ATTACK DEFENSE

by PentesterAcademy

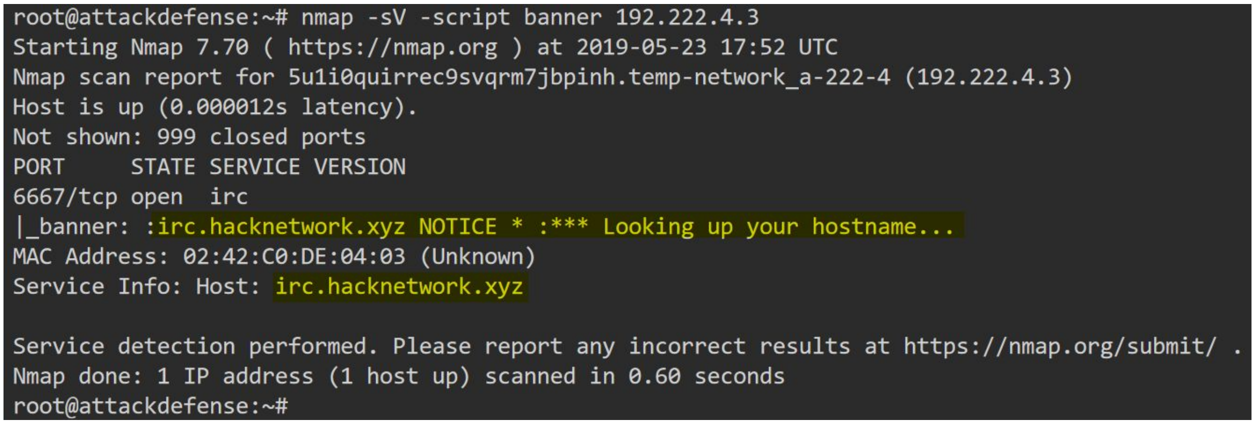
Name	Unrealircd Recon: Basics
URL	https://www.attackdefense.com/challengedetails?cid=514
Type	Network Recon : IRC Servers

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Q1. What is the host name of the IRC server running on the target machine? Also grab the banner.

Answer:
irc.hacknetwork.xyz
Banner: irc.hacknetwork.xyz NOTICE * :*** Looking up your hostname...

Command: nmap -sV -script banner 192.222.4.3



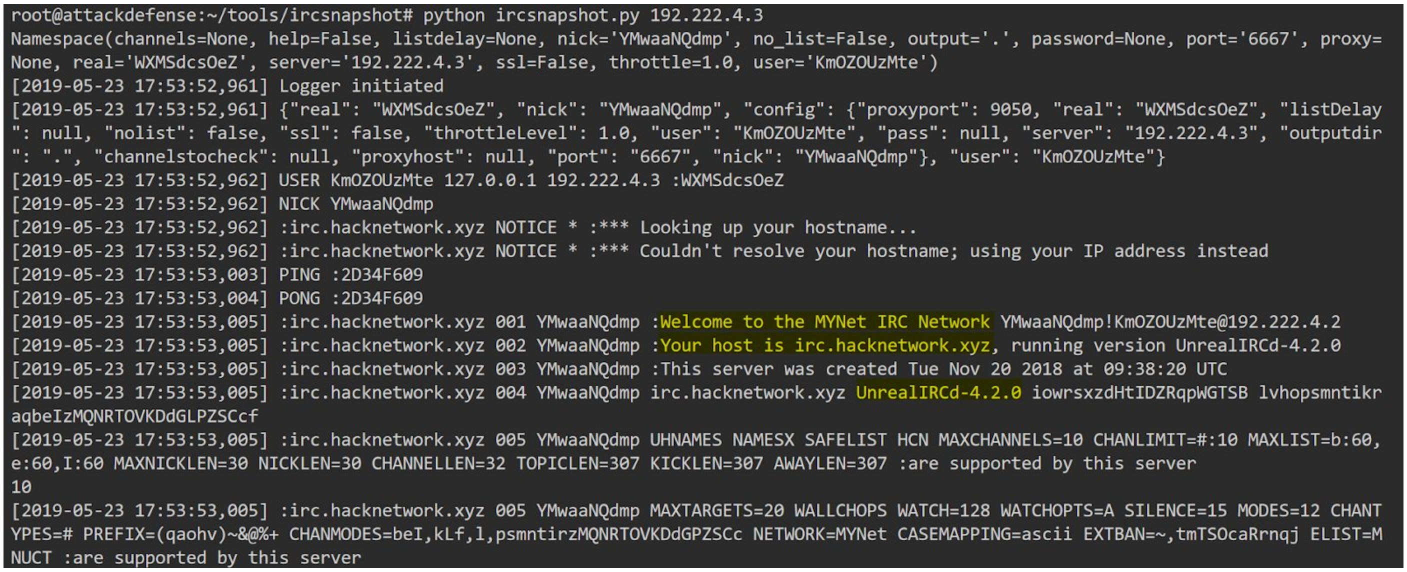
```
root@attackdefense:~# nmap -sV -script banner 192.222.4.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-23 17:52 UTC
Nmap scan report for 5u1i0quirrec9svqrm7jbpinh.temp-network_a-222-4 (192.222.4.3)
Host is up (0.000012s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE VERSION
6667/tcp open  irc
|_banner: :irc.hacknetwork.xyz NOTICE * :*** Looking up your hostname...
MAC Address: 02:42:C0:DE:04:03 (Unknown)
Service Info: Host: irc.hacknetwork.xyz

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.60 seconds
root@attackdefense:~#
```

