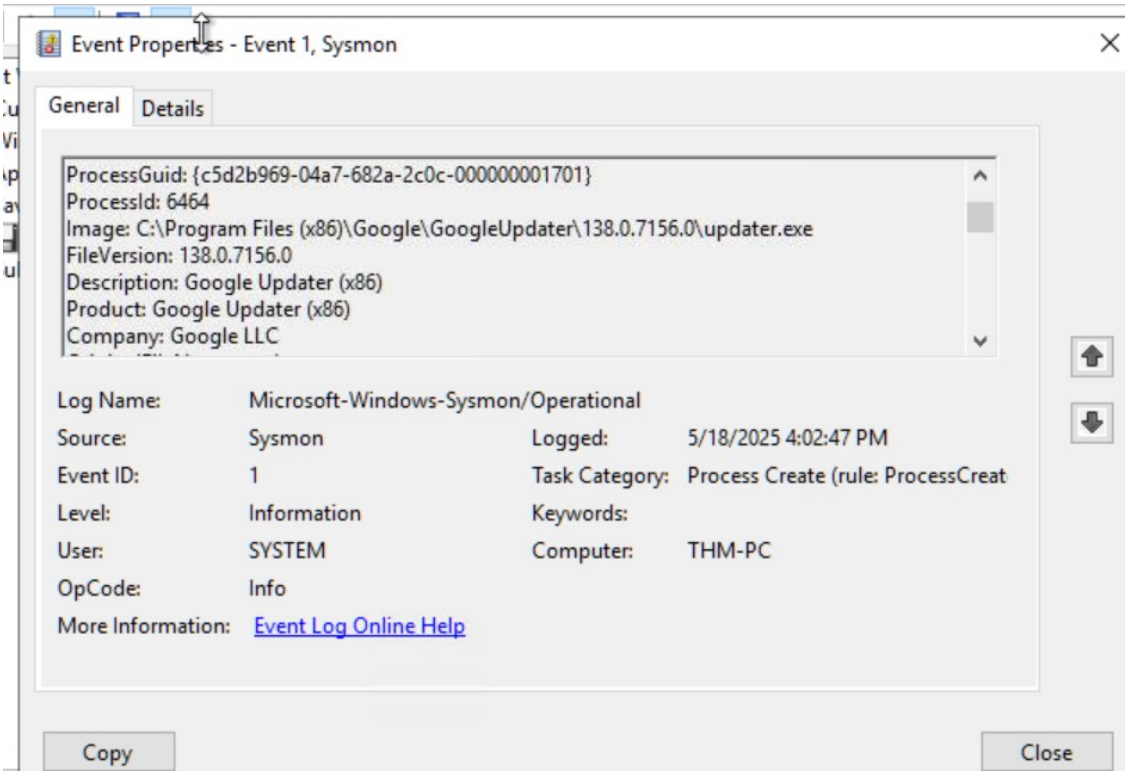

Figure 5.6 — Google Updater process detected, indicating Chrome is installed.

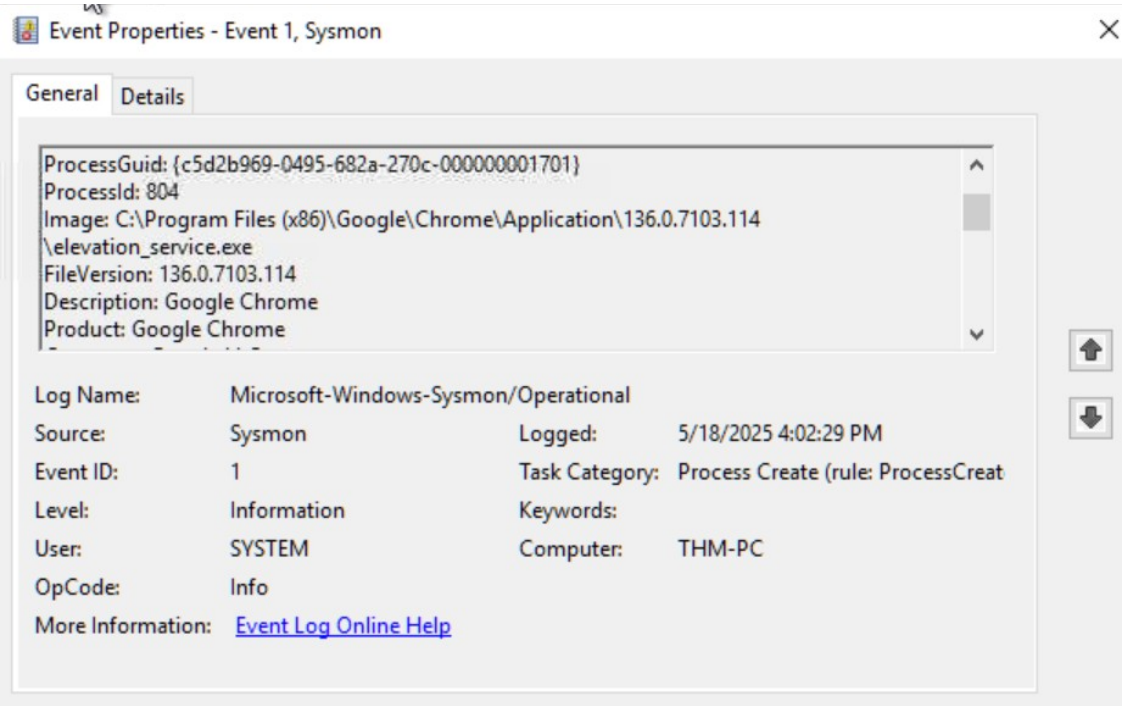

Figure 5.7 — Chrome's elevation_service.exe confirms Google Chrome as the browser in use.

