Lateral Movement Detection

Time	Event
2025-05-28T21:53:22+0530	05/28/2025 09:53:22 PM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-F049LOK SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=791230 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Logon Information: Logon Type:3 Restricted Admin Mode:- Virtual Account:No Elevated Token:No Impersonation Level:Impersonation New Logon: Security ID:S-1-5-21-743153983-3650556082-3479164291-1002 Account Name:testuser Account Domain:DESKTOP-F049LOK Logon ID:0x281338 Linked Logon ID:0x0 Network Account Name:- Network Account Domain:- Logon GUID:{00000000-0000-0000-0000-000000000000} Process Information: Process ID:0x0 Process Name:- Network Information: Workstation Name:- Source Network Address:192.168.246.131 Source Port:53684 Detailed Authentication Information: Logon Process:NtLmSsp Authentication Package:NTLM Transited Services:- Package Name (NTLM only):NTLM V2 Key Length:0 This event is generated when a logon session is created. It is generated on the computer that was accessed. 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. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.

Time	Event
2025-05-28T21:53:11+0530	05/28/2025 09:53:11 PM LogName=Security EventCode=4625 EventType=0 ComputerName=DESKTOP-F049LOK SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=791208 Keywords=Audit Failure TaskCategory=Logon OpCode=Info Message=An account failed to log on. Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Logon Type:3 Account For Which Logon Failed: Security ID:S-1-0-0 Account Name:testuser Account Domain:DESKTOP-F049LOK Failure Information: Failure Reason:Unknown user name or bad password. Status:0xC000006D Sub Status:0xC000006A Process Information: Caller Process ID:0x0 Caller Process Name:- Network Information: Workstation Name:- Source Network Address:192.168.246.131 Source Port:46828 Detailed Authentication Information: Logon Process:NtLmSsp Authentication Package:NTLM Transited Services:- Package Name (NTLM only):- Key Length:0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. 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. The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. 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. The authentication information fields provide detailed information about this specific logon request. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.