LEI: Segurança Informática e nas Organizações 2020-2021

Project 1: Exploration of Vulnerabilities

Delivery: November 16th, 23:59

1 Description

This work aims to allow students to explore the concepts related with the assessment of vulnerabilities, and to acknowledge the risk and impact of exploring common vulnerabilities.

The objective is for the students to assess the existence of CVEs in a existing host, which mimics a simple web page of an online store. The web page itself, the software installed, and the configurations will have vulnerabilities with various levels of impact.

The web page itself should be vulnerable to issues identified in the classes, and also has a myriad of other issues, which could potentially be exploited by an attacker. As an example, you may find wrong validations, bad authorization processes, bad configurations, bad practices, wrong permissions, dangerous file inclusions, unsafe programs, and many others.

The assignment should be conducted by groups of two students. Everything in the report is expected to be developed by the students, unless clearly stated otherwise. External content without a clear disclaimer or reference will result in a report for plagiarism.

A maximum of 2.5 points will be provided by this assignment. A 10% bonus, may be awarded if the students document multiple ways of completely compromising the host.

2 Preparation

Obtain the virtual machine available at the elearning web page. This file is a **compressed** disk volume with a Debian 64bits linux host. You will net a program supporting the **7Zip** compression format.

Obtain the disk image, create a virtual machine, and add the image as a hard disk.

Add a network interface to the virtual machine. Both `Bridge` and `HostOnly` interfaces can be used. The system will acquire an `IP` address using `DHCP` and no further configuration is required from your part. **DO NOT** use a `NAT` interface as it will not allow you to communicate with the servics.

Start the image, and after some time, the current `IP` address will be presented in the terminal. If you added a `HostOnly` interface, the address should be in the form `192.168.56.1xx`.

Access that address using a web browser and you should get the page of a simple online shop.

3 Work description

The expected deliverable of this assignment is to conduct a simple security assessment to the virtual machine, presenting the findings in a written report. We expect the analysis to contain a **critical** and **personal** view of each finding. Vulnerabilities found should be explored, and the exploration should be detailed.

Any tool can be used, but the report cannot solely consist of screen-shots or textual dumps out of the tools. Besides the findings, the **critical** and **personal** analysis will be evaluated.

Accessing the volume directly is out of the rules of engagement and should not be preformed. All interactions should be taken through the network interfaces.

Tasks to be completed:

1. Enumerate all communication ports available, describing their functionality.
2. Enumerate the operating system, services available, including versions. Describe the function of each service and validate if the information found is coherent (that is, it's really a specific server with that version).
3. Enumerate and describe all potential vulnerabilities containing a CVE Score of at least 7 (`http://cvedetails.com`).
4. Assess if public exploits are able to validate the existence of the vulnerability.
5. Analyze the web page and describe the vulnerabilities found.

6. Explore the vulnerabilities found, describing each step. In the end, describe the potential impact of the exploitation.

4 Useful tools

The following tools may automate some work and facilitate the execution of the assessment. Take in consideration that the systems in the virtual machine have specific protections to some of the tools. If you find this to be true, explore additional arguments made available by the tool.

- `ParrotOS`: A virtual machine with all the following tools pre-installed.
- `Kali`: A virtual machine with all the following tools pre-installed.
- `nmap`: Allows enumeration of communication ports, grabbing banners and execute scripts to validate the enumeration of CVEs (e.g, `--script vulners`)
- `nikto2`: Scans web pages and reports potential problems.
- `sqlmap`: Scans web pages looking for SQL Injection attacks.
- `dirb`: Scans web pages looking for a wide range of files and folders. Allows detecting misconfiguration issues.