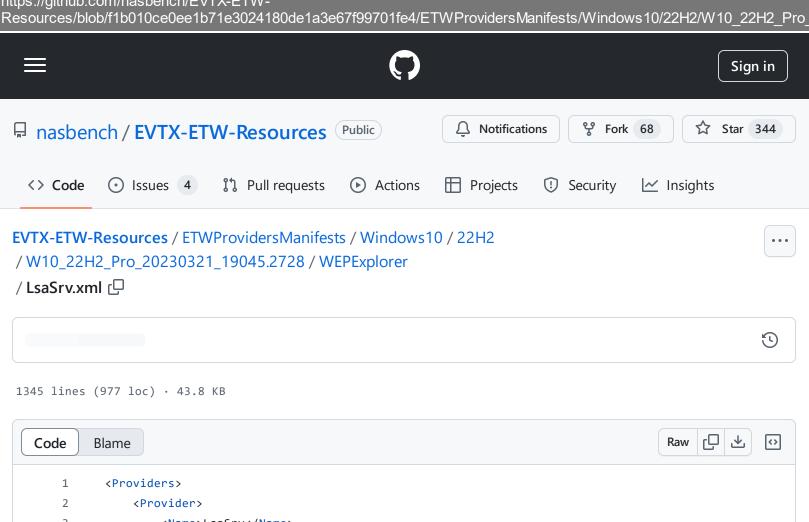
Resources/ETWProvidersManifests/Windows10/22H2/W10\_22H2\_Pro\_20230321\_19045.2728/WEPExplorer/LsaSrv.xn at f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 15:59 https://github.com/nasbench/EVTX-ETW-



```
3
               <Name>LsaSrv</Name>
 4
               <Metadata>
 5
                    <Guid>{199FE037-2B82-40A9-82AC-E1D46C792B99}</Guid>
 6
                    <ResourceFilePath>C:\Windows\System32\lsasrv.dll</ResourceFilePath>
                    <ParameterFilePath></ParameterFilePath>
 7
                    <MessageFilePath>C:\Windows\System32\lsasrv.dll</MessageFilePath>
 8
 9
                    <HelpLink>https://go.microsoft.com/fwlink/events.asp?CoName=Microsoft%20Corporation&amp
                    <PublisherMessage>Microsoft-Windows-LSA</PublisherMessage>
10
                    <Channels>
11
                        <Channel>
12
13
                            <Message>System</Message>
14
                            <Path>System</Path>
15
                            <Index>0</Index>
                            <Id>8</Id>
16
17
                            <Imported>true</Imported>
18
                        </Channel>
                        <Channel>
19
20
                            <Message></Message>
21
                            <Path>Microsoft-Windows-LSA/Performance</Path>
22
                            <Index>1</Index>
23
                            <Id>16</Id>
24
                            <Imported>false</Imported>
```

Resources/ETWProvidersManifests/Windows10/22H2/W10\_22H2\_Pro\_20230321\_19045.2728/WEPExplorer/LsaSrv.xn at f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 15:59 https://github.com/nasbench/EVTX-ETW-

Resources/blob/f1b010ce0ee1b71e3024180de1a3e67f99701fe4/ETWProvidersManifests/Windows10/22H2/W10 22H2 Pro

```
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/Windows10/22H2/W10\_22H2\_Pro\_20230321\_19045.2728/WEPExplorer/LsaSrv.xn at f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 15:59 https://github.com/nasbench/EVTX-ETW-

Resources/blob/f1b010ce0ee1b71e3024180de1a3e67f99701fe4/ETWProvidersManifests/Windows10/22H2/W10\_22H2\_Pro\_

```
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
                             <Task>0</Task>
105
106
                         </Opcode>
107
                         <Opcode>
108
                              <Message>Stop</Message>
                             <Name>win:Stop</Name>
109
                             <Value>2</Value>
110
111
                             <Task>0</Task>
                         </Opcode>
112
                     </Opcodes>
113
114
                     <Keywords>
115
                         <Keyword>
```

Ro at	t <b>f1b010ce0ee′</b> ttps://github.con	WProvidersManifests/Windows10/22H2/W10_22H2_Pro_20230321_19045.2728/WEPExplorer/LsaSrv.xr •1b71e3024180de1a3e67f99701fe4 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 15:59 m/nasbench/EVTX-ETW- /f1b010ce0ee1b71e3024180de1a3e67f99701fe4/ETWProvidersManifests/Windows10/22H2/W10_22H2_Pro_
	116	<message></message>
	116 117	<pre></pre> <pre>&lt;</pre>

R at	EVTX-ETW-Resources/ETWProvidersManifests/Windows10/22H2/W10_22H2_Pro_20230321_19045.2728/WEPExplorer/LsaSrv.xi at f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 15:59 https://github.com/nasbench/EVTX-ETW-					
