

## TASK 2

# Analyze a Related Suspicious File

Rev E

# Analyze a Related Suspicious File

1	Comparing Binaries Using Relyze .....	3
2	Crack and Decrypt the Password.....	5
3	Converting From HEX to ASCII .....	9
4	Run the Program.....	10
5	Connect to the IRC Channel.....	12
5.1	Open PuTTY.....	12
5.1.1	Input Host Name.....	13
5.1.2	Input Username.....	14
5.1.3	Input Password .....	14
5.2	Input irssi.....	15
5.2.1	Set Nickname .....	16
5.2.2	Request Network List.....	16
5.2.3	Connect to network (somber) .....	17
5.2.4	Join #nymeria.....	18
5.3	Observe conversation .....	18
5.3.1	Identify Other Players .....	19
5.3.2	See Who the Players Are .....	19

# Analyze a Related Suspicious File

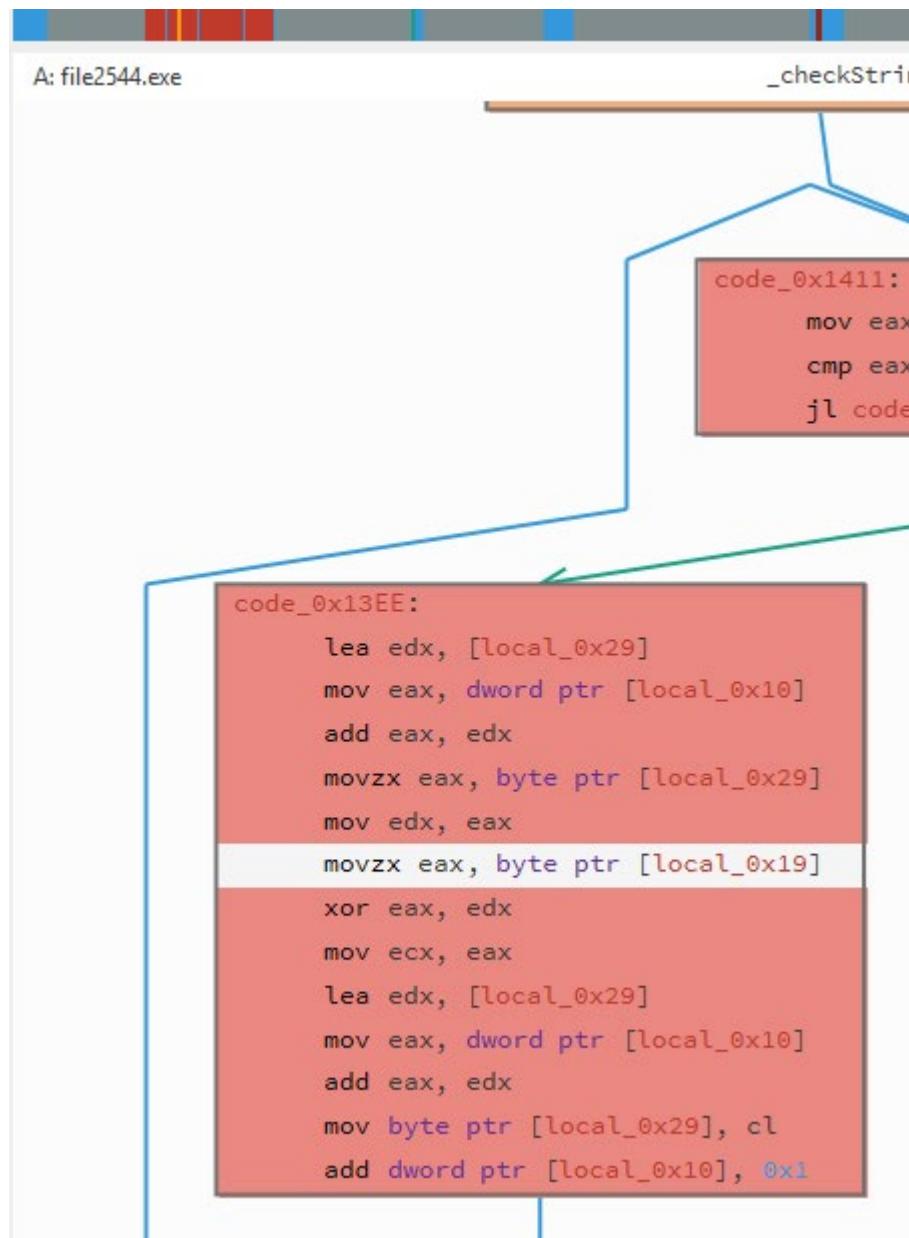
## 1 Comparing Binaries Using Relyze

In Relyze we see in code\_0x13EE:

```
xor eax, edx
```

and just above it

```
movzx eax, byte ptr [local_0x19]
```



## Analyze a Related Suspicious File

Search local\_0x19 it brings you to what appears could be an obfuscated password

```
push ebp
mov ebp, esp
sub esp, 0x38
mov dword ptr [local_0x14], 0x10
mov byte ptr [local_0x19], 0x41
mov byte ptr [local_0x29], 0x11
mov byte ptr [local_0x28], 0x20
mov byte ptr [local_0x27], 0x32
mov byte ptr [local_0x26], 0x32
mov byte ptr [local_0x25], 0x36
mov byte ptr [local_0x24], 0x2E
mov byte ptr [local_0x23], 0x33
mov byte ptr [local_0x22], 0x25
mov byte ptr [local_0x21], 0x12
mov byte ptr [local_0x20], 0x35
mov byte ptr [local_0x1F], 0x28
mov byte ptr [local_0x1E], 0x2D
mov byte ptr [local_0x1D], 0x2D
mov byte ptr [local_0x1C], 0x12
mov byte ptr [local_0x1B], 0x34
mov byte ptr [local_0x1A], 0x39
mov dword ptr [local_0x10], 0x0
jmp code_0x1411
```

# Analyze a Related Suspicious File

## 2 Crack and Decrypt the Password

Search for xor and key

Found in 0x13EE:

xor eax, edx

one will be the data

one will be the key

work backwards to determine which is which

```
code_0x13EE:  
    lea   edx, [local_0x29]  
    mov   eax, dword ptr [local_0x10]  
    add   eax, edx  
    movzx eax, byte ptr [local_0x29]  
    mov   edx, eax  
    movzx eax, byte ptr [local_0x19]  
    xor   eax, edx  
    mov   ecx, eax  
    lea   edx, [local_0x29]  
    mov   eax, dword ptr [local_0x10]  
    add   eax, edx  
    mov   byte ptr [local_0x29], cl  
    add   dword ptr [local_0x10], 0x1
```

One step above you can see movzx eax

```
code_0x13EE:  
    lea   edx, [local_0x29]  
    mov   eax, dword ptr [local_0x10]  
    add   eax, edx  
    movzx eax, byte ptr [local_0x29]  
    mov   edx, eax  
    movzx eax, byte ptr [local_0x19]  
    xor   eax, edx  
    mov   ecx, eax  
    lea   edx, [local_0x29]  
    mov   eax, dword ptr [local_0x10]  
    add   eax, edx  
    mov   byte ptr [local_0x29], cl  
    add   dword ptr [local_0x10], 0x1
```

Follow the path to local\_0x19 in the boxes above

# Analyze a Related Suspicious File

```
push ebp
mov ebp, esp
sub esp, 0x38
mov dword ptr [local_0x14], 0x10
mov byte ptr [local_0x19], 0x41
mov byte ptr [local_0x29], 0x11
mov byte ptr [local_0x28], 0x20
mov byte ptr [local_0x27], 0x32
mov byte ptr [local_0x26], 0x32
mov byte ptr [local_0x25], 0x36
mov byte ptr [local_0x24], 0x2E
mov byte ptr [local_0x23], 0x33
mov byte ptr [local_0x22], 0x25
mov byte ptr [local_0x21], 0x12
mov byte ptr [local_0x20], 0x35
mov byte ptr [local_0x1F], 0x28
mov byte ptr [local_0x1E], 0x2D
mov byte ptr [local_0x1D], 0x2D
mov byte ptr [local_0x1C], 0x12
mov byte ptr [local_0x1B], 0x34
mov byte ptr [local_0x1A], 0x39
mov dword ptr [local_0x10], 0x0
jmp code_0x1411
```

