

# Reverse Engineering and Exploitation

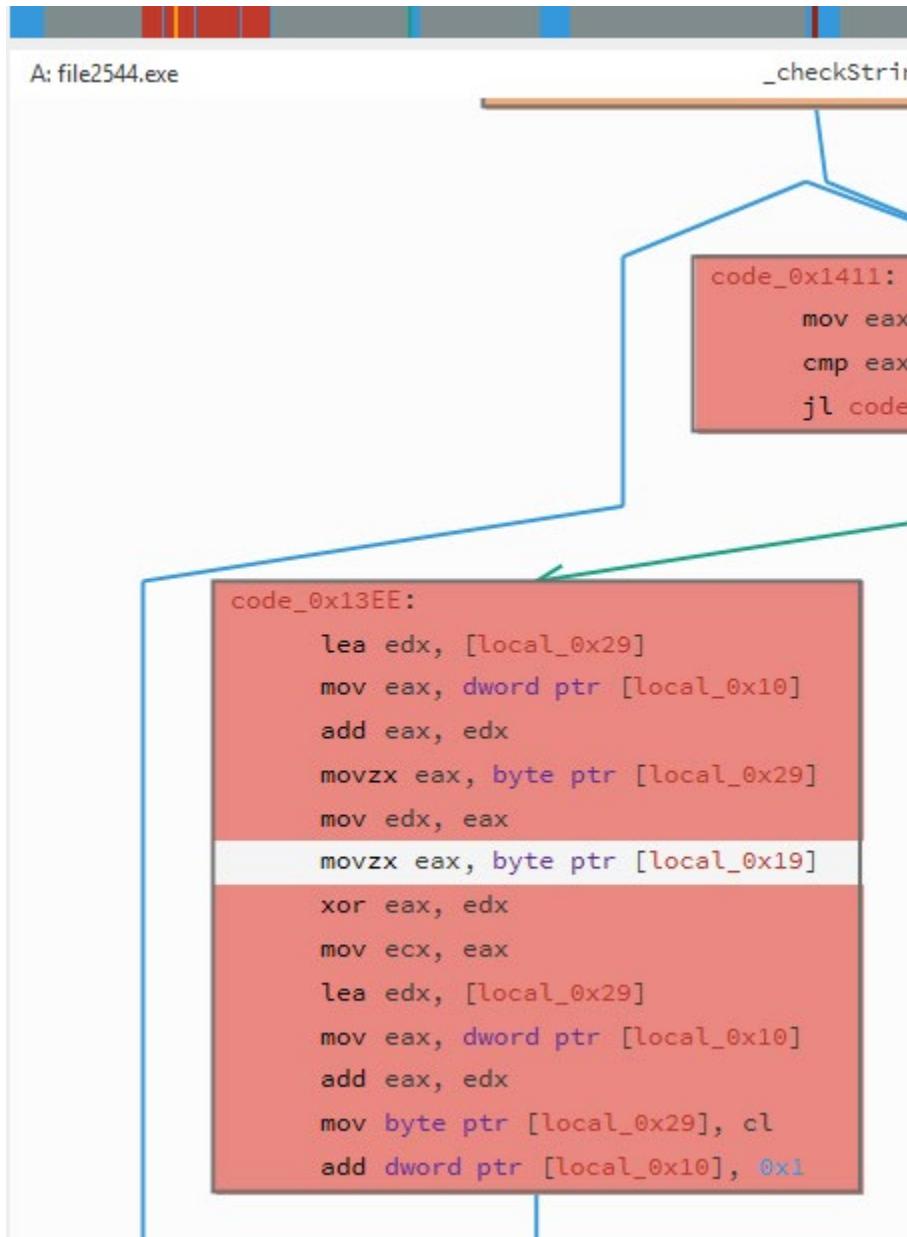
## Task 2 – Analyze a Related Suspicious File

In Relyze we see in code\_0x13EE:

```
xor eax, edx
```

and just above it

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



# Reverse Engineering and Exploitation

## Task 2 – 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
```

# Reverse Engineering and Exploitation

## Task 2 – Analyze a Related Suspicious File

### 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

# Reverse Engineering and Exploitation

## Task 2 – 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
```

# Reverse Engineering and Exploitation

## Task 2 – 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 (selected), To Base64, From Base64, To Hex, From Hex, To Hexdump, From Hexdump, URL Decode, Regular expression, Entropy, Fork, Magic.
- Recipe:** From Hex → XOR → To Hex.
- From Hex:** Delimiter 0x.
- XOR:** Key 41, HEX, Scheme Standard, Null preserving.
- Input:** 11203232362E33251235282020123439
- Output:** PasswordStillSux

# Reverse Engineering and Exploitation

## Task 2 – Analyze a Related Suspicious File

The screenshot shows the dCode XOR Cipher tool interface. At the top, there's a search bar for tools and a specific section for the XOR Cipher. The main area displays the results for an XOR cipher with the key '41'. It includes fields for the text to be XORed (Hexadecimal ASCII [00-7F] with automatic detection), the key size (1 byte), and the results format (ASCII (PRINTABLE) CHARACTERS). A large button labeled 'ENCRYPT / DECRYPT' is at the bottom. To the right, there's a sidebar with a 'Summary' section containing links to various XOR-related topics like XOR Decoder, XOR Calculator, and How to encrypt using XOR cipher. Below the summary is a 'Similar pages' section with links to ASCII Code and Binary Code.

