Incident Response: Windows Account Management Event (Part 2)

August 29, 2020   By Raj Chandel

For a system to perform well and ensure its maintenance, it is extremely important to monitor and manage events on a system. Event Logs are part of the Windows system, that are created by on a system and can be checked locally or remotely on regular intervals by an administrator or any user. These logs can then be imported and viewed in a SIEM tool to ensure efficient Incident Response.

Incident Response: Windows Account Management Event (Part 1)

Table of Contents

- **Security Policy Settings**
- **Advantage of security settings**
- **Event Log**
- **Account Management Events**
- **Events in Windows Server 2016**

Security Policy Settings

They are set of rules that an administrator uses to configure a computer or multiple devices for securing resources on a device or network. The Security Settings extension of the Local Group Policy Editor allows you to define a security configuration as part of a Group Policy Object (GPO).

The GPOs are linked to Active Directory containers such as sites, domains, or organizational units, and they enable you to manage security settings for multiple devices from any device joined to the domain. Security settings policies are used as part of your overall security implementation to help secure domain controllers, servers, clients, and other resources in your organization.

Advantage of Security Setting

- User is authenticated in a network or device.
- The defined resources that any user is permitted to access.
- Whether to record a user's or group's actions in the event log.
- Membership of a user in a group.

Event Log

The event logs usually keep a record of services from various sources and then stores them in a single place. Events logs can be of Security, System and Application event. As an incident responder, you should look for

multiple sources of log information and should not forget to look at the older log files which may be present in backup systems or volume shadow copies.

When the Event logs are assessed, the Event ID have various field details with them;

Field	Function
Log name	Defines the name of the event log
Source	The place from where it is generated in the system
Event ID	The identification number of the log
Level	The seriousness of the log
User	The account to which the log is related to
Logged	The systems date and time when the event was generated
Task Category	It is assigned by the source of log
Keywords	Its is used to group or categorise the events
Computer	The system on which the log was created
Description	It it's the information about the log

Account Management Events

The Account Management is extremely important and these events can be used to track the maintenance of users, group, and computer objects in Local users and groups, Active Directory.

Account Management events can be used to track a new user account, any password resets, or any new members being added to groups or being deleted from the group.

The account management events can be categorised into different types:

Events in Windows Server 2016

Now, Switch on your Windows Server 2016 to get you started.

Event ID 4727

Event ID	Description
4727	A security-enabled global group was created.

Purpose of Monitoring this Log:

- If any unknown group is created, an anomaly can be detected.

When you create a security-enabled – global(scope) group, then this event is generated.

Event ID 4728

Event ID	Description
4728	A member was added to a security-enabled global group.

Purpose of Monitoring this Log:

- If any unknown member is added to a group it can be detected.

When you add a new member to a security-enabled -global group, then this event is generated.

Keywords	Event ID	Task Category	Date and Time
Event ID: 4728 (2)			
Audit Success	4728	Security Group Man...	6/29/2020 9:54:43 AM
Audit Success	4728	Security Group Man...	6/29/2020 9:54:43 AM

www.hackingarticles.in

Event 4728, Microsoft Windows security auditing.   ✕

General   Details

A member was added to a security-enabled global group.

Subject:
    Security ID: ANONYMOUS LOGON
    Account Name: ANONYMOUS LOGON
    Account Domain: NT AUTHORITY
    Logon ID: 0x3E6

Member:
    Security ID: IGNITE\Administrator
    Account Name: CN=Administrator,CN=Users,DC=ignite,DC=local

| Log Name:	Security		
Source:	Microsoft Windows security	Logged:	6/29/2020 9:54:43 AM
Event ID:	4728	Task Category:	Security Group Management
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	DC1.ignite.local
OpCode:	Info		
More Information:	Event Log Online Help		

Event ID 4729

Event ID	Description
4729	A member was removed from a security enabled global group.

Purpose of Monitoring this Log:

- If a key member is removed from a group, it can be detected.

