Project Proposal: Multi-Stage Attack on a Linux Server

Jan Büchele
Henrik Lümkemann

April 22, 2025

System Setup

- **Operating System**: Ubuntu 16.04, installed on a local virtual machine (UTM or Parallels)
- **Vulnerable SSH Library**: libssh version prior to 0.8.0
- **Vulnerable Kernel**: A Linux kernel version known to be vulnerable to Dirty Cow

Project Objectives

1. Set up a vulnerable Linux system with known flaws.
2. Demonstrate how these vulnerabilities can be exploited using code or scripts.
3. Apply mitigation strategies *without downloading official patches*.

Selected Vulnerabilities

1. CVE-2018-10933 – libssh Authentication Bypass

- **Component**: libssh
- **Description**: A flaw in the SSH authentication allows attackers to bypass authentication by sending an SSH2_MSG_USERAUTH_SUCCESS message.
- **Impact**: Remote attackers can gain access without valid credentials.
- **Exploitation**: Exploitable using Python scripts.
- **Mitigation ideas (without patch)**:
  - Use keys instead of passwords.
  - Firewall rules to only allow known connections.

2. CVE-2016-5195 – Dirty COW

- **Component**: Linux kernel
- **Description**: A race condition in copy-on-write memory handling allows local users to write to read-only files and escalate privileges.

- **Impact**: Local privilege escalation to root.
- **Exploitation**: Exploitable with C scripts (e.g., overwriting `/etc/passwd`).
- **Mitigation idea (without patch)**:
  - Try to properly enforce access policies.

Note: As we are unsure about the complexity and perceived difficulty of the vulnerabilities, we consider Dirty COW optional. It can be included if the libssh vulnerability is considered too simple (feedback would be appreciated). Then it would be possible to combine both exploits, e.g. get access to system using ssh exploit and then get root priviliges through Dirty COW exploit.

References

- CVE-2016-5195 - Dirty COW
- CVE-2018-10933 - libssh Authentication Bypass