This shows that eax is the static value and is 41...41 is the key

With eax established now look into edx

```
code_0x13EE:
lea edx, [local_0x29]
mov eax, dword ptr [local_0x10]
add eax, edx
movzx eax, byte ptr [local_0x29]
mov edx, eax
movzx eax, byte ptr [local_0x19]
xor eax, edx
mov ecx, eax
lea edx, [local_0x29]
mov eax, dword ptr [local_0x10]
add eax, edx
mov byte ptr [local_0x29], cl
add dword ptr [local_0x10], 0x1
```

# Analyze a Related Suspicious File

```
push ebp
mov ebp, esp
sub esp, 0x38
mov dword ptr [local_0x14], 0x10
mov byte ptr [local_0x19], 0x41
mov byte ptr [local_0x29], 0x11
mov byte ptr [local_0x28], 0x20
mov byte ptr [local_0x27], 0x32
mov byte ptr [local_0x26], 0x32
mov byte ptr [local_0x25], 0x36
mov byte ptr [local_0x24], 0x2E
mov byte ptr [local_0x23], 0x33
mov byte ptr [local_0x22], 0x25
mov byte ptr [local_0x21], 0x12
mov byte ptr [local_0x20], 0x35
mov byte ptr [local_0x1F], 0x28
mov byte ptr [local_0x1E], 0x2D
mov byte ptr [local_0x1D], 0x2D
mov byte ptr [local_0x1C], 0x12
mov byte ptr [local_0x1B], 0x34
mov byte ptr [local_0x1A], 0x39
mov dword ptr [local_0x10], 0x0
jmp code_0x1411
```

Looking at the above starting at local\_0x29 and moving down...you can see that each is decreasing by 1 which has this appear to be a loop...

Using 41 as the key...cross referencing each corresponding number as a hexadecimal converting it over to ascii to get a corresponding number or letter...

Use CyberChef or XOR Cipher to convert the Hex

The screenshot shows the CyberChef interface with the following configuration:

- Operations:** Favourites (To Base64, From Base64, To Hex, From Hex, To Hexdump, From Hexdump, URL Decode, Regular expression, Entropy, Fork, Magic).
- Recipe:** From Hex → XOR.
- From Hex:** Delimiter 0x.
- XOR:** Key 41, Scheme Standard, Null preserving.
- Input:** 11203232362E33251235282020123439.
- Output:** PasswordStillSux.

# Analyze a Related Suspicious File

Search for a tool

\* SEARCH A TOOL ON dCODE BY KEYWORDS:  
e.g. type 'boolean'

\* BROWSE THE FULL dCODE TOOLS' LIST

Results

**PasswordStillSux**

XOR Cipher - [dCode](#)

Tag(s) : Modern Cryptography

Share

[+](#) [f](#) [t](#) [s](#) [m](#)

dCode and more

dCode is free and its tools are a valuable help in games, maths, geocaching, puzzles and problems to solve every day!  
A suggestion ? a feedback ? a bug ? an idea ? Write to [dCode!](#)

## XOR CIPHER

Cryptography > Modern Cryptography > XOR Cipher

**XOR DECODER**

\* TEXT TO BE XORED (MULTIPLIED BY XOR)  
Hexadecimal ASCII [00-7F] (Automatic Detection)

11 20 32 32 36 2E 33 25 12 35 28 2D 2D 12 34 39

**ENCRYPTION/DECRIPTION METHOD**

AUTOMATIC (BRUTEFORCE 1 TO 16 BYTES) ?

USE THE BINARY KEY

USE THE HEXADECIMAL KEY

USE THE ASCII KEY

KNOWING THE KEY SIZE (IN BYTES)

\* RESULTS FORMAT  ASCII (PRINTABLE) CHARACTERS

HEXADECIMAL 00-7F-FF

DECIMAL 0-127-255

OCTAL 000-177-377

BINARY 00000000-11111111

INTEGER NUMBER

FILE TO DOWNLOAD

**Summary**

- \* XOR Decoder
- \* XOR Calculator
- \* What is the XOR cipher? (Definition)
- \* How to encrypt using XOR cipher?
- \* How to decrypt XOR cipher?
- \* How to convert a text into binary?
- \* What is the truth table for XOR?
- \* How to recognize XOR ciphertext?
- \* What are the pros and cons of XOR?
- \* How to decipher XOR without the key?
- \* What are the variants of the XOR cipher?

**Similar pages**

- \* ASCII Code
- \* Binary Code

# Analyze a Related Suspicious File

## 3 Converting From HEX to ASCII

Converting file 1732 from HEX into ASCII

```
void __cdecl _checkString( int32_t p1 )
{
    uint32_t local_0x3C;
    uint32_t local_0x38;
    uint32_t local_0x34;
    uint32_t local_0x20;
    uint32_t local_0x1C;
    uint32_t local_0x18;
    uint32_t local_0x14;
    uint32_t local_0x10;

    push ebp
    mov ebp, esp
    sub esp, 0x38
    mov dword ptr [local_0x20], 0x73696854
    mov dword ptr [local_0x1C], 0x73736150
    mov dword ptr [local_0x18], 0x64726F77
    mov dword ptr [local_0x14], 0x21787553
    mov eax, dword ptr [p1]
    mov dword ptr [local_0x3C], eax
    call .idata$5_59 ; unsigned int __cdecl( char * _Str )
    cmp eax, 0x10
    jnz code_0x13FE
```

**RapidTables**

Home > Conversion > Number conversion > Hex code to ASCII text

Hex to ASCII Text String Converter

Enter hex bytes with any prefix / postfix / delimiter and press the *Convert* button  
(e.g. 45 78 61 6d 70 6C 65 21):

From To

Hexadecimal Text

Paste hex numbers or drop file

```
0x73696854
0x73736150
0x64726F77
0x21787553
```

Character encoding

ASCII

Text output ...

**RapidTables**

Home > Conversion > Number conversion > Hex code to ASCII text

Hex to ASCII Text String Converter

Enter hex bytes with any prefix / postfix / delimiter and press the *Convert* button  
(e.g. 45 78 61 6d 70 6C 65 21):

From To

Hexadecimal Text

Paste hex numbers or drop file

```
73696854
73736150
64726F77
21787553
```

Character encoding

ASCII

Text output ...

# Analyze a Related Suspicious File

Reverse the hexadecimal

Then rearrange to get proper order

The screenshots show two identical instances of the RapidTables Hex to ASCII Text String Converter. In the 'From' field, the dropdown is set to 'Hexadecimal'. In the 'To' field, the dropdown is set to 'Text'. Below these fields are 'Open File' and 'Search' buttons. A text area labeled 'Paste hex numbers or drop file' contains the following sequence of hex bytes:  
21 78 75 53  
53 75 78 21  
77 6F 72 64  
50 61 73 73  
54 68 69 73

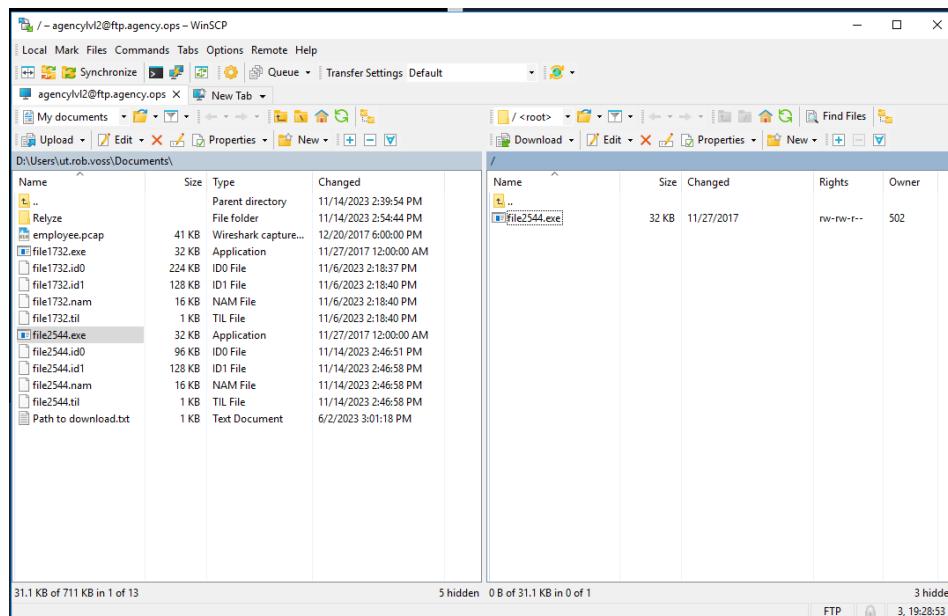
Below this area is a 'Character encoding' dropdown set to 'ASCII'. At the bottom of the interface are three buttons: 'Convert' (green), 'Reset' (grey), and 'Swap' (grey).

