Client Configuration Guide

Windows v2.1

This document is designed to quickly get you up and running on Microsoft Windows with the free KiTTY SSH client.

TELESPLOIT

December 1, 2017

Client Configuration Guide

Windows v2.1

Contents

telesploit

exploitation at a distance

www.telesploit.com

Overview

The Telesploit solution consists of three distinct parts: the Telesploit server, the Telesploit relay, and an SSH capable client.

Telesploit Server

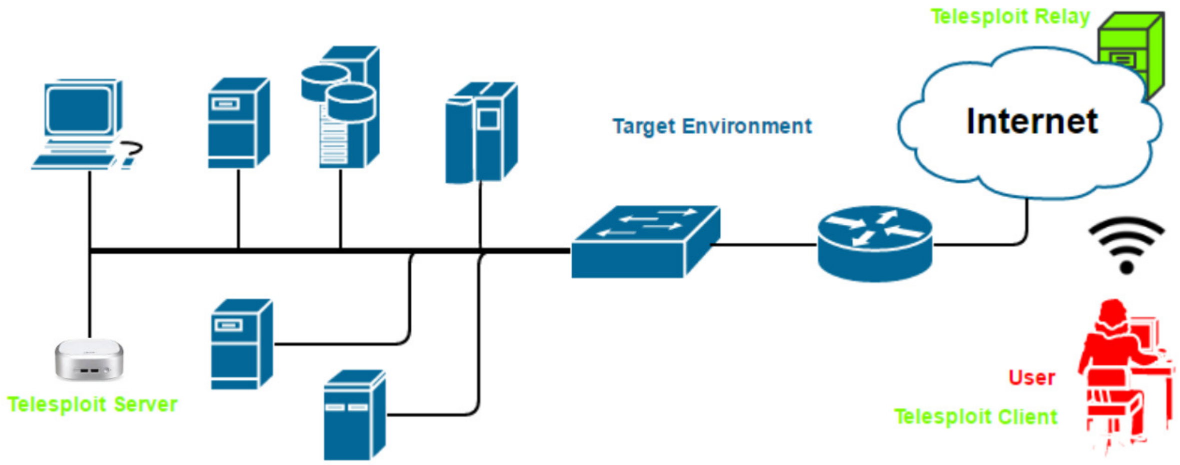
The server runs a customized version of Kali Linux and is deployed within the target environment. Once network connectivity and power have been applied to the device, it will automatically connect to the relay server and create TLS encapsulated reverse SSH tunnels in its default configuration. These connections provide access to a command line interface (SSH), remote desktop (VNC), web proxy (Squid), and many other applications on the Telesploit server.

Telesploit Relay

The relay runs in the cloud and provides secure access to the Telesploit server from Internet-connected clients using SSH key-based authentication. The relay includes pre-configured IRC and Mattermost servers for team-based communication and collaboration.

Client

The client connects to the Telesploit server via the relay. Penetration testing tools, such as Metasploit, can then be run directly from the server within the target environment or proxied through the established connections.



Client Setup

KiTTY Portable Download and Setup

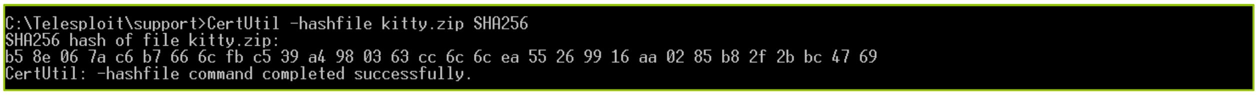
Download KiTTY Portable from http://www.9bis.net/kitty/. Place the program kitty_portable.exe in its own directory and run it. This will create several files and subdirectories. Close the application.

Telesploit will provide a URL to download the customized configuration files for connecting to your dedicated relay and server.

Example: https://relay-d015.telesploit.com/
b58e067ac6b7666cfbc539a4980363cc6c6cea55269916aa0285b82f2bbc4769/kitty.zip

The integrity may be validated by performing a sha256sum on the file. The value should match the subdirectory name in the URL.

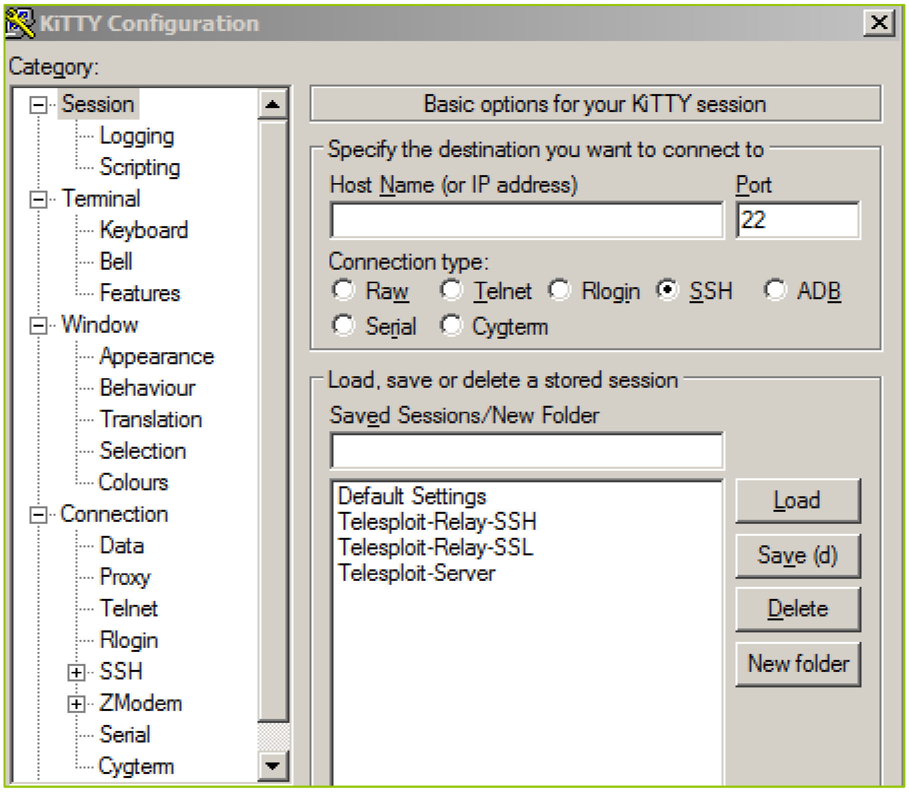
CertUtil -hashfile kitty.zip SHA256



```
C:\Telesploit\support>CertUtil -hashfile kitty.zip SHA256
SHA256 hash of file kitty.zip:
b5 8e 06 7a c6 b7 66 6c fb c5 39 a4 98 03 63 cc 6c 6c ea 55 26 99 16 aa 02 85 b8 2f 2b bc 47 69
CertUtil: -hashfile command completed successfully.
```

If the checksums match then place the archive, kitty.zip, in the same directory as kitty_portable.exe and unzip it. The file telesploit-readme.txt should appear in the directory and three new files will be added to the Sessions subdirectory.

Reopening the application should reveal three new entries, Telesploit-Relay-SSH, Telesploit-Relay-SSL, and Telesploit-Server.



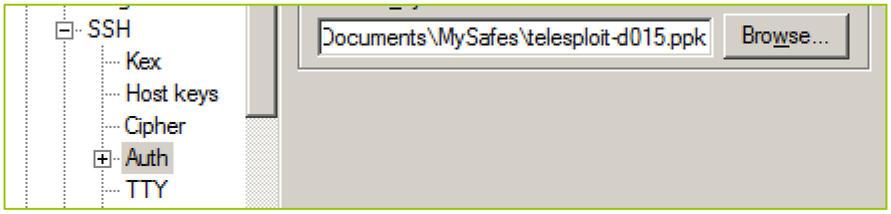
Host Name (or IP address):
Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ ADB ○ Serial ○ Cygterm

Saved Sessions/New Folder:

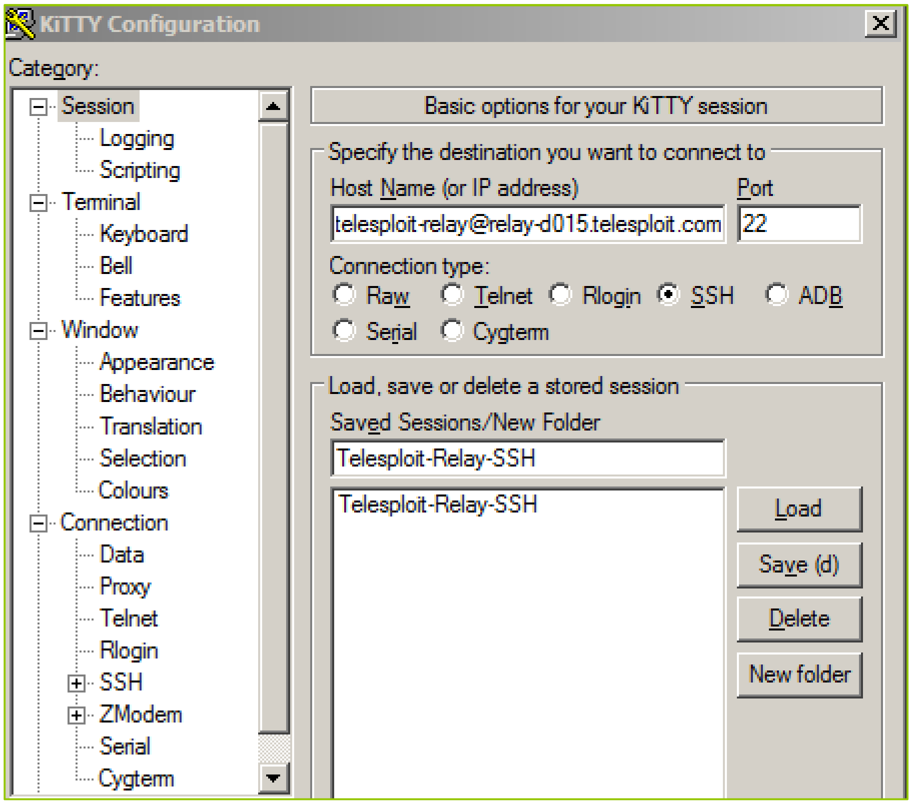
Default Settings
Telesploit-Relay-SSH
Telesploit-Relay-SSL
Telesploit-Server

Load each session and specify the private key that corresponds to the public key provided to Telesploit during the pre-deployment process.



Documents\MySafes\telesploit-d015.ppk

Return to the Session tab and select Save. Perform this action on all three sessions.



Host Name (or IP address): telesploit-relay@relay-d015.telesploit.com
Port: 22

Connection type:
○ Raw ○ Telnet ○ Rlogin ● SSH ○ ADB
○ Serial ○ Cygterm

Saved Sessions/New Folder: Telesploit-Relay-SSH

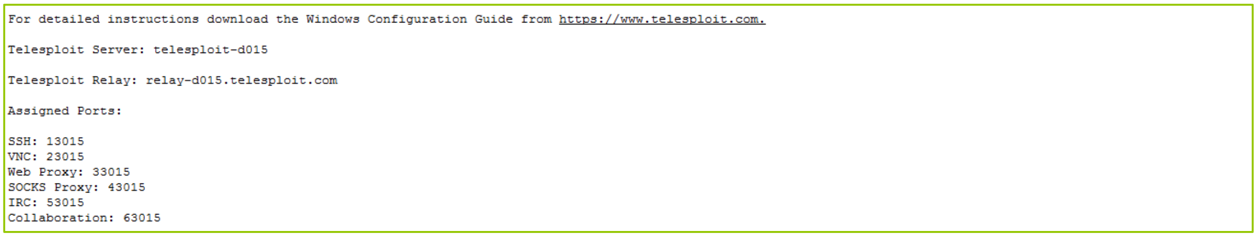
Telesploit-Relay-SSH

Telesploit-Relay-SSH: This configuration uses a direct SSH connection to the relay server to establish tunnels for accessing SSH, VNC, and Squid and SOCKS proxies running on the server. It also creates tunnels to access the IRC and Mattermost instances running on the relay.

Telesploit-Relay-SSL: This configuration creates an SSL/TLS connection to the relay server in order to establish tunnels for accessing SSH, VNC, and Squid and SOCKS proxies running on the server. It also creates tunnels to access the IRC and Mattermost instances running on the relay. Use this configuration when outbound SSH is restricted from your environment. It requires that ncat, part of the nmap suite, be installed on the local client.

Telesploit-Server: Once tunnels have been established to the relay this configuration may be used to establish console access on the server.

The readme.txt file contains the server, relay, and port assignments for your Telesploit deployment. These should be used to replace the examples given in the subsequent sections.

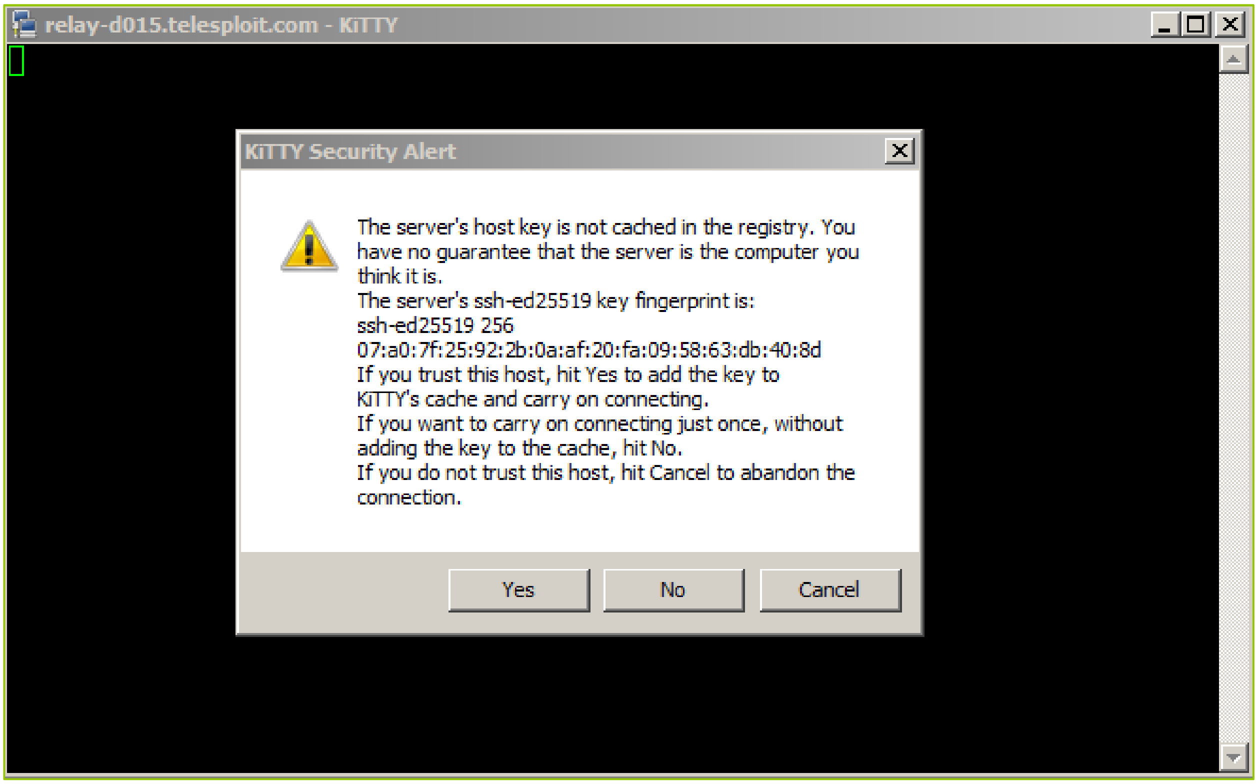


```
For detailed instructions download the Windows Configuration Guide from https://www.telesploit.com.

Telesploit Server: telesploit-d015

Telesploit Relay: relay-d015.telesploit.com

Assigned Ports:

SSH: 13015
VNC: 23015
Web Proxy: 33015
SOCKS Proxy: 43015
IRC: 53015
Collaboration: 63015
```

Establish SSH Tunnels and Connect to the Server

Once the KiTTY client has been configured for your environment, verify that you can create SSH tunnels to the relay by opening either Telesploit-Relay-SSH or Telesploit-Relay-SSL.

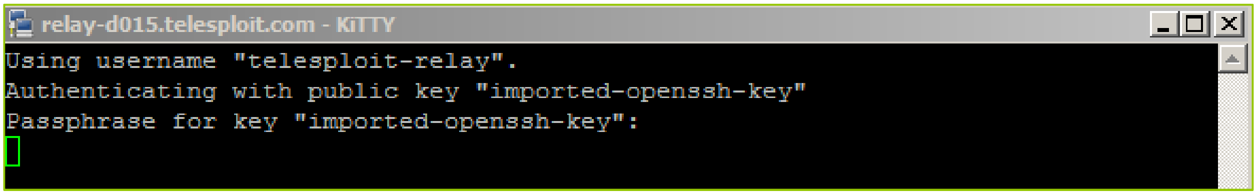
The first time you connect to the relay server KiTTY will pop-up a security alert indicating that the host key hasn't been cached.



