Segurança de Sistemas e Informação
(SEGSI)
PL05
*Jorge Pinto Leite (**JPL**)*
*Pedro Sousa Rodrigues (**DCR**)*
{@isep.ipp.pt}

Exercise 1: Hardening Linux

Hardening Linux systems [1] is extremely difficult in today's networks since there are several misconceptions with non-security people that Linux Systems are secure by design and therefore do not need hardening. This cannot be farther from the truth. Hardening a system, whatever operating system you are using comes with a degree of expertise that often misleads people. All hardening should reflect company policies to a better extent.

1. Run the lynis [2] tool on a standard Ubuntu machine and analyze it's results;
2. Perform the necessary refinements to comply with all requirements reported by the tool;
3. Open the corresponding CIS Benchmark for Ubuntu Servers [3] and perform a gap analysis (what lynis does and what is written in that benchmark);
4. How would you apply the Hardening at Scale?
5. What is Scap benchmark [4]?
6. What is AIDE [5] and what purpose does it fullfil?
7. What are AppArmour [6]/SELinux [7] how can you deploy it and what does it affect users?

Exercise 2: Hardening Windows

Windows is a very permissive system. It is built to work out of the box and requires little to basic operating knowledge. Due to that fact, using such systems in hostile or corporate environments without proper hardening can lead to compromise or data leakage.

1. Gater the CIS BenchMark for Windows 10/11 Workstations [8];
2. Try to implement a complete hardening of yourself;
3. What features would have been removed if you complied with all the improvements?
4. How can you deploy the hardening at scale on Windows-based environments?
5. Install O&O ShutUp [9] and improve your privacy;
6. Perform a Gap Analysis between the CIS benchmark and the O&O Shutup tool;

7. What is AppLocker [10] [11]?
8. Implement a basic AppLocker Policy;
9. Is it a good idea to implement only signed binaries as an AppLocker Policy?
10. Investigate what are LolBAS [12] and reflect on the previous question. Did your threat modeling change?

References

[1] decalage2, "Decalage2/awesome-security-hardening: A collection of awesome security hardening guides, tools and other resources." [Online]. Available: https://github.com/decalage2/awesome-security-hardening

[2] CISOfy, "Lynis - security auditing and hardening tool for linux/unix." [Online]. Available: https://cisofy.com/lynis/

[3] Canonical, "Cis ubuntu linux benchmarks." [Online]. Available: https://www.cisecurity.org/benchmark/ubuntu_linux

[4] I. T. L. Computer Security Division, "Scap content - security content automation protocol: Csrc." [Online]. Available: https://csrc.nist.gov/Projects/Security-Content-Automation-Protocol/SCAP-Content

[5] S. Biradar, "Enhancing linux security with advanced intrusion detection environment (aide)," Jan 2023. [Online]. Available: https://www.redhat.com/sysadmin/linux-security-aide

[6] [Online]. Available: https://apparmor.net/

[7] [Online]. Available: https://selinuxproject.org/page/Main_Page

[8] [Online]. Available: https://www.cisecurity.org/benchmark/microsoft_windows_desktop

[9] oo software, "O&o shutup10++: Free antispy tool for windows 10 and 11," Mar 2023. [Online]. Available: https://www.oo-software.com/en/shutup10

[10] Nsacyber, "Applocker-guidance: Configuration guidance for implementing application whitelisting with applocker." [Online]. Available: https://github.com/nsacyber/AppLocker-Guidance

[11] MotiBa, "Motiba/applocker: Applocker hardening policies." [Online]. Available: https://github.com/MotiBa/AppLocker

[12] [Online]. Available: https://lolbas-project.github.io/