Q2. Scan the target server with “ircsnapshot” tool and find out the server software name with version.

Answer: Unreal IRC 4.2.0

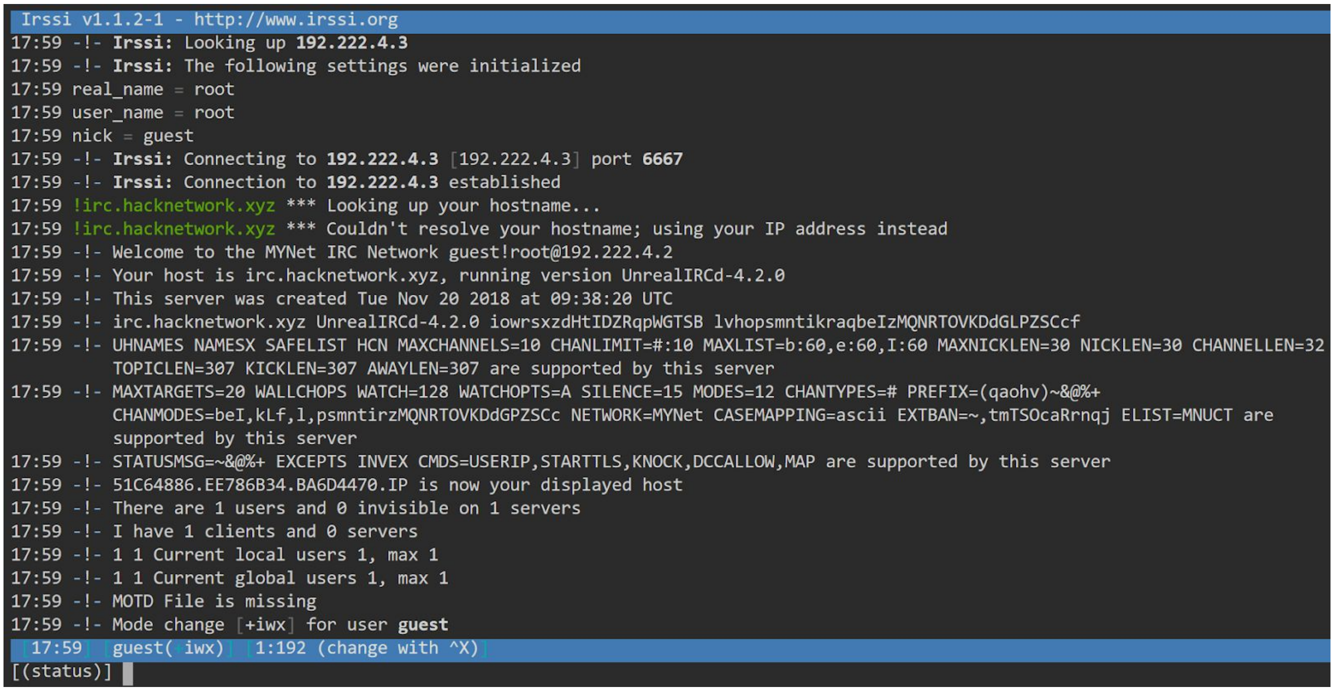
Commands:
cd tools/ircsnapshot
python ircsnapshot.py 192.222.4.3



```
root@attackdefense:~/tools/ircsnapshot# python ircsnapshot.py 192.222.4.3
Namespace(channels=None, help=False, listdelay=None, nick='YMwaaNQdmp', no_list=False, output='.', password=None, port='6667', proxy=
None, real='WXMSdcsOeZ', server='192.222.4.3', ssl=False, throttle=1.0, user='KmOZOUzMte')
[2019-05-23 17:53:52,961] Logger initiated
[2019-05-23 17:53:52,961] {"real": "WXMSdcsOeZ", "nick": "YMwaaNQdmp", "config": {"proxyport": 9050, "real": "WXMSdcsOeZ", "listDelay
": null, "nolist": false, "ssl": false, "throttleLevel": 1.0, "user": "KmOZOUzMte", "pass": null, "server": "192.222.4.3", "outputdir
": ".", "channelstocheck": null, "proxyhost": null, "port": "6667", "nick": "YMwaaNQdmp"}, "user": "KmOZOUzMte"}
[2019-05-23 17:53:52,962] USER KmOZOUzMte 127.0.0.1 192.222.4.3 :WXMSdcsOeZ
[2019-05-23 17:53:52,962] NICK YMwaaNQdmp
[2019-05-23 17:53:52,962] :irc.hacknetwork.xyz NOTICE * :*** Looking up your hostname...
[2019-05-23 17:53:52,962] :irc.hacknetwork.xyz NOTICE * :*** Couldn't resolve your hostname; using your IP address instead
[2019-05-23 17:53:53,003] PING :2D34F609
[2019-05-23 17:53:53,004] PONG :2D34F609
[2019-05-23 17:53:53,005] :irc.hacknetwork.xyz 001 YMwaaNQdmp :Welcome to the MYNet IRC Network YMwaaNQdmp!KmOZOUzMte@192.222.4.2
[2019-05-23 17:53:53,005] :irc.hacknetwork.xyz 002 YMwaaNQdmp :Your host is irc.hacknetwork.xyz, running version UnrealIRCd-4.2.0
[2019-05-23 17:53:53,005] :irc.hacknetwork.xyz 003 YMwaaNQdmp :This server was created Tue Nov 20 2018 at 09:38:20 UTC
[2019-05-23 17:53:53,005] :irc.hacknetwork.xyz 004 YMwaaNQdmp irc.hacknetwork.xyz UnrealIRCd-4.2.0 iowrsxzdHtIDZRqpWGTSB lvhopsmntikr
aqbeIzMQNRTOVKDdGLPZSCcf
[2019-05-23 17:53:53,005] :irc.hacknetwork.xyz 005 YMwaaNQdmp 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
10
[2019-05-23 17:53:53,005] :irc.hacknetwork.xyz 005 YMwaaNQdmp MAXTARGETS=20 WALLCHOPS WATCH=128 WATCHOPTS=A SILENCE=15 MODES=12 CHANT
YPES=# PREFIX=(qaohv)~&@%+ CHANMODES=beI,kLf,l,psmntirzMQNRTOVKDdGPZSCc NETWORK=MYNet CASEMAPPING=ascii EXTBAN=~,tmTSOcaRrnqj ELIST=M
NUCT :are supported by this server
```