The second screenshot shows the result of the conversion. The output text area displays:  
54 68 69 73  
53 68 69 73  
50 61 73 73  
77 6F 72 64  
53 75 78 21

Below the output area is another 'Character encoding' dropdown also set to 'ASCII'. The 'Convert' button is visible at the bottom.

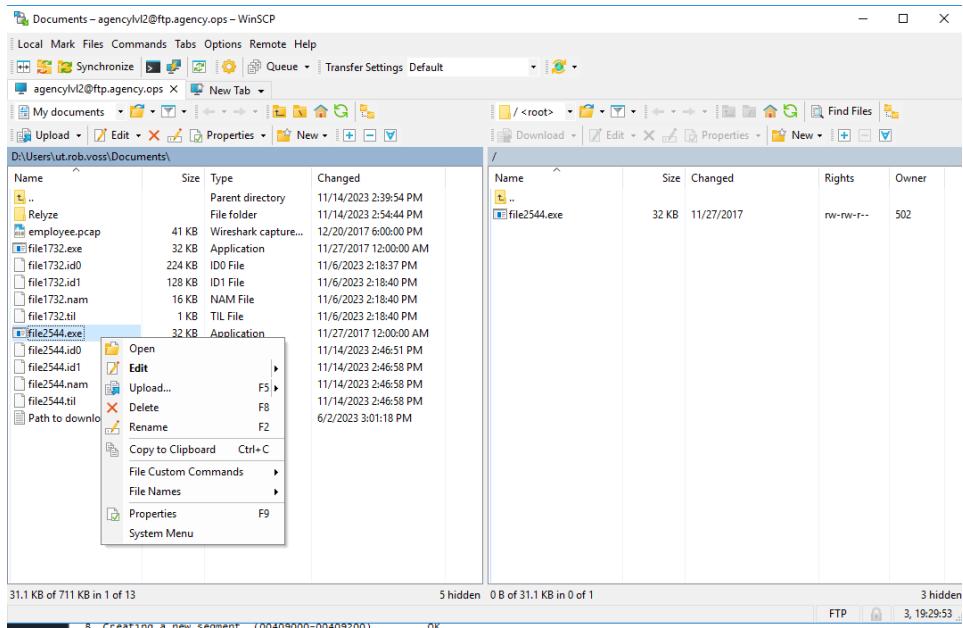
## 4 Run the Program

Open the Desktop and select the program

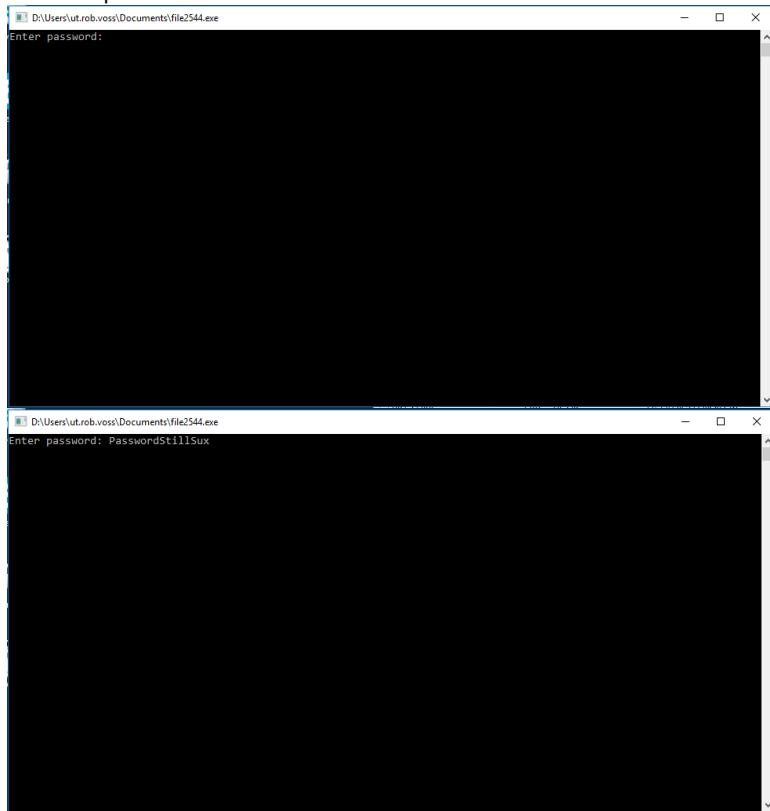


Open the program

# Analyze a Related Suspicious File

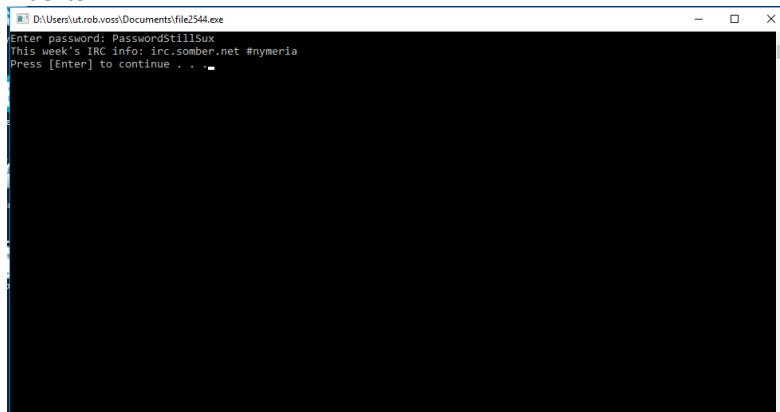


Enter the password: PasswordStillSux



# Analyze a Related Suspicious File

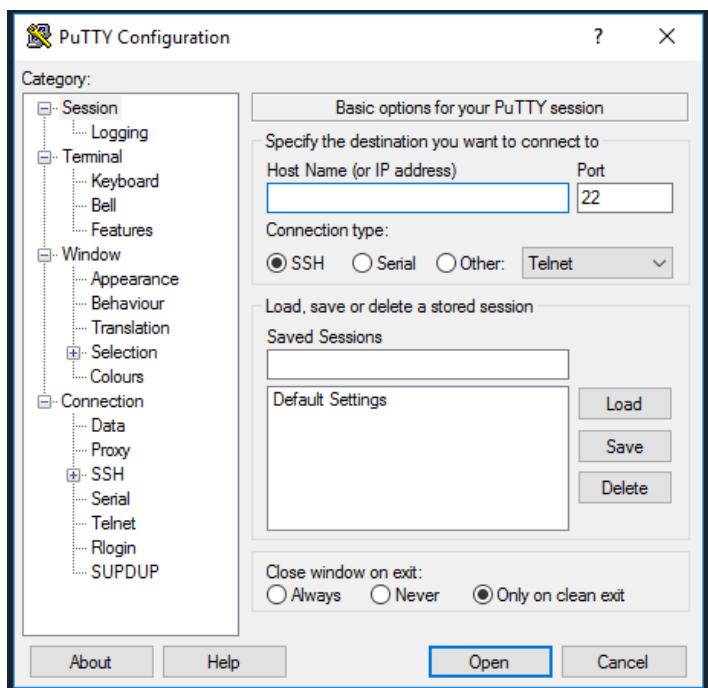
Hit enter:



D:\Users\ut\rob.voss\Documents\file2544.exe  
Enter password: PasswordStillSux  
This week's IRC info: irc.somber.net #nymeria  
Press [Enter] to continue . . .

