What is PsExec?

PsExec is a tool that executes commands on a remote Windows machine over SMB (port 445) by uploading a service binary to the ADMIN$ share, creating and starting a service, and relaying input and output over a named pipe. Built as a legitimate Sysinternals admin tool, it is also a favourite lateral-movement technique: with valid credentials or a stolen NTLM hash, an attacker runs commands on another host, frequently as SYSTEM. Impacket's `psexec.py` is the common offensive version.

HOW IT WORKS

01 The abuse and payload

With valid credentials or an NTLM hash for an account that is a local admin on the target, the attacker executes remotely:

- `psexec.py corp.local/user:Password1@10.0.0.5` (Impacket, interactive SYSTEM shell)
- With a stolen hash (Pass-the-Hash): `psexec.py -hashes :<nt-hash> corp.local/user@10.0.0.5`
- Native: `PsExec.exe \\10.0.0.5 -s cmd` (the `-s` runs as SYSTEM)

The attacker now has a shell on the next machine, dumps its credentials, and repeats. Documented techniques shown for defenders.

> NEEDS LOCAL ADMIN
>
> *PsExec requires the account to be a local administrator on the target (to write ADMIN$ and create a service). Limiting who is local admin where directly limits PsExec lateral movement.*

HOW TO DEFEND

- Limit local-administrator rights across the estate; use LAPS so a stolen local-admin hash does not unlock other machines.
- Segment SMB (445) so workstations cannot freely reach each other.
- Enable SMB signing and disable NTLM where possible to blunt Pass-the-Hash.
- Detect service creation by the Service Control Manager from remote sources and PsExec named-pipe patterns.
- Monitor for one account authenticating to many hosts in a short window.

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$)

Find the lateral-movement paths before an attacker does.

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

Open online