```
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 17:22:24.761162
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 17:22:24.851292
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 17:22:24.901363
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 17:22:40.373611
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 17:26:03.585817
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 17:26:05.628754
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 17:31:03.687342
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 17:36:03.788866
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 17:41:03.890392
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 17:41:08.777418
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
```

```
This event was created on:  2019-03-19 17:41:08.967691
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 17:41:08.977707
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 17:41:09.828930
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 17:42:05.859499
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:41:11.238661
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:41:11.458977
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:41:11.699322
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:41:11.719351
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:41:11.759409
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:41:11.909624
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:41:11.909624
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
```

```
No Match in Event ID List
This event was created on:  2019-03-19 20:41:11.919640
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:41:11.929653
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:41:11.979725
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:41:12.931093
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:41:13.151411
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:41:13.181454
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:41:13.221512
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:41:14.232965
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:41:14.563440
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:41:14.603498
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:41:14.933973
```

```
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:41:15.094204
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:41:15.144276
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:41:15.144276
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:41:15.154291
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:41:15.424679
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:41:15.424679
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:41:15.454723
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:41:15.514809
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:41:15.795212
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:41:15.835270
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
```

```
This event was created on:  2019-03-19 20:41:15.865313
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:41:15.885342
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:41:15.915384
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:41:15.995501
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:41:16.065601
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:41:16.135702
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:41:16.406090
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:41:16.436134
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:41:16.626408
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:41:17.026983
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:41:22.404716
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
```

```
No Match in Event ID List
This event was created on:  2019-03-19 20:42:00.148991
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:42:00.329248
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:42:00.419378
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:42:00.489479
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:42:37.392544
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:42:37.432602
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:42:37.602846
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:42:38.654358
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:42:38.704430
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:42:38.774530
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:43:24.560368
```

```
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:46:04.916016
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:46:20.518450
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:46:25.856125
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:47:56.436375
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:48:33.439581
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:48:33.459610
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:48:33.459610
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:48:33.499668
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:48:33.499668
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:48:33.499668
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
```

```
This event was created on:  2019-03-19 20:48:33.509682
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:48:33.559755
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:48:33.559755
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:48:33.860188
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:48:33.870201
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:48:33.920273
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:48:33.930288
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:48:36.644190
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:49:27.787731
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:49:27.807760
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:49:27.807760
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
```

```
No Match in Event ID List
This event was created on:  2019-03-19 20:49:27.857832
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:49:27.857832
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:49:27.857832
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:49:27.867846
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:49:27.967989
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:49:27.978004
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:49:27.988018
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:49:28.158264
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:49:28.158264
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:49:28.168278
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:49:31.212656
```

```
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:49:44.792181
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:49:44.802197
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:49:44.802197
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:49:44.822226
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:49:44.822226
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:49:44.822226
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:49:44.832239
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:49:44.972441
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:49:44.972441
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:49:44.982456
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
```

```
This event was created on:  2019-03-19 20:49:45.152700
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:49:45.162714
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:49:45.172729
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:49:47.245710
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:51:05.017540
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:52:25.933891
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:52:25.953920
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:52:25.953920
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:52:25.973949
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:52:25.973949
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:52:25.973949
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
```

```
No Match in Event ID List
This event was created on:  2019-03-19 20:52:25.983965
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:52:26.104137
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:52:26.104137
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:52:26.114151
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:52:26.274382
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:52:26.364511
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:52:26.364511
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:52:29.138500
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:52:47.124363
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:52:47.144392
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:52:47.144392
```

```
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:52:47.154406
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:52:47.164421
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:52:47.164421
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:52:47.164421
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:52:47.294607
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:52:47.294607
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:52:47.334665
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:52:47.474867
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:52:47.474867
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:52:47.484880
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
```

```
This event was created on:  2019-03-19 20:52:50.268885
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:56:05.149109
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:58:20.994444
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:58:21.014473
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:58:21.014473
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:58:21.044516
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:58:21.044516
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:58:21.054531
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:58:21.054531
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:58:28.214827
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:58:28.294941
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
```

```
No Match in Event ID List
This event was created on:  2019-03-19 20:58:28.304956
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:58:28.815691
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:58:31.860067
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:58:31.860067
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:58:35.745655
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:58:44.237867
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 21:00:01.518991
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 21:00:01.539021
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 21:10:34.489159
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 21:18:54.257790
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 21:18:57.202023
```

```
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 21:20:32.298765
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 21:20:32.298765
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 21:20:35.603518
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 21:21:05.306229
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 21:22:28.886410
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 21:22:33.202618
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 21:22:33.202618
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 21:22:33.593178
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 21:26:05.397739
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 21:26:08.852707
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
```

```
This event was created on:  2019-03-19 21:31:05.509277
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 21:36:05.610802
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 21:41:05.702312
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 21:41:11.440565
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 21:41:17.339046
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 21:41:17.339046
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 21:41:18.290413
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 21:41:18.410587
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:18:49.576239
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:18:49.856642
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:18:50.157072
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
```

```
No Match in Event ID List
This event was created on:  2019-03-19 23:18:50.217159
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:18:50.217159
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:18:50.387403
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:18:50.427462
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:18:50.467520
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:18:50.497562
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:18:50.627750
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:18:51.308729
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:18:51.599146
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:18:51.679262
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:18:51.789421
```

```
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:18:53.111320
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:18:53.501883
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:18:53.571983
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:18:53.922487
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:18:54.102747
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:18:54.172848
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:18:54.172848
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:18:54.182861
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:18:54.593452
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:18:54.603466
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
```

```
This event was created on:  2019-03-19 23:18:54.623495
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:18:54.783726
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:18:54.793739
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:18:54.813768
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:18:55.224360
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:18:55.404619
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:18:55.514776
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:18:55.544821
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:18:55.594893
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:18:55.654978
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:18:55.654978
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
```

```
No Match in Event ID List
This event was created on:  2019-03-19 23:18:55.725079
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:18:55.805195
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:18:55.835238
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:18:55.965425
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:18:56.055555
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:18:56.376015
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:18:56.406059
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:18:56.626375
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:18:57.237253
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:18:57.627815
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:18:58.278751
```

```
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:18:58.288765
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:18:58.489054
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:18:58.989775
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:19:04.187248
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:19:10.796751
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:20:19.155046
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:20:19.205118
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:20:19.205118
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:20:19.295248
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:21:01.325684
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
```

```
This event was created on:  2019-03-19 23:21:48.323263
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:23:41.105436
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_sysmon_11_
13_1_shime_appfix.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:24:08.294533
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_startup_Us
erShellStartup_Folder_Changed_sysmon_13.xml
No Match in Event ID List
This event was created on:  2019-05-28 23:09:38.589832
An Event ID: 1102, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_security_d
cshadow_4742.xml
Matched in Event ID List
This event was created on:  2019-05-08 03:00:11.778189
An Event ID: 4662, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_security_d
cshadow_4742.xml
Matched in Event ID List
This event was created on:  2019-05-08 03:00:37.541178
An Event ID: 4742, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_security_d
cshadow_4742.xml
Matched in Event ID List
This event was created on:  2019-05-08 03:00:37.572176
An Event ID: 4662, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_security_d
cshadow_4742.xml
Matched in Event ID List
This event was created on:  2019-05-08 03:00:37.583260
An Event ID: 4742, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_security_d
cshadow_4742.xml
Matched in Event ID List
This event was created on:  2019-05-08 03:00:37.586172
An Event ID: 4662, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_security_d
cshadow_4742.xml
Matched in Event ID List
This event was created on:  2019-05-08 03:00:37.591202
An Event ID: 4662, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_security_d
cshadow_4742.xml
Matched in Event ID List
This event was created on:  2019-05-08 03:00:37.615168
An Event ID: 4662, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_security_d
cshadow_4742.xml
```

```
Matched in Event ID List
This event was created on:  2019-05-08 03:00:37.621187
An Event ID: 4662, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_security_d
cshadow_4742.xml
Matched in Event ID List
This event was created on:  2019-05-08 03:00:37.623163
An Event ID: 4742, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_security_d
cshadow_4742.xml
Matched in Event ID List
This event was created on:  2019-05-08 03:00:37.624197
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_13_1_persistenc
e_via_winlogon_shell.xml
No Match in Event ID List
This event was created on:  2019-06-14 22:22:17.988371
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_13_1_persistenc
e_via_winlogon_shell.xml
No Match in Event ID List
This event was created on:  2019-06-14 22:22:21.503994
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_13_1_persistenc
e_via_winlogon_shell.xml
No Match in Event ID List
This event was created on:  2019-06-14 22:22:21.535246
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_13_1_persistenc
e_via_winlogon_shell.xml
No Match in Event ID List
This event was created on:  2019-06-14 22:22:21.535246
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_13_1_persistenc
e_via_winlogon_shell.xml
No Match in Event ID List
This event was created on:  2019-06-14 22:22:31.957119
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_13_1_persistenc
e_via_winlogon_shell.xml
No Match in Event ID List
This event was created on:  2019-06-14 22:22:32.222746
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_13_1_persistenc
e_via_winlogon_shell.xml
No Match in Event ID List
This event was created on:  2019-06-14 22:22:47.253994
An Event ID: 5, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_13_1_persistenc
e_via_winlogon_shell.xml
No Match in Event ID List
This event was created on:  2019-06-14 22:22:52.457119
```

```
An Event ID: 5, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_13_1_persistenc
e_via_winlogon_shell.xml
No Match in Event ID List
This event was created on:  2019-06-14 22:22:52.503994
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_13_1_persistenc
e_via_winlogon_shell.xml
No Match in Event ID List
This event was created on:  2019-06-14 22:22:55.441496
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_13_1_persistenc
e_via_winlogon_shell.xml
No Match in Event ID List
This event was created on:  2019-06-14 22:22:55.503994
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_13_1_persistenc
e_via_winlogon_shell.xml
No Match in Event ID List
This event was created on:  2019-06-14 22:22:55.566496
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_13_1_persistenc
e_via_winlogon_shell.xml
No Match in Event ID List
This event was created on:  2019-06-14 22:22:55.707119
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_13_1_persistenc
e_via_winlogon_shell.xml
No Match in Event ID List
This event was created on:  2019-06-14 22:23:06.691496
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_13_1_persistenc
e_via_winlogon_shell.xml
No Match in Event ID List
This event was created on:  2019-06-14 22:23:07.019621
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_13_1_persistenc
e_via_winlogon_shell.xml
No Match in Event ID List
This event was created on:  2019-06-14 22:23:07.082119
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_13_1_persistenc
e_via_winlogon_shell.xml
No Match in Event ID List
This event was created on:  2019-06-14 22:23:13.894621
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_13_1_persistenc
e_via_winlogon_shell.xml
No Match in Event ID List
This event was created on:  2019-06-14 22:23:13.957119
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_13_1_persistenc
e_via_winlogon_shell.xml
No Match in Event ID List
```

```
This event was created on:  2019-06-14 22:23:13.972746
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_13_1_persistenc
e_via_winlogon_shell.xml
No Match in Event ID List
This event was created on:  2019-06-14 22:23:15.054777
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_13_1_persistenc
e_via_winlogon_shell.xml
No Match in Event ID List
This event was created on:  2019-06-14 22:23:16.592861
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_13_1_persistenc
e_via_winlogon_shell.xml
No Match in Event ID List
This event was created on:  2019-06-14 22:23:23.405363
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_13_1_persistenc
e_via_winlogon_shell.xml
No Match in Event ID List
This event was created on:  2019-06-14 22:23:26.811613
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_13_1_persistenc
e_via_winlogon_shell.xml
No Match in Event ID List
This event was created on:  2019-06-14 22:23:26.999113
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_13_1_persistenc
e_via_winlogon_shell.xml
No Match in Event ID List
This event was created on:  2019-06-14 22:23:53.358488
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_1_persist_bitsj
ob_SetNotifyCmdLine.xml
No Match in Event ID List
This event was created on:  2019-05-13 18:02:49.160589
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_1_persist_bitsj
ob_SetNotifyCmdLine.xml
No Match in Event ID List
This event was created on:  2019-05-13 18:03:19.681479
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_1_persist_bitsj
ob_SetNotifyCmdLine.xml
No Match in Event ID List
This event was created on:  2019-05-13 18:03:19.681479
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_1_persist_bitsj
ob_SetNotifyCmdLine.xml
No Match in Event ID List
This event was created on:  2019-05-13 18:03:19.895876
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_1_persist_bitsj
ob_SetNotifyCmdLine.xml
```

```
No Match in Event ID List
This event was created on:  2019-05-13 18:03:21.212896
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_1_persist_bitsj
ob_SetNotifyCmdLine.xml
No Match in Event ID List
This event was created on:  2019-05-13 18:05:18.692038
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_20_21_1_Command
LineEventConsumer.xml
No Match in Event ID List
This event was created on:  2019-05-11 17:57:49.903160
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_20_21_1_Command
LineEventConsumer.xml
No Match in Event ID List
This event was created on:  2019-05-11 17:58:22.809408
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_20_21_1_Command
LineEventConsumer.xml
No Match in Event ID List
This event was created on:  2019-05-11 17:58:23.215658
An Event ID: 20, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_20_21_1_Command
LineEventConsumer.xml
No Match in Event ID List
This event was created on:  2019-05-11 17:58:23.340658
An Event ID: 21, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_20_21_1_Command
LineEventConsumer.xml
No Match in Event ID List
This event was created on:  2019-05-11 17:58:23.418783
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_20_21_1_Command
LineEventConsumer.xml
No Match in Event ID List
This event was created on:  2019-05-11 17:58:23.450035
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_20_21_1_Command
LineEventConsumer.xml
No Match in Event ID List
This event was created on:  2019-05-11 17:58:23.590658
An Event ID: 19, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_20_21_1_Command
LineEventConsumer.xml
No Match in Event ID List
This event was created on:  2019-05-11 17:58:39.746908
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_20_21_1_Command
LineEventConsumer.xml
No Match in Event ID List
This event was created on:  2019-05-11 17:58:50.090658
```

```
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_20_21_1_Command
LineEventConsumer.xml
No Match in Event ID List
This event was created on:  2019-05-11 17:58:54.762533
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_20_21_1_Command
LineEventConsumer.xml
No Match in Event ID List
This event was created on:  2019-05-11 17:58:54.762533
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_20_21_1_Command
LineEventConsumer.xml
No Match in Event ID List
This event was created on:  2019-05-11 17:58:54.887533
An Event ID: 20, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_20_21_1_Command
LineEventConsumer.xml
No Match in Event ID List
This event was created on:  2019-05-11 17:58:54.903160
An Event ID: 19, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_20_21_1_Command
LineEventConsumer.xml
No Match in Event ID List
This event was created on:  2019-05-11 17:58:54.981285
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_20_21_1_Command
LineEventConsumer.xml
No Match in Event ID List
This event was created on:  2019-05-11 17:58:55.028160
An Event ID: 21, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_20_21_1_Command
LineEventConsumer.xml
No Match in Event ID List
This event was created on:  2019-05-11 17:58:55.090658
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/sysmon_20_21_1_Command
LineEventConsumer.xml
No Match in Event ID List
This event was created on:  2019-05-11 17:58:55.153160
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/wmighost_sysmon_20_21_
1.xml
No Match in Event ID List
This event was created on:  2019-04-03 18:11:54.098351
An Event ID: 20, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/wmighost_sysmon_20_21_
1.xml
No Match in Event ID List
This event was created on:  2019-04-03 18:11:54.178467
An Event ID: 21, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/wmighost_sysmon_20_21_
1.xml
No Match in Event ID List
```

```
This event was created on:  2019-04-03 18:11:54.198496
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/wmighost_sysmon_20_21_
1.xml
No Match in Event ID List
This event was created on:  2019-04-03 18:12:00.016861
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persist_bitsadmin_Micr
osoft-Windows-Bits-Client-Operational.xml
No Match in Event ID List
This event was created on:  2019-05-12 18:02:05.215199
An Event ID: 59, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persist_bitsadmin_Micr
osoft-Windows-Bits-Client-Operational.xml
No Match in Event ID List
This event was created on:  2019-05-12 18:04:50.121447
An Event ID: 60, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persist_bitsadmin_Micr
osoft-Windows-Bits-Client-Operational.xml
No Match in Event ID List
This event was created on:  2019-05-12 18:04:50.137072
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persist_bitsadmin_Micr
osoft-Windows-Bits-Client-Operational.xml
No Match in Event ID List
This event was created on:  2019-05-13 14:50:01.999050
An Event ID: 59, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persist_bitsadmin_Micr
osoft-Windows-Bits-Client-Operational.xml
No Match in Event ID List
This event was created on:  2019-05-13 14:50:59.389677
An Event ID: 60, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persist_bitsadmin_Micr
osoft-Windows-Bits-Client-Operational.xml
No Match in Event ID List
This event was created on:  2019-05-13 14:50:59.405300
An Event ID: 12, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_accessibil
ity_features_osk_sysmon1.xml
No Match in Event ID List
This event was created on:  2019-05-16 16:08:30.516571
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_accessibil
ity_features_osk_sysmon1.xml
No Match in Event ID List
This event was created on:  2019-05-16 16:08:34.867569
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_accessibil
ity_features_osk_sysmon1.xml
No Match in Event ID List
This event was created on:  2019-05-16 16:08:40.360594
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_SilentProc
essExit_ImageHijack_sysmon_13_1.xml
```

```
No Match in Event ID List
This event was created on:  2019-06-19 17:22:37.897139
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_SilentProc
essExit_ImageHijack_sysmon_13_1.xml
No Match in Event ID List
This event was created on:  2019-06-19 17:22:41.709639
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_SilentProc
essExit_ImageHijack_sysmon_13_1.xml
No Match in Event ID List
This event was created on:  2019-06-19 17:22:41.709639
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_SilentProc
essExit_ImageHijack_sysmon_13_1.xml
No Match in Event ID List
This event was created on:  2019-06-19 17:22:43.944012
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_SilentProc
essExit_ImageHijack_sysmon_13_1.xml
No Match in Event ID List
This event was created on:  2019-06-19 17:22:43.944012
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_SilentProc
essExit_ImageHijack_sysmon_13_1.xml
No Match in Event ID List
This event was created on:  2019-06-19 17:22:45.694012
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_SilentProc
essExit_ImageHijack_sysmon_13_1.xml
No Match in Event ID List
This event was created on:  2019-06-19 17:22:55.397139
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_SilentProc
essExit_ImageHijack_sysmon_13_1.xml
No Match in Event ID List
This event was created on:  2019-06-19 17:22:58.944012
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_SilentProc
essExit_ImageHijack_sysmon_13_1.xml
No Match in Event ID List
This event was created on:  2019-06-19 17:23:01.928389
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_SilentProc
essExit_ImageHijack_sysmon_13_1.xml
No Match in Event ID List
This event was created on:  2019-06-19 17:23:01.990887
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_SilentProc
essExit_ImageHijack_sysmon_13_1.xml
No Match in Event ID List
This event was created on:  2019-06-19 17:23:02.350264
```

```
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_SilentProc
essExit_ImageHijack_sysmon_13_1.xml
No Match in Event ID List
This event was created on:  2019-06-19 17:23:10.334639
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persistence_SilentProc
essExit_ImageHijack_sysmon_13_1.xml
No Match in Event ID List
This event was created on:  2019-06-19 17:23:11.694012
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persist_turla_outlook_
backdoor_comhijack.xml
No Match in Event ID List
This event was created on:  2019-05-21 01:10:05.290459
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persist_turla_outlook_
backdoor_comhijack.xml
No Match in Event ID List
This event was created on:  2019-05-21 01:10:44.807281
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persist_turla_outlook_
backdoor_comhijack.xml
No Match in Event ID List
This event was created on:  2019-05-21 01:10:52.468296
An Event ID: 500, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/Persistence_Shime_Micr
osoft-Windows-Application-Experience_Program-Telemetry_500.xml
No Match in Event ID List
This event was created on:  2019-03-19 17:06:22.938129
An Event ID: 500, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/Persistence_Shime_Micr
osoft-Windows-Application-Experience_Program-Telemetry_500.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:48:33.469625
An Event ID: 500, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/Persistence_Shime_Micr
osoft-Windows-Application-Experience_Program-Telemetry_500.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:49:27.877861
An Event ID: 500, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/Persistence_Shime_Micr
osoft-Windows-Application-Experience_Program-Telemetry_500.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:49:44.882311
An Event ID: 500, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/Persistence_Shime_Micr
osoft-Windows-Application-Experience_Program-Telemetry_500.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:52:26.034037
An Event ID: 500, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/Persistence_Shime_Micr
osoft-Windows-Application-Experience_Program-Telemetry_500.xml
No Match in Event ID List
```

```
This event was created on:  2019-03-19 20:52:47.214493
An Event ID: 500, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/Persistence_Shime_Micr
osoft-Windows-Application-Experience_Program-Telemetry_500.xml
No Match in Event ID List
This event was created on:  2019-03-19 20:58:31.749910
An Event ID: 4732, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/Network_Service_Guest_
added_to_admins_4732.xml
Matched in Event ID List
This event was created on:  2019-09-22 11:22:05.201725
An Event ID: 4732, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/Network_Service_Guest_
added_to_admins_4732.xml
Matched in Event ID List
This event was created on:  2019-09-22 11:23:19.251926
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/Persistence_Winsock_Ca
talog Change EventId_1.xml
No Match in Event ID List
This event was created on:  2019-08-23 12:37:37.100801
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/Persistence_Winsock_Ca
talog Change EventId_1.xml
No Match in Event ID List
This event was created on:  2019-08-23 12:37:38.521158
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persist_valid_account_
guest_rid_hijack.xml
No Match in Event ID List
This event was created on:  2019-09-08 19:14:54.471523
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persist_valid_account_
guest_rid_hijack.xml
No Match in Event ID List
This event was created on:  2019-09-08 19:17:44.249168
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persist_valid_account_
guest_rid_hijack.xml
No Match in Event ID List
This event was created on:  2019-09-08 19:17:44.350763
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persist_valid_account_
guest_rid_hijack.xml
No Match in Event ID List
This event was created on:  2019-09-08 19:17:44.391388
An Event ID: 1102, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/DACL_DCSync_Right_Powe
rview_ Add-DomainObjectAcl.xml
Matched in Event ID List
This event was created on:  2019-03-25 21:28:11.073627
An Event ID: 4662, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/DACL_DCSync_Right_Powe
rview_ Add-DomainObjectAcl.xml
```

```
Matched in Event ID List
This event was created on:  2019-03-25 21:28:35.436632
An Event ID: 4662, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/DACL_DCSync_Right_Powe
rview_ Add-DomainObjectAcl.xml
Matched in Event ID List
This event was created on:  2019-03-25 21:28:35.440615
An Event ID: 4662, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/DACL_DCSync_Right_Powe
rview_ Add-DomainObjectAcl.xml
Matched in Event ID List
This event was created on:  2019-03-25 21:28:35.458618
An Event ID: 4662, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/DACL_DCSync_Right_Powe
rview_ Add-DomainObjectAcl.xml
Matched in Event ID List
This event was created on:  2019-03-25 21:28:35.461615
An Event ID: 4662, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/DACL_DCSync_Right_Powe
rview_ Add-DomainObjectAcl.xml
Matched in Event ID List
This event was created on:  2019-03-25 21:28:35.463625
An Event ID: 4662, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/DACL_DCSync_Right_Powe
rview_ Add-DomainObjectAcl.xml
Matched in Event ID List
This event was created on:  2019-03-25 21:28:35.465616
An Event ID: 4662, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/DACL_DCSync_Right_Powe
rview_ Add-DomainObjectAcl.xml
Matched in Event ID List
This event was created on:  2019-03-25 21:28:35.467611
An Event ID: 4662, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/DACL_DCSync_Right_Powe
rview_ Add-DomainObjectAcl.xml
Matched in Event ID List
This event was created on:  2019-03-25 21:28:35.470615
An Event ID: 4662, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/DACL_DCSync_Right_Powe
rview_ Add-DomainObjectAcl.xml
Matched in Event ID List
This event was created on:  2019-03-25 21:28:35.472614
An Event ID: 5136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/DACL_DCSync_Right_Powe
rview_ Add-DomainObjectAcl.xml
Matched in Event ID List
This event was created on:  2019-03-25 21:28:45.022631
An Event ID: 5136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/DACL_DCSync_Right_Powe
rview_ Add-DomainObjectAcl.xml
Matched in Event ID List
This event was created on:  2019-03-25 21:28:45.022631
```

```
An Event ID: 5136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/DACL_DCSync_Right_Powe
rview_ Add-DomainObjectAcl.xml
Matched in Event ID List
This event was created on:  2019-03-25 21:28:45.023630
An Event ID: 5136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/DACL_DCSync_Right_Powe
rview_ Add-DomainObjectAcl.xml
Matched in Event ID List
This event was created on:  2019-03-25 21:28:45.023630
An Event ID: 5136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/DACL_DCSync_Right_Powe
rview_ Add-DomainObjectAcl.xml
Matched in Event ID List
This event was created on:  2019-03-25 21:28:45.023630
An Event ID: 5136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/DACL_DCSync_Right_Powe
rview_ Add-DomainObjectAcl.xml
Matched in Event ID List
This event was created on:  2019-03-25 21:28:45.023630
An Event ID: 5136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/DACL_DCSync_Right_Powe
rview_ Add-DomainObjectAcl.xml
Matched in Event ID List
This event was created on:  2019-03-25 21:28:45.024635
An Event ID: 5136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/DACL_DCSync_Right_Powe
rview_ Add-DomainObjectAcl.xml
Matched in Event ID List
This event was created on:  2019-03-25 21:28:45.024635
An Event ID: 5136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/DACL_DCSync_Right_Powe
rview_ Add-DomainObjectAcl.xml
Matched in Event ID List
This event was created on:  2019-03-25 21:28:45.024635
An Event ID: 5136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/DACL_DCSync_Right_Powe
rview_ Add-DomainObjectAcl.xml
Matched in Event ID List
This event was created on:  2019-03-25 21:28:45.025627
An Event ID: 5136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/DACL_DCSync_Right_Powe
rview_ Add-DomainObjectAcl.xml
Matched in Event ID List
This event was created on:  2019-03-25 21:28:45.025627
An Event ID: 5136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/DACL_DCSync_Right_Powe
rview_ Add-DomainObjectAcl.xml
Matched in Event ID List
This event was created on:  2019-03-25 21:28:45.025627
An Event ID: 5136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/DACL_DCSync_Right_Powe
rview_ Add-DomainObjectAcl.xml
Matched in Event ID List
```

```
This event was created on:  2019-03-25 21:28:45.025627
An Event ID: 5136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/DACL_DCSync_Right_Powe
rview_ Add-DomainObjectAcl.xml
Matched in Event ID List
This event was created on:  2019-03-25 21:28:45.025627
An Event ID: 5136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/DACL_DCSync_Right_Powe
rview_ Add-DomainObjectAcl.xml
Matched in Event ID List
This event was created on:  2019-03-25 21:28:45.026630
An Event ID: 5136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/DACL_DCSync_Right_Powe
rview_ Add-DomainObjectAcl.xml
Matched in Event ID List
This event was created on:  2019-03-25 21:28:45.026630
An Event ID: 5136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/DACL_DCSync_Right_Powe
rview_ Add-DomainObjectAcl.xml
Matched in Event ID List
This event was created on:  2019-03-25 21:28:45.026630
An Event ID: 5136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/DACL_DCSync_Right_Powe
rview_ Add-DomainObjectAcl.xml
Matched in Event ID List
This event was created on:  2019-03-25 21:28:45.026630
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persist_firefox_comhij
ack_sysmon_11_13_7_1.xml
No Match in Event ID List
This event was created on:  2019-05-21 00:35:07.308922
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persist_firefox_comhij
ack_sysmon_11_13_7_1.xml
No Match in Event ID List
This event was created on:  2019-05-21 00:35:07.463144
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persist_firefox_comhij
ack_sysmon_11_13_7_1.xml
No Match in Event ID List
This event was created on:  2019-05-21 00:35:07.474159
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persist_firefox_comhij
ack_sysmon_11_13_7_1.xml
No Match in Event ID List
This event was created on:  2019-05-21 00:35:07.474159
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persist_firefox_comhij
ack_sysmon_11_13_7_1.xml
No Match in Event ID List
This event was created on:  2019-05-21 00:35:07.474159
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persist_firefox_comhij
ack_sysmon_11_13_7_1.xml
```

```
No Match in Event ID List
This event was created on:  2019-05-21 00:35:07.474159
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persist_firefox_comhij
ack_sysmon_11_13_7_1.xml
No Match in Event ID List
This event was created on:  2019-05-21 00:35:07.474159
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persist_firefox_comhij
ack_sysmon_11_13_7_1.xml
No Match in Event ID List
This event was created on:  2019-05-21 00:35:07.474159
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persist_firefox_comhij
ack_sysmon_11_13_7_1.xml
No Match in Event ID List
This event was created on:  2019-05-21 00:35:07.518223
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persist_firefox_comhij
ack_sysmon_11_13_7_1.xml
No Match in Event ID List
This event was created on:  2019-05-21 00:35:07.870729
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persist_firefox_comhij
ack_sysmon_11_13_7_1.xml
No Match in Event ID List
This event was created on:  2019-05-21 00:35:08.224337
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persist_firefox_comhij
ack_sysmon_11_13_7_1.xml
No Match in Event ID List
This event was created on:  2019-05-21 00:35:08.279417
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persist_firefox_comhij
ack_sysmon_11_13_7_1.xml
No Match in Event ID List
This event was created on:  2019-05-21 00:35:08.717041
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persist_firefox_comhij
ack_sysmon_11_13_7_1.xml
No Match in Event ID List
This event was created on:  2019-05-21 00:35:08.728058
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persist_firefox_comhij
ack_sysmon_11_13_7_1.xml
No Match in Event ID List
This event was created on:  2019-05-21 00:35:08.728058
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persist_firefox_comhij
ack_sysmon_11_13_7_1.xml
No Match in Event ID List
This event was created on:  2019-05-21 00:35:10.161518
```

```
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persist_firefox_comhij
ack_sysmon_11_13_7_1.xml
No Match in Event ID List
This event was created on:  2019-05-21 00:35:12.705164
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persist_firefox_comhij
ack_sysmon_11_13_7_1.xml
No Match in Event ID List
This event was created on:  2019-05-21 00:36:14.747768
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Persistence/persist_firefox_comhij
ack_sysmon_11_13_7_1.xml
No Match in Event ID List
This event was created on:  2019-05-21 00:36:14.747768
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_winrm_exec_sys
mon_1_winrshost.xml
No Match in Event ID List
This event was created on:  2019-05-16 01:31:36.426870
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_winrm_exec_sys
mon_1_winrshost.xml
No Match in Event ID List
This event was created on:  2019-05-16 01:31:36.454893
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_winrm_exec_sys
mon_1_winrshost.xml
No Match in Event ID List
This event was created on:  2019-05-16 01:31:36.456890
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_DCOM_MSHTA_Let
halHTA_Sysmon_3_1.xml
No Match in Event ID List
This event was created on:  2019-05-14 01:29:04.306887
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_DCOM_MSHTA_Let
halHTA_Sysmon_3_1.xml
No Match in Event ID List
This event was created on:  2019-05-14 01:29:05.534521
An Event ID: 4624, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_WMI_4624_4688_
TargetHost.xml
Matched in Event ID List
This event was created on:  2019-03-18 22:15:36.036375
An Event ID: 4624, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_WMI_4624_4688_
TargetHost.xml
Matched in Event ID List
This event was created on:  2019-03-18 22:15:49.583101
An Event ID: 4624, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_WMI_4624_4688_
TargetHost.xml
Matched in Event ID List
```

```
This event was created on:  2019-03-18 22:15:49.614294
An Event ID: 4624, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_WMI_4624_4688_
TargetHost.xml
Matched in Event ID List
This event was created on:  2019-03-18 22:15:49.614294
An Event ID: 4688, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_WMI_4624_4688_
TargetHost.xml
Matched in Event ID List
This event was created on:  2019-03-18 22:15:49.645889
An Event ID: 4688, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_WMI_4624_4688_
TargetHost.xml
Matched in Event ID List
This event was created on:  2019-03-18 22:15:49.676748
An Event ID: 4624, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_WMI_4624_4688_
TargetHost.xml
Matched in Event ID List
This event was created on:  2019-03-18 22:15:49.692402
An Event ID: 4624, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_WMI_4624_4688_
TargetHost.xml
Matched in Event ID List
This event was created on:  2019-03-18 22:16:19.989943
An Event ID: 18, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_sysmon_psexec_
smb_meterpreter.xml
No Match in Event ID List
This event was created on:  2019-04-30 20:26:51.793589
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_sysmon_psexec_
smb_meterpreter.xml
No Match in Event ID List
This event was created on:  2019-04-30 20:26:51.949839
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_sysmon_psexec_
smb_meterpreter.xml
No Match in Event ID List
This event was created on:  2019-04-30 20:26:51.981089
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_sysmon_psexec_
smb_meterpreter.xml
No Match in Event ID List
This event was created on:  2019-04-30 20:26:52.090464
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_sysmon_psexec_
smb_meterpreter.xml
No Match in Event ID List
This event was created on:  2019-04-30 20:26:52.106089
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_sysmon_psexec_
smb_meterpreter.xml
```

```
No Match in Event ID List
This event was created on:  2019-04-30 20:26:52.356089
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_sysmon_psexec_
smb_meterpreter.xml
No Match in Event ID List
This event was created on:  2019-04-30 20:26:52.371714
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_sysmon_psexec_
smb_meterpreter.xml
No Match in Event ID List
This event was created on:  2019-04-30 20:26:53.152962
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_sysmon_psexec_
smb_meterpreter.xml
No Match in Event ID List
This event was created on:  2019-04-30 20:26:53.199839
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_sysmon_psexec_
smb_meterpreter.xml
No Match in Event ID List
This event was created on:  2019-04-30 20:26:54.152962
An Event ID: 1102, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/net_share_drive_5
142.xml
Matched in Event ID List
This event was created on:  2019-03-17 19:26:42.116688
An Event ID: 5142, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/net_share_drive_5
142.xml
Matched in Event ID List
This event was created on:  2019-03-17 19:30:30.324835
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_typical_IIS_we
bshell_sysmon_1_10_traces.xml
No Match in Event ID List
This event was created on:  2019-05-24 01:33:53.112486
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_typical_IIS_we
bshell_sysmon_1_10_traces.xml
No Match in Event ID List
This event was created on:  2019-05-24 01:33:53.122499
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_typical_IIS_we
bshell_sysmon_1_10_traces.xml
No Match in Event ID List
This event was created on:  2019-05-24 01:33:53.182587
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_typical_IIS_we
bshell_sysmon_1_10_traces.xml
No Match in Event ID List
This event was created on:  2019-05-24 01:33:53.192600
```

```
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:22.134722
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:22.224850
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:22.264908
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:22.264908
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:22.284937
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:22.284937
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.356480
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.546751
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.546751
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.556767
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
```

```
This event was created on:  2019-03-18 14:23:23.556767
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.556767
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.556767
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.566780
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.566780
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.566780
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.566780
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.566780
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.576796
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.576796
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.576796
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
```

```
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.576796
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.586809
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.586809
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.586809
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.586809
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.586809
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.586809
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.596825
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.596825
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.596825
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.596825
```

```
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.596825
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.606838
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.606838
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.606838
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.606838
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.606838
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.616854
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.616854
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.616854
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.616854
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
```

```
This event was created on:  2019-03-18 14:23:23.616854
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.626867
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.626867
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.626867
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.636883
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.636883
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.636883
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.636883
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.636883
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.666924
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.666924
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
```

```
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.666924
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.666924
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.676941
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.676941
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.676941
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.676941
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.676941
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.676941
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.686953
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.686953
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.686953
```

```
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.686953
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.686953
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.686953
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.696968
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.696968
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.696968
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.696968
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.706982
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.706982
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.706982
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
```

```
This event was created on:  2019-03-18 14:23:23.706982
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.706982
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.706982
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.716997
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.716997
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.716997
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.716997
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.716997
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.727011
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.727011
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.727011
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
```

```
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.727011
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.727011
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.727011
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.737026
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.737026
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.737026
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.737026
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.737026
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.737026
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.747040
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.747040
```

```
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.747040
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.747040
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.747040
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.757055
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.757055
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.757055
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.757055
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.757055
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.767069
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.767069
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
```

```
This event was created on:  2019-03-18 14:23:23.767069
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.767069
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.767069
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.777084
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.777084
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.777084
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.777084
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.777084
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.777084
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.787098
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.787098
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
```

```
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.787098
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.797113
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.797113
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.797113
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.807125
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.807125
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.807125
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.807125
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.807125
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.817142
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.817142
```

```
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.817142
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.817142
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.827154
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.827154
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.827154
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.837172
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.837172
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.837172
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.837172
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.837172
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
```

```
This event was created on:  2019-03-18 14:23:23.847183
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.847183
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.847183
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.847183
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.857199
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.857199
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.867212
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.867212
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.867212
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.877228
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.877228
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
```

```
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.877228
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.877228
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.887241
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.887241
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.887241
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.887241
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.897257
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.897257
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.897257
