NS Lab 2C - Heartbleed

Hao Zhu (h.zhu@uva.nl)
Rex Valkering (rexvalkering@gmail.com)
Sam Ansmink (sam.ansmink@student.uva.nl)
Koen Koning (koenkoning@gmail.com)

Hand-in time (submit to blackboard) by November 13 11:59CET
Total points: 10

Abstract
This assignment is about security. You will exploit the Heartbleed security bug on a vulnerable web server.

This lab must be done individually.

Preparation

For this assignment you must use Python 2.x. It is already installed on the lab computers; otherwise you can download it from http://www.python.org. If you do not know Python, learn it. It is a very simple language.

You can find examples on socket programming in Python in your textbook, section 2.6.

Socket module documentation: http://docs.python.org/library/socket.html

About Heartbleed

Heartbleed is a security bug that was discovered in April 2014 in the OpenSSL library, which is a widely used TLS implementation. TLS is a cryptographic protocol used to provide secure connections over the internet, for example to access web mail or online banking.

The bug that Heartbleed exploits involves the “heartbeat” mechanism, which is used to keep a connection alive by periodically sending a “heartbeat” message. The heartbeat message contains a payload and a payload length that must be echoed by the recipient. However, in the OpenSSL implementation the payload length was never checked to be correct, causing OpenSSL to read data beyond the buffer where the message was stored and sending that back to the client (this is called a “buffer overread”). This allows any client to read random data from the server, which potentially includes passwords, session keys, and so on from other clients.

Although the Heartbleed bug was patched by the time it was publically announced, it was introduced two years before it was discovered. It is entirely possible malicious entities such as criminal hackers or government agencies had already discovered it and made use of it. Heartbleed is a very serious bug, and very easy to exploit.

More detailed explanation of Heartbleed: http://blog.cryptographyengineering.com/2014/04/attack-of-week-openssl-heartbleed.html

TLS Heartbeat protocol: http://tools.ietf.org/html/rfc6520

Submission

Submit you working code in the following files:

- lab2c-<yourname>.py (script)
- lab2c-<yourname>.txt (results)

Where <yourname> is <last name plus first letter of first name>, for example lab2c-koningk.

You must also write your full name and student number at the top of the files (in comments).

Task – Session Hijacking (10 pts)

There is a vulnerable HTTPS web server running at https://145.100.132.31:9876. Your task is use the Heartbleed exploit to hijack the sessions of other clients accessing the website (the clients and sessions are simulated).

The script **lab2c-<yourname>.py** implements the Heartbleed exploit. It is a slightly modified version of a Heartbleed proof-of-concept which you can find online. It will do one heartbeat and output the resulting raw data. Modify it to intercept HTTP requests and find as much as you can. Write down everything interesting you discover in **lab2c-<yourname>.txt** and hand it in, together with your modified script.

Discovering useful information with Heartbleed is like finding needles in a haystack, so be smart about how you are going to approach the problem.