**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 20 20 12 34 39

**ENCRYPTION/DECRYPTION 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

**ENCRYPT / DECRYPT**

**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

# Reverse Engineering and Exploitation

## Task 2 – Analyze a Related Suspicious File

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 |
| <input type="button" value="Open File"/> <input type="button" value=""/>  |      |
| Paste hex numbers or drop file  |      |
| 0x73696854<br>0x73736150<br>0x64726F77<br>0x21787553  |      |
| Character encoding  |      |
| ASCII   |      |
| <input type="button" value="Convert"/> <input type="button" value="Reset"/> <input type="button" value="Swap"/> |      |
| 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 |
| <input type="button" value="Open File"/> <input type="button" value=""/>  |      |
| Paste hex numbers or drop file  |      |
| 73696854<br>73736150<br>64726F77<br>21787553  |      |
| Character encoding  |      |
| ASCII   |      |
| <input type="button" value="Convert"/> <input type="button" value="Reset"/> <input type="button" value="Swap"/> |      |
| Text output ...   |      |

# Reverse Engineering and Exploitation

## Task 2 – Analyze a Related Suspicious File

Reverse the hexadecimal

Then rearrange to get proper order

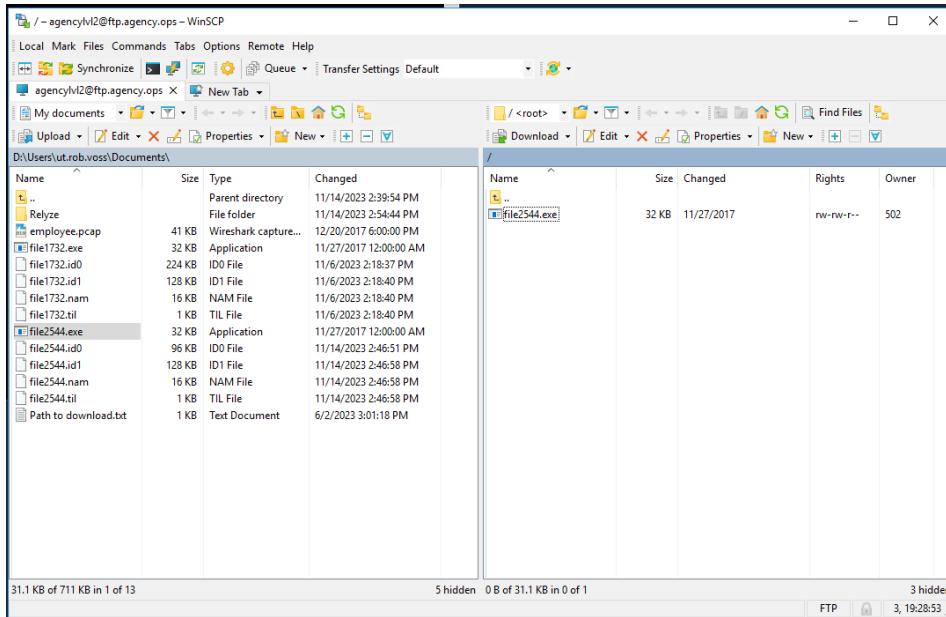
|   |   |
|---|---|
| <p><b>RapidTables</b></p> <p>Home &gt; Conversion &gt; Number conversion &gt; Hex code to ASCII text</p> <p><b>Hex to ASCII Text String Converter</b></p> <p>Enter hex bytes with any prefix / postfix / delimiter and press the <i>Convert</i> button<br/>(e.g. 45 78 61 6d 70 6C 65 21):</p> <p>From                  To<br/>Hexadecimal      Text<br/><input type="button" value="Open File"/> <input type="button" value=""/></p> <p>Paste hex numbers or drop file</p> <div style="border: 1px solid #ccc; padding: 5px; height: 100px; overflow-y: scroll;">21 78 75 53<br/>53 75 78 21<br/>77 6F 72 64<br/>50 61 73 73<br/>54 68 69 73</div> <p>Character encoding<br/>ASCII<br/><input type="button" value="Convert"/> <input type="button" value="Reset"/> <input type="button" value="Swap"/></p> <p>sihTssaPdrow!xuSSux!wordPassThis</p> | <p><b>RapidTables</b></p> <p>Home &gt; Conversion &gt; Number conversion &gt; Hex code to ASCII text</p> <p><b>Hex to ASCII Text String Converter</b></p> <p>Enter hex bytes with any prefix / postfix / delimiter and press the <i>Convert</i> button<br/>(e.g. 45 78 61 6d 70 6C 65 21):</p> <p>From                  To<br/>Hexadecimal      Text<br/><input type="button" value="Open File"/> <input type="button" value=""/></p> <p>Paste hex numbers or drop file</p> <div style="border: 1px solid #ccc; padding: 5px; height: 100px; overflow-y: scroll;">54 68 69 73<br/>54 68 69 73<br/>50 61 73 73<br/>77 6F 72 64<br/>53 75 78 21</div> <p>Character encoding<br/>ASCII<br/><input type="button" value="Convert"/> <input type="button" value="Reset"/> <input type="button" value="Swap"/></p> <p>sihTssaPdrow!xuSSux!wordPassThisThisPasswordSux!</p> |
|---|---|