You can go to the properties of the user and remove the user from the group.
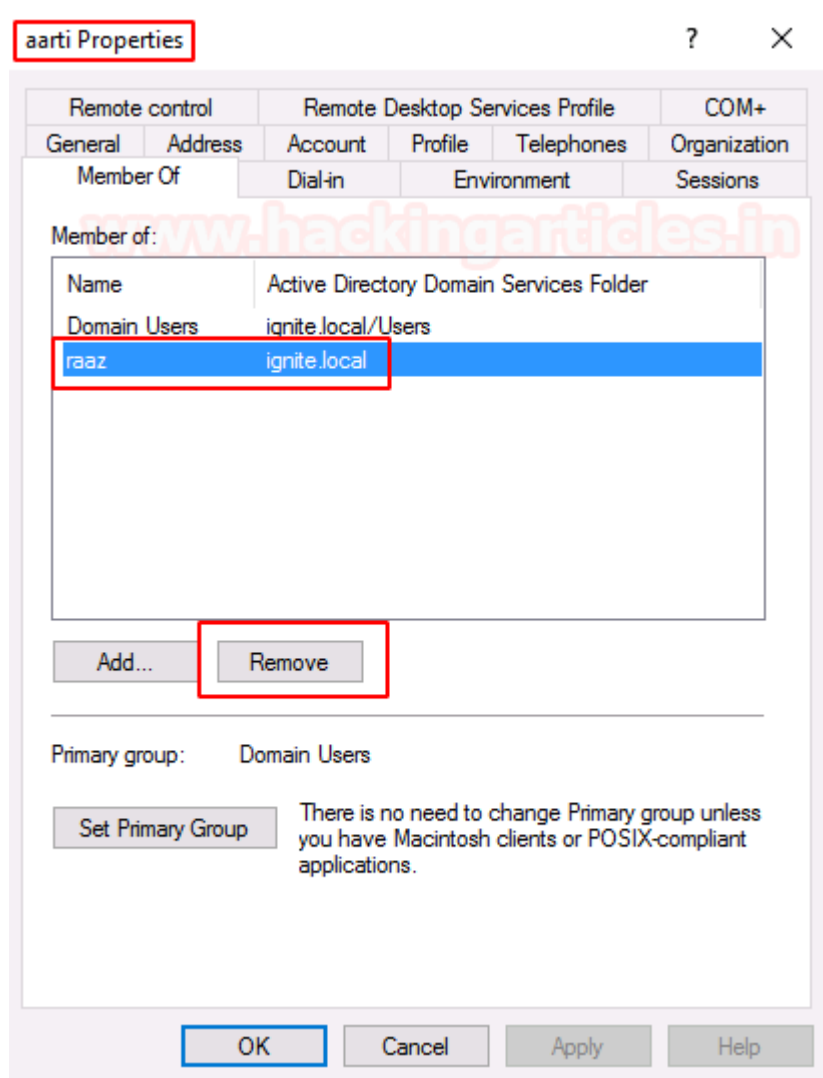
When a member is deleted from a group, this event is created.

Security Number of events: 6,009 (!) New events available

Keywords	Event ID	Task Category	Date and Time	
Event ID: 4729 (1)				
🔍 Audit Success	4729	Security Group Man...	8/27/2020 11:41:40 AM	
Event ID: 4731 (32)				

Event 4729, Microsoft Windows security auditing.   ✕

General Details

A member was removed from a security-enabled global group.

Subject:
    Security ID: IGNITE\Administrator
    Account Name: Administrator
    Account Domain: IGNITE
    Logon ID: 0x4ED85

Member:
    Security ID: IGNITE\aarti
    Account Name: CN=aarti,OU=Tech,DC=ignite,DC=local

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	8/27/2020 11:41:40 AM
Event ID:	4729	Task Category:	Security Group Management
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	DC1.ignite.local
OpCode:	Info		
More Information:	Event Log Online Help		

Event ID 4737

Event ID	Description
4737	A security-enabled global group was changed

Purpose of Monitoring this Log:

- If a group is changed, which wasn't supposed to, it is important to check this log.

When security enable group was changed, or any changes were made, this event was created.

