

# Lateral movement, in plain terms.

Lateral movement is the phase between owning one host and owning the network. This section breaks the execution techniques (PsExec, WMI, WinRM, SMB, DCOM, RDP) and the pivoting building blocks (reverse shells, port forwarding, SOCKS, chisel, ligolo-ng) into plain-language explainers with the real technical names, each ending with how a penetration test surfaces that path in your own environment.

## HOW IT WORKS

### 01 Key terms explained

Plain-language definitions of the techniques behind lateral movement and pivoting. Each page covers what it is, the attack, the payload, and how to defend.

#### Remote execution (Windows)

- What is PsExec?
- What is WMI lateral movement?
- What is WinRM?
- What are SMB admin shares?
- What is DCOM lateral movement?
- What is RDP session hijacking?

#### Shells and pivoting

- What is a reverse shell?
- What is a bind shell?
- What is port forwarding?
- What is SSH tunneling?
- What are SOCKS proxies and proxychains?
- What is chisel?
- What is ligolo-ng?

#### Related (Active Directory)

- Pass-the-Hash
- Pass-the-Ticket

### 02 How to read this section

The pages follow how an attacker actually spreads.

## SOURCES

- [1] MITRE ATT&CK: Lateral Movement (TA0008)
- [2] NIST SP 800-115 Technical Guide to Security Testing
- [3] Microsoft: Administrative shares (C\$, ADMIN\$, IPC\$)

## SecureLayer7

- Foundations first: what lateral movement and pivoting are.
- Remote execution: the Windows methods (PsExec, WMI, WinRM, SMB, DCOM, RDP) for running code on the next host.
- Shells and pivoting: reverse and bind shells, then port forwarding, SSH tunneling, SOCKS, chisel, and ligolo-ng to reach internal networks.
- Related: credential-reuse techniques from the Active Directory section (Pass-the-Hash, Pass-the-Ticket) that power most hops.

Each explainer ends with how a penetration test confirms the path in your own network.

**Find the lateral-movement paths before an attacker does.**

[securelayer7.net/learn/lateral-movement](https://securelayer7.net/learn/lateral-movement)

[Open online](#)