R	Resources/blob/f1b010ce0ee1b71e3024180de1a3e67f99701fe4/ETWProvidersManifests/Windows10/22H2/W10_22H2_Pr	O_				

R a h	EVTX-ETW-Resources/ETWProvidersManifests/Windows10/22H2/W10_22H2_Pro_20230321_19045.2728/WEPExplorer/LsaSrv.: tf1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 15:59 ttps://github.com/nasbench/EVTX-ETW-	
k	Resources/blob/f1b010ce0ee1b71e3024180de1a3e67f99701fe4/ETWProvidersManifests/Windows10/22H2/W10_22H2_Pr	0_

at f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nathttps://github.com/nasbench/EVTX-ETW-	2/W10_22H2_Pro_20230321_19045.2728/WEPExplorer/LsaSrv.xasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 15:59	
Resources/blob/r1b010ce0ee1b71e30241o0de1a3e07198	970 TIE4/ET W FTOVICETSIVATIIIESTS/WITICOWS TO/ZZHZ/W TO_ZZHZ_FTC	

R a h	EVTX-ETW-Resources/ETWProvidersManifests/Windows10/22H2/W10_22H2_Pro_20230321_19045.2728/WEPExplorer/LsaSrv.: tf1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 15:59 ttps://github.com/nasbench/EVTX-ETW-	
k	Resources/blob/f1b010ce0ee1b71e3024180de1a3e67f99701fe4/ETWProvidersManifests/Windows10/22H2/W10_22H2_Pr	0_

R at ht	VTX-ETW- Resources/ETWProvidersManifests/Windows10/22H2/W10_22H2_Pro_20230321_19045.2728/WEPExplorer/LsaSrv tf1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 15:59 ttps://github.com/nasbench/EVTX-ETW-	
R	resources/blob/f1b010ce0ee1b71e3024180de1a3e67f99701fe4/ETWProvidersManifests/Windows10/22H2/W10_22H2_P	ro <sub>_</sub>

at f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nathttps://github.com/nasbench/EVTX-ETW-	2/W10_22H2_Pro_20230321_19045.2728/WEPExplorer/LsaSrv.xasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 15:59	
Resources/blob/r1b010ce0ee1b71e30241o0de1a3e07198	970 TIE4/ET W FTOVICETSIVATIIIESTS/WITICOWS TO/ZZHZ/W TO_ZZHZ_FTC	

EVTX-ETW-Resources/ETWProvidersManifests/Windows10/22H2/W10_22H2_Pro_2023 at f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nasbench/EVTX-ETW-Resources/blob/f1b010ce0ee1b71e3024180de1a3e67f99701fe4/ETWProviders/	esources · GitHub - 31/10/2024 15:59
Resources/blob/11b010cedee1b71e30241o0de1a3e071997011e4/E1WP10vide1s1	varillests/vviridows10/22H2/vv10_22H2_P10

EVTX-ETW- Resources/ETWProvidersManifests/Wind at f1b010ce0ee1b71e3024180de1a3e67f99 https://github.com/nasbench/EVTX-ETW-	9701fe4 · nasbench/EVTX-ETW-Resc	ources · GitHub - 31/10/2024 15:59
Resources/blob/f1b010ce0ee1b71e3024180	0de1a3e67f99701fe4/ETWProvidersMar	nifests/Windows10/22H2/W10_22H2_Pro

at f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nathttps://github.com/nasbench/EVTX-ETW-	2/W10_22H2_Pro_20230321_19045.2728/WEPExplorer/LsaSrv.xasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 15:59	
Resources/blob/r1b010ce0ee1b71e30241o0de1a3e07198	970 TIE4/ET W FTOVICETSIVATIIIESTS/WITICOWS TO/ZZHZ/W TO_ZZHZ_FTC	

EVTX-ETW-Resources/ETWProvidersManifests/Windows10/22H2/W10_22H2_Pro_20230321_19045.2728/WEPExplorer/LsaSrv.xi at f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 15:59 https://github.com/nasbench/EVTX-ETW-					
Resources/blob/f1b010ce0ee1b71e302	 24180de1a3e67f99701fe4	1/ETWProvidersManifests	/Windows10/22H2/W10	_22H2_Pro	

at f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nathttps://github.com/nasbench/EVTX-ETW-	2/W10_22H2_Pro_20230321_19045.2728/WEPExplorer/LsaSrv.xasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 15:59	
