ECE/CS230 - Computer Systems Security @KAUST
Fall 2023

TA: Rana Alahmadi

Assignment 5

Submit your solutions as a .zip file at blackboard.kaust.edu.sa.
Include your **full name** in the submitted files.
Name the solutions folder as **x**-A5.zip, where **x** is your **last name**.

Preliminaries: Read about Metasploit and privilege escalation:

- https://www.csoonline.com/article/3379117/what-is-metasploit-and-how-to-use-this-popular-hacking-tool.html
- https://www.offensive-security.com/metasploit-unleashed/payloads/
- https://en.wikipedia.org/wiki/Privilege_escalation

Lab Objectives: The goal of this lab is for the student to learn to use the popular pentesting tools Kali Linux and Metasploit, train themselves to conduct documented attacks against known vulnerabilities, and write a report on such attacks. The student will also learn about how to use multiple attacks to conduct privilege escalation.

Lab deliverables: The student must submit a zip file containing two subfolders (a4/problem1/ and a4/problem2/).

- a4/problem1/ should contain the answers for the first problem (.pdf or .html, plus any additional file).
- a4/problem2/ should contain a script containing the attack, a text document (.pdf or .txt) describing the CVEs used and the attack, and optionally additional scripts that are called by the attack.

Lab preliminaries: For this lab, the students are expected to install a VM (e.g., through Virtualbox) running Kali Linux, a Debian-based distribution aimed at advanced penetration testing and security auditing.

In addition, the students will also be required to install Metasploitable, an intentionally vulnerable Linux virtual machine that can be used to conduct security training, test security tools, and practice common penetration techniques. The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development. Its best-known sub-project is the open source Metasploit Framework, a tool for developing and executing exploit code against a remote target machine. Other important sub-projects include the Opcode Database, shellcode archive and related research.

It is assumed that students will be able to install and connect those VMs by referring to online documentation. However, specific office hours will be reserved to help with issues regarding the installation of Virtualbox or VMs in preparation of this lab.

We provide VirtualBox images for Kali Linux and Metasploitable 2. The default credentials (username/password) are ***kali/kali*** and ***msfadmin/msfadmin***, respectively. The images for Kali and Metasploitable can be download from the course website link below under assignment 5:

https://sites.google.com/view/ececs230kaust/assignments

Problem 1 (50 points): The student must exploit and document the vulnerability CVE-2004-2687.

Distcc is a program to distribute builds of C, C++, Objective C or Objective C++ code across several machines on a network. distcc should always generate the same results as a local build, is simple to install and use, and is usually much faster than a local compile. distcc 2.x, as used in XCode 1.5 and others, when not configured to restrict access to the server port, allows remote attackers to execute arbitrary commands via compilation jobs, which are executed by the server without authorization checks. distcc does not perform any authentication or authorization of connections, and instead relies on third party access controls. It is possible that the flaw may allow arbitrary command execution resulting in a loss of integrity.

For this problem, the student must run Kali Linux and Metasploitable VMs, and demonstrate how to run the distccd exploit. The explanation should take the form of a demonstration, illustrating every step of the attack, *as if writing a report or blog post*.

In particular, pay attention to the following:

- The demonstration should include every step of the attack, and start at login on Kali and Metasploitable (VM installation can be omitted). The attack itself must start with extracting the IP of the vulnerable VM (e.g., using ifconfig) and running a port scan using the nmap tool.
- The demonstration should be complete and comprehensive. Consider that the target audience has the same level as other students in the class, but have no experience in using Metasploit.
- The demonstration should include screenshots of the various steps, highlighting the important information (e.g., which command is being run or what information to pay attention to in the output).

The demonstration can take either the form of a report (continuous text), slides, or a blog post. It can be submitted in PDF (report/slides) or html format. Either way, the demonstration must include both a text description, and screenshots of the attack.

The grading will be based on the following criteria:

1) The attack was conducted successfully, as shown by the screenshots (20 points)

2) No step is missing for replicating the attack (15 points)
3) The demonstration includes comprehensive explanations of each step, appropriate for a target audience similar to the other students taking this course (15 points)

Hint: Students are encouraged to follow online tutorials to complete this assignment. Several websites can help you get started with setting up your VM environment and using Metasploit. Remember that the submitted demonstration and screenshots must be strictly yours.

If you are lost, try to follow those steps:

- Install and run Virtualbox
- Create and start a new VM for Kali Linux
- Create and start a new VM for Metasploitable
- Find the IP of the target VM with ifconfig
- Scan the victim with nmap
- Start Metasploit with msfconsole
- Search and run the distccd exploit
- Verify that you are in (e.g., by running whoami)

Problem 2 (50 points): Using Kali Linux and Metasploitable, run a two-steps attack including code injection and privilege escalation to alter a vulnerable machine.

For this problem, the student should find two known vulnerabilities (that must be present in Metasploitable) to:

1) Gain access to the victim VM via code injection, i.e., become able to run commands on the target machine. This access *must* be unprivileged.
2) Use another vulnerability to perform privilege escalation and gain root access on the target machine.
3) Create the file /root/you_are_pwned in the root-only folder /root, which must contain the text "cs230 1337 haxx0r". The attack should not otherwise change the directory structure or filesystem permissions (i.e., other than the required file, the attack should not leave any trace; changing the permissions, then restoring them to the original state during cleanup is permissible).

The deliverable for this part of the assignment is a script, which can run on a stock version of Kali Linux, and will perform all the steps of the attack and create the required file. The script can be in any language you want (as it must run on a clean slate version of Kali, remember to install any dependencies at the beginning of the script). If you are unsure, we recommend using Bash and/or Python.

This script should be entirely automated except for environment parameters (e.g., the IP of the target machine). Include as a comment, near the top, how the script should be called from the CLI (e.g. $ ./attack 192.168.1.1).

In addition, you should also include a text document giving the name and a brief (1-2 paragraphs) description of the two CVEs that you exploited, as well as a short description of all the steps in the attack.

Note: Describing the CVEs is part of the assignment; the second part of this document will let you get a partial grade if your script fails to run or does not meet the requirements.

The grading will depend on how completely the assignment was fulfilled:

1) Selected two CVEs, present in Metasploitable, to perform code injection and privilege escalation, but did not build them into a complete attack (10 points out of 50).
2) The attack was built properly and completely (and is described in the text document deliverable), but does not work (20 points out of 50).
3) The attack was built and implemented properly, but the script needs tweaks or fixes to run on stock Kali Linux (35 points out of 50).
4) The attack was built properly, the script runs and completes the assignment (45 points out of 50)
5) Same as above, and the attack leaves no trace (filesystem permissions, additional files…) (50 points out of 50)