Modern RDP security

Ing. Ondřej Ševeček | GOPAS a.s. |
MCSM:Directory | MVP:Enterprise Security | CEH | CHFI | CISA |
ondrej@sevecek.com | www.sevecek.com |

moje kurzy v GOPASu

GLAB007 - capture the flag 1 - hackni si podnikovou síť
GLAB008 - capture the flag 2 - hackni si podnikovou síť
GOC175 - implementace bezpečnosti
GOC169 - ISO 27001
GOC172 - Kerberos troubleshooting
Agenda

• Password transport in full
• SSO principles
• Channel encryption with SSL/Kerberos/NLA
• User access to secure RDP servers
• Admin access to insecure endpoints
The problem

• **clean** password transport by default to enable SSO
  – SSL encrypted?!
  – transport on all versions, in-memory permanently until 2012 R2 and Windows 8.1

• compare with Enter-PSSession
  – double-hop authentication
  – Get-WSManCredSSP
  – Enable-WSManCredSSP -Role Client -DelegateComp
  – Enable-WSManCredSSP -Role Server
  – Enter-PSSession -Authentication CredSSP -Credential (Get-Credential)
The default scenario

- Client
  - Kerberos NLA pre-authentication
  - Full password
  - SSL encrypted

- RDP server
  - Certificate

- Second hop server
- Second hop server
The default scenario

- Client
- Kerberos NLA pre-authentication
- Full password
- SSL encrypted

RDP server
- Certificate
- TGT
- TGS

Second hop server
- Second hop server
Transport protection

- never ever skip **warnings**!
- verify lock icon!
  - NLA
  - valid SSL certificate on non-Kerberos scenarios
  - Kerberos authentication
    - or **both**
  - servicePrincipalName: TERMSRV/rdp.gopas.cz
Require server authentication on clients

![Image of RDP Client Require Server Authentication settings]

<table>
<thead>
<tr>
<th>Policy</th>
<th>Setting</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure server authentication for client</td>
<td>Enabled</td>
<td>Do not connect if authentication fails</td>
</tr>
</tbody>
</table>

Policy definitions (ADMX files) retrieved from the central store.
Two scenarios

• user access
  – limited user works on a secure server

• admin access
  – powerful privileged admin connects to insecure machines
User access

- limit password exposure
  - RDP SSO since Windows Vista/7/2008
  - prevent saving passwords

- never send clean password
  - /remoteGuard since Windows 10/2016
  - does not need Credentials Guard enabled on either side
Deny saving RDP passwords on clients

<table>
<thead>
<tr>
<th>Policy</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network access: Do not allow storage of passwords and credentials for network authentication</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Policy</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do not allow passwords to be saved</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
RDP SSO for limited users (2012R2/8.1 and older)

- **Client**
  - full password
  - Kerberos NLA pre-authentication
  - full password
  - ssl encrypted

- **RDP Server**
  - cert
  - TGT
  - TGS

- **Second Hop Server**
  - second hop server
  - second hop server

- **Encryption**
  - ssl encrypted
Client RDP SSO settings for standard users (2008/Vista/7+)
Remote Guard for limited users (2016/10 and newer)
RemoteGuard requirements

• Kerberos server authentication + Kerberos user NLA authentication
• Windows 10.1607+, Windows 2016+

• HKLM\System\CurrentControlSet\Control\LSA
  – DisableRestrictedAdmin = DWORD = 0
  – must be enabled on the remote RDP server

• /remoteGuard cmd switch requires Administrators membership
  – user get "The requested session access is denied" for non-Administrators
• use GPO client enforcement for non-Administrators
Enforce RemoteGuard on clients with GPO for non-Administrators
Admin access

• /restrictedAdmin
  – since 2012 R2/8.1
  – since 7/2008 R2 with update

• HKLM\System\CurrentControlSet\Control\LSA
  – DisableRestrictedAdmin = DWORD = 0
Restricted Admin mode (Windows 2012 R2/8.1 and update for 2008 R2/7 and newer)
Enforce restricted admin

• GPO forcing admin clients to use /restrictedAdmin

• Authentication policies
  – client with NLA
  – server even without NLA
  – Windows 2008R2/7 blocked by default
Děkuji za pozornost

moje kurzy v GOPASu

GLAB007 - capture the flag 1 - hackni si podnikovou síť
GLAB008 - capture the flag 2 - hackni si podnikovou síť
GOC175 - implementace bezpečnosti
GOC169 - ISO 27001
GOC172 - Kerberos troubleshooting

www.gopas.cz