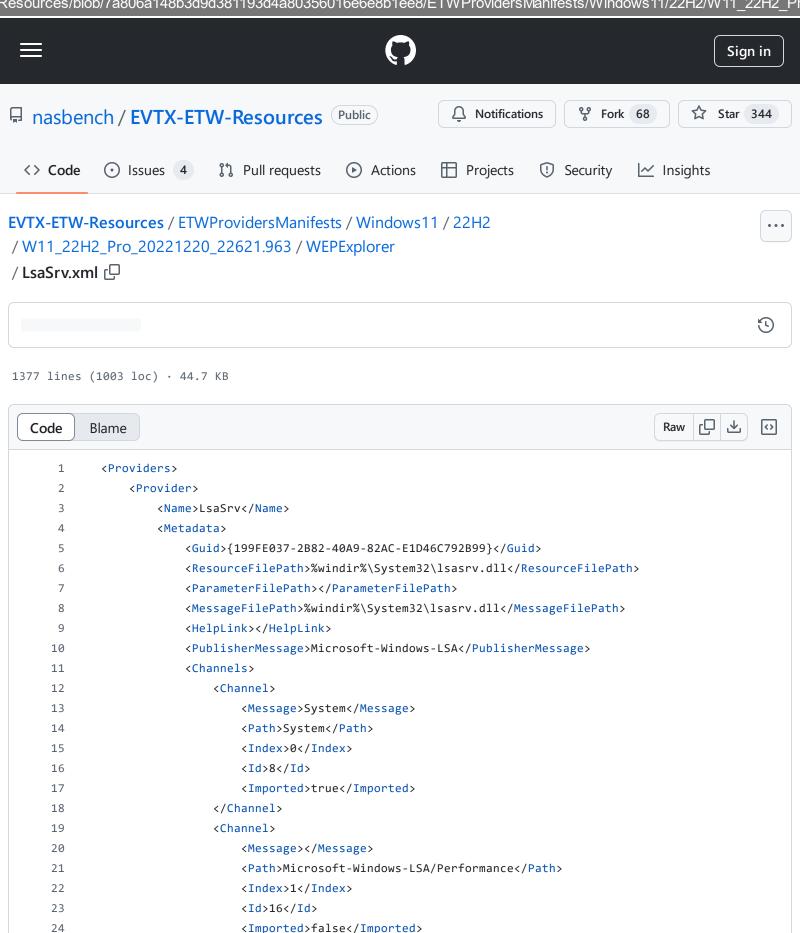
Resources/ETWProvidersManifests/Windows11/22H2/W11\_22H2\_Pro\_20221220\_22621.963/WEPExplorer/LsaSrv.xml at 7a806a148b3d9d381193d4a80356016e6e8b1ee8 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 15:42 https://github.com/nasbench/EVTX-ETW-

Resources/blob/7a806a148b3d9d381193d4a80356016e6e8b1ee8/ETWProvidersManifests/Windows11/22H2/W11 22H2 ProvidersManifests/Windows11/22H2/W11 22H2 ProvidersWandows11/22H2/W11 22H2 ProvidersWandows11/22H2/W11 22H2 ProvidersWandows11/22H2/W11 22H2/W11 22H2/W



Resources/ETWProvidersManifests/Windows11/22H2/W11\_22H2\_Pro\_20221220\_22621.963/WEPExplorer/LsaSrv.xml at 7a806a148b3d9d381193d4a80356016e6e8b1ee8 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 15:42 https://github.com/nasbench/EVTX-ETW-

Resources/blob/7a806a148b3d9d381193d4a80356016e6e8b1ee8/ETWProvidersManifests/Windows11/22H2/W11 22H2 Providers

```
25
                        </Channel>
26
                         <Channel>
27
                             <Message>Operational</Message>
28
                             <Path>Microsoft-Windows-LSA/Operational</Path>
29
                             <Index>2</Index>
30
                             <Id>17</Id>
31
                             <Imported>false</Imported>
32
                        </Channel>
33
                         <Channel>
34
                             <Message>Diagnostic</Message>
35
                             <Path>Microsoft-Windows-LSA/Diagnostic</Path>
36
                             <Index>3</Index>
37
                             <Id>18</Id>
38
                             <Imported>false</Imported>
39
                        </Channel>
40
                    </Channels>
41
                    <Levels>
42
                        <Level>
43
                             <Message>Critical</Message>
44
                             <Name>win:Critical</Name>
                             <Value>1</Value>
46
                        </Level>
47
                        <Level>
48
                             <Message>Error</Message>
49
                             <Name>win:Error</Name>
50
                             <Value>2</Value>
51
                        </Level>
52
                         <Level>
53
                             <Message>Warning</Message>
54
                             <Name>win:Warning</Name>
55
                             <Value>3</Value>
56
                        </Level>
57
                        <Level>
58
                             <Message>Information</Message>
59
                             <Name>win:Informational</Name>
                             <Value>4</Value>
60
61
                        </Level>
62
                    </Levels>
63
                    <Tasks>
64
65
                             <Message>Security Package Manager</Message>
66
                             <Name>CATEGORY SPM</Name>
67
                             <Value>1</Value>
68
                        </Task>
69
                        <Task>
70
                             <Messages| ocator</pre>/Messages
```

