Ч.

Client Configuration Guide

Linux/Mac v2.3

This document is designed to quickly get you up and running on Linux or Mac using a customized client configuration.

TELESPLOIT

November 28, 2017

Client Configuration Guide

Linux/Mac v2.3

Contents

OVERVIEW	2
Telesploit Server	2
TELESPLOIT RELAY	2
CLIENT	2
CLIENT SETUP	3
DOWNLOAD AND EXTRACT CLIENT	3
CONFIGURE CLIENT	4
ESTABLISH SSH TUNNELS AND CONNECT TO THE SERVER	5
DISCONNECTING FROM SERVER AND CLOSING TUNNELS	6
COMMON TOOL CONFIGURATIONS	6
Command Line Interface	6
Remote Desktop	7
Web Proxy	8
FILE TRANSFER	8
INTERNET RELAY CHAT	10
COLLABORATION1	12
TROUBLESHOOTING	13

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

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

Example: https://relay-

d015.teles ploit.com/8b85b0fbb32c0575bc3cb21cc1af7db4eb167eed0b0d2de101bc7572363415bc/teles ploit-d015-client.tar.gz

Download and Extract Client

Download the archive file. In this example we are accessing the Telesploit relay/server with the designation d015. Change the commands to reflect your assigned environment.

curl https://relay-

d015.telesploit.com/8b85b0fbb32c0575bc3cb21cc1af7db4eb167eed0b0d2de101bc7572363415b c/telesploit-d015-client.tar.gz -o telesploit-d015-client.tar.gz

```
support@telesploit:-/demo$ curl https://relay-d015.telesploit.com/8b85b0fbb32c0575bc3cb21cc1af7db4eb167eed0b0d2de101bc7572363415bc/telesploit
-d015-client.tar.gz -o telesploit-d015-client.tar.gz
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 4410 100 4410 0 0 13466 0 -:-:-:- -:-:- 13445
```

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

sha256sum telesploit-d015-client.tar.gz

```
support@telesploit:-/demo$ curl https://relay-d015.telesploit.com/8b85b0fbb32c0575bc3cb2lcclaf7db4eb167eed0b0d2de101bc7572363415bc/telesploit
-d015-client.tar.gz -o telesploit-d015-client.tar.gz
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 4410 100 4410 0 0 13466 0 -:-:-:- -:-:- 13445
support@telesploit:-/demo$
support@telesploit:-/demo$
sha256sum telesploit-d015-client.tar.gz
8b85b0fbb32c0575bc3cb2lcc1af7db4eb167eed0b0d2de101bc7572363415bc
telesploit-d015-client.tar.gz
```

If the checksum matches then extract the archive file and change into the newly created directory.

tar -zxvf telesploit-d015-client.tar.gz && cd telesploit-client/telesploit-d015

cumment@talecpleit. /demost tar _ youf talecpleit d015 client tar gz 55 cd talecpleit client/talecpleit d015
support detespiont/ demos tai -// tetespiont-deis-ctient. tai .gz aa cu tetespiont-ctient/ tetespiont-deis
telesploit-client/telesploit-d015/
telesploit-client/telesploit-d015/client-configs/
telesploit-client/telesploit-d015/client-configs/client.cfg
telesploit-client/telesploit-d015/console.sh
telesploit-client/telesploit-d015/setup_client.sh
telesploit-client/telesploit-d015/update-server/
telesploit-client/telesploit-d015/update-server/network.sh
telesploit-client/telesploit-d015/update-server/server.cfg
telesploit-client/telesploit-d015/update-server/encrypted-configs/
telesploit-client/telesploit-d015/update-server/keys.sh
telesploit-client/telesploit-d015/update-server/connection.sh
telesploit-client/telesploit-d015/create_tunnels.sh
telesploit-client/telesploit-d015/kill_tunnels.sh
<pre>support@telesploit:~/demo/telesploit-client/telesploit-d015\$</pre>

You should see the following files and directories:

oport@telesploit:-/demo/telesploit-client/telesploit-d015\$ ls ient-configs console.sh create tunnels.sh kill tunnels.sh readme.txt setup client.sh update-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.

<pre>./setup_client.sh ./create_tunnels.sh ./console.sh</pre>
For detailed instructions download the Linux/Mac Configuration Guide from <u>https://www.telesploit.com.</u>
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

Configure Client

The first time you setup your client you will need to run the script setup_client.sh. If you are in an environment that allows outbound SSH then it is recommended that you select that option. If you will be tunneling the SSH connections through TLS then neat (part of the nmap suite) will be required on your system. If your environment requires using a proxy for outbound TLS connections then both neat and proxytunnels are required. The proxy information will also need to be either entered in the configuration file client-configs/client.cfg or interactively from within the setup script.

./setup_client.sh



Enter the path to the private key corresponding to the public key previously provided to Telesploit. Tab complete is enabled on this field.

Enter the full path to the private key being used to access the telesploit server, e.g. /home/user/.ssh/user.id_rsa, followed by [ENTER]: ~/d emo/keys/telesploit-d015

Choose your connection type. SSH is recommended. Direct (TLS) requires neat to be installed while all proxy connection types require both neat and proxytunnels.



The script will then pull a file from the relay containing the SSH server's known fingerprint and compare it to a locally generated version. Matching files indicate that an active Man-in-the-Middle attack is not being performed against your connection.

Choose the telesploit client connection type [S/D/P/B/N]: S
saving connection status to ./client-configs/connection.cfg creating ssh config file and saving to ./client-configs/config
retrieving trusted fingerprint from https://relay-d015.telesploit.com/trusted % Total % Received % Xferd Average Speed Time Time Time Current Dload Upload Total Spent Left Speed
100 407 100 407 0 0 1067 0: 1068
retrieving ssh fingerprint from relay-dwij.telesploit.com
relay-duls.telesploit.com:22 SSH-2.0-0penSSH_7.2p2 Ubuntu-4ubuntu2.2
running diff against trusted and tested
Files ./client-configs/trusted and ./client-configs/tested are identical
identical files indicate a secure connection
non-matching files may indicate an active man-in-the-middle attack, review the files 'trusted' and 'tested' before continuing
Press any key to continue or Ctrl+C to exit

Enter the password for the private key corresponding to the public key previously provided to Telesploit. If you are not prompted for your password then verify the location and permissions on your private key and that you have neat installed if using TLS or proxy connections then re-run setup_client.sh.

enter the password for your SSH key for d015 at the prompt Enter passphrase for key '/home/support/demo/keys/telesploit-d015':

You should then be returned to the command prompt.

