Name: Ashish Das

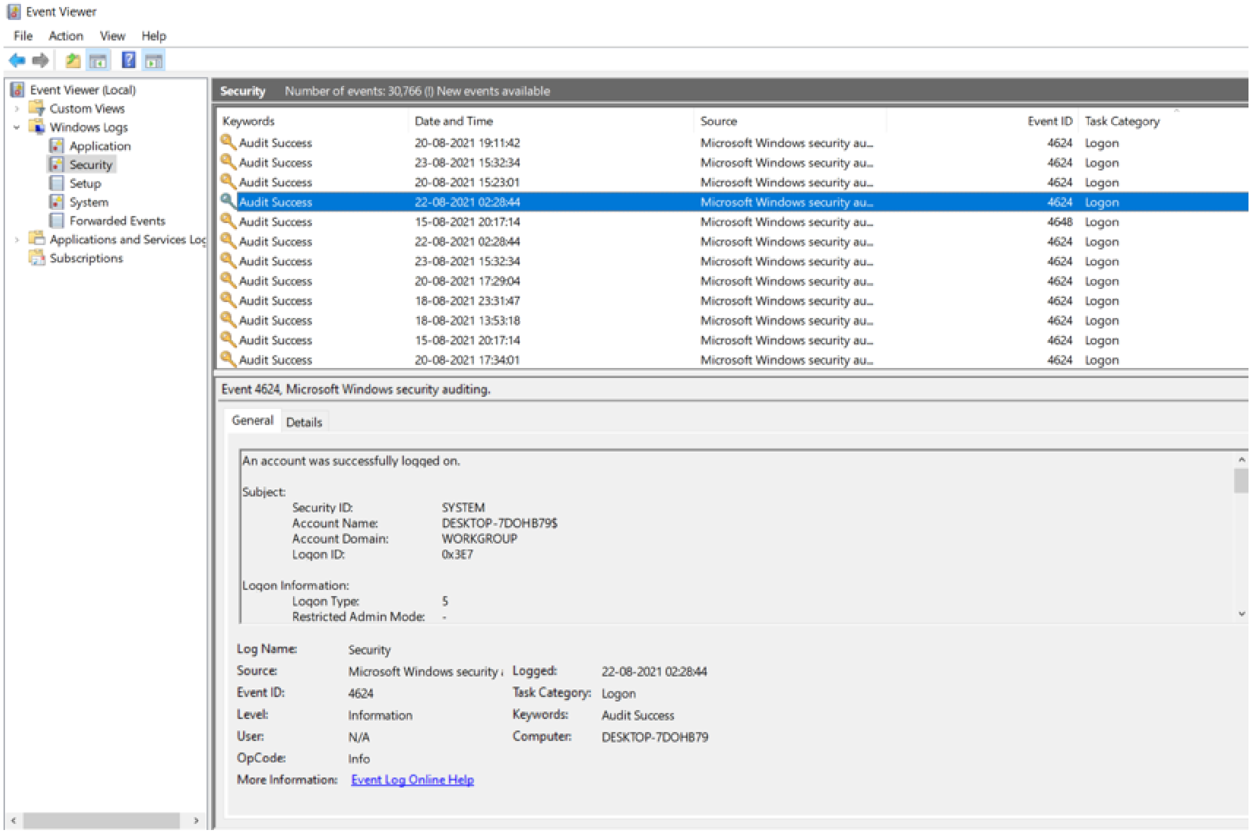
Reg. No.: 19BCE1160

Faculty: Nagraj S. V.

1. Use the Event Viewer tool in a Microsoft Windows computer and take screenshots of <u>THREE</u> security related events such as:
   a. Logon
   b. Special Logon
   c. A user's local group membership was enumerated.

Output:

a. An account was successfully logged on.