## 5 Connect to the IRC Channel

### 5.1 Open PuTTY



IP: 10.0.100.30

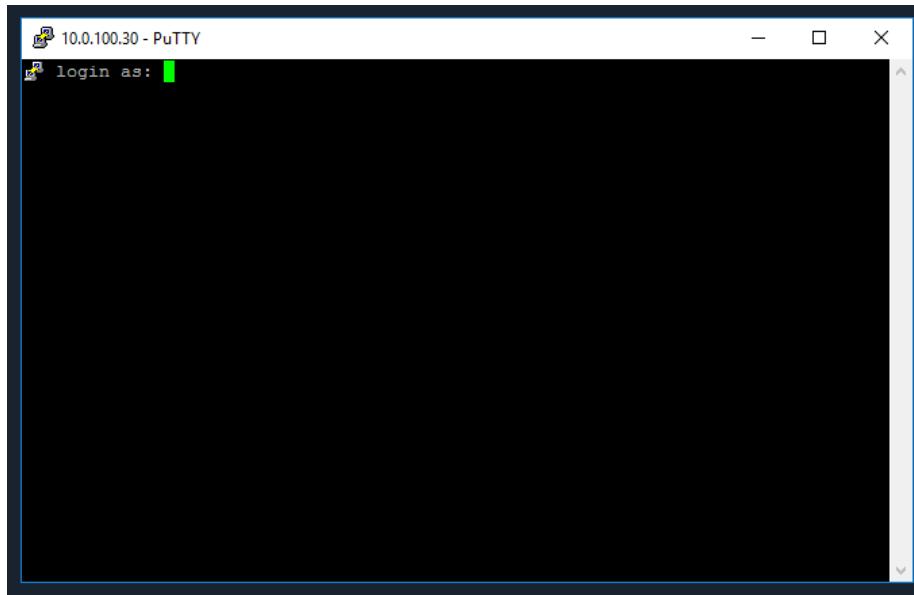
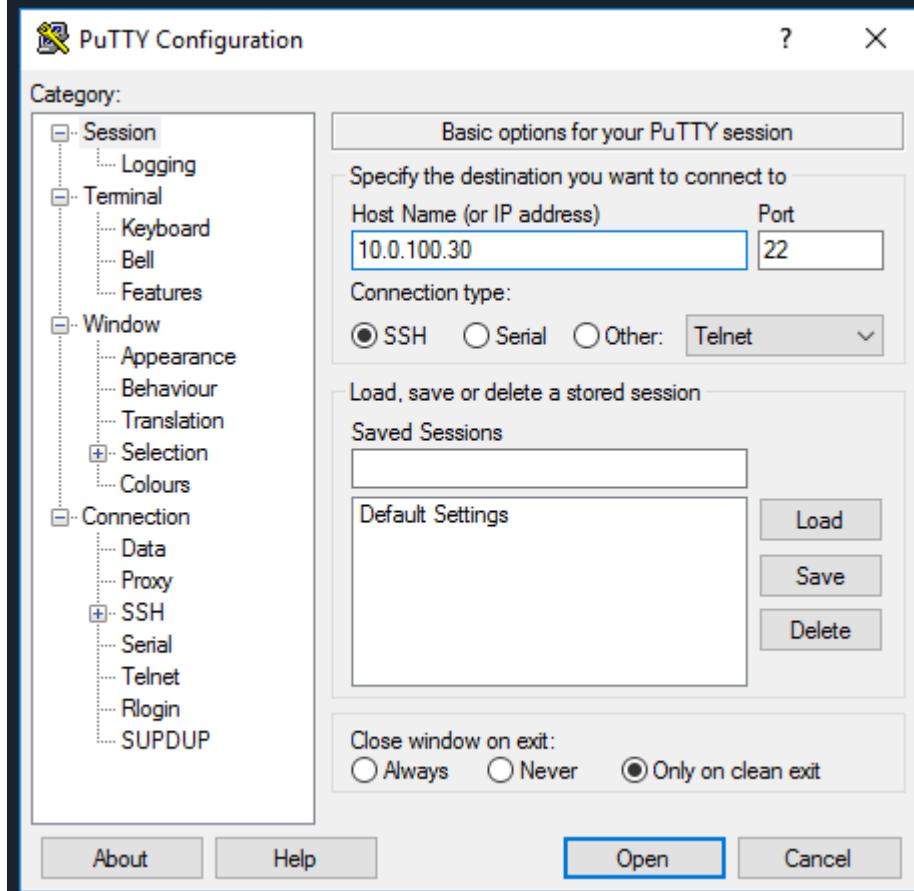
Username: traveler2721

Password: EuD3jwtre4jGIet07Tej

# Analyze a Related Suspicious File

## 5.1.1 Input Host Name

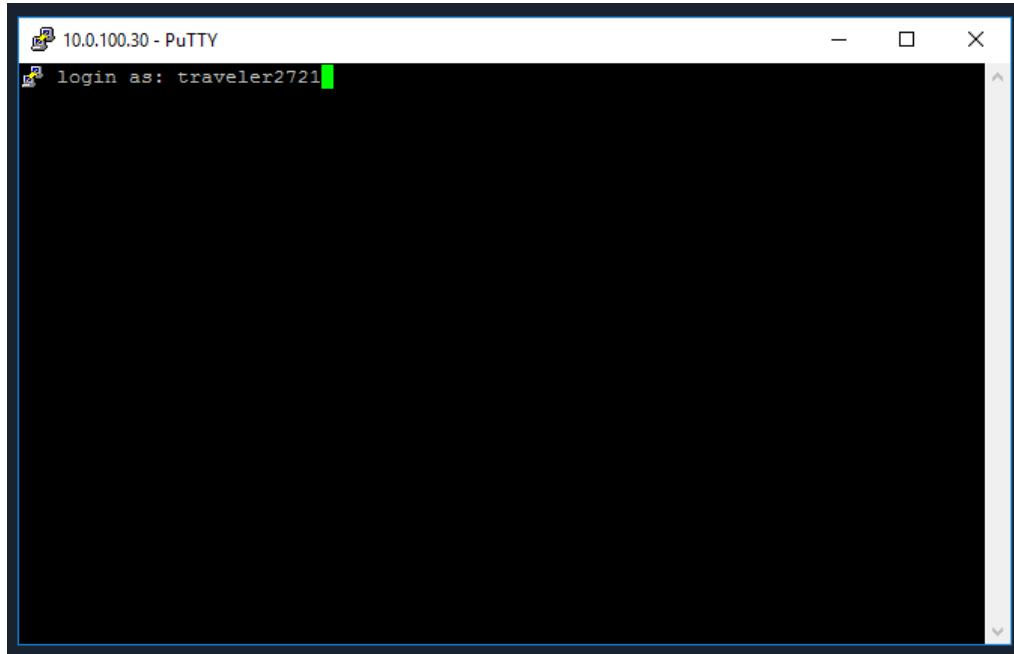
IP: 10.0.100.30



# Analyze a Related Suspicious File

## 5.1.2 Input Username

Username: traveler2721 (copy from above and right click on the mouse will paste in Linux) hit enter.



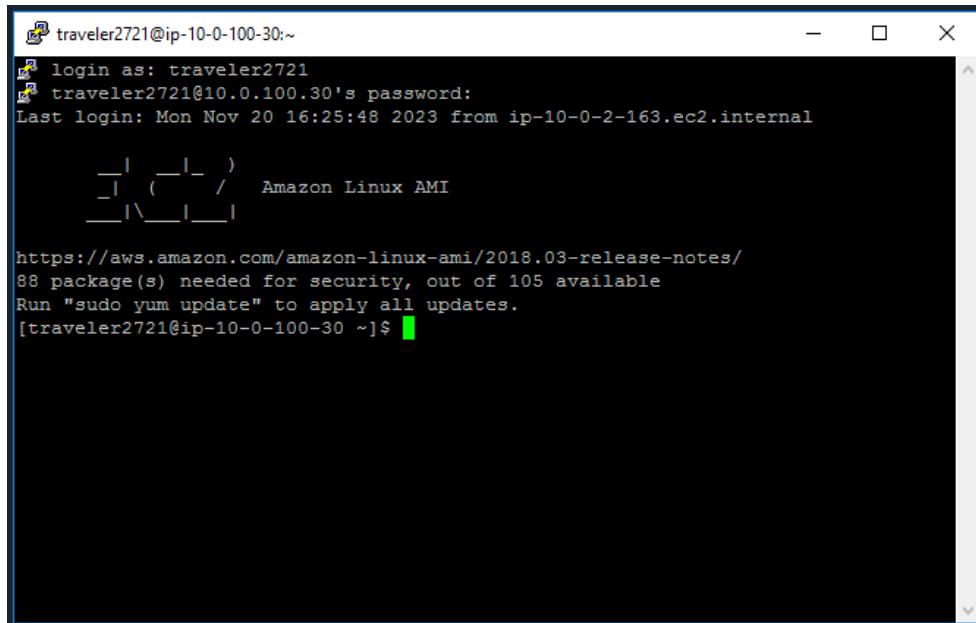
A screenshot of a PuTTY terminal window titled "10.0.100.30 - PuTTY". The window shows the command "login as: traveler2721" being typed into the text area. The text area has a dark background and light-colored text. The window has standard Windows-style window controls (minimize, maximize, close) at the top right.

