What is persistence?

Persistence is the attacker phase of keeping access to a compromised system over time, so a reboot, a closed vulnerability, or a password change does not end the intrusion. Attackers plant mechanisms that re-run their code automatically, registry run keys, scheduled tasks, services, WMI subscriptions, SSH keys, cron jobs, web shells, and rogue accounts. It maps to MITRE TA0003, and the defense is knowing every autostart location and detecting changes to them.

HOW IT WORKS

01 Where attackers persist

Persistence lives wherever the system auto-runs something:

- Windows: registry run keys, scheduled tasks-, services, the Startup folder, WMI event subscriptions, and accessibility backdoors.
- Linux: SSH authorized_keys, cron jobs, systemd services, and shell profiles.
- Cross-platform: web shells, rootkits, and rogue accounts.

02 Why it matters

Persistence is what turns a momentary compromise into a long-term presence. It is also what makes incident response hard: clean one foothold and the attacker returns through another.

The most durable persistence survives even drastic remediation, a Golden Ticket forged from the krbtgt key keeps working across the whole domain until that key is rotated twice.

> SURVIVE THE RESET
>
> *Persistence is judged by what it survives: a reboot, a patch, a password reset, a reimage. The strongest footholds outlast all of them, which is why eradication must find every one.*

SOURCES

[1] MITRE ATT&CK: Persistence (TA0003)

[2] MITRE ATT&CK: Boot or Logon Autostart Execution (T1547)

[3] NIST SP 800-83 Malware Incident Prevention and Handling

Find the backdoors an attacker would leave behind.
securelayer7.net/learn/persistence/what-is-persistence

Open online