The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.
The server's ssh-ed25519 key fingerprint is:
ssh-ed25519 256
07:a0:7f:25:92:2b:0a:af:20:fa:09:58:63:db:40:8d
If you trust this host, hit Yes to add the key to KiTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, hit No.
If you do not trust this host, hit Cancel to abandon the connection.

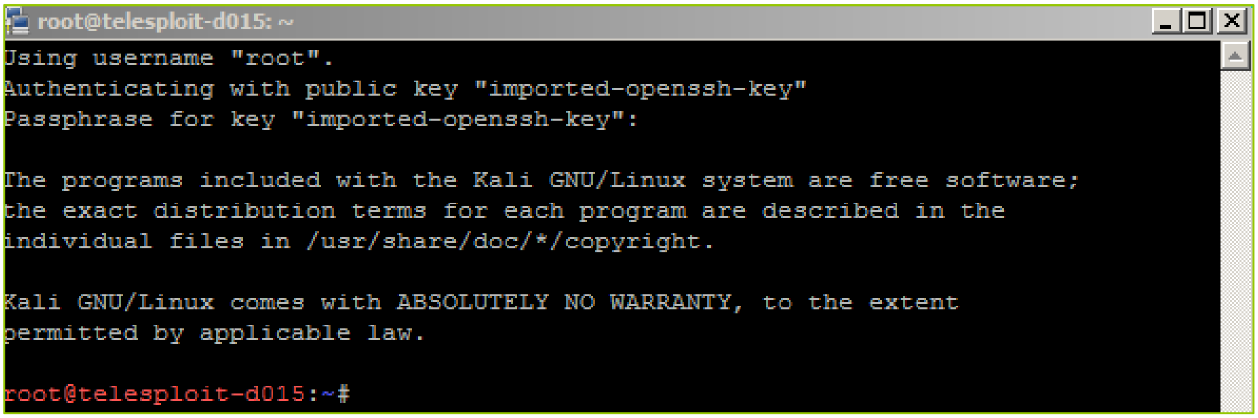
If you are connecting from a trusted environment accept the relay fingerprint and enter the passphrase for your private key.

The session window will appear to hang, but the tunnels will have been established. Minimizing the window will not have an effect on you connection. Closing the window will teardown the tunnels.



```
Using username "telesploit-relay".
Authenticating with public key "imported-openssh-key"
Passphrase for key "imported-openssh-key":
```

With the tunnels established open another instance of KiTTY and select Telesploit-Server. The first time you connect to the server you will receive another security alert. If you are connecting from a trusted environment accept the server fingerprint and enter the passphrase for your private key. You should now have a console session on the server.



```
Using username "root".
Authenticating with public key "imported-openssh-key"
Passphrase for key "imported-openssh-key":

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

root@telesploit-d015:~#
```

Common Tool Configuration

Please note that the SSH, VNC, Squid, and PostgreSQL services provided on the Telesploit server have been configured to only listen on localhost. If you install any additional services, such as Nessus, and do not want them to be exposed to the testing environment then restrict their access as well.

The following sections assume that you have configured the Telesploit client and established the required SSH tunnels.

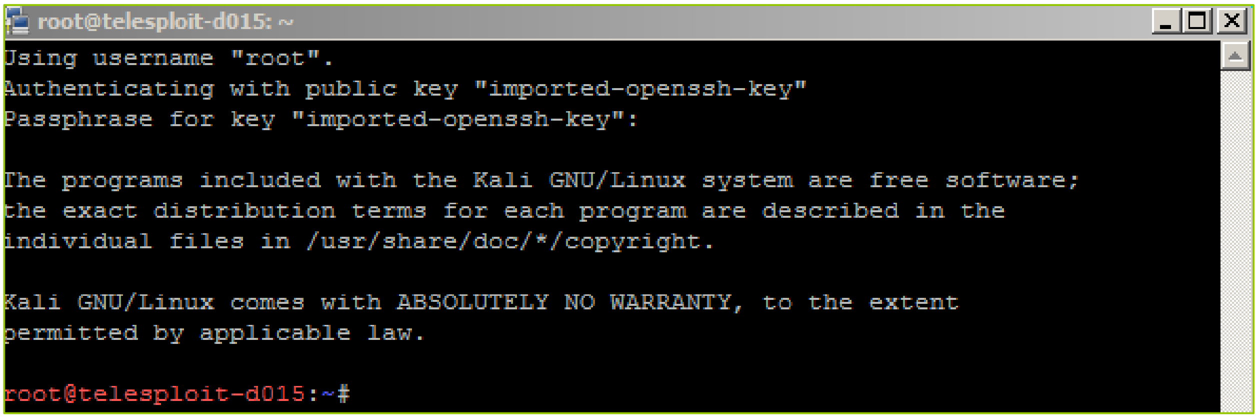
Command Line Interface

Your SSH client of choice may be used by configuring it with the following values. Adjust the port number to match your Telesploit deployment.

Example SSH Configuration

Host: localhost (127.0.0.1)
Username: root
Password: N/A
Private Key: Your SSH private key
Port: 13015
Note: As with any remote console, Telesploit recommends using a detachable session, such as screen, for long running processes.

This example uses KiTTY and the Telesploit-Server configuration.



```
Using username "root".
Authenticating with public key "imported-openssh-key"
Passphrase for key "imported-openssh-key":

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

root@telesploit-d015:~#
```

Remote Desktop

Your VNC client of choice may be used by configuring it with the following values. Adjust the port number to match your Telesploit deployment.

Example VNC Configuration

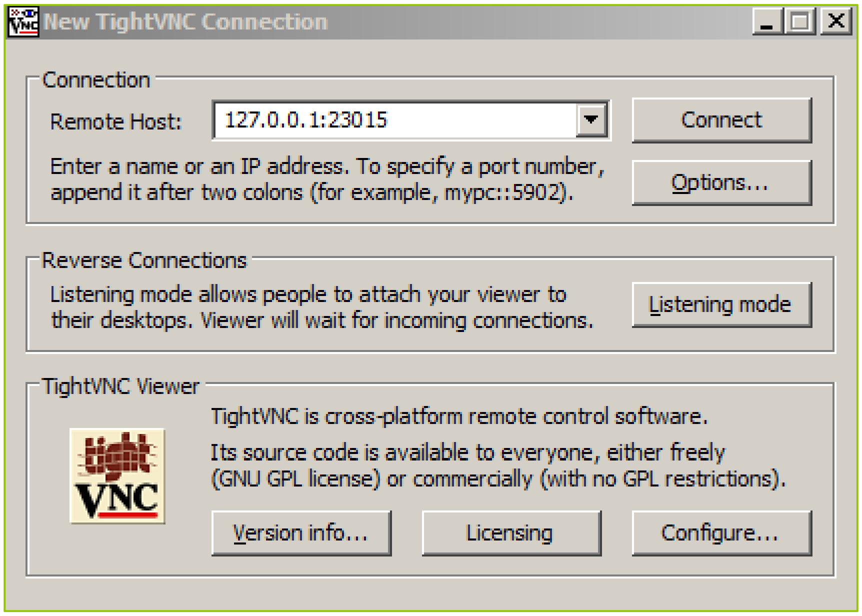
Host: localhost (127.0.0.1)

Username: <NONE>

Password: telesploit

Port: 23015

The following example uses the open source client, TightVNC.



Remote Host: 127.0.0.1:23015

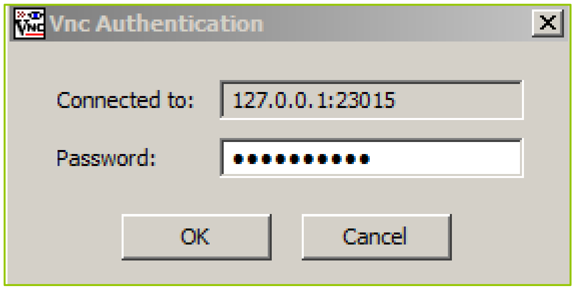
Enter a name or an IP address. To specify a port number, append it after two colons (for example, mypc::5902).

Listening mode allows people to attach your viewer to their desktops. Viewer will wait for incoming connections.

