Extra Credit Homework
CS 642: Information Security

December 10, 2014

This homework assignment is for extra credit. It can only make your grade go up, and you can turn in as much as you finish and still get bonus points (assuming the finished portions are correct). You *may not* work with a partner. It is due **Dec 18, 2014** by midnight local time.

1 ShellShock

Shellshock, also known as Bashdoor, is a Unix Bash vulnerability that was made public in September 2014. The bug affected a large number of Internet services since it allowed attackers to remotely execute arbitrary commands in vulnerable versions of Bash.

In this problem, you need to finish the following tasks:

- (Description) You should read materials about the Shellshock bug and what the error was in the source code of BASH. Provide a brief description (at most a few paragraphs) explaining the vulnerability and describe how to fix the bug.
- (Impact) Security experts said that exploits against ShellShock were used to generate Botnets and trigger DDoS attacks. Provide a brief description of how that might work, given your knowledge of the vulnerability.
- (Tester) You should write a script that tests whether a BASH environment is vulnerable. Provide the script and explain the details of your code (in a separate text file).

2 Heartbleed

The Heartbleed bug, an OpenSSL encryption flaw, was made public in April 2014. The bug had huge consequences, as the vulnerable software was used widely among website servers. Millions of servers were in danger of information leaks. Heartbleed allows hackers to remotely retrieve swathes of process memory from the openssl process. Although the retrieved chunk of memory is only up to 64 KB each time, it can be exploited repeatedly to attempt to obtain different memory chunks. The attacker exploits this by sending malformed heartbeat requests to the server

2.1 Environment Setup

For this problem, you are going to use a VirtualBox virtual machine for development and test. Set up Boxes on your own machine: Download the Heartbleed virtual machine tarball, heartbleed.tar.bz2 (approximately 400 MB). Decompress this tarball and import it using VirtualBox, as you did for the previous projects. This virtual machine contains an Ubuntu 12.04(LTS) system with a vulnerable openssl version. Once the HeartBleed VM is running, you can login to the ubuntu unity desktop using user “user”. There are two users in the system: “root” with password “root” and “user” with password “user”. You cannot simply login as a ”root”, so it is suggested to do all the root actions using “sudo”. There is an apache server running under the VM using address localhost (127.0.0.1) and its SSL connection (port 443) is open. If you have trouble running the VM image, email the TA for support.

2.2 Exploit Requirements

In this problem, you need to finish the following tasks:

1. (Description) First you should read up on the Heartbleed bug and what happens in the bug source code of OpenSSL. Provide a brief description (at most a few paragraphs) clearly explaining the vulnerability, including where it arises in the OpenSSL code base. Describe how to fix the bug.
2. (Exploitation) Write a script (Python/bash) or program (C/Java) to extract memory contents from the local vulnerable web server. You must dump at least 64 KB each time. The output format should be a hex dump of the 64 KB buffer.

3 Deliverables

The deliverables should contain your codes for the programming parts and a single TXT or PDF file with the writeup for all explanation parts. The TA will grade by reading your code and supplemental file as well as running your code against the vulnerable server a couple of times.

4 Supplemental Materials

Here are some materials for Shellshock:

- https://shellshocker.net/
- http://en.wikipedia.org/wiki/Shellshock_(software_bug)
- http://www.csoonline.com/article/2839054/vulnerabilities/report-criminals-use-shellshock-against-mail-servers-to-build-botnet.html

Here are some materials for Heartbleed:

- http://heartbleed.com/
- http://en.wikipedia.org/wiki/Heartbleed
- http://arstechnica.com/security/2014/04/how-i-used-heartbleed-to-steal-a-sites-private-crypto-key/

You may use exploit code you find on the Internet to help understand the vulnerability, but do *not* plagiarize exploit code or scripts. If in doubt ask the TA or instructor for permission before using any source you are unsure about.

There are still many vulnerable servers on the Internet. Do not run your exploit code against any server other than the local VM or other systems that you own. Running it against another user’s system could be considered a crime.

5 Grading

Each part is worth up to 2 points. Partial credit for the coding tasks will be given if code fails but a good description is given. If the code works and the description is comprehensive, then one will receive full credit.