## 5.1.3 Input Password

Input Password (copy from above and right click on the mouse will paste in Linux) hit enter.

*REMEMBER: PASSWORD IS ALWAYS INVISIBLE...YOU MIGHT NEED TO PUT IT IN TWICE TO MAKE THE CONNECTION.*

Password: EuD3jwtre4jGIEt07Tej

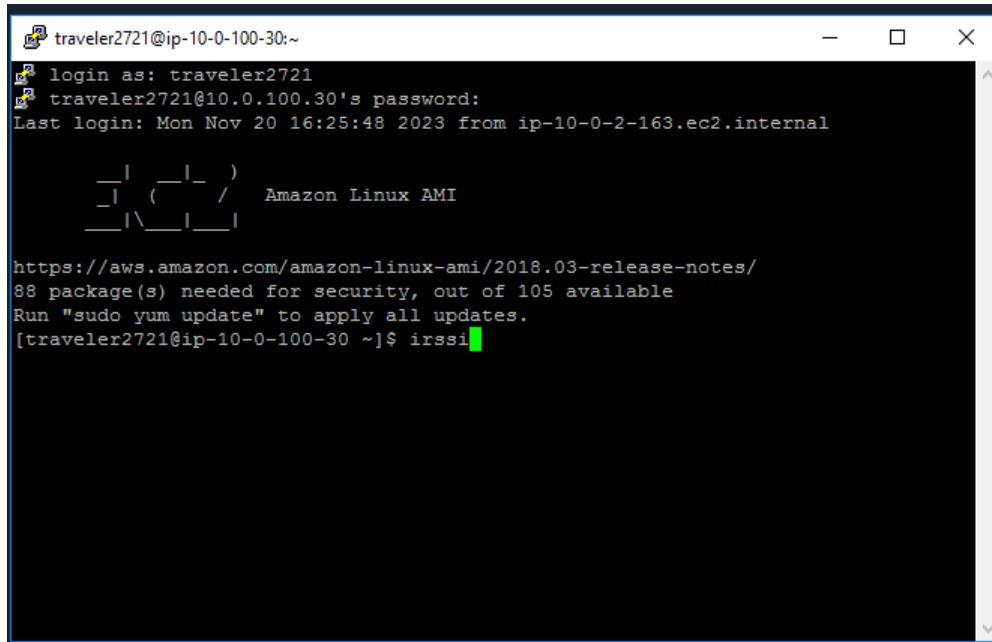


A screenshot of a PuTTY terminal window titled "traveler2721@ip-10-0-100-30:~". The window shows the password "EuD3jwtre4jGIEt07Tej" being typed. Below the password, the system displays a welcome message for Amazon Linux AMI and a link to the release notes. It also indicates that 88 packages are needed for security updates. The prompt "[traveler2721@ip-10-0-100-30 ~]\$" is visible at the bottom. The window has standard Windows-style window controls at the top right.

# Analyze a Related Suspicious File

## 5.2 Input irssi

Input irssi and hit enter



```
traveler2721@ip-10-0-100-30:~  
login as: traveler2721  
traveler2721@ip-10-0-100-30's password:  
Last login: Mon Nov 20 16:25:48 2023 from ip-10-0-2-163.ec2.internal  
_ _ | | _ / ) Amazon Linux AMI  
_ _ \|_|_ |  
https://aws.amazon.com/amazon-linux-ami/2018.03-release-notes/  
88 package(s) needed for security, out of 105 available  
Run "sudo yum update" to apply all updates.  
[traveler2721@ip-10-0-100-30 ~]$ irssi
```

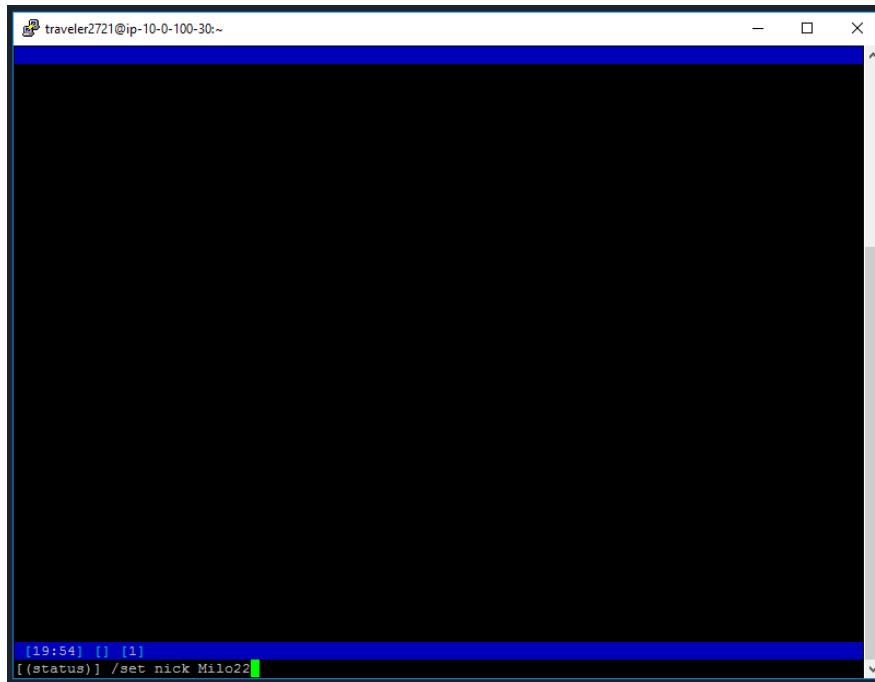


```
traveler2721@ip-10-0-100-30:~  
[19:13] [] [1]  
[(status)]
```

# Analyze a Related Suspicious File

## 5.2.1 Set Nickname

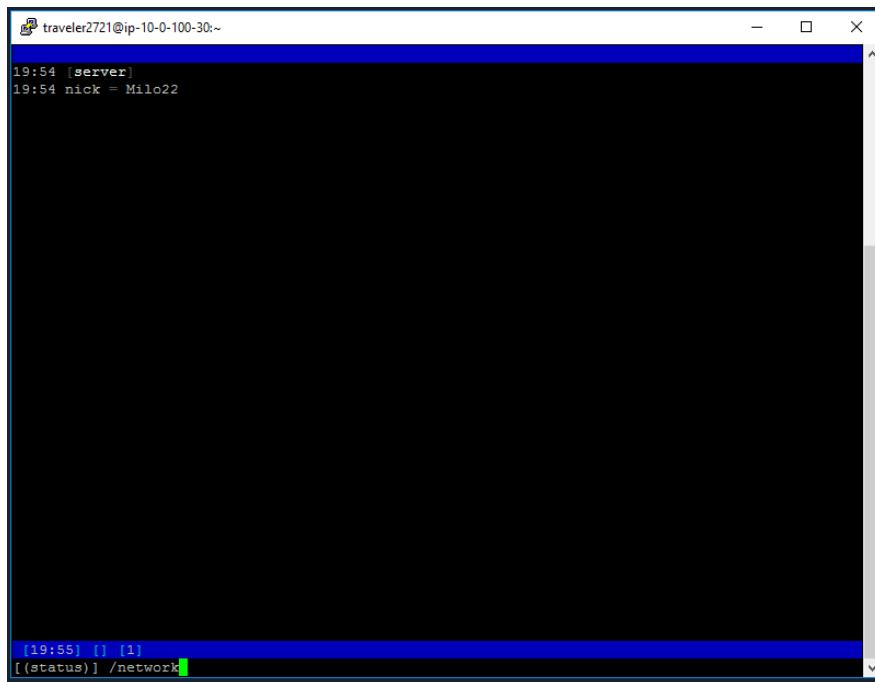
NOW ENTER: /set nick <nick name of choice>



A terminal window titled "traveler2721@ip-10-0-100-30:~". The window is mostly black with a blue header bar. In the bottom right corner of the header bar, there is a small white icon. The main area of the terminal is empty. At the bottom of the window, there is a blue status bar containing the text "[19:54] [] [1]" and "[status) ] /set nick Milo22". The cursor is positioned at the end of the command line.

