


## Jerome O

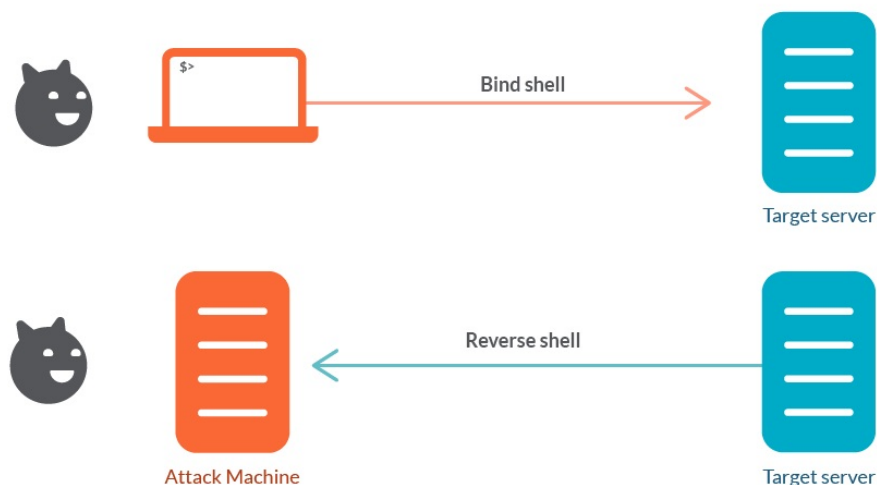


# Reverse shells and Bind shells

 Jerome O 1 day ago · 2 min read

So you've exploited a machine, now what? One of the common things you'd do as a CTF player/pentester is to get access to the machine using a shell.

A shell is basically a way to issue commands on a computer and when you're starting out, they'll come in two flavors: reverse and bind shells. The picture below should explain the main differences.



Picture from → <https://sysdig.com/blog/reverse-shell-falco-sysdig-secure/>

So, when you exploit some remote machine somewhere (with permission of the owner.... You did get permission, right?), you can open up a network connection on the compromised machine and YOU (the attacker) will connect to it. This is a bind shell.

A reverse shell is when YOU (the attacker) set up a network connection your end to "listen" for any incoming connections. When you send your exploit, usually there's a follow-up on what it should do next after compromising the remote machine (that you had permission to exploit...) and typically, it's to connect back to and give you a shell. So it's a reverse shell because instead of you connecting to another machine, \*russian accent\* the machine connects to YOU....

Hope this helped you in some way, this is a super, high-level overview on what reverse and bind shells are. Please make good decisions, kids.

Ctf

Infosec

Cybersecurity