Number of events: 30,766 (!) New events available

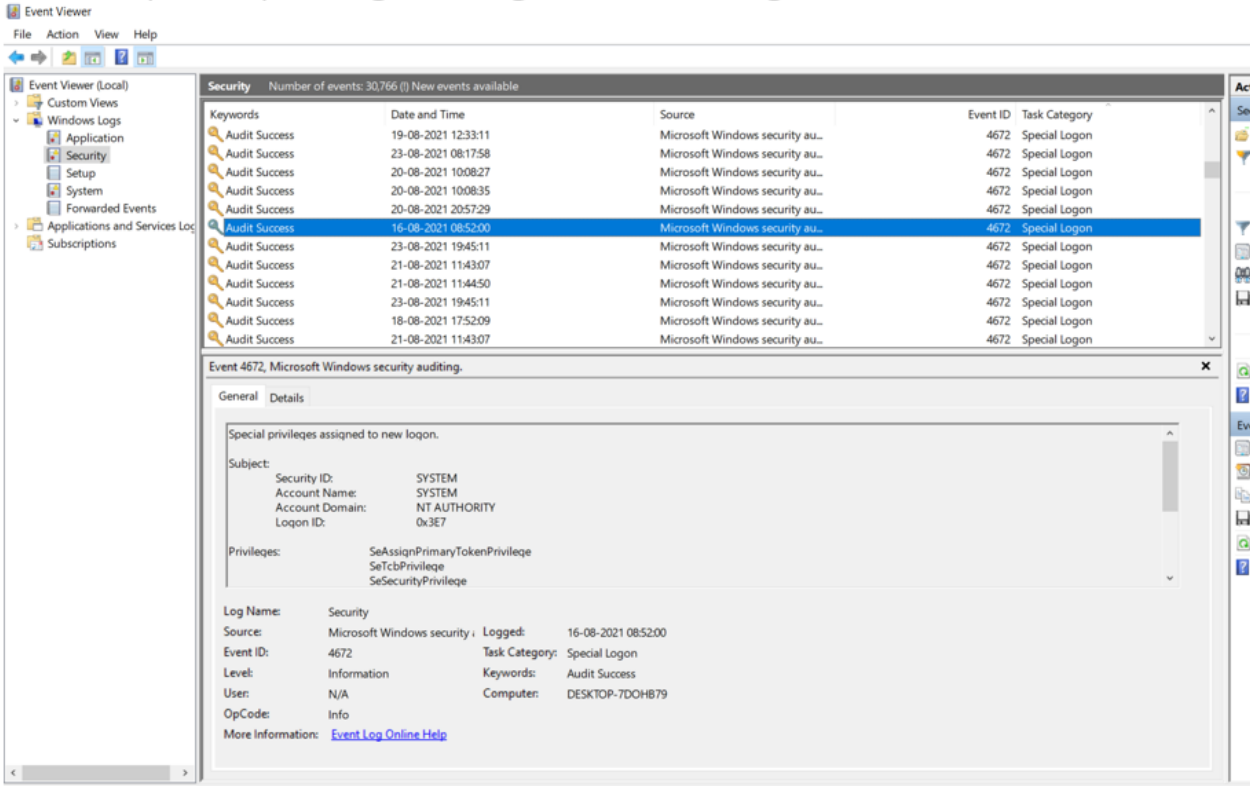
Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	20-08-2021 19:11:42	Microsoft Windows security au...	4624	Logon
Audit Success	23-08-2021 15:32:34	Microsoft Windows security au...	4624	Logon
Audit Success	20-08-2021 15:23:01	Microsoft Windows security au...	4624	Logon
Audit Success	22-08-2021 02:28:44	Microsoft Windows security au...	4624	Logon
Audit Success	15-08-2021 20:17:14	Microsoft Windows security au...	4648	Logon
Audit Success	22-08-2021 02:28:44	Microsoft Windows security au...	4624	Logon
Audit Success	23-08-2021 15:32:34	Microsoft Windows security au...	4624	Logon
Audit Success	20-08-2021 17:29:04	Microsoft Windows security au...	4624	Logon
Audit Success	18-08-2021 23:31:47	Microsoft Windows security au...	4624	Logon
Audit Success	18-08-2021 13:53:18	Microsoft Windows security au...	4624	Logon
Audit Success	15-08-2021 20:17:14	Microsoft Windows security au...	4624	Logon
Audit Success	20-08-2021 17:34:01	Microsoft Windows security au...	4624	Logon