# Reverse Engineering and Exploitation

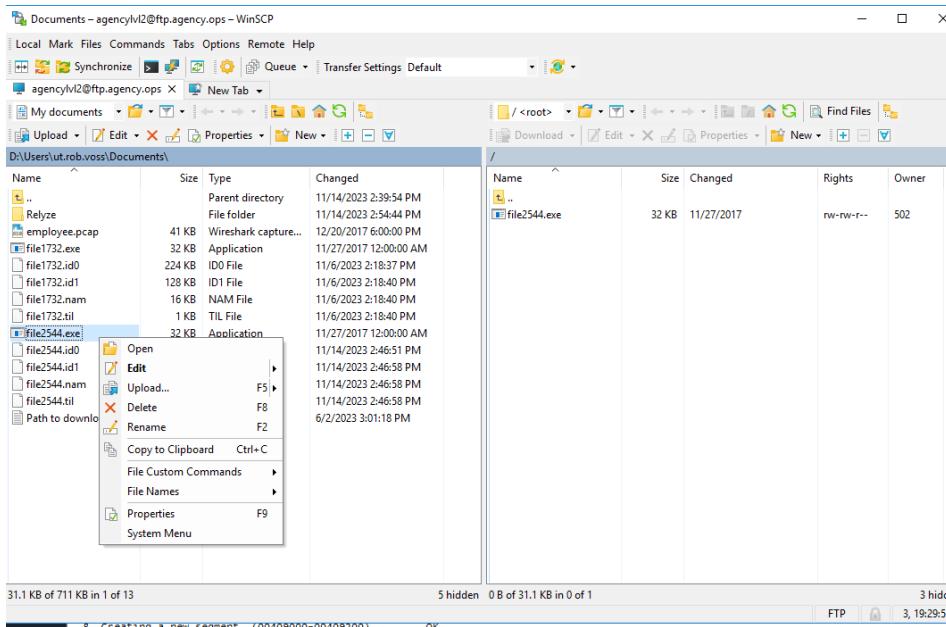
## Task 2 – Analyze a Related Suspicious File

### Run the Program

Open the Desktop and select the program



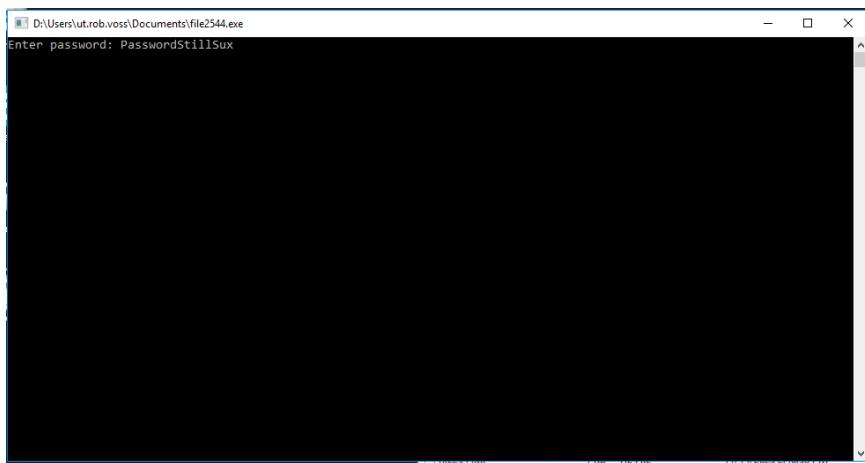
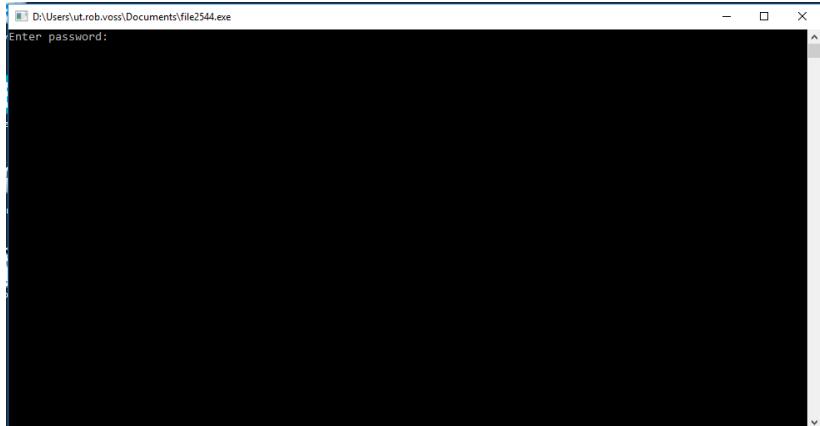
Open the program



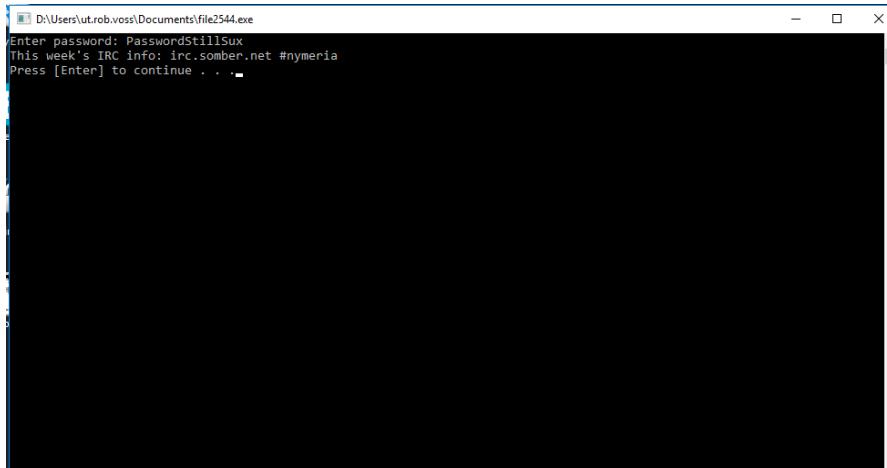
# Reverse Engineering and Exploitation

## Task 2 – Analyze a Related Suspicious File

Enter the password: PasswordStillSux



Hit enter:

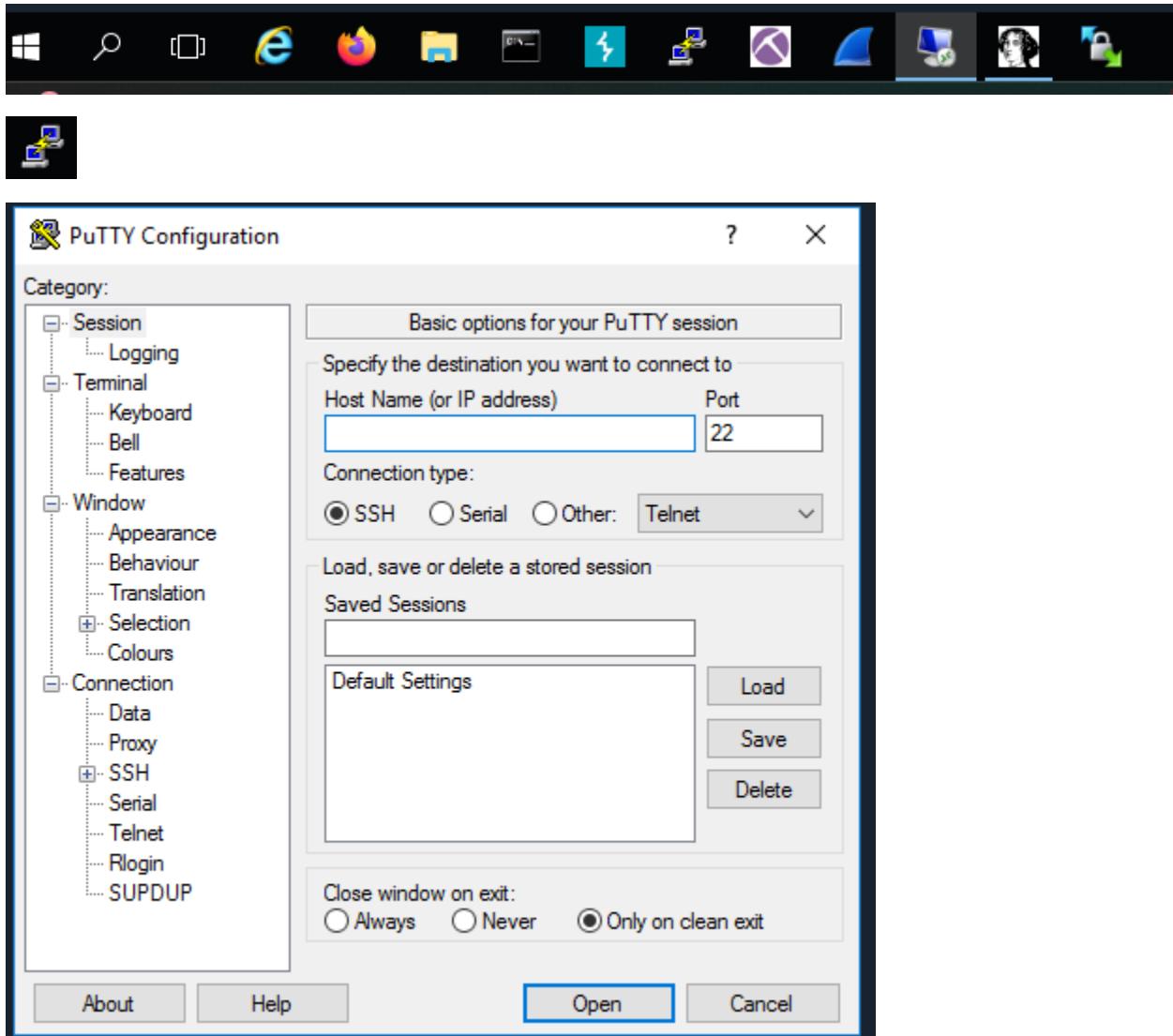


## Reverse Engineering and Exploitation

### Task 2 – Analyze a Related Suspicious File

## Connect to the IRC Channel

## Open PuTTY



IP: 10.0.100.30

Username: traveler2721

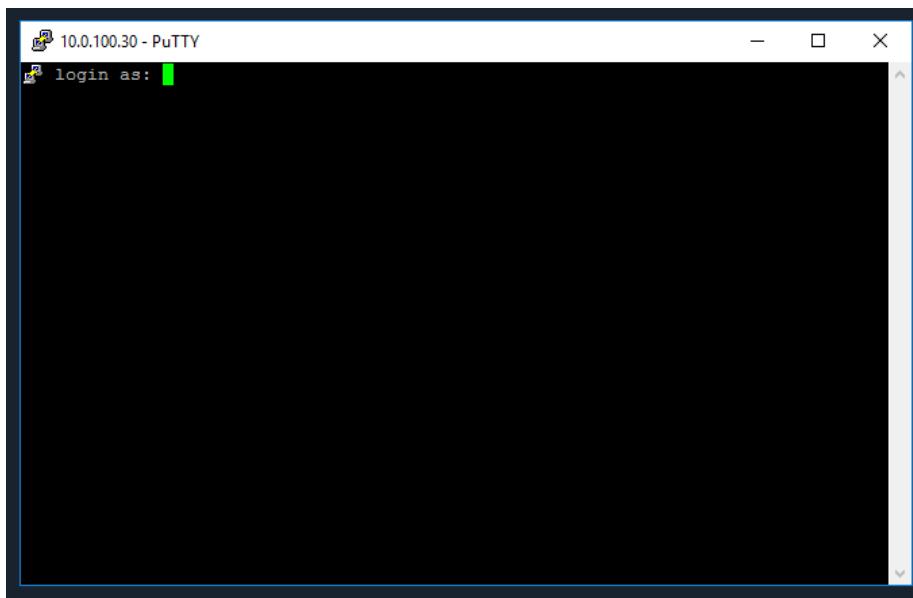
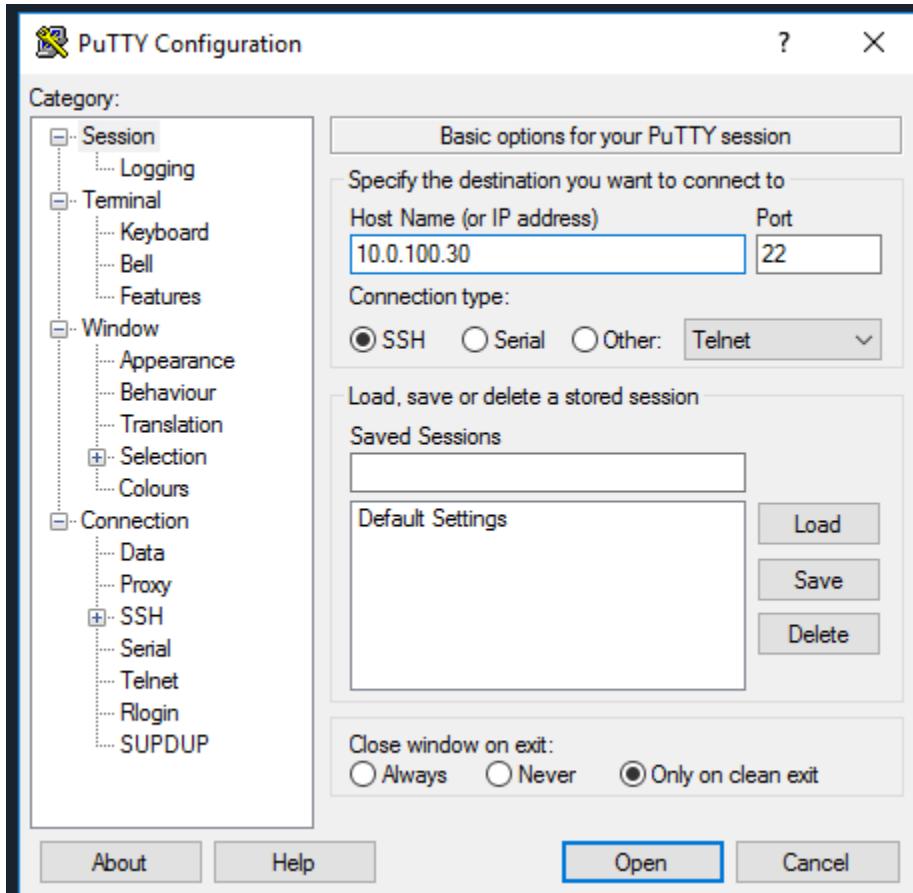
Password: EuD3jwtre4jGIEt07Tej