Resources/blob/r1b010ce0ee1b71e30241o0de1a3e07198	970 TIE4/ET W FTOVICETSIVATIIIESTS/WITICOWS TO/ZZHZ/W TO_ZZHZ_FTC	

at f1b010c	s/ETWProvidersNce0ee1b71e302418 ub.com/nasbench/E	8 <mark>0de1a3e67f99701</mark> EVTX-ETW-	fe4 · nasbench/E	EVTX-ETW-Resou	rces · GitHub - 31	PExplorer/LsaSrv.x 1/10/2024 15:59 2H2/W10_22H2_Pro
resources	5/BIOD/11801000000	157 10002+10000 18	3000/130/10 HC+//E	TWITTOWIGGISIWATIIN	313/WIIIdow3 10/2	2112100 10_22112_1 10

EVTX-ETW-Resources/ETWProvidersManifests/Windows10/22Fat f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nahttps://github.com/nasbench/EVTX-ETW-	asbench/EVTX-ETW-Resour	ces · GitHub - 31/10/2024 15:59
Resources/blob/f1b010ce0ee1b71e3024180de1a3e67f9	99701fe4/ETWProvidersManife	sts/Windows10/22H2/W10_22H2_Pro

EVTX-ETW-Resources/ETWProvidersManifests/Windows10/22Fat f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nahttps://github.com/nasbench/EVTX-ETW-	asbench/EVTX-ETW-Resour	ces · GitHub - 31/10/2024 15:59
Resources/blob/f1b010ce0ee1b71e3024180de1a3e67f9	99701fe4/ETWProvidersManife	sts/Windows10/22H2/W10_22H2_Pro

EVTX-ETW-Resources/ETWProvidersManifests/Windows10/22Fat f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nahttps://github.com/nasbench/EVTX-ETW-	asbench/EVTX-ETW-Resour	ces · GitHub - 31/10/2024 15:59
Resources/blob/f1b010ce0ee1b71e3024180de1a3e67f9	99701fe4/ETWProvidersManife	sts/Windows10/22H2/W10_22H2_Pro

EVTX-ETW- Resources/ETWProviders at f1b010ce0ee1b71e3024 https://github.com/nasbench Resources/blob/f1b010ce0e	<b>180de1a3e67f99701fe4</b> n/EVTX-ETW-	· nasbench/EVTX-ETW	/-Resources · GitHub	- 31/10/2024 15:59
1703001003/blob/1100100000	50 157 10002+10000 14000	7133701104/E17V110VIde	or striat life stay vv indows i	0/22112/110_22112_110

EVTX-ETW- Resources/ETWProvidersManifests/ at f1b010ce0ee1b71e3024180de1a3e https://github.com/nasbench/EVTX-ETV	67f99701fe4 · nasbenc	_22H2_Pro_20230321_1 h/EVTX-ETW-Resource	9045.2728/WEPExplo s · GitHub - 31/10/202	r <b>er/LsaSrv.x</b> 24 15:59
Resources/blob/f1b010ce0ee1b71e302	4180de1a3e67f99701fe4	l/ETWProvidersManifests	/Windows10/22H2/W	10_22H2_Pro

Resources/ETWProvidersManifests/Windows10/22H2/W10\_22H2\_Pro\_20230321\_19045.2728/WEPExplorer/LsaSrv.xn at f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 15:59 https://github.com/nasbench/EVTX-ETW-

Resources/blob/f1b010ce0ee1b71e3024180de1a3e67f99701fe4/ETWProvidersManifests/Windows10/22H2/W10 22H2 Pro

```
946
                     </Event>
947
                    <Event>
948
                         <Id>40969</Id>
949
                         <Version>0</Version>
950
                         <Channel>System</Channel>
951
                         <Level>Information</Level>
952
                         <Message><![CDATA[
        The Security System has received an authentication attempt, and determined that the protocol %1 is
953
954
                         <Template><![CDATA[
955
        <template xmlns="http://schemas.microsoft.com/win/2004/08/events">
          <data name="Protocol" inType="win:UnicodeString" outType="xs:string"/>
956
957
        </template>
958
        ]]></Template>
959
                     </Event>
                     <Fvent>
960
961
                         <Id>40970</Id>
962