Event 4624, Microsoft Windows security auditing.

```
An account was successfully logged on.

Subject:
        Security ID:            SYSTEM
        Account Name:           DESKTOP-7DOHB79$
        Account Domain:         WORKGROUP
        Logon ID:               0x3E7

Logon Information:
        Logon Type:             5
        Restricted Admin Mode:  -
```

Log Name:	Security		
Source:	Microsoft Windows security ε	Logged:	22-08-2021 02:28:44
Event ID:	4624	Task Category:	Logon
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	DESKTOP-7DOHB79
OpCode:	Info		
More Information:	Event Log Online Help		

b. Special privileges assigned to new logon.



Security Number of events: 30,766 (!) New events available

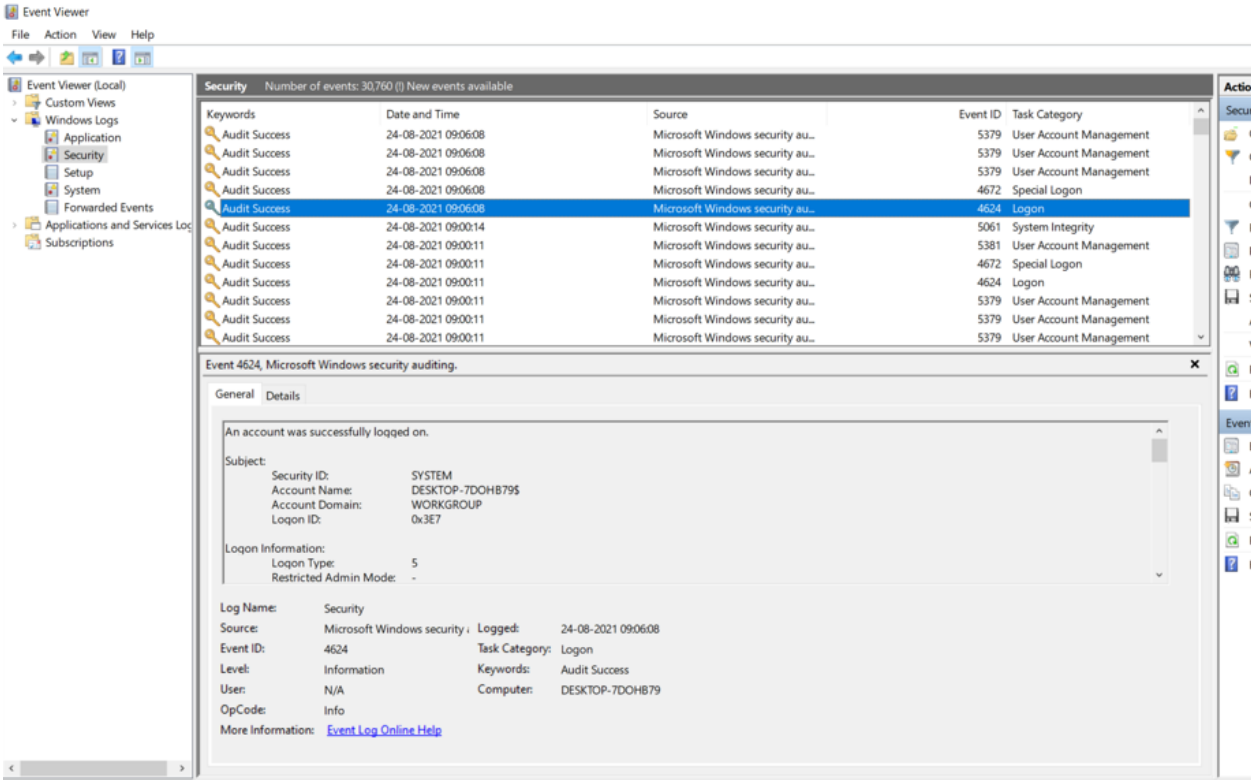
Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	19-08-2021 12:33:11	Microsoft Windows security au...	4672	Special Logon
Audit Success	23-08-2021 08:17:58	Microsoft Windows security au...	4672	Special Logon
Audit Success	20-08-2021 10:08:27	Microsoft Windows security au...	4672	Special Logon
Audit Success	20-08-2021 10:08:35	Microsoft Windows security au...	4672	Special Logon
Audit Success	20-08-2021 20:57:29	Microsoft Windows security au...	4672	Special Logon
Audit Success	16-08-2021 08:52:00	Microsoft Windows security au...	4672	Special Logon
Audit Success	23-08-2021 19:45:11	Microsoft Windows security au...	4672	Special Logon
Audit Success	21-08-2021 11:43:07	Microsoft Windows security au...	4672	Special Logon
Audit Success	21-08-2021 11:44:50	Microsoft Windows security au...	4672	Special Logon
Audit Success	23-08-2021 19:45:11	Microsoft Windows security au...	4672	Special Logon
Audit Success	18-08-2021 17:52:09	Microsoft Windows security au...	4672	Special Logon
Audit Success	21-08-2021 11:43:07	Microsoft Windows security au...	4672	Special Logon

