

# Forum:[Hack Forums](#)

Thread: [Simple TCP 'RAT' Using Winsock.](#)

**TerminallyIII** - November 11, 2019, 10:40 pm

Just started learning Winsock and I thought a RAT would be a nice project. The thing is the client does not execute commands like "dir" or "whoami" but will run commands that open processes such as Notepad. Take a look my code: [TCP Client Help - Pastebin.com](#) and please tell me what I'm doing wrong and how I can have this working as intended. Also any pointers on how I can add to this program's functionality would be greatly appreciated. ?

**YouthInAsia** - November 12, 2019, 7:14 am

send and recv don't guarantee to send the full amount also I doubt your command is 2048 bytes so..yah check for that

**HFDone** - November 12, 2019, 7:47 am

you need to send cmd /c and the string command or in the client add it at the beginning of cmd /C Carries out the command specified by string and then terminates  
so send cmd /c dir and it will work

**ModernJS** - November 12, 2019, 10:57 am

I'd say learn C, dump windows, lean mirai source code and see you on the dark side of moon

**YouthInAsia** - November 12, 2019, 6:05 pm

(Nov 12, 2019 11:57 AM)ModernJS Wrote: [\[CITE\]](#) I'd say learn C, dump windows, lean mirai source code and see you on the dark side of moon

Mirai is the most retarded shit ever written. Dump windows? Why? Because it has a better networking model than select/epoll? You're dense

**ModernJS** - November 16, 2019, 11:57 am

(Nov 12, 2019 07:05 PM)YouthInAsia Wrote: [\[CITE\]](#) Mirai is the most retarded Clay Davis ever written. Dump windows? Why? Because it has a better networking model than select/epoll? You're dense

I'm biased yes. But there's no point in messing and understanding private closed source libraries from microsoft. I love open source. Just my 2 cents. You maybe right.

**incognito04** - November 16, 2019, 2:58 pm

Instead of using send and recv to return and run commands use redirected handles. Firstly create your socket using WSASocket. Finally create a command prompt process and redirect it's input, output and stderr to the handle.