Establish SSH Tunnels and Connect to the Server

Once the client has been configured for your environment, verify that you can create SSH tunnels to the relay by running the script create_tunnels.sh. You will once again be prompted for the password to your SSH private key.

./create_tunnels.sh

```
support@telesploit:-/demo/telesploit-client/telesploit-d015$ ./create_tunnels.s
Enter passphrase for key '/home/support/demo/keys/telesploit-d015':
support@telesploit:-/demo/telesploit-client/telesploit-d015$
```

Once the tunnels have been established you can verify connectivity by connecting to the Telesploit server using the script console.sh. You will once again be prompted for the password to your SSH private key. If everything has been configured properly you should see a Kali Linux command prompt.

./console.sh

```
support@telesploit:-/demo/telesploit-client/telesploit-d015$ ./console.sh
Enter passphrase for key '/home/support/demo/keys/telesploit-d015':
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.
```

Disconnecting from Server and Closing Tunnels

Typing 'exit' at the server command prompt will return you to your local shell.

exit

root@telesploit-d015:-# exit
logout
Connection to localhost closed.
support@telesploit:~/demo/telesploit-client/telesploit-d015\$

When not performing testing, you may teardown the tunnels by running the script kill_tunnels.sh. You should immediately be returned to the command prompt.

./kill_tunnels.sh

support@telesploit:~/demo/telesploit-client/telesploit-d015\$./kill_tunnels.sh support@telesploit:~/demo/telesploit.client/telesploit.d015\$

The next time you wish to connect to the Telesploit server it is not necessary to re-run the setup_client.sh script, just use the create_tunnels.sh script to bring the tunnels back up.

Common Tool Configurations

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 the script console.sh included with the Telesploit client.

elesploit-client/telesploit-d015

./console.sh

Enter passphrase for key '/home/support/demo/keys/telesploit-d015': 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.

6

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 Remmina Remote Desktop Client. 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.

🛹 Connect 📑 🧟 💁 🔀		
VNC - 127.0.0.1:23015 Connect !		
Name Group Server		
	Connecting to '127.0.0.1:23015' Connecting to '127.0.0.1:23015' VNC password Save VNC password Cancel OK	

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



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.

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.



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.

a v ZIA v v k v k v k v k v k v k v k v k v k	Port: Quickcon	nect	
Local site: /home/support/dema/	Settings Select page: Connection FTP Active mode Passive mode FTP Proxy SFTP Generic proxy Transfers File exists action Interface Themes Date/time format Fileste format File idits Language File dedting OK Cancel	Public Key Authentication To support public key authentication, FileZilla needs to know the private keys to use private keys: 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 Alternatively you can use your system? SSH_AUTH_SOCK environment variable is set. Other SFTP options Enable compression	nedified Permission Owner/Grc onnected to any server
1 file and 2 directories. Total size: 4.5 KB	iority Chatur	Not connected.	
Queued files Failed transfers Successful transfers	- Caros		

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://localbost liserpame: root Dassword: Port: 13015 Quickconnect *			
Status: Concerting directions: 1005. Status: Concerting directions: 1005. Status: Concerted to localhost Status: Concerted to localhost			
Local site: /home/support/demo/	✓ Remote site: /root		
 support ano ssh demo keys telsploit-client lib libo4 lost+found 	¥ 2)/		
Filename A Filesize Filetype Last modified	Filename 🔨	Filesize Filetype Last modified Permission Owner/Gro	
► 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:	.cache .cache .config .dbus .gunupg .gvfs .local .mozilla .msf4 .nano .ssh .vnc Desktop Documents Downloads Music Pictures Public	Directory 11/20/2017 drwx.— root root Directory 11/07/2017 drwx.— root root Directory 11/07/2017 drwx.— root root Directory 11/07/2017 drwx.— root root Directory 06/03/2017 drwxw. root root Directory 06/11/2017 drwxw. root root Directory 06/11/2017 drwxw. root root Directory 01/21/2017 drwxw. root root Directory 01/12/2017 drwxw. root root Directory 06/03/2017 drwxw. root root	
1 file and 2 directories. Total size: 4.5 KB	34 files and 21 director	ries. Total size: 168.2 MB	
Server/Local File Directio Remote file Size Priority Status			
environdering Failed transform Successful transform			

Client Configuration Guide | 11/28/2017

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			😣 🗐 Не	xChat:	Edit relay-d	015		
User Information		localhost/53015			Add			
Nick name:	e: support poice: support_							
Second choice:								
Third choice:	support		Servers	Autojo	oin channels	Connect commands	Edic	
User name:	ser name: support			Connect to selected server only				
Networks			Connect to this network automatically					
relay-d015			Bypass proxy server					
2600net	2600net			Use SSL for all the servers on this network				
2ch		Kelliove	Accept invalid SSL certificates					
AccessIRC		Edit	🕑 Use g	obal us	er informatio	n		
AfterNET		Sort	Nick nam	e:				
Aitvaras			Conserved at					
Anthrochat		Favor	Second ci	noice:				
Skip networ	k list on startup 🗌 Show	favorites only	Realnam	e:				
			User nam	e:				
Close		Connect	Login me	thod:	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.

