Persistence, in plain terms.

Persistence is how an attacker keeps access after the first compromise, so a reboot or a password reset does not lock them out. This section breaks the Windows mechanisms (registry run keys, scheduled tasks, services, WMI subscriptions), the Linux ones (SSH keys, cron, systemd, shell profiles), and cross-platform backdoors (web shells, rootkits, rogue accounts) into plain-language explainers, each ending with how a penetration test surfaces the foothold in your environment.

HOW IT WORKS

01 Key terms explained

Plain-language definitions of the backdoors and autostart mechanisms attackers use to stay. Each page covers what it is, the technique, the payload, and how to defend.

Windows persistence

- What is a registry run key?
- What is a scheduled task backdoor?
- What is service persistence?
- What is the Startup folder?
- What is a WMI event subscription?
- What is an accessibility backdoor?

Linux persistence

- What is an SSH authorized_keys backdoor?
- What is a cron job backdoor?
- What is a systemd service backdoor?
- What is a malicious shell profile?

Cross-platform

- What is a web shell?
- What is a rootkit?
- What is a rogue account?

Related (Active Directory)

- DCSync, Golden and Silver tickets
- What is krbtgt?

02 How to read this section

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

The pages follow where an attacker hides to keep access.

- Foundations first: persistence and the backdoor.
- Windows persistence: registry run keys, scheduled tasks, services, the Startup folder, WMI event subscriptions, and accessibility backdoors.
- Linux persistence: SSH authorized_keys, cron jobs, systemd services, and shell profiles.
- Cross-platform: web shells, rootkits, and rogue accounts.
- Related: the Active Directory persistence techniques (Golden tickets, krbtgt) that survive even a domain-wide reset.

Each explainer ends with how a penetration test confirms the foothold in your environment.

Find the backdoors an attacker would leave behind.

securelayer7.net/learn/persistence

Open online