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.897257
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.897257
```

```
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.907270
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.907270
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.907270
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.907270
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.907270
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.917286
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.917286
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.917286
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.917286
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.917286
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
```

```
This event was created on:  2019-03-18 14:23:23.927299
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.927299
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.927299
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.927299
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.927299
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.927299
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.937315
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.937315
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.937315
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.937315
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.947327
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
```

```
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.947327
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.947327
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.947327
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.957344
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.957344
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.957344
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.967356
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.967356
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.967356
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.967356
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.967356
```

```
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.967356
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.977373
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.977373
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.977373
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.977373
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.977373
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.977373
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.977373
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.977373
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.977373
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
```

```
This event was created on:  2019-03-18 14:23:23.977373
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.977373
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.987385
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.987385
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.987385
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.987385
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.987385
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.987385
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.997400
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.997400
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.997400
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
```

```
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.997400
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.997400
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.997400
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.997400
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.997400
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.997400
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:23.997400
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.007414
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.007414
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.007414
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.007414
```

```
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.007414
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.007414
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.007414
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.017429
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.017429
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.017429
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.017429
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.017429
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.017429
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.017429
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
```

```
This event was created on:  2019-03-18 14:23:24.027443
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.027443
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.027443
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.027443
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.027443
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.027443
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.027443
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.027443
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.037458
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.037458
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.037458
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
```

```
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.047472
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.047472
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.047472
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.057487
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.057487
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.057487
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.057487
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.067501
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.067501
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.067501
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.077517
```

```
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.077517
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.087528
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.087528
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.087528
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.087528
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.097546
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.097546
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.107557
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.107557
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.107557
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
```

```
This event was created on:  2019-03-18 14:23:24.117575
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.117575
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.117575
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.127586
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.127586
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.137602
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.137602
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.137602
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.147615
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.147615
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.147615
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
```

```
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.147615
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.157631
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.157631
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.167645
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.167645
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.177660
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.177660
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.177660
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.187674
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.187674
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.197689
```

```
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.197689
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.197689
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.197689
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.207703
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.207703
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.207703
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.217718
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.217718
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.227730
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.227730
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
```

```
This event was created on:  2019-03-18 14:23:24.227730
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.237747
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.237747
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.237747
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.237747
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.247759
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.247759
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.247759
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.257776
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.257776
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.257776
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
```

```
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.267788
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.267788
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.267788
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.277803
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.277803
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.277803
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.277803
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.287817
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.287817
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.297832
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.297832
```

```
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.297832
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.307846
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.307846
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.307846
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.307846
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.307846
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.317862
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.317862
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.317862
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.317862
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
```

```
This event was created on:  2019-03-18 14:23:24.327875
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.327875
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.327875
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.327875
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.337891
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.337891
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.337891
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.337891
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.347904
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.347904
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.347904
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
```

```
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.347904
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.357920
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.357920
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.357920
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.357920
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.367931
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.367931
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.367931
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.367931
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.377949
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.377949
```

```
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.377949
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.377949
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.387960
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.387960
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.387960
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.387960
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.397978
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.397978
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.397978
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.407990
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
```

```
This event was created on:  2019-03-18 14:23:24.407990
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.407990
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.407990
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.418005
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.418005
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.418005
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.418005
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.428019
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.428019
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.428019
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.438034
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
```

```
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.438034
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.438034
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.448048
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.448048
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.448048
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.458063
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.458063
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.458063
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.458063
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.468077
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.468077
```

```
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.468077
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.478092
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.478092
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.478092
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.518150
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.518150
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.518150
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.558207
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.558207
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.558207
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
```

```
This event was created on:  2019-03-18 14:23:24.558207
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.568220
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.568220
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.568220
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.578236
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.578236
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.578236
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.588249
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.588249
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.588249
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.588249
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
```

```
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.598265
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.598265
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.598265
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.598265
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.608278
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.608278
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.608278
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.608278
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.608278
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.618294
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.618294
```

```
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.618294
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.618294
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.618294
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.628307
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.628307
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.628307
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.628307
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.638323
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.638323
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.638323
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
```

```
This event was created on:  2019-03-18 14:23:24.638323
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.638323
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.648335
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.648335
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.648335
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.648335
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.658352
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.658352
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.668364
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.668364
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.668364
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
```

```
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.678381
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.678381
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.678381
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.678381
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.688393
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.688393
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.688393
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.688393
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.698408
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.698408
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.698408
```

```
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.698408
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.708422
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.708422
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.708422
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.708422
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.718437
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.718437
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.718437
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.718437
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.728451
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
```

```
This event was created on:  2019-03-18 14:23:24.728451
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.728451
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.738466
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.738466
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.738466
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.738466
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.748480
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.748480
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.748480
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.748480
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.758495
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
```

```
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.758495
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.758495
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.758495
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.768509
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.768509
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.768509
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.768509
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.768509
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.778524
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.778524
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.778524
```

```
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.778524
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.778524
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.788536
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.788536
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.788536
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.788536
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.798553
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.808565
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.808565
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.808565
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
```

```
This event was created on:  2019-03-18 14:23:24.818583
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.818583
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.818583
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.818583
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.818583
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.828594
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.828594
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.828594
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.828594
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.828594
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.838610
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
```

```
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.838610
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.838610
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.838610
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.848623
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.848623
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.848623
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.848623
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.848623
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.848623
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.858639
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.858639
```

```
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.858639
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.858639
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.858639
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.868652
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.868652
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.868652
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.868652
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.878668
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.878668
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.878668
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
```

```
This event was created on:  2019-03-18 14:23:24.878668
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.878668
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.888681
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.888681
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.888681
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.888681
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.898697
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.898697
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.908710
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.908710
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.908710
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
```

```
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.908710
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.918726
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.918726
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.918726
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.918726
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.928740
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.928740
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.928740
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.928740
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.928740
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.968796
```

```
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.978811
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.988825
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.988825
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.988825
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.988825
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.998840
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:24.998840
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.008854
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.008854
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.008854
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
```

```
This event was created on:  2019-03-18 14:23:25.008854
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.018869
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.018869
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.018869
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.028883
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.028883
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.028883
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.028883
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.038898
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.038898
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.038898
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
```

```
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.038898
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.048912
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.048912
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.048912
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.048912
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.058928
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.058928
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.058928
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.058928
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.068941
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.068941
```

```
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.068941
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.068941
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.078957
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.078957
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.078957
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.078957
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.088968
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.088968
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.088968
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.088968
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
```

```
This event was created on:  2019-03-18 14:23:25.098986
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.098986
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.098986
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.098986
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.108997
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.108997
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.108997
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.119015
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.119015
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.119015
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.139042
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
```

```
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.149055
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.149055
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.159071
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.159071
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.169085
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.169085
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.179100
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.179100
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.179100
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.189114
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.189114
```

```
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.199129
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.209143
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.209143
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.209143
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.219158
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.219158
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.219158
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.219158
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.229170
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.229170
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
```

```
This event was created on:  2019-03-18 14:23:25.229170
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.239187
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.239187
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.239187
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.239187
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.239187
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.249199
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.249199
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.249199
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.249199
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.259216
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
```

```
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.259216
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.259216
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.259216
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.269228
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.269228
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.269228
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.269228
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.279243
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.279243
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.279243
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.279243
```

```
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.289257
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.289257
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.289257
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.289257
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.289257
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.299273
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.299273
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.299273
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.299273
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.309286
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
```

```
This event was created on:  2019-03-18 14:23:25.309286
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.309286
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.309286
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.319302
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.319302
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.319302
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.319302
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.319302
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.329315
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.329315
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.329315
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
```

```
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.329315
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.339331
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.339331
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.339331
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.339331
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.339331
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.349344
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.349344
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.349344
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.349344
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.359360
```

```
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.359360
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.359360
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.369371
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.369371
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.369371
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.379389
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.379389
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.379389
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.389400
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.389400
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
```

```
This event was created on:  2019-03-18 14:23:25.389400
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.399418
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.399418
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.399418
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.409430
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.409430
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.409430
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.409430
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.419445
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.419445
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.419445
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
```

```
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.419445
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.429459
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.429459
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.429459
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.439474
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.439474
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.439474
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.439474
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.449488
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.449488
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.449488
```

```
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.449488
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.459503
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.459503
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.459503
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.469517
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.469517
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.479532
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.479532
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.489546
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.489546
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
```

```
This event was created on:  2019-03-18 14:23:25.489546
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.499561
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.499561
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.509573
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.509573
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.509573
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.509573
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.519590
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.519590
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.519590
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.529602
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
```

```
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.529602
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.529602
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.539619
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.539619
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.539619
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.549631
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.549631
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.549631
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.559647
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.559647
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.559647
```

```
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.559647
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.559647
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.559647
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.569660
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.569660
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.569660
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.569660
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.569660
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.569660
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.579676
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
```

```
This event was created on:  2019-03-18 14:23:25.579676
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.579676
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.579676
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.579676
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.579676
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.589689
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.589689
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.589689
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.589689
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.589689
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.599705
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
```

```
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.599705
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.599705
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.599705
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.599705
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.599705
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.609718
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.609718
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.609718
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.609718
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.609718
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.619734
```

```
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.619734
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.619734
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.619734
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.619734
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.619734
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.619734
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.629747
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.629747
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.629747
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.629747
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
```

```
This event was created on:  2019-03-18 14:23:25.629747
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.629747
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.639763
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.639763
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.639763
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.639763
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.639763
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.639763
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.649775
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.649775
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.649775
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
```

```
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.649775
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.649775
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.659792
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.659792
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.659792
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.659792
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.659792
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.659792
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.659792
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.669804
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.669804
```

```
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.669804
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.669804
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.669804
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.679821
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.679821
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.679821
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.679821
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.679821
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.679821
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.689833
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
```

```
This event was created on:  2019-03-18 14:23:25.689833
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.689833
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.689833
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.689833
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.689833
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.699848
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.699848
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.699848
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.709862
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.709862
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.709862
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
```

```
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.709862
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.709862
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:25.709862
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:26.981691
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:26.981691
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:26.981691
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:27.021749
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:27.061808
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:27.071819
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:27.081837
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:27.081837
```

```
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:45.488304
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:45.548389
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:45.548389
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:45.598461
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:47.721514
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:47.721514
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:53.279507
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:53.279507
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:56.403999
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:56.403999
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
```

```
This event was created on:  2019-03-18 14:23:56.414013
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:58.386850
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:58.386850
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:23:59.117901
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:24:00.369701
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:24:04.105072
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:24:04.105072
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:24:04.115088
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:24:04.115088
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:24:04.115088
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:24:07.239580
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
```

```
No Match in Event ID List
This event was created on:  2019-03-18 14:24:07.249594
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:24:07.249594
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:24:07.529997
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:24:07.529997
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:24:07.630140
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:24:07.700243
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:24:09.913424
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:24:09.913424
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:24:09.913424
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:24:09.923439
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:24:09.933453
```

```
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:24:10.053625
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:24:10.053625
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:24:10.053625
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:24:10.053625
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_5145_Remote_Fi
leCopy.xml
No Match in Event ID List
This event was created on:  2019-03-18 14:24:10.063641
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_dcom_InternetE
xplorer.Application_sysmon_1.xml
No Match in Event ID List
This event was created on:  2019-05-19 02:02:21.068573
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_tsclient_start
up_folder.xml
No Match in Event ID List
This event was created on:  2019-05-14 14:03:45.100849
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_tsclient_start
up_folder.xml
No Match in Event ID List
This event was created on:  2019-05-14 14:04:05.697491
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_tsclient_start
up_folder.xml
No Match in Event ID List
This event was created on:  2019-05-14 14:04:06.339355
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_tsclient_start
up_folder.xml
No Match in Event ID List
This event was created on:  2019-05-14 14:04:28.860777
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/sysmon_1_exec_via
_sql_xpcmdshell.xml
No Match in Event ID List
```

```
This event was created on:  2019-11-03 13:51:58.263042
An Event ID: 169, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/RemotePowerShell_
MS_Windows-Remote_Management_EventID_169.xml
No Match in Event ID List
This event was created on:  2019-05-20 15:54:31.706909
An Event ID: 193, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/RemotePowerShell_
MS_Windows-Remote_Management_EventID_169.xml
No Match in Event ID List
This event was created on:  2019-05-20 15:54:31.706909
An Event ID: 169, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/RemotePowerShell_
MS_Windows-Remote_Management_EventID_169.xml
No Match in Event ID List
This event was created on:  2019-05-20 15:54:32.064405
An Event ID: 193, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/RemotePowerShell_
MS_Windows-Remote_Management_EventID_169.xml
No Match in Event ID List
This event was created on:  2019-05-20 15:54:32.064405
An Event ID: 169, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/RemotePowerShell_
MS_Windows-Remote_Management_EventID_169.xml
No Match in Event ID List
This event was created on:  2019-05-20 15:54:32.564899
An Event ID: 193, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/RemotePowerShell_
MS_Windows-Remote_Management_EventID_169.xml
No Match in Event ID List
This event was created on:  2019-05-20 15:54:32.564899
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_renamed_psexec
svc_5145.xml
No Match in Event ID List
This event was created on:  2019-01-19 12:57:09.530684
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_renamed_psexec
svc_5145.xml
No Match in Event ID List
This event was created on:  2019-01-19 12:57:09.530684
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_renamed_psexec
svc_5145.xml
No Match in Event ID List
This event was created on:  2019-01-19 12:57:09.540697
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_renamed_psexec
svc_5145.xml
No Match in Event ID List
This event was created on:  2019-01-19 12:57:30.400692
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_renamed_psexec
svc_5145.xml
```

```
No Match in Event ID List
This event was created on:  2019-01-19 12:57:30.400692
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_renamed_psexec
svc_5145.xml
No Match in Event ID List
This event was created on:  2019-01-19 12:57:32.223312
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_renamed_psexec
svc_5145.xml
No Match in Event ID List
This event was created on:  2019-01-19 12:57:32.233328
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_renamed_psexec
svc_5145.xml
No Match in Event ID List
This event was created on:  2019-01-19 12:57:32.794134
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_renamed_psexec
svc_5145.xml
No Match in Event ID List
This event was created on:  2019-01-19 12:57:32.804148
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_renamed_psexec
svc_5145.xml
No Match in Event ID List
This event was created on:  2019-01-19 12:57:40.595352
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_renamed_psexec
svc_5145.xml
No Match in Event ID List
This event was created on:  2019-01-19 12:57:41.716965
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_renamed_psexec
svc_5145.xml
No Match in Event ID List
This event was created on:  2019-01-19 12:57:41.716965
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_renamed_psexec
svc_5145.xml
No Match in Event ID List
This event was created on:  2019-01-19 12:57:42.237713
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_renamed_psexec
svc_5145.xml
No Match in Event ID List
This event was created on:  2019-01-19 12:57:42.237713
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_renamed_psexec
svc_5145.xml
No Match in Event ID List
This event was created on:  2019-01-19 13:00:10.350689
```

```
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_renamed_psexec
svc_5145.xml
No Match in Event ID List
This event was created on:  2019-01-19 13:00:10.350689
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_renamed_psexec
svc_5145.xml
No Match in Event ID List
This event was created on:  2019-01-19 13:00:10.350689
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_renamed_psexec
svc_5145.xml
No Match in Event ID List
This event was created on:  2019-01-19 13:00:10.380732
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_renamed_psexec
svc_5145.xml
No Match in Event ID List
This event was created on:  2019-01-19 13:00:10.540962
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_renamed_psexec
svc_5145.xml
No Match in Event ID List
This event was created on:  2019-01-19 13:00:10.711208
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_renamed_psexec
svc_5145.xml
No Match in Event ID List
This event was created on:  2019-01-19 13:00:10.711208
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_renamed_psexec
svc_5145.xml
No Match in Event ID List
This event was created on:  2019-01-19 13:00:10.711208
An Event ID: 1102, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_WMIC_4648_rpcs
s.xml
Matched in Event ID List
This event was created on:  2019-03-18 11:27:00.438450
An Event ID: 4688, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_WMIC_4648_rpcs
s.xml
Matched in Event ID List
This event was created on:  2019-03-18 11:27:05.425621
An Event ID: 4648, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_WMIC_4648_rpcs
s.xml
Matched in Event ID List
This event was created on:  2019-03-18 11:27:23.231224
An Event ID: 4648, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_WMIC_4648_rpcs
s.xml
Matched in Event ID List
```

```
This event was created on:  2019-03-18 11:27:23.261267
An Event ID: 4648, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_WMIC_4648_rpcs
s.xml
Matched in Event ID List
This event was created on:  2019-03-18 11:27:23.271280
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/powercat_revShell
_sysmon_1_3.xml
No Match in Event ID List
This event was created on:  2019-06-20 08:07:42.331810
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/powercat_revShell
_sysmon_1_3.xml
No Match in Event ID List
This event was created on:  2019-06-20 08:07:42.331810
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/powercat_revShell
_sysmon_1_3.xml
No Match in Event ID List
This event was created on:  2019-06-20 08:07:48.909935
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/powercat_revShell
_sysmon_1_3.xml
No Match in Event ID List
This event was created on:  2019-06-20 08:07:48.909935
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/powercat_revShell
_sysmon_1_3.xml
No Match in Event ID List
This event was created on:  2019-06-20 08:07:48.925562
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/powercat_revShell
_sysmon_1_3.xml
No Match in Event ID List
This event was created on:  2019-06-20 08:07:48.925562
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/powercat_revShell
_sysmon_1_3.xml
No Match in Event ID List
This event was created on:  2019-06-20 08:07:50.378685
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/powercat_revShell
_sysmon_1_3.xml
No Match in Event ID List
This event was created on:  2019-06-20 08:07:52.956810
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/powercat_revShell
_sysmon_1_3.xml
No Match in Event ID List
This event was created on:  2019-06-20 08:07:58.816185
An Event ID: 1102, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_4624_mimikatz_
sekurlsa_pth_source_machine.xml
```

```
Matched in Event ID List
This event was created on:  2019-03-18 11:06:25.485214
An Event ID: 4624, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_4624_mimikatz_
sekurlsa_pth_source_machine.xml
Matched in Event ID List
This event was created on:  2019-03-18 11:06:29.911579
An Event ID: 4672, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_4624_mimikatz_
sekurlsa_pth_source_machine.xml
Matched in Event ID List
This event was created on:  2019-03-18 11:06:29.911579
An Event ID: 4688, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_4624_mimikatz_
sekurlsa_pth_source_machine.xml
Matched in Event ID List
This event was created on:  2019-03-18 11:06:29.911579
An Event ID: 4688, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_4624_mimikatz_
sekurlsa_pth_source_machine.xml
Matched in Event ID List
This event was created on:  2019-03-18 11:06:29.961651
An Event ID: 4688, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_4624_mimikatz_
sekurlsa_pth_source_machine.xml
Matched in Event ID List
This event was created on:  2019-03-18 11:06:46.305151
An Event ID: 1638418454, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_xp_cmdshell_MS
SQL_Events.xml
No Match in Event ID List
This event was created on:  2019-11-04 09:27:25.986622
An Event ID: 1638418454, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_xp_cmdshell_MS
SQL_Events.xml
No Match in Event ID List
This event was created on:  2019-11-04 09:27:25.986622
An Event ID: 1638418454, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_xp_cmdshell_MS
SQL_Events.xml
No Match in Event ID List
This event was created on:  2019-11-04 09:27:26.041618
An Event ID: 1638418454, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_xp_cmdshell_MS
SQL_Events.xml
No Match in Event ID List
This event was created on:  2019-11-04 09:27:26.127037
An Event ID: 1638415457, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_xp_cmdshell_MS
SQL_Events.xml
No Match in Event ID List
This event was created on:  2019-11-04 09:27:26.143063
```

```
An Event ID: 1638415457, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_xp_cmdshell_MS
SQL_Events.xml
No Match in Event ID List
This event was created on:  2019-11-04 09:27:26.158621
An Event ID: 1638433205, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_xp_cmdshell_MS
SQL_Events.xml
No Match in Event ID List
This event was created on:  2019-11-04 09:27:26.315067
An Event ID: 1638433205, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_xp_cmdshell_MS
SQL_Events.xml
No Match in Event ID List
This event was created on:  2019-11-04 09:27:26.315067
An Event ID: 1638433205, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_xp_cmdshell_MS
SQL_Events.xml
No Match in Event ID List
This event was created on:  2019-11-04 09:27:26.315067
An Event ID: 1638415457, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_xp_cmdshell_MS
SQL_Events.xml
No Match in Event ID List
This event was created on:  2019-11-04 09:27:26.315067
An Event ID: 1638433205, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_xp_cmdshell_MS
SQL_Events.xml
No Match in Event ID List
This event was created on:  2019-11-04 09:27:26.315067
An Event ID: 1638433205, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_xp_cmdshell_MS
SQL_Events.xml
No Match in Event ID List
This event was created on:  2019-11-04 09:27:26.315067
An Event ID: 1638433205, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_xp_cmdshell_MS
SQL_Events.xml
No Match in Event ID List
This event was created on:  2019-11-04 09:27:26.315067
An Event ID: 1638433205, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_xp_cmdshell_MS
SQL_Events.xml
No Match in Event ID List
This event was created on:  2019-11-04 09:27:26.315067
An Event ID: 1638433205, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_xp_cmdshell_MS
SQL_Events.xml
No Match in Event ID List
This event was created on:  2019-11-04 09:27:26.315067
An Event ID: 1638433205, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_xp_cmdshell_MS
SQL_Events.xml
No Match in Event ID List
```

```
This event was created on:  2019-11-04 09:27:26.315067
An Event ID: 1638433205, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_xp_cmdshell_MS
SQL_Events.xml
No Match in Event ID List
This event was created on:  2019-11-04 09:27:26.315067
An Event ID: 1638433205, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_xp_cmdshell_MS
SQL_Events.xml
No Match in Event ID List
This event was created on:  2019-11-04 09:27:26.315067
An Event ID: 1638433205, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_xp_cmdshell_MS
SQL_Events.xml
No Match in Event ID List
This event was created on:  2019-11-04 09:27:26.315067
An Event ID: 1638415457, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_xp_cmdshell_MS
SQL_Events.xml
No Match in Event ID List
This event was created on:  2019-11-04 09:27:26.315067
An Event ID: 1638433205, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_xp_cmdshell_MS
SQL_Events.xml
No Match in Event ID List
This event was created on:  2019-11-04 09:27:27.315012
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/smb_bi_auth_conn_
spoolsample.xml
No Match in Event ID List
This event was created on:  2019-09-01 12:04:22.033684
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/smb_bi_auth_conn_
spoolsample.xml
No Match in Event ID List
This event was created on:  2019-09-01 12:04:22.908024
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_Remote_Service
01_5145_svcctl.xml
No Match in Event ID List
This event was created on:  2019-03-19 00:41:28.961628
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_PowershellRemo
ting_sysmon_1_wsmprovhost.xml
No Match in Event ID List
This event was created on:  2019-05-16 01:38:19.630865
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/spoolsample_5145.