P decail 12:01:23 Hange Case Top Cas	tered tered tered tered tered tered
2100122) map: last is up (2.5s istency). 2100122) map: All Deciman All Deciman Ports in 10 ab 100 122 are f 2100123 map: All Deciman Ports in 10 ab 100 122 are f 2100123 map: All Deciman Ports in 10 ab 100 122 are f 2100123 map: All Deciman Ports in 10 ab 100 122 are f 2100123 map: All Deciman Ports in 10 ab 100 122 are f 2100123 map: All Deciman Ports in 10 ab 100 122 are f 2100123 map: All Deciman Ports in 10 ab 100 122 are f 2100123 map: All Deciman Ports in 10 ab 100 122 are f 2100123 map: All Deciman Ports in 10 ab 100 122 are f 2100124 map: All Deciman Ports in 10 ab 100 122 are f 2100124 map: All Deciman Ports in 10 ab 100 122 are f 2100124 map: All Deciman Ports in 10 ab 100 122 are f 2100124 map: All Deciman Ports in 10 ab 100 122 are f 2100124 map: All Deciman Ports in 10 ab 100 122 are f 2100124 map: All Deciman Ports in 10 ab 100 122 are f 2100124 map: All Deciman Ports in 10 ab 100 122 are f 2100124 map: All Deciman Ports in 10 ab 100 122 are f 2100124 map: All Deciman Ports in 10 ab 100 122 are f 2100124 map: All Deciman Ports in 10 ab 100 120 are f 2100124 map: All Deciman Ports in 10 ab 100 120 are f 2100124 map: All Deciman Ports in 10 ab 100 120 are f 2100124 map: All Deciman Ports in 10 ab 100 120 are f 2100124 map: All Deciman Ports in 10 ab 100 120 are f 2100124 map: All Deciman Ports in 10 ab 100 120 are f 2100124 map: All Deciman Ports in 10 ab 1	tered tered tered tered tered tered tered tered tered
1210.120 maps Maps Team	tered tered tered tered tered
[210172] map: hest is up (1.6 statemcy). [210172] map: hest scale negror for 16.10.00.122 [210173] map: hest scale negror for 16.10.00.123 [210173] map: hest scale negror for 16.10.00.125 [210173] map: hest scale negror for 16.10.00.125 [210173] map: hest scale negror for 16.10.00.125 [210173] map: hest scale negror for 16.10.00.126 [210173] map: hest scale negror for 16.10.00.126 [210173] map: hest scale negror for 16.10.00.126 [210174] map: hest scale negror for 16.10.00.100.102 [210174] map: hest scale negror for 16.10.10.00.102 [210176] map: hest scale negror for 16.10.10.10.10.10.10.100 [210176] map: hest scale negror for 16.10.10.10.10.10.10.10.10.100 [2101760] map: hes	tered tered tered tered
[21:01:33] mmap: Next is up (3.5) 1.80:0.328 [21:01:33] mmap: Next is up (3.5) 1.80:0.328 [21:01:33] mmap: Next is up (3.5) 1.80:0.128 [21:01:33] mmap: Next is up (3.5) 1.80:0.128 [21:01:34] mmap: Next is up (3.6) 1.80:0.128 [21:01:35] mmap: Next is up (3.6)	tered tered tered tered
1210135 mms) Hell is up 12.8 later(7) 1210135 mms) Hell is up 12.8 later(7) 1210135 mms) Hell is up 13.6 later(7) 1210135 mms) Hell is up 13.7 later(7)	tered tered tered
[21:01:33] mmp) Hemp icon report for 10:10:00:26 [21:01:34] mmp) Hemp icon report for 10:10:00:126 [21:01:44] mmp) Hemp icon report for 10:10:00:126 [21:01:44] mmp) Hemp icon report for 10:10:00:127 [21:01:44] mmp) Hemp icon report for 10:10:00:127 [21:01:44] mmp) Hemp icon report for 10:10:00:127 [21:01:44] mmp) Hemp icon report for 10:10:00:128 [21:01:47] mmp) Hemp icon report for 10:10:10:00:128 [21:01:47] mmp) Hemp icon report for 10:10:10:00:128 [21:01:47] mmp) Hemp icon report for 10:10:10:10:128 [21:01:53] mmp) Hemp icon report for 10:10:10:10:128 [21:01:54] mmp) Hemp icon report for 10:10:10:10:128 [21:01:55] mmp) Hemp icon report for 10:10:10:128 [21:01:56] mmp) Discovered open port 139/tcp on 10:10:10:10:13 [21:01:56] mmp) Discovered open port 139/tcp on 10:10:10:10:10:13 [21:01:56] mmp) Discovered open port 139/tcp on 10:10:10:10:13 [21:01:56] mmp) Discovered open port 139/tcp on 10:10:10:10:10:10:10:10:10:10:10:10:10:1	tered tered tered
2101.201 mass Hall 16 0p 1.36 Latercy 2101.201 Hall 16 0p 1.36 Latercy Hall 16 0p 1.3	tered tered tered
[21:01:44] mmap: Neap :can report for 10:10:00:127 [21:01:44] mmap: Neap :can report for 10:10:10:10:10:10:10:10:10:10:10:10:10:1	tered tered
 121.01.40 121.01.40	tered tered
[21:01:47] mmap: Name and memory for 10:10:00.218 [21:01:53] mmap: Nall Dec Scamer ports Name and Nall Dec Scamer ports [21:01:53] mmap: Nall Dec Scamer ports Nall Dec Scamer ports [21:01:53] mmap: Nall Dec Scamer ports Nall Dec Scamer ports [21:01:54] mmap: Discovered gene port 1389/tcp on 10:0.10:0.128 Nall Dec Scamer ports [21:01:55] mmap: Discovered gene port 1389/tcp on 10:0.10:0.128 Nall Dec Scamer ports [21:01:56] mmap: Discovered gene port 1389/tcp on 10:0.10:0.13 Nall Dec Scamer ports [21:01:56] mmap: Discovered gene port 1389/tcp on 10:0.10:0.13 Nall Dec Scamer ports Nall Dec Scamer ports [21:01:56] mmap: Discovered gene port 1389/tcp on 10:0.10:0.13 Nall Dec Scamer ports Nall Dec Scamer ports [21:01:56] mmap: Discovered gene port 1489/tcp on 10:0.10:0.13 Nall Dec Scamer ports Nall Dec Scamer ports [21:02:03] mmap: Discovered gene port 1489/tcp on 10:0.10:0.10:0.10:0.13 Nall Dec Scamer ports Nall Dec Scamer ports [21:02:04] mmap: Discovered gene port 1489/tcp on 10:0.10:0.10:0.10:0.10:0.10:0.10:0.10:0	tered
121:01:56 mmp: 141.100 ⁶ scamed ports fm 10.10.10.121 are f 121:01:54 mmp: 141.100 ⁶ scamed ports are 2015 121:01:54 mmp: 141.100 ⁶ scamed ports are 2015 121:01:54 mmp: 151.011.011.011.011.011.011.011.011.011.	tered
