What is WMI lateral movement?

WMI (Windows Management Instrumentation) is a built-in Windows framework for managing systems locally and remotely. Attackers abuse it for lateral movement because it can execute commands on a remote host (via the `Win32_Process` class) using just valid credentials or an NTLM hash, without creating a service or dropping an obvious binary. Impacket's `wmiexec.py` gives a semi-interactive shell. Because WMI is legitimate management traffic, this technique is quieter than PsExec.

HOW IT WORKS

01 The abuse and payload

With valid credentials or a hash for a local admin on the target, the attacker runs commands via WMI:

- `wmiexec.py corp.local/user:Password1@10.0.0.5` (Impacket, semi-interactive)
- With a stolen hash: `wmiexec.py -hashes :<nt-hash> corp.local/user@10.0.0.5`
- Native PowerShell: `Invoke-WmiMethod -ComputerName 10.0.0.5 -Class Win32_Process -Name Create -ArgumentList "cmd /c ..."`

No service is created and no binary is written to disk in the obvious way, so WMI execution is stealthier than PsExec. Documented techniques shown for defenders.

> QUIETER THAN PSEXEC
>
> *WMI execution does not create a service and leaves a smaller footprint, which is exactly why attackers prefer it when stealth matters. Detection focuses on WMI process-creation events, not service creation.*

HOW TO DEFEND

- Limit local-administrator rights and use LAPS, since WMI execution still needs admin on the target.
- Segment and restrict WMI/DCOM traffic between workstations.
- Reduce NTLM and enforce signing to blunt Pass-the-Hash via WMI.
- Enable WMI activity logging and detect remote `Win32_Process` creation.
- Monitor for one account driving WMI execution across many hosts.

SOURCES

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

[2] Microsoft: Windows Management Instrumentation (WMI)

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

Find the lateral-movement paths before an attacker does.

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

Open online