Resources/ETWProvidersManifests/Windows11/22H2/W11\_22H2\_Pro\_20221220\_22621.963/WEPExplorer/LsaSrv.xml at 7a806a148b3d9d381193d4a80356016e6e8b1ee8 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 15:42 https://github.com/nasbench/EVTX-ETW-

Resources/blob/7a806a148b3d9d381193d4a80356016e6e8b1ee8/ETWProvidersManifests/Windows11/22H2/W11 22H2 Providers

```
THESSUBER EDUCATOR THESSUBER
 71
                             <Name>CATEGORY_LOCATOR</Name>
 72
                             <Value>2</Value>
 73
                         </Task>
 74
                         <Task>
 75
                             <Message>SPNEGO (Negotiator)
 76
                             <Name>CATEGORY NEGOTIATE</Name>
 77
                             <Value>3</Value>
 78
                         </Task>
 79
                         <Task>
 80
                              <Message>Logon Cache</Message>
                             <Name>CATEGORY_LOGON_CACHE</Name>
 81
 82
                              <Value>4</Value>
 83
                         </Task>
 84
                         <Task>
 85
                             <Message>LSA Logon</Message>
 86
                             <Name>CATEGORY_LSA_LOGON</Name>
 87
                             <Value>5</Value>
 88
                         </Task>
 89
                         <Task>
 90
                              <Message>LSA SID-Name Lookup</Message>
 91
                             <Name>CATEGORY_LSA_LOOKUP</Name>
 92
                             <Value>6</Value>
 93
                         </Task>
 94
                         <Task>
 95
                             <Message>Max</Message>
96
                             <Name>CATEGORY MAX CATEGORY</Name>
 97
                             <Value>7</Value>
 98
                         </Task>
99
                     </Tasks>
100
                     <Opcodes>
                         <Opcode>
101
102
                              <Message>Start</Message>
103
                             <Name>win:Start</Name>
                             <Value>1</Value>
104
105
                             <Task>0</Task>
106
                         </Opcode>
107
                         <Opcode>
108
                              <Message>Stop</Message>
109
                             <Name>win:Stop</Name>
                             <Value>2</Value>
110
111
                             <Task>0</Task>
                         </Opcode>
112
                     </Opcodes>
113
114
                     <Keywords>
115
                         <Keyword>
```

Resources/ETWProvidersManifests/Windows11/22H2/W11\_22H2\_Pro\_20221220\_22621.963/WEPExplorer/LsaSrv.xml at 7a806a148b3d9d381193d4a80356016e6e8b1ee8 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 15:42 https://github.com/nasbench/EVTX-ETW-

ht R	ps://github.com/nasbench/EVTX-E esources/blob/7a806a148b3d9d38	:TW- 1193d4a80356016e6e8b1ee8/ETWProvidersManifests/Windows11/22H2/W11_22H2_	Prc
	116	<pre><message></message></pre>	
	117	<name>WPDBusEnumStartTrigger</name>	

EVTX-ETW-Resources/ETWProvidersManifests/Windows11/22H2/W11_22H2_Pro_20221220_22621.963/WEPExplorer/LsaSr at 7a806a148b3d9d381193d4a80356016e6e8b1ee8 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 15:42 https://github.com/nasbench/EVTX-ETW-Resources/blob/7a806a148b3d9d381193d4a80356016e6e8b1ee8/ETWProvidersManifests/Windows11/22H2/W11_24H2/W11_22H	2

EVTX-ETW-Resources/ETWProvidersManifests/Windows11/22H2/W11_22H2_Pro_20221220_22621.963/WE at 7a806a148b3d9d381193d4a80356016e6e8b1ee8 · nasbench/EVTX-ETW-Resources · GitHub https://github.com/nasbench/EVTX-ETW-	- 31/10/2024 15:42
Resources/blob/7a806a148b3d9d381193d4a80356016e6e8b1ee8/ETWProvidersManifests/Windows	11/22H2/W11_22H2_Pr

