Assignment

Due: 11:55 pm 12 Aug 2025
Total Mark: 100 (30% of Final Mark)

General Instructions: Please read the following instructions carefully.

- You must create a folder for each question. – Create folders named as Q1,…,Q4.
- Your Python source codes or text, doc files for each question must be saved in the folder you have created.
- You must install a VirtualBox on your laptop or desktop. In the VirtualBox, you must have at least Kali, Ubuntu and Metasploitable2 virtual machines.
- **You must use tools and Python modules specified in each question.**

Important note*: You should submit your Python source code with brief readme files (for explaining how to run your program). Not doing so could result in a 20% reduction in the marks.*

1. Writing ARP Spoofer (20 marks)

   In this task, you will write a Python program that allows you to perform an ARP spoofing attack with a single command as follows:

   ```
   sudo python3 arpspoof.py <Victim_IP> <Router_IP>
   ```

   Your program must use the scapy package. (Do not use subprocess to call linux commands or other tools.) Also you can use the sys module to take user input arguments (<Victim_IP> and <Router_IP>). Your program must present a successful arp spoofing attack on Metasploitable2 (Meta 2) VM (victim) when the program is run on Kali VM (attacker).

   Hint: Visit the Scapy document page https://scapy.readthedocs.io/en/latest/ and search for arp.

2. Writing Cookie Stealer (30 marks)

   In this task, you will write a Python program to steal a cookie when a web site vulnerable to XSS reflected is injected by a Javascript code to send the website user's session cookie to the attacker's server. As usual, the attacker's server is Kali VM and the vulnerable website is Meta2 VM's DVWA, which you can access at http://<Meta2 IP>/DVWA from Kali VM. Set the DVMA security to "minimum".

   To store the stolen cookies in the Kali VM (server), you must use a lightweight Python web application framework called **Flask**. To use Flask, you first need to install python3-venv (venv = virtual environment) package on you your Kali VM. First, check your python3 version on Kali VM: python3 --version. If it is not version 3.12, you need to upgrade yours to Python 3.12: sudo apt install python3. After this, run sudo apt install python3.12-venv on the terminal.

Once the venv is installed, set up the Flask environment, referring to the following web page https://flask.palletsprojects.com/en/3.0.x/installation/#python-version (Read it carefully. You can use the same folder name "myproject" to do your task.)
You now 1) write a Python code importing the Flask module to receive a current session cookie from the victim (Meta2 VM) and 2) a Javascript code that needs to be put into the field "What's your name"of "XSS reflected" on DVWA. (Remember the DVWA security setting should be "medium".) The stolen cookies shouldhave a time stamp (use Python datetime module) be saved in a file called "cookies.txt" on Kali VM.

Summing up, your submission should be the Python code (25 marks) to perform 1) and 2) the Javascript code (5 marks) that should be inserted in the XSS reflected field. (Please save this code snippet in a text file.)

Hints

- You can also refer to User's Guide and API Reference on the left panel of the Flask page: https://flask.palletsprojects.com/en/3.0.x/# Focus on "request.args" and "redirect".
- For the Javascript code injection, refer to our lecture slides for Week 8 on XSS.

3. Writing ransomware (20 marks)

In this question, your task is to implement a simple ransomware using Python. (We learned the concept.) The assumption is the following: 1) An attacker breaks into a victim's machine that has OpenSSL installed (For compatibility, use Kali VM.); 2) the attacker put her public key in the victim's machine; 3) the victim has a file named my_secrets.txt in his root directory (You can write anything in my_secrets.txt.); 4) all the formats for ciphertext outputs should be base64 (human readable).

The ransomware should perform the following:

1) It randomly generates a 16-byte (128-bit) key for symmetric encryption and saves it to a file named key.txt. To generate a key you must use openssl rand –base64 16.
2) It also need to generate a public/private key pair (for the attacker).
3) Then it encrypts the file my_secrets.txt using the key that the attacker selected in step 1). We call this ciphertext data_cipher.txt.

4) The file key.txt will be encrypted using the attacker's public key generated in step 2)- We call this key_cipher.txt. (Remember the format of the resulting ciphertext should be base64.)
5) The file key.txt will be deleted.
6) The file my_secrets.txt will be deleted
7) It will finally display a message for ransom payment: "Your file important.txt is encrypted. To decrypt it, you need to pay me $1,000 and send key_cipher.txt to me."

Write a Python program that does the above steps. You can use subprocess and/or sys modules to do this task.

4. Gift voucher code cracking (30 marks)

**This is a CTF (Capture-The-Flag) style task. You need to submit a (instead of program codes) report in Word format for this task.

An online shopping retailer runs a server to generate gift voucher codes for customers. More specifically, 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 (weak one!) 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 running ./executable_server on the terminal. (You need to make the file executable. *If you use VMs on UTM, download* executable_server2) Then, use an appropriate tool you learned in CSCI369 to identify the open port between 12345 and 12500 for this service. (Note that the service is based on UDP, so you need to find a right option for that scanning. This option was not covered explicitly, but you can find it easily.) (5 marks)
b) Assume that you use your 7-digit UOW student number as a client ID. Based on the port identified from a), use a netcat command to obtain a gift voucher code for your client ID (i.e. your UOW student ID). (5 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||ClientID||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 Hashcat (**https://hashcat.net/hashcat/**) and Crunch (**https://www.kali.org/tools/crunch/**) tools** (both are available on Kali)**, 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 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 UOW student number, e.g. 5284611. 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.