2101153 mmap: Discovered open port 339/ttp on 10.10.100.13 2101154 mmap: Discovered open port 339/ttp on 10.10.100.13 2101155 mmap: Discovered open port 339/ttp on 10.10.100.13 2101156 mmap: Discovered open port 139/ttp on 10.10.100.13 2101156 mmap: Discovered open port 139/ttp on 10.10.100.13 2101156 mmap: Discovered open port 139/ttp on 10.10.100.13 2101157 mmap: Discovered open port 139/ttp on 10.10.100.13 2101157 mmap: Discovered open port 149/ttp on 10.10.100.13 2101157 mmap: Discovered Cam Thiiiiiii: Advant 1.000.000	
[21:01:54] mmail Discovered open port 338/rtcp on 10.10.00.11 [21:01:54] mmail Discovered open port 338/rtcp on 10.10.00.11 [21:01:56] mmail Discovered open port 338/rtcp on 10.10.00.11 [21:01:56] mmail Discovered open port 138/rtcp on 10.10.10.00.11 [21:01:56] mmail Discovered open port 138/rtcp on 10.10.10.00.01 [21:02:56] mmail Discovered open port 138/rtcp on 10.10.10.00.01 [21:02:56] mmail Connect Scan Thing: About 1.37% done; TfC: 2 [21:02:56] mmail Connect Scan Thing: About 1.47% done; TfC: 2 [21:02:56] mmail Connect Scan Thing: About 5.4% done; TfC: 2 [21:02:56] mmail Connect Scan Thing: About 7.4% done; TfC: 2 [21:02:56] mmail Connect Scan Thing: About 7.5% done; TfC: 2 [21:02:56] mmail Connect Scan Thing: About 7.5% done; TfC: 2 [21:02:12] mmail Connect Scan Thing: About 7.5% done; TfC: 2 [21:02:12] mmail Connect Scan Thing: About 7.5% done; TfC: 2 [21:02:12] mmail Connect Scan Thing: About 10.5%	
12101:50 mmp: ConnectSed Span port 1397/CD on 10.10.108 12101:51 mmp: ConnectSed Tabus mmp: ConnectSed Tabus 12101:52 mmp: ConnectSed Tabus mmp: ConnectSed Tabus 12101:53 mmp: ConnectSed Tabus mmp: ConnectSed Tabus 12101:54 mmp: ConnectSed Tabus Mmp: ConnectSed Tabus 12101:55 mmp: Discovered Gen port 1357/CD on 10.10.10.13 12101:56 mmp: Discovered Gen port 1457/CD on 10.10.10.13 12101:56 mmp: Discovered Gen port 1457/CD on 10.10.10.13 12101:56 mmp: Discovered Gen port 1457/CD on 10.10.10.11 12101:56 mmp: ConnectScan Tabus Mone FTC : 2 12101:56 mmp: ConnectScan Tabus Mone FTC : 2 12101:56 mmp: ConnectScan Tabus Mone FTC : 2 12101:51 mmp: ConnectScan Tabus	
[21] 01:58] mmp0 Connect Scan Thing; Abort 1.25% dome; FCT: 2 [21] 02:02 mmp0 Discovered gene port 135/rtcp in 10.108.109 [21] 02:02 mmp0 Discovered gene port 135/rtcp in 10.108.109 [21] 02:02 mmp0 Discovered gene port 135/rtcp in 10.108.109 [21] 02:02 mmp0 Discovered gene port 135/rtcp in 10.108.109 [21] 02:05 mmp0 Connect Scan Thing; Abort 3.7% dome; FCT: 2 [21] 02:05 mmp0 Connect Scan Thing; Abort 4.9% dome; FCT: 2 [21] 02:06 mmp0 Connect Scan Thing; Abort 5.4% dome; FCT: 2 [21] 02:07 mmp0 Connect Scan Thing; Abort 5.4% dome; FCT: 2 [21] 02:08 mmp0 Connect Scan Thing; Abort 7.5% dome; FCT: 2 [21] 02:01 mmp0 Connect Scan Thing; Abort 7.5% dome; FCT: 2 [21] 02:01 mmp0 Connect Scan Thing; Abort 7.5% dome; FCT: 2 [21] 02:01 mmp0 Connect Scan Thing; Abort 7.5% dome; FCT: 2 [21] 02:01 mmp0 Connect Scan Thing; Abort 7.5% dome; FCT: 2 [21] 02:01 mmp0 Connect Scan Thing; Abort 7.5% dome; FCT: 2 [21] 02:01 mmp0 Connect Scan Thing; A	
121.02.06 mmap: Discovered gene port 1397/cp on 10.10.10.00.10.10. 121.02.02.07 mmap: Discovered gene port 1397/cp on 10.10.10.10.10.10.10.10.10.10.10.10.10.1	36 (0:40:39 remaining)
1210-2501 mmap: Discovered open port 135/tcp on 10-18.186.31 1210-2507 mmap: Connect Scan Thing: About 4.190 done; FTC: 2 1210-2507 mmap: Connect Scan Thing: About 4.190 done; FTC: 2 1210-2507 mmap: Connect Scan Thing: About 4.190 done; FTC: 2 1210-2507 mmap: Connect Scan Thing: About 5.490 done; FTC: 2 1210-2507 mmap: Connect Scan Thing: About 5.490 done; FTC: 2 1210-2507 mmap: Connect Scan Thing: About 5.490 done; FTC: 2 1210-2507 mmap: Connect Scan Thing: About 5.490 done; FTC: 2 1210-2507 mmap: Connect Scan Thing: About 5.490 done; FTC: 2 1210-2511 mmap: Connect Scan Thing: About 5.590 done; FTC: 2 1210-2511 mmap: Connect Scan Thing: About 5.590 done; FTC: 2 1210-2514 mmap: Connect Scan Thing: About 1.595 done; FTC: 2 1210-2514 mmap: Connect Scan Thing: About 1.595 done; FTC: 2 1210-2514 mmap: Connect Scan Thing: About 15.495 done; FTC: 2 1210-2514 mmap: Connect Scan Thing: About 15.495 done; FTC: 2 1210-2514 mmap: Connect Scan Thing: About 15.495 done; FTC: 2 1210-2514 mmap: Connect Scan Thing: About 15.495 done; FTC: 2 1210-2514 mmap: Connect Scan Thing: About 15.495 done; FTC: 2 <td></td>	
121.022:05 mmap: Connect Scan Thing: About 3.74 done; ETC: 2 121.022:05 mmap: Connect Scan Thing: About 3.95 done; ETC: 2 121.022:06 mmap: Connect Scan Thing: About 3.94 done; ETC: 2 121.022:07 mmap: Connect Scan Thing: About 5.49 done; ETC: 2 121.022:08 mmap: Connect Scan Thing: About 5.49 done; ETC: 2 121.022:08 mmap: Connect Scan Thing: About 5.49 done; ETC: 2 121.022:08 mmap: Connect Scan Thing: About 5.49 done; ETC: 2 121.022:01 mmap: Connect Scan Thing: About 7.199 done; ETC: 2 121.022:01 mmap: Connect Scan Thing: About 7.99 done; ETC: 2 121.022:01 mmap: Connect Scan Thing: About 7.99 done; ETC: 2 121.022:01 mmap: Connect Scan Thing: About 7.99 done; ETC: 2 121.021:01 mmap: Connect Scan Thing: About 7.99 done; ETC: 2 121.021:01 mmap: Connect Scan Thing: About 7.99 done; ETC: 2 121.031:01 mmap: Connect Scan Thing: About 7.99 done; ETC: 2 121.031:14 mmap: Connect Scan Thing: About 11.59 done; ETC: 2 121.031:14 mmap: Connect Scan Thing: About 11.59 done; ETC: 2 121.031:14 mmap: Connect Scan Thing: About 11.59 done; ETC: 2 121.031:14 mmap: Connect Scan Thing: About 11.59 done; ETC: 2 <td></td>	