TightVNC is cross-platform remote control software.

Its source code is available to everyone, either freely (GNU GPL license) or commercially (with no GPL restrictions).

You will be prompted to enter the VNC password. As the VNC server is only listening on localhost, and connectivity requires SSH key authentication, this password is superfluous and has thus been set to 'telesploit' for all deployments.

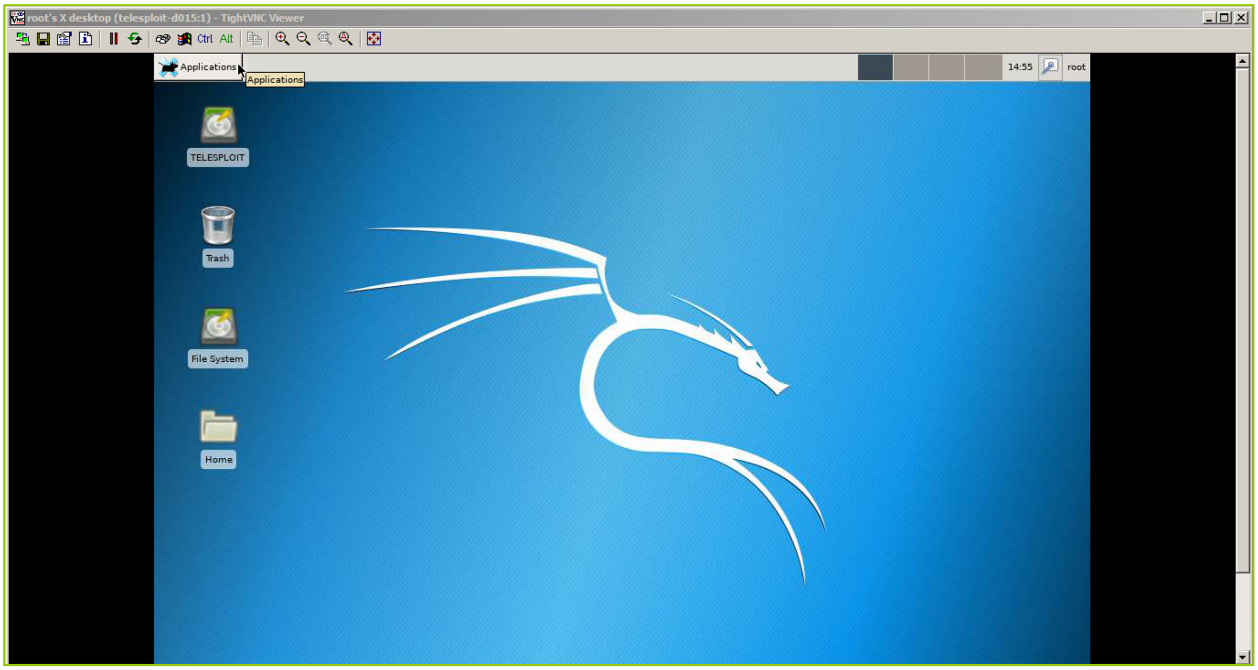


Vnc Authentication

Connected to: 127.0.0.1:23015

Password: ●●●●●●●●●●

Selecting the OK button will return a remote desktop on the Telesploit server.



root's X desktop (telesploit-d015:1) - TightVNC Viewer

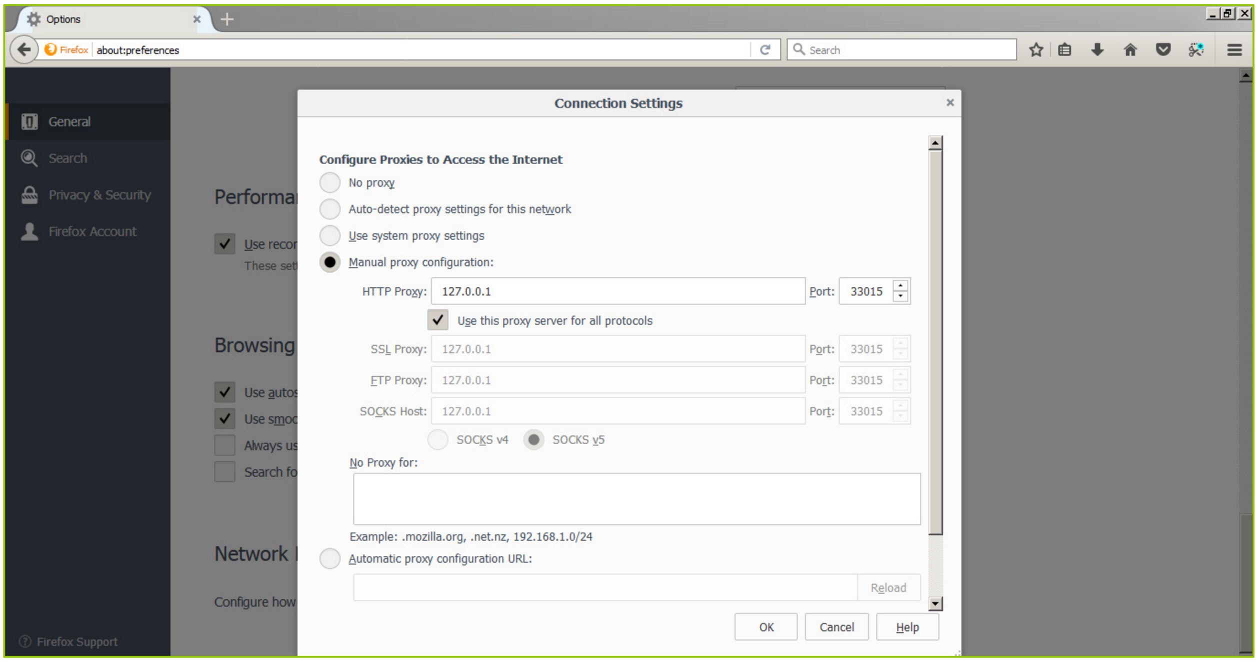
Web Proxy

Your browser and web application assessment tools of choice (e.g. Chrome, Edge, Burp Suite, Zap) may be used by configuring them with the following values. Adjust the port number to match your Telesploit deployment.

Example Web Proxy Configuration

Host: localhost (127.0.0.1)
Username: <NONE>
Password: <NONE>
Port: 33015

In Firefox these settings can be found under Options -> Network Proxy -> Settings.



Connection Settings

Configure Proxies to Access the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration:

HTTP Proxy: 127.0.0.1 Port: 33015

☑ Use this proxy server for all protocols

SSL Proxy: 127.0.0.1 Port: 33015

FTP Proxy: 127.0.0.1 Port: 33015

SOCKS Host: 127.0.0.1 Port: 33015

○ SOCKS v4 ● SOCKS v5

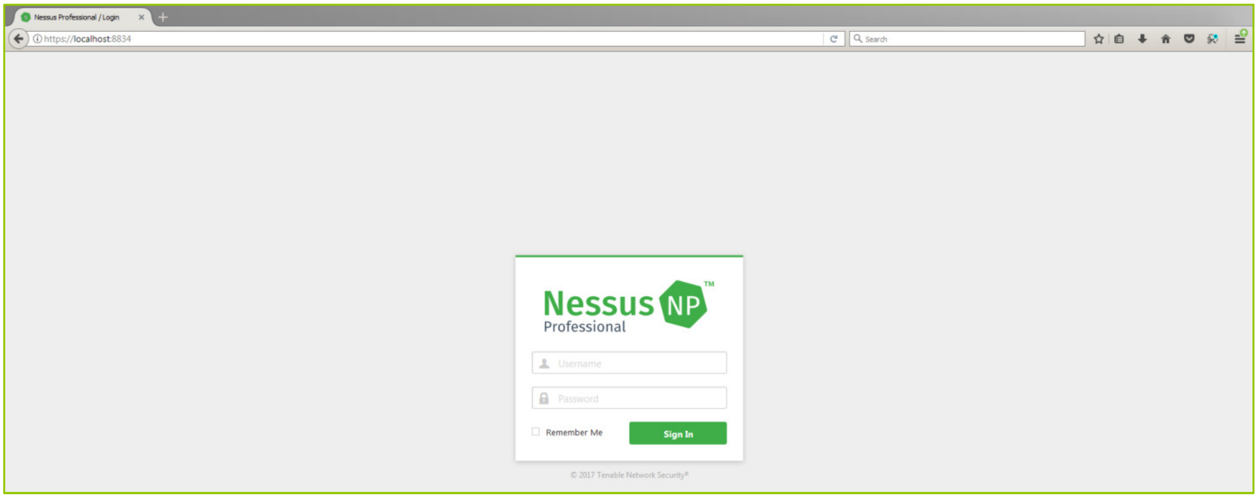
No Proxy for:

Example: .mozilla.org, .net.nz, 192.168.1.0/24

○ Automatic proxy configuration URL:

Web applications within the target environment can then be accessed by entering their IP address or Fully Qualified Domain Name along with port they are running on just as if you were testing from the local network.

