How to find Windows 7 privilege use failure

This howto describes how to find privilege use failure in Windows 7 Event Viewer. The howto believes you have already created the failure.

Preuss
2/12/2012

win7_x64 - VMware Player File Virtual Machine Help

Recycle Bin

Adobe Reader X

LibreOffice 3.4

Mozilla Firefox

After creating the privelege use failure, we need to logon as administrator.

4:54 PM
2/12/2012

To direct input to this virtual machine, press Ctrl+G.

vmware

win7_x64 - VMware Player File Virtual Machine Help

Local Security Policy

File Action View Help

- Security Settings
  - Account Policies
  - Local Policies
    - Audit Policy
    - User Rights Assignment
    - Security Options
  - Windows Firewall with Advanced Sec
  - Network List Manager Policies
  - Public Key Policies
  - Software Restriction Policies
  - Application Control Policies
  - IP Security Policies on Local Compute
  - Advanced Audit Policy Configuration

Policy	Security Setting
Audit account logon events	Success, Failure
Audit account management	Failure
Audit directory service access	No auditing
Audit logon events	Failure
Audit object access	Failure
Audit policy change	Failure
Audit privilege use	Failure
Audit process tracking	No auditing
Audit system events	No auditing

These are the Local Security | Audit Policy settings used for this example.

Administrative Tools

Size

2 KB
2 KB
2 KB
2 KB
2 KB
2 KB
2 KB
2 KB
2 KB
2 KB
2 KB
3 KB

Taskbar and Start Menu
VMware Tools
Windows Defender
Troubleshooting
Windows Anytime Upgrade
Windows Firewall
User Accounts
Windows CardSpace
Windows Update

4:57 PM
2/12/2012

To direct input to this virtual machine, press Ctrl+G.

vmware

win7_x64 - VMware Player File Virtual Machine Help

Event Viewer

File Action View Help

- Event Viewer (Local)
  - Custom Views
  - Windows Logs
    - Application
    - Security
    - Setup
    - System
    - Forwarded Events
  - Applications and Services Logs
  - Subscriptions

Security Number of events: 554 (!) New events available

Level	Date and Time	Source	Ev...	Task Category
Information	2/12/2012 5:03:19 PM	Microsoft Wind...	4656	File System
Information	2/12/2012 5:03:18 PM	Microsoft Wind...	4656	File System
Information	2/12/2012 5:03:09 PM	Microsoft Wind...	4673	Sensitive Privilege Use
Information	2/12/2012 5:03:07 PM	Microsoft Wind...	4656	Other Object Access...
Information	2/12/2012 5:03:07 PM	Microsoft Wind...	4656	Other Object Access...
Information	2/12/2012 5:03:07 PM	Microsoft Wind...	4656	Other Object Access...

Event 4656, Microsoft Windows security auditing.

General Details

as requested.

PREUSS-WIN7-X64\nxt
nxt
in: PREUSS-WIN7-X64
0x12b5cc

rity
osoft Windows security
mation

Logged: 2/12/2012 5:03:19 PM
Task Category: File System
Keywords: Audit Failure
Computer: preuss-win7-x64

OpCode: Info
More Information: Event Log Online Help

Open Event Viewer | Windows Logs | Security

Actions

Security
- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Clear Log...
- Filter Current Log...
- Properties
- Find...
- Save All Events As...
- Attach a Task To this L...
- View
- Refresh
- Help

Event 4656, Microsoft Wind...
- Event Properties
- Attach Task To This Ev...
- Copy
- Save Selected Events...
- Refresh
- Help

5:03 PM
2/12/2012

To direct input to this virtual machine, press Ctrl+G.

vmware

win7_x64 - VMware Player File Virtual Machine Help

Event Viewer

File Action View Help

Event Properties - Event 4673, Microsoft Windows security auditing.

General Details

A privileged service was called.

Subject:

Security ID:	PREUSS-WIN7-X64\preuss
Account Name:	preuss
Account Domain:	PREUSS-WIN7-X64
Logon ID:	0xd1c6f

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	2/12/2012 4:58:44 PM
Event ID:	4673	Task Category:	Sensitive Privilege Use
Level:	Information	Keywords:	Audit Failure
User:	N/A	Computer:	preuss-win7-x64
OpCode:	Info		
More Information:	Event Log Online Help		

Copy Close

This is a sensitive privilege failure use log entry. Use the copy button to create the next page entry.

Source: Microsoft Windows security Logged: 2/12/2012 4:58:44 PM
Event ID: 4673 Task Category: Sensitive Privilege Use
Level: Information Keywords: Audit Failure
User: N/A Computer: preuss-win7-x64
OpCode: Info
More Information: Event Log Online Help

Save All Events As...
Attach a Task To this L...
View
Refresh
Help
Event 4673, Microsoft Wind...
Event Properties
Attach Task To This Ev...
Copy
Save Selected Events...
Refresh
Help

5:10 PM
2/12/2012

vmware

win7_x64 - VMware Player File Virtual Machine Help

Event Viewer

File Action View Help

Untitled - Notepad

File Edit Format View Help

```
Log Name:      Security
Source:        Microsoft-Windows-Security-Auditing
Date:          2/12/2012 4:58:44 PM
Event ID:      4673
Task Category: Sensitive Privilege Use
Level:         Information
Keywords:      Audit Failure
User:          N/A
Computer:      preuss-win7-x64
Description:
A privileged service was called.

Subject:
        Security ID:            PREUSS-WIN7-X64\preuss
        Account Name:           preuss
        Account Domain:         PREUSS-WIN7-X64
        Logon ID:               0xd1c6f

Service:
        Server: Security
        Service Name:   -

Process:
        Process ID:     0x71c
        Process Name:   C:\Windows\System32\mmc.exe

Service Request Information:
        Privileges:             SeCreateGlobalPrivilege
Event Xml:
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
  <System>
    <Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-A5BA-3E3B0328C30D}" />
    <EventID>4673</EventID>
    <Version>0</Version>
```

This is the complete log entry for sensititve privilege use. The description shows this is a sensitive privilege service. Highlighted is the exact privilege requested and denied.

OpCode: Info

More Information: Event Log Online Help

Help

5:10 PM
2/12/2012

vmware