121.02.03 connect Scan Tialing, About 4.0% dome; TC: 2 121.02.03 map) Connect Scan Tialing, About 4.0% dome; TC: 2 121.02.03 map) Connect Scan Tialing, About 5.0% dome; TC: 2 121.02.03 map) Connect Scan Tialing, About 5.0% dome; TC: 2 121.02.03 map) Connect Scan Tialing, About 5.0% dome; TC: 2 121.02.03 map) Connect Scan Tialing, About 7.0% dome; TC: 2 121.02.03 map) Connect Scan Tialing, About 7.0% dome; TC: 2 121.02.03 map) Connect Scan Tialing, About 7.0% dome; TC: 2 121.02.03 map) Connect Scan Tialing, About 7.0% dome; TC: 2 121.02.03 map) Connect Scan Tialing, About 7.0% dome; TC: 2 121.02.03 map) Connect Scan Tialing, About 7.0% dome; TC: 2 121.03.03 map) Connect Scan Tialing, About 16.0% dome; TC: 2 121.03.03 map) Connect Scan Tialing, About 16.0% dome; TC: 2 121.07.03 map) Connect Scan Tialing, About 16.0% dome; TC: 2 121.07.03 map) Connect Scan Tialing, About 16.0% dome; TC: 2 121.07.03 map) Connect Scan Tialing, About 16.0% dome; TC: 2 121.07.03 map) Connect Scan Tialing, About 16.0% dome; TC: 2 121.07.03 map) Connect Scan Tialing, About 16.0% dome; TC: 2	25 (0:29:00 remaining)
[21102:08] mmap) Connect Scan Thung, About 5.494 done; TTC: 2 [21102:08] mmap) Connect Scan Thung, About 5.494 done; TTC: 2 [21102:08] mmap) Connect Scan Thung, About 5.494 done; TTC: 2 [21102:01] mmap) Connect Scan Thung, About 5.494 done; TTC: 2 [21102:01] mmap) Connect Scan Thung, About 7.194 done; TTC: 2 [21102:01] mmap) Connect Scan Thung, About 8.594 done; TTC: 2 [21102:01] mmap) Connect Scan Thung, About 8.594 done; TTC: 2 [21102:01] mmap) Connect Scan Thung, About 8.594 done; TTC: 2 [21102:01] mmap) Connect Scan Thung, About 8.594 done; TTC: 2 [21102:01] mmap) Connect Scan Thung, About 13.694 done; TTC: 2 [21102:01] mmap) Connect Scan Thung, About 13.694 done; TTC: 2 [21103:01] mmap) Connect Scan Thung, About 13.694 done; TTC: 2 [21109:01] mmap) Connect Scan Thung, About 13.694 done; TTC: 2 [21109:01] mmap) Connect Scan Thung, About 13.694 done; TTC: 2 [21109:01] mmap) Connect Scan Thung, About 13.694 done; TTC: 2 [21109:01] mmap) <td>51 (0:34:43 remaining) 36 (0:39:13 remaining)</td>	51 (0:34:43 remaining) 36 (0:39:13 remaining)
[21,02:11] map: 1 connect Scan Tailing: About 6.7% done; ETC; 2 [21,02:13] map: 1 connect Scan Tailing: About 7.5% done; ETC; 2 [21,02:14] map: 1 connect Scan Tailing: About 7.5% done; ETC; 2 [21,02:14] map: 1 connect Scan Tailing: About 7.5% done; ETC; 2 [21,02:14] map: 1 connect Scan Tailing: About 7.5% done; ETC; 2 [21,02:14] map: 1 connect Scan Tailing: About 7.5% done; ETC; 2 [21,02:14] map: 1 connect Scan Tailing: About 7.5% done; ETC; 2 [21,02:14] map: 1 connect Scan Tailing: About 7.5% done; ETC; 2 [21,02:14] map: 1 connect Scan Tailing: About 7.5% done; ETC; 2 [21,02:14] map: 1 connect Scan Tailing: About 16.5% done; ETC; 2 [21,07:13] map: 1 connect Scan Tailing: About 16.5% done; ETC; 2 [21,07:13] map: 1 connect Scan Tailing: About 16.5% done; ETC; 2 [21,07:14] map: 1 connect Scan Tailing: About 16.5% done; ETC; 2 [21,07:15] map: 1 connect Scan Tailing: About 16.5% done; ETC; 2 [21,07:16] map: 1 connect Scan Tailing: About 16.5% done; ETC; 2 [21,07:16] map: 1 connect Scan Tailing: About 16.5% done; ETC; 2 [21,10:16] map: 1 connect Scan Tailing: About 16.5% done; ETC; 2 [21,10:16] <t< td=""><td>41 (0:43:21 remaining)</td></t<>	41 (0:43:21 remaining)
12163:11 mmap: Innerecting send setup: for 18.0.18.0.13 12160:11 mmap: Innerecting send setup: for 18.0.18.0.13 12160:14 mmap: Innerecting send setup: for 18.0.18.0.13 12160:14 mmap: Innerecting send setup: for 18.0.18 12160:15 mmap: Innerecting send setup: for 18.0.18 12160:16 mmap: Innerecting send setup: for 18.0.18 12160:17 mmap: Innerectic sen 11.11.18 Moort 18.0.60 12160:18 mmap: Innerectic sen 11.11.18 Moort 18.0.60 12110:18 mmap: Innerectic sen 11.11.18 Moort 18.0.60 12110:18 mmap: Innerectic sen 11.11.18 Moort 18.0.60 1211111:18 mmap: Innerectic sen 11.11.18 <th>44 (0:40:0) (maining)</th>	44 (0:40:0) (maining)
[21] 02:14 mmap: Connect Scan Tianing: About 7.98% done; ETC: 2 [21] 02:14 mmap: Connect Scan Tianing: About 7.98% done; ETC: 2 [21] 02:14 mmap: Connect Scan Tianing: About 7.98% done; ETC: 2 [21] 02:14 mmap: Connect Scan Tianing: About 7.98% done; ETC: 2 [21] 02:14 mmap: Connect Scan Tianing: About 10.64% done; ETC: 2 [21] 02:14 mmap: Connect Scan Tianing: About 10.64% done; ETC: 2 [21] 02:14 mmap: Connect Scan Tianing: About 10.64% done; ETC: 2 [21] 02:15 mmap: Connect Scan Tianing: About 10.54% done; ETC: 2 [21] 02:16 mmap: Connect Scan Tianing: About 10.54% done; ETC: 2 [21] 02:16 mmap: Connect Scan Tianing: About 10.54% done; ETC: 2 [21] 10:951 mmap: Connect Scan Tianing: About 10.54% done; ETC: 2 [21] 10:96 mmap: Connect Scan Tianing: About 10.54% done; ETC: 2 [21] 10:97 mmap: Connect Scan Tianing: About 10.54% done; ETC: 2 [21] 11:96 mmap: Connect Scan Tianing: About 10.64% done; ETC: 2 [21] 11:97 mmap: Connect Scan Tianing: About 10.97% done; ETC: 2 [to 5 due to 15 out of 41 dropped probes since tast increase. 51 (0)51/53 remaining)
