

## failed (4625) logins

RDP Brute Force failed logins.

Time	Event
2025-05-28T14:01:01+0530	<p>05/28/2025 02:01:01 PM LogName=Security EventCode=4625 EventType=0 ComputerName=DESKTOP-F049LOK SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=738057 Keywords=Audit Failure TaskCategory=Logon OpCode=Info Message=An account failed to log on.</p> <p>Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0</p> <p>Logon Type:3</p> <p>Account For Which Logon Failed: Security ID:S-1-0-0 Account Name:testuser Account Domain:</p> <p>Failure Information: Failure Reason:Unknown user name or bad password. Status:0xC000006D Sub Status:0xC000006A</p> <p>Process Information: Caller Process ID:0x0 Caller Process Name:-</p> <p>Network Information: Workstation Name:kali Source Network Address:192.168.246.131 Source Port:0</p> <p>Detailed Authentication Information: Logon Process:NtLmSsp Authentication Package:NTLM Transited Services:- Package Name (NTLM only):- Key Length:0</p> <p>This event is generated when a logon request fails. It is generated on the computer where access was attempted.</p> <p>The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.</p> <p>The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network).</p> <p>The Process Information fields indicate which account and process on the system requested the logon.</p> <p>The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.</p> <p>The authentication information fields provide detailed information about this specific logon request.</p> <ul style="list-style-type: none"><li>- Transited services indicate which intermediate services have participated in this logon request.</li><li>- Package name indicates which sub-protocol was used among the NTLM protocols.</li><li>- Key length indicates the length of the generated session key. This will be 0 if no session key was requested.</li></ul>

Time	Event
2025-05-28T14:01:01+0530	<p>05/28/2025 02:01:01 PM</p> <p>LogName=Security  EventCode=4625  EventType=0  ComputerName=DESKTOP-F049LOK  SourceName=Microsoft Windows security auditing.  Type=Information  RecordNumber=738054  Keywords=Audit Failure  TaskCategory=Logon  OpCode=Info  Message=An account failed to log on.</p> <p>Subject:  Security ID:S-1-0-0  Account Name:-  Account Domain:-  Logon ID:0x0</p> <p>Logon Type:3</p> <p>Account For Which Logon Failed:  Security ID:S-1-0-0  Account Name:testuser  Account Domain:</p> <p>Failure Information:  Failure Reason:Unknown user name or bad password.  Status:0xC000006D  Sub Status:0xC000006A</p> <p>Process Information:  Caller Process ID:0x0  Caller Process Name:-</p> <p>Network Information:  Workstation Name:kali  Source Network Address:192.168.246.131  Source Port:0</p> <p>Detailed Authentication Information:  Logon Process:NtLmSsp  Authentication Package:NTLM  Transited Services:-  Package Name (NTLM only):-  Key Length:0</p> <p>This event is generated when a logon request fails. It is generated on the computer where access was attempted.</p> <p>The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.</p> <p>The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network).</p> <p>The Process Information fields indicate which account and process on the system requested the logon.</p> <p>The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.</p> <p>The authentication information fields provide detailed information about this specific logon request.</p> <ul style="list-style-type: none"> <li>- Transited services indicate which intermediate services have participated in this logon request.</li> <li>- Package name indicates which sub-protocol was used among the NTLM protocols.</li> <li>- Key length indicates the length of the generated session key. This will be 0 if no session key was requested.</li> </ul>

Time	Event
2025-05-28T14:01:01+0530	<p>05/28/2025 02:01:01 PM</p> <p>LogName=Security  EventCode=4625  EventType=0  ComputerName=DESKTOP-F049LOK  SourceName=Microsoft Windows security auditing.  Type=Information  RecordNumber=738050  Keywords=Audit Failure  TaskCategory=Logon  OpCode=Info  Message=An account failed to log on.</p> <p>Subject:  Security ID:S-1-0-0  Account Name:-  Account Domain:-  Logon ID:0x0</p> <p>Logon Type:3</p> <p>Account For Which Logon Failed:  Security ID:S-1-0-0  Account Name:testuser  Account Domain:</p> <p>Failure Information:  Failure Reason:Unknown user name or bad password.  Status:0xC000006D  Sub Status:0xC000006A</p> <p>Process Information:  Caller Process ID:0x0  Caller Process Name:-</p> <p>Network Information:  Workstation Name:kali  Source Network Address:192.168.246.131  Source Port:0</p> <p>Detailed Authentication Information:  Logon Process:NtLmSsp  Authentication Package:NTLM  Transited Services:-  Package Name (NTLM only):-  Key Length:0</p> <p>This event is generated when a logon request fails. It is generated on the computer where access was attempted.</p> <p>The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.</p> <p>The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network).</p> <p>The Process Information fields indicate which account and process on the system requested the logon.</p> <p>The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.</p> <p>The authentication information fields provide detailed information about this specific logon request.</p> <ul style="list-style-type: none"> <li>- Transited services indicate which intermediate services have participated in this logon request.</li> <li>- Package name indicates which sub-protocol was used among the NTLM protocols.</li> <li>- Key length indicates the length of the generated session key. This will be 0 if no session key was requested.</li> </ul>

