# successful (4624) logins

## RDP Brute Force Successful Logins

| Time | Event |
| --- | --- |
| 2025-05-28T14:01:02+0530 | 05/28/2025 02:01:02 PM<br>LogName=Security<br>EventCode=4624<br>EventType=0<br>ComputerName=DESKTOP-F049LOK<br>SourceName=Microsoft Windows security auditing.<br>Type=Information<br>RecordNumber=738060<br>Keywords=Audit Success<br>TaskCategory=Logon<br>OpCode=Info<br>Message=An account was successfully logged on.<br><br>Subject:<br>Security ID:S-1-0-0<br>Account Name:-<br>Account Domain:-<br>Logon ID:0x0<br><br>Logon Information:<br>Logon Type:3<br>Restricted Admin Mode:-<br>Virtual Account:No<br>Elevated Token:No<br><br>Impersonation Level:Impersonation<br><br>New Logon:<br>Security ID:S-1-5-21-743153983-3650556082-3479164291-1002<br>Account Name:testuser<br>Account Domain:DESKTOP-F049LOK<br>Logon ID:0xE79E13<br>Linked Logon ID:0x0<br>Network Account Name:-<br>Network Account Domain:-<br>Logon GUID:{00000000-0000-0000-0000-000000000000}<br><br>Process Information:<br>Process ID:0x0<br>Process Name:-<br><br>Network Information:<br>Workstation Name:kali<br>Source Network Address:192.168.246.131<br>Source Port:0<br><br>Detailed Authentication Information:<br>Logon Process:NtLmSsp<br>Authentication Package:NTLM<br>Transited Services:-<br>Package Name (NTLM only):NTLM V2<br>Key Length:128<br><br>This event is generated when a logon session is created. It is generated on the computer that was accessed.<br><br>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.<br><br>The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network).<br><br>The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on.<br><br>The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.<br><br>The impersonation level field indicates the extent to which a process in the logon session can impersonate.<br><br>The authentication information fields provide detailed information about this specific logon request.<br>- Logon GUID is a unique identifier that can be used to correlate this event with a KDC event.<br>- Transited services indicate which intermediate services have participated in this logon request.<br>- Package name indicates which sub-protocol was used among the NTLM protocols.<br>- Key length indicates the length of the generated session key. This will be 0 if no session key was requested. |

| Time | Event |
| --- | --- |
| 2025-05-28T13:45:32+0530 | 05/28/2025 01:45:32 PM<br>LogName=Security<br>EventCode=4624<br>EventType=0<br>ComputerName=DESKTOP-F049LOK<br>SourceName=Microsoft Windows security auditing.<br>Type=Information<br>RecordNumber=737167<br>Keywords=Audit Success<br>TaskCategory=Logon<br>OpCode=Info<br>Message=An account was successfully logged on.<br><br>Subject:<br>Security ID:S-1-0-0<br>Account Name:-<br>Account Domain:-<br>Logon ID:0x0<br><br>Logon Information:<br>Logon Type:3<br>Restricted Admin Mode:-<br>Virtual Account:No<br>Elevated Token:No<br><br>Impersonation Level:Impersonation<br><br>New Logon:<br>Security ID:S-1-5-21-743153983-3650556082-3479164291-1002<br>Account Name:testuser<br>Account Domain:DESKTOP-F049LOK<br>Logon ID:0xE04898<br>Linked Logon ID:0x0<br>Network Account Name:-<br>Network Account Domain:-<br>Logon GUID:{00000000-0000-0000-0000-000000000000}<br><br>Process Information:<br>Process ID:0x0<br>Process Name:-<br><br>Network Information:<br>Workstation Name:kali<br>Source Network Address:192.168.246.131<br>Source Port:0<br><br>Detailed Authentication Information:<br>Logon Process:NtLmSsp<br>Authentication Package:NTLM<br>Transited Services:-<br>Package Name (NTLM only):NTLM V2<br>Key Length:128<br><br>This event is generated when a logon session is created. It is generated on the computer that was accessed.<br><br>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.<br><br>The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network).<br><br>The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on.<br><br>The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.<br><br>The impersonation level field indicates the extent to which a process in the logon session can impersonate.<br><br>The authentication information fields provide detailed information about this specific logon request.<br>- Logon GUID is a unique identifier that can be used to correlate this event with a KDC event.<br>- Transited services indicate which intermediate services have participated in this logon request.<br>- Package name indicates which sub-protocol was used among the NTLM protocols.<br>- Key length indicates the length of the generated session key. This will be 0 if no session key was requested. |