121.02:13 mmap: 1 connect Scan Thing: About 9.79 More; ETC: 2 121.02:14 mmap: 1 connect Scan Thing: About 10.64 More; ETC: 2 121.02:14 mmap: 1 connect Scan Thing: About 10.64 More; ETC: 2 121.02:14 mmap: 1 connect Scan Thing: About 10.64 More; ETC: 2 121.02:14 mmap: 1 connect Scan Thing: About 13.64 More; ETC: 2 121.07:14 mmap: 1 connect Scan Thing: About 13.64 More; ETC: 2 121.07:15 mmap: 1 connect Scan Thing: About 13.64 More; ETC: 2 121.07:16 mmap: 1 connect Scan Thing: About 13.64 More; ETC: 2 121.07:17 mmap: 1 connect Scan Thing: About 13.64 More; ETC: 2 121.07:18 mmap: 1 connect Scan Thing: About 18.64 More; ETC: 2 121.07:19 mmap: 1 connect Scan Thing: About 18.64 More; ETC: 2 121.19:51 mmap: 1 connect Scan Thing: About 18.64 More; ETC: 2 121.19:52 mmap: 1 connect Scan Thing: About 18.64 More; ETC: 2 121.19:53 mmap: 1 connect Scan Thing: About 18.64 More; ETC: 2 121.19:53 mmap: 1 connect Scan Thing: About 18.77 More; 18.10.10.10.11 121.19:53 mmap: 1 connect Scan Thing: About 18.77 More; 18.10.10.10.11 121.19:53 mmap: 1 connect Scan Thing: About 2.64 More; ETC: 20.11.11.10.10.13 121.19:53	55 (0:55:02 remaining)
21:00:143 mmapl [Increasing send delay for [0.10.01.31 from 22:00:123 mmapl [Connect Sem Tissing. Adduct 11.586, doine; ETC: 21:00:123 mmapl [Connect Sem Tissing. Adduct 11.586, doine; ETC: 22:00:123 mmapl [Connect Sem Tissing. Adduct 11.586, doine; ETC: 22:00:123 mmapl [Connect Sem Tissing. Adduct 13.696, doine; ETC: 22:00:123 mmapl [Connect Sem Tissing. Adduct 13.695, doine; ETC: 22:10:123 mmapl [Connect Sem Tissing. Adduct 13.695, doine; ETC: 22:11:12:03 mmapl [Connect Sem Tissing. Adduct 18.695, doine; ETC: 22:11:12:04 mmapl [Connect Sem Tissing. Adduct 18.695, doine; ETC: 22:11:12:05 mmapl [Connect Sem Tissing. Adduct 18.695, doine; ETC: 22:11:12:06 mmapl [Connect Sem Tissing. Adduct 18.696, doine; ETC: 22:11:12:07 mmapl [Connect Sem Tissing. Adduct 18.696, doine; ETC: 22:11:12:07 mmapl [Connect Sem Tissing. Adduct 18.696, doine; ETC: 22:11:12:07 mmapl [Connect Sem Tissing. Adduct 18.697, doine; ETC: 22:11:12:07 mmapl [Connect Sem Tissing. Adduct 18.697, doine; ETC: 22:11:12:07 mmapl [Connect Sem Tissing. Adduct 18.697, doine; ETC: 21:12:07 mmapl [Connect Sem Tissing. Adduct 27.697, doine; ETC: 21:16	59 (0:56:05 femaining) 03 (1:01:16 remaining)
121-04-220 mmap:1 Increasing send daily for 10.010.01.011 from 121.07.14 121.07.14 mmap:1 Increasing send daily for 10.01.010.010.0111 from 21.07.14 121.07.14 mmap:1 Increasing send daily for 10.01.010.010.0111 from 21.07.14 121.07.14 mmap:1 Connect Scan Thing: About 15.5% done; ETC: 21.00.01 121.07.15 mmap:1 Connect Scan Thing: About 15.5% done; ETC: 21.01.07 121.07.15 mmap:1 Connect Scan Thing: About 16.5% done; ETC: 21.01.07 121.01.07 mmap:1 Connect Scan Thing: About 16.5% done; ETC: 21.01.07 121.01.07 mmap:1 Connect Scan Thing: About 16.6% done; ETC: 21.01.07 121.01.07 mmap:1 Connect Scan Thing: About 16.6% done; ETC: 21.01.07 121.01.07 mmap:1 Connect Scan Thing: About 18.0% done; ETC: 21.01.07 121.01.07 mmap:1 Connect Scan Thing: About 21.0% done; ETC: 21.01.07 121.01.08 mmap:1 Connect Scan Thing: About 21.0% done; ETC: 21.01.07 121.01.08 mmap:1 Connect Scan Thing: About 21.0% done; ETC: 21.00.07 121.01.08 mmap:1 Connect Scan Thing: About 21.0% done; ETC: 21.01.07	to 10 due to 11 out of 11 dropped probes since last increase.
2 (207-13) map: Incomesting serians/series/s	:12 (1:08:29 remaining)
[21:08:56] mmap2 Connect Scan Thing: About 16.5% Mone; FT:: [21:09:51] mmap2 Connect Scan Thing: About 16.5% Mone; FT:: [21:10:51] mmap2 Connect Scan Thing: About 16.5% Mone; FT:: [21:10:51] mmap2 Connect Scan Thing: About 16.5% Mone; FT:: [21:10:52] mmap2 Connect Scan Thing: About 16.9% Mone; FT:: [21:13:26] mmap2 Connect Scan Thing: About 16.9% Mone; FT:: [21:13:26] mmap2 Connect Scan Thing: About 18.9% Mone; FT:: [21:13:26] mmap2 Connect Scan Thing: About 18.9% Mone; FT:: [21:13:26] mmap2 Connect Scan Thing: About 18.9% Mone; FT:: [21:13:26] mmap2 Connect Scan Thing: About 21.9% done; FT:: [21:16:30] mmap2 Connect Scan Thing: About 21.9% done; FT:: [21:16:30] mmap2 Connect Scan Thing: About 21.9% done; FT:: [21:16:30] mmap2 Connect Scan Thing: About 21.9% done; FT:: [21:16:30] mmap2 Connect Scan Thing: About 21.9% done; FT:: [21:16:30] mmap2 Connect Scan Thing: About 21.9% done; FT:: [21:16:30] mmap2 Connect Scan Thinig: A	to 20 due to 11 out of 11 dropped probes since last increase. :11 (1:04:17 remaining)
221:19:331 mmap: [connect Scan Thaing: About 18.6% does; ETC: 221:13:60 mmap: [connect Scan Thaing: About 18.6% does; ETC: 23:13:60 mmap: [connect Scan Thaing: About 18.6% does; ETC: 24:13:60 mmap: [connect Scan Thaing: About 18.6% does; ETC: 21:13:60 mmap: [connect Scan Thaing: About 18.6% does; ETC: 21:13:63 mmap: [connect Scan Thaing: About 18.6% does; ETC: 21:15:53 mmap: [connect Scan Thaing: About 18.6% does; ETC: 21:15:53 mmap: [connect Scan Thaing: About 18.6% does; ETC: 21:16:30 mmap: [connect Generged Generged 18.6% does; ETC: 21:16:30 mmap: [connect Scan Thaing: About 23.6% does; ETC: 21:16:30 mmap: [connect Scan Thaing: About 27.6% does; ETC: 21:16:30 mmap: [connect Scan Thaing: About 27.6% does; ETC:	1:17 (1:08:10 remaining)
