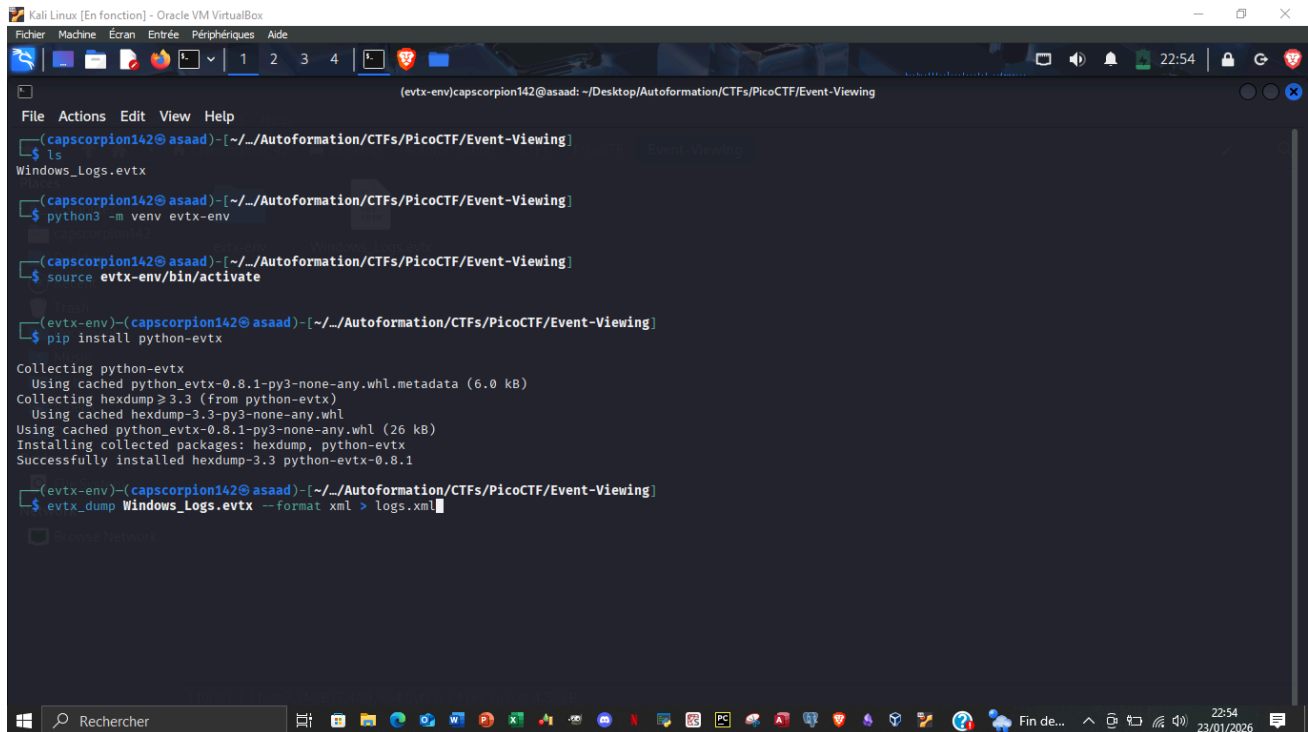


Event-Viewing

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



```
Kali Linux [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide

(evtx-env)capscorpion142@asaad: ~/Desktop/Autoformation/CTFs/PicoCTF/Event-Viewing

$ ls
Windows_Logs.evtx

$ python3 -m venv evtx-env

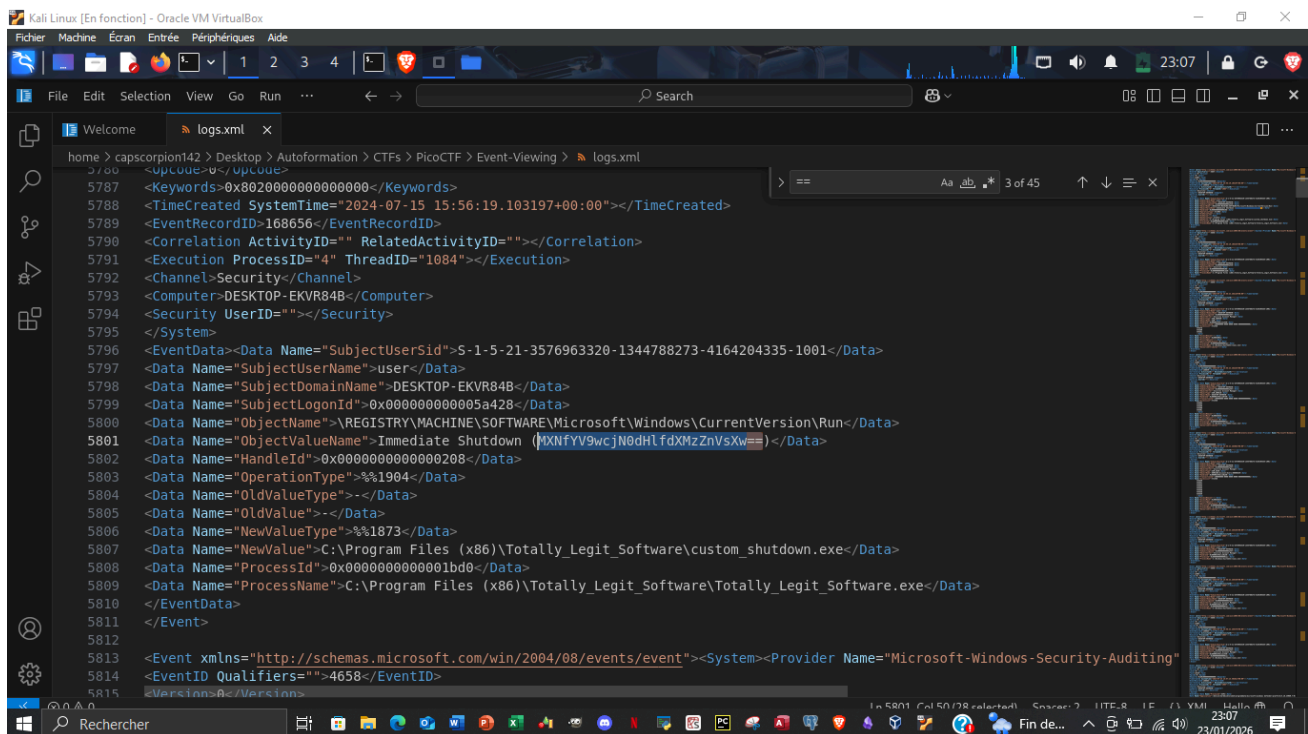
$ source evtx-env/bin/activate

(evtx-env)-(capscorpion142@asaad) ~/Desktop/Autoformation/CTFs/PicoCTF/Event-Viewing
$ 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
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-env)-(capscorpion142@asaad) ~/Desktop/Autoformation/CTFs/PicoCTF/Event-Viewing
$ evtx_dump Windows_Logs.evtx --format xml > logs.xml
```

