# What is lateral movement?

Lateral movement is the phase where an attacker, having compromised one machine, moves across the network to other hosts to reach valuable systems and credentials. It usually combines stolen credentials (a password, an NTLM hash, or a Kerberos ticket) with a remote-execution method like SMB/PsExec, WMI, WinRM, or RDP. The goal is to repeat compromise host by host until reaching a Domain Controller or the target data. It is mostly built on legitimate administration tools, which is what makes it hard to spot.

## HOW IT WORKS

### 01 How it works: credentials plus execution

Lateral movement almost always has two ingredients:

- A credential: a cleartext password, an NTLM hash (used via Pass-the-Hash), or a Kerberos ticket (used via Pass-the-Ticket).
- A remote-execution method: a way to run commands on the next machine, such as SMB/PsExec, WMI, WinRM, DCOM, or RDP.

The attacker dumps credentials on host A, reuses them to execute on host B, dumps host B for fresher credentials, and repeats. This is the engine that turns one compromise into a domain takeover.

### 02 The common techniques

The remote-execution methods each have their own page:

- PsExec: runs commands via an SMB-created service, often as SYSTEM.
- WMI: executes through Windows Management Instrumentation, no new service.
- WinRM: PowerShell remoting over 5985/5986.
- SMB and admin shares: C$/ADMIN$ for file copy and execution.
- DCOM: execution through Distributed COM objects.
- RDP hijacking: taking over an existing remote-desktop session.

### 03 How a pentest tests for it

## 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$)

A penetration test starts from a single foothold and tries to move across the network exactly as an intruder would, mapping which credentials unlock which hosts and how few hops it takes to reach a Domain Controller. The deliverable is the real path, with the specific credential reuse and execution method behind each hop and a fix for each one.

> WHY IT HIDES
>
> *Lateral movement uses the same tools administrators use (SMB, WMI, WinRM, RDP). The traffic looks legitimate, so detection depends on spotting unusual patterns, not unusual tools.*

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

securelayer7.net/learn/lateral-movement/what-is-lateral-movement

Open online