xml
No Match in Event ID List
This event was created on:  2019-09-01 11:54:22.450676
An Event ID: 18, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/lm_sysmon_18_rems
hell_over_namedpipe.xml
```

```
No Match in Event ID List
This event was created on:  2019-04-29 20:59:14.447313
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/lm_sysmon_18_rems
hell_over_namedpipe.xml
No Match in Event ID List
This event was created on:  2019-04-29 20:59:15.575970
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/lm_sysmon_18_rems
hell_over_namedpipe.xml
No Match in Event ID List
This event was created on:  2019-04-29 20:59:21.539310
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/lm_sysmon_18_rems
hell_over_namedpipe.xml
No Match in Event ID List
This event was created on:  2019-04-29 20:59:21.539310
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/lm_sysmon_18_rems
hell_over_namedpipe.xml
No Match in Event ID List
This event was created on:  2019-04-29 20:59:22.144045
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/lm_sysmon_18_rems
hell_over_namedpipe.xml
No Match in Event ID List
This event was created on:  2019-04-29 20:59:22.144045
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/lm_sysmon_18_rems
hell_over_namedpipe.xml
No Match in Event ID List
This event was created on:  2019-04-29 20:59:55.472170
An Event ID: 91, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_winrm_target_w
rmlogs_91_wsmanShellStarted_poorLog.xml
No Match in Event ID List
This event was created on:  2019-05-16 01:33:54.567896
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_sysmon_3_DCOM_
ShellBrowserWindow_ShellWindows.xml
No Match in Event ID List
This event was created on:  2019-05-14 00:29:52.744024
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_sysmon_3_DCOM_
ShellBrowserWindow_ShellWindows.xml
No Match in Event ID List
This event was created on:  2019-05-14 00:32:22.775274
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_sysmon_3_DCOM_
ShellBrowserWindow_ShellWindows.xml
No Match in Event ID List
This event was created on:  2019-05-14 00:32:36.775274
```

```
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_impacket_docme
xec_mmc_sysmon_01.xml
No Match in Event ID List
This event was created on:  2019-04-30 20:35:11.856089
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_impacket_docme
xec_mmc_sysmon_01.xml
No Match in Event ID List
This event was created on:  2019-04-30 20:35:12.449839
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_impacket_docme
xec_mmc_sysmon_01.xml
No Match in Event ID List
This event was created on:  2019-04-30 20:35:13.168589
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_impacket_docme
xec_mmc_sysmon_01.xml
No Match in Event ID List
This event was created on:  2019-04-30 20:35:13.168589
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_impacket_docme
xec_mmc_sysmon_01.xml
No Match in Event ID List
This event was created on:  2019-04-30 20:35:13.418589
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_impacket_docme
xec_mmc_sysmon_01.xml
No Match in Event ID List
This event was created on:  2019-04-30 20:35:13.418589
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_impacket_docme
xec_mmc_sysmon_01.xml
No Match in Event ID List
This event was created on:  2019-04-30 20:35:13.449839
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_impacket_docme
xec_mmc_sysmon_01.xml
No Match in Event ID List
This event was created on:  2019-04-30 20:35:13.512339
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_impacket_docme
xec_mmc_sysmon_01.xml
No Match in Event ID List
This event was created on:  2019-04-30 20:35:13.543589
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_REMCOM_5145_Ta
rgetHost.xml
No Match in Event ID List
This event was created on:  2019-02-16 17:54:26.956251
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_REMCOM_5145_Ta
rgetHost.xml
No Match in Event ID List
```

```
This event was created on:  2019-02-16 17:54:26.956251
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_REMCOM_5145_Ta
rgetHost.xml
No Match in Event ID List
This event was created on:  2019-02-16 17:54:26.956251
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_REMCOM_5145_Ta
rgetHost.xml
No Match in Event ID List
This event was created on:  2019-02-16 17:54:41.256813
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_REMCOM_5145_Ta
rgetHost.xml
No Match in Event ID List
This event was created on:  2019-02-16 17:55:47.181608
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_REMCOM_5145_Ta
rgetHost.xml
No Match in Event ID List
This event was created on:  2019-02-16 17:55:47.181608
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_REMCOM_5145_Ta
rgetHost.xml
No Match in Event ID List
This event was created on:  2019-02-16 17:55:47.181608
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_REMCOM_5145_Ta
rgetHost.xml
No Match in Event ID List
This event was created on:  2019-02-16 17:56:01.472158
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_REMCOM_5145_Ta
rgetHost.xml
No Match in Event ID List
This event was created on:  2019-02-16 17:57:41.475956
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_REMCOM_5145_Ta
rgetHost.xml
No Match in Event ID List
This event was created on:  2019-02-16 17:57:41.475956
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_REMCOM_5145_Ta
rgetHost.xml
No Match in Event ID List
This event was created on:  2019-02-16 17:57:41.475956
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_REMCOM_5145_Ta
rgetHost.xml
No Match in Event ID List
This event was created on:  2019-02-16 17:57:55.766504
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_REMCOM_5145_Ta
rgetHost.xml
```

```
No Match in Event ID List
This event was created on:  2019-02-16 18:19:18.442326
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_REMCOM_5145_Ta
rgetHost.xml
No Match in Event ID List
This event was created on:  2019-02-16 18:19:18.442326
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_REMCOM_5145_Ta
rgetHost.xml
No Match in Event ID List
This event was created on:  2019-02-16 18:19:18.442326
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_REMCOM_5145_Ta
rgetHost.xml
No Match in Event ID List
This event was created on:  2019-02-16 18:19:18.442326
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_REMCOM_5145_Ta
rgetHost.xml
No Match in Event ID List
This event was created on:  2019-02-16 18:19:18.442326
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_REMCOM_5145_Ta
rgetHost.xml
No Match in Event ID List
This event was created on:  2019-02-16 18:19:18.442326
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_REMCOM_5145_Ta
rgetHost.xml
No Match in Event ID List
This event was created on:  2019-02-16 18:19:18.442326
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_REMCOM_5145_Ta
rgetHost.xml
No Match in Event ID List
This event was created on:  2019-02-16 18:19:18.442326
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_REMCOM_5145_Ta
rgetHost.xml
No Match in Event ID List
This event was created on:  2019-02-16 18:19:18.442326
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_REMCOM_5145_Ta
rgetHost.xml
No Match in Event ID List
This event was created on:  2019-02-16 18:19:18.442326
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_REMCOM_5145_Ta
rgetHost.xml
No Match in Event ID List
This event was created on:  2019-02-16 18:19:18.442326
```

```
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_REMCOM_5145_Ta
rgetHost.xml
No Match in Event ID List
This event was created on:  2019-02-16 18:19:18.442326
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_REMCOM_5145_Ta
rgetHost.xml
No Match in Event ID List
This event was created on:  2019-02-16 18:19:18.442326
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_REMCOM_5145_Ta
rgetHost.xml
No Match in Event ID List
This event was created on:  2019-02-16 18:19:18.442326
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_REMCOM_5145_Ta
rgetHost.xml
No Match in Event ID List
This event was created on:  2019-02-16 18:19:18.442326
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_REMCOM_5145_Ta
rgetHost.xml
No Match in Event ID List
This event was created on:  2019-02-16 18:19:18.442326
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_REMCOM_5145_Ta
rgetHost.xml
No Match in Event ID List
This event was created on:  2019-02-16 18:19:18.442326
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_REMCOM_5145_Ta
rgetHost.xml
No Match in Event ID List
This event was created on:  2019-02-16 18:19:18.522442
An Event ID: 1102, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_ScheduledTask_
ATSVC_target_host.xml
Matched in Event ID List
This event was created on:  2019-03-19 00:02:00.383089
An Event ID: 4624, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_ScheduledTask_
ATSVC_target_host.xml
Matched in Event ID List
This event was created on:  2019-03-19 00:02:04.179623
An Event ID: 4776, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_ScheduledTask_
ATSVC_target_host.xml
Matched in Event ID List
This event was created on:  2019-03-19 00:02:04.210688
An Event ID: 4672, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_ScheduledTask_
ATSVC_target_host.xml
Matched in Event ID List
```

```
This event was created on:  2019-03-19 00:02:04.210688
An Event ID: 4624, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_ScheduledTask_
ATSVC_target_host.xml
Matched in Event ID List
This event was created on:  2019-03-19 00:02:04.210688
An Event ID: 4776, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_ScheduledTask_
ATSVC_target_host.xml
Matched in Event ID List
This event was created on:  2019-03-19 00:02:04.226250
An Event ID: 4672, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_ScheduledTask_
ATSVC_target_host.xml
Matched in Event ID List
This event was created on:  2019-03-19 00:02:04.226250
An Event ID: 4624, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_ScheduledTask_
ATSVC_target_host.xml
Matched in Event ID List
This event was created on:  2019-03-19 00:02:04.226250
An Event ID: 5140, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_ScheduledTask_
ATSVC_target_host.xml
Matched in Event ID List
This event was created on:  2019-03-19 00:02:04.226250
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_ScheduledTask_
ATSVC_target_host.xml
No Match in Event ID List
This event was created on:  2019-03-19 00:02:04.241919
An Event ID: 4776, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_ScheduledTask_
ATSVC_target_host.xml
Matched in Event ID List
This event was created on:  2019-03-19 00:02:04.257776
An Event ID: 4672, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_ScheduledTask_
ATSVC_target_host.xml
Matched in Event ID List
This event was created on:  2019-03-19 00:02:04.257776
An Event ID: 4624, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_ScheduledTask_
ATSVC_target_host.xml
Matched in Event ID List
This event was created on:  2019-03-19 00:02:04.257776
An Event ID: 4698, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_ScheduledTask_
ATSVC_target_host.xml
Matched in Event ID List
This event was created on:  2019-03-19 00:02:04.319944
An Event ID: 4688, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_ScheduledTask_
ATSVC_target_host.xml
```

```
Matched in Event ID List
This event was created on:  2019-03-19 00:02:04.319944
An Event ID: 4688, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_ScheduledTask_
ATSVC_target_host.xml
Matched in Event ID List
This event was created on:  2019-03-19 00:02:04.335562
An Event ID: 4688, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_ScheduledTask_
ATSVC_target_host.xml
Matched in Event ID List
This event was created on:  2019-03-19 00:02:04.335562
An Event ID: 4699, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_ScheduledTask_
ATSVC_target_host.xml
Matched in Event ID List
This event was created on:  2019-03-19 00:02:04.351252
An Event ID: 5140, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_ScheduledTask_
ATSVC_target_host.xml
Matched in Event ID List
This event was created on:  2019-03-19 00:02:04.367441
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_ScheduledTask_
ATSVC_target_host.xml
No Match in Event ID List
This event was created on:  2019-03-19 00:02:04.398153
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_ScheduledTask_
ATSVC_target_host.xml
No Match in Event ID List
This event was created on:  2019-03-19 00:02:04.398153
An Event ID: 4688, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_ScheduledTask_
ATSVC_target_host.xml
Matched in Event ID List
This event was created on:  2019-03-19 00:02:04.398153
An Event ID: 5140, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_ScheduledTask_
ATSVC_target_host.xml
Matched in Event ID List
This event was created on:  2019-03-19 00:02:07.430208
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_ScheduledTask_
ATSVC_target_host.xml
No Match in Event ID List
This event was created on:  2019-03-19 00:02:07.445772
An Event ID: 5140, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_ScheduledTask_
ATSVC_target_host.xml
Matched in Event ID List
This event was created on:  2019-03-19 00:02:07.508324
```

```
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_ScheduledTask_
ATSVC_target_host.xml
No Match in Event ID List
This event was created on:  2019-03-19 00:02:07.523676
An Event ID: 4776, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_ScheduledTask_
ATSVC_target_host.xml
Matched in Event ID List
This event was created on:  2019-03-19 00:02:16.835958
An Event ID: 4661, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_ScheduledTask_
ATSVC_target_host.xml
Matched in Event ID List
This event was created on:  2019-03-19 00:02:17.117342
An Event ID: 4661, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_ScheduledTask_
ATSVC_target_host.xml
Matched in Event ID List
This event was created on:  2019-03-19 00:02:17.117342
An Event ID: 4661, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_ScheduledTask_
ATSVC_target_host.xml
Matched in Event ID List
This event was created on:  2019-03-19 00:02:17.117342
An Event ID: 4672, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_ScheduledTask_
ATSVC_target_host.xml
Matched in Event ID List
This event was created on:  2019-03-19 00:02:21.460920
An Event ID: 4624, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_ScheduledTask_
ATSVC_target_host.xml
Matched in Event ID List
This event was created on:  2019-03-19 00:02:21.460920
An Event ID: 4672, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_ScheduledTask_
ATSVC_target_host.xml
Matched in Event ID List
This event was created on:  2019-03-19 00:02:21.929554
An Event ID: 4624, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_ScheduledTask_
ATSVC_target_host.xml
Matched in Event ID List
This event was created on:  2019-03-19 00:02:21.929554
An Event ID: 163847045, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_Remote_Service
02_7045.xml
No Match in Event ID List
This event was created on:  2019-03-03 09:20:28.621489
An Event ID: 163847045, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_Remote_Service
02_7045.xml
No Match in Event ID List
```

```
This event was created on:  2019-03-03 09:24:24.699652
An Event ID: 163847045, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_Remote_Service
02_7045.xml
No Match in Event ID List
This event was created on:  2019-03-19 00:41:29.008934
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_add_new_namedp
ipe_tp_nullsession_registry_turla_like_ttp.xml
No Match in Event ID List
This event was created on:  2019-07-03 20:10:06.475561
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_wmiexec_impack
et_sysmon_whoami.xml
No Match in Event ID List
This event was created on:  2019-04-30 20:32:50.902962
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_wmiexec_impack
et_sysmon_whoami.xml
No Match in Event ID List
This event was created on:  2019-04-30 20:32:51.168589
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_wmiexec_impack
et_sysmon_whoami.xml
No Match in Event ID List
This event was created on:  2019-04-30 20:32:51.246714
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_wmiexec_impack
et_sysmon_whoami.xml
No Match in Event ID List
This event was created on:  2019-04-30 20:32:51.324839
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_wmiexec_impack
et_sysmon_whoami.xml
No Match in Event ID List
This event was created on:  2019-04-30 20:32:51.371714
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_wmiexec_impack
et_sysmon_whoami.xml
No Match in Event ID List
This event was created on:  2019-04-30 20:32:52.402962
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Lateral_Movement/LM_wmiexec_impack
et_sysmon_whoami.xml
No Match in Event ID List
This event was created on:  2019-04-30 20:32:52.402962
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:32:55.583666
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
```

```
No Match in Event ID List
This event was created on:  2019-07-29 21:32:57.633156
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:32:58.659405
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:32:58.711830
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:32:59.234755
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:32:59.582600
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:03.193386
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:03.254713
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:03.886610
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:03.966393
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:04.008881
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:08.202019
```

```
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:08.318895
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:08.446373
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:13.214691
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:13.225412
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:18.286776
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:18.310205
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:18.583990
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:19.891563
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:20.186247
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:20.711067
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
```

```
This event was created on:  2019-07-29 21:33:20.711201
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:21.567755
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:23.215719
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:23.232565
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:23.507565
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:24.104733
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:24.563745
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:25.202818
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:28.250664
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:28.374372
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:29.341501
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
```

```
No Match in Event ID List
This event was created on:  2019-07-29 21:33:29.565737
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:29.646278
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:30.074656
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:34.295069
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:34.411036
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:34.483713
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:39.312305
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:39.358047
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:39.372599
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:39.907322
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:44.268288
```

```
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:44.287386
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:44.641176
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:44.819319
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:45.581171
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:46.095762
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:49.340889
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:49.748806
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:49.889688
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:50.104868
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:53.776442
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
```

```
This event was created on:  2019-07-29 21:33:53.843592
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:54.246155
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:54.630548
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:54.718576
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:56.665354
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:58.256845
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:58.286383
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:58.485477
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:58.543692
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:58.598591
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:33:58.683058
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
```

```
No Match in Event ID List
This event was created on:  2019-07-29 21:34:00.330767
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:00.420235
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:00.434980
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:00.442242
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:00.460196
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:00.466818
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:00.707405
An Event ID: 12, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:00.715900
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:00.724165
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:00.731449
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:00.970968
```

```
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:01.057426
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:01.090446
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:01.660498
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:05.237600
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:05.252684
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:05.502592
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:05.542307
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:10.373482
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:10.388197
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:10.708141
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
```

```
This event was created on:  2019-07-29 21:34:11.041109
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:11.501503
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:12.352682
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:15.226408
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:15.252184
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:15.658167
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:20.238304
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:20.262274
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:20.459064
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:21.867100
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:21.867544
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
```

```
No Match in Event ID List
This event was created on:  2019-07-29 21:34:25.202955
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:25.269897
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:25.659355
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:30.237041
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:30.258081
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:30.685270
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:30.807634
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:35.313087
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:35.337717
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:35.347710
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:35.838188
```

```
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:35.878708
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:35.918011
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:35.982779
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:36.421272
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:36.534473
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:36.548586
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:40.261290
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:40.385519
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:40.889027
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:41.793312
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
```

```
This event was created on:  2019-07-29 21:34:45.242405
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:45.311644
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:45.606737
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/panache_sy
smon_vs_EDRTestingScript.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:34:45.660036
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:42:51.446281
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:42:53.295578
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:43:03.303217
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:43:46.623217
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:44:08.161839
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:44:08.185343
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:44:08.221460
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
```

```
No Match in Event ID List
This event was created on:  2019-07-19 14:44:08.240767
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:44:08.268803
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:44:08.288860
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:44:08.307215
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:44:09.150759
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:44:09.176039
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:44:09.253714
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:44:09.278042
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:44:09.310810
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:44:09.351887
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:44:26.222431
```

```
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:44:26.246189
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:44:32.101995
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:44:49.679319
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:44:53.219597
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:44:53.258049
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:44:53.292454
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:44:53.330492
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:44:53.349171
An Event ID: 12, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:44:53.371305
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:44:53.402498
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
```

```
This event was created on:  2019-07-19 14:45:06.075724
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:45:06.137175
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:45:06.161409
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:45:06.196457
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:45:06.213490
An Event ID: 12, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:45:06.240379
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:45:06.267992
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:45:19.483250
An Event ID: 12, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:45:24.234606
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:45:31.287863
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:45:55.034351
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
```

```
No Match in Event ID List
This event was created on:  2019-07-19 14:45:55.105804
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:45:55.621447
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:45:55.681219
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:45:55.699293
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:45:56.033241
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:45:56.069496
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:46:19.052666
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:46:19.443586
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:46:19.484316
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:46:20.767101
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:46:20.775471
```

```
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:46:20.787647
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:46:20.802189
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:46:20.817503
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:46:20.824926
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:46:20.830944
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:46:20.841297
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:46:20.849228
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:46:20.858982
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:46:51.883827
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:46:51.957888
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
```

```
This event was created on:  2019-07-19 14:47:21.972038
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:47:37.096235
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:47:37.127264
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:47:37.147055
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:47:37.168863
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:47:37.215704
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:47:40.691439
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:47:40.706041
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:47:40.863054
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:47:45.585327
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:47:45.624945
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
```

```
No Match in Event ID List
This event was created on:  2019-07-19 14:47:45.773399
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:47:45.958874
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:47:46.112440
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:47:46.302557
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:47:51.816822
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:47:51.865963
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:47:51.997980
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:47:52.010792
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:47:52.046322
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:47:57.227966
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:47:57.274199
```

```
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:48:04.103365
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:48:04.131411
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:48:05.365622
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:48:30.640915
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:48:30.660875
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:48:30.799469
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:48:30.807486
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:48:30.900988
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:48:30.917349
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:48:31.012222
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
```

```
This event was created on:  2019-07-19 14:48:31.041710
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:48:31.134375
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:48:31.157171
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:48:31.240294
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:48:36.834888
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:48:36.882586
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:48:37.264351
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:48:37.347265
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:48:41.050661
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:48:41.085108
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:48:41.109076
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
```

```
No Match in Event ID List
This event was created on:  2019-07-19 14:48:46.238056
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:48:57.466583
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:48:57.524876
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:48:57.557947
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:48:57.570057
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:49:31.690830
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:49:32.150328
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:49:32.180586
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:49:32.227373
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:49:32.249443
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:49:32.304939
```

```
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:49:32.335445
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:49:32.389557
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:49:32.413389
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:49:32.463556
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:49:32.497480
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:49:32.551678
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:49:32.585243
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:49:32.660402
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:49:32.678106
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:49:32.728252
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
```

```
This event was created on:  2019-07-19 14:49:32.743507
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:49:32.789066
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:49:32.807707
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:49:32.850893
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:49:32.868914
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:49:32.921206
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:49:32.937862
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:49:32.975132
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:49:32.990534
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:49:33.036329
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:49:33.059629
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
```

```
No Match in Event ID List
This event was created on:  2019-07-19 14:49:33.147860
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:49:33.175814
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:49:33.225775
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:49:33.251690
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:49:33.303358
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:49:33.331942
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:49:33.375717
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:49:33.392502
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:49:33.559319
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:49:33.572020
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:49:33.619257
```

```
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:49:33.632549
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:49:39.229170
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:49:39.255339
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:49:41.660271
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:49:41.691050
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:49:43.569071
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:49:51.996250
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:49:52.048002
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:49:52.053917
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:49:52.210871
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
```

```
This event was created on:  2019-07-19 14:49:52.275627
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:50:02.174887
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:50:02.194098
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:50:02.220425
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:50:02.249575
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:50:07.279972
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:50:07.299767
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:50:07.322063
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:50:07.357082
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:50:10.266630
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:50:10.282757
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
```

```
No Match in Event ID List
This event was created on:  2019-07-19 14:50:10.295725
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:50:10.324831
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:50:13.109148
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:50:13.127594
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:50:13.153168
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:50:13.185015
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:50:14.678185
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:50:14.692289
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:50:14.716040
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:50:14.827320
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:50:17.941637
```

```
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:50:17.963903
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:50:17.990891
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:50:18.009563
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:50:19.467476
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:50:19.491238
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:50:19.516949
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:50:19.549320
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:50:25.376030
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:50:50.046476
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:50:50.086594
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
```

```
This event was created on:  2019-07-19 14:50:53.011280
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:50:53.062635
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:50:55.991997
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:50:56.047770
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:50:56.182989
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:06.728088
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:06.753239
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:06.888029
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:09.823311
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:09.845415
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:22.314203
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
```

```
No Match in Event ID List
This event was created on:  2019-07-19 14:51:22.333687
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:34.797834
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:35.014759
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:35.038553
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:35.579746
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:35.988890
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:36.549351
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:37.034212
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:37.513802
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:38.020924
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:38.517290
```

```
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:39.028528
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:39.537548
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:40.027416
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:40.431643
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:41.066183
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:41.408155
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:41.894760
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:42.466303
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:43.036823
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:43.503725
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
```

```
This event was created on:  2019-07-19 14:51:44.030207
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:44.507586
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:45.011023
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:45.501104
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:46.007996
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:46.500643
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:47.022478
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:47.546213
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:48.044107
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:48.507061
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:49.010847
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
```

```
No Match in Event ID List
This event was created on:  2019-07-19 14:51:49.550571
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:50.021860
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:50.507309
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:51.013865
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:51.520525
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:52.008684
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:52.448023
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:53.019661
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:53.546070
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:54.036268
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:54.581396
```

```
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:55.015097
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:55.552895
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:56.049780
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:56.534039
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:57.034578
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:57.558979
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:58.020845
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:58.457253
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:59.001038
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:51:59.537445
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
```

```
This event was created on:  2019-07-19 14:52:00.063263
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:00.515358
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:00.940746
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:01.546532
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:02.018354
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:02.565195
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:03.059986
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:03.520267
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:04.024998
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:04.522070
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:05.036474
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
```

```
No Match in Event ID List
This event was created on:  2019-07-19 14:52:05.516287
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:06.019043
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:06.440338
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:07.053555
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:07.413017
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:08.043890
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:08.500980
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:09.012394
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:09.474607
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:10.014662
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:10.522083
```

```
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:11.031391
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:11.504766
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:12.023792
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:12.547001
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:13.030186
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:13.489719
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:14.036343
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:14.552206
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:15.051989
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:15.548891
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
```

```
This event was created on:  2019-07-19 14:52:16.040836
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:16.584660
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:17.041742
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:17.511280
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:18.015717
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:18.509474
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:18.990812
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:19.541967
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:20.006071
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:20.543625
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:21.036354
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
```

```
No Match in Event ID List
This event was created on:  2019-07-19 14:52:21.488548
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:22.030117
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:22.542713
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:23.037136
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:23.534355
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:24.026848
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:24.521357
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:25.035419
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:25.529053
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:26.007576
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:26.534525
```

```
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:27.040676
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:27.493847
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:28.017254
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:28.537739
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:29.110739
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:29.561041
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:30.054688
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:30.526930
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:31.015533
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:31.476374
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
```

```
This event was created on:  2019-07-19 14:52:32.005405
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:32.515755
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:33.004824
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:33.515261
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:33.900604
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:34.490131
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:35.031006
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:35.411333
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:35.999052
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:36.510406
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:36.905558
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
```

```
No Match in Event ID List
This event was created on:  2019-07-19 14:52:37.449512
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:37.947397
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:38.514036
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:38.992107
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:39.508768
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:40.034157
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:40.520117
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:40.960737
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:41.512133
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:41.967752
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:42.436453
```

```
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:42.881147
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:43.478228
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:43.951490
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:44.408569
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:44.926708
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:45.532341
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:45.970699
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:46.405594
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:46.879627
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:47.411270
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
```

```
This event was created on:  2019-07-19 14:52:47.993061
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:48.567659
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:49.026358
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:49.408182
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:50.047132
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:50.521467
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:51.038097
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:51.517311
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:52.009583
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:52.553984
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:53.037943
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
```

```
No Match in Event ID List
This event was created on:  2019-07-19 14:52:53.555449
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:54.026604
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:54.529327
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:54.999069
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:55.533232
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:56.017145
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:56.507835
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:57.003769
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:57.544210
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:58.011660
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:58.563175
```

```
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:59.016718
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:52:59.522314
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:00.077917
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:00.621782
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:01.018412
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:01.515442
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:02.019558
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:02.556423
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:03.031588
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:03.557358
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
```

```
This event was created on:  2019-07-19 14:53:04.044834
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:04.539310
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:05.023798
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:05.517408
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:06.023037
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:06.535011
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:07.047480
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:07.533779
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:07.912922
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:08.521156
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:09.042999
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
```

```
No Match in Event ID List
This event was created on:  2019-07-19 14:53:09.515224
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:10.036308
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:10.556026
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:11.022720
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:11.504023
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:12.040415
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:12.537703
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:13.022730
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:13.509249
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:14.020058
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:14.513998
```

```
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:15.001936
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:15.518183
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:16.026970
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:16.521608
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:17.037718
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:17.438835
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:18.043760
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:18.544506
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:19.012392
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:19.546167
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
```

```
This event was created on:  2019-07-19 14:53:20.009003
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:20.571709
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:21.020943
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:21.520859
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:22.035442
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:22.520782
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:23.011339
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:23.546013
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:23.993414
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:24.504868
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:25.008133
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
```

```
No Match in Event ID List
This event was created on:  2019-07-19 14:53:25.544561
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:26.004364
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:26.430801
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:27.009926