Event 4672, Microsoft Windows security auditing.

```
Special privileges assigned to new logon.

Subject:
        Security ID:        SYSTEM
        Account Name:       SYSTEM
        Account Domain:     NT AUTHORITY
        Logon ID:           0x3E7

Privileges:         SeAssignPrimaryTokenPrivilege
                    SeTcbPrivilege
                    SeSecurityPrivilege
```

Log Name:	Security		
Source:	Microsoft Windows security a	Logged:	16-08-2021 08:52:00
Event ID:	4672	Task Category:	Special Logon
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	DESKTOP-7DOHB79
OpCode:	Info		
More Information:	Event Log Online Help		

c. A user's local group membership was enumerated.



Security Number of events: 30,760 (!) New events available

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	24-08-2021 09:06:08	Microsoft Windows security au...	5379	User Account Management
Audit Success	24-08-2021 09:06:08	Microsoft Windows security au...	5379	User Account Management
Audit Success	24-08-2021 09:06:08	Microsoft Windows security au...	5379	User Account Management
Audit Success	24-08-2021 09:06:08	Microsoft Windows security au...	4672	Special Logon
Audit Success	24-08-2021 09:06:08	Microsoft Windows security au...	4624	Logon
Audit Success	24-08-2021 09:00:14	Microsoft Windows security au...	5061	System Integrity
Audit Success	24-08-2021 09:00:11	Microsoft Windows security au...	5381	User Account Management
Audit Success	24-08-2021 09:00:11	Microsoft Windows security au...	4672	Special Logon
Audit Success	24-08-2021 09:00:11	Microsoft Windows security au...	4624	Logon
Audit Success	24-08-2021 09:00:11	Microsoft Windows security au...	5379	User Account Management
Audit Success	24-08-2021 09:00:11	Microsoft Windows security au...	5379	User Account Management
Audit Success	24-08-2021 09:00:11	Microsoft Windows security au...	5379	User Account Management

Event 4624, Microsoft Windows security auditing.

