Exploitable External   
Service

Graphical user interface, application

Description automatically generated

Summary

Attack Explains: After the compromised Piwigo web server, we are going to pivot to the brailee.ogden windows 10. We are using the credentials we found in qdpm and try to access target’s windows account by using Evil-winrm. After gained access to the windows, we are going to execute Invoke-Snows to bypass powershell command limitation.

Target Address: 192.168.3.80

Target System: Windows 10 Password: ‘Winter2022’, ‘vagrant’

Target Account: brailee.ogden (windows account), vagrant (reverse shell)

Tools: SSh, Evil-winrm, Invoke-Snow.ps1, Proxychains

Establish ssh connection to access vagrant account to pivot to windows 10.

Text

Description automatically generated

Download Evil-winrm in Red directory.

Text

Description automatically generated

Check the red directory if Evil-winrm is download successfully.

Text

Description automatically generated

We are going to execute the evil-winrm.rb file.

Graphical user interface, text

Description automatically generated

Creating scripts directory to put the Invoke-snow.ps1

Graphical user interface, text, chat or text message, website

Description automatically generated

We are going to create Invoke-Snow.ps1 by adding base64 code of AMSI bypass in scripts directory in evil-winrm folder.

Text

Description automatically generated

Verify Invoke-Snow.ps1, we can see the code works as disable security of the system

Text

Description automatically generated

to pivot and access windows 10, we can proxychains and use brailee.ogden’s credentials.

And using -s to access the scripts folder so we can execute Invoke-Snow.ps1

Text

Description automatically generated

At first, when we try to execute “amsiutils” command, the command is blocked.

After executing “Invoke-Snow.ps1”, it bypasses the ASMI powershell security.

Trying to execute “ amsiutils” command, and it did not show the error response meaning the ASMI bypass Invoke-Snow.ps1 executed successfully.

Text

Description automatically generated