# Reverse Engineering and Exploitation

## Task 2 – Analyze a Related Suspicious File

Input Host name and click OPEN

IP: 10.0.100.30

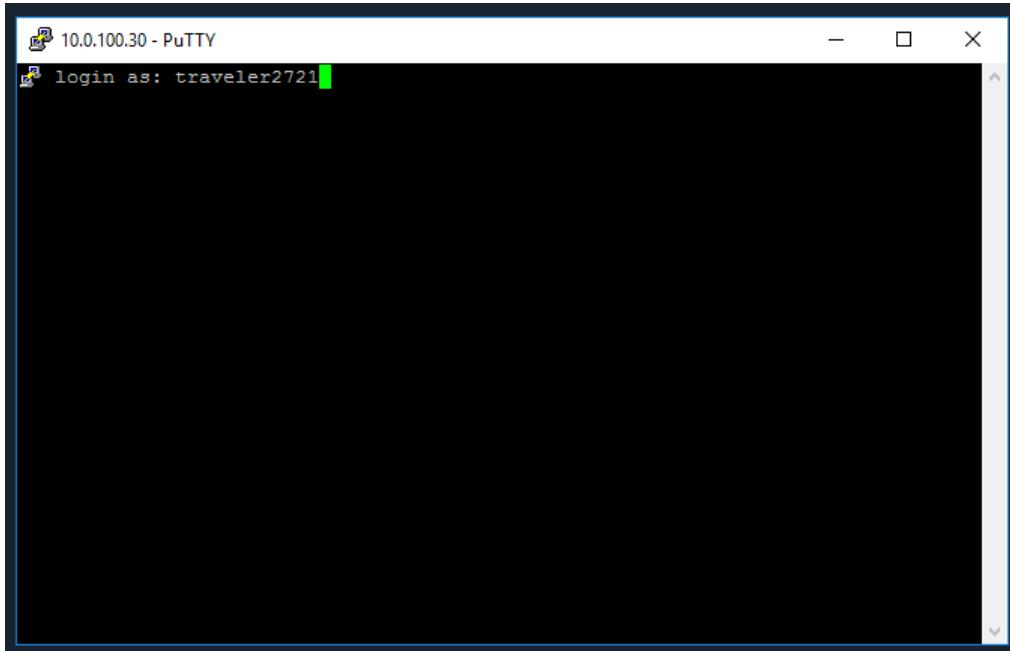


# Reverse Engineering and Exploitation

## Task 2 – Analyze a Related Suspicious File

Input Username (right click on the mouse will paste in Linux) and hit enter.