Browser used by Sarah	**Google Chrome**

5.2 File Downloaded

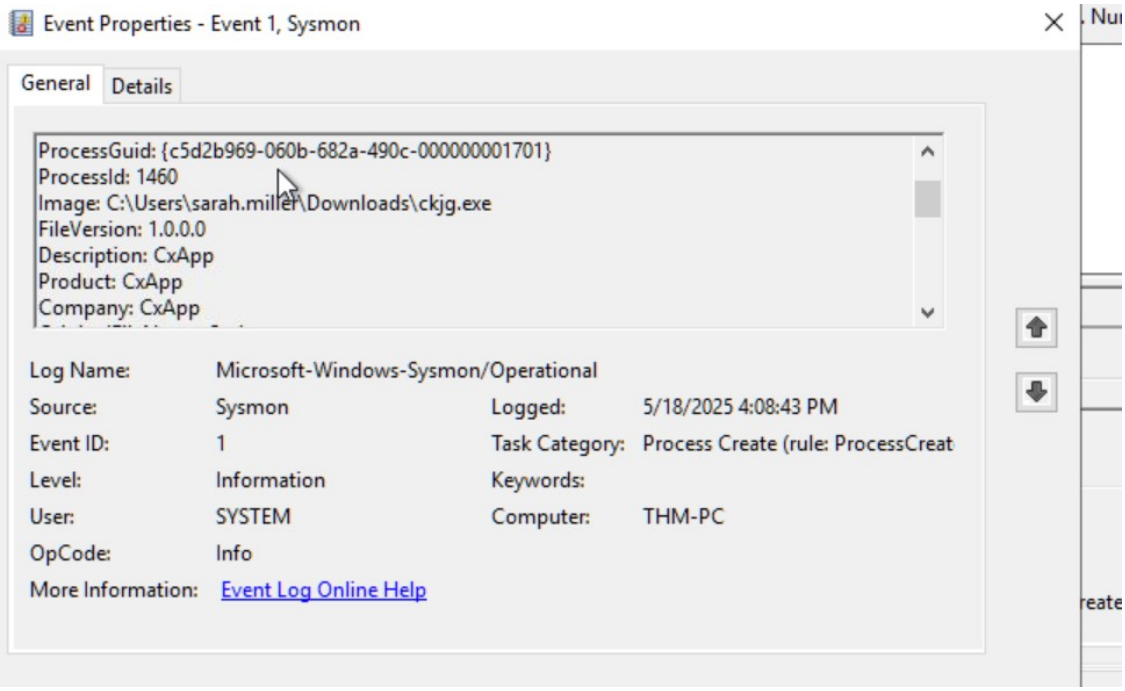

Figure 5.8 — Process ckjg.exe launched from Downloads, vaguely described as "CxApp" — a disguised/malicious executable.