Security   Number of events: 6,009 (!) New events available

Keywords	Event ID	Task Category	Date and Time
Event ID: 4737 (19)			
Audit Success	4737	Security Group Man...	6/29/2020 9:39:58 AM
Audit Success	4737	Security Group Man...	6/29/2020 9:39:58 AM
Audit Success	4737	Security Group Man...	8/17/2020 6:03:49 AM
Audit Success	4737	Security Group Man...	8/17/2020 6:03:49 AM
Audit Success	4737	Security Group Man...	6/29/2020 9:54:43 AM

Event 4737, Microsoft Windows security auditing.   ✕

General   Details

A security-enabled global group was changed.

Subject:
     Security ID: SYSTEM
     Account Name: WIN-KQOBSEOR8SO$
     Account Domain: WORKGROUP
     Logon ID: 0x3E7

Group:
     Security ID: IGNITE\Domain Users
     Group Name: None
     Group Domain: WIN-KOOBSEOR8SO

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	6/29/2020 9:39:58 AM
Event ID:	4737	Task Category:	Security Group Management
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	WIN-KQOBSEOR8SO
OpCode:	Info		
More Information:	Event Log Online Help		

Event ID 4741

Event ID	Description
4741	A computer account was created.

Purpose of Monitoring this Log:

- If an unverified computer account is created, which could cause potential harm.

Create a new computer account, using system properties by changing settings.
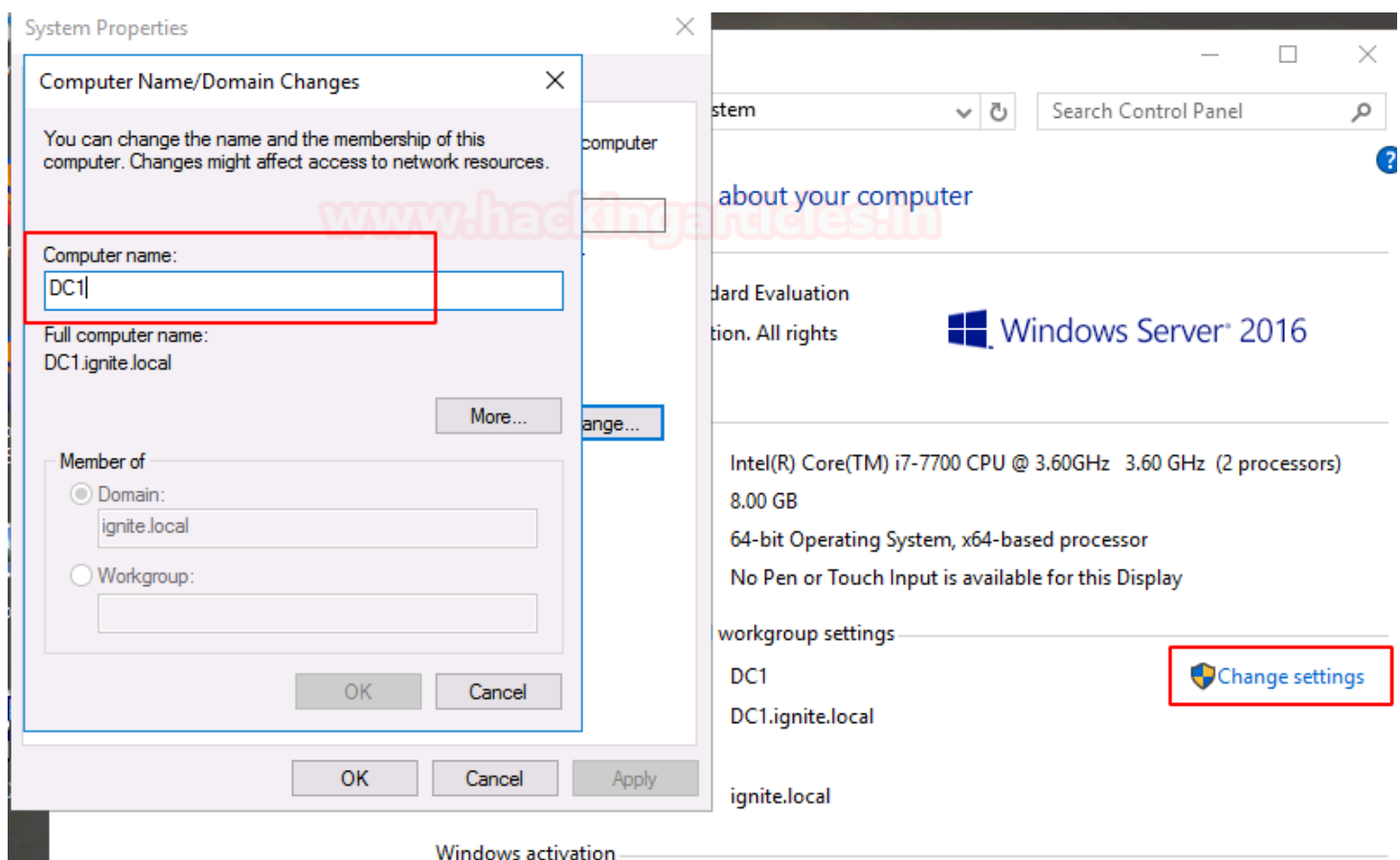
When a new computer account is created, this event is created

