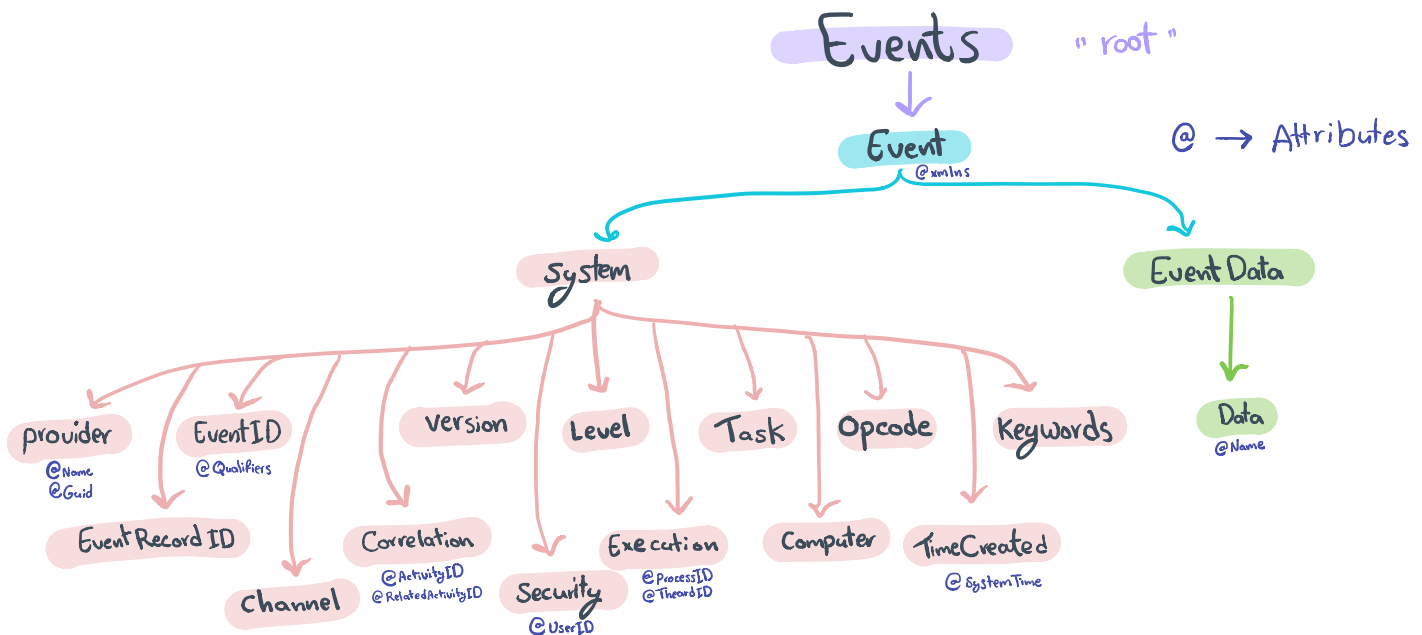


Lab 7

Name	Email
Norah Alsadhan	Norah-ALsadhan@hotmail.com



➤ RogueWinRM.evtx

Microsoft Windows Sysmon

We have 7 events in RogueWinRM.evtx, four of them to "Process creation" and their eventID is 1, two of them for "Network connection" and their eventID is 3, and the last one for "Process terminated" and its event ID is 5. (Windows Security log Encyclopedia, n.d.)