File downloaded	**C:\Users\sarah.miller\Downloads\ckjg.exe**

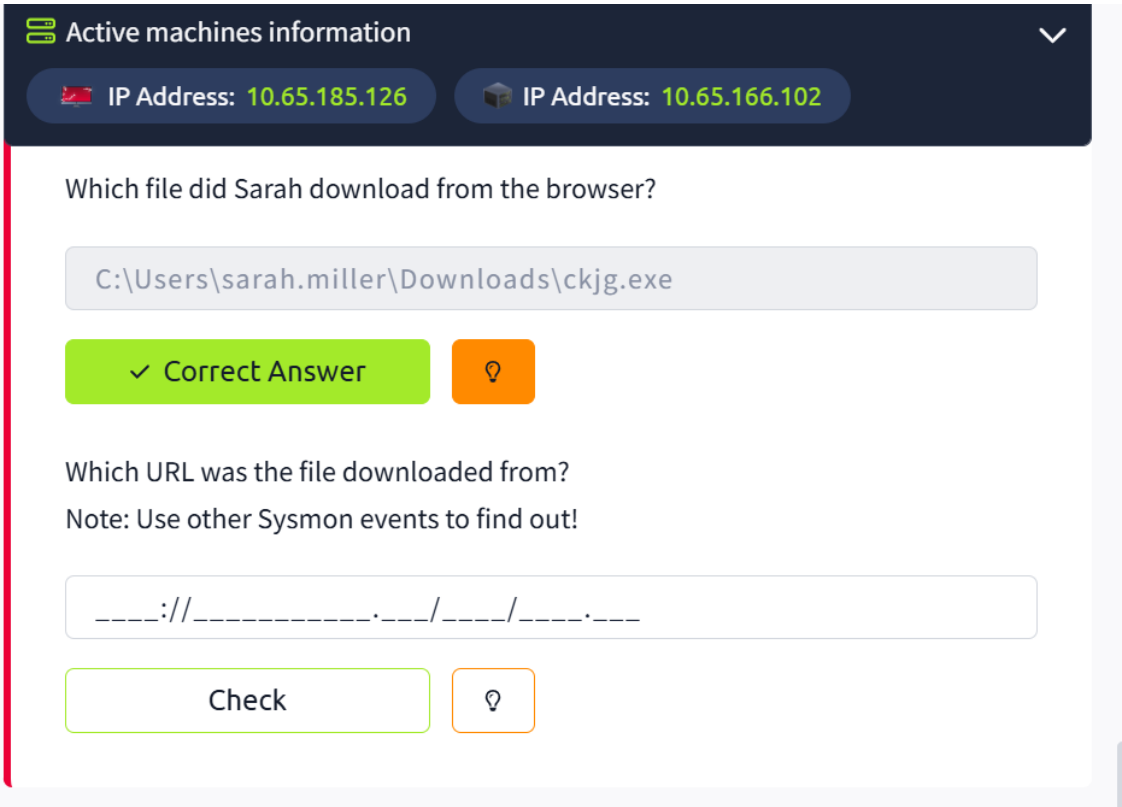

Figure 5.9 — Answer confirmed correct in the room interface.

5.3 Source URL of the Download

Method: Event ID 15 (FileCreateStreamHash) records the Zone.Identifier alternate data stream that browsers attach to downloaded files, which can include the referring and host URLs (reference: SANS ISC diary, "Sysmon and Alternate Data Streams").

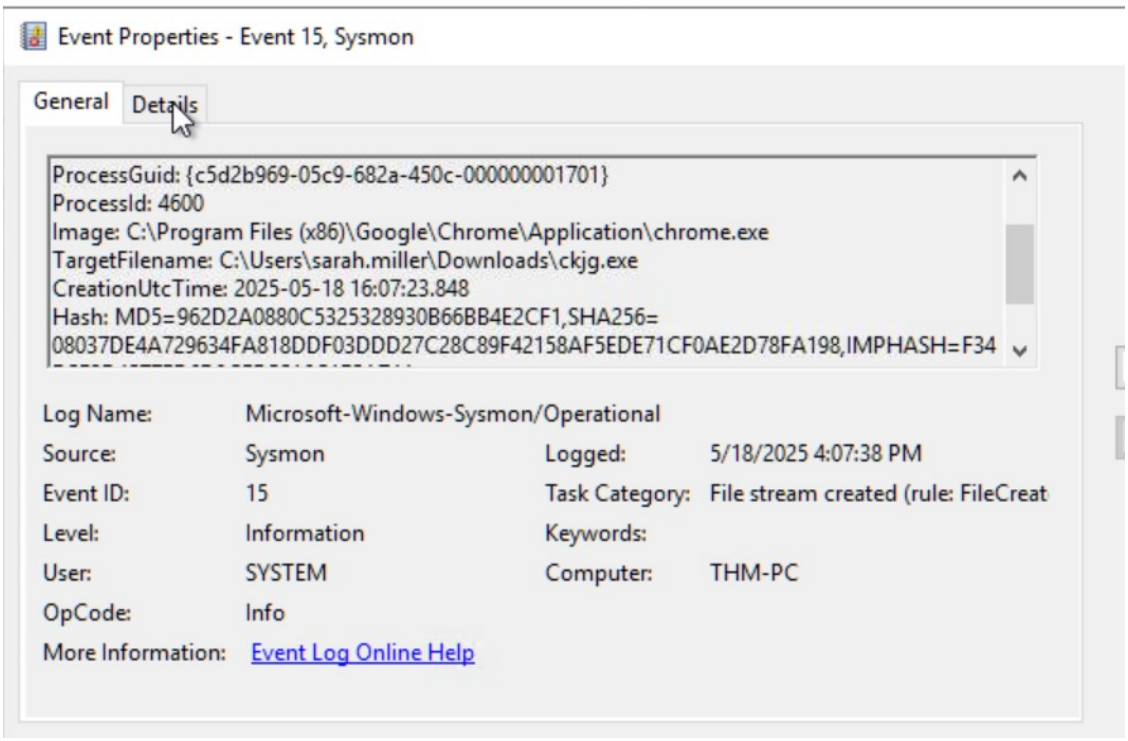

Figure 5.10 — Event 15 confirming chrome.exe created the file ckjg.exe.