Q3. Connect to IRC server using irssi client and answer the following questions:

Command: irssi -c 192.222.4.3 -n guest

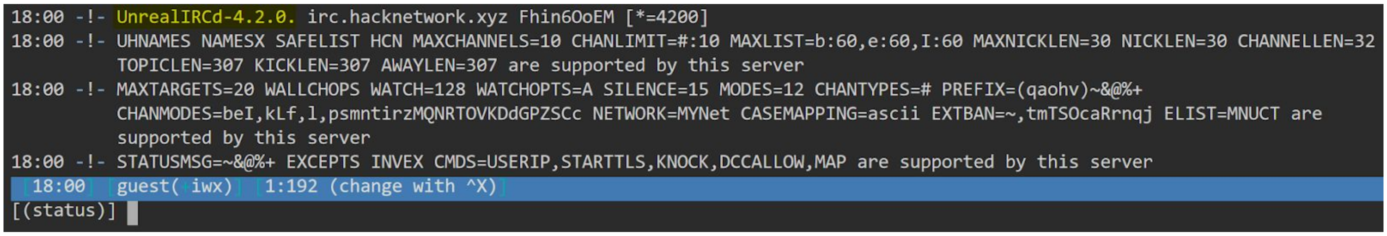


```
 Irssi v1.1.2-1 - http://www.irssi.org
17:59 -!- Irssi: Looking up 192.222.4.3
17:59 -!- Irssi: The following settings were initialized
17:59 real_name = root
17:59 user_name = root
17:59 nick = guest
17:59 -!- Irssi: Connecting to 192.222.4.3 [192.222.4.3] port 6667
17:59 -!- Irssi: Connection to 192.222.4.3 established
17:59 !irc.hacknetwork.xyz *** Looking up your hostname...
17:59 !irc.hacknetwork.xyz *** Couldn't resolve your hostname; using your IP address instead
17:59 -!- Welcome to the MYNet IRC Network guest!root@192.222.4.2
17:59 -!- Your host is irc.hacknetwork.xyz, running version UnrealIRCd-4.2.0
17:59 -!- This server was created Tue Nov 20 2018 at 09:38:20 UTC
17:59 -!- irc.hacknetwork.xyz UnrealIRCd-4.2.0 iowrsxzdHtIDZRqpWGTSB lvhopsmntikraqbeIzMQNRTOVKDdGLPZSCcf
17:59 -!- 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
17:59 -!- MAXTARGETS=20 WALLCHOPS WATCH=128 WATCHOPTS=A SILENCE=15 MODES=12 CHANTYPES=# PREFIX=(qaohv)~&@%+
          CHANMODES=beI,kLf,l,psmntirzMQNRTOVKDdGPZSCc NETWORK=MYNet CASEMAPPING=ascii EXTBAN=~,tmTSOcaRrnqj ELIST=MNUCT are
