How to find failed Windows 7 logons

This howto describes how to find failed Windows 7 logons in the Event Viewer. The howto believes you already know how to fail to logon to Windows 7.

Preuss
2/12/2012

win7_x64 - VMware Player File Virtual Machine Help

Recycle Bin

Adobe Reader X

LibreOffice 3.4

Mozilla Firefox

First, we need to fail to logon to Windows 7. It really does not matter what account you fail to logon.

Now we are logon as administrator to view the Event Viewer.

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 Policies settings used to record the logon failure in Event Viewer.

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
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.

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
PREUSS-WIN7-X64
0x12b5cc

rity
osoft Windows security
rmation

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 the Event Viewer and go to 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 Viewer (Local)

Custo

Windo

Ap

Se

Se

Sy

Fo

Applic

Subsc

Event Properties - Event 4625, Microsoft Windows security auditing.

General Details

An account failed to log on.

Subject:

Security ID:	SYSTEM
Account Name:	PREUSS-WIN7-X64$
Account Domain:	MAIT
Logon ID:	0x3e7

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	2/12/2012 4:57:37 PM
Event ID:	4625	Task Category:	Logon
Level:	Information	Keywords:	Audit Failure
User:	N/A	Computer:	preuss-win7-x64
OpCode:	Info		

More Information: Event Log Online Help

Copy

Level: Information Keywords:

User: N/A Computer:

OpCode: Info

More Information: Event Log Online Help

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...

ft Wind...

This Ev...

vents...

Look for an event listing like the one pictured. Note the event tells us an account failed to log on. Select copy to get a copy of the log entry.

5:05 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

Untitled - Notepad

File Edit Format View Help

```
Log Name:      Security
Source:        Microsoft-Windows-Security-Auditing
Date:          2/12/2012 4:57:37 PM
Event ID:      4625
Task Category: Logon
Level:         Information
Keywords:      Audit Failure
User:          N/A
Computer:      preuss-win7-x64
Description:
An account failed to log on.

Subject:
        Security ID:            SYSTEM
        Account Name:           PREUSS-WIN7-X64$
        Account Domain:         MAIT
        Logon ID:               0x3e7

Logon Type:                     2

Account For Which Logon Failed:
        Security ID:            NULL SID
        Account Name:           preuss
        Account Domain:         PREUSS-WIN7-X64

Failure Information:
        Failure Reason:         Unknown user name or bad password.
        Status:                 0xc000006d
        Sub Status:             0xc000006a

Process Information:
        Caller Process ID:      0xa9c
        Caller Process Name:    C:\Windows\System32\winlogon.exe
```

This part of the log entry. It gives us all the detail we need. We see the description: An account failed to log on. We also see what account failed to logon, preuss.

OpCode: Info

More Information: Event Log Online Help

Help

5:06 PM
2/12/2012

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

vmware