Web-enabled applications running on the Telesploit server itself, such as Nessus (license not included), can be accessed by entering localhost or 127.0.0.1 and the port number.



https://localhost:8834

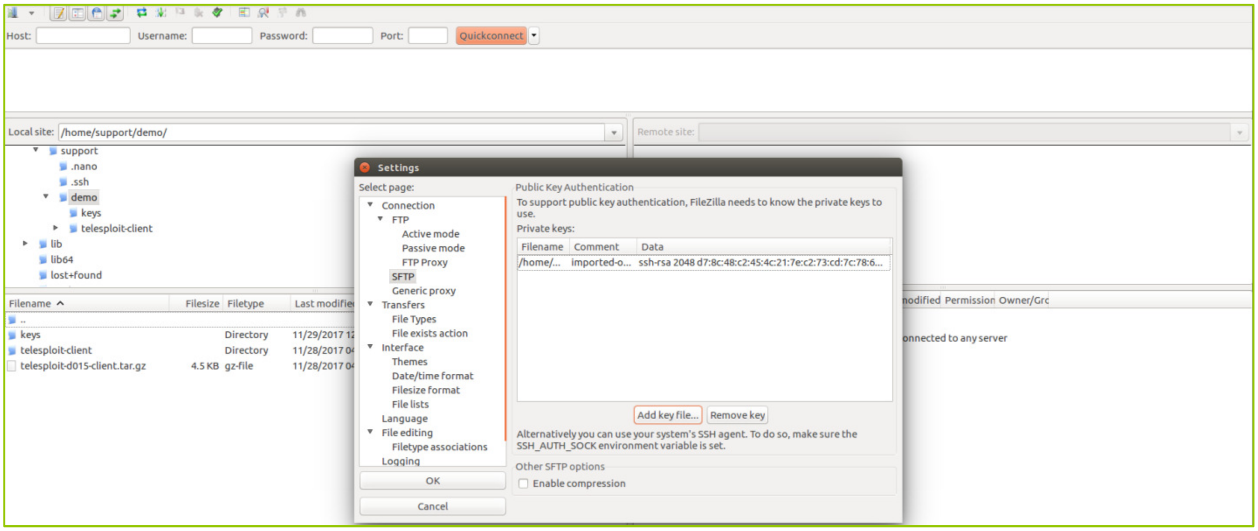
File Transfer

In addition to command line utilities, such as scp, file transfer tools like FileZilla may be used by configuring them with the following values. Adjust the port number to match your Telesploit deployment.

Example File Transfer Configuration

Host: localhost (127.0.0.1)
Username: root
Password: N/A
Private Key: Your SSH private key
Port: 13015

The following example uses FileZilla. To configure the application to use your SSH private key select Edit -> Preferences -> SFTP -> Add key file.



Host: Username: Password: Port: Quickconnect

Local site: /home/support/demo/

Remote site:

Settings

Select page:

- Connection
  - FTP
    - Active mode
    - Passive mode
    - FTP Proxy
  - SFTP
  - Generic proxy
- Transfers
  - File Types
  - File exists action
- Interface
  - Themes
  - Date/time format
  - Filesize format
  - File lists
- Language
- File editing
  - Filetype associations
- Logging

Public Key Authentication

To support public key authentication, FileZilla needs to know the private keys to use.

Private keys:

Filename	Comment	Data
/home/...	imported-o...	ssh-rsa 2048 d7:8c:48:c2:45:4c:21:7e:c2:73:cd:7c:78:6...

Add key file... Remove key

Alternatively you can use your system's SSH agent. To do so, make sure the SSH_AUTH_SOCK environment variable is set.

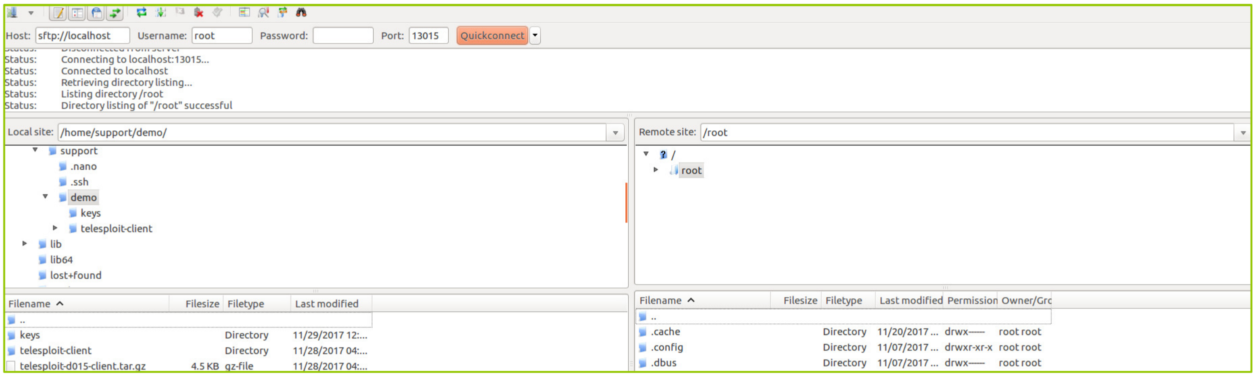
Other SFTP options

☐ Enable compression

OK

Cancel

Enter sftp://localhost in the Host field, leave the password blank to force key-based authentication, and enter the SSH port number assigned to your deployment in the Port field. Select Quickconnect, accept the SSH fingerprint, and enter the password to your private key.



Host: sftp://localhost Username: root Password: Port: 13015 Quickconnect

```
Status:     Connecting to localhost:13015...
Status:     Connected to localhost
Status:     Retrieving directory listing...
Status:     Listing directory /root
Status:     Directory listing of "/root" successful
```

Local site: /home/support/demo/

Remote site: /root

Filename	Filesize	Filetype	Last modified
..			
keys		Directory	11/29/2017 12:...
telesploit-client		Directory	11/28/2017 04:...
telesploit-d015-client.tar.gz	4.5 KB	gz-file	11/28/2017 04:...

Filename	Filesize	Filetype	Last modified	Permission	Owner/Grc
..					
.cache		Directory	11/20/2017 ...	drwx------	root root
.config		Directory	11/07/2017 ...	drwxr-xr-x	root root
.dbus		Directory	11/07/2017 ...	drwx------	root root

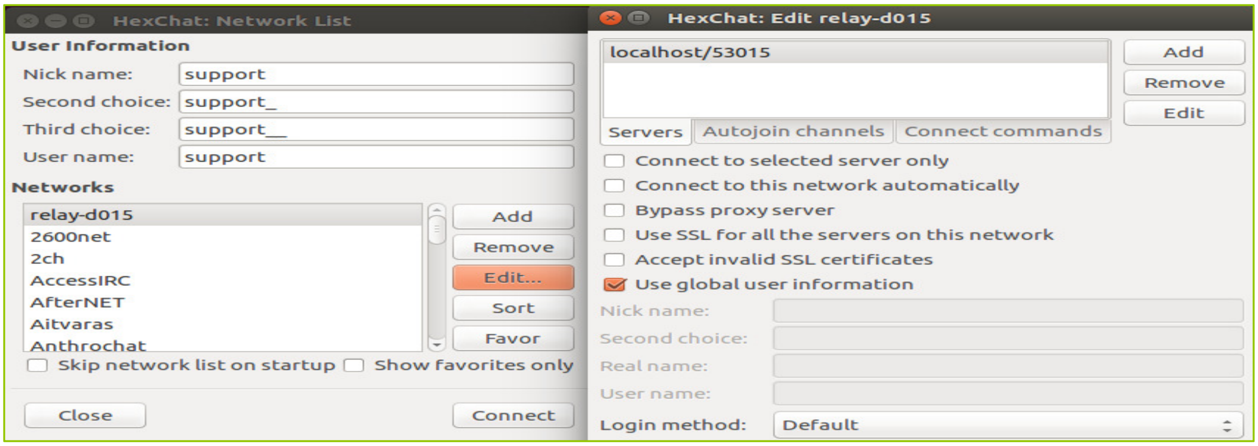
Internet Relay Chat

The Telesploit relay has an IRC server built in and both the client and server create SSH tunnels to communicate with it. Your IRC client of choice may be used by configuring it with the following values. Adjust the port number to match your Telesploit deployment.