[21111:56] mmap] Connect Scan Thing: About 16.98% Mode; ETC: [2113:36] mmap] Connect Scan Thing: About 16.94% Mode; ETC: [2113:52] map] Connect Scan Thing: About 18.94% Mode; ETC: [2113:52] map] Connect Scan Thing: About 19.7% Mode; ETC: [2113:52] map] Connect Scan Thing: About 39.7% doe; ETC: [2115:24] map] Connect Scan Thing: About 31.7% doe; ETC: [2116:60] map] Connect Scan Thing: About 21.3% doe; ETC: [2116:72] map] Connect Scan Thing: About 21.3% doe; ETC: [2117:01] map] Connect Scan Thing; About 21.5% doe; ETC: [2117:01] map] Connect Scan Thing; About 27.4% doe; ETC:	(122) (112) (mail(11)) (27) (116) (22) (mail(10)) (27) (116) (22) (mail(10))
121:13:261 mmp) [Connect Can Tiang; About 3.0% (More; FC; 21:13:53) 121:15:24 mmp) [Connect Can Tiang; About 3.0% (More; FC; 21:13:53) 121:15:25 mmp) [Connect Can Tiang; About 3.0% (More; FC; 21:13:53) 121:15:26 mmp) [Connect Can Tiang; About 3.0% (More; FC; 21:13:53) 121:15:26 mmp) [Connect Can Tiang; About 3.0% (More; FC; 21:13:53) 121:16:301 mmp) [Connect Can Tiang; About 3.0% (More; FC; 21:17:30) 121:16:301 mmp) [Connect Can Tiang; About 27:0% (More; FC; 21:17:30)	:33 (1:21:25 remaining) '30 (1:26:27 remaining)
 [21:15:24] mmap] Lonnect Scan Tianng: About 19.70% done; EfC: [21:15:26] mmap] Lonnect Scan Tianng: About 21.32% done; EfC: [21:16:06] mmap] Lonnect Scan Tianng: About 21.32% done; EfC: [21:16:06] mmap] Lonnect Scan Tianng: About 23.01% hore; EfC: [21:16:06] mmap] Lonnect Scan Tianng: About 24.04% done; EfC: [21:17:01] mmap] Lonnect Scan Tianng: About 24.04% done; EfC: [21:17:01] mmap] Lonnect Scan Tianng: About 24.49% done; EfC: [21:17:01] mmap] Lonnect Scan Tianng: About 24.04% done; EfC: 	in the second
[21:16:00] mmpl Connect Scan Timing: About 21.32% done; FTC: [21:16:25] mmpl Discovered open port 1027/tc on 10.10.100.13 [21:16:30] mmpl Connect Scan Timing: About 23.0% done; FTC: [21:17:30] mmpl Connect Scan Timing: About 27.45% done; FTC:	:36 (1:21:08 remaining)
<pre>[21:16:25] mmapl [Discovered upper port lbc//tcp on 10.10.100.15 [21:16:30] mmapl [Connect Scan Timing: About 23.01% done; ETC: [21:17:01] mmapl [Connect Scan Timing: About 24.95% done; ETC: [21:17:30] mmapl [Connect Scan Timing: About 27.43% done; ETC:</pre>	
<pre>[21:17:01] nmap1 Connect Scan Timing: About 24.95% done; ETC: [21:17:30] nmap1 Connect Scan Timing: About 27.43% done; ETC: </pre>	:31 (1:15:39 remaining)
(Exit index connect bean finiting, About Eritor doney effer i	:31 (1:15:39 remains) :26 (1:10:17 remaining)
[21:18:03] nmap1 Connect Scan Timing: About 29.55% done; ETC: 3	31 (1:15:39 remaining) 226 (1:10:17 remaining) 21 (1:10:40 remaining)
[21:18:39] nmapl Connect Scan Timing: About 31.69% done; ETC: [21:19:30] nmapl Connect Scan Timing: About 34.28% done; ETC:	231 (1:15:39 remaining) 236 (1:10:17 remaining) 212 (1:04:00 remaining) 125 (0:95:12 remaining) 116 (0:53:6 remaining)
[21:19:53] nmap1 Discovered open port 1026/tcp on 10.10.100.13	131 (115:30 remaining) 226 (110:17 remaining) 21.10:04:07 remaining) 21.10:04:07 remaining) 21.10:05:07 remaining) 20.00:04:07:07 remaining) 20.00:04:07:07 remaining)
[21:20:31] Imapi Connect Scan Timing: About 37.10% done; ETC: . [21:21:19] nmapi Connect Scan Timing: About 40.07% done; ETC: .	31 (1:15:39 remaining) 226 (1:10:17 remaining) 221 (1:04:00 remaining) 131 (0:53:06 remaining) 134 (0:63:01 remaining) 035 (0:64:00 remaining) 036 (0:64:00 remaining)
[21:21:57] nmap1 Connect Scan Timing: About 42.80% done; ETC: [21:22:38] nmap1 Connect Scan Timing: About 45.60% done; ETC:	131 (115:39 remining) 226 (110:17 remining) 210 (10:00) Provide Prov
[21:23:03] nmapl Connect Scan Timing: About 43:50% done; ETC:	11 (115:39 remaining) 126 (110:17 remaining) 121 (10:40 remaining) 131 (0:8117 remaining) 138 (0:8017 remaining) 148 (0:8400 remaining) 148 (0:8400 remaining) 159 (0:8325 remaining) 159 (0:8325 remaining)
[21:23:33] nmap1 Connect Scan Timing: About 51.56% done; ETC: [21:25:42] nmap1 Connect Scan Timing: About 56.12% done; ETC:	11 (115:39 remining) 22 (110:17 remining) 23 (110:17 remining) 11 (013:34 remining) 11 (013:34 remining) 10 (013:34 remining) 10 (013:35 remining) 10 (013:35 remining) 15 (013:3
[21:26:04] nmap1 Discovered open port 49152/tcp on 10.10.100.1	11 (115:30 remaining) 12 (110:17 remaining) 12 (110:10 remaining) 13 (05:01 remaining) 13 (05:01 remaining) 16 (05:02 remaining) 16 (05:02 remaining) 17 (05:02 remaining) 17 (05:02 remaining) 17 (05:02 remaining) 17 (05:02 remaining) 17 (05:02 remaining) 17 (05:02 remaining) 18 (05:02 remaining) 19 (05:02 remaining) 19 (05:02 remaining) 19 (05:02 remaining) 19 (05:02 remaining) 19 (05:02 remaining)
[21:27:27] nmap1 connect Scan Timing: About 60.43% done; ETC: :	11 (115:39 remaining) 22 (1:10:17 remaining) 23 (1:10:17 remaining) 24 (1:10:17 remaining) 25 (1:10:14 remaining) 25 (1:10:14 remaining) 25 (1:10:14 remaining) 25 (1:10:15 remaining)