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:27.555029
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:28.035648
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:28.511669
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:29.009975
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:29.534903
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:30.034506
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:30.521002
```

```
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:31.013359
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:31.530607
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:32.058762
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:32.614765
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:33.018881
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:33.548567
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:34.005413
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:34.556141
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:35.024666
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:35.559595
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
```

```
This event was created on:  2019-07-19 14:53:36.025921
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:36.536600
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:37.012815
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:37.505228
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:38.043577
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:38.588993
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:39.024685
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:39.518484
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:40.006783
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:40.535082
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:40.982571
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
```

```
No Match in Event ID List
This event was created on:  2019-07-19 14:53:41.530684
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:42.061924
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:42.276409
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:42.301844
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:42.404356
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:42.815966
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:42.841951
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:42.964348
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:43.445040
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:43.574379
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:44.026062
```

```
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:44.054071
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:44.117123
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:45.157639
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:46.204885
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:46.565529
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:46.589405
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:46.848703
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:46.893188
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:46.975168
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:47.083069
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
```

```
This event was created on:  2019-07-19 14:53:47.239317
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:54.976854
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:53:55.018274
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:54:01.925833
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:54:01.955256
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:54:16.782667
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:54:16.830061
An Event ID: 19, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:54:57.044624
An Event ID: 20, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:54:58.819105
An Event ID: 21, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:57:02.378479
An Event ID: 21, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:57:02.806044
An Event ID: 20, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
```

```
No Match in Event ID List
This event was created on:  2019-07-19 14:57:02.895491
An Event ID: 19, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:57:02.977165
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:57:03.235828
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:57:03.309488
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:57:03.961277
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:57:03.974754
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:57:04.210562
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:57:04.270645
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:57:04.294575
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:57:04.333864
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:57:04.361120
```

```
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:57:04.412851
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:57:04.414679
An Event ID: 5, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:57:04.600397
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:57:04.643015
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:57:14.715973
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:57:14.758535
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:57:14.944277
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:57:14.991615
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:57:15.776993
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:57:16.496456
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
```

```
This event was created on:  2019-07-19 14:57:16.552097
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:57:44.283188
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:57:46.073650
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:57:46.094355
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:57:46.207201
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:57:46.422426
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:57:46.459732
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:57:46.608480
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:57:46.640160
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:57:46.828722
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:57:46.849871
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
```

```
No Match in Event ID List
This event was created on:  2019-07-19 14:57:46.927288
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:57:47.218346
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:57:47.238554
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:57:50.398445
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:57:50.453840
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:57:52.923611
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:57:52.982725
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:57:53.882435
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:57:54.099318
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:57:54.129841
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:57:54.165319
```

```
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:57:55.069080
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:57:55.138824
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:57:55.236765
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 14:57:58.359020
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 15:09:40.973074
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 15:09:43.329082
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 15:09:59.931135
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 15:10:52.700901
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 15:11:07.994501
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 15:11:08.184715
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
```

```
This event was created on:  2019-07-19 15:11:16.487989
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 15:11:16.986675
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 15:11:17.027187
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 15:11:17.107912
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 15:11:17.149273
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 15:11:17.224751
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 15:11:17.243643
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 15:11:21.090401
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 15:11:21.105495
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 15:11:23.317303
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 15:11:23.336763
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
```

```
No Match in Event ID List
This event was created on:  2019-07-19 15:11:26.549875
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 15:11:26.642464
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 15:11:26.686584
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 15:11:26.852818
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 15:11:26.884594
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 15:11:26.971596
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 15:11:26.989143
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 15:11:27.082079
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 15:11:27.169216
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 15:11:27.202862
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 15:11:27.233257
```

```
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 15:11:27.258253
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 15:11:50.764090
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/PanacheSys
mon_vs_AtomicRedTeam01.xml
No Match in Event ID List
This event was created on:  2019-07-19 15:12:05.755598
An Event ID: 1116, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/WinDefende
r_Events_1117_1116_AtomicRedTeam.xml
No Match in Event ID List
This event was created on:  2019-07-18 20:40:00.730675
An Event ID: 1116, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/WinDefende
r_Events_1117_1116_AtomicRedTeam.xml
No Match in Event ID List
This event was created on:  2019-07-18 20:40:16.396421
An Event ID: 1116, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/WinDefende
r_Events_1117_1116_AtomicRedTeam.xml
No Match in Event ID List
This event was created on:  2019-07-18 20:41:16.418509
An Event ID: 1116, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/WinDefende
r_Events_1117_1116_AtomicRedTeam.xml
No Match in Event ID List
This event was created on:  2019-07-18 20:41:17.508276
An Event ID: 1116, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/WinDefende
r_Events_1117_1116_AtomicRedTeam.xml
No Match in Event ID List
This event was created on:  2019-07-18 20:41:48.236137
An Event ID: 1117, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/WinDefende
r_Events_1117_1116_AtomicRedTeam.xml
No Match in Event ID List
This event was created on:  2019-07-18 20:51:50.275471
An Event ID: 1116, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/WinDefende
r_Events_1117_1116_AtomicRedTeam.xml
No Match in Event ID List
This event was created on:  2019-07-18 20:51:50.798994
An Event ID: 1117, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/WinDefende
r_Events_1117_1116_AtomicRedTeam.xml
No Match in Event ID List
```

```
This event was created on:  2019-07-18 20:53:31.900808
An Event ID: 1117, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/WinDefende
r_Events_1117_1116_AtomicRedTeam.xml
No Match in Event ID List
This event was created on:  2019-07-18 20:53:31.902611
An Event ID: 1117, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/WinDefende
r_Events_1117_1116_AtomicRedTeam.xml
No Match in Event ID List
This event was created on:  2019-07-18 20:53:31.905405
An Event ID: 1117, was found in file
/home/user/CI5235_Coursework/evtx_logs/Automated_Testing_Tools/WinDefende
r_Events_1117_1116_AtomicRedTeam.xml
No Match in Event ID List
This event was created on:  2019-07-18 20:53:31.952568
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_13_1_m
eterpreter_getsystem_NamedPipeImpersonation.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:46:15.199614
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_13_1_m
eterpreter_getsystem_NamedPipeImpersonation.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:46:15.199614
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_13_1_m
eterpreter_getsystem_NamedPipeImpersonation.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:46:15.215239
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_13_1_m
eterpreter_getsystem_NamedPipeImpersonation.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:46:15.246489
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_11_1_7
_uacbypass_cliconfg.xml
No Match in Event ID List
This event was created on:  2019-05-10 13:49:29.586782
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_11_1_7
_uacbypass_cliconfg.xml
No Match in Event ID List
This event was created on:  2019-05-10 13:49:29.789907
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_11_1_7
_uacbypass_cliconfg.xml
No Match in Event ID List
This event was created on:  2019-05-10 13:49:34.946156
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_11_1_7
_uacbypass_cliconfg.xml
```

```
No Match in Event ID List
This event was created on:  2019-05-10 13:49:39.930532
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_11_1_7
_uacbypass_cliconfg.xml
No Match in Event ID List
This event was created on:  2019-05-10 13:49:40.164907
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_11_1_7
_uacbypass_cliconfg.xml
No Match in Event ID List
This event was created on:  2019-05-10 13:49:45.133657
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_11_1_7
_uacbypass_cliconfg.xml
No Match in Event ID List
This event was created on:  2019-05-10 13:49:45.378775
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_11_1_7
_uacbypass_cliconfg.xml
No Match in Event ID List
This event was created on:  2019-05-10 13:49:45.387562
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_11_1_1
5_WScriptBypassUAC.xml
No Match in Event ID List
This event was created on:  2019-05-09 02:52:18.765888
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_11_1_1
5_WScriptBypassUAC.xml
No Match in Event ID List
This event was created on:  2019-05-09 02:52:18.844011
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_11_1_1
5_WScriptBypassUAC.xml
No Match in Event ID List
This event was created on:  2019-05-09 02:52:18.922136
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_11_1_1
5_WScriptBypassUAC.xml
No Match in Event ID List
This event was created on:  2019-05-09 02:52:18.953388
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_11_1_1
5_WScriptBypassUAC.xml
No Match in Event ID List
This event was created on:  2019-05-09 02:52:18.969011
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_11_1_1
5_WScriptBypassUAC.xml
No Match in Event ID List
This event was created on:  2019-05-09 02:52:19.250261
```

```
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_11_1_1
5_WScriptBypassUAC.xml
No Match in Event ID List
This event was created on:  2019-05-09 02:52:21.250261
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_11_1_1
5_WScriptBypassUAC.xml
No Match in Event ID List
This event was created on:  2019-05-09 02:52:21.265888
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_11_1_1
5_WScriptBypassUAC.xml
No Match in Event ID List
This event was created on:  2019-05-09 02:52:21.281513
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_11_1_1
5_WScriptBypassUAC.xml
No Match in Event ID List
This event was created on:  2019-05-09 02:52:21.297136
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_11_1_1
5_WScriptBypassUAC.xml
No Match in Event ID List
This event was created on:  2019-05-09 02:52:21.594011
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_11_1_1
5_WScriptBypassUAC.xml
No Match in Event ID List
This event was created on:  2019-05-09 02:52:23.500261
An Event ID: 15, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_11_1_1
5_WScriptBypassUAC.xml
No Match in Event ID List
This event was created on:  2019-05-09 02:52:23.500261
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_11_1_1
5_WScriptBypassUAC.xml
No Match in Event ID List
This event was created on:  2019-05-09 02:52:23.500261
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_11_1_1
5_WScriptBypassUAC.xml
No Match in Event ID List
This event was created on:  2019-05-09 02:52:23.531513
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
36_FileCreate.xml
No Match in Event ID List
This event was created on:  2019-08-03 12:32:34.577608
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
36_FileCreate.xml
No Match in Event ID List
```

```
This event was created on:  2019-08-03 12:32:34.875975
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
36_FileCreate.xml
No Match in Event ID List
This event was created on:  2019-08-03 12:32:35.085976
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
36_FileCreate.xml
No Match in Event ID List
This event was created on:  2019-08-03 12:32:35.137611
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
36_FileCreate.xml
No Match in Event ID List
This event was created on:  2019-08-03 12:32:35.531645
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
36_FileCreate.xml
No Match in Event ID List
This event was created on:  2019-08-03 12:32:36.794792
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
36_FileCreate.xml
No Match in Event ID List
This event was created on:  2019-08-03 12:32:36.812510
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
36_FileCreate.xml
No Match in Event ID List
This event was created on:  2019-08-03 12:32:37.160948
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
36_FileCreate.xml
No Match in Event ID List
This event was created on:  2019-08-03 12:32:37.184555
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
36_FileCreate.xml
No Match in Event ID List
This event was created on:  2019-08-03 12:32:37.261044
An Event ID: 5, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
36_FileCreate.xml
No Match in Event ID List
This event was created on:  2019-08-03 12:32:38.640202
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
36_FileCreate.xml
No Match in Event ID List
This event was created on:  2019-08-03 12:32:49.013517
An Event ID: 5, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
36_FileCreate.xml
```

```
No Match in Event ID List
This event was created on:  2019-08-03 12:32:49.525843
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
43.xml
No Match in Event ID List
This event was created on:  2019-08-04 07:26:33.984755
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
43.xml
No Match in Event ID List
This event was created on:  2019-08-04 07:26:34.302721
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
43.xml
No Match in Event ID List
This event was created on:  2019-08-04 07:26:34.689747
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
43.xml
No Match in Event ID List
This event was created on:  2019-08-04 07:26:35.182896
An Event ID: 5, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
43.xml
No Match in Event ID List
This event was created on:  2019-08-04 07:26:36.239723
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
37_FileCreate.xml
No Match in Event ID List
This event was created on:  2019-08-03 12:31:14.789736
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
37_FileCreate.xml
No Match in Event ID List
This event was created on:  2019-08-03 12:31:15.096243
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
37_FileCreate.xml
No Match in Event ID List
This event was created on:  2019-08-03 12:31:15.354147
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
37_FileCreate.xml
No Match in Event ID List
This event was created on:  2019-08-03 12:31:15.364929
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
37_FileCreate.xml
No Match in Event ID List
This event was created on:  2019-08-03 12:31:15.779749
```

```
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
37_FileCreate.xml
No Match in Event ID List
This event was created on:  2019-08-03 12:31:27.049698
An Event ID: 5, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
37_FileCreate.xml
No Match in Event ID List
This event was created on:  2019-08-03 12:31:27.683760
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
22.xml
No Match in Event ID List
This event was created on:  2019-08-03 12:08:13.636089
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
22.xml
No Match in Event ID List
This event was created on:  2019-08-03 12:08:13.818382
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
22.xml
No Match in Event ID List
This event was created on:  2019-08-03 12:08:13.874887
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
22.xml
No Match in Event ID List
This event was created on:  2019-08-03 12:08:14.372734
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
22.xml
No Match in Event ID List
This event was created on:  2019-08-03 12:08:14.977322
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
22.xml
No Match in Event ID List
This event was created on:  2019-08-03 12:08:15.664608
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
22.xml
No Match in Event ID List
This event was created on:  2019-08-03 12:08:16.721581
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
22.xml
No Match in Event ID List
This event was created on:  2019-08-03 12:08:16.753775
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
22.xml
No Match in Event ID List
```

```
This event was created on:  2019-08-03 12:08:16.853764
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
22.xml
No Match in Event ID List
This event was created on:  2019-08-03 12:08:19.888069
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
22.xml
No Match in Event ID List
This event was created on:  2019-08-03 12:08:19.915119
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
22.xml
No Match in Event ID List
This event was created on:  2019-08-03 12:08:20.731415
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
22.xml
No Match in Event ID List
This event was created on:  2019-08-03 12:08:21.128265
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
22.xml
No Match in Event ID List
This event was created on:  2019-08-03 12:08:21.954596
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
22.xml
No Match in Event ID List
This event was created on:  2019-08-03 12:08:23.524313
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
22.xml
No Match in Event ID List
This event was created on:  2019-08-03 12:08:23.554777
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
22.xml
No Match in Event ID List
This event was created on:  2019-08-03 12:08:23.555174
An Event ID: 5, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
22.xml
No Match in Event ID List
This event was created on:  2019-08-03 12:08:25.165592
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
22.xml
No Match in Event ID List
This event was created on:  2019-08-03 12:08:55.408920
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_11_7_1
_uacbypass_windirectory_mocking.xml
```

```
No Match in Event ID List
This event was created on:  2019-07-27 22:43:41.424255
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_11_7_1
_uacbypass_windirectory_mocking.xml
No Match in Event ID List
This event was created on:  2019-07-27 22:43:41.755255
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_11_7_1
_uacbypass_windirectory_mocking.xml
No Match in Event ID List
This event was created on:  2019-07-27 22:43:41.755405
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_11_7_1
_uacbypass_windirectory_mocking.xml
No Match in Event ID List
This event was created on:  2019-07-27 22:43:41.757215
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_11_7_1
_uacbypass_windirectory_mocking.xml
No Match in Event ID List
This event was created on:  2019-07-27 22:43:42.033041
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_11_7_1
_uacbypass_windirectory_mocking.xml
No Match in Event ID List
This event was created on:  2019-07-27 22:43:42.033421
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_11_7_1
_uacbypass_windirectory_mocking.xml
No Match in Event ID List
This event was created on:  2019-07-27 22:43:42.161810
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_11_7_1
_uacbypass_windirectory_mocking.xml
No Match in Event ID List
This event was created on:  2019-07-27 22:43:42.392879
An Event ID: 5, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_11_7_1
_uacbypass_windirectory_mocking.xml
No Match in Event ID List
This event was created on:  2019-07-27 22:43:42.938087
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_11_7_1
_uacbypass_windirectory_mocking.xml
No Match in Event ID List
This event was created on:  2019-07-27 22:43:43.016956
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
39.xml
No Match in Event ID List
This event was created on:  2019-08-03 15:08:06.262501
```

```
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
39.xml
No Match in Event ID List
This event was created on:  2019-08-03 15:08:06.419321
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
39.xml
No Match in Event ID List
This event was created on:  2019-08-03 15:08:06.730202
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
39.xml
No Match in Event ID List
This event was created on:  2019-08-03 15:08:06.796976
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
39.xml
No Match in Event ID List
This event was created on:  2019-08-03 15:08:07.144865
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
39.xml
No Match in Event ID List
This event was created on:  2019-08-03 15:08:07.508961
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
39.xml
No Match in Event ID List
This event was created on:  2019-08-03 15:08:07.558918
An Event ID: 1102, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/security_4624
_4673_token_manip.xml
Matched in Event ID List
This event was created on:  2019-05-11 17:10:06.342443
An Event ID: 4688, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/security_4624
_4673_token_manip.xml
Matched in Event ID List
This event was created on:  2019-05-11 17:10:10.342443
An Event ID: 4688, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/security_4624
_4673_token_manip.xml
Matched in Event ID List
This event was created on:  2019-05-11 17:10:10.608070
An Event ID: 4688, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/security_4624
_4673_token_manip.xml
Matched in Event ID List
This event was created on:  2019-05-11 17:10:10.623695
An Event ID: 4611, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/security_4624
_4673_token_manip.xml
Matched in Event ID List
```

```
This event was created on:  2019-05-11 17:10:10.654945
An Event ID: 4673, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/security_4624
_4673_token_manip.xml
Matched in Event ID List
This event was created on:  2019-05-11 17:10:10.654945
An Event ID: 4688, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/security_4624
_4673_token_manip.xml
Matched in Event ID List
This event was created on:  2019-05-11 17:10:10.748695
An Event ID: 4611, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/security_4624
_4673_token_manip.xml
Matched in Event ID List
This event was created on:  2019-05-11 17:10:10.795570
An Event ID: 4673, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/security_4624
_4673_token_manip.xml
Matched in Event ID List
This event was created on:  2019-05-11 17:10:10.795570
An Event ID: 4688, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/security_4624
_4673_token_manip.xml
Matched in Event ID List
This event was created on:  2019-05-11 17:10:10.795570
An Event ID: 4688, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/security_4624
_4673_token_manip.xml
Matched in Event ID List
This event was created on:  2019-05-11 17:10:10.826820
An Event ID: 4624, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/security_4624
_4673_token_manip.xml
Matched in Event ID List
This event was created on:  2019-05-11 17:10:10.889318
An Event ID: 4688, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/security_4624
_4673_token_manip.xml
Matched in Event ID List
This event was created on:  2019-05-11 17:10:10.889318
An Event ID: 4688, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/security_4624
_4673_token_manip.xml
Matched in Event ID List
This event was created on:  2019-05-11 17:10:10.904945
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
23.xml
No Match in Event ID List
This event was created on:  2019-08-03 12:06:53.680435
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
23.xml
```

```
No Match in Event ID List
This event was created on:  2019-08-03 12:06:53.933989
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
23.xml
No Match in Event ID List
This event was created on:  2019-08-03 12:06:53.943771
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
23.xml
No Match in Event ID List
This event was created on:  2019-08-03 12:06:54.900549
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
23.xml
No Match in Event ID List
This event was created on:  2019-08-03 12:06:54.972195
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
23.xml
No Match in Event ID List
This event was created on:  2019-08-03 12:06:55.455099
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
23.xml
No Match in Event ID List
This event was created on:  2019-08-03 12:06:55.620600
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
23.xml
No Match in Event ID List
This event was created on:  2019-08-03 12:06:55.820406
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_13_1_U
ACBypass_SDCLTBypass.xml
No Match in Event ID List
This event was created on:  2019-05-09 02:07:51.116072
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_13_1_U
ACBypass_SDCLTBypass.xml
No Match in Event ID List
This event was created on:  2019-05-09 02:07:51.131697
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_13_1_U
ACBypass_SDCLTBypass.xml
No Match in Event ID List
This event was created on:  2019-05-09 02:07:51.131697
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_13_1_U
ACBypass_SDCLTBypass.xml
No Match in Event ID List
This event was created on:  2019-05-09 02:07:56.149275
```

```
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_13_1_U
ACBypass_SDCLTBypass.xml
No Match in Event ID List
This event was created on:  2019-05-09 02:08:00.446150
An Event ID: 4624, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Invoke_TokenD
uplication_UAC_Bypass4624.xml
Matched in Event ID List
This event was created on:  2019-08-05 09:39:30.697731
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
33.xml
No Match in Event ID List
This event was created on:  2019-08-03 10:14:02.589464
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
33.xml
No Match in Event ID List
This event was created on:  2019-08-03 10:14:02.929209
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
33.xml
No Match in Event ID List
This event was created on:  2019-08-03 10:14:02.934826
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
33.xml
No Match in Event ID List
This event was created on:  2019-08-03 10:14:07.652988
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
33.xml
No Match in Event ID List
This event was created on:  2019-08-03 10:14:07.665552
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
33.xml
No Match in Event ID List
This event was created on:  2019-08-03 10:14:08.065273
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
33.xml
No Match in Event ID List
This event was created on:  2019-08-03 10:14:08.472101
An Event ID: 12, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
33.xml
No Match in Event ID List
This event was created on:  2019-08-03 10:14:08.681362
An Event ID: 5, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
33.xml
No Match in Event ID List
```

```
This event was created on:  2019-08-03 10:14:08.799778
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_7_el
evate_uacbypass_sysprep.xml
No Match in Event ID List
This event was created on:  2019-05-14 02:32:48.290682
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_7_el
evate_uacbypass_sysprep.xml
No Match in Event ID List
This event was created on:  2019-05-14 02:32:48.290682
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_7_el
evate_uacbypass_sysprep.xml
No Match in Event ID List
This event was created on:  2019-05-14 02:32:48.359432
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_7_el
evate_uacbypass_sysprep.xml
No Match in Event ID List
This event was created on:  2019-05-14 02:32:48.359432
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_7_el
evate_uacbypass_sysprep.xml
No Match in Event ID List
This event was created on:  2019-05-14 02:32:51.143806
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_7_el
evate_uacbypass_sysprep.xml
No Match in Event ID List
This event was created on:  2019-05-14 02:32:51.453182
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_7_el
evate_uacbypass_sysprep.xml
No Match in Event ID List
This event was created on:  2019-05-14 02:32:51.453182
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_7_el
evate_uacbypass_sysprep.xml
No Match in Event ID List
This event was created on:  2019-05-14 02:32:51.470369
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_7_el
evate_uacbypass_sysprep.xml
No Match in Event ID List
This event was created on:  2019-05-14 02:32:51.470369
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_7_el
evate_uacbypass_sysprep.xml
No Match in Event ID List
This event was created on:  2019-05-14 02:32:51.487556
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_7_el
evate_uacbypass_sysprep.xml
```

```
No Match in Event ID List
This event was created on:  2019-05-14 02:32:51.487556
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_7_el
evate_uacbypass_sysprep.xml
No Match in Event ID List
This event was created on:  2019-05-14 02:32:51.487556
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_7_el
evate_uacbypass_sysprep.xml
No Match in Event ID List
This event was created on:  2019-05-14 02:32:51.814119
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_7_el
evate_uacbypass_sysprep.xml
No Match in Event ID List
This event was created on:  2019-05-14 02:32:51.831306
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_7_el
evate_uacbypass_sysprep.xml
No Match in Event ID List
This event was created on:  2019-05-14 02:32:51.831306
An Event ID: 4703, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/win10_4703_Se
DebugPrivilege_enabled.xml
Matched in Event ID List
This event was created on:  2019-08-14 12:48:15.921507
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_7_11
_sysprep_uacbypass.xml
No Match in Event ID List
This event was created on:  2019-05-11 16:54:02.071392
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_7_11
_sysprep_uacbypass.xml
No Match in Event ID List
This event was created on:  2019-05-11 16:54:02.305765
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_7_11
_sysprep_uacbypass.xml
No Match in Event ID List
This event was created on:  2019-05-11 16:54:07.508890
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_7_11
_sysprep_uacbypass.xml
No Match in Event ID List
This event was created on:  2019-05-11 16:54:07.524517
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_7_11
_sysprep_uacbypass.xml
No Match in Event ID List
This event was created on:  2019-05-11 16:54:12.493267
```

```
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_7_11
_sysprep_uacbypass.xml
No Match in Event ID List
This event was created on:  2019-05-11 16:54:12.821392
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_7_11
_sysprep_uacbypass.xml
No Match in Event ID List
This event was created on:  2019-05-11 16:54:18.069437
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
30.xml
No Match in Event ID List
This event was created on:  2019-08-03 11:23:15.364738
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
30.xml
No Match in Event ID List
This event was created on:  2019-08-03 11:23:15.560614
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
30.xml
No Match in Event ID List
This event was created on:  2019-08-03 11:23:15.579857
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
30.xml
No Match in Event ID List
This event was created on:  2019-08-03 11:23:17.433718
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
30.xml
No Match in Event ID List
This event was created on:  2019-08-03 11:23:17.541143
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
30.xml
No Match in Event ID List
This event was created on:  2019-08-03 11:23:18.619446
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
30.xml
No Match in Event ID List
This event was created on:  2019-08-03 11:23:18.666714
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
30.xml
No Match in Event ID List
This event was created on:  2019-08-03 11:23:18.694576
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
30.xml
No Match in Event ID List
```

```
This event was created on:  2019-08-03 11:23:18.715586
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
30.xml
No Match in Event ID List
This event was created on:  2019-08-03 11:23:18.803791
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
30.xml
No Match in Event ID List
This event was created on:  2019-08-03 11:23:18.824713
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_prives
c_from_admin_to_system_handle_inheritance.xml
No Match in Event ID List
This event was created on:  2019-05-11 18:10:42.434408
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_prives
c_from_admin_to_system_handle_inheritance.xml
No Match in Event ID List
This event was created on:  2019-05-11 18:10:42.637533
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_prives
c_from_admin_to_system_handle_inheritance.xml
No Match in Event ID List
This event was created on:  2019-05-11 18:10:42.668783
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/privesc_rotte
n_potato_from_webshell_metasploit_sysmon_1_8_3.xml
No Match in Event ID List
This event was created on:  2019-05-26 15:47:56.667118
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/privesc_rotte
n_potato_from_webshell_metasploit_sysmon_1_8_3.xml
No Match in Event ID List
This event was created on:  2019-05-26 15:47:56.667118
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/privesc_rotte
n_potato_from_webshell_metasploit_sysmon_1_8_3.xml
No Match in Event ID List
This event was created on:  2019-05-26 15:47:56.727203
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/privesc_rotte
n_potato_from_webshell_metasploit_sysmon_1_8_3.xml
No Match in Event ID List
This event was created on:  2019-05-26 15:47:57.628500
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/privesc_rotte
n_potato_from_webshell_metasploit_sysmon_1_8_3.xml
No Match in Event ID List
This event was created on:  2019-05-26 15:47:58.830229
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/privesc_rotte
n_potato_from_webshell_metasploit_sysmon_1_8_3.xml
```

```
No Match in Event ID List
This event was created on:  2019-05-26 15:47:58.830229
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/privesc_rotte
n_potato_from_webshell_metasploit_sysmon_1_8_3.xml
No Match in Event ID List
This event was created on:  2019-05-26 15:47:59.871725
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/privesc_rotte
n_potato_from_webshell_metasploit_sysmon_1_8_3.xml
No Match in Event ID List
This event was created on:  2019-05-26 15:47:59.871725
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/privesc_rotte
n_potato_from_webshell_metasploit_sysmon_1_8_3.xml
No Match in Event ID List
This event was created on:  2019-05-26 15:48:00.732964
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/privesc_rotte
n_potato_from_webshell_metasploit_sysmon_1_8_3.xml
No Match in Event ID List
This event was created on:  2019-05-26 15:48:00.732964
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/privesc_rotte
n_potato_from_webshell_metasploit_sysmon_1_8_3.xml
No Match in Event ID List
This event was created on:  2019-05-26 15:48:00.752993
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/privesc_rotte
n_potato_from_webshell_metasploit_sysmon_1_8_3.xml
No Match in Event ID List
This event was created on:  2019-05-26 15:48:00.752993
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/privesc_rotte
n_potato_from_webshell_metasploit_sysmon_1_8_3.xml
No Match in Event ID List
This event was created on:  2019-05-26 15:48:01.864592
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_13_1_1
2_11_perfmonUACBypass.xml
No Match in Event ID List
This event was created on:  2019-05-10 12:21:57.077543
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_13_1_1
2_11_perfmonUACBypass.xml
No Match in Event ID List
This event was created on:  2019-05-10 12:21:57.286667
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_13_1_1
2_11_perfmonUACBypass.xml
No Match in Event ID List
This event was created on:  2019-05-10 12:22:02.434315
```

```
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_13_1_1
2_11_perfmonUACBypass.xml
No Match in Event ID List
This event was created on:  2019-05-10 12:22:08.465096
An Event ID: 12, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_13_1_1
2_11_perfmonUACBypass.xml
No Match in Event ID List
This event was created on:  2019-05-10 12:22:13.897461
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_7_11
_mcx2prov_uacbypass.xml
No Match in Event ID List
This event was created on:  2019-05-11 09:50:08.248989
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_7_11
_mcx2prov_uacbypass.xml
No Match in Event ID List
This event was created on:  2019-05-11 09:50:08.491568
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_7_11
_mcx2prov_uacbypass.xml
No Match in Event ID List
This event was created on:  2019-05-11 09:50:13.494730
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_7_11
_mcx2prov_uacbypass.xml
No Match in Event ID List
This event was created on:  2019-05-11 09:50:13.509892
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_7_11
_mcx2prov_uacbypass.xml
No Match in Event ID List
This event was created on:  2019-05-11 09:50:18.404903
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_7_11
_mcx2prov_uacbypass.xml
No Match in Event ID List
This event was created on:  2019-05-11 09:50:18.654903
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_7_11
_mcx2prov_uacbypass.xml
No Match in Event ID List
This event was created on:  2019-05-11 09:50:26.779903
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_7_11
_mcx2prov_uacbypass.xml
No Match in Event ID List
This event was created on:  2019-05-11 09:50:27.018183
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_7_11
_mcx2prov_uacbypass.xml
No Match in Event ID List
```

```
This event was created on:  2019-05-11 09:50:27.030880
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_7_11
_migwiz.xml
No Match in Event ID List
This event was created on:  2019-05-11 16:46:10.125532
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_7_11
_migwiz.xml
No Match in Event ID List
This event was created on:  2019-05-11 16:46:10.344282
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_7_11
_migwiz.xml
No Match in Event ID List
This event was created on:  2019-05-11 16:46:15.500532
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_7_11
_migwiz.xml
No Match in Event ID List
This event was created on:  2019-05-11 16:46:15.547407
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_7_11
_migwiz.xml
No Match in Event ID List
This event was created on:  2019-05-11 16:46:20.531782
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_7_11
_migwiz.xml
No Match in Event ID List
This event was created on:  2019-05-11 16:46:20.828657
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_7_11
_migwiz.xml
No Match in Event ID List
This event was created on:  2019-05-11 16:46:26.203657
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
32.xml
No Match in Event ID List
This event was created on:  2019-08-03 10:51:46.511812
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
32.xml
No Match in Event ID List
This event was created on:  2019-08-03 10:51:46.647421
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
32.xml
No Match in Event ID List
This event was created on:  2019-08-03 10:51:46.685993
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
32.xml
```

```
No Match in Event ID List
This event was created on:  2019-08-03 10:51:47.219517
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
32.xml
No Match in Event ID List
This event was created on:  2019-08-03 10:51:48.431273
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
32.xml
No Match in Event ID List
This event was created on:  2019-08-03 10:51:48.675629
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
32.xml
No Match in Event ID List
This event was created on:  2019-08-03 10:51:48.696407
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
32.xml
No Match in Event ID List
This event was created on:  2019-08-03 10:51:49.371552
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_11_e
xec_as_system_via_schedtask.xml
No Match in Event ID List
This event was created on:  2019-05-12 00:32:24.461386
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_11_e
xec_as_system_via_schedtask.xml
No Match in Event ID List
This event was created on:  2019-05-12 00:32:30.211386
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_11_e
xec_as_system_via_schedtask.xml
No Match in Event ID List
This event was created on:  2019-05-12 00:32:30.227013
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_11_e
xec_as_system_via_schedtask.xml
No Match in Event ID List
This event was created on:  2019-05-12 00:32:35.258263
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_11_e
xec_as_system_via_schedtask.xml
No Match in Event ID List
This event was created on:  2019-05-12 00:32:35.352013
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_11_e
xec_as_system_via_schedtask.xml
No Match in Event ID List
This event was created on:  2019-05-12 00:32:40.342245
```

```
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
56.xml
No Match in Event ID List
This event was created on:  2019-08-04 10:16:29.676336
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
56.xml
No Match in Event ID List
This event was created on:  2019-08-04 10:16:31.175295
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
56.xml
No Match in Event ID List
This event was created on:  2019-08-04 10:16:31.476803
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
56.xml
No Match in Event ID List
This event was created on:  2019-08-04 10:16:31.485931
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
56.xml
No Match in Event ID List
This event was created on:  2019-08-04 10:16:31.609571
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
56.xml
No Match in Event ID List
This event was created on:  2019-08-04 10:16:31.949078
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
56.xml
No Match in Event ID List
This event was created on:  2019-08-04 10:16:32.001791
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
56.xml
No Match in Event ID List
This event was created on:  2019-08-04 10:16:32.438711
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
56.xml
No Match in Event ID List
This event was created on:  2019-08-04 10:16:50.009125
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
56.xml
No Match in Event ID List
This event was created on:  2019-08-04 10:16:50.455910
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
56.xml
No Match in Event ID List
```

```
This event was created on:  2019-08-04 10:16:55.299641
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
56.xml
No Match in Event ID List
This event was created on:  2019-08-04 10:16:55.441261
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
56.xml
No Match in Event ID List
This event was created on:  2019-08-04 10:16:55.446480
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
56.xml
No Match in Event ID List
This event was created on:  2019-08-04 10:16:55.643799
An Event ID: 5, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
56.xml
No Match in Event ID List
This event was created on:  2019-08-04 10:16:55.712009
An Event ID: 163847045, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/System_7045_n
amedpipe_privesc.xml
No Match in Event ID List
This event was created on:  2019-05-12 12:52:43.702578
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
45.xml
No Match in Event ID List
This event was created on:  2019-08-04 08:56:16.228363
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
45.xml
No Match in Event ID List
This event was created on:  2019-08-04 08:56:16.650579
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
45.xml
No Match in Event ID List
This event was created on:  2019-08-04 08:56:16.967768
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
45.xml
No Match in Event ID List
This event was created on:  2019-08-04 08:56:18.321764
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
45.xml
No Match in Event ID List
This event was created on:  2019-08-04 08:56:20.446159
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
45.xml
```

```
No Match in Event ID List
This event was created on:  2019-08-04 08:56:20.937952
An Event ID: 12, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
45.xml
No Match in Event ID List
This event was created on:  2019-08-04 08:56:22.193542
An Event ID: 5, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
45.xml
No Match in Event ID List
This event was created on:  2019-08-04 08:56:22.267944
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
54.xml
No Match in Event ID List
This event was created on:  2019-08-04 09:33:57.582769
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
54.xml
No Match in Event ID List
This event was created on:  2019-08-04 09:33:57.800852
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
54.xml
No Match in Event ID List
This event was created on:  2019-08-04 09:33:58.087776
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
54.xml
No Match in Event ID List
This event was created on:  2019-08-04 09:33:58.127146
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
54.xml
No Match in Event ID List
This event was created on:  2019-08-04 09:33:58.713953
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
54.xml
No Match in Event ID List
This event was created on:  2019-08-04 09:33:58.714466
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
54.xml
No Match in Event ID List
This event was created on:  2019-08-04 09:33:58.774477
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
54.xml
No Match in Event ID List
This event was created on:  2019-08-04 09:33:59.225170
```

```
An Event ID: 5, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
54.xml
No Match in Event ID List
This event was created on:  2019-08-04 09:34:00.871325
An Event ID: 5, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
54.xml
No Match in Event ID List
This event was created on:  2019-08-04 09:34:01.014212
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
41.xml
No Match in Event ID List
This event was created on:  2019-08-03 15:16:30.389233
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
41.xml
No Match in Event ID List
This event was created on:  2019-08-03 15:16:31.012035
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
41.xml
No Match in Event ID List
This event was created on:  2019-08-03 15:16:31.779224
An Event ID: 5, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
41.xml
No Match in Event ID List
This event was created on:  2019-08-03 15:16:31.875849
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_13_U
ACBypass_AppPath_Control.xml
No Match in Event ID List
This event was created on:  2019-05-09 03:25:24.630444
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_13_U
ACBypass_AppPath_Control.xml
No Match in Event ID List
This event was created on:  2019-05-09 03:25:24.896070
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_13_U
ACBypass_AppPath_Control.xml
No Match in Event ID List
This event was created on:  2019-05-09 03:25:25.067945
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
53.xml
No Match in Event ID List
This event was created on:  2019-08-04 09:10:28.612995
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
53.xml
No Match in Event ID List
```

```
This event was created on:  2019-08-04 09:10:28.807909
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
53.xml
No Match in Event ID List
This event was created on:  2019-08-04 09:10:28.893192
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
53.xml
No Match in Event ID List
This event was created on:  2019-08-04 09:10:28.925642
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
53.xml
No Match in Event ID List
This event was created on:  2019-08-04 09:10:29.060589
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
53.xml
No Match in Event ID List
This event was created on:  2019-08-04 09:10:29.409803
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
53.xml
No Match in Event ID List
This event was created on:  2019-08-04 09:10:29.431166
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
53.xml
No Match in Event ID List
This event was created on:  2019-08-04 09:10:30.395226
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
53.xml
No Match in Event ID List
This event was created on:  2019-08-04 09:10:30.752831
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
53.xml
No Match in Event ID List
This event was created on:  2019-08-04 09:10:30.972589
An Event ID: 12, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
53.xml
No Match in Event ID List
This event was created on:  2019-08-04 09:10:35.391457
An Event ID: 12, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
53.xml
No Match in Event ID List
This event was created on:  2019-08-04 09:10:35.397312
An Event ID: 12, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
53.xml
```

```
No Match in Event ID List
This event was created on:  2019-08-04 09:10:35.402941
An Event ID: 5, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
53.xml
No Match in Event ID List
This event was created on:  2019-08-04 09:10:35.454962
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
38.xml
No Match in Event ID List
This event was created on:  2019-08-03 13:50:26.614416
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
38.xml
No Match in Event ID List
This event was created on:  2019-08-03 13:50:26.782724
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
38.xml
No Match in Event ID List
This event was created on:  2019-08-03 13:50:27.060244
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
38.xml
No Match in Event ID List
This event was created on:  2019-08-03 13:50:27.356586
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
38.xml
No Match in Event ID List