Event ID 4742

Event ID	Description
4742	A computer account was changed.
Purpose of Monitoring this Log:	

- If an organisation has database servers, domain controllers, administration workstations, it is important to check.

When any changes are made to the computer account, this event is generated.

Keywords	Event ID	Task Category	Date and Time
Audit Success	4742	Computer Account ...	8/27/2020 11:24:36 AM
Audit Success	4742	Computer Account ...	6/29/2020 10:09:19 AM
Audit Success	4742	Computer Account ...	8/27/2020 11:24:36 AM
Audit Success	4742	Computer Account ...	6/29/2020 9:54:59 AM
Audit Success	4742	Computer Account ...	6/29/2020 9:55:23 AM
Audit Success	4742	Computer Account	8/17/2020 5:48:58 AM

Event 4742, Microsoft Windows security auditing.

General   Details

A computer account was changed.

Subject:
    Security ID: SYSTEM
    Account Name: DC1$
    Account Domain: IGNITE
    Logon ID: 0x8E925

Computer Account That Was Changed:
    Security ID: IGNITE\DC1$
    Account Name: DC1$
    Account Domain: IGNITE

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	8/27/2020 11:24:36 AM
Event ID:	4742	Task Category:	Computer Account Management
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	DC1.ignite.local
OpCode:	Info		
More Information:	Event Log Online Help		

Event ID 4743

Event ID	Description
4743	A computer account was deleted.

Purpose of Monitoring this Log:

- Any critical account is deleted, it is important to check.

Event ID 4754

Event ID	Description
4754	A security-enabled universal group was created

Purpose of Monitoring this Log:

- To prevent any privilege abuse.
- Detect any potential malicious activity.

When a computer account is deleted, this event is generated.

Event ID 4755

Event ID	Description
4755	A security-enabled universal group was changed.

Purpose of Monitoring this Log:

- To maintain any compliance mandates.

When any changes are made in a security-enabled universal(scope) group, this log is created.

Security Number of events: 6,009 (!) New events available

Keywords	Event ID	Task Category	Date and Time	
Audit Success	4755	Security Group Man...	6/29/2020 9:54:43 AM	
Audit Success	4755	Security Group Man...	6/29/2020 9:54:43 AM	
Audit Success	4755	Security Group Man...	8/17/2020 6:03:49 AM	
Audit Success	4755	Security Group Man...	8/17/2020 6:03:49 AM	
Audit Success	4755	Security Group Man...	6/29/2020 9:54:43 AM	

Event 4755, Microsoft Windows security auditing.   ✕

General Details

A security-enabled universal group was changed.