- Then we open that file xml:



```
Kali Linux [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide

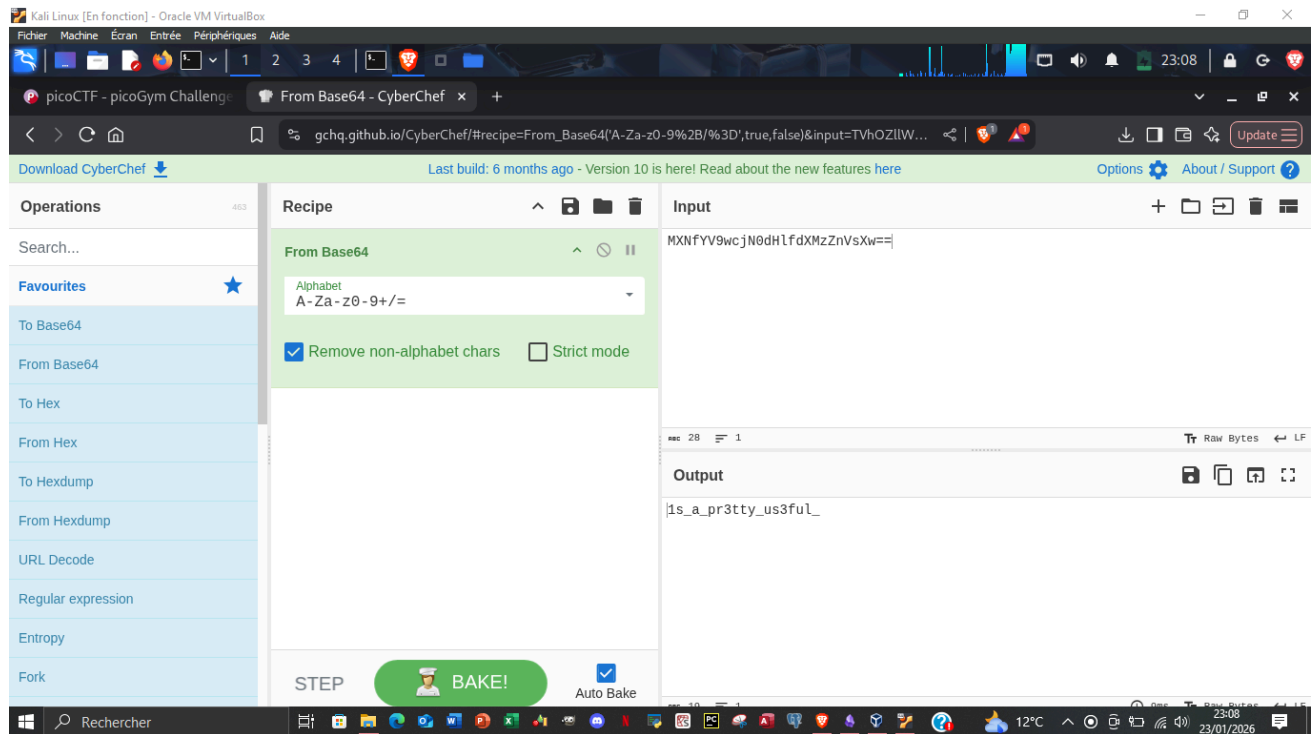
File Edit Selection View Go Run ... Search

home > capscorpion142 > Desktop > Autoformation > CTFs > PicoCTF > Event-Viewing > logs.xml

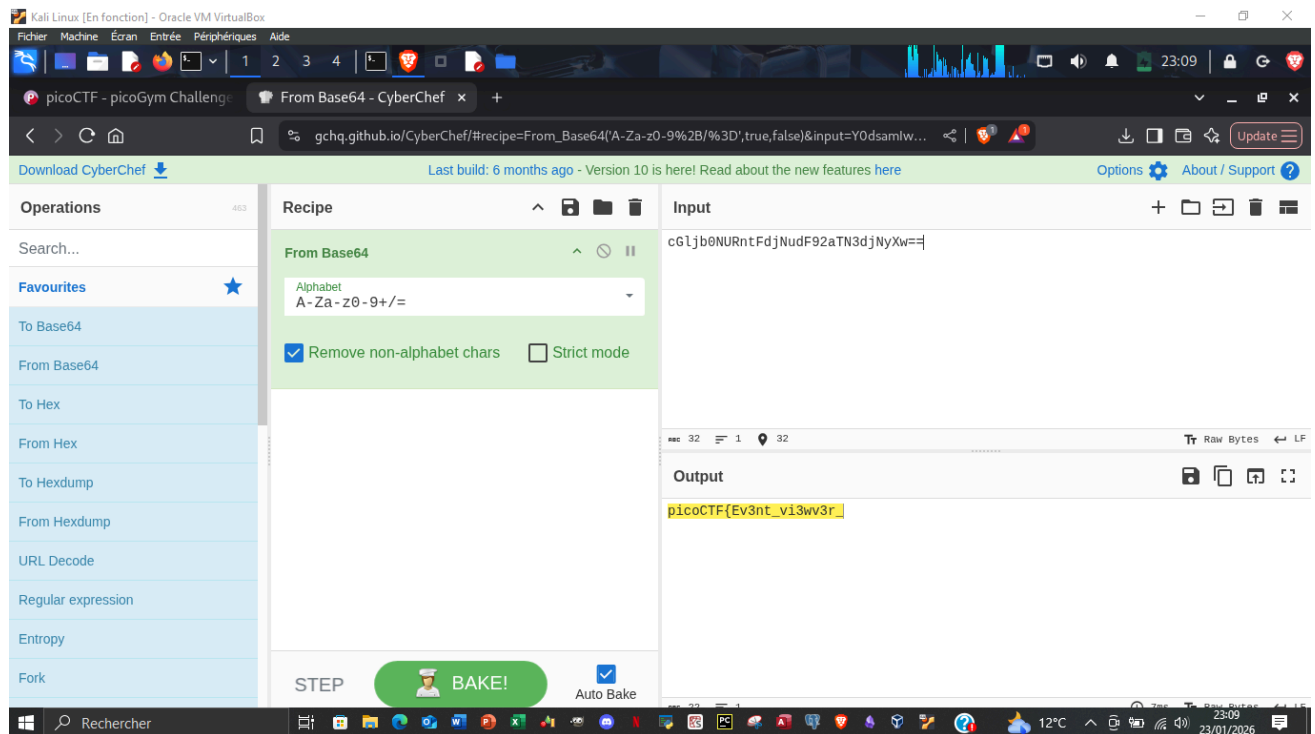
5787 <Keywords>0x8020000000000000</Keywords>
5788 <TimeCreated SystemTime>2024-07-15 15:56:19.103197+00:00</TimeCreated>
5789 <EventRecordID>168656</EventRecordID>
5790 <Correlation ActivityID="" RelatedActivityID=""></Correlation>
5791 <Execution ProcessID="4" ThreadID="1084"></Execution>
5792 <Channel>Security</Channel>
5793 <Computer>DESKTOP-EKVR84B</Computer>
5794 <Security UserID=""></Security>
5795 </System>
5796 <EventData><Data Name="SubjectUserSid">S-1-5-21-3576963320-1344788273-4164204335-1001</Data>
5797 <Data Name="SubjectUserName">user</Data>
5798 <Data Name="SubjectDomainName">DESKTOP-EKVR84B</Data>
5799 <Data Name="SubjectLogonId">0x00000000000005a428</Data>
5800 <Data Name="ObjectName">\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run</Data>
5801 <Data Name="ObjectValueName">Immediate Shutdown (0XNfYV9wcjN0dHlfdXmZznVsXw==)</Data>
5802 <Data Name="HandleId">0x0000000000000208</Data>
5803 <Data Name="OperationType">%%1904</Data>
5804 <Data Name="OldValueType"></Data>
5805 <Data Name="OldValue"></Data>
5806 <Data Name="NewValueType">%%1873</Data>
5807 <Data Name="NewValue">C:\Program Files (x86)\Totally_Legit_Software\custom_shutdown.exe</Data>
5808 <Data Name="ProcessId">0x00000000000001bd0</Data>
5809 <Data Name="ProcessName">C:\Program Files (x86)\Totally_Legit_Software\Totally_Legit_Software.exe</Data>
5810 </EventData>
5811 </Event>
5812
5813 <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><System><Provider Name="Microsoft-Windows-Security-Auditing"
5814 <EventID Qualifiers="">4658</EventID>
5815 <Versions></Versions>
```