Example IRC Configuration

Host: localhost (127.0.0.1)
Username: <ANY>
Password: <NONE>
Port: 53015

The following example uses HexChat.



HexChat: Network List

User Information

Nick name: support
Second choice: support_
Third choice: support__
User name: support

Networks

relay-d015
2600net
2ch
AccessIRC
AfterNET
Aitvaras
Anthrochat

□ Skip network list on startup □ Show favorites only

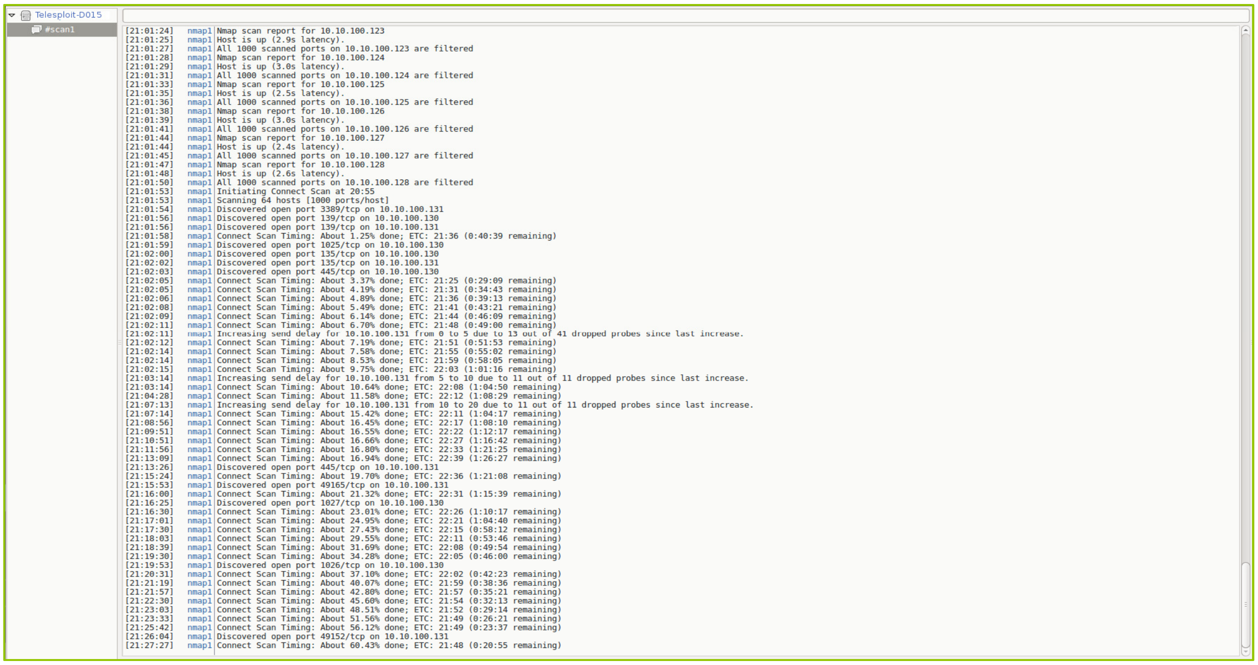
HexChat: Edit relay-d015

localhost/53015

□ Connect to selected server only
□ Connect to this network automatically
□ Bypass proxy server
□ Use SSL for all the servers on this network
□ Accept invalid SSL certificates
☑ Use global user information

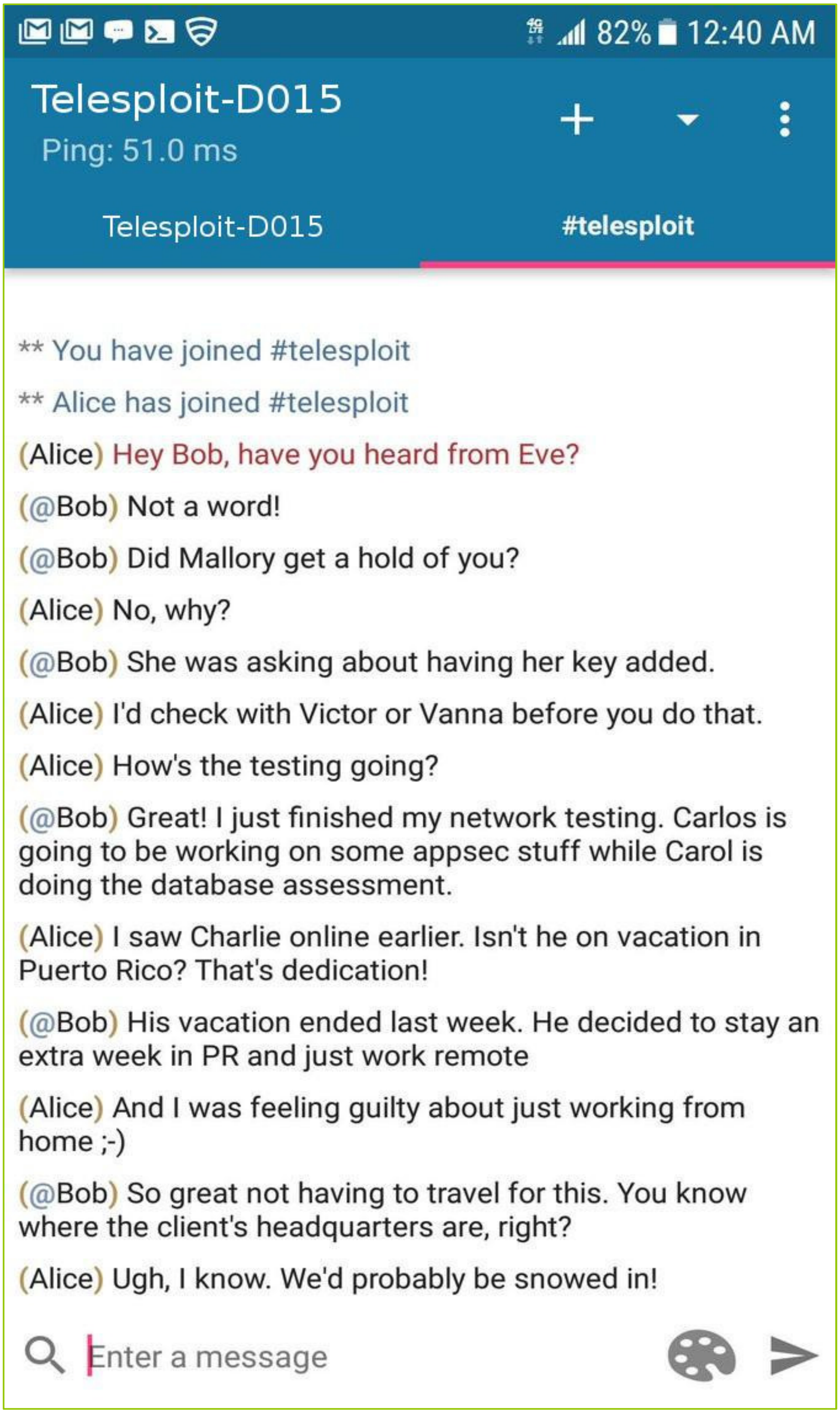
Nick name:
Second choice:
Real name:
User name:
Login method: Default

