

Event-Viewing

- First we create a Python Environment...
- Then we convert the evtx file into a logs.xml file using this tool we installed:

The screenshot shows a terminal window on a Kali Linux desktop. The user has navigated to their home directory and run several commands to set up a virtual environment and install a tool named 'python-evtx'. Finally, they run the command `evtx_dump Windows_Logs.evtx --format xml > logs.xml` to convert the event log file into XML format.

```
$ ls
$ python3 -m venv evtx-env
$ source evtx-env/bin/activate
$ pip install python-evtx
Collecting python-evtx
  Using cached python_evtx-0.8.1-py3-none-any.whl.metadata (6.0 kB)
Collecting hexdump>3.3 (from python-evtx)
  Using cached hexdump-3.3-py3-none-any.whl (26 kB)
Using cached python_evtx-0.8.1-py3-none-any.whl (26 kB)
Installing collected packages: hexdump, python-evtx
Successfully installed hexdump-3.3 python-evtx-0.8.1
$ evtx_dump Windows_Logs.evtx --format xml > logs.xml
```

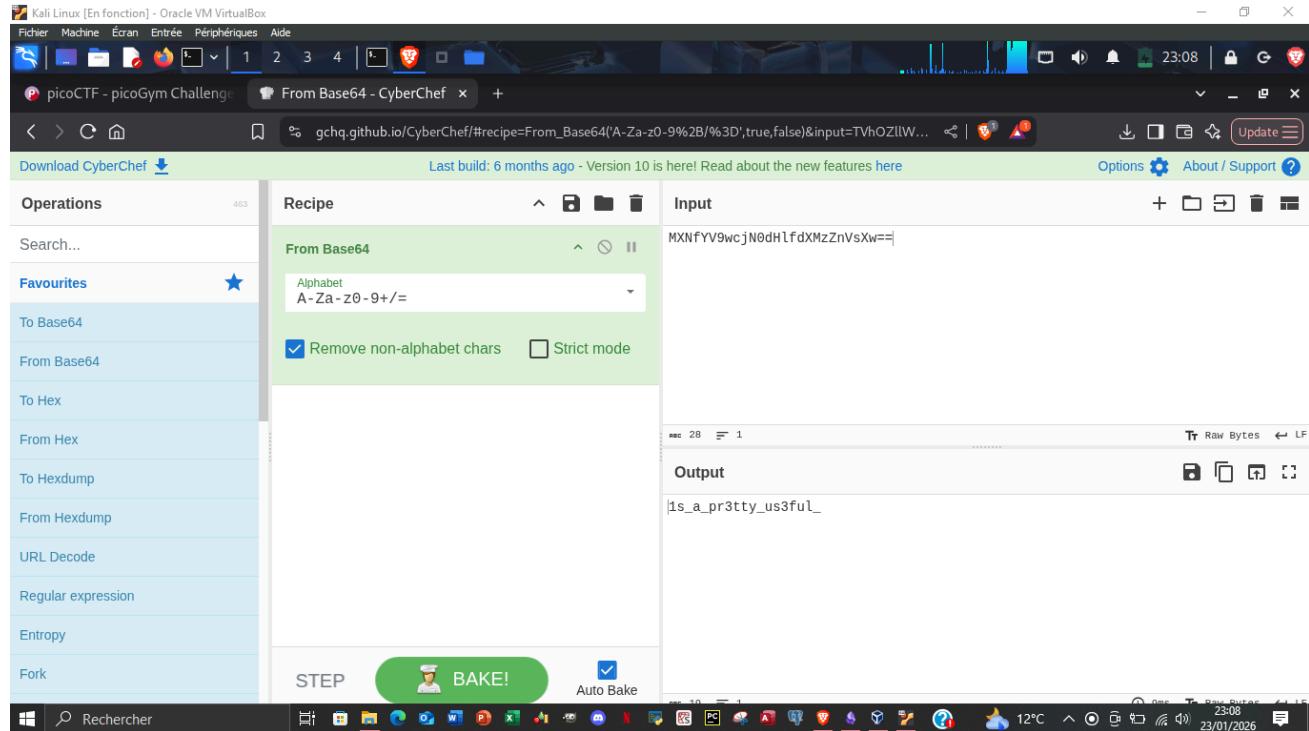
- Then we open that file xml:

The screenshot shows a Microsoft Edge browser window displaying the XML content of the 'logs.xml' file. The XML structure includes various event details such as time created, subject user ID, and object name.