## 5.2.2 Request Network List

/network and hit enter



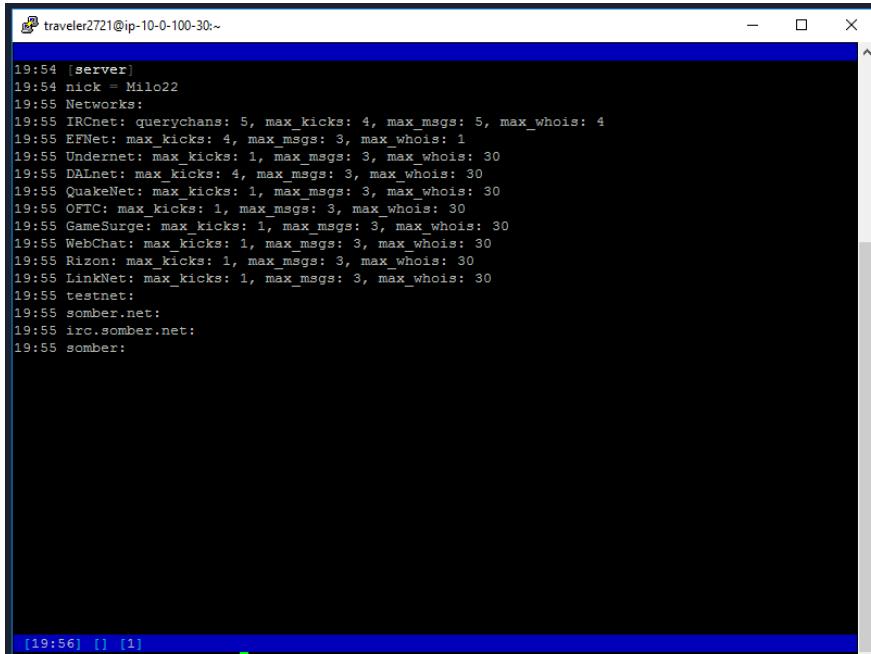
A terminal window titled "traveler2721@ip-10-0-100-30:~". The window is mostly black with a blue header bar. In the bottom right corner of the header bar, there is a small white icon. The main area of the terminal is empty. At the bottom of the window, there is a blue status bar containing the text "[19:54] [] [1]" and "[status) ] /network". The cursor is positioned at the end of the command line.

Connect to network as found in WinSCP (This week's IRC info: irc.somber.net #nymeria)

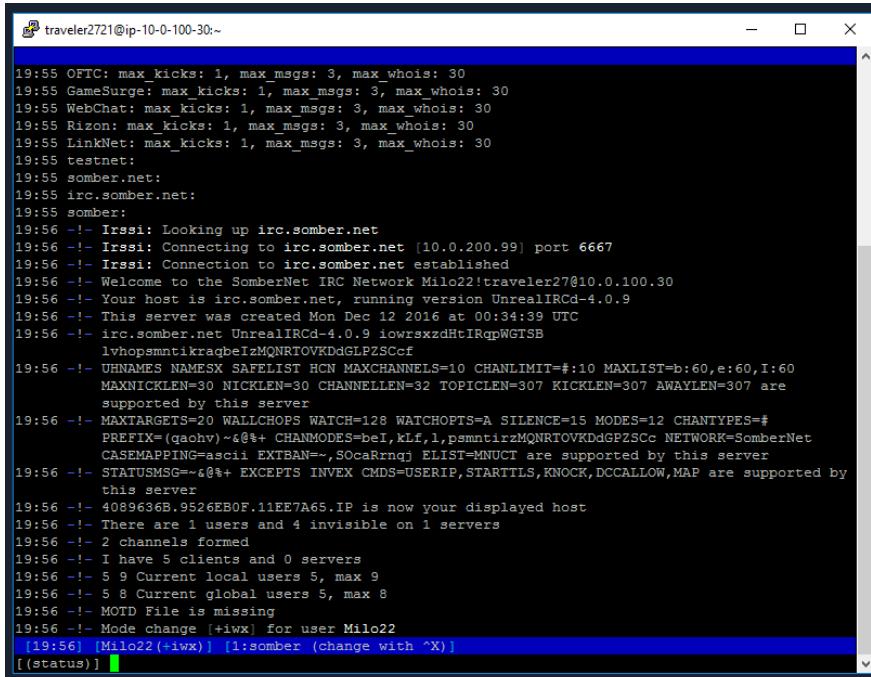
# Analyze a Related Suspicious File

## 5.2.3 Connect to network (sombert)

/connect somber and hit enter



```
traveler2721@ip-10-0-100-30:~  
19:54 [server]  
19:54 nick = Milo22  
19:55 Networks:  
19:55 IRNet: querychans: 5, max_kicks: 4, max_msgs: 5, max_whois: 4  
19:55 EFNet: max_kicks: 4, max_msgs: 3, max_whois: 1  
19:55 Undernet: max_kicks: 1, max_msgs: 3, max_whois: 30  
19:55 DALnet: max_kicks: 4, max_msgs: 3, max_whois: 30  
19:55 QuakeNet: max_kicks: 1, max_msgs: 3, max_whois: 30  
19:55 OFTC: max_kicks: 1, max_msgs: 3, max_whois: 30  
19:55 GameSurge: max_kicks: 1, max_msgs: 3, max_whois: 30  
19:55 WebChat: max_kicks: 1, max_msgs: 3, max_whois: 30  
19:55 Rizon: max_kicks: 1, max_msgs: 3, max_whois: 30  
19:55 LinkNet: max_kicks: 1, max_msgs: 3, max_whois: 30  
19:55 testnet:  
19:55 somber.net:  
19:55 irc.somber.net:  
19:55 somber:  
[19:56] [] [1]  
[(status)] /connect somber
```