This event was created on:  2019-08-03 13:50:29.101425
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
38.xml
No Match in Event ID List
This event was created on:  2019-08-03 13:50:29.424082
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
38.xml
No Match in Event ID List
This event was created on:  2019-08-03 13:50:29.459513
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
38.xml
No Match in Event ID List
This event was created on:  2019-08-03 13:50:29.461449
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_13_1_c
ompmgmtlauncherUACBypass.xml
No Match in Event ID List
This event was created on:  2019-05-10 13:32:48.200716
```

```
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_13_1_c
ompmgmtlauncherUACBypass.xml
No Match in Event ID List
This event was created on:  2019-05-10 13:32:48.412971
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_13_1_c
ompmgmtlauncherUACBypass.xml
No Match in Event ID List
This event was created on:  2019-05-10 13:32:58.549885
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_13_1_c
ompmgmtlauncherUACBypass.xml
No Match in Event ID List
This event was created on:  2019-05-10 13:33:29.424885
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
34.xml
No Match in Event ID List
This event was created on:  2019-08-03 09:46:48.209719
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
34.xml
No Match in Event ID List
This event was created on:  2019-08-03 09:46:48.726303
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
34.xml
No Match in Event ID List
This event was created on:  2019-08-03 09:46:48.924856
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
34.xml
No Match in Event ID List
This event was created on:  2019-08-03 09:46:49.402550
An Event ID: 12, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
34.xml
No Match in Event ID List
This event was created on:  2019-08-03 09:46:49.436855
An Event ID: 5, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_UACME_
34.xml
No Match in Event ID List
This event was created on:  2019-08-03 09:46:49.502371
An Event ID: 1102, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/4624 LT3
AnonymousLogon Localhost - JuicyPotato.xml
Matched in Event ID List
This event was created on:  2019-11-15 08:19:02.298512
An Event ID: 4624, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/4624 LT3
AnonymousLogon Localhost - JuicyPotato.xml
Matched in Event ID List
```

```
This event was created on:  2019-11-15 08:19:16.102510
An Event ID: 4634, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/4624 LT3
AnonymousLogon Localhost - JuicyPotato.xml
Matched in Event ID List
This event was created on:  2019-11-15 08:19:17.134468
An Event ID: 4776, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/privexchange_
dirkjan.xml
Matched in Event ID List
This event was created on:  2019-02-02 09:16:52.479004
An Event ID: 4624, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/privexchange_
dirkjan.xml
Matched in Event ID List
This event was created on:  2019-02-02 09:16:58.787262
An Event ID: 4776, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/privexchange_
dirkjan.xml
Matched in Event ID List
This event was created on:  2019-02-02 09:17:22.562534
An Event ID: 4624, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/privexchange_
dirkjan.xml
Matched in Event ID List
This event was created on:  2019-02-02 09:17:22.563017
An Event ID: 4662, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/privexchange_
dirkjan.xml
Matched in Event ID List
This event was created on:  2019-02-02 09:17:23.193672
An Event ID: 4624, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/privexchange_
dirkjan.xml
Matched in Event ID List
This event was created on:  2019-02-02 09:17:23.206182
An Event ID: 5136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/privexchange_
dirkjan.xml
Matched in Event ID List
This event was created on:  2019-02-02 09:17:27.629412
An Event ID: 5136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/privexchange_
dirkjan.xml
Matched in Event ID List
This event was created on:  2019-02-02 09:17:27.629829
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_13_1_U
AC_Bypass_EventVwrBypass.xml
No Match in Event ID List
This event was created on:  2019-05-09 01:59:28.669022
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_13_1_U
AC_Bypass_EventVwrBypass.xml
```

```
No Match in Event ID List
This event was created on:  2019-05-09 01:59:28.684647
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_13_1_U
AC_Bypass_EventVwrBypass.xml
No Match in Event ID List
This event was created on:  2019-05-09 01:59:28.684647
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_13_1_U
AC_Bypass_EventVwrBypass.xml
No Match in Event ID List
This event was created on:  2019-05-09 01:59:28.950272
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_13_1_U
AC_Bypass_EventVwrBypass.xml
No Match in Event ID List
This event was created on:  2019-05-09 01:59:29.090897
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/Sysmon_13_1_U
AC_Bypass_EventVwrBypass.xml
No Match in Event ID List
This event was created on:  2019-05-09 02:00:01.794022
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_13_1
1_cmstp_ini_uacbypass.xml
No Match in Event ID List
This event was created on:  2019-05-11 17:28:17.176430
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_13_1
1_cmstp_ini_uacbypass.xml
No Match in Event ID List
This event was created on:  2019-05-11 17:28:17.363930
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_13_1
1_cmstp_ini_uacbypass.xml
No Match in Event ID List
This event was created on:  2019-05-11 17:28:19.567055
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_13_1
1_cmstp_ini_uacbypass.xml
No Match in Event ID List
This event was created on:  2019-05-11 17:28:22.598305
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Privilege_Escalation/sysmon_1_13_1
1_cmstp_ini_uacbypass.xml
No Match in Event ID List
This event was created on:  2019-05-11 17:28:22.598305
An Event ID: 1102, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:23:37.147709
```

```
An Event ID: 5158, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:23:43.570211
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:23:43.570211
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:23:43.570211
An Event ID: 4672, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:23:43.570211
An Event ID: 4624, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:23:43.570211
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:23:51.772354
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:23:52.491922
An Event ID: 4624, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:23:52.491922
An Event ID: 5140, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:23:52.507387
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
No Match in Event ID List
This event was created on:  2019-03-18 23:23:52.507387
An Event ID: 4661, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
```

```
This event was created on:  2019-03-18 23:23:52.522461
An Event ID: 4661, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:23:52.522461
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
No Match in Event ID List
This event was created on:  2019-03-18 23:23:52.538513
An Event ID: 4661, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:23:52.538513
An Event ID: 4661, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:23:52.538513
An Event ID: 5158, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:23:57.397648
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:23:57.397648
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:23:57.397648
An Event ID: 4672, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:23:57.397648
An Event ID: 4624, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:23:57.397648
An Event ID: 5140, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:23:57.397648
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
```

```
No Match in Event ID List
This event was created on:  2019-03-18 23:23:57.397648
An Event ID: 4661, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:24:07.584864
An Event ID: 5158, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:24:07.601240
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:24:07.601240
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:24:07.601240
An Event ID: 4661, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:24:07.601240
An Event ID: 4661, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:24:07.601240
An Event ID: 5158, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:24:07.615925
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:24:07.615925
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:24:07.615925
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:24:07.772839
```

```
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:24:08.069208
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:24:08.069208
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:24:08.069208
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:24:08.069208
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:24:08.069208
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:24:08.069208
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:24:08.069208
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:24:08.069208
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:24:08.240883
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:24:08.287941
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
```

```
This event was created on:  2019-03-18 23:24:08.320019
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:24:11.085218
An Event ID: 4661, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:24:11.413551
An Event ID: 4661, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:24:11.413551
An Event ID: 4661, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:24:11.413551
An Event ID: 4661, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:24:11.741724
An Event ID: 4661, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:24:11.741724
An Event ID: 4661, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:24:11.741724
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:24:15.631792
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:24:15.647430
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:24:15.647430
An Event ID: 4776, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
```

```
Matched in Event ID List
This event was created on:  2019-03-18 23:24:15.647430
An Event ID: 4661, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:24:15.662977
An Event ID: 4661, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:24:15.662977
An Event ID: 4661, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:24:15.662977
An Event ID: 5158, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:24:20.960030
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:24:20.960030
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:24:20.960030
An Event ID: 4672, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:24:20.960030
An Event ID: 4624, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/dicovery_4661_net_group_
domain_admins_target.xml
Matched in Event ID List
This event was created on:  2019-03-18 23:24:20.960030
An Event ID: 18, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_enum_shares_ta
rget_sysmon_3_18.xml
No Match in Event ID List
This event was created on:  2019-05-14 17:42:52.833387
An Event ID: 18, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_enum_shares_ta
rget_sysmon_3_18.xml
No Match in Event ID List
This event was created on:  2019-05-14 17:42:52.848383
```

```
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_enum_shares_ta
rget_sysmon_3_18.xml
No Match in Event ID List
This event was created on:  2019-05-14 17:42:53.854380
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_enum_shares_ta
rget_sysmon_3_18.xml
No Match in Event ID List
This event was created on:  2019-05-14 17:43:03.888378
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:22:56.571136
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:22:56.930513
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:22:57.149261
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:23:00.883638
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:23:00.899261
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:23:00.899261
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:23:00.899261
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:23:00.899261
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
```

```
This event was created on:  2019-04-30 07:23:00.899261
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:23:00.899261
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:23:00.899261
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:23:00.899261
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:23:00.899261
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:23:00.899261
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:23:00.899261
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:23:00.899261
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:23:00.899261
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:23:00.914886
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:23:00.914886
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
```

```
No Match in Event ID List
This event was created on:  2019-04-30 07:23:00.914886
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:23:00.914886
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:23:00.914886
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:23:00.914886
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:23:00.914886
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:23:00.914886
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:23:00.914886
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:23:00.914886
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:23:00.914886
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:23:00.914886
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:23:00.914886
```

```
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:23:00.914886
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:23:00.914886
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:23:00.914886
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:23:00.914886
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:23:00.914886
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:23:00.914886
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:23:00.914886
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:23:00.914886
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:23:00.914886
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:23:00.914886
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
```

```
This event was created on:  2019-04-30 07:23:00.930513
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:23:00.930513
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:23:00.930513
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:23:00.930513
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:23:00.930513
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:23:00.930513
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:23:00.930513
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:23:00.930513
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:23:00.930513
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:23:00.930513
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:23:00.930513
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_meterpreter_ps
_cmd_process_listing_sysmon_10.xml
```

```
No Match in Event ID List
This event was created on:  2019-04-30 07:23:00.930513
An Event ID: 4798, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_local_user_or_
group_windows_security_4799_4798.xml
Matched in Event ID List
This event was created on:  2019-08-05 09:24:56.740217
An Event ID: 4798, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_local_user_or_
group_windows_security_4799_4798.xml
Matched in Event ID List
This event was created on:  2019-08-05 09:24:56.774258
An Event ID: 4799, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_local_user_or_
group_windows_security_4799_4798.xml
Matched in Event ID List
This event was created on:  2019-08-05 09:25:03.867962
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_sysmon_3_Invok
e_UserHunter_SourceMachine.xml
No Match in Event ID List
This event was created on:  2019-05-14 17:17:26.440651
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_sysmon_3_Invok
e_UserHunter_SourceMachine.xml
No Match in Event ID List
This event was created on:  2019-05-14 17:17:26.738626
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_sysmon_3_Invok
e_UserHunter_SourceMachine.xml
No Match in Event ID List
This event was created on:  2019-05-14 17:17:38.250959
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_sysmon_3_Invok
e_UserHunter_SourceMachine.xml
No Match in Event ID List
This event was created on:  2019-05-14 17:17:38.250959
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_sysmon_3_Invok
e_UserHunter_SourceMachine.xml
No Match in Event ID List
This event was created on:  2019-05-14 17:17:38.250959
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_sysmon_3_Invok
e_UserHunter_SourceMachine.xml
No Match in Event ID List
This event was created on:  2019-05-14 17:17:38.250959
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_sysmon_3_Invok
e_UserHunter_SourceMachine.xml
No Match in Event ID List
This event was created on:  2019-05-14 17:17:38.250959
```

```
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_sysmon_3_Invok
e_UserHunter_SourceMachine.xml
No Match in Event ID List
This event was created on:  2019-05-14 17:17:38.250959
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_sysmon_3_Invok
e_UserHunter_SourceMachine.xml
No Match in Event ID List
This event was created on:  2019-05-14 17:17:38.250959
An Event ID: 18, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_sysmon_18_Invo
ke_UserHunter_NetSessionEnum_DC-srvsvc.xml
No Match in Event ID List
This event was created on:  2019-05-14 17:31:27.973400
An Event ID: 1102, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_bloodhound.xml
Matched in Event ID List
This event was created on:  2019-01-20 07:00:50.800224
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_bloodhound.xml
No Match in Event ID List
This event was created on:  2019-01-20 07:00:56.784849
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_bloodhound.xml
No Match in Event ID List
This event was created on:  2019-01-20 07:01:20.972601
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_bloodhound.xml
No Match in Event ID List
This event was created on:  2019-01-20 07:01:41.206379
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_bloodhound.xml
No Match in Event ID List
This event was created on:  2019-01-20 07:02:45.409321
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_bloodhound.xml
No Match in Event ID List
This event was created on:  2019-01-20 07:02:45.424917
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_bloodhound.xml
No Match in Event ID List
This event was created on:  2019-01-20 07:02:45.440693
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_bloodhound.xml
No Match in Event ID List
This event was created on:  2019-01-20 07:02:45.472383
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_bloodhound.xml
No Match in Event ID List
This event was created on:  2019-01-20 07:02:45.503201
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_bloodhound.xml
No Match in Event ID List
```

```
This event was created on:  2019-01-20 07:02:45.550112
An Event ID: 1102, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_psloggedon.xml
Matched in Event ID List
This event was created on:  2019-01-20 07:29:57.863892
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_psloggedon.xml
No Match in Event ID List
This event was created on:  2019-01-20 07:30:10.645117
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_psloggedon.xml
No Match in Event ID List
This event was created on:  2019-01-20 07:30:10.660099
An Event ID: 5145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Discovery/discovery_psloggedon.xml
No Match in Event ID List
This event was created on:  2019-01-20 07:30:10.660099
An Event ID: 4624, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_4624.xml
Matched in Event ID List
This event was created on:  2019-02-13 15:14:52.409735
An Event ID: 4624, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_4624.xml
Matched in Event ID List
This event was created on:  2019-02-13 15:15:04.175283
An Event ID: 4624, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_4624.xml
Matched in Event ID List
This event was created on:  2019-02-13 15:15:04.635946
An Event ID: 4624, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_4624.xml
Matched in Event ID List
This event was created on:  2019-02-13 15:15:04.911343
An Event ID: 4624, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_4624.xml
Matched in Event ID List
This event was created on:  2019-02-13 15:15:05.065565
An Event ID: 4624, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_4624.xml
Matched in Event ID List
This event was created on:  2019-02-13 15:15:05.660418
An Event ID: 4624, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_4624.xml
Matched in Event ID List
This event was created on:  2019-02-13 15:15:05.924797
```

```
An Event ID: 4624, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_4624.xml
Matched in Event ID List
This event was created on:  2019-02-13 15:15:07.422945
An Event ID: 4624, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_4624.xml
Matched in Event ID List
This event was created on:  2019-02-13 15:15:08.216084
An Event ID: 4624, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_4624.xml
Matched in Event ID List
This event was created on:  2019-02-13 15:15:08.689762
An Event ID: 4624, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_4624.xml
Matched in Event ID List
This event was created on:  2019-02-13 15:15:36.367607
An Event ID: 4624, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_4624.xml
Matched in Event ID List
This event was created on:  2019-02-13 15:17:38.018242
An Event ID: 4624, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_4624.xml
Matched in Event ID List
This event was created on:  2019-02-13 15:17:38.779337
An Event ID: 4624, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_4624.xml
Matched in Event ID List
This event was created on:  2019-02-13 15:19:51.259834
An Event ID: 4624, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_4624.xml
Matched in Event ID List
This event was created on:  2019-02-13 15:26:53.356781
An Event ID: 4624, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_4624.xml
Matched in Event ID List
This event was created on:  2019-02-13 15:29:40.657347
An Event ID: 4624, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_4624.xml
Matched in Event ID List
This event was created on:  2019-02-13 15:31:19.529518
An Event ID: 4624, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_4624.xml
Matched in Event ID List
```

```
This event was created on:  2019-02-13 15:31:31.556812
An Event ID: 1102, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:01:41.593830
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:01:47.512341
An Event ID: 4688, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:01:47.562412
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:02:04.426662
An Event ID: 4648, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:02:04.426662
An Event ID: 4624, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:02:04.426662
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:02:04.466719
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:02:04.476734
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:02:04.476734
An Event ID: 4648, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:02:04.526806
An Event ID: 4624, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
```

```
Matched in Event ID List
This event was created on:  2019-02-13 18:02:04.526806
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:02:05.418087
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:02:05.458145
An Event ID: 4688, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:02:05.528246
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:02:19.518362
An Event ID: 4688, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:03:28.318441
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:03:28.348558
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:03:29.121593
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:03:29.121593
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:03:32.183609
An Event ID: 4688, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:03:35.704838
```

```
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:03:36.025299
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:03:36.025299
An Event ID: 4688, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:03:42.664848
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:04:01.632120
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:04:01.632120
An Event ID: 5158, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:04:01.722248
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:04:01.722248
An Event ID: 5158, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:04:01.722248
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:04:01.722248
An Event ID: 5158, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:04:01.722248
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
```

```
This event was created on:  2019-02-13 18:04:01.722248
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:04:43.171852
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:04:43.171852
An Event ID: 4672, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:04:43.171852
An Event ID: 4624, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:04:43.171852
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:04:45.905783
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:04:45.905783
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:04:57.442371
An Event ID: 4672, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:04:57.442371
An Event ID: 4624, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:04:57.442371
An Event ID: 4688, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:04:57.462399
An Event ID: 4688, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
```

```
Matched in Event ID List
This event was created on:  2019-02-13 18:04:57.462399
An Event ID: 4688, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:04:57.542515
An Event ID: 4688, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:04:57.672703
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:04:58.283581
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:04:58.323637
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:04:58.333654
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:04:58.333654
An Event ID: 4648, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:04:58.363695
An Event ID: 4624, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:04:58.363695
An Event ID: 4672, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:04:58.363695
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:04:58.413769
```

```
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:04:58.413769
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:04:58.413769
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:04:58.543955
An Event ID: 4688, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:05:00.997484
An Event ID: 4688, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:05:04.802956
An Event ID: 4688, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:05:04.802956
An Event ID: 4688, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:05:04.873055
An Event ID: 4688, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:05:05.123417
An Event ID: 4688, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:05:05.253603
An Event ID: 4688, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:05:06.575504
An Event ID: 4688, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
```

```
This event was created on:  2019-02-13 18:05:06.585520
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:05:18.592783
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:05:18.592783
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:05:18.592783
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:05:18.592783
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:05:18.592783
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:05:18.592783
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:05:18.602798
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:05:18.602798
An Event ID: 5158, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:05:18.702944
An Event ID: 5158, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:05:18.702944
An Event ID: 5158, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
```

```
Matched in Event ID List
This event was created on:  2019-02-13 18:05:18.702944
An Event ID: 5158, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:05:18.702944
An Event ID: 5158, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:05:18.702944
An Event ID: 5158, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:05:18.702944
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:05:18.712955
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:05:18.712955
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:05:18.712955
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:05:18.712955
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:05:18.712955
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:05:18.712955
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:05:18.712955
```

```
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:05:18.712955
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:05:18.773043
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:05:18.773043
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:05:18.793072
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:05:18.793072
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:05:19.684355
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:05:19.734425
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:05:19.734425
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:05:21.597103
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:05:21.597103
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
```

```
This event was created on:  2019-02-13 18:05:21.607119
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:05:21.607119
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:05:24.601423
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:05:24.601423
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:05:24.611439
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunnel_
5156.xml
Matched in Event ID List
This event was created on:  2019-02-13 18:05:24.611439
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:01:46.884037
An Event ID: 5, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:01:50.699524
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:02:21.934439
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:02:22.965921
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:02:48.502642
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
```

```
No Match in Event ID List
This event was created on:  2019-02-16 10:02:48.502642
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:03:02.272442
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:03:02.272442
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:03:47.086882
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:03:48.058277
An Event ID: 5, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:03:48.078306
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:04:04.141405
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:04:04.151419
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:04:04.221519
An Event ID: 5, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:04:04.221519
An Event ID: 6, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:04:04.231533
```

```
An Event ID: 6, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:04:04.231533
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:04:04.351707
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:04:04.892485
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:04:04.892485
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:04:04.962585
An Event ID: 5, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:04:04.962585
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:04:05.092772
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:04:05.092772
An Event ID: 6, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:04:05.122816
An Event ID: 6, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:04:05.122816
An Event ID: 6, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
```

```
This event was created on:  2019-02-16 10:04:05.122816
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:04:05.283047
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:04:05.563450
An Event ID: 5, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:05:06.200642
An Event ID: 5, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:05:06.200642
An Event ID: 5, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:05:06.410944
An Event ID: 5, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:05:06.971750
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:05:22.794502
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:05:22.794502
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:05:22.794502
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:05:22.794502
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
```

```
No Match in Event ID List
This event was created on:  2019-02-16 10:05:22.794502
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:05:22.794502
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:05:22.794502
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:05:22.794502
An Event ID: 6, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:05:25.488375
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:05:26.499830
An Event ID: 5, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:05:26.529873
An Event ID: 5, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:05:26.529873
An Event ID: 5, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:05:26.539886
An Event ID: 5, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:05:26.539886
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:05:34.871868
```

```
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:05:34.871868
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:05:34.871868
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:05:34.871868
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:05:34.871868
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:05:46.929205
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:05:46.929205
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:05:46.929205
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:05:46.929205
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:05:46.929205
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:05:46.929205
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
```

```
This event was created on:  2019-02-16 10:05:59.056644
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:05:59.056644
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:05:59.056644
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:05:59.056644
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:05:59.056644
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:06:00.558804
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:06:00.558804
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:06:00.558804
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:06:00.558804
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:06:00.558804
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:06:02.311325
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
```

```
No Match in Event ID List
This event was created on:  2019-02-16 10:06:02.561684
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:06:03.062405
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:06:03.062405
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_sysmon-3-
rdp-tun.xml
No Match in Event ID List
This event was created on:  2019-02-16 10:06:38.843855
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2018-11-06 21:31:54.070986
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2018-11-06 21:32:00.420115
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2018-11-06 21:32:00.540287
An Event ID: 261, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2018-11-06 21:45:34.878929
An Event ID: 261, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2018-11-06 21:45:50.281076
An Event ID: 1149, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2018-11-06 21:45:50.411263
An Event ID: 261, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2018-11-06 21:48:54.981853
```

```
An Event ID: 261, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2018-11-06 21:49:31.083765
An Event ID: 1149, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2018-11-06 21:49:31.193924
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2018-11-22 10:35:54.700581
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2018-11-22 10:36:03.453165
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2018-11-22 10:36:03.573339
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2018-11-22 12:14:20.036047
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2018-11-22 12:14:20.807156
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2018-11-22 12:14:21.498150
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2018-12-02 13:12:57.971851
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2018-12-02 13:12:59.043392
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
```

```
This event was created on:  2018-12-02 13:12:59.203623
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2018-12-21 11:54:48.701435
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2018-12-21 11:54:49.482557
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2018-12-21 11:54:49.622759
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2018-12-21 14:45:28.179192
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2018-12-21 14:45:28.629839
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2018-12-21 14:45:29.280775
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2018-12-21 17:20:18.578184
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2018-12-21 17:20:19.459450
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2018-12-21 17:20:19.749868
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2018-12-21 17:21:42.376190
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
```

```
No Match in Event ID List
This event was created on:  2018-12-21 17:21:43.081202
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2018-12-21 17:21:44.028559
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2018-12-21 17:23:30.011665
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2018-12-21 17:23:30.562456
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2018-12-21 17:23:31.036135
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2018-12-21 17:26:28.269035
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2018-12-21 17:26:28.863890
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2018-12-21 17:26:29.271473
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2018-12-23 01:47:23.872688
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2018-12-23 01:47:24.523623
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2018-12-23 01:47:25.114473
```

```
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2018-12-23 12:34:22.016422
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2018-12-23 12:34:23.248194
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2018-12-23 12:34:23.929173
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2018-12-29 19:35:20.165724
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2018-12-29 19:35:20.936832
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2018-12-29 19:35:21.147135
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2018-12-29 20:18:19.331249
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2018-12-29 20:18:20.963596
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2018-12-29 20:18:21.684633
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-08 12:31:08.589264
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
```

```
This event was created on:  2019-01-08 12:31:09.280256
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-08 12:31:09.530617
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-17 19:21:01.800783
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-17 19:21:02.832266
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-17 19:21:03.443146
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-17 19:25:22.595198
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-17 19:25:23.706797
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-17 19:25:24.668179
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-17 20:30:02.760105
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-17 20:30:03.421055
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-17 20:30:04.142092
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
```

```
No Match in Event ID List
This event was created on:  2019-01-17 21:03:33.425283
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-17 21:03:34.119284
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-17 21:03:34.308558
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-19 11:34:08.796888
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-19 11:34:09.547970
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-19 11:34:10.178877
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-19 12:20:37.756737
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-19 12:20:38.362606
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-19 12:20:38.671047
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-19 14:31:26.896128
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-19 14:31:27.857510
```

```
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-19 14:31:28.167955
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-19 20:33:17.566996
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-19 20:33:18.438250
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-19 20:33:18.778738
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-19 20:43:35.123838
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-19 20:43:35.574486
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-19 20:43:35.955032
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-19 20:52:28.029467
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-19 20:52:28.473885
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-19 20:52:28.813969
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
```

```
This event was created on:  2019-01-19 21:03:27.630730
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-19 21:03:29.649977
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-19 21:03:30.244293
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-19 21:18:40.452051
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-19 21:18:42.633007
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-19 21:18:42.880745
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-19 22:19:47.283878
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-19 22:19:48.099480
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-19 22:19:48.595060
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-20 13:34:14.249203
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-20 13:34:15.346703
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
```

```
No Match in Event ID List
This event was created on:  2019-01-20 13:34:15.795134
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-21 12:15:33.938274
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-21 12:15:34.920408
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-21 12:15:35.036779
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-21 12:16:32.063545
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-21 12:16:32.964083
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-21 12:16:33.360275
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-21 13:22:08.843588
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-21 13:22:09.850801
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-21 13:22:09.957140
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-22 13:19:35.402824
```

```
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-22 13:19:36.313730
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-22 13:19:36.547476
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-25 08:54:21.119736
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-25 08:54:21.827995
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-25 08:54:22.289467
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-28 15:17:39.509209
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-28 15:17:40.599688
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-28 15:17:40.744148
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-28 16:05:44.196819
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-28 16:05:45.044643
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
```

```
This event was created on:  2019-01-28 16:05:45.600718
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-28 16:39:09.752388
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-28 16:39:11.074501
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-28 16:39:11.752630
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-29 10:40:46.795031
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-29 10:40:47.900557
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-29 10:40:48.480406
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-29 22:54:04.319923
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-29 22:54:05.060284
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-29 22:54:05.498682
An Event ID: 261, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-29 22:58:34.995092
An Event ID: 261, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
```

```
No Match in Event ID List
This event was created on:  2019-01-29 22:59:37.084372
An Event ID: 1149, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-29 23:00:10.212008
An Event ID: 261, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-29 23:15:24.164234
An Event ID: 261, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-29 23:16:28.646955
An Event ID: 1149, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-29 23:16:39.762939
An Event ID: 261, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-29 23:50:40.730331
An Event ID: 261, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-29 23:54:04.665623
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-29 23:54:54.730976
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-29 23:54:55.470333
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-29 23:54:55.621817
An Event ID: 261, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-29 23:56:17.851288
```

```
An Event ID: 261, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-29 23:57:54.299974
An Event ID: 1149, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-29 23:58:05.245712
An Event ID: 261, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-30 00:00:50.843832
An Event ID: 261, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-30 00:01:00.497713
An Event ID: 1149, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-01-30 00:01:00.547785
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-01 10:26:57.663111
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-01 10:26:58.696407
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-01 10:26:59.284283
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-02 16:12:53.471403
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-02 16:12:54.933416
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
```

```
This event was created on:  2019-02-02 16:12:56.285360
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-02 17:16:10.753069
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-02 17:16:12.196604
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-02 17:16:13.818937
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-02 20:25:38.398096
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-02 20:25:39.673111
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-02 20:25:41.495731
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-02 21:28:12.359316
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-02 21:28:14.008718
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-02 21:28:15.621037
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-02 22:35:13.949436
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
```

```
No Match in Event ID List
This event was created on:  2019-02-02 22:35:15.576292
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-02 22:35:28.314610
An Event ID: 261, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-02 22:39:00.497213
An Event ID: 261, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-02 22:39:42.597752
An Event ID: 1149, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-02 22:40:13.572290
An Event ID: 261, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-02 22:42:54.728239
An Event ID: 261, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-02 22:44:33.680527
An Event ID: 1149, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-02 22:44:55.932522
An Event ID: 261, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-02 23:02:41.826338
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-02 23:36:28.081221
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-02 23:36:29.268005
```

```
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-02 23:36:30.926876
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-03 01:08:18.188990
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-03 01:08:19.503481
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-03 01:08:20.865438
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-03 03:05:56.544275
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-03 03:05:58.148428
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-03 03:05:59.951019
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-04 12:02:44.206947
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-04 12:02:44.927244
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-04 12:02:46.301628
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
```

```
This event was created on:  2019-02-04 12:13:24.810781
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-04 12:13:25.552061
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-04 12:13:26.584757
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-04 12:37:59.567163
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-04 12:38:00.222670
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-04 12:38:01.953529
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-04 13:46:45.991890
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-04 13:46:47.020168
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-04 13:46:48.413015
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-04 20:13:11.672703
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-04 20:13:12.397015
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
```

```
No Match in Event ID List
This event was created on:  2019-02-04 20:13:13.818548
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-04 21:36:57.697525
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-04 21:36:58.760916
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-04 21:37:00.983162
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-06 09:47:36.926695
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-06 09:47:37.847633
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-06 09:47:39.273567
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-07 20:06:49.261013
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-07 20:06:50.195995
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-07 20:06:51.532980
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-08 09:23:46.465374
```

```
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-08 09:23:49.605038
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-08 09:24:02.603376
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-08 16:09:19.326967
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-08 16:09:20.439516
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-08 16:09:21.905754
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-10 11:02:26.394484
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-10 11:02:29.208672
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-10 11:02:42.427679
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-13 12:18:48.588120
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-13 12:18:49.474949
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
```

```
This event was created on:  2019-02-13 12:18:50.723932
An Event ID: 261, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-13 12:23:42.178295
An Event ID: 261, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-13 12:23:53.754942
An Event ID: 1149, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-13 12:23:53.875114
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-13 14:05:43.500158
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-13 14:05:44.336826
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-13 14:05:45.553709
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-13 15:15:14.054340
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-13 15:15:14.846869
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-13 15:15:16.973652
An Event ID: 1155, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-13 17:18:28.040384
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
```

```
No Match in Event ID List
This event was created on:  2019-02-13 17:18:30.771694
An Event ID: 1136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-13 17:18:41.657347
An Event ID: 261, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-13 17:50:15.741018
An Event ID: 261, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-13 17:50:55.608345
An Event ID: 1149, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-13 17:51:19.943336
An Event ID: 261, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-13 18:04:01.632120
