

Forum:[Hack Forums](#)

Thread: [How do i make a program wait?](#)

bytespm - March 15, 2025, 2:35 pm

Im currently trying to develop a client program that opens shell and continuously sends commands that comes from server and sends output to the server. its basically a reverse shell but theres gonna be more than 1 computer so i need a client-server architecture. My client program needs to start everytime a computer starts (win10) and waits server input everysecond (if i put input in a while true will it work?). Does anyone know how to do it ? Im open to every kind of tip, thanks!

DramaKing - March 15, 2025, 8:31 pm

I know very little Python, but even I can easily find out that you need to put 'time.sleep(1)' in your loop to have the thread sleep for one second. It's also odd that a client program waits on input from a server.

Control Alt Elite - March 15, 2025, 9:57 pm

Generally speaking if you're taking actions against more than one host, you want to have the connection driven by the client. So I recommend having the client reach out to the server over HTTP and asking some question like "Is there any command for me to execute"? And if the operator did put in a command to execute, the server would reply with that command. This way your communication channel is simplified.

LiNixx - March 15, 2025, 10:43 pm

This is really going to depend on what language you use and how you go about processing the commands, if you are piping the command to cmd then most languages will pause the programs execution, hand off to cmd, and then waits for cmd's execution to stop and return before moving on. If you are doing the processing through your own function then most all languages have a wait() or sleep() function you can use in your code

bytespm - March 16, 2025, 1:58 am

(Mar 15, 2025 09:57 PM)Control Alt Elite Wrote: [\[CITE\]](#) Generally speaking if you're taking actions against more than one host, you want to have the connection driven by the client. So I recommend having the client reach out to the server over HTTP and asking some question like "Is there any command for me to execute"? And if the operator did put in a command to execute, the server would reply with that command. This way your communication channel is simplified.

Thats what i was doing but with raw sockets. I will test the program in my home network, then try http later. But now i have 1 more question, when do you think the client should ask this question? Every second?

Control Alt Elite - March 16, 2025, 9:59 am

Raw sockets are ok, but they get to be a bit complicated when you consider NATing. You can find success going the raw sockets approach, though. You can go every second. That's fine. It's not the stealthiest because of the amount of chatter it'll make - but if you're just practicing, that's fine.

Tha Sneak - March 17, 2025, 9:56 pm

Code import time

```
print("Waiting for 3 seconds...")
time.sleep(3)
```

```
print("Done!")
```

I believe you are talking about delaying execution, correct?

Phantom_NiNja - March 18, 2025, 3:42 am

(Mar 15, 2025 02:35 PM)bytespm Wrote: [\[CITE\]](#) Im currently trying to develop a client program that opens shell and continuously sends commands that comes from server and sends output to the server. its basically a reverse shell but theres gonna be more than 1 computer so i need a client-server architecture. My client program needs to start everytime a computer starts (win10) and waits server input everysecond (if i put input in a while true will it work?). Does anyone know how to do it ? Im open to every kind of tip, thanks!

It depends on what language you're using there's many functions that does this... like sleep(), delay(), wait().

If you don't want to use those you can use while and just have a counter in milliseconds.

However, in a client-server relationship. You wouldn't need to pause. You need to bind your application to an ip address and listen on a specific port.

both software needs to do this. You need to build the system to interrupt the current state and jump to running the commands from the server.

if it's a reverse shell your shell program would have to dial out to a server which means it needs to have either an ip address or a domain name.
and port. The server will have to bind on that specific port and listen for commands.

for the client software to start when the target computer boots. you either need to put it in the startup older for windows 10 or make modifications to registry. It's hard to have this work on systems that computer experts run because they can defeat this process.

hope this helps any.

I would create a function and use a while loop that way you can customize how you want it to work. and you can add in interrupts to it so that while waiting if you get a response from the other side it will stop the waiting function.
process the commands and then go back and restart the waiting function.

bytespm - March 18, 2025, 8:43 am

(Mar 17, 2025 09:56 PM)Tha Sneak Wrote: [\[CITE\]](#) [code]

I believe you are talking about delaying execution, correct?

I got all i need, but thanks ?

(Mar 18, 2025 03:42 AM)Phantom_NiNja Wrote: [\[CITE\]](#) for the client software to start when the target computer boots. you either need to put it in the startup older for windows 10 or make modifications to registry. It's hard to have this work on systems that computer experts run because they can defeat this process.

Then how modern malicious softwares do that ?

bachenbenno - April 4, 2025, 3:48 pm

(Mar 18, 2025 08:43 AM)bytespm Wrote: [\[CITE\]](#) I got all i need, but thanks ?

Then how modern malicious softwares do that ?

Dependent on your programming language i suggest not to invent the reel again.

HTTP listeners always listen asynchronous by separate thread to incoming requests.

Python I would suggest to try aiohttp. It comes with async http listener.

If you want to implement it on your own, create a separate thread waiting for the incoming HTTP context.

Do not block the main thread with some active waiting loops.

Modern malicious software writes to registry, startup folder, task scheduler, windows service, browser plugin to re-start with the computer/browser.

Robert Rouge - April 5, 2025, 8:33 am

(Mar 18, 2025 08:43 AM)bytespm Wrote: [\[CITE\]](#) Then how modern malicious softwares do that ?
hello, suggest learn more before attempt to make malicious softwares.
not saying you no can, just think that you sign up for frustrations and maybe trouble.

learn to use ai and search. here is ai result:

Quote:To add a program to startup programmatically in Python for the current user, you can use the pywin32 package to create a registry entry in the Windows Registry under HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run. Use the run_at_startup_set function to specify the application name and path.
there are multiple ways to add a program to startup.