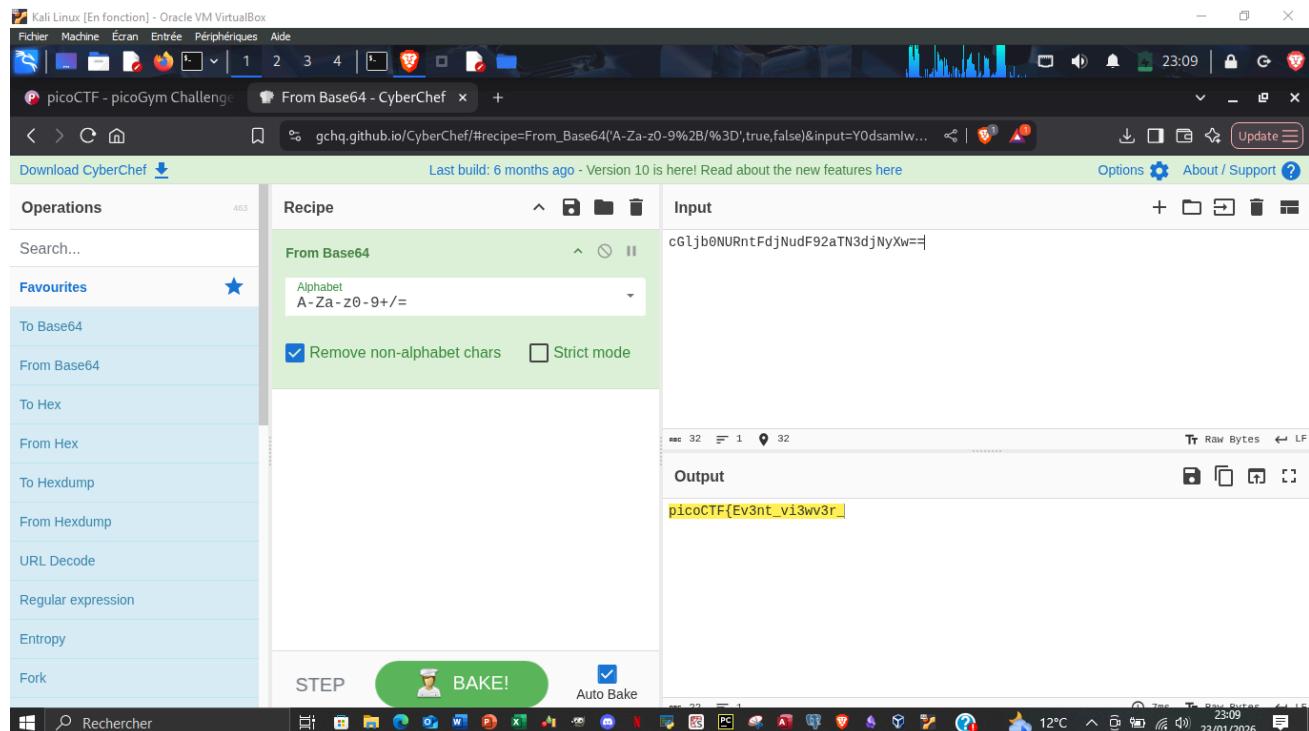
```
<Event>
  <System>
    <Provider Name="Microsoft-Windows-Security-Auditing" />
    <EventID Qualifiers="4658">4658</EventID>
    <Version>0</Version>
  </System>
  <Keywords>0x8020000000000000</Keywords>
  <TimeCreated SystemTime="2024-07-15T15:56:19.103197+00:00" />
  <EventRecordID>168656</EventRecordID>
  <Correlation ActivityID="" RelatedActivityID="" />
  <Execution ProcessID="4" ThreadID="1084" />
  <Channel>Security</Channel>
  <Computer>DESKTOP-EKVR84B</Computer>
  <Security UserID="" />
  <System>
    <EventData><Data Name="SubjectUserName">S-1-5-21-3576963320-1344788273-4164204335-1001</Data>
    <Data Name="SubjectDomainName">user</Data>
    <Data Name="SubjectLogonId">0x000000000000a428</Data>
    <Data Name="ObjectName">\REGISTRY\ACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run</Data>
    <Data Name="ObjectValueName">Immediate Shutdown [XNfyY9wcjN0dHlfDXMzNvSw==]</Data>
    <Data Name="HandleId">0x0000000000000208</Data>
    <Data Name="OperationType">%1904</Data>
    <Data Name="OldValueType">-</Data>
    <Data Name="OldValue"></Data>
    <Data Name="NewValueType">%1873</Data>
    <Data Name="newValue">C:\Program Files (x86)\Totally_Legit_Software\custom_shutdown.exe</Data>
    <Data Name="ProcessId">0x000000000001bd0</Data>
    <Data Name="ProcessName">C:\Program Files (x86)\Totally_Legit_Software\Totally_Legit_Software.exe</Data>
  </EventData>
  <Event>
```

- And so, we investigate that file for anything suspicious...
- As we know, the flag is divided in three pieces...

- We decode the first piece:



- here's the second piece:



- The last piece after I filtered with "shutdown":

```

<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><System><Provider Name="Microsoft-Windows-Security-Auditing" Qualifiers="4658"/><EventID>32768</EventID><Version>0</Version><Level>4</Level><Task>0</Task><Opcode>0</Opcode><Keywords>0x8080000000000000</Keywords><TimeCreated SystemTime="2024-07-15 17:01:05.393583+00:00"/><EventRecordID>3801</EventRecordID><Correlation ActivityID="" RelatedActivityID="" /><Execution ProcessID="432" ThreadID="3496" /><Channel>System</Channel><Computer>DESKTOP-EKVR84B</Computer><Security UserID="S-1-5-21-3576963320-1344788273-4164204335-1001" /><System><EventData><Data Name="param1">C:\Windows\system32\shutdown.exe (DESKTOP-EKVR84B)</Data><Data Name="param2">DESKTOP-EKVR84B</Data><Data Name="param3">No title for this reason could be found</Data><Data Name="param4">0x800000ff</Data><Data Name="param5">shutdown</Data><Data Name="param6">dDAwbF84MwJhM2ZlOx0</Data><Data Name="param7">DESKTOP-EKVR84B\user</Data></EventData></Event>

```

Download CyberChef [Download](#)

Last build: 6 months ago - Version 10 is here! Read about the new features [here](#)

Operations 463

Search...

Favourites

To Base64

From Base64

To Hex

From Hex

To Hexdump

From Hexdump

URL Decode

Regular expression

Entropy

Fork

Recipe

From Base64

Alphabet: A-Za-z0-9+/=

Remove non-alphabet chars Strict mode

Input

dDAwbF84MwJhM2ZlOx0=

Output

t001_81ba3fe9}

STEP Auto Bake

- The flag :