General Details

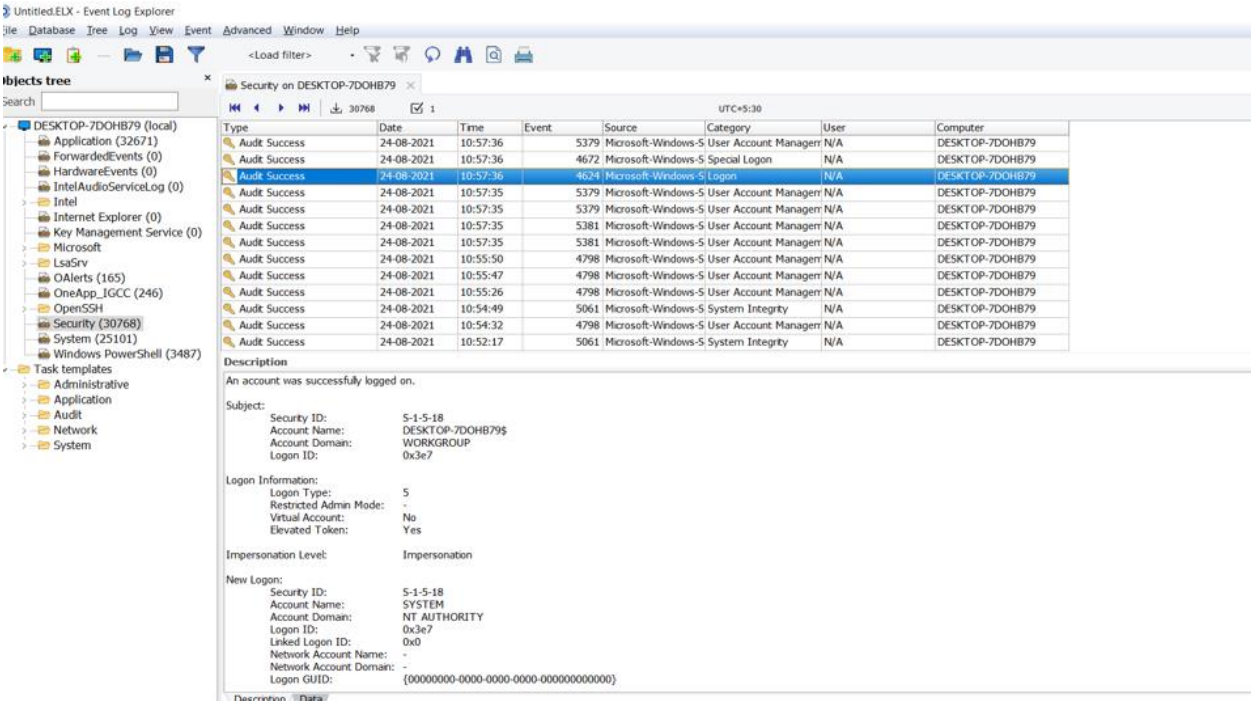
```
An account was successfully logged on.

Subject:
        Security ID:            SYSTEM
        Account Name:           DESKTOP-7DOHB79$
        Account Domain:         WORKGROUP
        Logon ID:               0x3E7

Logon Information:
        Logon Type:             5
        Restricted Admin Mode:  -
```

Log Name:	Security		
Source:	Microsoft Windows security a	Logged:	24-08-2021 09:06:08
Event ID:	4624	Task Category:	Logon
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	DESKTOP-7DOHB79
OpCode:	Info		
More Information:	Event Log Online Help		

2. **Download Event Log Explorer tool on a Windows computer and take screenshots of two security related events such as those listed in the previous exercise.**

