Homework #5

Due Time: 2019/5/19 (Sun.) 22:00
Contact TAs: `vegetable@csie.ntu.edu.tw`

Submission

- Put all answers **in one single PDF file** named **[studentID].pdf**, in the same order as the problem sheet. Do not repeat problem descriptions, just organize them by problem number in a tidy manner.
- Put all required files including `prob1-d.pcapng`, `prob2-b.*`, `prob4-a.pkt`, `prob4-b.pkt`, `prob4-c.pkt`, `sha1-1.pdf`, and `sha1-2.pdf` into a folder named **HW5-[studentID]/**, and compress the folder into a zip file named **[studentID].zip**.
- Submit 2 files on NTU COOL (`https://cool.ntu.edu.tw`):
  - The **[studentID].pdf** file to section **Homework 5**.
  - The **[studentID].zip** file to section **Homework 5 - Codes and other files**.

Instructions and Announcements

- Discussions with others are encouraged. However, you should write down your solutions **in your own words**. In addition, for **each and every** problem you have to specify the references (the URL of the web page you consulted or the people you discussed with) on the first page of your solution to that problem.
- Problems below will be related to the materials taught in the class and may be far beyond that. Try to search for additional information on the Internet and give a reasonable answer.
- Some problems below may not have standard solutions. We will give you the points if your answer is followed by reasonable explanations.
- It is highly suggested to **start your work early** since this homework set might be more difficult than previous ones.
- **NO LATE SUBMISSION OR PLAGIARISM IS ALLOWED.**

Network Administration - Security

Note that for problems with prefix `CTF`, which stands for "Catch The Flag", you should provide your scripts (if any), writeup which explains your thoughts and steps to solve the problem, and the flag itself. The flags are guaranteed to be in the format: "NASA{xxx}". Any programming language is acceptable, but you should provide the way to compile/execute your script.

1. More on SYN Cookies (13%)

As learned in class, SYN cookies can mitigate SYN flooding attacks. However, have you ever thought about the implementation of SYN cookie on a TCP packet?

(a) (2%) Explain why SYN cookies can mitigate SYN flooding attacks.

(b) (2%) Explain why the cookie needs to contain a timestamp.

(c) (2%) Explain why the cookie needs to contain the client IP address.

(d) (3%) Based on your work in Lab7, please capture the packets with SYN Cookie using `Wireshark` and save them in `prob1-d.pcapng`. Using `Apache` as your web server is highly suggested, and this link provides some basic tutorials to set up `Apache` server.

(e) (4%) Based on the captured packets in (d), please describe the difference in TCP header columns between the packets with SYN Cookies and those without SYN Cookies.

2. DDoS Mitigation (8%)

Proof-of-work is a commonly strategy for DDoS defense. The users will be asked to solve a puzzle, which usually takes some time to solve, before accessing the service. Only the users who solved the puzzle can access the service.

(a) (2%) Explain why requesting users to solve a puzzle can mitigate DDoS Attack.

(b) (6%) (CTF) You would like to access Alice's service, which can be accessed by typing `nc linux10.csie.org 15001` in the terminal. However, Alice requires all users to solve a puzzle within 2 minutes to access her service. Can you solve the puzzle within the time constraint? The server source code is provided in `code2-b.py`. Save your script (if any) as `prob2-b.*`, where `*` can be replaced with any programming language.

3. SSL Stripping (17%)

In this problem, you are asked to implement an attacker doing SSL stripping attack. To demonstrate its functionality, you will attack your own machine. That is, you should set proxy on your victim machine to reroute all the traffic to the attacker. Therefore, as learned in class, the attacker can see all the traffic content if the victim accidentally uses HTTP protocol to connect to an HTTPS-required website.

(a) (10%) Please follow the instructions and tutorial on this link to implement the SSLStrip attacker on a VM using Kali linux. Show its functionality by rerouting the traffic of the host machine to the attacker and revealing the HTTPS traffic content between the host machine and the remote website here. Please do not attack the website itself. Write down all the steps you have done with some screenshots and the disclosed HTTPS traffic content in your report. You should be able to intercept and see what the user typed in the account and password columns.

