Operating Systems Security – Assignment 6

2017/2018
Due Date: 11 Jan 2018 (23:59 CET)

Institute for Computing and Information Sciences,
Radboud University, The Netherlands.

1 Capture the Flag

This last assignment is a capture-the-flag exercise. We set up a vulnerable server and your task is it to find and exploit the vulnerabilities on that server. In this exercise sheet you find only very minimal information, but throughout the next weeks we will send e-mail with more and more hints. Obviously you can also ignore those hints and keep playing on level "hard". To find out about the vulnerabilities and how to exploit them, Google will prove very useful.

1.1 Basic information

The server is reachable at `http://ossec-host.cs.ru.nl` and is running an http service on port 80.

1.2 Submission information

In your submission, please do not only give the content of the flags, but describe in detail how you obtained it.

1.3 Get a shell

Your first task is to get a shell on this server. Once you have obtained a shell on the server, you should look through the filesystem for a file called flag1; the content of this file is your first target. You will find the content "encrypted" with the TOPKEK cipher, so to finalize this first stage, you will need some cryptanalysis. **In the same directory as flag1, you will find the username and password that you can use to connect over SSH with.**
Note: You will find the program `curl` very useful when interacting with the web- server from the command line.

1.4 Become root

The system that you obtained a shell on is not kept very up-to-date and has a vulnerability that allows you to escalate your privileges and become root. Find out what part of the system is vulnerable, find a suitable exploit for the vulnerability and become root. Once you have a root shell, you have access to the second flag, a piece of text hidden inside 25MB of gibberish in a file in the `/root` directory. To extract the flag from the gibberish it probably makes sense to write a small program.

Hint: Typical privilege-escalation vulnerabilities are in setuid-root programs or in the kernel.

Hint: You may find `https://www.exploit-db.com` helpful.