18.9.59.3.9.4 (L1) Ensure 'Require user authentication for remote connections by using Network Level Authentication' is set to 'Enabled' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting allows you to specify whether to require user authentication for remote connections to the RD Session Host server by using Network Level Authentication.

The recommended state for this setting is: `Enabled`.

Rationale:

Requiring that user authentication occur earlier in the remote connection process enhances security.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services:UserAuthentication
```

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled`:

```
Computer Configuration\Policies\Administrative Templates\Windows
Components\Remote Desktop Services\Remote Desktop Session
Host\Security\Require user authentication for remote connections by using
Network Level Authentication
```

Note: This Group Policy path is provided by the Group Policy template `TerminalServer.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.
Note #2: In the Microsoft Windows Vista Administrative Templates, this setting was initially named *Require user authentication using RDP 6.0 for remote connections*, but it was renamed starting with the Windows Server 2008 (non-R2) Administrative Templates.

Impact:

Only client computers that support Network Level Authentication can connect to the RD Session Host server.

Note: Some third party two-factor authentication solutions (e.g. RSA Authentication Agent) can be negatively affected by this setting, as Network Level Authentication will expect the user's Windows password, and once successfully authenticated, pass the credential along to the Windows session on the RDP host (to complete the login). If a two-factor agent is present and expecting a different credential at the RDP logon screen, this initial connection may result in a failed logon attempt.

Default Value:

Windows Server 2008 R2 and older: Disabled.

Windows Server 2012 (non-R2) and newer: Enabled.

References:

1. CCE-37330-8

CIS Controls:

Version 6

3.4 Use Only Secure Channels For Remote System Administration
Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.

Version 7

4.5 Use Multifactor Authentication For All Administrative Access
Use multi-factor authentication and encrypted channels for all administrative account access.