Output:

a. *An account was successfully logged on.*

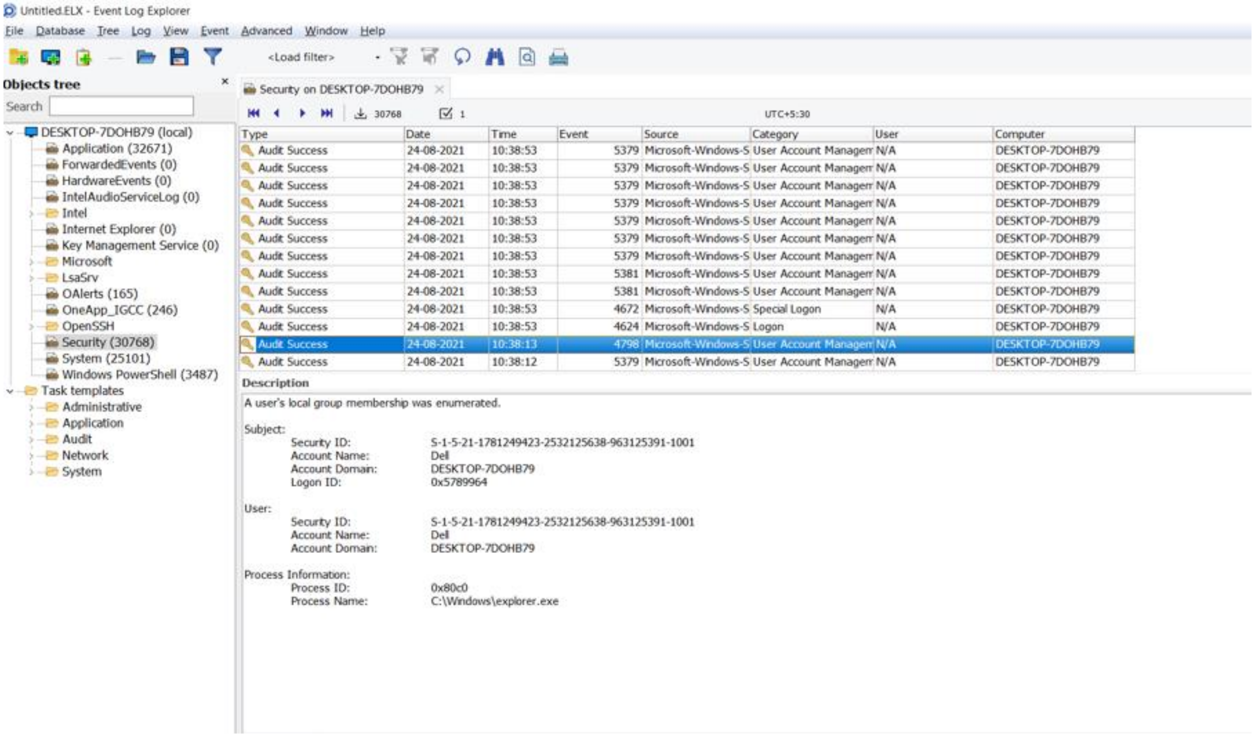


Type	Date	Time	Event	Source	Category	User	Computer
Audit Success	24-08-2021	10:57:36	5379	Microsoft-Windows-S	User Account Managem	N/A	DESKTOP-7DOHB79
Audit Success	24-08-2021	10:57:36	4672	Microsoft-Windows-S	Special Logon	N/A	DESKTOP-7DOHB79
Audit Success	24-08-2021	10:57:36	4624	Microsoft-Windows-S	Logon	N/A	DESKTOP-7DOHB79
Audit Success	24-08-2021	10:57:35	5379	Microsoft-Windows-S	User Account Managem	N/A	DESKTOP-7DOHB79
Audit Success	24-08-2021	10:57:35	5379	Microsoft-Windows-S	User Account Managem	N/A	DESKTOP-7DOHB79
Audit Success	24-08-2021	10:57:35	5381	Microsoft-Windows-S	User Account Managem	N/A	DESKTOP-7DOHB79
Audit Success	24-08-2021	10:57:35	5381	Microsoft-Windows-S	User Account Managem	N/A	DESKTOP-7DOHB79
Audit Success	24-08-2021	10:55:50	4798	Microsoft-Windows-S	User Account Managem	N/A	DESKTOP-7DOHB79
Audit Success	24-08-2021	10:55:47	4798	Microsoft-Windows-S	User Account Managem	N/A	DESKTOP-7DOHB79
Audit Success	24-08-2021	10:55:26	4798	Microsoft-Windows-S	User Account Managem	N/A	DESKTOP-7DOHB79
Audit Success	24-08-2021	10:54:49	5061	Microsoft-Windows-S	System Integrity	N/A	DESKTOP-7DOHB79
Audit Success	24-08-2021	10:54:32	4798	Microsoft-Windows-S	User Account Managem	N/A	DESKTOP-7DOHB79
Audit Success	24-08-2021	10:52:17	5061	Microsoft-Windows-S	System Integrity	N/A	DESKTOP-7DOHB79