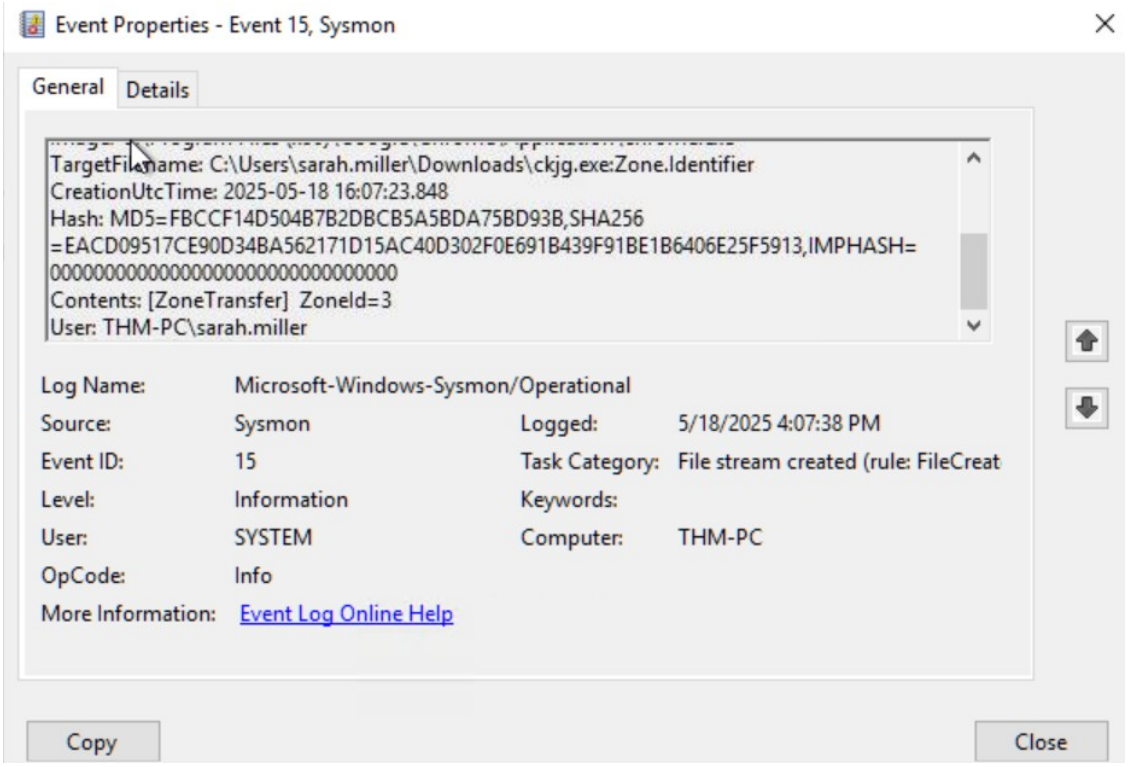

Figure 5.11 — Zone.Identifier stream event showing ZoneId=3 (Internet zone).

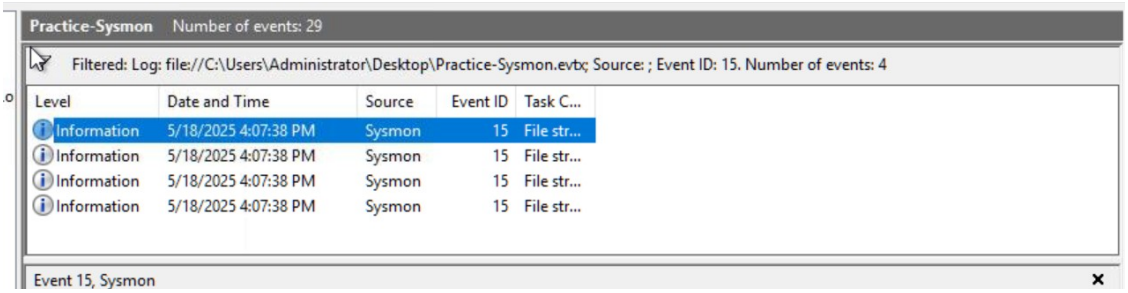

Figure 5.12 — All four Event ID 15 entries reviewed for this file.

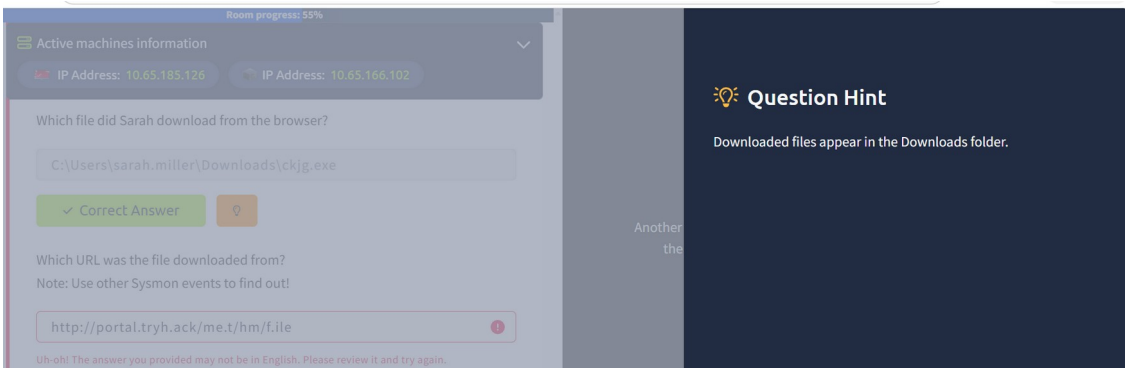

Figure 5.13 — In-room hint confirming downloaded files appear in the Downloads folder.

