Cyber Security Assessment
and Management
Bruno Sousa, bmsousa@dei.uc.pt

Assignment #2
Security Assessment and Improvement

December 18th @ 23:59 (soft deadline)

OBJECTIVE:

Understand the process, advantages, and disadvantages of using automated tools in tasks of security assessment. Apply attack surface analysis in practice. **This assignment can be done individually or in groups of two.** Parts of the exercise are identified as specific for groups of two.

CONTEXT:

The assignment requires the virtual machines available at the following link. You will need to download the virtual machine and install them on your machine:

- **WebServer**, includes a server setup to support a 2-tier web application. This web application is supported by an HTTP server and has a backend database server.
- **Desktop** includes a desktop VM with vulnerabilities.

You will need to download the virtual machine and install them on your machine.

For the webserver check if it is working properly, e.g., by typing in your browser http://192.168.56.7/ (this address may change) and accessing the desktop machine using the interface of the VMs manager.
You should download a Kali Linux VM, which already includes the Metasploit framework to use in the necessary steps. For the assessment you should have a scenario like the one pictured in the figure

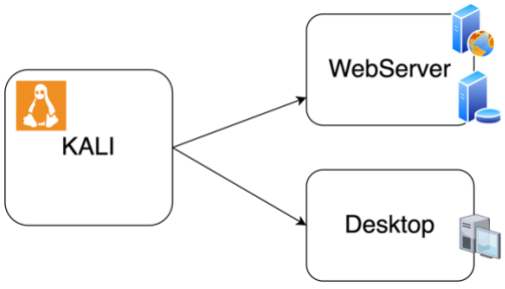

Figure 1 - Assessment Scenario

For groups only: There is also a desktop machine that is used by the staff to access the web application, store files, and send emails. **This machine should be considered during all the steps of the assignment.**

Notice: do not update either of the systems before phase 2 of the assignment!
Notice: The image only work for x86 platforms. For M1 and beyond it will not work! In this case it is recommended to use Metasploit2. There is a video showing how the emulation can be activated. Note that in this case the part 2 needs to be adapted.

***Notice*: If you have issues with M1 and beyond chipset, and the previous step did not solve your issue, please fill out this form, so that resources can be provided to you.**
https://forms.gle/kJEFQq9phWZJAxJw7

EXERCISE:

The exercise includes the following phases, which are detailed next:

0. Information gathering: study the setup provided, and understand the supported web application and desktop machine. Study the tools that may be useful to accomplish the objectives proposed.
1. Security Assessment
2. Security Improvement
3. Security Reassessment

1. Security Assessment

In this phase, you assess the system without modifying, updating, or improving it. Any modification that you consider necessary, should be enumerated in one report that will be the basis of the action in phase 2. The assessment activities are divided into the following four key steps, and should be as much as possible based on automated tools:

a) Measurement of *simplified* attack surface

Take advantage of the provided tools and others that you deem necessary.
Simplified means you should limit your analysis to the variables below using the 'bias' values presented on T05. You should also adjust the bias values where you consider necessary, as these values were originally proposed for Windows OSes.

Open sockets	Open RPC endpoints	Services	Enabled accounts
Open TPC ports	Open named pipes	Services running by default	Enabled accounts in admin group
Open UDP Ports	Dynamic web pages	Services running as SYSTEM	Guest accounts enabled

b) Check the system for outdated software and famous vulnerabilities

Analyze the services and software versions included in the setup and check the system for some of the most recent famous vulnerabilities. Use automated tools to support you in this task.

c) Creation of an exploit for one of the vulnerabilities found in b)

Use the Metasploit framework (or another tool) to help you create an exploit for one of the vulnerabilities you found in **step b)**.

d) Analysis according to CIS Benchmarks

Check how compliant the system is with the CIS Benchmark CIS_Debian_Linux_7_Benchmark_v1.0.0. The document is included in the assignment materials, and you should focus on the recommendations included in points: 3, 4, and 5 **(groups should apply recommendations points 8, 9, and 10 on the desktop machine).**

e) External analysis of the web application

Perform an analysis of the security of the web application available in the Web Server machine. This application is an entry point into the system and can be used to cause harm to it. Document vulnerabilities and demonstrate one method of exploitation for one of them.

2. Security Improvement

Analyze the output of each step of the previous phase and define a set of **a) configuration changes** to perform (including disabling software that does not contribute to the objectives of the system under test (SUT), changing the level of access to the system or part of it, etc.), and **b) security controls** to deploy (includes firewalls, intrusion detection systems, etc.).
Remember that the purpose of the SUT is to support the web application. Therefore, the sole configuration restriction is that the web application continues to be accessible from outside the virtual machine.

3. Security Reassessment

Repeat the measurement of the simplified attack surface, using the same tools and the same procedure that was followed in phase I. Discuss if the obtained results and the potential difference in the results accurately portray the improvement in the system's security.
Discuss how helpful were the tools and benchmarks used.

4. Relevant Information

vms: nuno / qwertyui

DELIVERABLES:

You should deliver a small report including:

- The computations of simplified attack surface;
- All the tasks and commands necessary for each one of the steps of phase 1.
- An enumeration of the security improvements performed in phase 2, and the reasoning behind each one.
- The discussions relative to phase 3.
- The key assumptions and decisions that are not demonstrable in the remaining deliverables.