Description

```
An account was successfully logged on.

Subject:
        Security ID:            S-1-5-18
        Account Name:           DESKTOP-7DOHB79$
        Account Domain:         WORKGROUP
        Logon ID:               0x3e7

Logon Information:
        Logon Type:             5
        Restricted Admin Mode:  -
        Virtual Account:        No
        Elevated Token:         Yes

Impersonation Level:            Impersonation

New Logon:
        Security ID:            S-1-5-18
        Account Name:           SYSTEM
        Account Domain:         NT AUTHORITY
        Logon ID:               0x3e7
        Linked Logon ID:        0x0
        Network Account Name:   -
        Network Account Domain: -
        Logon GUID:             {00000000-0000-0000-0000-000000000000}
```

b. A user's local group membership was enumerated.



Type	Date	Time	Event	Source	Category	User	Computer
Audit Success	24-08-2021	10:38:53	5379	Microsoft-Windows-S	User Account Managem	N/A	DESKTOP-7DOHB79
Audit Success	24-08-2021	10:38:53	5379	Microsoft-Windows-S	User Account Managem	N/A	DESKTOP-7DOHB79
Audit Success	24-08-2021	10:38:53	5379	Microsoft-Windows-S	User Account Managem	N/A	DESKTOP-7DOHB79
Audit Success	24-08-2021	10:38:53	5379	Microsoft-Windows-S	User Account Managem	N/A	DESKTOP-7DOHB79
Audit Success	24-08-2021	10:38:53	5379	Microsoft-Windows-S	User Account Managem	N/A	DESKTOP-7DOHB79
Audit Success	24-08-2021	10:38:53	5379	Microsoft-Windows-S	User Account Managem	N/A	DESKTOP-7DOHB79
Audit Success	24-08-2021	10:38:53	5379	Microsoft-Windows-S	User Account Managem	N/A	DESKTOP-7DOHB79
Audit Success	24-08-2021	10:38:53	5381	Microsoft-Windows-S	User Account Managem	N/A	DESKTOP-7DOHB79
Audit Success	24-08-2021	10:38:53	5381	Microsoft-Windows-S	User Account Managem	N/A	DESKTOP-7DOHB79
Audit Success	24-08-2021	10:38:53	4672	Microsoft-Windows-S	Special Logon	N/A	DESKTOP-7DOHB79
Audit Success	24-08-2021	10:38:53	4624	Microsoft-Windows-S	Logon	N/A	DESKTOP-7DOHB79
Audit Success	24-08-2021	10:38:13	4798	Microsoft-Windows-S	User Account Managem	N/A	DESKTOP-7DOHB79
Audit Success	24-08-2021	10:38:12	5379	Microsoft-Windows-S	User Account Managem	N/A	DESKTOP-7DOHB79

Description

```
A user's local group membership was enumerated.

Subject:
        Security ID:            S-1-5-21-1781249423-2532125638-963125391-1001
        Account Name:           Dell
        Account Domain:         DESKTOP-7DOHB79
        Logon ID:               0x5789964

User:
        Security ID:            S-1-5-21-1781249423-2532125638-963125391-1001
        Account Name:           Dell
        Account Domain:         DESKTOP-7DOHB79

Process Information:
        Process ID:             0x80c0
        Process Name:           C:\Windows\explorer.exe
```