Auditing Tools

Document Name :	Auditing Tools
Version :	1.0
Version Date :	16/07/2022
Modified By :	Marc MARTINEZ
Creation Date :	16/07/2022
Created by :	Marc MARTINEZ
Approved by :	Marc MARTINEZ
Confidentiality Level :	INTERNAL

Modification History

	Date	Author	Commentary
1.0	16/07/2022	Marc MARTINEZ	Creation of the document

Introduction

It’s important to test out the robustness and security of the developped application.

While the angle we chose to approach, pentesting, is mainly focused on confidentiality, this also affect the integrity and disponibility of the systems, once someone manages to get in the systems.

Content

Auditing Process

The Security Team knows severals simples auditing tools that can be useful to detect vulnerabilities or to pen tests the systems.

Most of these tools can be easily accessible by using the linux distribution Kali Linux as they are installed by default on this specific distribution (netstat, hydra, john the ripper,…).

Of course these tools can also be installed on others linux system.

Some tools can also works on windows OS.

It’s the case of wireshark, a network probing tool, that we can use to see what packets are being sent through differents protocols or mediums.

This will help us see if one can easily gather data from the IoT devises by simply listening passively to their communications.

We can also try and see active devises trying to communicate with our devises through that tool.

Back on the linux tools, we can use nestat to try and find open ports on the systems we could try to use for pentesting.

Once a list is made for each system, we can use brute forcing tools like hydra or john the ripper to try and get in. Depending on the lenght and complexity of the passwords and the brute forcing securities (ie : fail2ban), this process can be rather long or even ends up banning the IP of the pentesting machine from the iptables of the tested system. This would result in a positive audit.

If the security teams manage to get in, this would be considered a vulnerability and would need to be patched.

Auditing Documentation

Audits like this must be conducted every sprints during developpement phase of the project. As well as before the delivery of the project.

Audits like this must be conducted every semester once the project is delivered and in production, to keep the security of our systems up to date.

The Security Team is in charge of the security audits.

All audits must be well documented and the vulnerabilities found must be tracked for patching. All documentation regarding the audits and vulnerabilities is to be treated as confidential. The results should however be accessible to the others team members so that the concerned teams can patchs the vulnerabilities.

Tools suggested and required budget

- Kali Linux (free)
- Hydra (free)
- Netstat (free)
- John the Ripper (free)
- Wireshark (free)
- Two (2) days of man hours (1600 €) per audits.