                         <Version>0</Version>
                         <Channel>System</Channel>
963
964
                         <Level>Warning</Level>
965
                         <Message><![CDATA[
966
        The Security System has detected a downgrade attempt when contacting the 3-part SPN
967
968
         %1
969
970
         with error code %2. Authentication was denied.]]></Message>
971
                         <Template><![CDATA[
972
        <template xmlns="http://schemas.microsoft.com/win/2004/08/events">
973
          <data name="Target" inType="win:UnicodeString" outType="xs:string"/>
          <data name="Error" inType="win:UnicodeString" outType="xs:string"/>
974
975
        </template>
976
        ]]></Template>
977
                     </Event>
978
                    <Event>
979
                         <Id>45056</Id>
980
                         <Version>0</Version>
981
                         <Channel>System</Channel>
982
                         <Level>Warning</Level>
983
                         <Message><![CDATA[
984
        Logon cache was disabled. Intermittent authentication failures may result during periods of network
                         <Template><![CDATA[
985
986
        11sc/Temnlates
```

Resources/ETWProvidersManifests/Windows10/22H2/W10\_22H2\_Pro\_20230321\_19045.2728/WEPExplorer/LsaSrv.xn at f1b010ce0ee1b71e3024180de1a3e67f99701fe4 · nasbench/EVTX-ETW-Resources · GitHub - 31/10/2024 15:59 https://github.com/nasbench/EVTX-ETW-

```
987
                      </Event>
 988
                      <Event>
 989
                          <Id>45057</Id>
 990
                          <Version>0</Version>
 991
                          <Channel>System</Channel>
 992
                          <Level>Information</Level>
 993
                          <Message><![CDATA[
         A failed logon attempt has caused a logon cache entry for user %1 to be deleted. The authentication
 994
 995
                          <Template><![CDATA[
 996
         <template xmlns="http://schemas.microsoft.com/win/2004/08/events">
           <data name="Username" inType="win:UnicodeString" outType="xs:string"/>
 997
           <data name="Package" inType="win:UnicodeString" outType="xs:string"/>
 998
           <data name="Error" inType="win:UnicodeString" outType="xs:string"/>
 999
         </template>
1000
         ]]></Template>
1001
1002
                      </Event>
1003
                      <Event>
                          <Id>45058</Id>
1004
1005
                          <Version>0</Version>
                          <Channel>System</Channel>
1006
                          <Level>Information</Level>
1007
1008
                          <Message><![CDATA[
1009
         A logon cache entry for user %1 was the oldest entry and was removed. The timestamp of this entry w
1010
                          <Template><![CDATA[
         <template xmlns="http://schemas.microsoft.com/win/2004/08/events">
1011
           <data name="UserName" inType="win:UnicodeString" outType="xs:string"/>
1012
           <data name="TimeStamp" inType="win:SYSTEMTIME" outType="xs:dateTime"/>
1013
1014
         </template>
         ]]></Template>
1015
                      </Event>
1016
1017
                 </EventMetadata>
1018
             </Provider>
1019
         </Providers>
```