➤ I didn't find anything suspicious, so I think there is no security threat

>> privexchange - dirkjan.evtx

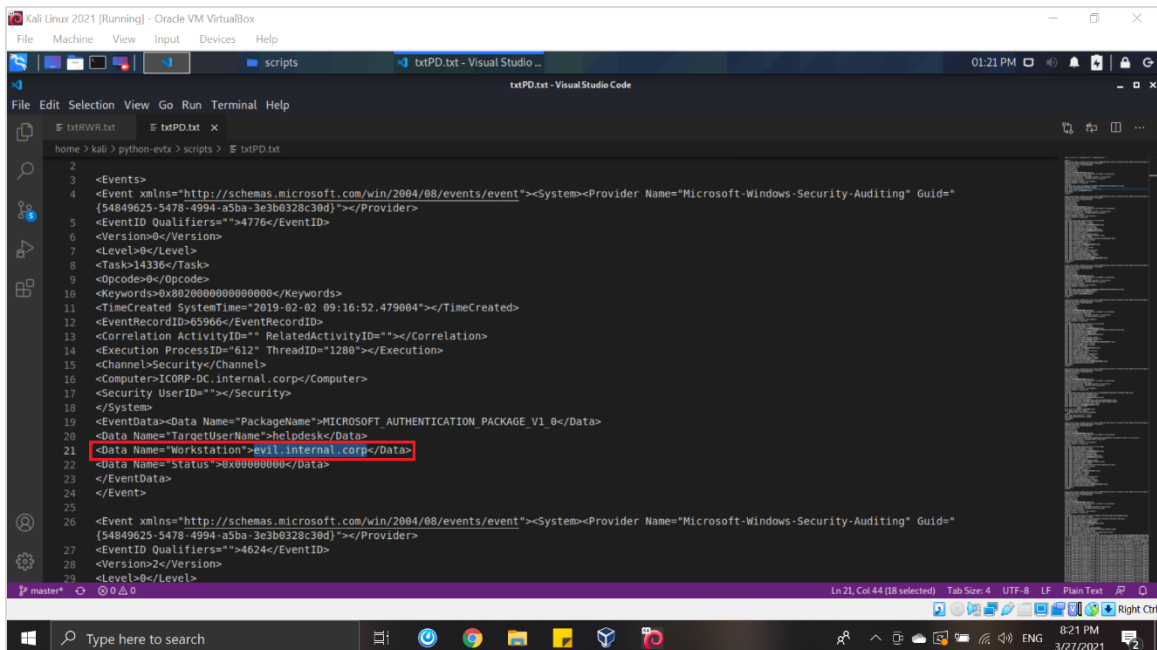
Microsoft Windows Security Auditing

We have 8 events: (Windows Security log Encyclopedia, n.d.)

- Three of them for event ID "4624" ⇒ "An account was successfully logged on".
- Two of them for event ID "4776" ⇒ "The domain controller attempted to validate the credentials for an account".
- Two of them for event ID "5136" ⇒ "A directory service object was modified".
- Last one for event ID "4662" ⇒ "An operation was performed on an object".

>> I think there is a security threat from following figures

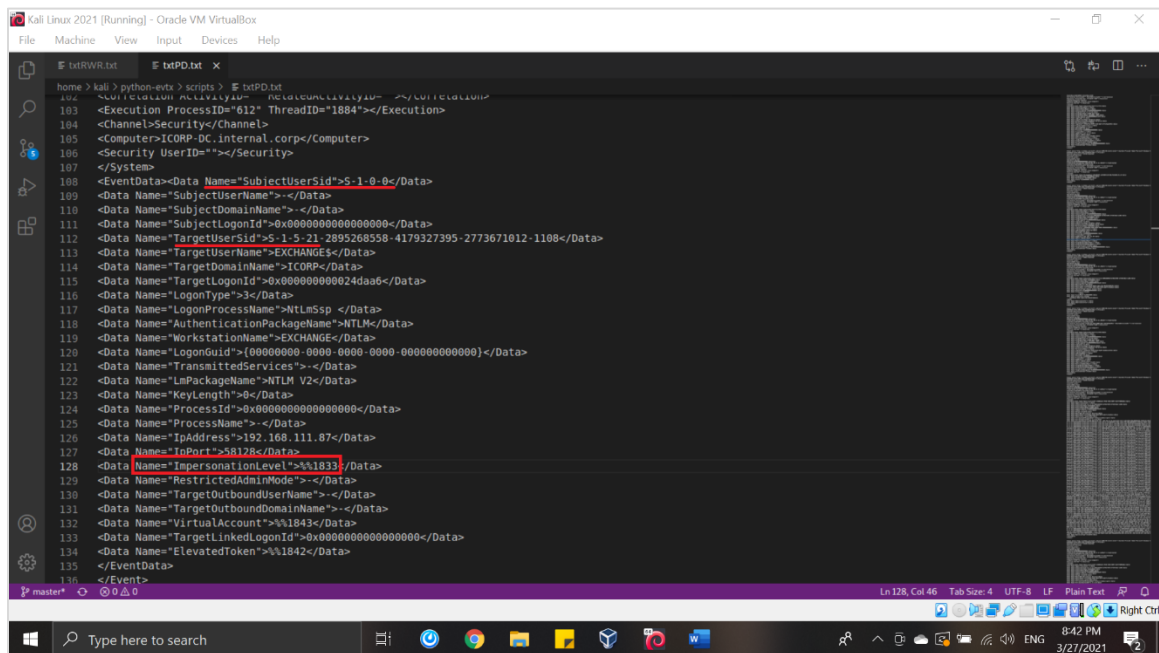
In Figure 1, I found a suspicious name.



```
<Events>
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><System><Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-a5ba-3e3b0328c30d}"></Provider>
<EventID Qualifiers="">4776</EventID>
<Version>0</Version>
<Level>0</Level>
<Task>14336</Task>
<Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords>
<TimeCreated SystemTime="2019-02-02 09:16:52.479004"></TimeCreated>
<EventRecordID>65966</EventRecordID>
<Correlation ActivityID="" RelatedActivityID=""></Correlation>
<Execution ProcessID="612" ThreadID="1280"></Execution>
<Channel>Security</Channel>
<Computer>ICORP-DC.internal.corp</Computer>
<Security UserID=""></Security>
</System>
<EventData><Data Name="PackageName">MICROSOFT_AUTHENTICATION_PACKAGE_V1_0</Data>
<Data Name="TargetUserName">helpdesk</Data>
<Data Name="Workstation">evil.internal.corp</Data>
<Data Name="Status">0x00000000</Data>
</EventData>
</Event>
</Events>
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><System><Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-a5ba-3e3b0328c30d}"></Provider>
<EventID Qualifiers="">4624</EventID>
<Version>2</Version>
<Level>0</Level>
```

