Null Session - What it is, why it’s risky, and how to disable anonymous access

Gridinsoft Help Center

What it is

A null session is a network connection made without a username or password. On older Windows setups, an anonymous user can connect to special shares like IPC$ to list users, groups, and shared folders or talk to services that use named pipes and RPC.

Why it matters

Even though no files are stolen directly, null sessions give attackers a map of your network - who exists, what shares are open, and where to try passwords next. That reconnaissance speeds up phishing, brute force, and lateral movement.

How it works - quick tour

- Connects to a host’s IPC$ share with blank credentials.
- Uses SMB/RPC to enumerate users, groups, and shares.
- Feeds that intel into password spraying or targeted attacks.

Red flags

- Anonymous or "Anonymous Logon" entries in security logs.
- Unexpected access to IPC$ on servers or desktops.
- Tools that rapidly list accounts and shares from one source IP.

Prevent it

- Disable SMB1 and keep Windows fully updated.
- Set policies to restrict anonymous access to named pipes and shares.
- Limit or remove the IPC$ exposure on hosts that do not need it.
- Use a host-based firewall to allow SMB only from trusted subnets.
- Enforce strong passwords and MFA for admin access.
- Monitor for Event ID 4624 with Logon Type 3 showing Anonymous Logon and alert on repeated hits.