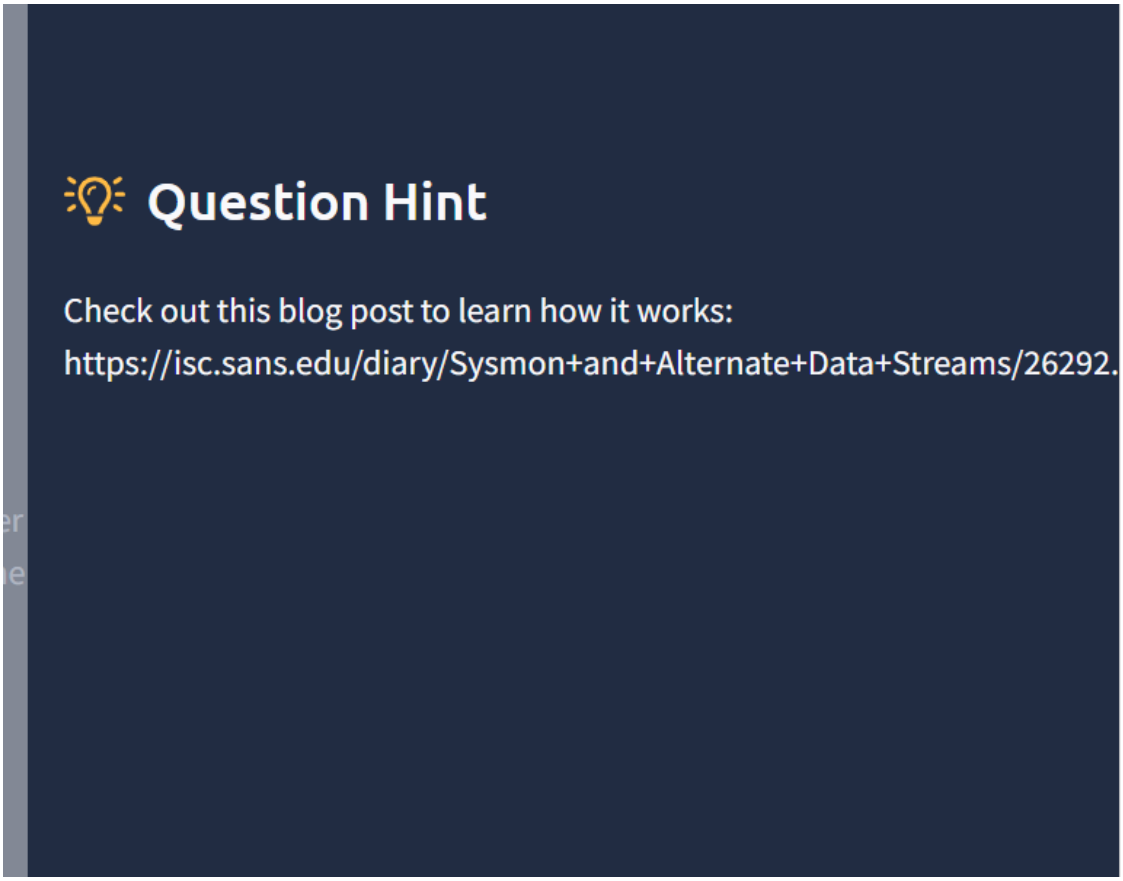

Figure 5.14 — In-room hint pointing to the SANS ISC diary on Sysmon Alternate Data Streams.

Download URL	http://gettsveriff.com/bgj3/ckjg.exe

6. Task 6 — Sysmon: Files and Network

6.1 Persistence File

Persistence file	C:\Users\sarah.miller\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\DeleteApp.url

Placing a .url shortcut file in the Startup folder is a simple, common persistence technique that automatically executes on every subsequent user login.

6.2 Command & Control Server

Method: Filter Event ID 3 (Network Connection) and inspect the Image and Destination fields.

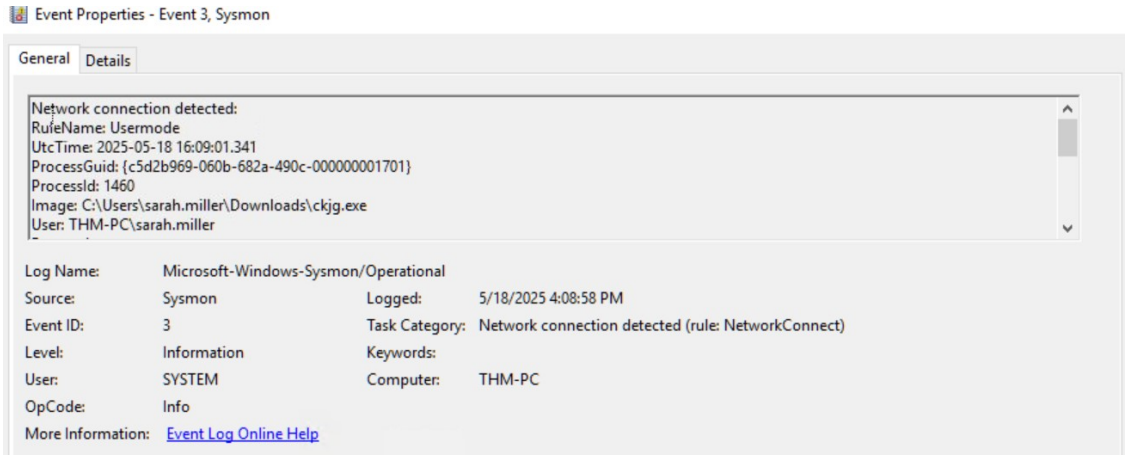

Figure 6.1 — Network connection detected, initiated by ckjg.exe (the downloaded malware).