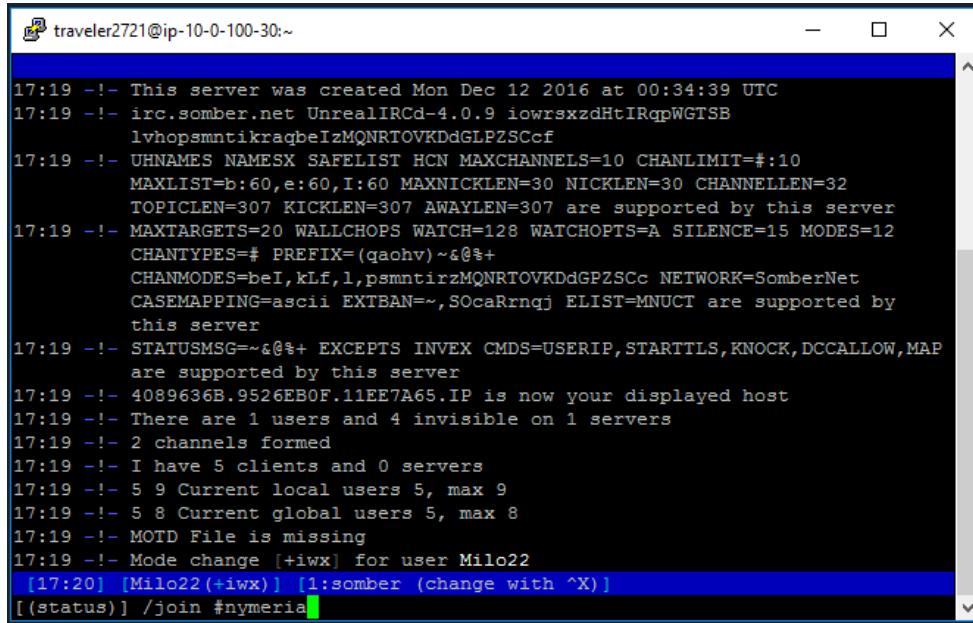
  


```
traveler2721@ip-10-0-100-30:~  
19:55 OFTC: max_kicks: 1, max_msgs: 3, max_whois: 30  
19:55 GameSurge: max_kicks: 1, max_msgs: 3, max_whois: 30  
19:55 WebChat: max_kicks: 1, max_msgs: 3, max_whois: 30  
19:55 Rizon: max_kicks: 1, max_msgs: 3, max_whois: 30  
19:55 LinkNet: max_kicks: 1, max_msgs: 3, max_whois: 30  
19:55 testnet:  
19:55 somber.net:  
19:55 somber:  
19:56 -- Irssi: Looking up irc.somber.net  
19:56 -- Irssi: Connecting to irc.somber.net [10.0.200.99] port 6667  
19:56 -- Irssi: Connection to irc.somber.net established  
19:56 -- Welcome to the SomberNet IRC Network Milo22!traveler27@10.0.100.30  
19:56 -- Your host is irc.somber.net, running version UnrealIRCd-4.0.9  
19:56 -- This server was created Mon Dec 12 2016 at 00:34:39 UTC  
19:56 -- irc.somber.net UnrealIRCd-4.0.9 iowrsxzdHtIRqpNGTSE  
lvhopsmttkraqbeIzMQRTOVKDdGLPZSCcf  
19:56 -- UHNAMES NAMESX SAFELIST HCN MAXCHANNELS=10 CHANLIMIT=#:10 MAXLIST=b:60,e:60,I:60  
MAXNICKLEN=30 NICKLEN=30 CHANNELLEN=32 TOPICLEN=307 KICKLEN=307 AWAYLEN=307 are  
supported by this server  
19:56 -- MAXTARGETS=20 WALLCHOPS WATCH=128 WATCHOPTS=A SILENCE=15 MODES=12 CHANTYPES=#  
PREFIX=(qachv)~&@+ CHANMODES=beI,kI!,l,psmntirzMQNRTOVKDdGPZSCc NETWORK=SomberNet  
CASEMAPPING=ascii EXTBAN=-,SocArnqj ELIST=MNUCT are supported by this server  
19:56 -- STATUSMSG=-&%++ EXCEPTS INVEX CMDS=USERIP,STARTTLS,KNOCK,DCCALLOW,MAP are supported by  
this server  
19:56 -- 4089636B.9526EB0F.11EE7A65.IP is now your displayed host  
19:56 -- There are 1 users and 4 invisible on 1 servers  
19:56 -- 2 channels formed  
19:56 -- I have 5 clients and 0 servers  
19:56 -- 5 9 Current local users 5, max 9  
19:56 -- 5 8 Current global users 5, max 8  
19:56 -- MOTD File is missing  
19:56 -- Mode change [+iwx] for user Milo22  
[19:56] [Milo22(+iwx)] [1:somber (change with ^X)]  
[(status)]
```

# Analyze a Related Suspicious File

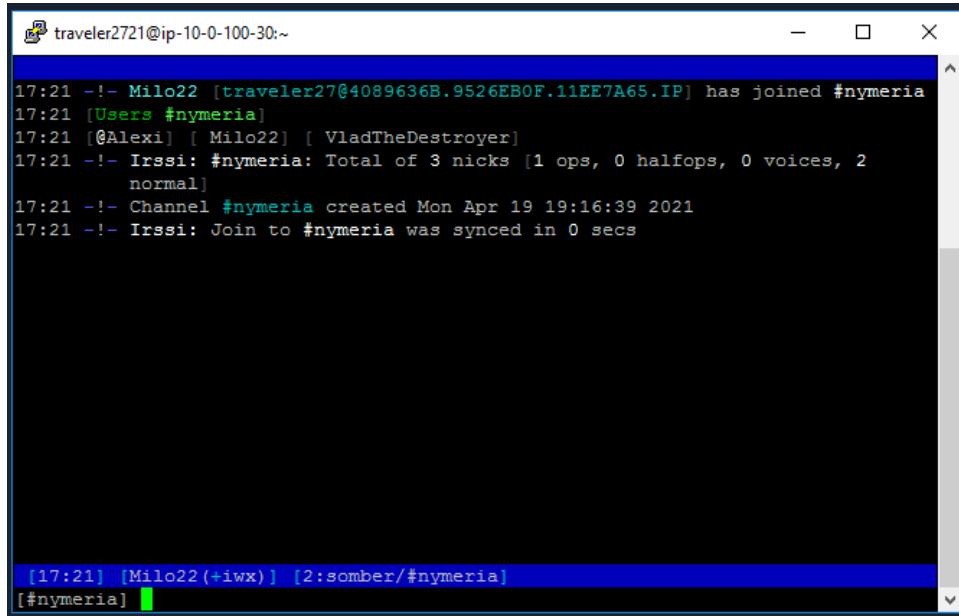
## 5.2.4 Join #nymeria

/join #nymeria and hit enter



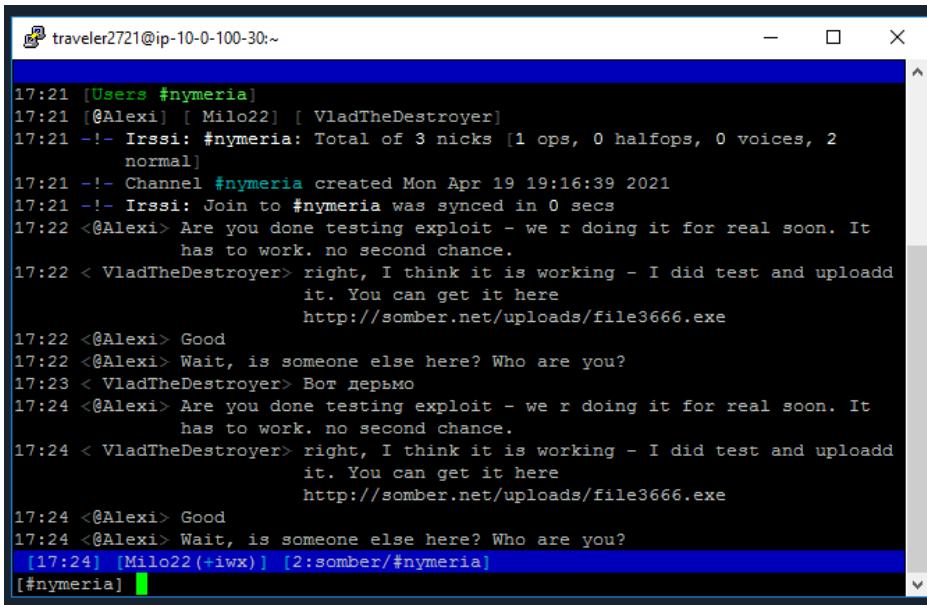
```
traveler2721@ip-10-0-100-30:~  
17:19 -!- This server was created Mon Dec 12 2016 at 00:34:39 UTC  
17:19 -!- irc.somber.net UnrealIRCd-4.0.9 iowrsxzdHtIRqpWGTB  
    lvhopsmtikraqbeIzMQRTOVKDdGLPZSCcf  
17:19 -!- UHNAME NAMESX SAFELIST HCN MAXCHANNELS=10 CHANLIMIT=#:10  
    MAXLIST=b:60,e:60,I:60 MAXNICKLEN=30 NICKLEN=30 CHANNELLEN=32  
    TOPICLEN=307 KICKLEN=307 AWAYLEN=307 are supported by this server  
17:19 -!- MAXTARGETS=20 WALLCHOPS WATCH=128 WATCHOPTS=A SILENCE=15 MODES=12  
    CHANTYPES=# PREFIX=(qaohv)~&%&+  
    CHANMODES=beI,kLf,l,psmmtirzMQNRTOVKDDGPZSCc NETWORK=SomberNet  
    CASEMAPPING=ascii EXTBAN=~,SOcaRrnqj ELIST=MNUCT are supported by  
    this server  
17:19 -!- STATUSMSG=~&%+ EXCEPTS INVEX CMDS=USERIP,STARTTLS,KNOCK,DCCALLOW,MAP  
    are supported by this server  
17:19 -!- 4089636B.9526EB0F.11EE7A65.IP is now your displayed host  
17:19 -!- There are 1 users and 4 invisible on 1 servers  
17:19 -!- 2 channels formed  
17:19 -!- I have 5 clients and 0 servers  
17:19 -!- 5 9 Current local users 5, max 9  
17:19 -!- 5 8 Current global users 5, max 8  
17:19 -!- MOTD File is missing  
17:19 -!- Mode change [+iwx] for user Milo22  
[17:20] [Milo22(+iwx)] [1:somber (change with ^X)]  
[(status)] /join #nymeria
```

