Comprehensive Fedora 21 Persistence Detection Playbook

Contents

No table of contents entries found.

This guide walks through all potential persistence mechanisms an attacker could use and how to find and remove them.

---

1. Systemd Exploitation

Check for unauthorized systemd services

- **Look for unexpected services in /etc/systemd/system/ and /usr/lib/systemd/system/**
- **Command: find /etc/systemd/system /usr/lib/systemd/system -type f -name "*.service" -o -name "*.timer"**
- **List enabled services: systemctl list-unit-files --state=enabled**
- **Investigate a specific service: systemctl cat <service-name>**
- **Remediation: Disable and remove malicious services**
  - **systemctl stop <service> (stops the service)**
  - **systemctl disable <service> (prevents it from starting on boot)**
  - **rm /etc/systemd/system/<service>.service (deletes the service file)**
  - **systemctl daemon-reload (refreshes systemd's list)**

Check for malicious systemd timers

- **Attackers may use timers instead of cron for persistence**

- **Command: systemctl list-timers --all (shows active timers)**
- **Investigate a timer: systemctl cat <timer-name>.timer**
- **Remediation: Disable and remove malicious timers**
    - **systemctl stop <timer>**
    - **systemctl disable <timer>**
    - **rm /etc/systemd/system/<timer>.timer**

Check for suspicious PID 1 behavior

- **PID 1 (systemd) should not be acting unusually**
- **Verify that PID 1 is systemd: ls -l /proc/1/exe**
- **Look for errors: journalctl -p err -u systemd -b**
- **Find failed services: systemctl --failed**
- **Remediation: If systemd is not functioning correctly, reinstall it**

---

2. Kernel and Rootkits

Scan for known rootkits

- **Run chkrootkit to scan for common rootkits**
- **Run rkhunter --check to check for malware**
- **Investigate suspicious results in /var/log/rkhunter/rkhunter.log**

Check for suspicious kernel modules

- **List loaded modules: lsmod (check for unfamiliar entries)**
- **Find unusual kernel object files: find /lib/modules/$(uname -r) -type f -name "*.ko"**
- **Get details about a module: modinfo <module-name>**
- **Remediation: Remove a malicious module**
    - **rmmod <module-name> (unloads the module)**

        - **mv /lib/modules/<module-path>.ko /tmp/ (moves it out of the way)**

Look for hidden processes and files

    - **Scan /dev for suspicious files: find /dev -type f**
    - **Check for hidden directories: find /dev -type d -name ".*"**
    - **Run unhide-linux and unhide-tcp to look for hidden processes**
    - **Remediation: If /dev contains non-device files, delete them**

---

3. File System Manipulations

Check for unauthorized cron jobs

    - **List cron jobs: ls -la /etc/cron.* /etc/cron.d /var/spool/cron**
    - **Check root's crontab: crontab -l -u root**
    - **Remediation: Remove unauthorized cron jobs**
        - **crontab -e -u root (edit and remove)**
        - **rm -f /etc/cron.d/malicious**

Look for startup script modifications

    - **Check rc.local: cat /etc/rc.local**
    - **List init scripts: ls -la /etc/init.d/ /etc/rc.d/**
    - **Remediation: Remove malicious entries**

- **Check for immutable files (chattr abuse)**
    - **Find immutable files: lsattr -R /etc /usr /var | grep 'i-'**
    - **Remediation: Remove immutable flag and delete files**
        - **chattr -i /path/to/malicious/file**
        - **rm /path/to/malicious/file**

---

4. Network Configuration Persistence

Check firewall rules and unexpected resets

- **View firewall status: systemctl status iptables**
- **List current iptables rules: iptables -L -n -v**
- **Remediation: Reset and reconfigure iptables**
    - **iptables -F (flush all rules)**
    - **iptables -P INPUT DROP (set a default deny policy)**
    - **systemctl restart iptables**

Check for rogue network services

- **List listening ports: ss -tunlp**
- **Check for unexpected processes: netstat -tulnp**
- **Identify a process running on a port: readlink -f /proc/<PID>/exe**
- **Remediation: Kill rogue processes and delete their files**
    - **kill -9 <PID>**
    - **rm /path/to/malware**

---

5. Userland Persistence

Check for unauthorized users

- **List system users: getent passwd | grep "/bin/bash"**
- **Look for UID 0 (root-level accounts): awk -F: '$3 == 0 {print $1}' /etc/passwd**
- **Remediation: Remove unauthorized users**
    - **userdel -r <malicious-user>**

Check sudoers for backdoor access

- **Validate sudoers file: visudo -c**

- **Check sudoers directory: ls -la /etc/sudoers.d/**
- **Remediation: Edit sudoers with visudo to remove unauthorized access**

Look for unauthorized SSH keys

- **Search for unexpected keys: grep -R "ssh-" /root/.ssh/authorized_keys /home/*/.ssh/authorized_keys**
- **Remediation: Remove suspicious SSH keys**

---

6. Binary and Library Injection

Check /etc/ld.so.preload for rogue libraries

- **View preload file: cat /etc/ld.so.preload**
- **Remediation: Clear the preload file**
  - **> /etc/ld.so.preload**

Check for unauthorized shared libraries

- **List shared libraries: find /lib /usr/lib -type f -name "*.so*"**
- **Verify package integrity: rpm -Va | grep '^..5'**
- **Remediation: Reinstall affected packages**
  - **yum reinstall coreutils**

Check for system binary replacements

- **Scan for altered system binaries: rpm -Va | grep '^..5'**
- **Remediation: Restore legitimate binaries**
  - **yum reinstall <package-name>**

---

7. Log Tampering and Anomaly Detection

Check for audit log tampering

- **Ensure auditd is running: systemctl status auditd**
- **View active audit rules: auditctl -l**
- **Remediation: Restart auditd and reset rules**
  - **systemctl restart auditd**

Check for missing or cleared logs

- **View login history: last**
- **Check for missing logs: ls -lh /var/log/secure**
- **Remediation: Protect logs from tampering**
  - **chattr +a /var/log/secure**

Examine systemd journal for anomalies

- **View recent critical messages: journalctl -xe**
- **Check logs from the previous boot: journalctl -b -1**

---

8. Hardware or Firmware-Level Persistence

Check BIOS/UEFI integrity

- **Get firmware details: fwupdmgr get-devices**
- **List UEFI boot entries: efibootmgr -v**
- **Remediation: Remove suspicious boot entries**
  - **efibootmgr -b <BootNum> -B**

Check ACPI and firmware modifications

- **Dump ACPI tables: acpidump > acpi_tables.txt**
- **Check PCI devices: lspci -vv**