Figure 1

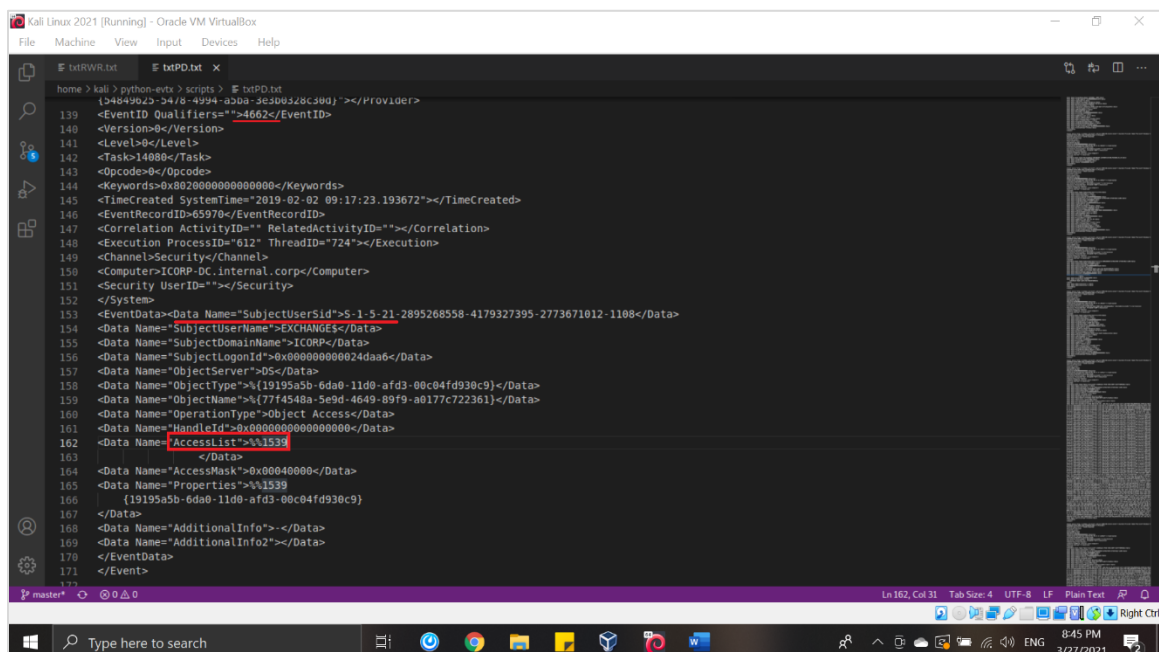
In Figure 2, the impersonation level was "%1833", which means Impersonation. (Impersonation Level, 2019).



```
home > kali > python-evtx > scripts > E txdp.txt
102 <Execution ProcessID="612" ThreadID="1884"></Execution>
103 <ChannelSecurity/Channel>
104 <Computer>ICORP-DC.internal.corp</Computer>
105 <Security UserID=""></Security>
106 </System>
107 <EventData><Data Name="SubjectUserSid">S-1-0-0</Data>
108 <Data Name="SubjectUserName"></Data>
109 <Data Name="SubjectDomainName"></Data>
110 <Data Name="SubjectLogonId">0x0000000000000000</Data>
111 <Data Name="TargetUserSid">S-1-5-21-2895268558-4179327395-2773671012-1108</Data>
112 <Data Name="TargetUserName">EXCHANGE</Data>
113 <Data Name="TargetDomainName">ICORP</Data>
114 <Data Name="TargetLogonId">0x0000000000000000</Data>
115 <Data Name="LogonType">3</Data>
116 <Data Name="LogonProcessName">NtLmSsp</Data>
117 <Data Name="AuthenticationPackageName">NTLM</Data>
118 <Data Name="WorkstationName">EXCHANGE</Data>
119 <Data Name="LogonGuid">{00000000-0000-0000-0000-000000000000}</Data>
120 <Data Name="TransmittedServices"></Data>
121 <Data Name="LmPackageName">NTLM V2</Data>
122 <Data Name="KeyLength">0</Data>
123 <Data Name="ProcessId">0x0000000000000000</Data>
124 <Data Name="ProcessName"></Data>
125 <Data Name="IpAddress">192.168.111.87</Data>
126 <Data Name="InPort">58128</Data>
127 <Data Name="ImpersonationLevel">%1833</Data>
128 <Data Name="RestrictedAdminMode"></Data>
129 <Data Name="TargetOutboundUserName"></Data>
130 <Data Name="TargetOutboundDomainName"></Data>
131 <Data Name="VirtualAccount">%1843</Data>
132 <Data Name="TargetLinkedLogonId">0x0000000000000000</Data>
133 <Data Name="ElevatedToken">%1842</Data>
134 </EventData>
135 </Event>
```