An Event ID: 261, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-13 18:04:45.905783
An Event ID: 1149, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/DE_RDP_Tunneli
ng_TerminalServices-RemoteConnectionManagerOperational_1149.xml
No Match in Event ID List
This event was created on:  2019-02-13 18:04:57.452387
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/tunna_iis_rdp_
smb_tunneling_sysmon_3.xml
No Match in Event ID List
This event was created on:  2019-09-03 11:04:07.207048
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/tunna_iis_rdp_
smb_tunneling_sysmon_3.xml
No Match in Event ID List
This event was created on:  2019-09-03 11:04:07.207130
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/tunna_iis_rdp_
smb_tunneling_sysmon_3.xml
No Match in Event ID List
This event was created on:  2019-09-03 11:04:56.358688
```

```
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/tunna_iis_rdp_
smb_tunneling_sysmon_3.xml
No Match in Event ID List
This event was created on:  2019-09-03 11:04:58.463053
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/tunna_iis_rdp_
smb_tunneling_sysmon_3.xml
No Match in Event ID List
This event was created on:  2019-09-03 11:05:22.837679
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/tunna_iis_rdp_
smb_tunneling_sysmon_3.xml
No Match in Event ID List
This event was created on:  2019-09-03 11:05:22.837749
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/tunna_iis_rdp_
smb_tunneling_sysmon_3.xml
No Match in Event ID List
This event was created on:  2019-09-03 11:33:24.177710
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/tunna_iis_rdp_
smb_tunneling_sysmon_3.xml
No Match in Event ID List
This event was created on:  2019-09-03 11:33:24.177923
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/tunna_iis_rdp_
smb_tunneling_sysmon_3.xml
No Match in Event ID List
This event was created on:  2019-09-03 11:34:37.129225
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/tunna_iis_rdp_
smb_tunneling_sysmon_3.xml
No Match in Event ID List
This event was created on:  2019-09-03 11:34:37.129370
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/tunna_iis_rdp_
smb_tunneling_sysmon_3.xml
No Match in Event ID List
This event was created on:  2019-09-03 11:36:26.005428
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Command_and_Control/tunna_iis_rdp_
smb_tunneling_sysmon_3.xml
No Match in Event ID List
This event was created on:  2019-09-03 11:36:26.005493
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_sysmon_1_ftp.xml
No Match in Event ID List
This event was created on:  2019-05-12 17:20:01.980574
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_sysmon_1_ftp.xml
No Match in Event ID List
This event was created on:  2019-05-12 17:20:31.183699
```

```
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_sysmon_1_ftp.xml
No Match in Event ID List
This event was created on:  2019-05-12 17:20:49.443464
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_sysmon_1_ftp.xml
No Match in Event ID List
This event was created on:  2019-05-12 17:20:49.458113
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/Sysmon_meterpreter_Refle
ctivePEInjection_to_notepad_.xml
No Match in Event ID List
This event was created on:  2019-07-03 20:39:29.223482
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/Sysmon_meterpreter_Refle
ctivePEInjection_to_notepad_.xml
No Match in Event ID List
This event was created on:  2019-07-03 20:39:30.129732
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/Sysmon_meterpreter_Refle
ctivePEInjection_to_notepad_.xml
No Match in Event ID List
This event was created on:  2019-07-03 20:39:30.145357
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/Sysmon_meterpreter_Refle
ctivePEInjection_to_notepad_.xml
No Match in Event ID List
This event was created on:  2019-07-03 20:39:30.160984
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/Sysmon_meterpreter_Refle
ctivePEInjection_to_notepad_.xml
No Match in Event ID List
This event was created on:  2019-07-03 20:39:30.176607
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/Sysmon_meterpreter_Refle
ctivePEInjection_to_notepad_.xml
No Match in Event ID List
This event was created on:  2019-07-03 20:39:30.192232
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/Sysmon_meterpreter_Refle
ctivePEInjection_to_notepad_.xml
No Match in Event ID List
This event was created on:  2019-07-03 20:39:30.207859
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/Sysmon_meterpreter_Refle
ctivePEInjection_to_notepad_.xml
No Match in Event ID List
This event was created on:  2019-07-03 20:39:30.223482
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/Sysmon_meterpreter_Refle
ctivePEInjection_to_notepad_.xml
No Match in Event ID List
This event was created on:  2019-07-03 20:39:30.239109
```

```
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/Sysmon_meterpreter_Refle
ctivePEInjection_to_notepad_.xml
No Match in Event ID List
This event was created on:  2019-07-03 20:39:30.254732
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/Sysmon_meterpreter_Refle
ctivePEInjection_to_notepad_.xml
No Match in Event ID List
This event was created on:  2019-07-03 20:39:30.254732
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/Sysmon_meterpreter_Refle
ctivePEInjection_to_notepad_.xml
No Match in Event ID List
This event was created on:  2019-07-03 20:39:30.254732
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/Sysmon_meterpreter_Refle
ctivePEInjection_to_notepad_.xml
No Match in Event ID List
This event was created on:  2019-07-03 20:39:31.707859
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_sysmon_1_lolbin_run
dll32_advpack_RegisterOCX.xml
No Match in Event ID List
This event was created on:  2019-05-12 14:18:03.589506
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_sysmon_1_lolbin_run
dll32_advpack_RegisterOCX.xml
No Match in Event ID List
This event was created on:  2019-05-12 14:18:09.589506
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_wmic_xsl_internet_s
ysmon_3_1_11.xml
No Match in Event ID List
This event was created on:  2019-05-23 16:48:35.487223
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_wmic_xsl_internet_s
ysmon_3_1_11.xml
No Match in Event ID List
This event was created on:  2019-05-23 16:49:05.736570
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_wmic_xsl_internet_s
ysmon_3_1_11.xml
No Match in Event ID List
This event was created on:  2019-05-23 16:49:05.862062
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_wmic_xsl_internet_s
ysmon_3_1_11.xml
No Match in Event ID List
This event was created on:  2019-05-23 16:49:07.731892
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_wmic_xsl_internet_s
ysmon_3_1_11.xml
No Match in Event ID List
```

```
This event was created on:  2019-05-23 16:49:08.208763
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_wmic_xsl_internet_s
ysmon_3_1_11.xml
No Match in Event ID List
This event was created on:  2019-05-23 16:49:08.422098
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_wmic_xsl_internet_s
ysmon_3_1_11.xml
No Match in Event ID List
This event was created on:  2019-05-23 16:49:09.576626
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_wmic_xsl_internet_s
ysmon_3_1_11.xml
No Match in Event ID List
This event was created on:  2019-05-23 16:50:44.582500
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_driveby_cve-2018-
15982_sysmon_1_10.xml
No Match in Event ID List
This event was created on:  2019-05-22 04:02:11.307032
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_driveby_cve-2018-
15982_sysmon_1_10.xml
No Match in Event ID List
This event was created on:  2019-05-22 04:02:11.307032
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_sysmon_1_rundll32_p
cwutl_LaunchApplication.xml
No Match in Event ID List
This event was created on:  2019-05-12 17:09:02.275164
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/sysmon_lolbin_bohops_vsh
adow_exec.xml
No Match in Event ID List
This event was created on:  2019-05-28 02:13:52.171926
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/sysmon_lolbin_bohops_vsh
adow_exec.xml
No Match in Event ID List
This event was created on:  2019-05-28 02:13:52.429310
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/sysmon_lolbin_bohops_vsh
adow_exec.xml
No Match in Event ID List
This event was created on:  2019-05-28 02:13:53.507099
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/sysmon_lolbin_bohops_vsh
adow_exec.xml
No Match in Event ID List
This event was created on:  2019-05-28 02:14:48.819881
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/sysmon_lolbin_bohops_vsh
adow_exec.xml
```

```
No Match in Event ID List
This event was created on:  2019-05-28 02:14:49.194881
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/sysmon_lolbin_bohops_vsh
adow_exec.xml
No Match in Event ID List
This event was created on:  2019-05-28 02:14:50.413631
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_sysmon_1_11_lolbin_
rundll32_shdocvw_openurl.xml
No Match in Event ID List
This event was created on:  2019-05-12 13:55:56.626501
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_sysmon_1_11_lolbin_
rundll32_shdocvw_openurl.xml
No Match in Event ID List
This event was created on:  2019-05-12 13:56:12.329624
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_sysmon_1_11_lolbin_
rundll32_shdocvw_openurl.xml
No Match in Event ID List
This event was created on:  2019-05-12 13:56:12.652868
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_sysmon_1_11_lolbin_
rundll32_shdocvw_openurl.xml
No Match in Event ID List
This event was created on:  2019-05-12 13:56:46.573767
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_sysmon_1_11_lolbin_
rundll32_shdocvw_openurl.xml
No Match in Event ID List
This event was created on:  2019-05-12 13:56:46.605017
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_sysmon_1_11_lolbin_
rundll32_shdocvw_openurl.xml
No Match in Event ID List
This event was created on:  2019-05-12 13:57:39.662634
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/sysmon_vbs_sharpshooter_
stageless_meterpreter.xml
No Match in Event ID List
This event was created on:  2019-06-15 07:21:50.488632
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/sysmon_vbs_sharpshooter_
stageless_meterpreter.xml
No Match in Event ID List
This event was created on:  2019-06-15 07:21:51.035509
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/sysmon_vbs_sharpshooter_
stageless_meterpreter.xml
No Match in Event ID List
This event was created on:  2019-06-15 07:22:05.691757
```

```
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/sysmon_vbs_sharpshooter_
stageless_meterpreter.xml
No Match in Event ID List
This event was created on:  2019-06-15 07:22:05.973009
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/sysmon_vbs_sharpshooter_
stageless_meterpreter.xml
No Match in Event ID List
This event was created on:  2019-06-15 07:22:08.473009
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_sysmon_1_lolbin_ren
amed_regsvr32_scrobj.xml
No Match in Event ID List
This event was created on:  2019-05-12 18:48:52.219755
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_sysmon_1_lolbin_ren
amed_regsvr32_scrobj.xml
No Match in Event ID List
This event was created on:  2019-05-12 18:48:52.766630
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/sysmon_1_11_rundll32_cpl
_ostap.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:11:11.156704
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/sysmon_1_11_rundll32_cpl
_ostap.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:11:17.364511
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/sysmon_1_11_rundll32_cpl
_ostap.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:11:17.587732
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/sysmon_1_11_rundll32_cpl
_ostap.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:11:17.621241
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/sysmon_1_11_rundll32_cpl
_ostap.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:11:19.098104
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_sysmon_1_11_lolbin_
rundll32_openurl_FileProtocolHandler.xml
No Match in Event ID List
This event was created on:  2019-05-12 13:30:32.931757
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_sysmon_1_11_lolbin_
rundll32_openurl_FileProtocolHandler.xml
No Match in Event ID List
```

```
This event was created on:  2019-05-12 13:30:46.181757
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_sysmon_1_11_lolbin_
rundll32_openurl_FileProtocolHandler.xml
No Match in Event ID List
This event was created on:  2019-05-12 13:30:46.400505
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_sysmon_1_11_lolbin_
rundll32_openurl_FileProtocolHandler.xml
No Match in Event ID List
This event was created on:  2019-05-12 13:30:46.556755
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_sysmon_1_11_lolbin_
rundll32_openurl_FileProtocolHandler.xml
No Match in Event ID List
This event was created on:  2019-05-12 13:32:58.167194
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_sysmon_1_11_lolbin_
rundll32_openurl_FileProtocolHandler.xml
No Match in Event ID List
This event was created on:  2019-05-12 13:33:37.078800
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_sysmon_1_11_lolbin_
rundll32_openurl_FileProtocolHandler.xml
No Match in Event ID List
This event was created on:  2019-05-12 13:33:59.743078
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_sysmon_1_11_lolbin_
rundll32_openurl_FileProtocolHandler.xml
No Match in Event ID List
This event was created on:  2019-05-12 13:37:49.604921
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_sysmon_1_11_lolbin_
rundll32_openurl_FileProtocolHandler.xml
No Match in Event ID List
This event was created on:  2019-05-12 13:38:00.523670
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_sysmon_1_11_lolbin_
rundll32_openurl_FileProtocolHandler.xml
No Match in Event ID List
This event was created on:  2019-05-12 13:38:00.712732
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_sysmon_1_11_lolbin_
rundll32_openurl_FileProtocolHandler.xml
No Match in Event ID List
This event was created on:  2019-05-12 13:38:01.383045
An Event ID: 17, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/Exec_via_cpl_Application
_Experience_EventID_17_ControlPanelApplet.xml
No Match in Event ID List
This event was created on:  2019-07-18 21:50:20.049400
An Event ID: 17, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/Exec_via_cpl_Application
_Experience_EventID_17_ControlPanelApplet.xml
```

```
No Match in Event ID List
This event was created on:  2019-07-29 21:11:17.282188
An Event ID: 17, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/Exec_via_cpl_Application
_Experience_EventID_17_ControlPanelApplet.xml
No Match in Event ID List
This event was created on:  2019-07-29 21:14:29.638744
An Event ID: 17, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/Exec_via_cpl_Application
_Experience_EventID_17_ControlPanelApplet.xml
No Match in Event ID List
This event was created on:  2019-08-23 11:17:00.483376
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_sysmon_1_lolbin_pca
lua.xml
No Match in Event ID List
This event was created on:  2019-05-12 17:01:43.391861
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_sysmon_1_lolbin_pca
lua.xml
No Match in Event ID List
This event was created on:  2019-05-12 17:01:50.781013
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_sysmon_1_lolbin_pca
lua.xml
No Match in Event ID List
This event was created on:  2019-05-12 17:01:51.007950
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-03-19 13:05:42
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-03-19 13:05:42
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-03-19 13:05:42
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-03-19 13:05:44
An Event ID: 163841040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-03-23 18:35:40
```

```
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-03-23 19:05:19
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-03-23 19:07:20
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-03-23 19:08:03
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-03-23 19:08:03
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-03-23 19:08:03
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-03-23 19:08:03
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-03-23 19:12:38
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-03-23 19:12:39
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-03-23 19:12:39
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-03-23 19:12:41
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
```

```
This event was created on:  2019-07-30 11:24:57
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-07-30 11:25:08
An Event ID: 163841040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-20 09:45:49
An Event ID: 163841040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-20 09:47:43
An Event ID: 163841040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:04:21
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:07:32
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:07:38
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:07:38
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:07:39
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:07:39
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:07:42
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
```

```
No Match in Event ID List
This event was created on:  2019-09-23 09:07:45
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:07:46
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:07:46
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:07:47
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:07:47
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:07:50
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:07:53
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:07:53
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:07:53
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:07:54
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:07:54
```

```
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:07:54
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:07:54
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:07:55
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:07:55
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:07:56
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:08:00
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:08:01
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:08:02
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:08:04
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:08:04
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
```

```
This event was created on:  2019-09-23 09:08:04
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:08:04
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:08:06
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:08:13
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:08:16
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:08:18
An Event ID: 163841040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:08:21
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:08:22
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:08:56
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:09:00
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:09:00
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
```

```
No Match in Event ID List
This event was created on:  2019-09-23 09:09:00
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:09:00
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:09:02
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:09:02
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:09:05
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:09:09
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:09:11
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:09:11
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:09:13
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:09:13
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:09:15
```

```
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:09:31
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:09:32
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:09:32
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:09:33
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:09:33
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:09:34
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:09:34
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:09:35
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:09:35
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:09:35
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
```

```
This event was created on:  2019-09-23 09:09:35
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:09:36
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:09:36
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:09:37
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:09:37
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:09:38
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:09:38
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:09:41
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:09:41
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:09:43
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:09:43
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
```

```
No Match in Event ID List
This event was created on:  2019-09-23 09:09:46
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:09:52
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:09:55
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:09:57
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:10:05
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:10:53
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:10:57
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:11:02
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:11:03
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:11:03
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:11:06
```

```
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:11:08
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:11:09
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:11:09
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:11:10
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:11:13
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:11:15
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:11:26
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:11:27
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:11:27
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:11:27
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
```

```
This event was created on:  2019-09-23 09:11:27
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:11:28
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:11:28
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:11:28
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:11:28
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:11:28
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:11:29
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:11:30
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:11:37
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:11:38
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:11:40
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
```

```
No Match in Event ID List
This event was created on:  2019-09-23 09:11:42
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:11:42
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:11:44
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:11:52
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:11:55
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:11:55
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:11:55
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:11:57
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:12:05
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:14:31
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:14:34
```

```
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:14:34
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:14:37
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:14:37
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:14:38
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:14:43
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:14:45
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:14:45
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:14:46
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:14:46
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:14:49
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
```

```
This event was created on:  2019-09-23 09:15:00
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:15:01
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:15:01
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:15:01
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:15:01
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:15:02
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:15:02
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:15:02
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:15:02
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:15:03
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:15:03
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
```

```
No Match in Event ID List
This event was created on:  2019-09-23 09:15:05
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:15:07
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:15:09
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:15:11
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:15:13
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:15:13
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:15:13
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:15:13
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:15:15
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:15:21
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:15:24
```

```
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:15:26
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:15:33
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:16:28
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:16:34
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:16:34
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:16:37
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:16:37
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:16:39
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:16:40
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:16:42
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
```

```
This event was created on:  2019-09-23 09:16:42
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:16:43
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:16:45
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:16:48
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:16:48
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:16:48
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:17:11
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:17:13
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:17:13
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:17:14
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:17:14
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
```

```
No Match in Event ID List
This event was created on:  2019-09-23 09:17:19
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:17:19
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:17:19
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:17:19
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:17:21
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:17:21
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:17:23
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:17:23
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:17:23
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:17:25
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:17:27
```

```
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:17:36
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:17:40
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:17:42
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:17:48
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:18:30
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:18:35
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:18:38
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:18:40
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:18:40
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:18:42
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
```

```
This event was created on:  2019-09-23 09:18:42
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:18:44
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:18:44
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:18:46
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:18:46
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:18:48
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:18:52
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:18:53
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:18:53
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:18:54
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:18:54
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
```

```
No Match in Event ID List
This event was created on:  2019-09-23 09:18:54
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:18:54
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:18:55
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:18:55
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:18:56
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:18:56
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:18:58
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:19:00
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:19:03
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:19:03
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:19:04
```

```
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:19:04
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:19:06
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:19:06
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:19:07
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:19:13
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:19:15
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:19:17
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:19:24
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:22:03
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:22:09
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
```

```
This event was created on:  2019-09-23 09:22:09
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:22:12
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:22:12
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:22:15
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:22:15
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:22:16
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:22:16
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:22:18
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:22:18
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:22:19
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:22:19
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
```

```
No Match in Event ID List
This event was created on:  2019-09-23 09:22:22
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:22:28
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:22:29
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:22:29
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:22:30
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:22:30
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:22:31
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:22:31
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:22:31
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:22:31
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:22:32
```

```
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:22:32
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:22:32
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:22:33
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:22:33
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:22:33
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:22:34
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:22:34
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:22:36
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:22:36
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:22:39
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
```

```
This event was created on:  2019-09-23 09:22:39
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:22:41
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:22:41
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:22:43
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:22:49
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:22:51
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:22:53
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:23:00
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:43:05
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:43:13
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:43:13
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
```

```
No Match in Event ID List
This event was created on:  2019-09-23 09:43:15
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:43:15
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:43:17
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:43:18
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:43:19
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:43:19
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:43:21
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:43:22
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:43:24
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:43:36
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:43:37
```

```
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:43:37
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:43:38
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:43:38
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:43:41
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:43:41
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:43:42
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:43:43
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:43:44
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:43:44
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:43:46
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
```

```
This event was created on:  2019-09-23 09:43:49
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:43:51
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:43:51
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:43:51
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:43:51
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:43:53
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:43:59
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:44:01
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:44:06
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:44:13
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:45:25
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
```

```
No Match in Event ID List
This event was created on:  2019-09-23 09:45:29
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:45:29
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:45:29
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:45:30
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:45:32
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:45:33
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:45:34
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:45:36
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:45:38
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:45:38
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:45:39
```

```
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:45:39
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:45:42
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:45:53
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:45:54
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:45:54
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:45:55
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:45:55
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:45:56
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:45:56
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:45:56
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
```

```
This event was created on:  2019-09-23 09:45:56
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:45:57
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:45:57
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:45:58
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:45:58
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:46:00
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:46:00
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:46:03
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:46:03
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:46:04
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:46:10
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
```

```
No Match in Event ID List
This event was created on:  2019-09-23 09:46:13
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:46:15
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-09-23 09:46:22
An Event ID: 01040, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-10-31 14:48:42
An Event ID: 01042, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/rogue_msi_url_1040_1042.
xml
No Match in Event ID List
This event was created on:  2019-10-31 14:48:42
An Event ID: 2, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/Exec_sysmon_meterpreter_
reversetcp_msipackage.xml
No Match in Event ID List
This event was created on:  2019-04-30 22:48:58.901474
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/Exec_sysmon_meterpreter_
reversetcp_msipackage.xml
No Match in Event ID List
This event was created on:  2019-04-30 22:48:59.260851
An Event ID: 2, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/Exec_sysmon_meterpreter_
reversetcp_msipackage.xml
No Match in Event ID List
This event was created on:  2019-04-30 22:49:08.760851
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/Exec_sysmon_meterpreter_
reversetcp_msipackage.xml
No Match in Event ID List
This event was created on:  2019-04-30 22:49:09.542101
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/Exec_sysmon_meterpreter_
reversetcp_msipackage.xml
No Match in Event ID List
This event was created on:  2019-04-30 22:49:09.760851
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/Exec_sysmon_meterpreter_
reversetcp_msipackage.xml
No Match in Event ID List
This event was created on:  2019-04-30 22:49:09.792101
```

```
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/Exec_sysmon_meterpreter_
reversetcp_msipackage.xml
No Match in Event ID List
This event was created on:  2019-04-30 22:49:10.198349
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/Exec_sysmon_meterpreter_
reversetcp_msipackage.xml
No Match in Event ID List
This event was created on:  2019-04-30 22:52:27.588976
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_persist_rundll32_ms
hta_scheduledtask_sysmon_1_3_11.xml
No Match in Event ID List
This event was created on:  2019-05-21 15:32:57.286253
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_persist_rundll32_ms
hta_scheduledtask_sysmon_1_3_11.xml
No Match in Event ID List
This event was created on:  2019-05-21 15:32:57.286253
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_persist_rundll32_ms
hta_scheduledtask_sysmon_1_3_11.xml
No Match in Event ID List
This event was created on:  2019-05-21 15:32:57.867088
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_persist_rundll32_ms
hta_scheduledtask_sysmon_1_3_11.xml
No Match in Event ID List
This event was created on:  2019-05-21 15:32:59.389278
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_persist_rundll32_ms
hta_scheduledtask_sysmon_1_3_11.xml
No Match in Event ID List
This event was created on:  2019-05-21 15:32:59.769825
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_persist_rundll32_ms
hta_scheduledtask_sysmon_1_3_11.xml
No Match in Event ID List
This event was created on:  2019-05-21 15:32:59.809883
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_persist_rundll32_ms
hta_scheduledtask_sysmon_1_3_11.xml
No Match in Event ID List
This event was created on:  2019-05-21 15:33:00.140358
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_persist_rundll32_ms
hta_scheduledtask_sysmon_1_3_11.xml
No Match in Event ID List
This event was created on:  2019-05-21 15:33:01.141798
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/sysmon_lolbas_rundll32_z
ipfldr_routethecall_shell.xml
No Match in Event ID List
```

```
This event was created on:  2019-08-14 12:17:14.614738
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/sysmon_lolbas_rundll32_z
ipfldr_routethecall_shell.xml
No Match in Event ID List
This event was created on:  2019-08-14 12:17:14.893929
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/sysmon_exec_from_vss_per
sistence.xml
No Match in Event ID List
This event was created on:  2019-05-27 15:12:38.241299
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/sysmon_exec_from_vss_per
sistence.xml
No Match in Event ID List
This event was created on:  2019-05-27 15:12:38.290375
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/sysmon_exec_from_vss_per
sistence.xml
No Match in Event ID List
This event was created on:  2019-05-27 15:12:43.990982
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/sysmon_exec_from_vss_per
sistence.xml
No Match in Event ID List
This event was created on:  2019-05-27 15:12:44.055763
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/sysmon_exec_from_vss_per
sistence.xml
No Match in Event ID List
This event was created on:  2019-05-27 15:12:45.405336
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/sysmon_exec_from_vss_per
sistence.xml
No Match in Event ID List
This event was created on:  2019-05-27 15:12:45.491711
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/sysmon_exec_from_vss_per
sistence.xml
No Match in Event ID List
This event was created on:  2019-05-27 15:12:46.981642
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/sysmon_exec_from_vss_per
sistence.xml
No Match in Event ID List
This event was created on:  2019-05-27 15:12:47.402708
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/sysmon_exec_from_vss_per
sistence.xml
No Match in Event ID List
This event was created on:  2019-05-27 15:12:47.478285
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/sysmon_exec_from_vss_per
sistence.xml
```

```
No Match in Event ID List
This event was created on:  2019-05-27 15:12:48.655113
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/sysmon_exec_from_vss_per
sistence.xml
No Match in Event ID List
This event was created on:  2019-05-27 15:12:48.763079
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/sysmon_exec_from_vss_per
sistence.xml
No Match in Event ID List
This event was created on:  2019-05-27 15:12:48.827858
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/sysmon_exec_from_vss_per
sistence.xml
No Match in Event ID List
This event was created on:  2019-05-27 15:12:54.447495
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/sysmon_exec_from_vss_per
sistence.xml
No Match in Event ID List
This event was created on:  2019-05-27 15:12:54.544664
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/sysmon_exec_from_vss_per
sistence.xml
No Match in Event ID List
This event was created on:  2019-05-27 15:12:54.632118
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/sysmon_exec_from_vss_per
sistence.xml
No Match in Event ID List
This event was created on:  2019-05-27 15:12:59.519770
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/sysmon_exec_from_vss_per
sistence.xml
No Match in Event ID List
This event was created on:  2019-05-27 15:12:59.578070
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_sysmon_1_7_jscript9
_defense_evasion.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:50:36.858385
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_sysmon_1_7_jscript9
_defense_evasion.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:50:36.889322
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_sysmon_1_7_jscript9
_defense_evasion.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:51:14.254967
```

```
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_sysmon_1_11_lolbin_
rundll32_zipfldr_RouteTheCall.xml
No Match in Event ID List
This event was created on:  2019-05-12 13:58:39.850134
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_sysmon_1_11_lolbin_
rundll32_zipfldr_RouteTheCall.xml
No Match in Event ID List
This event was created on:  2019-05-12 13:58:54.897009
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/sysmon_mshta_sharpshoote
r_stageless_meterpreter.xml
No Match in Event ID List
This event was created on:  2019-06-15 07:13:42.294109
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/sysmon_mshta_sharpshoote
r_stageless_meterpreter.xml
No Match in Event ID List
This event was created on:  2019-06-15 07:13:44.106609
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/sysmon_mshta_sharpshoote
r_stageless_meterpreter.xml
No Match in Event ID List
This event was created on:  2019-06-15 07:14:32.809734
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_sysmon_lobin_regsvr
32_sct.xml
No Match in Event ID List
This event was created on:  2019-05-12 18:35:05.155949
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_sysmon_lobin_regsvr
32_sct.xml
No Match in Event ID List
This event was created on:  2019-05-12 18:35:05.780949
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_sysmon_lobin_regsvr
32_sct.xml
No Match in Event ID List
This event was created on:  2019-05-12 18:35:06.562199
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/Sysmon_Exec_CompiledHTML
.xml
No Match in Event ID List
This event was created on:  2019-07-26 07:39:14.375565
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/Sysmon_Exec_CompiledHTML
.xml
No Match in Event ID List
This event was created on:  2019-07-26 07:39:14.935858
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/susp_explorer_exec.xml
No Match in Event ID List
This event was created on:  2019-08-14 11:53:29.688459
```

```
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/susp_explorer_exec.xml
No Match in Event ID List
This event was created on:  2019-08-14 11:53:30.010139
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/susp_explorer_exec.xml
No Match in Event ID List
This event was created on:  2019-08-14 11:53:30.022856
An Event ID: 4698, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/temp_scheduled_task_4698
_4699.xml
Matched in Event ID List
This event was created on:  2019-03-19 00:02:04.319944
An Event ID: 4699, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/temp_scheduled_task_4698
_4699.xml
Matched in Event ID List
This event was created on:  2019-03-19 00:02:04.351252
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_msxsl_xsl_sysmon_1_
7.xml
No Match in Event ID List
This event was created on:  2019-05-23 17:26:08.716858
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_msxsl_xsl_sysmon_1_
7.xml
No Match in Event ID List
This event was created on:  2019-05-23 17:26:08.947189
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Execution/exec_msxsl_xsl_sysmon_1_
7.xml
No Match in Event ID List
This event was created on:  2019-05-23 17:26:09.437895
An Event ID: 16, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/babyshark_mimika
tz_powershell.xml
No Match in Event ID List
This event was created on:  2019-04-18 16:55:37.014980
An Event ID: 4, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/babyshark_mimika
tz_powershell.xml
No Match in Event ID List
This event was created on:  2019-04-18 16:55:37.115124
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/babyshark_mimika
tz_powershell.xml
No Match in Event ID List
This event was created on:  2019-04-18 16:55:37.125139
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/babyshark_mimika
tz_powershell.xml
No Match in Event ID List
This event was created on:  2019-04-18 16:55:37.125139
```

```
An Event ID: 5, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/babyshark_mimika
tz_powershell.xml
No Match in Event ID List
This event was created on:  2019-04-18 16:55:38.076506
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/babyshark_mimika
tz_powershell.xml
No Match in Event ID List
This event was created on:  2019-04-18 16:55:44.045090
An Event ID: 16, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/babyshark_mimika
tz_powershell.xml
No Match in Event ID List
This event was created on:  2019-04-18 16:55:44.135218
An Event ID: 5, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/babyshark_mimika
tz_powershell.xml
No Match in Event ID List
This event was created on:  2019-04-18 16:55:44.145233
An Event ID: 12, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/babyshark_mimika
tz_powershell.xml
No Match in Event ID List
This event was created on:  2019-04-18 16:55:51.275486
An Event ID: 12, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/babyshark_mimika
tz_powershell.xml
No Match in Event ID List
This event was created on:  2019-04-18 16:55:51.275486
An Event ID: 12, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/babyshark_mimika
tz_powershell.xml
No Match in Event ID List
This event was created on:  2019-04-18 16:55:51.275486
An Event ID: 12, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/babyshark_mimika
tz_powershell.xml
No Match in Event ID List
This event was created on:  2019-04-18 16:55:51.285500
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/babyshark_mimika
tz_powershell.xml
No Match in Event ID List
This event was created on:  2019-04-18 16:56:08.370066
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/babyshark_mimika
tz_powershell.xml
No Match in Event ID List
This event was created on:  2019-04-18 16:56:24.893827
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/babyshark_mimika
tz_powershell.xml
No Match in Event ID List
```

```
This event was created on:  2019-04-18 16:57:04.681038
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/babyshark_mimika
tz_powershell.xml
No Match in Event ID List
This event was created on:  2019-04-18 16:57:06.954308
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/babyshark_mimika
tz_powershell.xml
No Match in Event ID List
This event was created on:  2019-04-18 16:57:52.910389
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/babyshark_mimika
tz_powershell.xml
No Match in Event ID List
This event was created on:  2019-04-18 16:58:12.979246
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/babyshark_mimika
tz_powershell.xml
No Match in Event ID List
This event was created on:  2019-04-18 16:58:13.389835
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/babyshark_mimika
tz_powershell.xml
No Match in Event ID List
This event was created on:  2019-04-18 16:58:13.650211
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/babyshark_mimika
tz_powershell.xml
No Match in Event ID List
This event was created on:  2019-04-18 16:58:13.740339
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/babyshark_mimika
tz_powershell.xml
No Match in Event ID List
This event was created on:  2019-04-18 16:58:14.811880
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/babyshark_mimika
tz_powershell.xml
No Match in Event ID List
This event was created on:  2019-04-18 16:58:14.871967
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/babyshark_mimika
tz_powershell.xml
No Match in Event ID List
This event was created on:  2019-04-18 17:00:09.977482
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/babyshark_mimika
tz_powershell.xml
No Match in Event ID List
This event was created on:  2019-04-18 17:01:34.168541
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/babyshark_mimika
tz_powershell.xml
```

```
No Match in Event ID List
This event was created on:  2019-04-18 17:01:34.448944
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/babyshark_mimika
tz_powershell.xml
No Match in Event ID List
This event was created on:  2019-04-18 17:01:34.659248
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/babyshark_mimika
tz_powershell.xml
No Match in Event ID List
This event was created on:  2019-04-18 17:01:34.689291
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/babyshark_mimika
tz_powershell.xml
No Match in Event ID List
This event was created on:  2019-04-18 17:01:35.680716
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/babyshark_mimika
tz_powershell.xml
No Match in Event ID List
This event was created on:  2019-04-18 17:01:35.720774
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/babyshark_mimika
tz_powershell.xml
No Match in Event ID List
This event was created on:  2019-04-18 17:01:49.961250
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/babyshark_mimika
tz_powershell.xml
No Match in Event ID List
This event was created on:  2019-04-18 17:03:03.321806
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/babyshark_mimika
tz_powershell.xml
No Match in Event ID List
This event was created on:  2019-04-18 17:03:03.441978
An Event ID: 4915218456, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/MSSQL_multiple_f
ailed_logon_EventID_18456.xml
No Match in Event ID List
This event was created on:  2019-11-04 13:46:01.171339
An Event ID: 4915218456, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/MSSQL_multiple_f
ailed_logon_EventID_18456.xml
No Match in Event ID List
This event was created on:  2019-11-04 13:46:01.187637
An Event ID: 4915218456, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/MSSQL_multiple_f
ailed_logon_EventID_18456.xml
No Match in Event ID List
This event was created on:  2019-11-04 13:46:01.202730
```

```
An Event ID: 4915218456, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/MSSQL_multiple_f
ailed_logon_EventID_18456.xml
No Match in Event ID List
This event was created on:  2019-11-04 13:46:01.202730
An Event ID: 4915218456, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/MSSQL_multiple_f