## 5.3 Observe conversation



```
traveler2721@ip-10-0-100-30:~  
17:21 -!- Milo22 [traveler27@4089636B.9526EB0F.11EE7A65.IP] has joined #nymeria  
17:21 [Users #nymeria]  
17:21 [@Alexi] [ Milo22] [ VladTheDestroyer]  
17:21 -!- Irssi: #nymeria: Total of 3 nicks [1 ops, 0 halfops, 0 voices, 2  
    normal]  
17:21 -!- Channel #nymeria created Mon Apr 19 19:16:39 2021  
17:21 -!- Irssi: Join to #nymeria was synced in 0 secs  
  
[17:21] [Milo22(+iwx)] [2:somber/#nymeria]  
[#nymeria]
```

# Analyze a Related Suspicious File



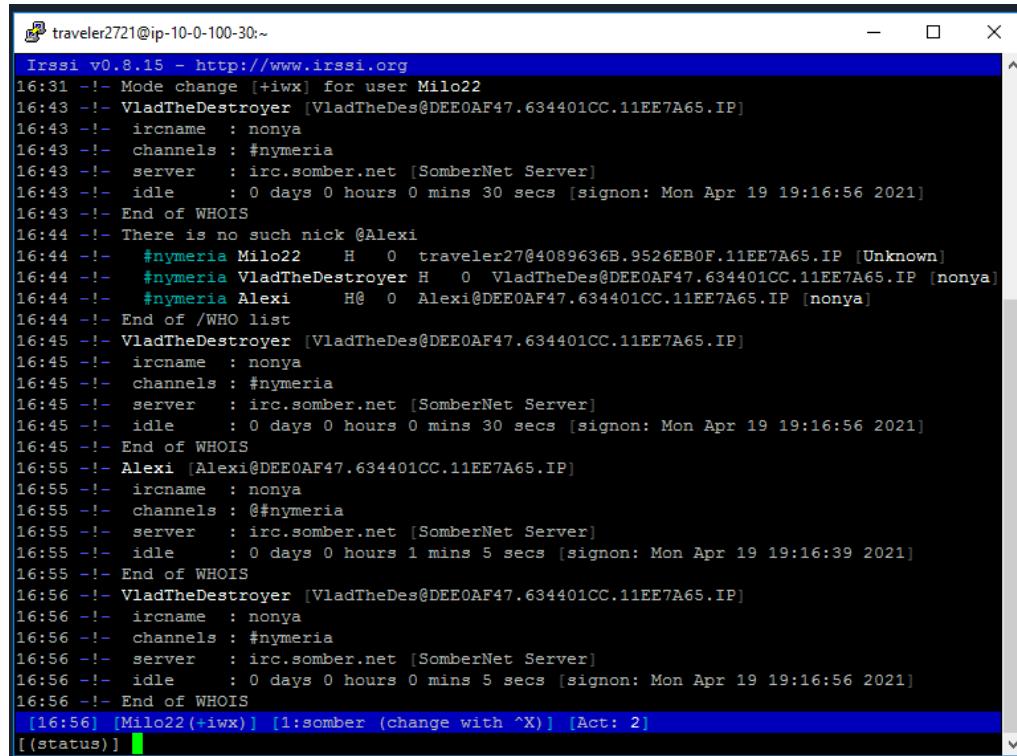
```
traveler2721@ip-10-0-100-30:~  
17:21 [Users #nymeria]  
17:21 [ @Alexi ] [ Milo22 ] [ VladTheDestroyer]  
17:21 -!- Irssi: #nymeria: Total of 3 nicks [1 ops, 0 halfops, 0 voices, 2  
normal]  
17:21 -!- Channel #nymeria created Mon Apr 19 19:16:39 2021  
17:21 -!- Irssi: Join to #nymeria was synced in 0 secs  
17:22 <@Alexi> Are you done testing exploit - we r doing it for real soon. It  
has to work. no second chance.  
17:22 < VladTheDestroyer> right, I think it is working - I did test and uploadad  
it. You can get it here  
http://somber.net/uploads/file3666.exe  
17:22 <@Alexi> Good  
17:22 <@Alexi> Wait, is someone else here? Who are you?  
17:23 < VladTheDestroyer> Bot лерьмо  
17:24 <@Alexi> Are you done testing exploit - we r doing it for real soon. It  
has to work. no second chance.  
17:24 < VladTheDestroyer> right, I think it is working - I did test and uploadad  
it. You can get it here  
http://somber.net/uploads/file3666.exe  
17:24 <@Alexi> Good  
17:24 <@Alexi> Wait, is someone else here? Who are you?  
[17:24] [Milo22(+iwx)] [2:somber/#nymeria]  
[#nymeria]
```

## 5.3.1 Identify Other Players

Other players noted are: VladTheDestroyer and Alexi

## 5.3.2 See Who the Players Are

/who and /whois



```
traveler2721@ip-10-0-100-30:~  
Irssi v0.8.15 - http://www.irssi.org  
16:31 --!- Mode change [+iwx] for user Milo22  
16:43 --!- VladTheDestroyer [VladTheDes@DEEOAF47.634401CC.11EE7A65.IP]  
16:43 --!- ircname : nonya  
16:43 --!- channels : #nymeria  
16:43 --!- server : irc.somber.net [SomberNet Server]  
16:43 --!- idle : 0 days 0 hours 0 mins 30 secs [signon: Mon Apr 19 19:16:56 2021]  
16:43 --!- End of WHOIS  
16:44 --!- There is no such nick @Alexi  
16:44 --!- #nymeria Milo22 H 0 traveler27@4089636B.9526EB0F.11EE7A65.IP [Unknown]  
16:44 --!- #nymeria VladTheDestroyer H 0 VladTheDes@DEEOAF47.634401CC.11EE7A65.IP [nonya]  
16:44 --!- #nymeria Alexi H@ 0 Alexi@DEEOAF47.634401CC.11EE7A65.IP [nonya]  
16:44 --!- End of /WHO list  
16:45 --!- VladTheDestroyer [VladTheDes@DEEOAF47.634401CC.11EE7A65.IP]  
16:45 --!- ircname : nonya  
16:45 --!- channels : #nymeria  
16:45 --!- server : irc.somber.net [SomberNet Server]  
16:45 --!- idle : 0 days 0 hours 0 mins 30 secs [signon: Mon Apr 19 19:16:56 2021]  
16:45 --!- End of WHOIS  
16:55 --!- Alexi [Alexi@DEEOAF47.634401CC.11EE7A65.IP]  
16:55 --!- ircname : nonya  
16:55 --!- channels : @#nymeria  
16:55 --!- server : irc.somber.net [SomberNet Server]  
16:55 --!- idle : 0 days 0 hours 1 mins 5 secs [signon: Mon Apr 19 19:16:39 2021]  
16:55 --!- End of WHOIS  
16:56 --!- VladTheDestroyer [VladTheDes@DEEOAF47.634401CC.11EE7A65.IP]  
16:56 --!- ircname : nonya  
16:56 --!- channels : #nymeria  
16:56 --!- server : irc.somber.net [SomberNet Server]  
16:56 --!- idle : 0 days 0 hours 0 mins 5 secs [signon: Mon Apr 19 19:16:56 2021]  
16:56 --!- End of WHOIS  
[16:56] [Milo22(+iwx)] [1:somber (change with ^X)] [Act: 2]  
[(status)]
```