EVTX-ETW-Resources/ETWProvidersManifests/Windows11/22H2/W11_22H2_Pro_20221220_22621.963/Vat 7a806a148b3d9d381193d4a80356016e6e8b1ee8 · nasbench/EVTX-ETW-Resources · GitHuhttps://github.com/nasbench/EVTX-ETW-Resources/blob/7a806a148b3d9d381193d4a80356016e6e8b1ee8/ETWProvidersManifests/Windows	<b>ub</b> - 31/10/2024 15:42

EVTX-ETW- Resources/ETWProvidersManifests/Windows11/22H2/W11_22H2_Pro_20221220_22621.963/WEPExplorer/LsaSrv.xm at 7a806a148b3d9d381193d4a80356016e6e8b1ee8 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 15:42 https://github.com/nasbench/EVTX-ETW-						
Resources/blob/7a806a148b3d9d381193d4a80356016e6e8b1ee8/ETWProvidersManifests/Windows11/22H2/W11_22	H2_Pr					

EVTX-ETW-Resources/ETWProvidersManifests/Windows11/22H2/W11_22H2_Pro_20221220_22621.963/WEPExplorer/LsaSrv.xr at 7a806a148b3d9d381193d4a80356016e6e8b1ee8 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 15:42 https://github.com/nasbench/EVTX-ETW-Resources/blob/7a806a148b3d9d381193d4a80356016e6e8b1ee8/ETWProvidersManifests/Windows11/22H2/W11 22H2 F	
Resources/blob/7a80ba148b3d9d381193d4a8035b01bebe8b1ee8/E1WProvidersivanilests/Windows11/22H2/W11_22H2_F	11

EVTX-ETW- Resources/ETWProvidersManifests/Windows11/22H2/W11_22H2_Pro_20221220_22621.963/WEPExplorer/LsaSrv.xm at 7a806a148b3d9d381193d4a80356016e6e8b1ee8 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 15:42 https://github.com/nasbench/EVTX-ETW- Resources/blob/7a806a148b3d9d381193d4a80356016e6e8b1ee8/ETWProvidersManifests/Windows11/22H2/W11_22H2_Pr						

at 7a806a148b3 https://github.co	<b>WProvidersManife</b> 3d9d381193d4a8038 m/nasbench/EVTX-l	<b>56016e6e8b1ee8</b> · ETW-	nasbench/EVTX	-ETW-Resources	• <b>GitHub</b> - 31/10	)/2024 15:42
Resources/blob	)/7a806a148b3d9d38	31193d4a80356016e	e6e8b1ee8/ETWF	ProvidersManifests	/Windows11/22H	2/W11_22H2_Pr

EVTX-ETW- Resources/ETWProvidersManifests/Windows11/22H2/W11_22H2_Pro_20221220_22621.963/WEPExplorer/LsaSrv.xm at 7a806a148b3d9d381193d4a80356016e6e8b1ee8 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 15:42 nttps://github.com/nasbench/EVTX-ETW- Resources/blob/7a806a148b3d9d381193d4a80356016e6e8b1ee8/ETWProvidersManifests/Windows11/22H2/W11_22H2_Pr						

at 7a806a148b3d9d381193 https://github.com/nasbend	rsManifests/Windows11/22H2/W 3d4a80356016e6e8b1ee8 · nask sh/EVTX-ETW- 3b3d9d381193d4a80356016e6e8	pench/EVTX-ETW-Resource	ces · GitHub - 31/10/2024	15:42
Resources/blob/raoooa140	5D3U3U301133U426U330U10e0e0	preeo/ErwFrovidersivalille	Sts/VVIIIdOWST1/ZZFIZ/VVT1	_22N2_PI

EVTX-ETW-Resources/ETWProvidersManifests/Windows11/22H2/W11_22H2_Pro_20221220_22621.963/WEPExplorer/Lsa at 7a806a148b3d9d381193d4a80356016e6e8b1ee8 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 15 https://github.com/nasbench/EVTX-ETW-	5:42
Resources/blob/7a806a148b3d9d381193d4a80356016e6e8b1ee8/ETWProvidersManifests/Windows11/22H2/W11_2	2H2_Pr

Resources/ETWProvidersManifests/Windows11/22H2/W11\_22H2\_Pro\_20221220\_22621.963/WEPExplorer/LsaSrv.xml at 7a806a148b3d9d381193d4a80356016e6e8b1ee8 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 15:42 https://github.com/nasbench/EVTX-ETW-