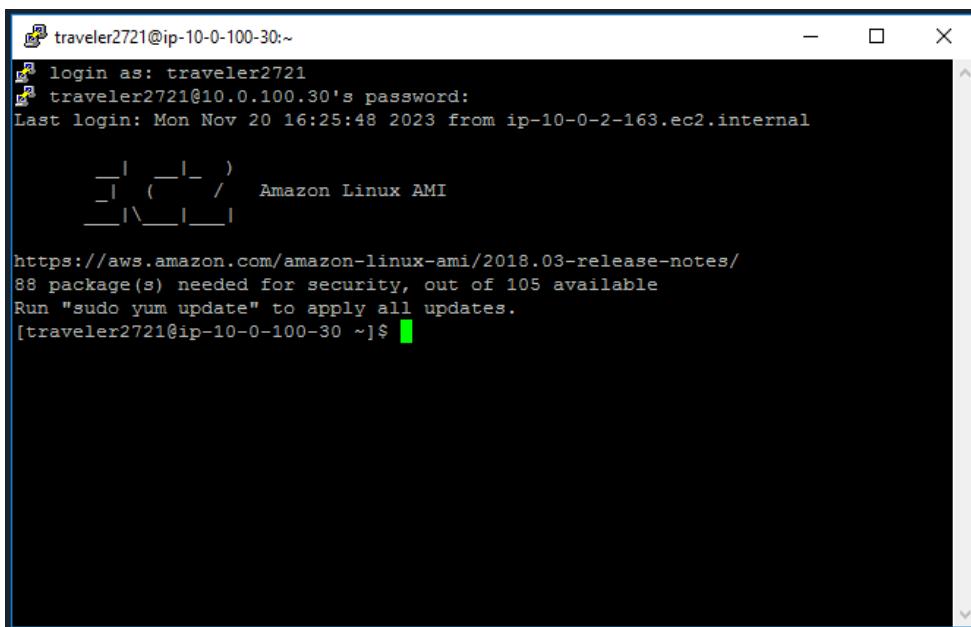
Username: **traveler2721**



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

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

Password: **EuD3jwtre4jGIEt07Tej**



## Reverse Engineering and Exploitation

### Task 2 – Analyze a Related Suspicious File

Input irssi and hit enter

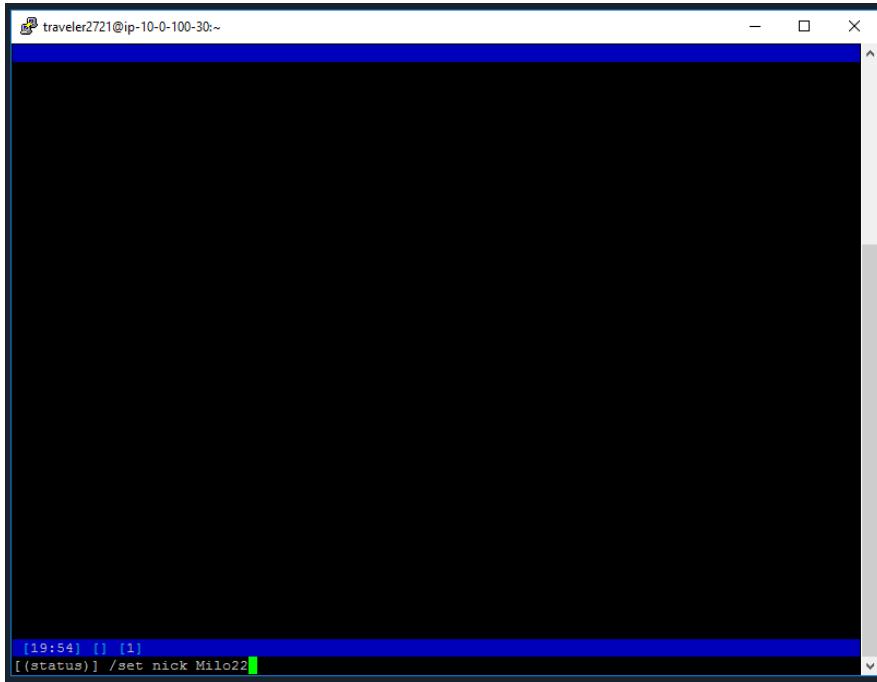
```
traveler2721@ip-10-0-100-30:~  
login as: traveler2721  
traveler2721@ip-10-0-100-30's password:  
Last login: Mon Nov 20 16:25:48 2023 from ip-10-0-2-163.ec2.internal  
  
_ _ | _ _ | )  
_ | ( _ /     Amazon Linux AMI  
_ | \_ | __ |  
  
https://aws.amazon.com/amazon-linux-ami/2018.03-release-notes/  
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
```

A screenshot of a terminal window titled "traveler2721@ip-10-0-100-30:~". The window is mostly blank black space. The title bar is blue. The bottom status bar is also blue and shows "[19:13] [ ] [1]" and "[status) ]" with a green progress bar.

# Reverse Engineering and Exploitation

## Task 2 – Analyze a Related Suspicious File

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

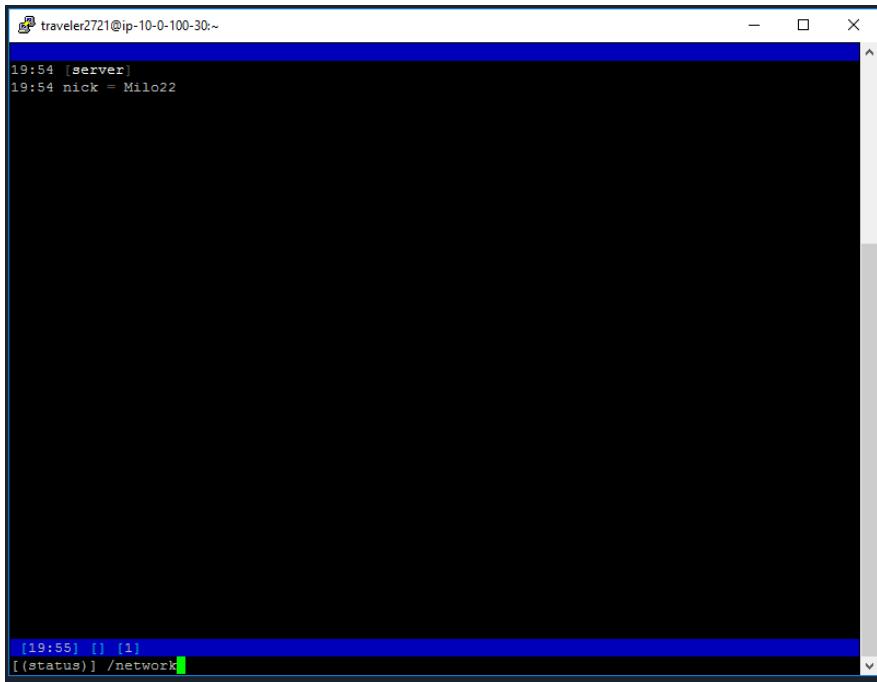


```
traveler2721@ip-10-0-100-30:~
```

```
[19:54] [] [1]
[status) ] /set nick Milo22
```

