What are SMB admin shares?

SMB administrative shares are hidden shares Windows creates automatically on every machine: C$ (the C: drive), ADMIN$ (the Windows folder), and IPC$ (inter-process communication). They exist for remote administration and are accessible to local administrators over SMB (port 445). Attackers abuse them to copy tools, read or plant files, and execute code on remote hosts, the foundation under PsExec and similar tools. With a stolen password or NTLM hash for a local admin, they are a direct lateral-movement path.

HOW IT WORKS

01 The abuse and payload

With local-admin credentials or a hash for the target, the attacker uses the shares to move and execute:

- Browse or copy: `smbclient //10.0.0.5/C$ -U corp/user` or `copy payload.exe \\10.0.0.5\C$\Windows\Temp\`
- Map a share: `net use \\10.0.0.5\ADMIN$ /user:corp\user Password1`
- Execute via SMB without a service: `smbexec.py corp.local/user:Password1@10.0.0.5` (Impacket)
- PsExec and smbexec rely on ADMIN$ and IPC$ to drop and run code.

Documented techniques shown for defenders.

> THE BASE LAYER
>
> *Admin shares are what PsExec, smbexec, and file copy all sit on top of. They require local admin on the target, so limiting local-admin reach limits this entire family.*

HOW TO DEFEND

- Limit local-administrator rights and use LAPS so one stolen hash does not unlock every machine.
- Segment SMB (445) so workstations cannot reach each other's admin shares.
- Enable SMB signing and reduce NTLM to blunt Pass-the-Hash.
- Monitor for access to C$/ADMIN$ from unusual sources and for files written to Windows\Temp via SMB.
- Consider host firewalls blocking inbound 445 except from management hosts.

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-smb-admin-shares

Open online