ailed_logon_EventID_18456.xml
No Match in Event ID List
This event was created on:  2019-11-04 13:46:01.222452
An Event ID: 4915218456, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/MSSQL_multiple_f
ailed_logon_EventID_18456.xml
No Match in Event ID List
This event was created on:  2019-11-04 13:46:01.233944
An Event ID: 4915218456, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/MSSQL_multiple_f
ailed_logon_EventID_18456.xml
No Match in Event ID List
This event was created on:  2019-11-04 13:46:01.248423
An Event ID: 4915218456, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/MSSQL_multiple_f
ailed_logon_EventID_18456.xml
No Match in Event ID List
This event was created on:  2019-11-04 13:46:01.248882
An Event ID: 4915218456, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/MSSQL_multiple_f
ailed_logon_EventID_18456.xml
No Match in Event ID List
This event was created on:  2019-11-04 13:46:01.266434
An Event ID: 4915218456, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/MSSQL_multiple_f
ailed_logon_EventID_18456.xml
No Match in Event ID List
This event was created on:  2019-11-04 13:46:01.279825
An Event ID: 4662, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/CA_DCSync_4662.x
ml
Matched in Event ID List
This event was created on:  2019-05-08 02:10:43.487217
An Event ID: 4662, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/CA_DCSync_4662.x
ml
Matched in Event ID List
This event was created on:  2019-05-08 02:10:43.487217
An Event ID: 4662, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/CA_DCSync_4662.x
ml
Matched in Event ID List
This event was created on:  2019-05-08 02:10:43.487217
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/CA_keefarce_keep
ass_credump.xml
No Match in Event ID List
```

```
This event was created on:  2019-04-27 18:47:00.046848
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/CA_keefarce_keep
ass_credump.xml
No Match in Event ID List
This event was created on:  2019-04-27 18:47:00.062475
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/CA_keefarce_keep
ass_credump.xml
No Match in Event ID List
This event was created on:  2019-04-27 18:47:00.062475
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/CA_keefarce_keep
ass_credump.xml
No Match in Event ID List
This event was created on:  2019-04-27 18:47:00.062475
An Event ID: 5, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/CA_keefarce_keep
ass_credump.xml
No Match in Event ID List
This event was created on:  2019-04-27 18:47:00.124973
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/CA_sysmon_hashdu
mp_cmd_meterpreter.xml
No Match in Event ID List
This event was created on:  2019-04-30 12:43:43.784178
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/CA_sysmon_hashdu
mp_cmd_meterpreter.xml
No Match in Event ID List
This event was created on:  2019-04-30 12:43:43.784178
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/CA_sysmon_hashdu
mp_cmd_meterpreter.xml
No Match in Event ID List
This event was created on:  2019-04-30 12:43:43.784178
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/CA_sysmon_hashdu
mp_cmd_meterpreter.xml
No Match in Event ID List
This event was created on:  2019-04-30 12:43:43.784178
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/CA_sysmon_hashdu
mp_cmd_meterpreter.xml
No Match in Event ID List
This event was created on:  2019-04-30 12:43:43.784178
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/CA_sysmon_hashdu
mp_cmd_meterpreter.xml
No Match in Event ID List
This event was created on:  2019-04-30 12:43:43.784178
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/CA_sysmon_hashdu
mp_cmd_meterpreter.xml
```

```
No Match in Event ID List
This event was created on:  2019-04-30 12:43:43.784178
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/CA_sysmon_hashdu
mp_cmd_meterpreter.xml
No Match in Event ID List
This event was created on:  2019-04-30 12:43:43.784178
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/CA_sysmon_hashdu
mp_cmd_meterpreter.xml
No Match in Event ID List
This event was created on:  2019-04-30 12:43:43.784178
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/sysmon_10_11_lsa
ss_memdump.xml
No Match in Event ID List
This event was created on:  2019-03-17 19:09:41.328867
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/sysmon_10_11_lsa
ss_memdump.xml
No Match in Event ID List
This event was created on:  2019-03-17 19:09:41.328867
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/sysmon_10_11_lsa
ss_memdump.xml
No Match in Event ID List
This event was created on:  2019-03-17 19:10:03.991455
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/sysmon_10_11_lsa
ss_memdump.xml
No Match in Event ID List
This event was created on:  2019-03-17 19:10:03.991455
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/sysmon_13_keylog
ger_directx.xml
No Match in Event ID List
This event was created on:  2019-03-17 20:42:51.504059
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/sysmon_13_keylog
ger_directx.xml
No Match in Event ID List
This event was created on:  2019-03-17 20:42:51.504059
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/sysmon_13_keylog
ger_directx.xml
No Match in Event ID List
This event was created on:  2019-03-17 20:42:51.504059
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/sysmon_13_keylog
ger_directx.xml
No Match in Event ID List
This event was created on:  2019-03-17 20:42:51.504059
```

```
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/sysmon_13_keylog
ger_directx.xml
No Match in Event ID List
This event was created on:  2019-03-17 20:43:12.784658
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/sysmon_13_keylog
ger_directx.xml
No Match in Event ID List
This event was created on:  2019-03-17 20:43:16.309727
An Event ID: 0326, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/dc_applog_ntdsut
il_dfir_325_326_327.xml
No Match in Event ID List
This event was created on:  2019-11-26 23:55:00
An Event ID: 0325, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/dc_applog_ntdsut
il_dfir_325_326_327.xml
No Match in Event ID List
This event was created on:  2019-11-26 23:55:00
An Event ID: 0327, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/dc_applog_ntdsut
il_dfir_325_326_327.xml
No Match in Event ID List
This event was created on:  2019-11-26 23:55:02
An Event ID: 0327, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/dc_applog_ntdsut
il_dfir_325_326_327.xml
No Match in Event ID List
This event was created on:  2019-11-26 23:55:02
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/sysmon_10_1_memd
ump_comsvcs_minidump.xml
No Match in Event ID List
This event was created on:  2019-08-30 12:54:07.873791
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/sysmon_10_1_memd
ump_comsvcs_minidump.xml
No Match in Event ID List
This event was created on:  2019-08-30 12:54:08.171875
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/sysmon_10_1_memd
ump_comsvcs_minidump.xml
No Match in Event ID List
This event was created on:  2019-08-30 12:54:08.257122
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/sysmon_10_1_memd
ump_comsvcs_minidump.xml
No Match in Event ID List
This event was created on:  2019-08-30 12:54:08.354050
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/sysmon_10_1_memd
ump_comsvcs_minidump.xml
No Match in Event ID List
```

```
This event was created on:  2019-08-30 12:54:08.396725
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/sysmon_10_1_memd
ump_comsvcs_minidump.xml
No Match in Event ID List
This event was created on:  2019-08-30 12:54:08.439957
An Event ID: 3, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/sysmon_3_10_Invo
ke-Mimikatz_hosted_Github.xml
No Match in Event ID List
This event was created on:  2019-05-02 14:48:53.950750
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/sysmon_3_10_Invo
ke-Mimikatz_hosted_Github.xml
No Match in Event ID List
This event was created on:  2019-05-02 14:50:17.955524
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/sysmon_10_11_out
lfank_dumpert_and_andrewspecial_memdump.xml
No Match in Event ID List
This event was created on:  2019-06-21 07:35:37.185148
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/sysmon_10_11_out
lfank_dumpert_and_andrewspecial_memdump.xml
No Match in Event ID List
This event was created on:  2019-06-21 07:35:37.329185
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/sysmon_10_11_out
lfank_dumpert_and_andrewspecial_memdump.xml
No Match in Event ID List
This event was created on:  2019-06-21 07:35:37.329185
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/sysmon_10_11_out
lfank_dumpert_and_andrewspecial_memdump.xml
No Match in Event ID List
This event was created on:  2019-06-21 07:35:37.377197
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/sysmon_10_11_out
lfank_dumpert_and_andrewspecial_memdump.xml
No Match in Event ID List
This event was created on:  2019-06-21 07:35:50.128027
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/sysmon_10_11_out
lfank_dumpert_and_andrewspecial_memdump.xml
No Match in Event ID List
This event was created on:  2019-06-21 07:35:50.259077
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/sysmon_10_11_out
lfank_dumpert_and_andrewspecial_memdump.xml
No Match in Event ID List
This event was created on:  2019-06-21 07:35:50.259077
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/sysmon_10_11_out
lfank_dumpert_and_andrewspecial_memdump.xml
```

```
No Match in Event ID List
This event was created on:  2019-06-21 07:35:50.264109
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/sysmon_10_11_out
lfank_dumpert_and_andrewspecial_memdump.xml
No Match in Event ID List
This event was created on:  2019-06-21 07:35:50.729225
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/sysmon_10_11_out
lfank_dumpert_and_andrewspecial_memdump.xml
No Match in Event ID List
This event was created on:  2019-06-21 07:35:50.729225
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/sysmon_10_11_out
lfank_dumpert_and_andrewspecial_memdump.xml
No Match in Event ID List
This event was created on:  2019-06-21 07:35:50.749237
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/sysmon_10_11_out
lfank_dumpert_and_andrewspecial_memdump.xml
No Match in Event ID List
This event was created on:  2019-06-21 07:36:50.450184
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/sysmon_10_11_out
lfank_dumpert_and_andrewspecial_memdump.xml
No Match in Event ID List
This event was created on:  2019-06-21 07:36:51.681566
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/sysmon_10_11_out
lfank_dumpert_and_andrewspecial_memdump.xml
No Match in Event ID List
This event was created on:  2019-06-21 07:36:51.681566
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/sysmon_10_11_out
lfank_dumpert_and_andrewspecial_memdump.xml
No Match in Event ID List
This event was created on:  2019-06-21 07:36:51.682571
An Event ID: 17, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/sysmon17_18_keke
o_tsssp_default_np.xml
No Match in Event ID List
This event was created on:  2019-09-06 13:49:35.433683
An Event ID: 18, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/sysmon17_18_keke
o_tsssp_default_np.xml
No Match in Event ID List
This event was created on:  2019-09-06 13:49:39.823362
An Event ID: 18, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/sysmon17_18_keke
o_tsssp_default_np.xml
No Match in Event ID List
This event was created on:  2019-09-06 14:58:44.918619
```

```
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/sysmon_10_lsass_
mimikatz_sekurlsa_logonpasswords.xml
No Match in Event ID List
This event was created on:  2019-03-17 19:37:11.661928
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/discovery_sysmon
_1_iis_pwd_and_config_discovery_appcmd.xml
No Match in Event ID List
This event was created on:  2019-05-27 01:28:42.711006
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/discovery_sysmon
_1_iis_pwd_and_config_discovery_appcmd.xml
No Match in Event ID List
This event was created on:  2019-05-27 01:29:17.000311
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/discovery_sysmon
_1_iis_pwd_and_config_discovery_appcmd.xml
No Match in Event ID List
This event was created on:  2019-05-27 01:29:17.110470
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/discovery_sysmon
_1_iis_pwd_and_config_discovery_appcmd.xml
No Match in Event ID List
This event was created on:  2019-05-27 01:29:17.190584
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/discovery_sysmon
_1_iis_pwd_and_config_discovery_appcmd.xml
No Match in Event ID List
This event was created on:  2019-05-27 01:29:17.270700
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/discovery_sysmon
_1_iis_pwd_and_config_discovery_appcmd.xml
No Match in Event ID List
This event was created on:  2019-05-27 01:29:17.350815
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/discovery_sysmon
_1_iis_pwd_and_config_discovery_appcmd.xml
No Match in Event ID List
This event was created on:  2019-05-27 01:29:17.581146
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/discovery_sysmon
_1_iis_pwd_and_config_discovery_appcmd.xml
No Match in Event ID List
This event was created on:  2019-05-27 01:29:17.661263
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/discovery_sysmon
_1_iis_pwd_and_config_discovery_appcmd.xml
No Match in Event ID List
This event was created on:  2019-05-27 01:29:17.731363
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/discovery_sysmon
_1_iis_pwd_and_config_discovery_appcmd.xml
No Match in Event ID List
```

```
This event was created on:  2019-05-27 01:29:17.811478
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/discovery_sysmon
_1_iis_pwd_and_config_discovery_appcmd.xml
No Match in Event ID List
This event was created on:  2019-05-27 01:29:17.891594
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/discovery_sysmon
_1_iis_pwd_and_config_discovery_appcmd.xml
No Match in Event ID List
This event was created on:  2019-05-27 01:29:17.971708
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/discovery_sysmon
_1_iis_pwd_and_config_discovery_appcmd.xml
No Match in Event ID List
This event was created on:  2019-05-27 01:29:18.041809
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/discovery_sysmon
_1_iis_pwd_and_config_discovery_appcmd.xml
No Match in Event ID List
This event was created on:  2019-05-27 01:29:18.121923
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/discovery_sysmon
_1_iis_pwd_and_config_discovery_appcmd.xml
No Match in Event ID List
This event was created on:  2019-05-27 01:29:18.202040
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/discovery_sysmon
_1_iis_pwd_and_config_discovery_appcmd.xml
No Match in Event ID List
This event was created on:  2019-05-27 01:29:18.282154
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/discovery_sysmon
_1_iis_pwd_and_config_discovery_appcmd.xml
No Match in Event ID List
This event was created on:  2019-05-27 01:29:18.352255
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/discovery_sysmon
_1_iis_pwd_and_config_discovery_appcmd.xml
No Match in Event ID List
This event was created on:  2019-05-27 01:29:18.432371
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/discovery_sysmon
_1_iis_pwd_and_config_discovery_appcmd.xml
No Match in Event ID List
This event was created on:  2019-05-27 01:29:18.522501
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/discovery_sysmon
_1_iis_pwd_and_config_discovery_appcmd.xml
No Match in Event ID List
This event was created on:  2019-05-27 01:29:18.662703
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/discovery_sysmon
_1_iis_pwd_and_config_discovery_appcmd.xml
```

```
No Match in Event ID List
This event was created on:  2019-05-27 01:29:18.742817
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/discovery_sysmon
_1_iis_pwd_and_config_discovery_appcmd.xml
No Match in Event ID List
This event was created on:  2019-05-27 01:29:18.822931
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/discovery_sysmon
_1_iis_pwd_and_config_discovery_appcmd.xml
No Match in Event ID List
This event was created on:  2019-05-27 01:29:18.893032
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/discovery_sysmon
_1_iis_pwd_and_config_discovery_appcmd.xml
No Match in Event ID List
This event was created on:  2019-05-27 01:29:18.973148
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/discovery_sysmon
_1_iis_pwd_and_config_discovery_appcmd.xml
No Match in Event ID List
This event was created on:  2019-05-27 01:29:19.063278
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/discovery_sysmon
_1_iis_pwd_and_config_discovery_appcmd.xml
No Match in Event ID List
This event was created on:  2019-05-27 01:29:19.143393
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/discovery_sysmon
_1_iis_pwd_and_config_discovery_appcmd.xml
No Match in Event ID List
This event was created on:  2019-05-27 01:29:19.233522
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/discovery_sysmon
_1_iis_pwd_and_config_discovery_appcmd.xml
No Match in Event ID List
This event was created on:  2019-05-27 01:29:19.323652
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/discovery_sysmon
_1_iis_pwd_and_config_discovery_appcmd.xml
No Match in Event ID List
This event was created on:  2019-05-27 01:29:19.403767
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/discovery_sysmon
_1_iis_pwd_and_config_discovery_appcmd.xml
No Match in Event ID List
This event was created on:  2019-05-27 01:29:19.473867
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/discovery_sysmon
_1_iis_pwd_and_config_discovery_appcmd.xml
No Match in Event ID List
This event was created on:  2019-05-27 01:29:19.563997
```

```
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/discovery_sysmon
_1_iis_pwd_and_config_discovery_appcmd.xml
No Match in Event ID List
This event was created on:  2019-05-27 01:29:19.784315
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/discovery_sysmon
_1_iis_pwd_and_config_discovery_appcmd.xml
No Match in Event ID List
This event was created on:  2019-05-27 01:29:19.894472
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/discovery_sysmon
_1_iis_pwd_and_config_discovery_appcmd.xml
No Match in Event ID List
This event was created on:  2019-05-27 01:29:19.964573
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/discovery_sysmon
_1_iis_pwd_and_config_discovery_appcmd.xml
No Match in Event ID List
This event was created on:  2019-05-27 01:29:20.034674
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/discovery_sysmon
_1_iis_pwd_and_config_discovery_appcmd.xml
No Match in Event ID List
This event was created on:  2019-05-27 01:29:20.124804
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/discovery_sysmon
_1_iis_pwd_and_config_discovery_appcmd.xml
No Match in Event ID List
This event was created on:  2019-05-27 01:29:20.204920
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/discovery_sysmon
_1_iis_pwd_and_config_discovery_appcmd.xml
No Match in Event ID List
This event was created on:  2019-05-27 01:29:20.305063
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/discovery_sysmon
_1_iis_pwd_and_config_discovery_appcmd.xml
No Match in Event ID List
This event was created on:  2019-05-27 01:29:20.435251
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/discovery_sysmon
_1_iis_pwd_and_config_discovery_appcmd.xml
No Match in Event ID List
This event was created on:  2019-05-27 01:29:20.555424
An Event ID: 1102, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 09:09:14.916618
An Event ID: 4662, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
```

```
This event was created on:  2019-03-25 10:05:30.695604
An Event ID: 4662, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 10:33:53.024616
An Event ID: 5136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 10:33:56.457630
An Event ID: 5136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 10:33:56.457630
An Event ID: 4662, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 10:34:07.385616
An Event ID: 5136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 10:34:16.458632
An Event ID: 5136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 10:34:16.458632
An Event ID: 4662, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 10:35:09.463610
An Event ID: 5136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 10:35:16.462616
An Event ID: 5136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 10:35:16.462616
An Event ID: 4662, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 10:35:30.873621
An Event ID: 5136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
```

```
Matched in Event ID List
This event was created on:  2019-03-25 10:35:36.463627
An Event ID: 5136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 10:35:36.463627
An Event ID: 4719, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 10:36:03.974607
An Event ID: 4719, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 10:36:03.974607
An Event ID: 4662, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 11:05:30.695618
An Event ID: 4662, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 11:14:33.721634
An Event ID: 4662, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 11:14:42.489624
An Event ID: 5136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 11:14:43.566645
An Event ID: 5136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 11:14:43.566645
An Event ID: 5136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 11:14:43.566645
An Event ID: 5136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 11:14:43.566645
```

```
An Event ID: 4719, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 11:14:50.755610
An Event ID: 4719, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 11:14:50.755610
An Event ID: 4738, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 11:15:58.239601
An Event ID: 4662, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 11:18:39.465626
An Event ID: 5136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 11:18:40.768633
An Event ID: 5136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 11:18:40.768633
An Event ID: 4662, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 11:19:07.186630
An Event ID: 5136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 11:19:10.770607
An Event ID: 5136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 11:19:10.770607
An Event ID: 4719, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 11:19:22.590620
An Event ID: 4719, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
```

```
This event was created on:  2019-03-25 11:19:22.590620
An Event ID: 4738, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 11:19:35.820604
An Event ID: 4702, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 11:22:45.080608
An Event ID: 4702, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 11:52:45.143618
An Event ID: 4662, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 12:05:30.683609
An Event ID: 4702, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 12:22:45.317606
An Event ID: 4662, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 12:31:35.143635
An Event ID: 5136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 12:31:44.810604
An Event ID: 5136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 12:31:44.810604
An Event ID: 4662, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 12:33:36.036642
An Event ID: 4662, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 12:33:40.714643
An Event ID: 5136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
```

```
Matched in Event ID List
This event was created on:  2019-03-25 12:33:44.816656
An Event ID: 5136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 12:33:44.816656
An Event ID: 5136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 12:33:44.816656
An Event ID: 5136, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 12:33:44.816656
An Event ID: 4719, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 12:33:59.275612
An Event ID: 4719, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 12:33:59.275612
An Event ID: 4738, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 12:37:49.638676
An Event ID: 4738, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 12:48:09.195618
An Event ID: 4702, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 12:52:45.500610
An Event ID: 4738, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 13:01:41.932610
An Event ID: 4742, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/ACL_ForcePwd_SPN
Add_User_Computer_Accounts.xml
Matched in Event ID List
This event was created on:  2019-03-25 13:01:41.935604
```

```
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/CA_keepass_KeeTh
ief_Get-KeePassDatabaseKey.xml
No Match in Event ID List
This event was created on:  2019-04-27 18:55:04.710608
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/CA_keepass_KeeTh
ief_Get-KeePassDatabaseKey.xml
No Match in Event ID List
This event was created on:  2019-04-27 18:55:04.980137
An Event ID: 1102, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/CA_chrome_firefo
x_opera_4663.xml
Matched in Event ID List
This event was created on:  2019-04-27 19:27:55.274059
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/CA_chrome_firefo
x_opera_4663.xml
Matched in Event ID List
This event was created on:  2019-04-27 19:31:15.355062
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/CA_chrome_firefo
x_opera_4663.xml
Matched in Event ID List
This event was created on:  2019-04-27 19:33:05.308187
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/CA_chrome_firefo
x_opera_4663.xml
Matched in Event ID List
This event was created on:  2019-04-27 19:33:18.699755
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/CA_chrome_firefo
x_opera_4663.xml
Matched in Event ID List
This event was created on:  2019-04-27 19:33:50.134295
An Event ID: 4104, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/phish_windows_cr
edentials_powershell_scriptblockLog_4104.xml
No Match in Event ID List
This event was created on:  2019-09-09 13:35:08.655802
An Event ID: 4104, was found in file
/home/user/CI5235_Coursework/evtx_logs/Credential_Access/phish_windows_cr
edentials_powershell_scriptblockLog_4104.xml
No Match in Event ID List
This event was created on:  2019-09-09 13:35:09.315229
An Event ID: 1102, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:07.524200
An Event ID: 5156, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
```

```
This event was created on:  2019-03-19 23:35:08.786015
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:14.634424
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:14.634424
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:14.764612
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:14.764612
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:14.904814
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:14.904814
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.045015
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.045015
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.185217
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.185217
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
```

```
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.205246
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.215260
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.215260
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.215260
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.295376
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.295376
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.295376
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.295376
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.295376
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.295376
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.295376
```

```
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.295376
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.295376
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.295376
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.295376
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.295376
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.295376
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.295376
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.295376
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.295376
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.295376
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
```

```
This event was created on:  2019-03-19 23:35:15.295376
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.295376
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.295376
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.295376
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.295376
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.315405
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.315405
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.315405
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.315405
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.315405
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.315405
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
```

```
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.315405
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.315405
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.315405
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.315405
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.315405
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.315405
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.315405
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.315405
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.315405
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.315405
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.315405
```

```
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.315405
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.325418
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.325418
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.325418
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.325418
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.325418
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.325418
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.325418
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.325418
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.325418
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
```

```
This event was created on:  2019-03-19 23:35:15.325418
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.325418
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.325418
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.325418
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.325418
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.325418
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.325418
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.325418
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.325418
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.325418
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.325418
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
```

```
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.325418
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.325418
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.325418
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.325418
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.325418
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.325418
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.325418
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.325418
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.325418
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.325418
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.335432
```

```
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.335432
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.335432
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.335432
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.335432
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.335432
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.335432
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.335432
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.335432
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.335432
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.335432
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
```

```
This event was created on:  2019-03-19 23:35:15.335432
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.335432
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.335432
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.335432
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.335432
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.335432
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.335432
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.335432
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.335432
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.335432
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.335432
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
```

```
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.365477
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.365477
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.365477
An Event ID: 4663, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_1102_security_l
og_cleared.xml
Matched in Event ID List
This event was created on:  2019-03-19 23:35:15.365477
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_powershell_exec
policy_changed_sysmon_13.xml
No Match in Event ID List
This event was created on:  2019-05-24 15:38:21.485899
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_powershell_exec
policy_changed_sysmon_13.xml
No Match in Event ID List
This event was created on:  2019-05-24 15:38:58.238747
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_powershell_exec
policy_changed_sysmon_13.xml
No Match in Event ID List
This event was created on:  2019-05-24 15:38:58.489107
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_powershell_exec
policy_changed_sysmon_13.xml
No Match in Event ID List
This event was created on:  2019-05-24 15:38:58.529163
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_powershell_exec
policy_changed_sysmon_13.xml
No Match in Event ID List
This event was created on:  2019-05-24 15:38:58.569221
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/apt10_jjs_sideload
ing_prochollowing_persist_as_service_sysmon_1_7_8_13.xml
No Match in Event ID List
This event was created on:  2019-05-26 04:01:42.385506
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/apt10_jjs_sideload
ing_prochollowing_persist_as_service_sysmon_1_7_8_13.xml
No Match in Event ID List
This event was created on:  2019-05-26 04:01:42.545736
```

```
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/apt10_jjs_sideload
ing_prochollowing_persist_as_service_sysmon_1_7_8_13.xml
No Match in Event ID List
This event was created on:  2019-05-26 04:01:42.625851
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/apt10_jjs_sideload
ing_prochollowing_persist_as_service_sysmon_1_7_8_13.xml
No Match in Event ID List
This event was created on:  2019-05-26 04:01:42.645880
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/apt10_jjs_sideload
ing_prochollowing_persist_as_service_sysmon_1_7_8_13.xml
No Match in Event ID List
This event was created on:  2019-05-26 04:01:42.966341
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/apt10_jjs_sideload
ing_prochollowing_persist_as_service_sysmon_1_7_8_13.xml
No Match in Event ID List
This event was created on:  2019-05-26 04:01:42.966341
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/apt10_jjs_sideload
ing_prochollowing_persist_as_service_sysmon_1_7_8_13.xml
No Match in Event ID List
This event was created on:  2019-05-26 04:01:43.567204
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/apt10_jjs_sideload
ing_prochollowing_persist_as_service_sysmon_1_7_8_13.xml
No Match in Event ID List
This event was created on:  2019-05-26 04:01:43.567204
An Event ID: 5, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/apt10_jjs_sideload
ing_prochollowing_persist_as_service_sysmon_1_7_8_13.xml
No Match in Event ID List
This event was created on:  2019-05-26 04:01:44.047895
An Event ID: 5, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/apt10_jjs_sideload
ing_prochollowing_persist_as_service_sysmon_1_7_8_13.xml
No Match in Event ID List
This event was created on:  2019-05-26 04:01:44.598688
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/apt10_jjs_sideload
ing_prochollowing_persist_as_service_sysmon_1_7_8_13.xml
No Match in Event ID List
This event was created on:  2019-05-26 04:01:47.082258
An Event ID: 1638415457, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_xp_cmdshell_ena
bled_MSSQL_EID_15457.xml
No Match in Event ID List
This event was created on:  2019-11-04 09:27:26.143063
An Event ID: 1638415457, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_xp_cmdshell_ena
bled_MSSQL_EID_15457.xml
No Match in Event ID List
```

```
This event was created on:  2019-11-04 09:27:26.158621
An Event ID: 1638415457, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_xp_cmdshell_ena
bled_MSSQL_EID_15457.xml
No Match in Event ID List
This event was created on:  2019-11-04 09:27:26.315067
An Event ID: 1638415457, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_xp_cmdshell_ena
bled_MSSQL_EID_15457.xml
No Match in Event ID List
This event was created on:  2019-11-04 09:27:26.315067
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_portforward_net
sh_rdp_sysmon_13_1.xml
No Match in Event ID List
This event was created on:  2019-05-23 17:45:34.538296
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_portforward_net
sh_rdp_sysmon_13_1.xml
No Match in Event ID List
This event was created on:  2019-05-23 17:46:04.671625
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_portforward_net
sh_rdp_sysmon_13_1.xml
No Match in Event ID List
This event was created on:  2019-05-23 17:46:05.022129
An Event ID: 104, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_104_system_log_
cleared.xml
No Match in Event ID List
This event was created on:  2019-03-19 23:34:25.894341
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_PsScriptBlockLo
gging_disabled_sysmon12_13.xml
No Match in Event ID List
This event was created on:  2019-05-19 18:05:07.719919
An Event ID: 12, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_PsScriptBlockLo
gging_disabled_sysmon12_13.xml
No Match in Event ID List
This event was created on:  2019-05-19 18:05:33.454296
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/sysmon_13_rdp_sett
ings_tampering.xml
No Match in Event ID List
This event was created on:  2019-03-17 20:17:44.537010
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/sysmon_13_rdp_sett
ings_tampering.xml
No Match in Event ID List
This event was created on:  2019-03-17 20:17:44.637156
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/sysmon_13_rdp_sett
ings_tampering.xml
```

```
No Match in Event ID List
This event was created on:  2019-03-17 20:17:44.797384
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/sysmon_13_rdp_sett
ings_tampering.xml
No Match in Event ID List
This event was created on:  2019-03-17 20:17:45.478365
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/sysmon_13_rdp_sett
ings_tampering.xml
No Match in Event ID List
This event was created on:  2019-03-17 20:17:45.628580
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/sysmon_13_rdp_sett
ings_tampering.xml
No Match in Event ID List
This event was created on:  2019-03-17 20:17:45.648609
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/sysmon_13_rdp_sett
ings_tampering.xml
No Match in Event ID List
This event was created on:  2019-03-17 20:17:52.949106
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/sysmon_13_rdp_sett
ings_tampering.xml
No Match in Event ID List
This event was created on:  2019-03-17 20:17:52.979149
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/sysmon_13_rdp_sett
ings_tampering.xml
No Match in Event ID List
This event was created on:  2019-03-17 20:18:05.086559
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/sysmon_13_rdp_sett
ings_tampering.xml
No Match in Event ID List
This event was created on:  2019-03-17 20:18:09.282593
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/sysmon_13_rdp_sett
ings_tampering.xml
No Match in Event ID List
This event was created on:  2019-03-17 20:18:09.282593
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/sysmon_13_rdp_sett
ings_tampering.xml
No Match in Event ID List
This event was created on:  2019-03-17 20:18:09.312635
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/sysmon_13_rdp_sett
ings_tampering.xml
No Match in Event ID List
This event was created on:  2019-03-17 20:18:09.643112
```

```
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/sysmon_13_rdp_sett
ings_tampering.xml
No Match in Event ID List
This event was created on:  2019-03-17 20:18:12.096640
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/sysmon_13_rdp_sett
ings_tampering.xml
No Match in Event ID List
This event was created on:  2019-03-17 20:20:14.512665
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/sysmon_13_rdp_sett
ings_tampering.xml
No Match in Event ID List
This event was created on:  2019-03-17 20:20:17.907547
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/sysmon_13_rdp_sett
ings_tampering.xml
No Match in Event ID List
This event was created on:  2019-03-17 20:20:17.917561
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/sysmon_13_rdp_sett
ings_tampering.xml
No Match in Event ID List
This event was created on:  2019-03-17 20:20:17.927576
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/sysmon_13_rdp_sett
ings_tampering.xml
No Match in Event ID List
This event was created on:  2019-03-17 20:22:59.399761
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/sysmon_13_rdp_sett
ings_tampering.xml
No Match in Event ID List
This event was created on:  2019-03-17 20:23:12.188150
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/process_suspend_sy
smon_10_ga_800.xml
No Match in Event ID List
This event was created on:  2019-04-28 16:29:42.988125
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_UAC_Disabled_Sy
smon_12_13.xml
No Match in Event ID List
This event was created on:  2019-05-16 14:17:15.762709
An Event ID: 12, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_UAC_Disabled_Sy
smon_12_13.xml
No Match in Event ID List
This event was created on:  2019-05-16 14:17:15.763712
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_UAC_Disabled_Sy
smon_12_13.xml
No Match in Event ID List
```

```
This event was created on:  2019-05-16 14:17:15.763712
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_sysmon_13_VBA_S
ecurity_AccessVBOM.xml
No Match in Event ID List
This event was created on:  2019-05-15 04:18:40.474644
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/sysmon_2_11_evasio
n_timestomp_MACE.xml
No Match in Event ID List
This event was created on:  2019-04-30 10:12:45.583363
An Event ID: 2, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/sysmon_2_11_evasio
n_timestomp_MACE.xml
No Match in Event ID List
This event was created on:  2019-04-30 10:13:42.052113
An Event ID: 12, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_Powershell_CLM_
Disabled_Sysmon_12.xml
No Match in Event ID List
This event was created on:  2019-05-16 13:10:13.760916
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/meterpreter_migrat
e_to_explorer_sysmon_8.xml
No Match in Event ID List
This event was created on:  2019-04-30 07:26:34.133638
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:08.348797
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:16.176922
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:16.208170
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:16.223797
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:16.255045
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
```

```
No Match in Event ID List
This event was created on:  2019-05-18 17:16:16.270672
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:16.286295
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:16.317545
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:16.333170
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:16.348797
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:16.364420
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:16.380045
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:16.395672
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:16.411295
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:16.426922
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:16.458170
```

```
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:16.473797
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:16.489420
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:16.505045
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:16.520672
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:16.536295
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:16.551922
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:16.567545
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:16.583170
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:16.598797
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:16.614420
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
```

```
This event was created on:  2019-05-18 17:16:16.630045
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:16.661295
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:16.692545
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:16.708170
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:16.723797
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:16.739420
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:16.755045
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:16.770672
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:16.801922
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:16.817545
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:16.833170
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
```

```
No Match in Event ID List
This event was created on:  2019-05-18 17:16:16.848797
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:16.864420
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:16.880045
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:16.895672
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:16.926922
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:16.942545
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:16.973797
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:16.989420
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:17.005045
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:17.020672
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:17.036295
```

```
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:17.051922
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:17.083170
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:17.098797
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:17.114420
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:17.130045
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:17.145672
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:17.161295
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:17.176922
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:17.192545
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:17.208170
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
```

```
This event was created on:  2019-05-18 17:16:17.223797
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:17.239420
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:17.270672
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:17.286295
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:17.301922
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:17.317545
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:17.348797
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:17.364420
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:17.380045
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:17.395672
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:17.426922
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
```

```
No Match in Event ID List
This event was created on:  2019-05-18 17:16:17.442545
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:17.489420
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:17.505045
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:17.520672
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:17.536295
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:17.551922
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:17.567545
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:17.567545
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:17.583170
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:17.598797
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:17.614420
```

```
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:17.661295
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:17.708170
An Event ID: 8, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:17.786295
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_unmanagedpowers
hell_psinject_sysmon_7_8_10.xml
No Match in Event ID List
This event was created on:  2019-05-18 17:16:18.833170
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_timestomp_and_d
ll_sideloading_and_RunPersist.xml
No Match in Event ID List
This event was created on:  2019-04-27 15:57:25.868864
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_timestomp_and_d
ll_sideloading_and_RunPersist.xml
No Match in Event ID List
This event was created on:  2019-04-27 15:57:27.087612
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_timestomp_and_d
ll_sideloading_and_RunPersist.xml
No Match in Event ID List
This event was created on:  2019-04-27 15:57:53.368864
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_timestomp_and_d
ll_sideloading_and_RunPersist.xml
No Match in Event ID List
This event was created on:  2019-04-27 15:57:53.587612
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_timestomp_and_d
ll_sideloading_and_RunPersist.xml
No Match in Event ID List
This event was created on:  2019-04-27 15:57:53.650112
An Event ID: 2, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_timestomp_and_d
ll_sideloading_and_RunPersist.xml
No Match in Event ID List
This event was created on:  2019-04-27 15:57:53.650112
An Event ID: 11, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_timestomp_and_d
ll_sideloading_and_RunPersist.xml
No Match in Event ID List
```

```
This event was created on:  2019-04-27 15:57:53.650112
An Event ID: 2, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_timestomp_and_d
ll_sideloading_and_RunPersist.xml
No Match in Event ID List
This event was created on:  2019-04-27 15:57:53.650112
An Event ID: 2, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_timestomp_and_d
ll_sideloading_and_RunPersist.xml
No Match in Event ID List
This event was created on:  2019-04-27 15:57:53.650112
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_timestomp_and_d
ll_sideloading_and_RunPersist.xml
No Match in Event ID List
This event was created on:  2019-04-27 15:57:53.837612
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_timestomp_and_d
ll_sideloading_and_RunPersist.xml
No Match in Event ID List
This event was created on:  2019-04-27 15:57:53.837612
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_timestomp_and_d
ll_sideloading_and_RunPersist.xml
No Match in Event ID List
This event was created on:  2019-04-27 15:57:53.837612
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_timestomp_and_d
ll_sideloading_and_RunPersist.xml
No Match in Event ID List
This event was created on:  2019-04-27 15:57:53.837612
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_timestomp_and_d
ll_sideloading_and_RunPersist.xml
No Match in Event ID List
This event was created on:  2019-04-27 15:57:53.853237
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_timestomp_and_d
ll_sideloading_and_RunPersist.xml
No Match in Event ID List
This event was created on:  2019-04-27 15:57:53.853237
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_timestomp_and_d
ll_sideloading_and_RunPersist.xml
No Match in Event ID List
This event was created on:  2019-04-27 15:57:53.868864
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_timestomp_and_d
ll_sideloading_and_RunPersist.xml
No Match in Event ID List
This event was created on:  2019-04-27 15:57:53.868864
An Event ID: 7, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_timestomp_and_d
ll_sideloading_and_RunPersist.xml
```

```
No Match in Event ID List
This event was created on:  2019-04-27 15:57:53.868864
An Event ID: 13, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_timestomp_and_d
ll_sideloading_and_RunPersist.xml
No Match in Event ID List
This event was created on:  2019-04-27 15:57:53.884487
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_timestomp_and_d
ll_sideloading_and_RunPersist.xml
No Match in Event ID List
This event was created on:  2019-04-27 15:57:53.931362
An Event ID: 10, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_timestomp_and_d
ll_sideloading_and_RunPersist.xml
No Match in Event ID List
This event was created on:  2019-04-27 15:57:53.931362
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_timestomp_and_d
ll_sideloading_and_RunPersist.xml
No Match in Event ID List
This event was created on:  2019-04-27 15:57:54.134487
An Event ID: 5, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/DE_timestomp_and_d
ll_sideloading_and_RunPersist.xml
No Match in Event ID List
This event was created on:  2019-04-27 15:57:54.165737
An Event ID: 1, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/de_hiding_files_vi
a_attrib_cmdlet.xml
No Match in Event ID List
This event was created on:  2019-05-19 17:32:00.482983
An Event ID: 4985, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/Win_4985_T1186_Pro
cess_Doppelganging.xml
Matched in Event ID List
This event was created on:  2019-08-14 14:06:44.495674
An Event ID: 4985, was found in file
/home/user/CI5235_Coursework/evtx_logs/Defense_Evasion/Win_4985_T1186_Pro
cess_Doppelganging.xml
Matched in Event ID List
This event was created on:  2019-08-14 14:06:44.849884
An Event ID: 131, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:16:28.543879
An Event ID: 65, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:16:28.546169
```

```
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:16:28.548439