Time	Event
2025-05-28T14:01:00+0530	<p>05/28/2025 02:01:00 PM</p> <p>LogName=Security  EventCode=4625  EventType=0  ComputerName=DESKTOP-F049LOK  SourceName=Microsoft Windows security auditing.  Type=Information  RecordNumber=738045  Keywords=Audit Failure  TaskCategory=Logon  OpCode=Info  Message=An account failed to log on.</p> <p>Subject:  Security ID:S-1-0-0  Account Name:-  Account Domain:-  Logon ID:0x0</p> <p>Logon Type:3</p> <p>Account For Which Logon Failed:  Security ID:S-1-0-0  Account Name:testuser  Account Domain:</p> <p>Failure Information:  Failure Reason:Unknown user name or bad password.  Status:0xC000006D  Sub Status:0xC000006A</p> <p>Process Information:  Caller Process ID:0x0  Caller Process Name:-</p> <p>Network Information:  Workstation Name:kali  Source Network Address:192.168.246.131  Source Port:0</p> <p>Detailed Authentication Information:  Logon Process:NtLmSsp  Authentication Package:NTLM  Transited Services:-  Package Name (NTLM only):-  Key Length:0</p> <p>This event is generated when a logon request fails. It is generated on the computer where access was attempted.</p> <p>The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.</p> <p>The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network).</p> <p>The Process Information fields indicate which account and process on the system requested the logon.</p> <p>The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.</p> <p>The authentication information fields provide detailed information about this specific logon request.</p> <ul style="list-style-type: none"> <li>- Transited services indicate which intermediate services have participated in this logon request.</li> <li>- Package name indicates which sub-protocol was used among the NTLM protocols.</li> <li>- Key length indicates the length of the generated session key. This will be 0 if no session key was requested.</li> </ul>

Time	Event
2025-05-28T13:45:21+0530	<p>05/28/2025 01:45:21 PM</p> <p>LogName=Security  EventCode=4625  EventType=0  ComputerName=DESKTOP-F049LOK  SourceName=Microsoft Windows security auditing.  Type=Information  RecordNumber=737152  Keywords=Audit Failure  TaskCategory=Logon  OpCode=Info  Message=An account failed to log on.</p> <p>Subject:  Security ID:S-1-0-0  Account Name:-  Account Domain:-  Logon ID:0x0</p> <p>Logon Type:3</p> <p>Account For Which Logon Failed:  Security ID:S-1-0-0  Account Name:root  Account Domain:testuser</p> <p>Failure Information:  Failure Reason:Unknown user name or bad password.  Status:0xC000006D  Sub Status:0xC0000064</p> <p>Process Information:  Caller Process ID:0x0  Caller Process Name:-</p> <p>Network Information:  Workstation Name:kali  Source Network Address:192.168.246.131  Source Port:0</p> <p>Detailed Authentication Information:  Logon Process:NtLmSsp  Authentication Package:NTLM  Transited Services:-  Package Name (NTLM only):-  Key Length:0</p> <p>This event is generated when a logon request fails. It is generated on the computer where access was attempted.</p> <p>The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.</p> <p>The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network).</p> <p>The Process Information fields indicate which account and process on the system requested the logon.</p> <p>The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.</p> <p>The authentication information fields provide detailed information about this specific logon request.</p> <ul style="list-style-type: none"> <li>- Transited services indicate which intermediate services have participated in this logon request.</li> <li>- Package name indicates which sub-protocol was used among the NTLM protocols.</li> <li>- Key length indicates the length of the generated session key. This will be 0 if no session key was requested.</li> </ul>