What is a bind shell?

A bind shell is a shell session where the compromised machine opens a listening port and waits for the attacker to connect in, receiving command-line control. It is the opposite direction of a reverse shell. Bind shells are simpler but require the attacker to reach an inbound port on the target, which firewalls and NAT usually block, so they are less common than reverse shells in real engagements except on directly reachable hosts.

HOW IT WORKS

01 How it works and payload

The target opens a listener bound to a shell; the attacker connects:

- Target (listen and serve a shell): `nc -lvnp 4444 -e /bin/bash` (or a `mkfifo` variant where `-e` is unavailable)
- Attacker (connect in): `nc TARGET-IP 4444`
- Windows target: a PowerShell TCP listener that pipes input to `cmd`.

The attacker now has a shell, but only because they could reach port 4444 on the target. Documented techniques shown for defenders.

> NEEDS INBOUND ACCESS
>
> *A bind shell only works if the attacker can reach the target's listening port. Inbound firewall rules usually block this, which is why reverse shells are preferred. Tight ingress filtering defeats bind shells.*

HOW TO DEFEND

- Filter inbound (ingress) traffic so unexpected listening ports are unreachable.
- Use host firewalls to block unsolicited inbound connections to workstations and servers.
- Monitor for processes opening unexpected listening ports, especially shells.
- Use application allow-listing to stop unauthorised tools from running.
- Segment so even a reachable bind shell cannot pivot widely.

SOURCES

[1] MITRE ATT&CK: Lateral Movement (TA0008)

[2] NIST SP 800-115 Technical Guide to Security Testing

[3] Linux man-pages: ssh(1)

Find the lateral-movement paths before an attacker does.

securelayer7.net/learn/lateral-movement/what-is-a-bind-shell

Open online