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:16:28.548452
An Event ID: 141, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:16:28.549456
An Event ID: 143, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:16:34.851925
An Event ID: 226, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:16:34.851971
An Event ID: 142, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:16:34.851986
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:16:34.852436
An Event ID: 102, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:16:34.852451
An Event ID: 145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:16:34.852455
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:16:34.852505
An Event ID: 103, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
```

```
This event was created on:  2019-08-27 17:16:34.852505
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:16:34.852510
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:16:34.852516
An Event ID: 131, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:42.659937
An Event ID: 65, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:42.662613
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:42.665415
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:42.665430
An Event ID: 141, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:42.666792
An Event ID: 143, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:42.684162
An Event ID: 226, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:42.684210
An Event ID: 142, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:42.684229
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
```

```
No Match in Event ID List
This event was created on:  2019-08-27 17:17:42.684807
An Event ID: 102, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:42.684826
An Event ID: 145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:42.684828
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:42.684835
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:42.684839
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:42.684843
An Event ID: 103, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:42.684856
An Event ID: 131, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:44.948782
An Event ID: 65, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:44.952095
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:44.956211
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:44.956255
```

```
An Event ID: 141, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:44.958157
An Event ID: 101, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:45.621407
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:45.621433
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:45.621445
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:45.621473
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:45.621618
An Event ID: 104, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:45.622038
An Event ID: 71, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:45.622046
An Event ID: 227, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:45.622335
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:45.622351
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
```

```
This event was created on:  2019-08-27 17:17:45.623693
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:45.623751
An Event ID: 98, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:45.624254
An Event ID: 100, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:45.624260
An Event ID: 135, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:45.624287
An Event ID: 130, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:45.625322
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:45.626534
An Event ID: 131, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:45.647913
An Event ID: 66, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:46.547380
An Event ID: 33, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:46.553440
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:46.553442
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
```

```
No Match in Event ID List
This event was created on:  2019-08-27 17:17:46.567173
An Event ID: 135, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:46.567417
An Event ID: 169, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:46.567652
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:46.567978
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:46.567982
An Event ID: 135, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:46.568399
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:46.568485
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:46.571623
An Event ID: 162, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:46.742779
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:46.751617
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:46.754324
```

```
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:46.754370
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:47.401146
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:47.416897
An Event ID: 168, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:47.421539
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:47.617830
An Event ID: 68, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:47.625961
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:47.627583
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:47.875929
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:48.098223
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:48.118258
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
```

```
This event was created on:  2019-08-27 17:17:48.161579
An Event ID: 227, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:48.480997
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:49.145441
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:49.145576
An Event ID: 227, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:49.145603
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:49.157368
An Event ID: 227, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:49.157740
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:49.157921
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:49.236879
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:49.548286
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:49.758976
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
```

```
No Match in Event ID List
This event was created on:  2019-08-27 17:17:49.816111
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:50.112074
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:51.994240
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:53.201986
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:55.038021
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:17:57.029985
An Event ID: 228, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:26:41.767599
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:26:41.767616
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:26:41.767632
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:26:41.772884
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:26:41.772888
```

```
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:26:41.784435
An Event ID: 103, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:26:41.784929
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:26:41.816319
An Event ID: 143, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:26:41.829224
An Event ID: 226, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:26:41.829256
An Event ID: 142, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:26:41.829273
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:26:41.866907
An Event ID: 102, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:26:41.866940
An Event ID: 145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:26:41.866941
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:26:41.866949
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
```

```
This event was created on:  2019-08-27 17:26:41.866955
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:26:41.866959
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:26:41.867214
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:26:41.867237
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:26:41.867243
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:26:41.867249
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:26:41.867256
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:26:41.870134
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:26:41.870150
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:26:41.870157
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:26:41.870165
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
```

```
No Match in Event ID List
This event was created on:  2019-08-27 17:26:41.870939
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:26:41.870977
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:26:41.872190
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:26:41.872511
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:26:41.873337
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:26:41.873816
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:26:41.874819
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:26:41.875307
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:26:41.875984
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:26:41.876690
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-27 17:26:41.877310
```

```
An Event ID: 229, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 03:36:49.647284
An Event ID: 227, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 03:36:49.647339
An Event ID: 229, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 03:36:49.647356
An Event ID: 229, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 03:36:49.826771
An Event ID: 70, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 03:36:49.826775
An Event ID: 129, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 03:36:49.907396
An Event ID: 129, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 03:36:49.907570
An Event ID: 129, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 03:36:49.997723
An Event ID: 129, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 03:36:49.999348
An Event ID: 229, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 18:59:59.825874
An Event ID: 227, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
```

```
This event was created on:  2019-08-28 18:59:59.825935
An Event ID: 229, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 18:59:59.825951
An Event ID: 229, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 18:59:59.972883
An Event ID: 70, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 18:59:59.972885
An Event ID: 129, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 18:59:59.999935
An Event ID: 129, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 19:00:00.000151
An Event ID: 129, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 19:00:00.013855
An Event ID: 129, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 19:00:00.015667
An Event ID: 131, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:52.049362
An Event ID: 65, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:52.062550
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:52.065178
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
```

```
No Match in Event ID List
This event was created on:  2019-08-28 10:02:52.065191
An Event ID: 141, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:52.079420
An Event ID: 142, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:52.171679
An Event ID: 143, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:52.171680
An Event ID: 226, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:52.171728
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:52.172186
An Event ID: 102, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:52.172249
An Event ID: 145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:52.172253
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:52.172258
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:52.172264
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:52.172266
```

```
An Event ID: 103, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:52.172291
An Event ID: 131, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:54.594028
An Event ID: 65, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:54.608280
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:54.616022
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:54.616045
An Event ID: 141, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:54.623096
An Event ID: 101, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:55.034092
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:55.034121
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:55.034134
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:55.034166
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
```

```
This event was created on:  2019-08-28 10:02:55.035675
An Event ID: 104, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:55.037159
An Event ID: 71, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:55.037169
An Event ID: 227, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:55.038342
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:55.038370
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:55.041475
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:55.041615
An Event ID: 98, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:55.041983
An Event ID: 100, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:55.041988
An Event ID: 135, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:55.042017
An Event ID: 130, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:55.043068
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
```

```
No Match in Event ID List
This event was created on:  2019-08-28 10:02:55.045151
An Event ID: 131, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:55.075224
An Event ID: 66, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:55.898117
An Event ID: 33, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:55.938219
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:55.938782
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:55.960373
An Event ID: 135, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:55.960571
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:55.960899
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:55.960901
An Event ID: 169, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:55.961475
An Event ID: 135, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:55.961624
```

```
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:55.961754
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:55.965504
An Event ID: 162, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:56.943882
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:57.006348
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:57.006559
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:57.006565
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:57.206612
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:57.218672
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:57.310715
An Event ID: 168, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:57.313540
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
```

```
This event was created on:  2019-08-28 10:02:57.579079
An Event ID: 227, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:57.739267
An Event ID: 68, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:58.219519
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:58.222162
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:58.340822
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:58.343098
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:58.344133
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:58.505753
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:58.505932
An Event ID: 227, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:58.506155
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:58.529013
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
```

```
No Match in Event ID List
This event was created on:  2019-08-28 10:02:58.581463
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:58.603285
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:58.603336
An Event ID: 227, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:58.603401
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:59.042809
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:02:59.068663
An Event ID: 107, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:07:43.924049
An Event ID: 226, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:07:43.924559
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:07:44.045027
An Event ID: 102, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:07:44.045467
An Event ID: 145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:07:44.045473
```

```
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:07:44.045485
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:07:44.045490
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:07:44.045498
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:07:44.045523
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:07:44.045527
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:07:44.045851
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:07:44.045879
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:07:44.045898
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:07:44.045902
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:07:44.045925
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
```

```
This event was created on:  2019-08-28 10:07:44.045935
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:07:44.045942
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:07:44.046436
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:07:44.046455
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:07:44.046688
An Event ID: 228, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:07:44.046722
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:07:44.046728
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:07:44.046738
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:07:44.047239
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:07:44.047523
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:07:44.047920
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
```

```
No Match in Event ID List
This event was created on:  2019-08-28 10:07:44.092049
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:07:44.092054
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:07:44.095476
An Event ID: 103, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 10:07:44.095484
An Event ID: 131, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:28.567844
An Event ID: 65, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:28.569815
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:28.572178
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:28.572189
An Event ID: 141, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:28.573231
An Event ID: 143, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:28.632364
An Event ID: 226, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:28.632406
```

```
An Event ID: 142, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:28.632460
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:28.632847
An Event ID: 102, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:28.632860
An Event ID: 145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:28.632862
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:28.632868
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:28.632874
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:28.632875
An Event ID: 103, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:28.632971
An Event ID: 131, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:31.117966
An Event ID: 65, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:31.128525
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
```

```
This event was created on:  2019-08-28 13:42:31.141161
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:31.141207
An Event ID: 141, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:31.146120
An Event ID: 101, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:32.091261
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:32.091290
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:32.091307
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:32.091337
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:32.091518
An Event ID: 104, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:32.091930
An Event ID: 71, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:32.091946
An Event ID: 227, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:32.092123
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
```

```
No Match in Event ID List
This event was created on:  2019-08-28 13:42:32.092138
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:32.093397
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:32.093559
An Event ID: 98, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:32.094490
An Event ID: 100, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:32.094498
An Event ID: 135, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:32.094530
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:32.095062
An Event ID: 130, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:32.095655
An Event ID: 131, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:32.133560
An Event ID: 66, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:32.648924
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:32.653196
```

```
An Event ID: 33, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:32.653240
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:32.667931
An Event ID: 135, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:32.668625
An Event ID: 169, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:32.669275
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:32.669603
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:32.669605
An Event ID: 135, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:32.669683
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:32.670603
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:32.672911
An Event ID: 162, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:33.484566
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
```

```
This event was created on:  2019-08-28 13:42:33.506128
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:33.517904
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:33.518063
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:33.663103
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:33.670704
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:33.802269
An Event ID: 168, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:33.841494
An Event ID: 68, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:34.083382
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:34.088589
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:34.096851
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:34.141495
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
```

```
No Match in Event ID List
This event was created on:  2019-08-28 13:42:34.176392
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:34.184328
An Event ID: 227, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:34.245193
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:34.625687
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:34.625977
An Event ID: 227, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:34.626001
An Event ID: 227, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:34.688728
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:34.689238
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:34.689390
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:34.701433
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:34.744837
```

```
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:34.944834
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:42:34.993677
An Event ID: 228, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:57:47.556559
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:57:47.556570
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:57:47.556583
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:57:47.559168
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:57:47.559170
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:57:47.677689
An Event ID: 103, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:57:47.677696
An Event ID: 142, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:57:47.678234
An Event ID: 226, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
```

```
This event was created on:  2019-08-28 13:57:47.678255
An Event ID: 143, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:57:47.684361
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:57:47.697565
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:57:47.699562
An Event ID: 102, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:57:47.699591
An Event ID: 145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:57:47.699593
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:57:47.699600
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:57:47.699604
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:57:47.699610
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:57:47.699955
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:57:47.700211
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
```

```
No Match in Event ID List
This event was created on:  2019-08-28 13:57:47.700216
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:57:47.700222
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:57:47.700228
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:57:47.703621
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:57:47.703632
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:57:47.703638
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:57:47.703644
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:57:47.704176
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:57:47.704191
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:57:47.705780
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:57:47.706978
```

```
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:57:47.708944
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:57:47.709391
An Event ID: 131, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:34.152891
An Event ID: 65, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:34.155205
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:34.157835
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:34.157852
An Event ID: 141, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:34.159256
An Event ID: 142, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:34.188311
An Event ID: 143, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:34.188311
An Event ID: 226, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:34.188351
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
```

```
This event was created on:  2019-08-28 13:58:34.188831
An Event ID: 102, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:34.188848
An Event ID: 145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:34.188852
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:34.188856
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:34.188862
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:34.188866
An Event ID: 103, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:34.188866
An Event ID: 131, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:35.380169
An Event ID: 65, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:35.383442
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:35.386803
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:35.386818
An Event ID: 141, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
```

```
No Match in Event ID List
This event was created on:  2019-08-28 13:58:35.388456
An Event ID: 101, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:35.453152
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:35.453165
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:35.453171
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:35.453182
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:35.453243
An Event ID: 104, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:35.453411
An Event ID: 71, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:35.453415
An Event ID: 227, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:35.453484
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:35.453489
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:35.454020
```

```
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:35.454063
An Event ID: 98, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:35.454187
An Event ID: 100, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:35.454189
An Event ID: 135, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:35.454199
An Event ID: 130, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:35.454632
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:35.455215
An Event ID: 131, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:35.466009
An Event ID: 66, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:36.260864
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:36.264944
An Event ID: 33, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:36.264957
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
```

```
This event was created on:  2019-08-28 13:58:36.278646
An Event ID: 135, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:36.279203
An Event ID: 169, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:36.279840
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:36.279957
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:36.279991
An Event ID: 135, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:36.280077
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:36.280811
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:36.283255
An Event ID: 162, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:36.369984
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:36.419182
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:36.419420
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
```

```
No Match in Event ID List
This event was created on:  2019-08-28 13:58:36.419424
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:36.920641
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:36.925022
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:37.033384
An Event ID: 168, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:37.042881
An Event ID: 68, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:37.269314
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:37.403608
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:37.633371
An Event ID: 227, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:37.766420
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:37.876478
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:37.924122
```

```
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:37.932581
An Event ID: 227, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:38.113651
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:38.114691
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:38.114710
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:38.170778
An Event ID: 227, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:38.171110
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:38.171188
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:38.188967
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:38.234795
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 13:58:38.539696
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
```

```
This event was created on:  2019-08-28 13:58:38.540911
An Event ID: 143, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.304729
An Event ID: 226, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.304762
An Event ID: 143, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.304775
An Event ID: 143, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.304779
An Event ID: 143, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.304785
An Event ID: 143, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.304790
An Event ID: 143, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.304796
An Event ID: 143, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.304802
An Event ID: 143, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.304804
An Event ID: 143, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.304810
An Event ID: 143, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
```

```
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.304815
An Event ID: 143, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.304821
An Event ID: 143, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.304827
An Event ID: 143, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.304831
An Event ID: 143, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.304836
An Event ID: 143, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.304840
An Event ID: 143, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.304846
An Event ID: 143, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.304852
An Event ID: 143, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.304857
An Event ID: 143, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.304861
An Event ID: 142, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.304871
```

```
An Event ID: 143, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.305252
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.442551
An Event ID: 102, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.443129
An Event ID: 145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.443134
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.443146
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.443155
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.443159
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.443241
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.443245
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.443592
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
```

```
This event was created on:  2019-08-28 14:13:36.443617
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.443638
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.443642
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.443674
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.443682
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.443689
An Event ID: 228, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.444040
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.444050
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.444065
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.444128
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.444143
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
```

```
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.444433
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.444847
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.446739
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.447756
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.448259
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.449718
An Event ID: 103, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.449730
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:13:36.461603
An Event ID: 131, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.475754
An Event ID: 65, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.477829
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.480158
```

```
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.480173
An Event ID: 141, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.481396
An Event ID: 101, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.517082
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.517094
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.517099
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.517109
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.517164
An Event ID: 104, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.517265
An Event ID: 71, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.517269
An Event ID: 227, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.517307
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
```

```
This event was created on:  2019-08-28 14:22:27.517313
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.517712
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.517729
An Event ID: 98, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.517851
An Event ID: 100, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.517853
An Event ID: 101, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.517855
An Event ID: 135, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.517857
An Event ID: 135, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.517862
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.518242
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.518927
An Event ID: 66, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.566500
An Event ID: 33, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
```

```
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.571306
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.571321
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.572847
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.572897
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.572903
An Event ID: 169, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.573229
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.573240
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.573244
An Event ID: 163, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.573269
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.573427
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.573429
```

```
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.573433
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.573561
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.573574
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.573580
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.608698
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.903246
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.906075
An Event ID: 227, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.906170
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.906225
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.906654
An Event ID: 227, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
```

```
This event was created on:  2019-08-28 14:22:27.906759
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.906876
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.909201
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.913498
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.913549
An Event ID: 227, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.913626
An Event ID: 227, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:27.969936
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:28.063572
An Event ID: 227, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:28.083727
An Event ID: 228, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:28.986345
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:28.986349
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
```

```
No Match in Event ID List
This event was created on:  2019-08-28 14:22:28.986359
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:29.108671
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:29.108675
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:29.379696
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:29.400585
An Event ID: 66, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:29.605927
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:29.934744
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:30.414749
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:31.112606
An Event ID: 227, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:31.112717
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:31.113621
```

```
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:31.552280
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:31.563282
An Event ID: 227, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:31.563383
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:31.563429
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:31.566732
An Event ID: 227, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:31.566841
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:31.566969
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:31.569963
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:31.904352
An Event ID: 227, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:31.904459
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
```

```
This event was created on:  2019-08-28 14:22:31.906311
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:32.165985
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:32.166853
An Event ID: 227, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:32.167011
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:32.196226
An Event ID: 227, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:32.196404
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:32.196444
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:32.379629
An Event ID: 142, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:33.495173
An Event ID: 226, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:33.495213
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:33.576227
An Event ID: 102, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
```

```
No Match in Event ID List
This event was created on:  2019-08-28 14:22:33.576536
An Event ID: 145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:33.576540
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:33.576546
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:33.576553
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:33.576557
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:33.576559
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:33.576571
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:33.576572
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:33.576584
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:33.576586
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:33.576588
```

```
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:33.576828
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:33.576841
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:33.577267
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:33.579636
An Event ID: 228, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:33.589798
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:33.589907
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:33.589918
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:33.650684
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:33.650688
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:22:33.651484
An Event ID: 103, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
```

```
This event was created on:  2019-08-28 14:22:33.651489
An Event ID: 131, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:22.108549
An Event ID: 65, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:22.111967
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:22.115549
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:22.115566
An Event ID: 141, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:22.133938
An Event ID: 101, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:27.080194
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:27.080370
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:27.080383
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:27.080410
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:27.080717
An Event ID: 104, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
```

```
No Match in Event ID List
This event was created on:  2019-08-28 14:51:27.080936
An Event ID: 71, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:27.080946
An Event ID: 227, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:27.081015
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:27.081026
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:27.086359
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:27.086605
An Event ID: 98, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:27.087080
An Event ID: 100, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:27.087088
An Event ID: 101, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:27.087093
An Event ID: 135, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:27.087103
An Event ID: 135, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:27.087116
```

```
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:27.088650
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:27.088717
An Event ID: 66, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:27.287643
An Event ID: 33, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:27.294708
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:27.294811
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:29.263100
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:29.263208
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:29.263226
An Event ID: 169, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:29.263468
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:29.263733
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
```

```
This event was created on:  2019-08-28 14:51:29.263744
An Event ID: 163, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:29.263758
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:29.264536
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:29.264547
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:29.264559
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:29.264921
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:29.264984
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:29.267834
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:29.336559
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:29.446323
An Event ID: 227, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:29.446402
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
```

```
No Match in Event ID List
This event was created on:  2019-08-28 14:51:29.446451
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:29.452698
An Event ID: 227, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:29.452772
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:29.452774
An Event ID: 227, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:29.573984
An Event ID: 227, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:29.637939
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:29.668140
An Event ID: 142, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:36.108965
An Event ID: 226, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:36.109138
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:36.247915
An Event ID: 102, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:36.249525
```

```
An Event ID: 145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:36.249537
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:36.249565
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:36.249588
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:36.249605
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:36.249672
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:36.249683
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:36.249947
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:36.249962
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:36.249971
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:36.249987
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
```

```
This event was created on:  2019-08-28 14:51:36.249998
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:36.250029
An Event ID: 228, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:36.251421
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:36.251448
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:36.251478
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:36.327837
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:36.327854
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:36.337988
An Event ID: 103, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:51:36.338009
An Event ID: 131, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:40.476818
An Event ID: 65, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:40.488781
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
```

```
No Match in Event ID List
This event was created on:  2019-08-28 14:52:40.497429
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:40.497452
An Event ID: 141, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:40.499702
An Event ID: 101, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:45.542519
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:45.542528
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:45.542532
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:45.542540
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:45.542597
An Event ID: 104, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:45.542667
An Event ID: 71, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:45.542669
An Event ID: 227, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:45.542688
```

```
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:45.542692
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:45.543694
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:45.543718
An Event ID: 98, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:45.543819
An Event ID: 100, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:45.543819
An Event ID: 101, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:45.543821
An Event ID: 135, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:45.543825
An Event ID: 135, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:45.543829
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:45.544193
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:45.544210
An Event ID: 66, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
```

```
This event was created on:  2019-08-28 14:52:45.590691
An Event ID: 33, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:45.595114
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:45.595203
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:47.597195
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:47.597246
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:47.597279
An Event ID: 169, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:47.597359
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:47.597403
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:47.597406
An Event ID: 163, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:47.597408
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:47.597641
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
```

```
No Match in Event ID List
This event was created on:  2019-08-28 14:52:47.597645
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:47.597647
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:47.598394
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:47.598410
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:47.598417
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:47.631588
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:47.779629
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:47.779671
An Event ID: 227, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:47.779741
An Event ID: 132, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:47.784681
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:47.784769
```

```
An Event ID: 227, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:47.784895
An Event ID: 227, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:47.824137
An Event ID: 227, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:47.874178
An Event ID: 258, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:47.908010
An Event ID: 142, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:54.918890
An Event ID: 226, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:54.919008
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:55.046904
An Event ID: 102, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:55.048157
An Event ID: 145, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:55.048166
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:55.048185
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
```

```
This event was created on:  2019-08-28 14:52:55.048201
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:55.048212
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:55.048264
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:55.048271
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:55.048298
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:55.048307
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:55.048315
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:55.048323
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:55.048330
An Event ID: 148, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:55.048346
An Event ID: 228, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:55.049461
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
```

```
No Match in Event ID List
This event was created on:  2019-08-28 14:52:55.049482
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:55.049507
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:55.126610
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:55.126623
An Event ID: 72, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:55.154373
An Event ID: 103, was found in file
/home/user/CI5235_Coursework/evtx_logs/Other/rdpcorets_148_mst120_bluekee
p_rpdscan_full.xml
No Match in Event ID List
This event was created on:  2019-08-28 14:52:55.154400
ANALYSIS SUMMARY
166 log files analysed.
4735 Event IDs found.
480 Event IDs matched in Event ID List.
This data has been logged in a file called:
analysis_log_05_Jan_2020_13:20:45.txt
```