(b) (2%) It is known that HSTS can mitigate such attack since it can prevent the user to connect to the website via HTTP if the user has connected to it before. Please list two websites that applies HSTS on their service, and give their HSTS headers respectively.

(c) (2%) In an HSTS header, there is a column called `max-age`. Briefly explain its purpose.

(d) (3%) What potential vulnerabilities might occur if the value of `max-age` is set to be 0 in HSTS header? Briefly justify your answer.

4. Security on Cisco Switch (12%)

You have learned how to set up a Cisco switch several weeks ago. In this problem, we would like to go further to implement some security prevention on Cisco switches using Cisco Packet Tracer.

(a) (4%) Construct a network topology with one switch and two PCs with same MAC address. What will happen when the two PCs with identical MAC address connect simultaneously to the Cisco switch? Please conduct some experiments on Cisco Packet Tracer and observe the changes in Mac address table. On port `Gi0/1`, there should be a victim PC with MAC address `0255.7711.abcd`; and on Port `Gi0/2`, there should be a malicious PC also with MAC address `0255.7711.abcd`. Can both of the two PCs with identical MAC address access the Internet simultaneously? Briefly explain your answer, your experiment, and the commands you applied in your network settings. Save your Cisco Packet Tracer file as `prob4-a.pkt`.

(b) (3%) Based on your work in (a), please enable Port Security of `(Gi0/1, 0255.7711.abcd)` on the switch so that the attacker cannot spoof the MAC address of the victim PC. Write down the commands you applied to set up the new function, and save your Cisco Packet Tracer file as `prob4-b.pkt`.

(c) (5%) Construct a network topology with one switch, two DHCP servers, and one PC client. The DHCP pools of the two DHCP servers should be **disjoint**. One of the DHCP server is malicious, so the client should never take its offer. However, under normal settings, when the client requests for a DHCP offer, it might receive offers from both the authentic DHCP server and the malicious DHCP server. Please configure the switch such that the DHCP offers are allowed only from the port of the authentic DHCP server, and offers from other ports will be blocked. Briefly explain your answer, your experiment, and the commands you applied in your network settings. Save your Cisco Packet Tracer file as `prob4-c.pkt`.

System Administration - Security

Before you start

- Write down what you did step by step **following our instructions**, and provide explanation and the commands you use for each step, except explicitly stated otherwise, to earn full credit.
- Use this VM for the following tasks (user/password: `nasa` and `nasa2019`).

1. There's nothing there but root

You are given a machine, but you don't have root credential.

a. Find something (5%)

There's an unusual file under `/etc`; try to find it out and recover it. Tell me how you find it (you don't need to print the content of the file here).

Hint: Vim swap file

b. Strange file (10%)

`SUID` is a special type of permission given to certain system executables, such as `passwd`, `chsh` etc. However, `SUID` should be managed with care because it enables a normal user to do something that she otherwise is not allowed to do.

1. Explain why `passwd` should have `SUID` permission. (3%)
2. In the given VM, we intentionally added `SUID` permission to some files that typically does not have `SUID`. Find at least 2 such executables and demonstrate how you can use them to do something that only a privileged user can do. (7%)

c. Root password (7%)

Try to find the root password using what you've found in the task 1.

Hints:

- john the ripper
- hashcat
- rockyou

d. Single login (6%)

Try to log in from single-user mode, using the root password you've found in previous task. Give a screenshot as a proof.

2. Try another hash (10%)

Replace the `[id]` parameter with your own student ID: https://www.csie.ntu.edu.tw/~joe/nasa_hw/passwd.php?id=b07902000. You will see a hashed string. Find out what hash is used, and show me the deciphered string.

Hint:

- hashcat
- deciphered string length ≤ 8

3. SHA1 of PDFs (12%)

Give me two PDF files that display different content, but have the same SHA-1 digest. One of them contains your student ID, while the other does not. Save the two PDF files as `sha1-1.pdf` and `sha1-2.pdf`.

Hint: https://shattered.io/