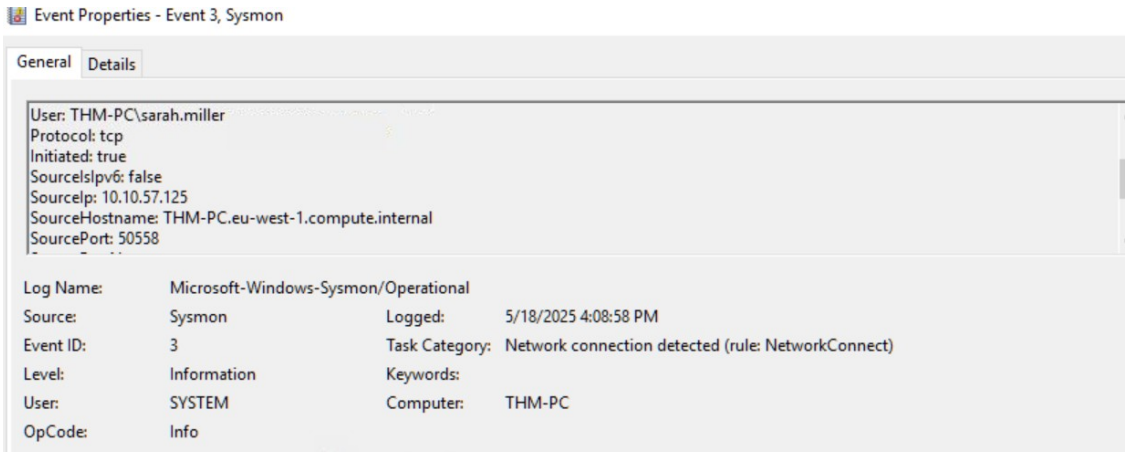

Figure 6.2 — Source connection details: sarah.miller, TCP, source IP and port.

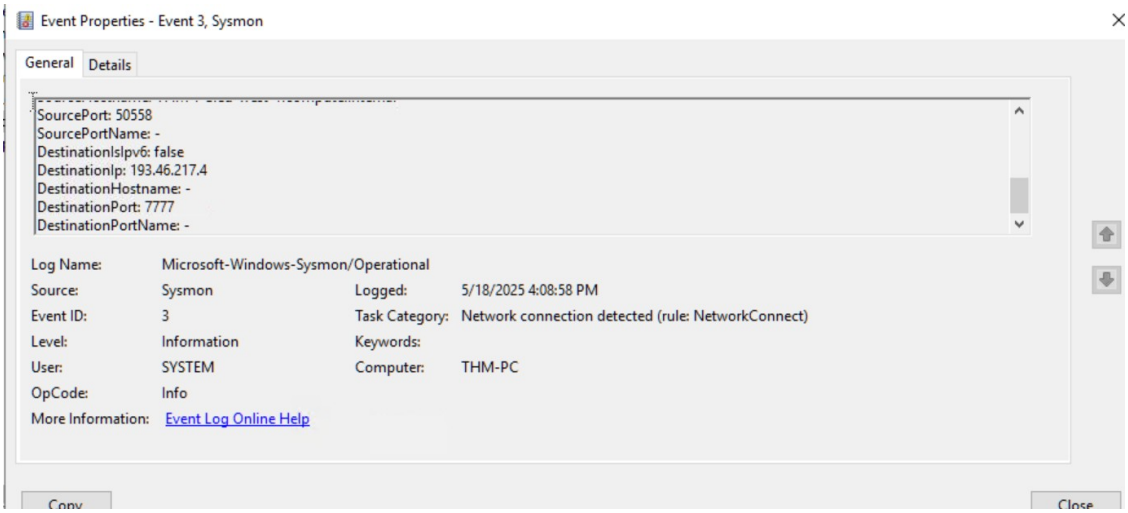

Figure 6.3 — Destination fields revealing the C2 server IP and port.

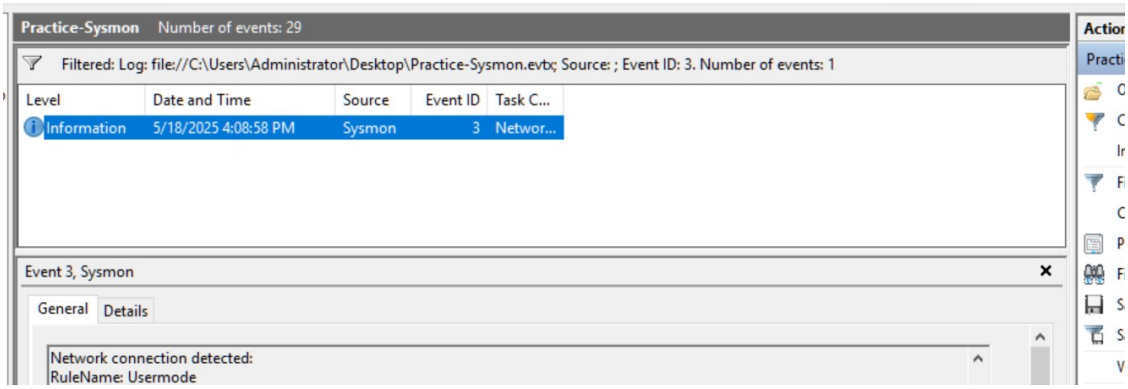

Figure 6.4 — Confirming this was the only Event ID 3 entry in the log.