- 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":

```
home > capscontrol42 > Desktop > Autoformation > CTFs > PicoCTF > Event-Viewing > logs.xml
170152 <EventID Qualifiers="32768">1074</EventID>
170153 <Version>0</Version>
170154 <Level>4</Level>
170155 <Task>0</Task>
170156 <Opcode>0</Opcode>
170157 <Keywords>0x8000000000000000</Keywords>
170158 <TimeCreated SystemTime="2024-07-15 17:01:05.393583+00:00"></TimeCreated>
170159 <EventRecordID>3801</EventRecordID>
170160 <Correlation ActivityID="" RelatedActivityID=""></Correlation>
170161 <Execution ProcessID="432" ThreadID="3496"></Execution>
170162 <Channel>System</Channel>
170163 <Computer>DESKTOP-EKVR84B</Computer>
170164 <Security UserID="S-1-5-21-3576963320-1344788273-4164204335-1001"></Security>
170165 </System>
170166 <EventData><Data Name="param1">C:\Windows\system32\shutdown.exe (DESKTOP-EKVR84B)</Data>
170167 <Data Name="param2">DESKTOP-EKVR84B</Data>
170168 <Data Name="param3">No title for this reason could be found</Data>
170169 <Data Name="param4">0x800000ff</Data>
170170 <Data Name="param5">shutdown</Data>
170171 <Data Name="param6">dDAwbF84MWJhM2ZlOX0=</Data>
170172 <Data Name="param7">DESKTOP-EKVR84B\user</Data>
170173 </EventData>
170174 </Event>
170175
170176 <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><System><Provider Name="Microsoft-Windows-Security-Auditing"
170177 <EventID Qualifiers="">4658</EventID>
170178 <Version>0</Version>
170179 <Level>0</Level>
170180 <Task>12812</Task>
```

Download CyberChef Last build: 6 months ago - Version 10 is here! Read about the new features here Options About / Support

Operations 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 t00l_81ba3fe9

STEP **BAKE!** Auto Bake

- The flag :