Subject:
    Security ID: ANONYMOUS LOGON
    Account Name: ANONYMOUS LOGON
    Account Domain: NT AUTHORITY
    Logon ID: 0x3E6

Group:
    Security ID: IGNITE\Schema Admins
    Group Name: Schema Admins
    Group Domain: IGNITE

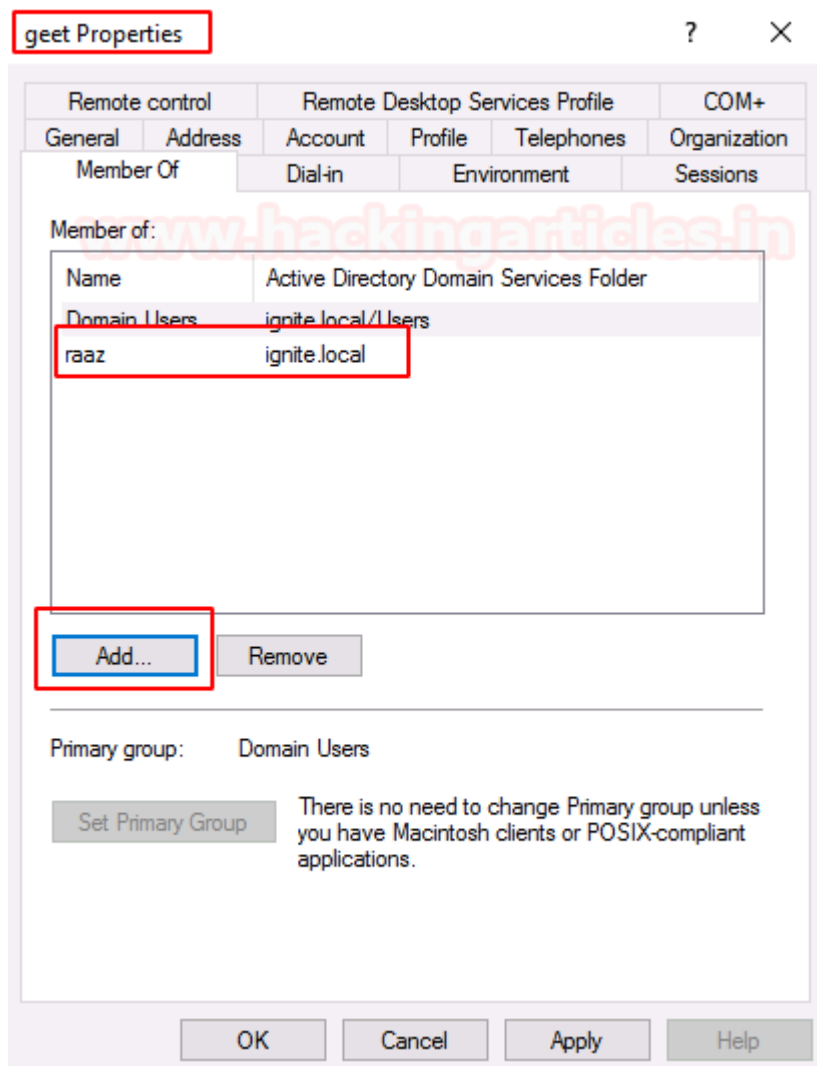| Log Name:	Security		
Source:	Microsoft Windows security	Logged:	6/29/2020 9:54:43 AM
Event ID:	4755	Task Category:	Security Group Management
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	DC1.ignite.local
OpCode:	Info		
More Information:	Event Log Online Help		

Event ID 4756

Event ID	Description
4756	A member was added to a security-enabled universal group

Purpose of Monitoring this Log:

- To keep a check on restricted member being added to a group.

You can add the user to the group using

When a new member is added to a security-enabled universal group, add this event is created.

Event ID 4799

Event ID	Description
4799	A security-enabled local group membership was enumerated. Large numbers of these events may be indicative of adversary group enumeration

Purpose of Monitoring this Log:

- To check every time a membership is enumerated for a local or domain security group and to also to see who enumerated the membership

When a member from a group is enumerated, this event will be generated.

You can try out the below event ID using Domain Controller:

Event ID	Description
4723	An attempt was made to change an account's password

Purpose of Monitoring this Log:

- To track back this event to a logon event with a matching Logon ID to identify the source workstation or server from which this account's password was changed

Event ID	Description
4757	A member was removed from a security-enabled universal group.

Purpose of Monitoring this Log:

- To maintain any compliance mandates.

Event ID	Description
4758	A security-enabled universal group was deleted
Purpose of Monitoring this Log:	
• To detect any malicious activity in the domain.	

Conclusion: Hence, being an incident responder, you can maintain the activity of users using account management event in windows**.**