RDP DFIR

Successful Remote Interactive Logon

- **Security**
  - **EID 4624** — An account was successfully logged on — Logon Types
    - If NLA is enabled a 4624 event with logon type 3 will be logged before one of these logon types
    - 10 — Successful User Account RemoteInteractive Logon
    - 12 — Successful User Account RemoteInteractive Logon Using Cached Credentials
    - 7 — Successful User Account RemoteInteractive Logon : Workstation was Unlocked
  - **EID 4776** — The domain controller attempted to validate the credentials for an account
    - Error Code — *0x0* — Successful Logon
    - This event occurs only on the computer that is authoritative for the provided credentials. For domain accounts, the domain controller is authoritative. For local accounts, the local computer is authoritative.
    - It shows successful and unsuccessful credential validation attempts.
    - Logon Account : the name of the account that had its credentials validated by the Authentication Package.
    - Source Workstation : The name of the computer from which the logon attempt originated.
- **TerminalServices-RemoteConnectionManager**
  - **EID 261** — Listener X received a connection — Service listening for inbound connection requests over the RDP Protocol
  - **EID 1149** — Remote Desktop Services: User authentication succeeded
    - An Event ID 1149 DOES NOT indicate successful authentication to a target, simply a successful RDP network connection
    - If you specify the RestrictedAdmin option, the username and domain will be blank.
    - If you turn off NLA and log on with Rdesktop, ID 1149 will not be recorded.
  - **EID 1158** — Remote Desktop Services accepted a connection from IP address
    - This will be available in the Administrative log records
    - Will also display the source IP
- **TerminalServices-LocalSessionManager**
  - **EID 41** — Begin session arbitration — Provides the session ID for potential correlations with other events
  - **EID 42** — End session arbitration — Provides the session ID for potential correlations with other events
  - **EID 21** — Remote Desktop Services: Session logon succeeded
    - If the source network address is not LOCAL the IP is the source of the remote authentication
    - Also provides the session ID
  - **EID 22** — Remote Desktop Services: Shell start notification received
    - If the source network address is not LOCAL the IP is the source of the Remote authentication
    - Also provides the session ID
  - **EID 25** — Remote Desktop Services: Session reconnection succeeded
    - Also provides the session ID
    - Also provides the source IP
  - **EID 24** — Remote Desktop Services: Session has been disconnecte
    - Also provides the session ID
    - Also provides the source IP
- **RemoteDesktopServices-RdpCoreTS** — **EID 131** — The server accepted a new TCP connection from client SOURCE IP:PORT.

Unsuccessful Remote Interactive Logon

NLA Enabled

- **Security**
  - **NTLM** — **EID 4776** — The domain controller attempted to validate the credentials for an account
    - Suspicious Error Codes
      - *0xC0000064* — User name does not exist
      - *0xC0000070* — User logon from unauthorized workstation
      - *0xC0000072* — User logon to account disabled by administrator
      - *0xC000006F* — User logon outside authorized hours
      - *0xC0000413* — Logon Failure: The machine you are logging onto is protected by an authentication firewall. The specified account is not allowed to authenticate to the machine
      - *0xC000018C* — The logon request failed because the trust relationship between the primary domain and the trusted domain failed
      - *0xC000015B* — The user has not been granted the requested logon type (aka logon right) at this machine
    - This event occurs only on the computer that is authoritative for the provided credentials. For domain accounts, the domain controller is authoritative. For local accounts, the local computer is authoritative.
    - It shows successful and unsuccessful credential validation attempts.
    - Logon Account : the name of the account that had its credentials validated by the Authentication Package.
    - Source Workstation : The name of the computer from which the logon attempt originated.
  - **Kerberos** — **EID 4771** — Kerberos pre-authentication failed
    - Account Name = Source host
    - Client Address = Source IP.
    - Common Failure Codes
      - 0x6 — Bad user name, or new computer/user account has not replicated to DC yet
      - 0x7 — New computer account has not replicated yet or computer is pre-w2k
      - 0x9 — administrator should reset the password on the account
      - 0xC — Workstation restriction
      - 0x12 — Account disabled, expired, locked out, logon hours.
      - 0x17 — The user's password has expired.
      - 0x18 — Usually means bad password
- **TerminalServices-RemoteConnectionManager**
  - Only logged during unsuccessful remote interactive authentications for "Windows Server 2008" and "Windows SBS Server 2011"
  - **EID 1149** — Remote Desktop Services: User authentication succeeded
    - An Event ID 1149 DOES NOT indicate successful authentication to a target, simply a successful RDP network connection
    - if username and domain are blank that can be due to the specification of RestrictedAdmin option
    - If you turn off NLA and log on with Rdesktop, ID 1149 will not be recorded.
  - **EID 261** — Listener X received a connection — Service listening for inbound connection requests over the RDP Protocol
- **RemoteDesktopServices-RdpCoreTS**
  - **EID 140**
    - A connection from the client computer with an IP address of SOURCE IP failed because the user name or password is not correct.
    - Despite the event description it will only be recorded when the user name DOES NOT EXIST
    - For a username that exists use a correlation between EID 4625 & EID 131
  - **EID 131**
    - The server accepted a new TCP connection from client SOURCE IP:PORT.
    - Records the source IP of every RDP authentication attempt
    - To be correlated with EID 4625 in order to identify the source IP (depending on the OS version)

In both cases will be followed by EID 4625 with Logon Type 3 due to NLA enablement

NLA Disabled

- **Security** — **EID 4625** — An account failed to log on
  - RDP Security Layer must be set to RDP otherwise all pertinent details of the logon failure will not be recorded, nor will you even be able to tell that the logon attempt came over RDP
  - Logon Type = 10
  - Client Address = Source IP (depending on the OS version)
  - Account Name
- **RemoteDesktopServices-RdpCoreTS**
  - **EID 140**
    - A connection from the client computer with an IP address of SOURCE IP failed because the user name or password is not correct.
    - Despite the event description it will only be recorded when the user name DOES NOT EXIST
    - For a username that exists use a correlation between EID 4625 & EID 131
  - **EID 131**
    - The server accepted a new TCP connection from client SOURCE IP:PORT.
    - Records the source IP of every RDP authentication attempt
    - To be correlated with EID 4625 in order to identify the source IP (depending on the OS version)

Others

- **Security**
  - **EID 4778** — A session was reconnected to a Window Station
    - Account Name
    - Source IP
  - **EID 4779** — A session was disconnected from a Window Station
    - Account Name
    - Source IP
  - **EID 4688** — Process Creation — rdpclip.exe

References

- https://purerds.org/remote-desktop-security/auditing-remote-desktop-services-logon-failures-1/
- https://portl39.hatenablog.com/entry/2019/03/23/091740
- https://ponderthebits.com/2018/02/windows-rdp-related-event-logs-identification-tracking-and-investigation/
- https://www.13cubed.com/downloads/rdp_flowchart.pdf
- https://dfironthemountain.wordpress.com/2019/02/15/rdp-event-log-dfir/