What is WinRM?

WinRM (Windows Remote Management) is the Microsoft service that powers PowerShell remoting, listening on TCP 5985 (HTTP) or 5986 (HTTPS). Where it is enabled, an attacker with valid credentials (or a usable hash) for a permitted user gets an interactive remote PowerShell session on the target. It is legitimate administration, but a clean and quiet lateral-movement path. The common offensive client is Evil-WinRM, and access usually requires membership in Remote Management Users or local admin.

HOW IT WORKS

01 The abuse and payload

With valid credentials for a permitted account, the attacker opens a remote PowerShell session:

- `evil-winrm -i 10.0.0.5 -u user -p Password1` (interactive PowerShell on the target)
- With a hash where supported: `evil-winrm -i 10.0.0.5 -u user -H <nt-hash>`
- Native: `Enter-PSSession -ComputerName 10.0.0.5 -Credential corp\user`

WinRM gives a clean, fully interactive shell and is a common path on hosts where it is enabled. Documented techniques shown for defenders.

> CHECK 5985/5986
>
> *A reachable WinRM port (5985/5986) plus valid credentials for a member of Remote Management Users or a local admin is a direct lateral-movement path. Restrict who is in that group and where the port is reachable.*

HOW TO DEFEND

- Restrict WinRM reachability with the firewall so only management hosts can reach 5985/5986.
- Limit the Remote Management Users group and local-admin membership.
- Prefer HTTPS (5986) with proper certificates and disable Basic auth.
- Reduce NTLM and enforce strong authentication to blunt hash reuse.
- Monitor for PowerShell remoting sessions and script-block logging on unexpected source-to-destination pairs.

SOURCES

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

[2] Microsoft: Windows Remote Management (WinRM)

[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-winrm

Open online