C2 server (IP:Port)	193.46.217.4:7777

6.3 Malicious Domain

Domain resolving to C2 IP	hkfasfsafg.click

A random-character domain name paired with a low-cost, high-abuse top-level domain (.click) is a common indicator of malicious infrastructure.

7. Task 7 — PowerShell History Review

Performed directly on the Windows VM by reviewing the Administrator's PowerShell history file.

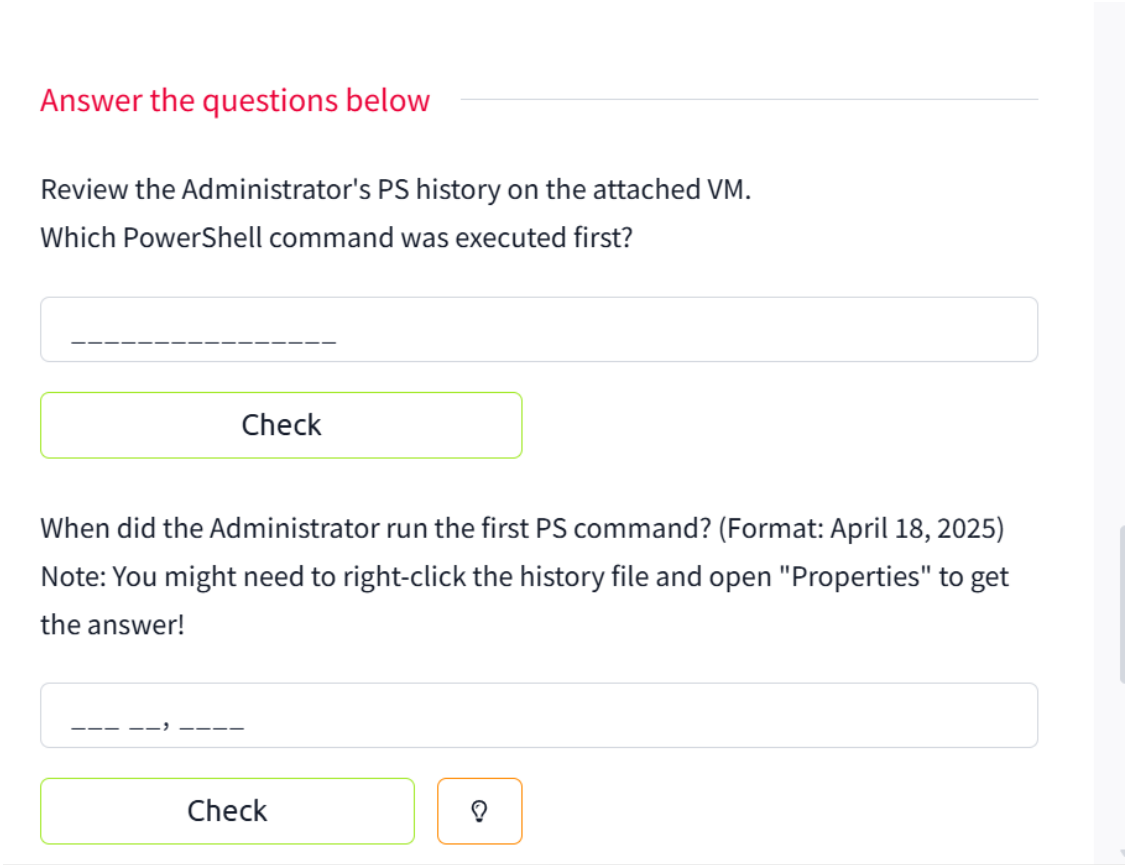

Figure 7.1 — Task interface for PowerShell history questions.

7.1 First PowerShell Command Executed

ANSWER	Get-ComputerInfo

A reconnaissance command commonly run early by an attacker (or administrator) to profile a system's OS version, hotfixes, hardware, and domain membership.

7.2 Date First Command Was Run

ANSWER	May 18, 2025

Found via right-click -> Properties on the PowerShell history file (ConsoleHost_history.txt), checking the file's creation/modified timestamp, consistent with the timeline of the Sysmon-logged activity.

7.3 Flag in PowerShell History

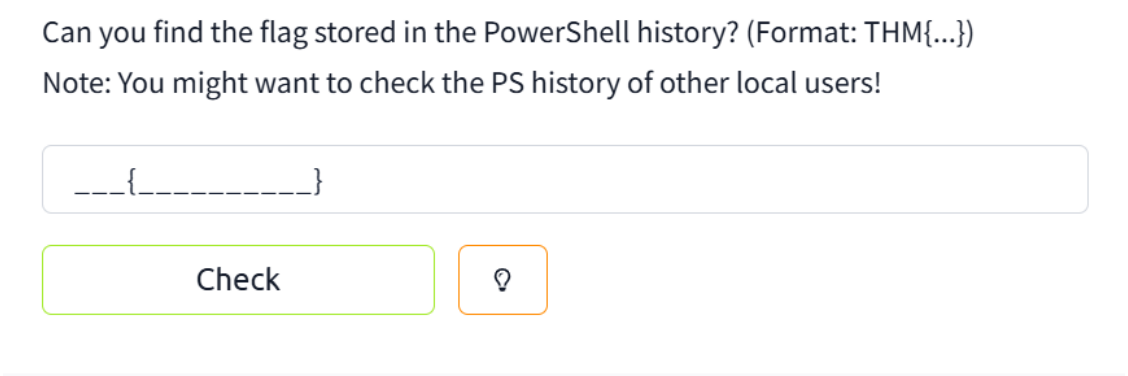

Figure 7.2 — Final task question requesting the flag.