Resources/blob/7a806a148b3d9d381193d4a80356016e6e8b1ee8/ETWProvidersManifests/Windows11/22H2/W11 22H2 ProvidersManifests/Windows11/22H2/W11 ProvidersManifests/W11 ProvidersManifests/Windows11/22H2/W11 ProvidersWandows11/22H2/W11 ProvidersWandows11/22H2/W11 ProvidersWandows11/22H2/W11 ProvidersWandows11/22H2/W11 ProvidersWandows11/22H2/W11 ProvidersWandows11/22H2/W11 ProvidersWandows11/22H2/W11 ProvidersWandows11/22H2/

```
972
                         <Level>Information</Level>
973
                         <Message><![CDATA[
974
        The Security System has received an authentication request directly for authentication protocol %1.
975
                         <Template><![CDATA[
        <template xmlns="http://schemas.microsoft.com/win/2004/08/events">
976
977
          <data name="Protocol" inType="win:UnicodeString" outType="xs:string"/>
978
        </template>
979
        ]]></Template>
980
                     </Event>
981
                     <Event>
982
                         <Id>40968</Id>
983
                         <Version>0</Version>
984
                         <Channel>System</Channel>
985
                         <Level>Warning</Level>
                         <Message><I[CDATA[</pre>
986
```

Resources/ETWProvidersManifests/Windows11/22H2/W11\_22H2\_Pro\_20221220\_22621.963/WEPExplorer/LsaSrv.xml at 7a806a148b3d9d381193d4a80356016e6e8b1ee8 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 15:42 https://github.com/nasbench/EVTX-ETW-

```
987
         The Security System has received an authentication request that could not be decoded. The request h
 988
                          <Template><![CDATA[
 989
         ]]></Template>
 990
                      </Event>
 991
                      <Event>
 992
                          <Id>40969</Id>
 993
                          <Version>0</Version>
                          <Channel>System</Channel>
 994
 995
                          <Level>Information</Level>
 996
                          <Message><![CDATA[
         The Security System has received an authentication attempt, and determined that the protocol %1 is
 997
                          <Template><![CDATA[
 998
         <template xmlns="http://schemas.microsoft.com/win/2004/08/events">
 999
           <data name="Protocol" inType="win:UnicodeString" outType="xs:string"/>
1000
1001
         </template>
1002
         ]]></Template>
1003
                      </Event>
1004
                      <Event>
1005
                          <Id>45056</Id>
                          <Version>0</Version>
1006
1007
                          <Channel>System</Channel>
1008
                          <Level>Warning</Level>
1009
                          <Message><![CDATA[
1010
         Logon cache was disabled. Intermittent authentication failures may result during periods of network
1011
                          <Template><![CDATA[
1012
         ]]></Template>
1013
                      </Event>
1014
                      <Event>
1015
                          <Id>45057</Id>
                          <Version>0</Version>
1016
1017
                          <Channel>System</Channel>
1018
                          <Level>Information</Level>
1019
                          <Message><![CDATA[
1020
         A failed logon attempt has caused a logon cache entry for user %1 to be deleted. The authentication
                          <Template><![CDATA[
1021
         <template xmlns="http://schemas.microsoft.com/win/2004/08/events">
1022
           <data name="Username" inType="win:UnicodeString" outType="xs:string"/>
1023
           <data name="Package" inType="win:UnicodeString" outType="xs:string"/>
1024
1025
           <data name="Error" inType="win:UnicodeString" outType="xs:string"/>
1026
         </template>
1027
         ]]></Template>
1028
                      </Event>
1029
                      <Event>
1030
                          <Id>45058</Id>
1031
                          <Version>0</Version>
```

Resources/ETWProvidersManifests/Windows11/22H2/W11\_22H2\_Pro\_20221220\_22621.963/WEPExplorer/LsaSrv.xml at 7a806a148b3d9d381193d4a80356016e6e8b1ee8 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 15:42 https://github.com/nasbench/EVTX-ETW-

Resources/blob/7a806a148b3d9d381193d4a80356016e6e8b1ee8/ETWProvidersManifests/Windows11/22H2/W11 22H2 ProvidersManifests/Windows11/22H2/W11 ProvidersManifests/W11 ProvidersManifests/Windows11/22H2/W11 ProvidersManifests/Windows11/22H2/W11 ProvidersManifests/W11 ProvidersManifests/Windows11/22H2/W11 ProvidersManifests/W11 ProvidersW11 ProvidersW

```
<cnannel>System</cnannel>
1033
                         <Level>Information</Level>
1034
                         <Message><![CDATA[
1035
         A logon cache entry for user %1 was the oldest entry and was removed. The timestamp of this entry w
1036
                         <Template><![CDATA[
1037
         <template xmlns="http://schemas.microsoft.com/win/2004/08/events">
           <data name="UserName" inType="win:UnicodeString" outType="xs:string"/>
1038
           <data name="TimeStamp" inType="win:SYSTEMTIME" outType="xs:dateTime"/>
1039
1040
         </template>
1041
         ]]></Template>
1042
                     </Event>
                 </EventMetadata>
1043
             </Provider>
1044
         </Providers>
1045
```