In addition to communication between team members, the IRC server can be used to provide updates from scanners and other tools running on the Telesploit server. Dedicate a channel for the output of each discrete activity and immediately know its status without cycling through multiple consoles or screen sessions.



```
[21:01:24]   nmap1 Nmap scan report for 10.10.100.123
[21:01:25]   nmap1 Host is up (2.9s latency).
[21:01:27]   nmap1 All 1000 scanned ports on 10.10.100.123 are filtered
[21:01:28]   nmap1 Nmap scan report for 10.10.100.124
[21:01:29]   nmap1 Host is up (3.0s latency).
[21:01:31]   nmap1 All 1000 scanned ports on 10.10.100.124 are filtered
[21:01:33]   nmap1 Nmap scan report for 10.10.100.125
[21:01:35]   nmap1 Host is up (2.5s latency).
[21:01:36]   nmap1 All 1000 scanned ports on 10.10.100.125 are filtered
[21:01:38]   nmap1 Nmap scan report for 10.10.100.126
[21:01:39]   nmap1 Host is up (3.0s latency).
[21:01:41]   nmap1 All 1000 scanned ports on 10.10.100.126 are filtered
[21:01:44]   nmap1 Nmap scan report for 10.10.100.127
[21:01:44]   nmap1 Host is up (2.4s latency).
[21:01:45]   nmap1 All 1000 scanned ports on 10.10.100.127 are filtered
[21:01:47]   nmap1 Nmap scan report for 10.10.100.128
[21:01:48]   nmap1 Host is up (2.6s latency).
[21:01:50]   nmap1 All 1000 scanned ports on 10.10.100.128 are filtered
[21:01:53]   nmap1 Initiating Connect Scan at 20:55
[21:01:53]   nmap1 Scanning 64 hosts [1000 ports/host]
[21:01:54]   nmap1 Discovered open port 3389/tcp on 10.10.100.131
[21:01:56]   nmap1 Discovered open port 139/tcp on 10.10.100.130
[21:01:56]   nmap1 Discovered open port 139/tcp on 10.10.100.131
[21:01:58]   nmap1 Connect Scan Timing: About 1.25% done; ETC: 21:36 (0:40:39 remaining)
[21:01:59]   nmap1 Discovered open port 1025/tcp on 10.10.100.130
[21:02:00]   nmap1 Discovered open port 135/tcp on 10.10.100.130
[21:02:02]   nmap1 Discovered open port 135/tcp on 10.10.100.131
[21:02:03]   nmap1 Discovered open port 445/tcp on 10.10.100.130
[21:02:05]   nmap1 Connect Scan Timing: About 3.37% done; ETC: 21:25 (0:29:09 remaining)
[21:02:05]   nmap1 Connect Scan Timing: About 4.19% done; ETC: 21:31 (0:34:43 remaining)
[21:02:06]   nmap1 Connect Scan Timing: About 4.89% done; ETC: 21:36 (0:39:13 remaining)
[21:02:08]   nmap1 Connect Scan Timing: About 5.49% done; ETC: 21:41 (0:43:21 remaining)
[21:02:09]   nmap1 Connect Scan Timing: About 6.14% done; ETC: 21:44 (0:46:09 remaining)
[21:02:11]   nmap1 Connect Scan Timing: About 6.70% done; ETC: 21:48 (0:49:00 remaining)
[21:02:11]   nmap1 Increasing send delay for 10.10.100.131 from 0 to 5 due to 13 out of 41 dropped probes since last increase.
[21:02:12]   nmap1 Connect Scan Timing: About 7.19% done; ETC: 21:51 (0:51:53 remaining)
[21:02:14]   nmap1 Connect Scan Timing: About 7.58% done; ETC: 21:55 (0:55:02 remaining)
[21:02:14]   nmap1 Connect Scan Timing: About 8.53% done; ETC: 21:59 (0:58:05 remaining)
[21:02:15]   nmap1 Connect Scan Timing: About 9.75% done; ETC: 22:03 (1:01:16 remaining)
[21:03:14]   nmap1 Increasing send delay for 10.10.100.131 from 5 to 10 due to 11 out of 11 dropped probes since last increase.
[21:03:14]   nmap1 Connect Scan Timing: About 10.64% done; ETC: 22:08 (1:04:50 remaining)
[21:04:28]   nmap1 Connect Scan Timing: About 11.58% done; ETC: 22:12 (1:08:29 remaining)
[21:07:13]   nmap1 Increasing send delay for 10.10.100.131 from 10 to 20 due to 11 out of 11 dropped probes since last increase.
[21:07:14]   nmap1 Connect Scan Timing: About 15.42% done; ETC: 22:11 (1:04:17 remaining)
[21:08:56]   nmap1 Connect Scan Timing: About 16.45% done; ETC: 22:17 (1:08:10 remaining)
[21:09:51]   nmap1 Connect Scan Timing: About 16.55% done; ETC: 22:22 (1:12:17 remaining)
[21:10:51]   nmap1 Connect Scan Timing: About 16.66% done; ETC: 22:27 (1:16:42 remaining)
[21:11:56]   nmap1 Connect Scan Timing: About 16.80% done; ETC: 22:33 (1:21:25 remaining)
[21:13:09]   nmap1 Connect Scan Timing: About 16.94% done; ETC: 22:39 (1:26:27 remaining)
[21:13:26]   nmap1 Discovered open port 445/tcp on 10.10.100.131
[21:15:24]   nmap1 Connect Scan Timing: About 19.70% done; ETC: 22:36 (1:21:08 remaining)
[21:15:53]   nmap1 Discovered open port 49165/tcp on 10.10.100.131
[21:16:00]   nmap1 Connect Scan Timing: About 21.32% done; ETC: 22:31 (1:15:39 remaining)
[21:16:25]   nmap1 Discovered open port 1027/tcp on 10.10.100.130
[21:16:30]   nmap1 Connect Scan Timing: About 23.01% done; ETC: 22:26 (1:10:17 remaining)
[21:17:01]   nmap1 Connect Scan Timing: About 24.95% done; ETC: 22:21 (1:04:40 remaining)
[21:17:30]   nmap1 Connect Scan Timing: About 27.43% done; ETC: 22:15 (0:58:12 remaining)
[21:18:03]   nmap1 Connect Scan Timing: About 29.55% done; ETC: 22:11 (0:53:46 remaining)
[21:18:39]   nmap1 Connect Scan Timing: About 31.69% done; ETC: 22:08 (0:49:54 remaining)
[21:19:30]   nmap1 Connect Scan Timing: About 34.28% done; ETC: 22:05 (0:46:00 remaining)
[21:19:53]   nmap1 Discovered open port 1026/tcp on 10.10.100.130
[21:20:31]   nmap1 Connect Scan Timing: About 37.10% done; ETC: 22:02 (0:42:23 remaining)
[21:21:19]   nmap1 Connect Scan Timing: About 40.07% done; ETC: 21:59 (0:38:36 remaining)
[21:21:57]   nmap1 Connect Scan Timing: About 42.80% done; ETC: 21:57 (0:35:21 remaining)
[21:22:30]   nmap1 Connect Scan Timing: About 45.60% done; ETC: 21:54 (0:32:13 remaining)
[21:23:03]   nmap1 Connect Scan Timing: About 48.51% done; ETC: 21:52 (0:29:14 remaining)
[21:23:33]   nmap1 Connect Scan Timing: About 51.56% done; ETC: 21:49 (0:26:21 remaining)
[21:25:42]   nmap1 Connect Scan Timing: About 56.12% done; ETC: 21:49 (0:23:37 remaining)
[21:26:04]   nmap1 Discovered open port 49152/tcp on 10.10.100.131
[21:27:27]   nmap1 Connect Scan Timing: About 60.43% done; ETC: 21:48 (0:20:55 remaining)
```

Stay connected on the go with mobile SSH and chat applications.



** You have joined #telesploit

** Alice has joined #telesploit

(Alice) Hey Bob, have you heard from Eve?

(@Bob) Not a word!

(@Bob) Did Mallory get a hold of you?

(Alice) No, why?

(@Bob) She was asking about having her key added.

(Alice) I'd check with Victor or Vanna before you do that.

(Alice) How's the testing going?

(@Bob) Great! I just finished my network testing. Carlos is going to be working on some appsec stuff while Carol is doing the database assessment.

(Alice) I saw Charlie online earlier. Isn't he on vacation in Puerto Rico? That's dedication!

(@Bob) His vacation ended last week. He decided to stay an extra week in PR and just work remote

(Alice) And I was feeling guilty about just working from home ;-)

(@Bob) So great not having to travel for this. You know where the client's headquarters are, right?