Flag	THM{it_was_me!}

Found by checking the PowerShell history of other local users on the system, not just the Administrator account, per the in-room hint.

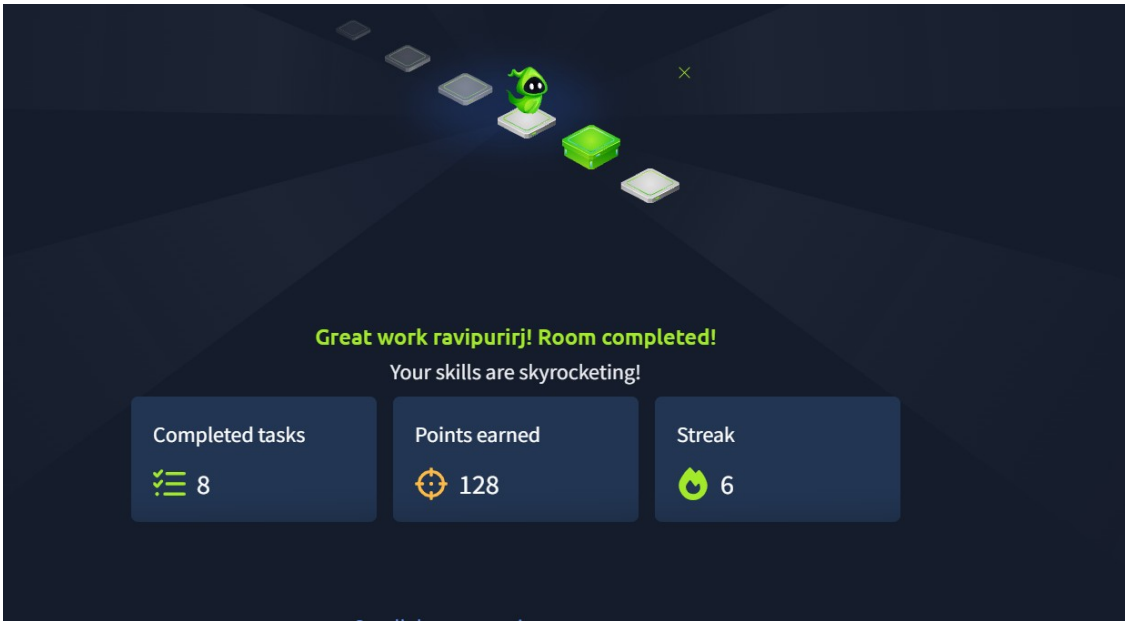

Figure 7.3 — Room completion screen: 128 points, 8/8 tasks completed.

8. Summary and Attack Chain

The investigation reconstructed the following end-to-end attack chain:

- 1. Initial access: Brute-force RDP attack from 10.10.53.248 — 14 failed logon attempts (Event ID 4625) within seconds before succeeding.
- 2. Compromise: Successful RDP logon (Event ID 4624, Logon Type 10) as Administrator, Logon ID 0x183c36d.
- 3. Backdoor account: A new local account, svc_sysrestore, was created (Event ID 4720) under the same attacker session.
- 4. Privilege escalation: The backdoor account was added to Backup Operators and Remote Desktop Users (Event ID 4732).
- 5. Malware delivery: User sarah.miller downloaded ckjg.exe via Google Chrome from http://gettsveriff.com/bgj3/ckjg.exe (Sysmon Event IDs 1 and 15).
- 6. Persistence: The malware placed a .url shortcut in the Startup folder for automatic execution on login (Sysmon Event ID 11).
- 7. Command and Control: The malware connected to 193.46.217.4:7777, resolving to the domain hkfasfsafg.click (Sysmon Event ID 3).
- 8. Post-exploitation: PowerShell history on the Administrator account showed reconnaissance (Get-ComputerInfo) dated May 18, 2025, and a flag was recovered from another local user's PowerShell history.

Event ID Reference Table

Stage	Event ID(s)	Purpose
Brute force	4625	Failed logon attempts
Compromise	4624	Successful logon; Logon Type reveals RDP (10)
Backdoor creation	4720	New local account created
Privilege escalation	4732 / 4728	Group membership changes
Malware download	Sysmon 1, 15	Process creation; browser download metadata
Persistence	Sysmon 11	New file creation (Startup folder)
C2 communication	Sysmon 3	Outbound network connections

Detection and Monitoring Recommendations

- Alert on repeated 4625 events from a single source IP within a short time window, correlated with any 4624 success shortly after from the same account/IP.
- Treat 4720 (account creation) and 4732/4728 (privileged group changes) as high-priority alerts, especially when tied to a Logon ID from a recent RDP session rather than console access.

- Deploy Sysmon with Zone.Identifier ADS logging enabled to capture browser download provenance for forensic reconstruction of malware delivery.
- Flag outbound connections to non-standard high ports (e.g. 7777) as potential C2 traffic, especially from user-writable directories such as Downloads.
- Regularly audit Startup folder contents and scheduled tasks across all user profiles for unauthorized persistence mechanisms.