          supported by this server
17:59 -!- STATUSMSG=~&@%+ EXCEPTS INVEX CMDS=USERIP,STARTTLS,KNOCK,DCCALLOW,MAP are supported by this server
17:59 -!- 51C64886.EE786B34.BA6D4470.IP is now your displayed host
17:59 -!- There are 1 users and 0 invisible on 1 servers
17:59 -!- I have 1 clients and 0 servers
17:59 -!- 1 1 Current local users 1, max 1
17:59 -!- 1 1 Current global users 1, max 1
17:59 -!- MOTD File is missing
17:59 -!- Mode change [+iwx] for user guest
 [17:59] [guest(+iwx)] [1:192 (change with ^X)]
[(status)]
```

Q3.1 What is the version of the IRC server.

Answer: 4.2.0

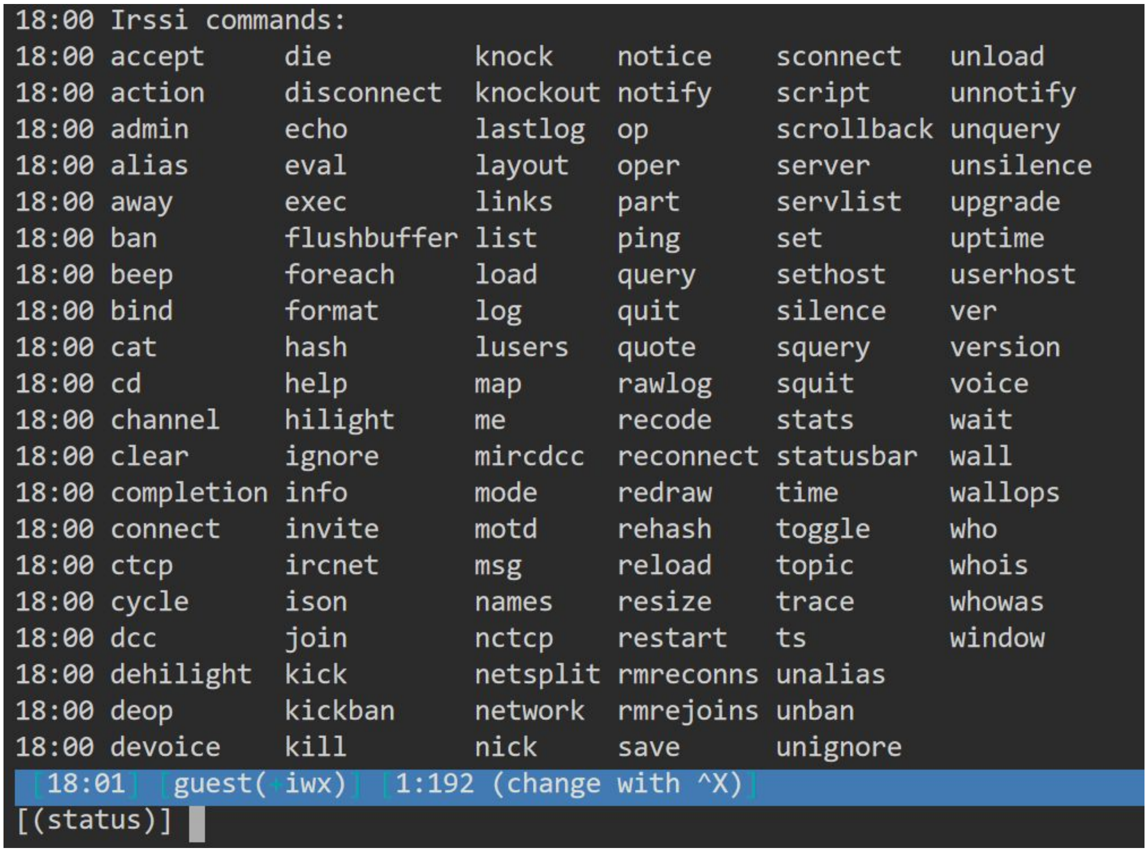
Command: /VERSION



```
18:00 -!- UnrealIRCd-4.2.0. irc.hacknetwork.xyz Fhin6OoEM [*=4200]
18:00 -!- 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
18:00 -!- MAXTARGETS=20 WALLCHOPS WATCH=128 WATCHOPTS=A SILENCE=15 MODES=12 CHANTYPES=# PREFIX=(qaohv)~&@%+
          CHANMODES=beI,kLf,l,psmntirzMQNRTOVKDdGPZSCc NETWORK=MYNet CASEMAPPING=ascii EXTBAN=~,tmTSOcaRrnqj ELIST=MNUCT are
          supported by this server
18:00 -!- STATUSMSG=~&@%+ EXCEPTS INVEX CMDS=USERIP,STARTTLS,KNOCK,DCCALLOW,MAP are supported by this server
 [18:00] [guest(+iwx)] [1:192 (change with ^X)]
[(status)]
```