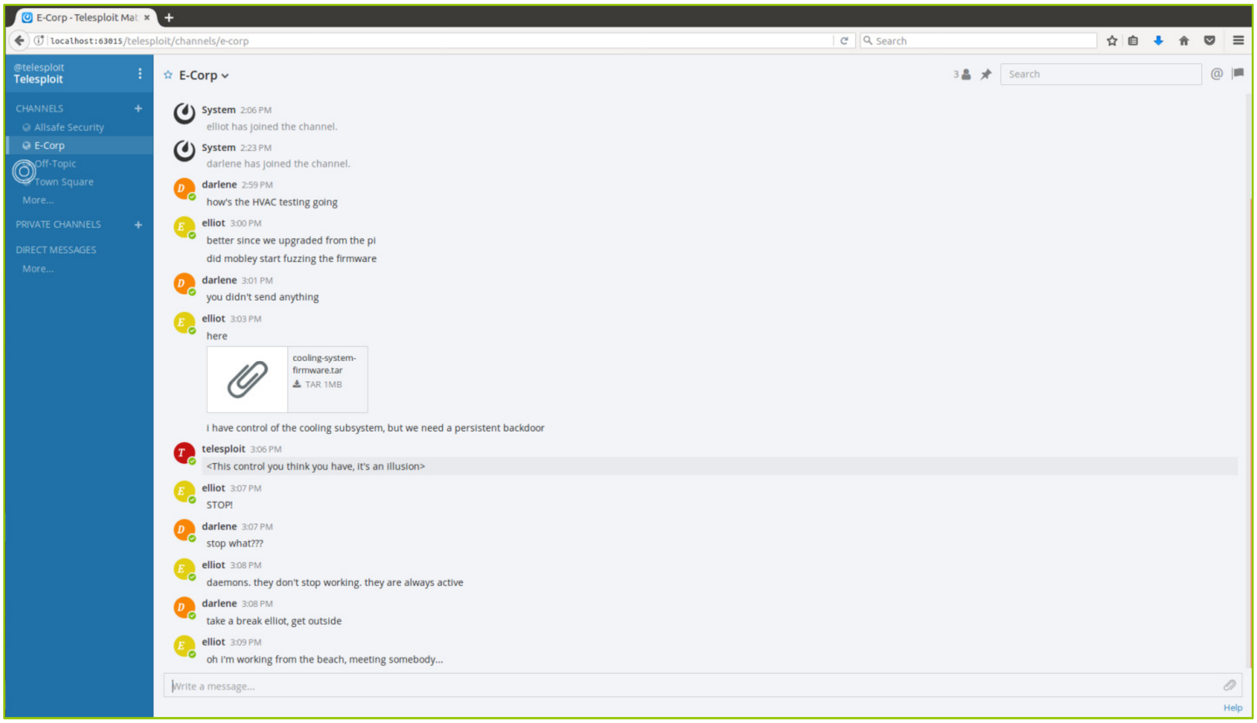
(Alice) Ugh, I know. We'd probably be snowed in!

Collaboration

The Telesploit relay has a Mattermost instance installed and both the client and server create SSH tunnels to communicate with it. A web browser or Mattermost client may be used by configuring them with the following values. Adjust the port number to match your Telesploit deployment.

Example Mattermost Configuration
Host: localhost (127.0.0.1)
Username: <Assigned by Mattermost Admin>
Password: <Assigned by Mattermost Admin>
Port: 63015

The first configured user will become the Mattermost admin. The following example uses a standard browser to access the collaboration platform.



System 2:06 PM
elliot has joined the channel.

System 2:23 PM
darlene has joined the channel.

darlene 2:59 PM
how's the HVAC testing going

elliot 3:00 PM
better since we upgraded from the pi
did mobley start fuzzing the firmware

darlene 3:01 PM
you didn't send anything

elliot 3:03 PM
here
cooling-system-firmware.tar
TAR 1MB
i have control of the cooling subsystem, but we need a persistent backdoor

telesploit 3:06 PM
<This control you think you have, it's an illusion>

elliot 3:07 PM
STOP!

darlene 3:07 PM
stop what???

elliot 3:08 PM
daemons. they don't stop working. they are always active

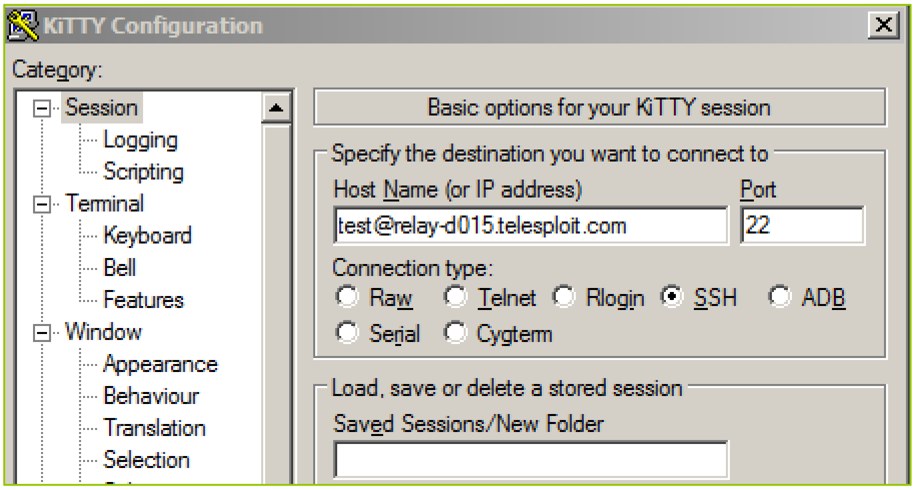
darlene 3:08 PM
take a break elliot, get outside

elliot 3:09 PM
oh i'm working from the beach, meeting somebody...

Troubleshooting

If you are unable to connect to the Telesploit server, then verify that you are able to directly connect to the relay.

If your client is configured to use an SSH connection, then try directly accessing the SSH server on the relay.



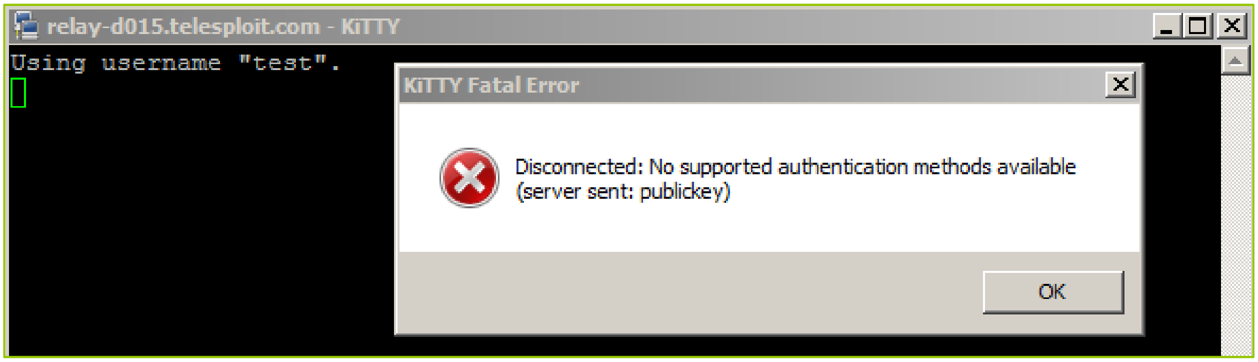
Specify the destination you want to connect to

Host Name (or IP address): test@relay-d015.telesploit.com

Port: 22

Connection type:
○ Raw ○ Telnet ○ Rlogin ● SSH ○ ADB
○ Serial ○ Cygterm

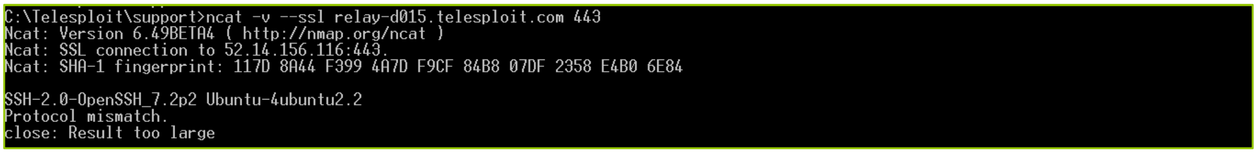
You will not be able to successfully login with the above settings, but it will validate that nothing is blocking your access and that the relay is up.



```
Using username "test".
```

Disconnected: No supported authentication methods available (server sent: publickey)

If you are using SSL/TLS proxied connections, then try accessing the SSH server through the HA Proxy running on the relay using ncat. You should see output similar to the following if nothing is blocking your access and the HA Proxy and SSH server are up.



```
C:\Telesploit\support>ncat -v --ssl relay-d015.telesploit.com 443
Ncat: Version 6.49BETA4 ( http://nmap.org/ncat )
Ncat: SSL connection to 52.14.156.116:443.
Ncat: SHA-1 fingerprint: 117D 8A44 F399 4A7D F9CF 84B8 07DF 2358 E4B0 6E84

SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.2
Protocol mismatch.
close: Result too large
```

If either of the above tests result in timeouts or no connections then verify that your outbound connections are not being blocked by a firewall or Intrusion Prevention System. Contact Telesploit support for additional assistance.