Request network list

/network and hit enter



```
traveler2721@ip-10-0-100-30:~
```

```
19:54 [server]
19:54 nick = Milo22
```

```
[19:55] [] [1]
[status) ] /network
```

# Reverse Engineering and Exploitation

## Task 2 – Analyze a Related Suspicious File

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

/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
```

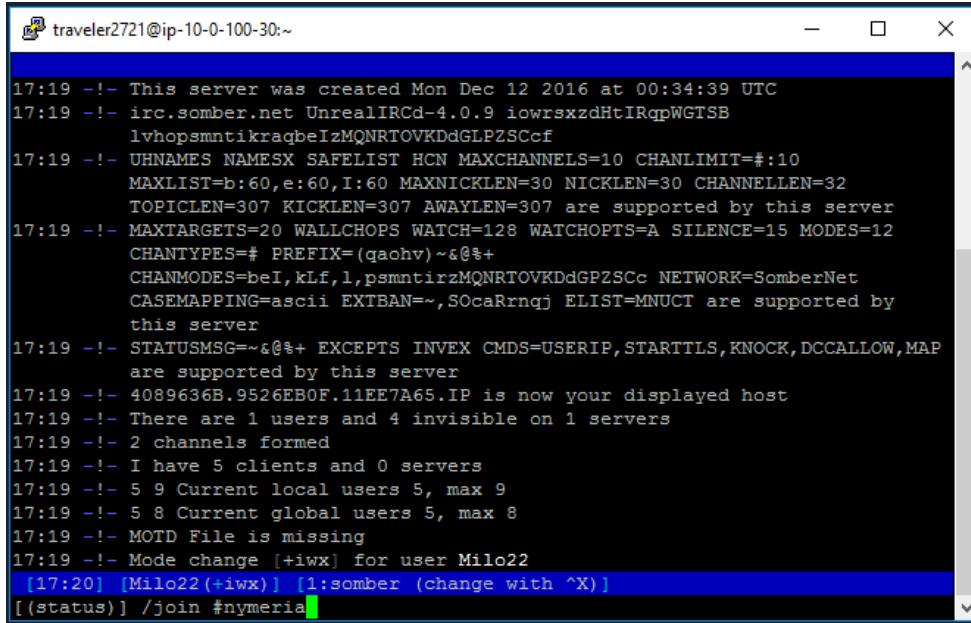
```
traveler2721@ip-10-0-100-30:~  
19:55 OFTC: max_kicks: 1, max_msgs: 3, max_whois: 30  
19:55 GameSurge: max_kicks: 1, max_msgs: 3, max_whois: 30  
19:55 WebChat: max_kicks: 1, max_msgs: 3, max_whois: 30  
19:55 Rizon: max_kicks: 1, max_msgs: 3, max_whois: 30  
19:55 LinkNet: max_kicks: 1, max_msgs: 3, max_whois: 30  
19:55 testnet:  
19:55 somber.net:  
19:55 irc.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 iowrsxzDhtIRqpWGTsB  
lyhopsmntikragbeIzMQRNTOVKDdGLPZSCcf  
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=(qaohv)~&@%+ CHANMODES=beI,klf,l,psmntirzMQNRTOVKDdGPZSCc NETWORK=SomberNet  
CASEMAPPING=ascii EXTBAN=~,SocaRrnqj ELIST=MNUCT are supported by this server  
19:56 -!- STATUSMSG=~&@%+ EXCEPTS INVEK 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)]
```

# Reverse Engineering and Exploitation

## Task 2 – Analyze a Related Suspicious File

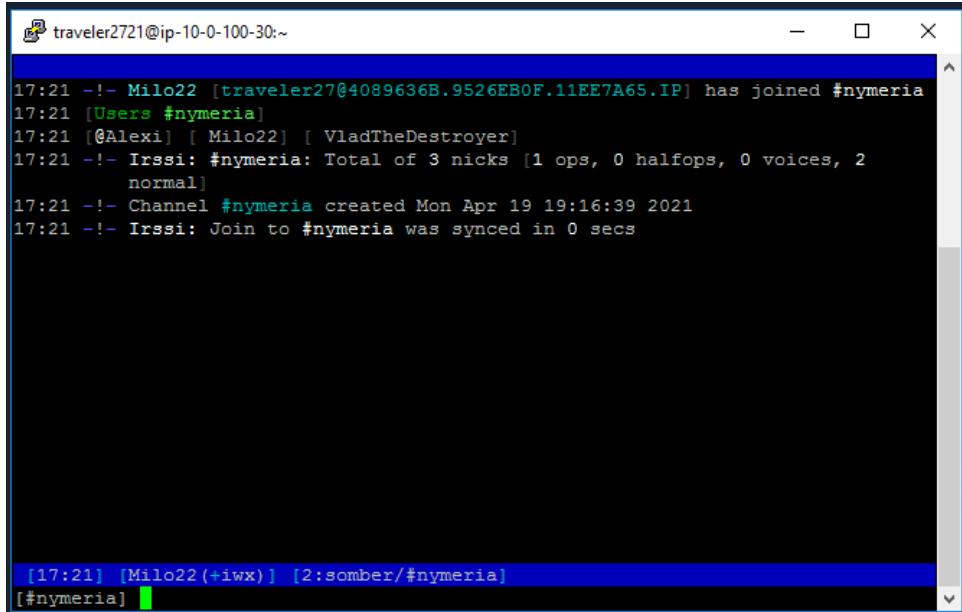
Join #nymeria

/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 iowrsxzdhIRqpWGTSB  
    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=(qachv) ~&@%+  
    CHANMODES=beI,kLf,l,psmntirzMQNRTOVKDDGPZSCc 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
```