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



Client Configuration Guide | 11/28/2017

11

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.

E-Corp - Telesploit Mat	+					
(Iocalhost:63015/tele	ploit/channels/e-corp	C Q Search	☆自	÷ ش		=
@telesploit Telesploit	☆ E-Corp v	3 👗 📌 Search			@	
Telesploit CHANNELS Allade Security CHANNELS CHANNELS OPORT-TOPIC OPORT-TOPIC PRIVATE CHANNELS HORE PRIVATE CHANNELS CHANNELS CHANNELS CHANNELS CHANNELS CHANNELS CHANNELS CHANNELS	i E-Cuip v We list has joined the channel. We list has joined the channel.					
					He	p

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

ssh test@relay-d014.telesploit.com

```
support@telesploit:-/demo/telesploit-client/telesploit-d015$ ssh test@relay-d015.telesploit.com
The authenticity of host 'relay-d015.telesploit.com (52.14.156.116)' can't be established.
ECDSA key fingerprint is SHA256:zxnvFixtNVPkdLRvukdrBmFkaLzlzHCn2/VCFkLIZE.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'relay-d015.telesploit.com,52.14.156.116' (ECDSA) to the list of known hosts.
Permission denied (publickey).
```

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

ncat -v --ssl relay-d015.telesploit.com 443

```
support@telesploit:-/demo/telesploit-client/telesploit-d015$ ncat -v --ssl relay-d015.telesploit.com 443
Ncat: Version 7.01 ( https://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.
```

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.

If the tests are successful then verify that the tunnels have been created by running netstat and reviewing the output.

If the tunnels have not been created then the output should look similar to the following depending on what services you have running.

netstat -plnt

	_					
support	@telesplo	it:~/demo/telesploit-cl	ient/telesploit-d015\$ net	tstat -plnt		
(No inf	o could b	e read for "-p": geteui	d()=1001 but you should h	be root.)		
Active	Internet	connections (only serve	ers)			
Proto R	lecv-Q Sen	d-Q Local Address	Foreign Address	State	PID/Program name	
tcp	0	0 127.0.0.1:5141	0.0.0.0:*	LISTEN		
tcp	Θ	0 127.0.1.1:53	0.0.0:*	LISTEN		
tcp	Θ	0 127.0.0.1:631	0.0.0:*	LISTEN		
tcp6	Θ	0 ::1:631	:::*	LISTEN		

If the tunnels have been established then the output should look similar to the following, again depending on what services you have running.

netstat -plnt | sort -k7

_								
sup	port@teles	ploit:	~/demo/te	elesploit-client	/telesploit-d015\$ ne	etstat -plnt so	sort -k7	
(No	t all proc	esses	could be	identified. non	-owned process info			
wi	11 not be	shown	VOU WOUL	d have to be ro	ot to see it all)			
Act	ive Intern	et cor	nections	(only cervers)	or to see it atti,			
ACC.	The Turcein		meccrons	(only servers)				
tcp	0	6) 127.0.0.	1:5141	0.0.0.0:*	LISTEN		
tcp	0	6) 127.0.0.	1:631	0.0.0.0:*	LISTEN		
tcp	Θ	6) 127.0.1.	1:53	0.0.0.0:*	LISTEN		
tcp	6 0	6) ::1:631		:::*	LISTEN		
tcp	0	6	127.0.0.	1:13015	0.0.0.0:* SSH	LISTEN	5339/ssh	
tcp	0	e	127.0.0.	1:23015	0.0.0.0:* VNC	LISTEN	5339/ssh	
tcp	0	e	127.0.0.	1:33015	0.0.0.0:* Squid	LISTEN	5339/ssh	
tcp	0	6	127.0.0.	1:43015	0.0.0.0:* socks	LISTEN	5339/ssh	
tcp	0	6	127.0.0.	1:53015	0.0.0.0:* IRC	LISTEN	5339/ssh	
tcp	0		127.0.0.	1:63015	0.0.0.0:* Mattermost	LISTEN	5339/ssh	
Pro	to Recv-0	Send-() Local Ad	dress	Foreign Address	State	PID/Program name	

If the tunnels have not been established then re-run the script create_tunnels.sh. If the tunnels have been established run the script kill_tunnels.sh followed by create_tunnels.sh to clear any hung connections.

If you receive an error similar to the following after running create_tunnels.sh then the tunnels have already been established.



If you receive an error similar to the following after running kill_tunnels.sh then there are no active tunnels to teardown.



If you are still unable to create SSH tunnels to the relay then run the script kill_tunnels.sh followed by setup_client.sh before once again executing create_tunnels.sh. If this still fails then please contact Telesploit support.