Figure 2

In Figure 3, in event ID "4662", the operation was performed and became the SubjectUserSid from "S-1-0-0" to "S-1-5-21" and with AccessList "%1539" the permission to modify the discretionary access control list (DACL). (An attempt was made to access an object,2017)



```
home > kali > python-evtx > scripts > E txdp.txt
139 {24849023-3478-4994-a30a-3e300320c30d}></Provider>
140 <EventID Qualifiers="4662"></EventID>
141 <Version>0</Version>
142 <Level>0</Level>
143 <Task>14000</Task>
144 <Opcode>0</Opcode>
145 <Keywords>0x8020000000000000</Keywords>
146 <TimeCreated SystemTime="2019-02-02 09:17:23.193672"></TimeCreated>
147 <EventRecordID>65970</EventRecordID>
148 <Correlation ActivityID="" RelatedActivityID=""></Correlation>
149 <Execution ProcessID="612" ThreadID="724"></Execution>
150 <ChannelSecurity/Channel>
151 <Computer>ICORP-DC.internal.corp</Computer>
152 <Security UserID=""></Security>
153 </System>
154 <EventData><Data Name="SubjectUserSid">S-1-5-21-2895268558-4179327395-2773671012-1108</Data>
155 <Data Name="SubjectUserName">EXCHANGE</Data>
156 <Data Name="SubjectDomainName">ICORP</Data>
157 <Data Name="SubjectLogonId">0x0000000000000000</Data>
158 <Data Name="ObjectServer">05</Data>
159 <Data Name="ObjectType">%{19195a5b-6da0-11d0-afd3-00c04fd93bc9}</Data>
160 <Data Name="ObjectName">%{7f1454ba-5e9d-4649-89f9-a0177c722361}</Data>
161 <Data Name="OperationType">Object Access</Data>
162 <Data Name="HandleId">0x0000000000000000</Data>
163 <Data Name="AccessList">%1539</Data>
164 <Data Name="AccessMask">0x00040000</Data>
165 <Data Name="Properties">%1539
166 {19195a5b-6da0-11d0-afd3-00c04fd93bc9}
167 </Data>
168 <Data Name="AdditionalInfo"></Data>
169 <Data Name="AdditionalInfo2"></Data>
170 </EventData>
171 </Event>
```

Figure 3

References:

- 1- Randy's Windows Security Log Encyclopedia. (n.d.). Randy Franklin Smith's Ultimate Windows Security. Retrieved March 27, 2021, from <https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/default.aspx>
- 2- Windows Account Logon Impersonation Level. (2019, December 27). MyClassNotes. <https://thisismyclassnotes.blogspot.com/2019/12/windows-account-logon-impersonation.html>
- 3- D. (2017, April 19). 4663(S) An attempt was made to access an object. (Windows 10) - Windows security. Microsoft Docs. <https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4663>