Q3.2 What command can list all available/supported commands?

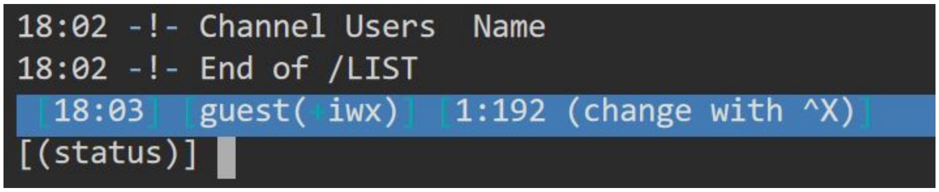
Command: /HELP



```
18:00 Irssi commands:
18:00 accept     die         knock    notice    sconnect   unload
18:00 action     disconnect  knockout notify    script     unnotify
18:00 admin      echo        lastlog  op        scrollback unquery
18:00 alias      eval        layout   oper      server     unsilence
18:00 away       exec        links    part      servlist   upgrade
18:00 ban        flushbuffer list     ping      set        uptime
18:00 beep       foreach     load     query     sethost    userhost
18:00 bind       format      log      quit      silence    ver
18:00 cat        hash        lusers   quote     squery     version
18:00 cd         help        map      rawlog    squit      voice
18:00 channel    hilight     me       recode    stats      wait
18:00 clear      ignore      mircdcc  reconnect statusbar  wall
18:00 completion info        mode     redraw    time       wallops
18:00 connect    invite      motd     rehash    toggle     who
18:00 ctcp       ircnet      msg      reload    topic      whois
18:00 cycle      ison        names    resize    trace      whowas
18:00 dcc        join        nctcp    restart   ts         window
18:00 dehilight  kick        netsplit rmreconns unalias
18:00 deop       kickban     network  rmrejoins unban
18:00 devoice    kill        nick     save      unignore
 [18:01] [guest(+iwx)] [1:192 (change with ^X)]
[(status)] 
```

Q4.3 What command can list channels?

