

Forum:[Hack Forums](#)

Thread: [TCP/IP socket client, need some guidance](#)

?E???????d . - October 19, 2015, 11:16 am

Hello ?

I wanted to create a bot to send login/join packets to a game server. So it will join then send more packets for it to write something in the chat, but I'm not sure how to do this. If someone could help me, I'd appreciate it so much! :)

This is the code I got so far:

Code import socket

```
# Create a TCP/IP socket
sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
```

```
# Connect the socket to the port where the server is listening
server_address = ('79.133.198.11x', 23073)
sock.connect(server_address)
```

```
# Trying to send something
PACKET = "Hello World!".encode('utf-8')
sock.send(PACKET)
```

```
# Close connection
sock.close()
```

FYI, the game I picked to try on is "Soldat" a old 2d shooting game. Also, someone told me I could use wireshark or some packet sniffer but I have no clue in what form to put it into the code and how to send it.

Please help me! ?

EDIT: I installed Wireshark and listened to port 23073 while I connected to the server and gave me this data (UDP protocol):

[illegible]

How could I apply that to the code and send that packet to the established connection?

h0lyl337 - November 18, 2015, 4:35 pm

```
try socket.send(packet.pcap)
```

Pentahedron - November 19, 2015, 4:53 pm

You must look at the handshake that is made to initiate a connection. Usually there is a ~4 message

long sequence where the 2 nodes send packets between them to sync (on level 4). For example, in these packets, the username, and a command to login might be sent.

To catch the handshake, setup wireshark and filter all packets that aren't from the game server. Post the pcap file somewhere (and provide a link) so we can analyse it.

Also, this won't be easy :p. the data is encoded and there are predefined symbols/strings that mean things to the server and client that we don't know (yet). When you captured the data you posted, did your username have "Major" or was there any text with "Major" in it?

PM for questions

Pseudonym - November 21, 2015, 6:01 am

UDP is stateless protocol, it doesn't have any handshakes, it doesn't establish connection nor it does close it. I would recommend learn something about UDP before trying to use it.

Feanor - November 22, 2015, 7:14 am

Have you tried making a udp socket? :)

Pentahedron - November 28, 2015, 2:37 am

(Nov 21, 2015 07:01 AM)Pseudonym Wrote: [\[CITE\]](#) UDP is stateless protocol, it doesn't have any handshakes, it doesn't establish connection nor it does close it. I would recommend learn something about UDP before trying to use it.

UDP doesn't have a handshake. Though inside the UDP packet, the application may do a /handshake/ of it's own. After some research I realized the term "/negotiation/" is more accurate.

To prove my point lets look at TFTP. It utilizes UDP, though still has some packets transferred before the real packets with the data are sent. These initial packets negotiate parameters (and other things), but the point is, they must be sent to successfully transfer a file through TFTP.

In conclusion, just because a protocol uses UDP underneath it, doesn't mean it doesn't have some negotiating/handshake packets sent before the real data (on the application layer).