CT437 Assignment 1

Ethical Hacking and Penetration Testing using Kali Linux and Metasploit

Overview

In this hands-on assignment you will explore the open-source penetration testing tool *Metasploit*, that is widely used by cybersecurity professionals in industry. It is a very versatile tool, which provides you with practical examples of vulnerabilities, exploits, and threat actions (as discussed in the lectures).

This tool, as well as many others, are part of the *Kali-Linux* distribution, which you probably need to download and run in a virtual machine (VM) on your own computer or use Microsoft Azure cloud services (which are available to UoG students for free). Further on, you need to install a target VM (i.e. *Metasploitable 2*), so the entire exercise will take place within a safe sandbox environment.

Alternatively, you can deploy your sandbox environment via docker (i.e. use containers rather than VM), if you are comfortable with this tool. Also, if you have already a Linux laptop, you can install Metasploit directly and just create a target VM.

Apple M* users can't use Virtualbox, but there are various other options (see https://machow2.com/best-virtual-machine-mac/). Alternatively, use Azure cloud services.

While there are plenty of introductory videos about Metasploit on the web, I'd expect you to engage with and critically reflect on your submission, i.e., showing a high level of understanding / domain expertise, both of which being reflected in your presentation and video demo. Note that in many job interviews you are asked security-related questions, so being able to talk proficiently about your project with confidence would help you to pass that hurdle 😊

Problem 1: [2 marks]

Install a Kali Linux VM / container using a hypervisor or cloud-based services and create a user account entailing your full name (i.e., in your subsequent videos an open shell must show your name in the directory path). Further on, install *Metasploitable 2* as your target sandbox.

Problem 1 Marking Scheme

- 2 marks for creating a sandbox environment.
- Note that we cannot mark problem 2, unless we see a personalised account you are using.

Problem 2: [18 marks]

Familiarise yourself with the Metasploit tool. Pick three exploit types of your choice, like for example:

- A buffer overflow exploit
- A backdoor exploit
- An SQL injection exploit
- An ftp exploit

Identify a concrete Metasploit exploit for each of your choices, making sure they are supported by *Metasploitable 2*. For each exploit conduct a pen-testing cycle using *msfconsole* as an interface. Document all steps of your attacks via a presentation and a video (see below).

Deliverables and Marking Scheme:

1. A comprehensive PowerPoint presentation (> 20 slides) that includes an outline of Metasploit, its key features and building blocks (e.g. Tools, Plugins, Libraries, Interfaces and Modules), a summary of the exploits you applied, and a summary of your findings (i.e. experiments and results), and the relevance / importance of the tool.
   Up to 6 marks are awarded for a detailed, well written & structured presentation.
2. A 5 - 10 minutes demo (pre-recorded with voice overlay) where you introduce yourself and showcase Metasploit as well as your experiments. Note that Kali Linux provides a screen recorder.
   Important: It must be evident that you run the tool on your own computer, therefore create an account using your full name that is visible in your video via the bash shell or similar.
   Up to 12 marks are awarded for a comprehensive video where you show and explain all exploits step-by-step, including the used building blocks mentioned above.

Please note:

- Your video must be limited to 250 MB in size.
- Large deliverables (i.e., videos) that cannot be uploaded to Canvas can be submitted via Dropbox or OneDrive link.
- Please use your own hardware for the experiments.
- You can run Kali Linux as VM as follows:
  - Install Oracle VirtualBox (https://www.virtualbox.org/).
  - Import the preconfigured Kali Linux VM (https://www.kali.org/get-kali/#kali-virtual-machines), update it and make a snapshot you can revert too.
  - Install Metasploitable 2 via https://sourceforge.net/projects/metasploitable/files/Metasploitable2/
- VirtualBox may not work in the presence of Windows' Hyper-V. If you run into problems, please look up instructions on how to disable this hypervisor.