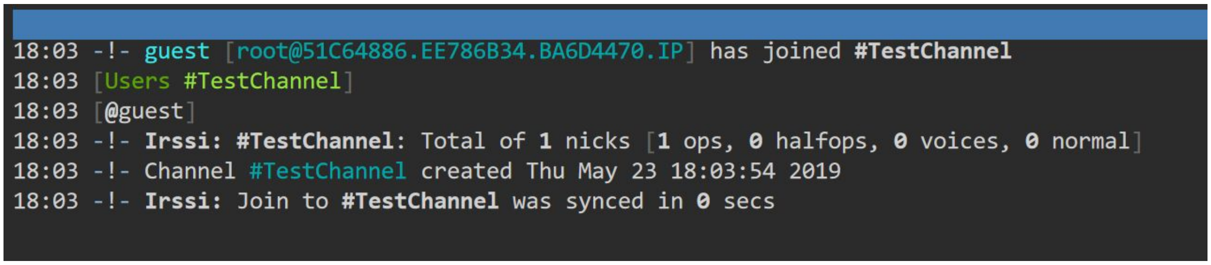
Command: /LIST -YES



```
18:02 -!- Channel Users  Name
18:02 -!- End of /LIST
 [18:03] [guest(+iwx)] [1:192 (change with ^X)]
[(status)] 
```

Q4.4 What command is used to switch/join a channel?

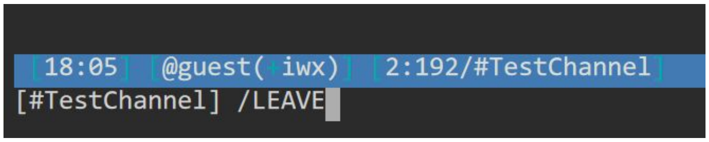
Command: /JOIN #channel_name



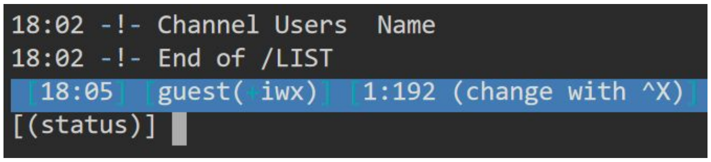
```
18:03 -!- guest [root@51C64886.EE786B34.BA6D4470.IP] has joined #TestChannel
18:03 [Users #TestChannel]
18:03 [@guest]
18:03 -!- Irssi: #TestChannel: Total of 1 nicks [1 ops, 0 halfops, 0 voices, 0 normal]
18:03 -!- Channel #TestChannel created Thu May 23 18:03:54 2019
18:03 -!- Irssi: Join to #TestChannel was synced in 0 secs
```

Q4.5 What command is used to leave a channel?

Command: /LEAVE or /PART



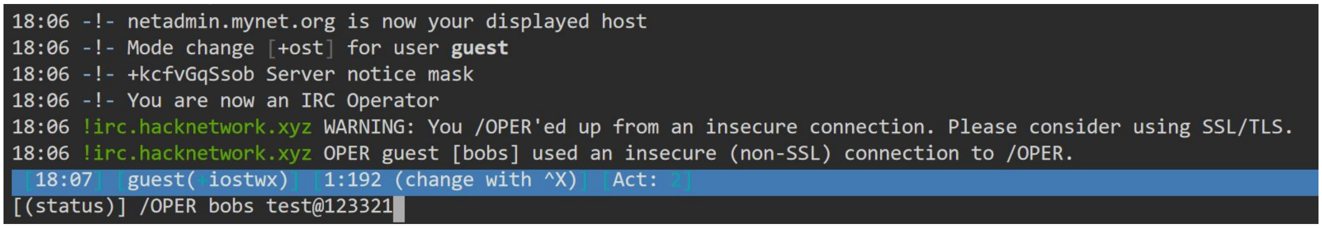
```
 [18:05] [@guest(+iwx)] [2:192/#TestChannel]
[#TestChannel] /LEAVE
```



```
18:02 -!- Channel Users  Name
18:02 -!- End of /LIST
 [18:05] [guest(+iwx)] [1:192 (change with ^X)]
[(status)]
```

Q.4.6 What command is used to switch to operator mode? Operator username is bobs and password is test@123321?

Command: /OPER bobs test@123321



```
18:06 -!- netadmin.mynet.org is now your displayed host
18:06 -!- Mode change [+ost] for user guest
18:06 -!- +kcfvGqSsob Server notice mask
18:06 -!- You are now an IRC Operator
18:06 !irc.hacknetwork.xyz WARNING: You /OPER'ed up from an insecure connection. Please consider using SSL/TLS.
18:06 !irc.hacknetwork.xyz OPER guest [bobs] used an insecure (non-SSL) connection to /OPER.
 [18:07] [guest(+iostwx)] [1:192 (change with ^X)] [Act: 2]
[(status)] /OPER bobs test@123321
```

References:

1. UnrealIRCd (https://www.unrealircd.org/)
2. Irssi (https://irssi.org/)
3. Ircsnapshot (https://github.com/bwall/ircsnapshot)