

2.1.1

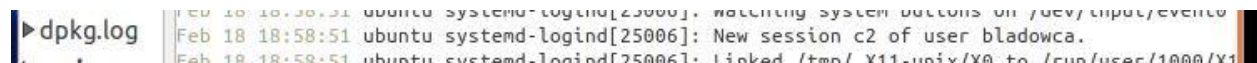
```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>
  <Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-A5BA-3E3B0328C30D}" />
  <EventID>4624</EventID>
  <Version>0</Version>
  <Level>0</Level>
  <Task>12544</Task>
  <Opcode>0</Opcode>
  <Keywords>0x8020000000000000</Keywords>
  <TimeCreated SystemTime="2015-02-19T15:07:13.224479400Z" />
  <EventRecordID>33508</EventRecordID>
  <Correlation />
  <Execution ProcessID="620" ThreadID="1784" />
  <Channel>Security</Channel>
  <Computer>ASUS_U52F</Computer>
  <Security />
</System>
- <EventData>
  <Data Name="SubjectUserSid">S-1-5-18</Data>
  <Data Name="SubjectUserName">ASUS_U52F$</Data>
  <Data Name="SubjectDomainName">WORKGROUP</Data>
  <Data Name="SubjectLogonId">0x3e7</Data>
  <Data Name="TargetUserSid">S-1-5-18</Data>
  <Data Name="TargetUserName">SYSTEM</Data>
  <Data Name="TargetDomainName">NT AUTHORITY</Data>
  <Data Name="TargetLogonId">0x3e7</Data>
  <Data Name="LogonType">5</Data>
```

```

<Data Name="LogonProcessName">Advapi</Data>
<Data Name="AuthenticationPackageName">Negotiate</Data>
<Data Name="WorkstationName" />
<Data Name="LogonGuid">{00000000-0000-0000-0000-000000000000}</Data>
<Data Name="TransmittedServices">-</Data>
<Data Name="LmPackageName">-</Data>
<Data Name="KeyLength">0</Data>
<Data Name="ProcessId">0x23c</Data>
<Data Name="ProcessName">C:\Windows\System32\services.exe</Data>
<Data Name="IpAddress">-</Data>
<Data Name="IpPort">-</Data>
</EventData>
</Event>

```

2.1.2



2.1.3

```

- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>
  <Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-A5BA-3E3B0328C30D}" />
  <EventID>4732</EventID>
  <Version>0</Version>
  <Level>0</Level>
  <Task>13826</Task>
  <Opcode>0</Opcode>
  <Keywords>0x8020000000000000</Keywords>
  <TimeCreated SystemTime="2015-02-15T22:55:56.547402800Z" />
  <EventRecordID>30793</EventRecordID>
  <Correlation />

```

```
<Execution ProcessID="628" ThreadID="5444" />
<Channel>Security</Channel>
<Computer>ASUS_U52F</Computer>
<Security />
</System>
- <EventData>
  <Data Name="MemberName">-</Data>
  <Data Name="MemberSid">S-1-5-21-2646407836-544368989-4209113281-1013</Data>
  <Data Name="TargetUserName">Users</Data>
  <Data Name="TargetDomainName">Builtin</Data>
  <Data Name="TargetSid">S-1-5-32-545</Data>
  <Data Name="SubjectUserSid">S-1-5-21-2646407836-544368989-4209113281-1000</Data>
  <Data Name="SubjectUserName">Casey</Data>
  <Data Name="SubjectDomainName">ASUS_U52F</Data>
  <Data Name="SubjectLogonId">0x3684d</Data>
  <Data Name="PrivilegeList">-</Data>
</EventData>
</Event>
```

2.1.4

```
Feb 19 09:24:54 ubuntu lightdm: pam_kwallet(lightdm-greeter:session): pam_kwallet: open_session called without kwallet_key
Feb 19 09:25:01 ubuntu lightdm: pam_succeed_if(lightdm:auth): requirement "user ingroup nopasswdlogin" not met by user "bladowca"
Feb 19 09:27:48 ubuntu lightdm: pam_kwallet(lightdm:auth): pam_sm_authenticate
```