Project 2: Exploitation

Date: 4/2/2019

Group 2:

Gael Sanchez

Jacob Gibson

Johannes Schneemann

Rogelio Garza

Zachary Golla

Section I (Introduction) (10%)

Summarize what you have done in the project and clearly state the responsibility of each group member, e.g. who did which task, who wrote which part of the report, how your group was coordinated, etc.

Section II (Task II) (15%)

a) Show whether or not you can read the files in /root/files of Computer B.2 with local login and SSH login.

Used command cd /root/files response: permission denied

b) Find and report exactly how many bytes are needed to crash the echo service.

c) Show which user ID is running the echo service in Computer B.2.

d) Show which user ID is running the SSH service in Computer B.2.

Section III (Task III) (30%)

a) Show that the echo service can be exploited by the provided shell code.

b) Show the exploiting packet captured in Computer A.B.

c) Report how you retrieve the files from Computer B.2 to Computer A.B. Give steps in details.

d) Show the content of the smallest file in the retrieved files.

e) Show the injected SQL statement.

f) Show the screenshot of the web page that show all user IDs, first names, and last names.

Section IV (Task IV) (15%)

a) Discuss the reason that randomization can defeat the attack.

b) Assume only the low 16 bits of the stack address is randomized. What is the probability that an exploiting packet can compromise the server? Assume an attacker can send 10 exploiting packets every second. How long can the attacker compromise the server?

c) Discuss the reason that exec-shield can defeat the attack.

d) Discuss if exec-shield prevents stack overflow. If not, what attack can be achieved?

End of Report

Task I: Setup the network

1) Check that all devices are wired according to Figure 1 (at the end of this document).

Done

2) Check that the NICs of Computer A.B, B.1, and B.2 are configured according to Figure 1.

Done

3) Login to your user account in Computer B.2 and start the echo service(run the command "/root/echoserver/tcps" in a terminal and keep the terminal open).

Note that only B.2 has this service to be exploited. The service is not a daemon. You shall restart the service whenever you reboot the computer or relogin.

Done Response: blinking cursor not sure if actually started

4) Make sure the SSH service and the **Metasploit2** VM are started in Computer B.2.

Don't know where the metasploit vm is

5) Configure the Firewall B using Cisco Configuration Professional such that outside computers can access (a) the echo service (port 30000) and the web service (80) and the SSH service (port 22) of the internal servers, and (b) the SSH service (port 22) of the internal workstations.

Done

Task II: Test the services

1) Login to your user account in Computer B.2. Check whether you can read any file in the directory /root/files.

Done Response: Permission denied

2) After start the echo service in Computer B.2, find the user ID associated with the service process. (Note that you shall start the service as a regular user. Do not use the root account to start the service.)

Using the top command and sorting by user with " u User02" tcps is running as User02

3) Login to your user account in Computer A.B,

3.1) Connect to the echo service in Computer B.2, and check whether the echo service running smoothly with various inputs, for example, inputs of fewer than 8 bytes and inputs of more than 10 bytes.

3.2) Connect to the SSH service in Computer B.2, and check whether you can read any file in the directory /root/files.

3.3) Browse the Metasploit2 VM in Computer B.2, open the DVWA website, and login with admin/password.

Task III: Exploit the service

DO NOT change anything in /root of B.2.

Make your own programs and tests in A.B or B.1 before launching exploitation against B.2.

III.A: Exploit the echo service

1) Make an exploiting program to exploit the echo service from Computer A.B.

The provided source code tcps.c and tcph.c are the source code of the echo server for you to find the vulnerability.

The provided source code tcpc.c and attack.c are for your reference only. You need to make your own programs based on them.

2) Find the files in /root/files in Computer B.2.

3) Retrieve the files to Computer A.B. (Do not assume the files are text files, although they are text files. You shall find a method to transfer the files from B.2 to A.B.)

III.B: Exploit the DVWA website.

1) Go to “DVWA Security” on the left pannel, set the Script Security to medium.

2) Go to “SQL Injection” on the left pannel, read the source code by click “view source” at the bottom-right.

3) Inject SQL statements to obtain all user ids, first names and last names. (Hint: use union and select sql statements)

Task IV: Defend the echo service

Two defense mechanisms have been implemented in Linux. One mechanism randomizes the address space of stack memory (so called randomization). The other mechanism disables execute permission in the stack memory (so called exec-shield).

Four shell scripts are provided to enable or disable the two defense mechanisms: enablerandom.sh, disablerandom.sh, enableexe.sh, and disableexe.sh. When execute the scripts, you need to provide the root password.

1) Enable the randomization mechanism to test if the exploitation can work. Disable it after the test.

2) Enable the exec-shield mechanism to test if the exploitation can work. Disable it after the test.