Second Hop Remoting with PowerShell

examlabpractice.com

The “Second hop problem”

The "second hop problem" refers to a situation like the following:

1. You are logged in to ServerA
2. From ServerA, you start a remote PowerShell session to connect to ServerB
3. A command you run on ServerB via your PowerShell Remoting session attempts to access a resource on ServerC
4. Access to the resource on ServerC is denied, because the credentials you used to create the PowerShell Remoting session are not passed from ServerB to ServerC

CredSSP

- You can use the Credential Security Support Provider (CredSSP) for authentication.
- CredSSP caches credentials on the remote server (ServerB), so using it opens you up to credential theft attacks.
- If the remote computer is compromised, the attacker has access to the user's credentials. CredSSP is disabled by default on both client and server computers. You should enable CredSSP only in the most trusted environments.

Pros and Cons of CredSSP

Pros

- It works for all servers with Windows Server 2008 or later.

Cons

- Has security vulnerabilities.
- Requires configuration of both client and server roles.

Activating CredSSP

On ServerA, run the Enable-WSManCredSSP

This command is shown here.

Enable-WSManCredSSP -Role Client -DelegateComputer *.examlabpractice.com -Force

Now, make a change on ServerB to permit it to use delegated credentials. This command is shown here.

Enable-WSMaCredSSP -Role Server –Force

STEP BY STEP GUIDE FOR DOING THIS CAN BE FOUND HERE:

https://devblogs.microsoft.com/scripting/enable-powershell-second-hop-functionality-with-credssp/

Kerberos Delegation

- Using resource-based Kerberos delegation (introduced in Windows Server 2012), you configure credential delegation on the server object where resources reside.
- In the second hop scenario, you configure ServerC to specify from where it accepts delegated credentials.

Pros and Cons of Kerberos Delegation

Pros

- Credentials are not stored.
- Configured using PowerShell cmdlets. No special coding required.
- Does not require Domain Administrator access to configure.
- Works across domains and forests.

Cons

- Requires Windows Server 2012 or later.
- Does not support the second hop for WinRM.
- Requires rights to update objects and Service Principal Names (SPNs).

Activating Kerberos Delegation