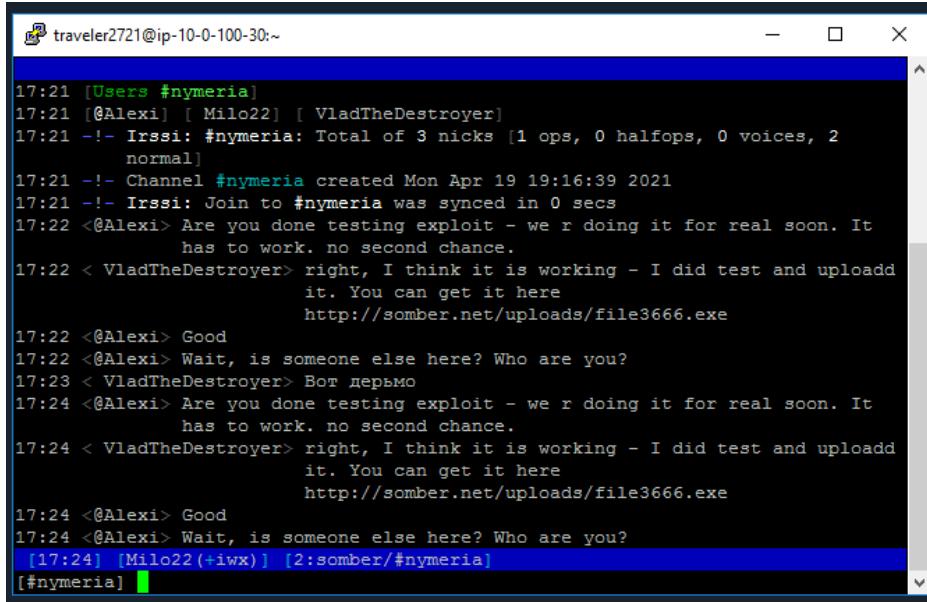
Observe conversation



```
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]
```

# Reverse Engineering and Exploitation

## Task 2 – Analyze a Related Suspicious File

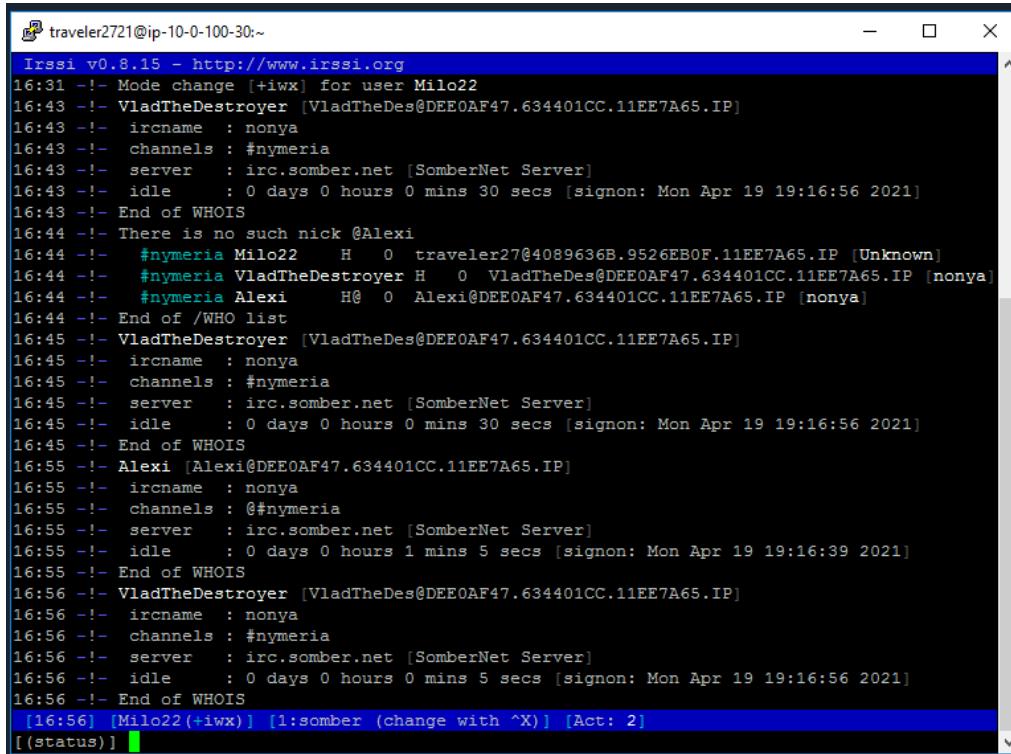


```
traveler2721@ip-10-0-100-30:~  
17:21 [Users #nymeria]  
17:21 [@Alexi] [ Milo22] [ VladTheDestroyer]  
17:21 !- Irssi: #nymeria: Total of 3 nicks [1 ops, 0 halfops, 0 voices, 2  
normal]  
17:21 !- Channel #nymeria created Mon Apr 19 19:16:39 2021  
17:21 !- Irssi: Join to #nymeria was synced in 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 uploadadd  
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> Вот дермо  
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 uploadadd  
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]
```

Other players noted are: VladTheDestroyer and Alexi

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@DEE0AF47.634401CC.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@DEE0AF47.634401CC.11EE7A65.IP [nonya]  
16:44 !- #nymeria Alexi H@ 0 Alexi@DEE0AF47.634401CC.11EE7A65.IP [nonya]  
16:44 !- End of /WHO list  
16:45 !- VladTheDestroyer [VladTheDes@DEE0AF47.634401CC.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@DEE0AF47.634401CC.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@DEE0AF47.634401CC.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)]
```