**COMP7904 Information Security: attacks and defense**

**Assignment 1**

**Student ID: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Disclaimer**

*“All lecture notes, handouts and discussions relating to technological means of hacking, virus attacks, denial of services or any other means of attacking a computer system are for the sole educational purpose of teaching COMP7904 (Information Security: attacks and defense). Those are not intended to be adopted or applied to launch any attack on or to cause any damage to any computer system, and do not in any way encourage anyone to engage in such acts. By taking this course, you also agree not to adopt or apply any of the technological means discussed or otherwise disclosed in this course to engage in such acts.”*

1. **You need to answer all the questions and provide the related screenshots.**
2. **Save your assignment worksheet in PDF format.**
3. **Zip your source code in zip format.**
4. **Submit TWO(2) files to Moodle. (1 PDF & 1 Zip)**

**Download the material (A1.zip) from Moodle.**

1. **Cracking passwords [10 marks]**

You are required to submit your source code for this task. [4 marks]

We assume that Eve have cracked a database as follows.

|  |  |
| --- | --- |
| **Username** | **SHA512(Password)** |
| Alice | e37c759cb92c4c2e7d39c6f9854c3c73d3643f2a316601ff60f412c15a6bf91829ae33670a43a956628ed02371edbf942413aac06f52b481c60c8bd48efa19ad |
| Bob | 834a0ff42987bff586f49f2f4e77e18c207adec957ac81eafdf6a4a90229331dbde9072d962cea44de1e18cbb34b6384a82f016ab86460660cca47786d97f66f |

We know that the passwords are hashed using **SHA512** algorithm without “salt”.

Please help Eve to find the password of Alice and Bob. (i.e., you need to find Alice\_password such that SHA**512**(Alice\_password) = e37c759cb92c4c2e7d39c6f9854c3c73d3643f2a316601ff60f412c15a6bf91829ae33670a43a956628ed02371edbf942413aac06f52b481c60c8bd48efa19ad

, and the same as Bob’s)

**Write your own code** to crack the password. Use whatever programming language you like together with related APIs/Packages to find Alice’s and Bob’s passwords. **A dictionary of password (dict.txt) is provided in A1.zip**.

*If you use Python, you may need to select the UTF8 encode scheme for the input of the SHA512 hash function. You need to make sure your hash function performs the same as the one in https://gchq.github.io/CyberChef/*

|  |  |
| --- | --- |
| **Username** | **Password** |
| Alice | [2 marks] |
| Bob | [2 marks] |

|  |
| --- |
| **Screenshots** [2 marks] |
|  |

1. **John the ripper [10 marks]**

Use john to crack Task 1 Alice and Bob’s password. Provide the command you use and the screenshots.

|  |
| --- |
| **Commands** [2 marks] |
|  |
| **Screenshots** [2 marks] |
|  |

Use john to crack the password of user ‘kali’ in **passwd** and **shadow**.

* 1. The password hash is salted
  2. Hint: Use **mutated** /usr/share/john/password.lst as dictionary

|  |
| --- |
| **What hash algorithm was used?** [2 marks] |
|  |
| **What is the password of user ‘kali’?** [2 marks] |
|  |
| **Screenshots** [2 marks] |
|  |

1. **Whois lookup [10 marks]**

Please gather the whois information of the following domains: **megacorpone.com** and **hku.hk**.

Fill in your findings

|  |
| --- |
| Domain Name: **megacorpone.com** |
| **Registrar** [1 mark] |
|  |
| **Name Servers** [1 mark] |
|  |
| **Creation Date** [1 mark] |
|  |
| **Contact Information (List all Names, Addresses, Phone numbers, Email addresses)** [2 marks] |
|  |

|  |
| --- |
| Domain Name: **hku.hk** |
| **Registrar** [1 mark] |
|  |
| **Name Servers** [1 mark] |
|  |
| **Expiry Date** [1 mark] |
|  |
| **Contact Information (List all Names, Addresses, Phone numbers, Email addresses)** [2 marks] |
|  |

1. **DNS Enumeration [20 marks]**

You are required to submit your shell script for this task. [4 marks]

Use **host** command to:

* 1. Create a Bash script for DNS forward lookup brute force. (You can fill in your code to the skeleton code file “**dns\_forward\_lookup.sh**”.)
  2. Create a Bash script that can identify the name servers and test DNS zone transfer on each of them. (You can fill in your code to the skeleton code file “**dns\_axfr.sh**”.)

Example outputs of dns\_forward\_lookup.sh

一張含有 文字 的圖片

自動產生的描述

Example outputs of dns\_axfr.sh:

一張含有 文字 的圖片

自動產生的描述

Use your scripts above to perform DNS forward lookup and attempt zone transfer on **megacorpone.com** and **hku.hk**. (Common service names are provided in list.txt.)

|  |
| --- |
| **megacorpone.com** |
| **DNS forward lookup results** [1.5 marks] |
|  |
| **DNS zone transfer results (Please fill NONE if zone transfer is not success)** [1.5 marks] |
|  |

|  |
| --- |
| **hku.hk** |
| **DNS forward lookup results** [1.5 marks] |
|  |
| **DNS zone transfer results (Please fill NONE if zone transfer is not success)** [1.5 marks] |
|  |

|  |
| --- |
| **Describe the pros and cons for recursive queries and iterative queries in a DNS query from the security point of view.** [10 marks] |
|  |

1. **Google Hacking [25 marks]**

Please use the Google Hacking technique and the Google Hacking Database (GHDB) to conduct information gathering. Give an example how to use Google’s operators to conduct information gathering (e.g. password or other sensitive information) from the Internet. You cannot use the same example in the lecture.

|  |
| --- |
| **Your Google search query** [3 marks] |
|  |
| **Explain the purpose of your search query and what kind of information you are able to find** [10 marks] |
|  |
| **Please suggest counter measures for such kind of information leakage** [10 marks] |
|  |
| **Screenshots of your search results** [2 marks] |
|  |

1. **Shodan [25 marks]**

Using the Shadon.io to identify machines in Hong Kong have exposed the “Remote Desktop Protocol” (RDP) service to the public internet. Please provide the filtering query in the screenshot and explain your command.

|  |
| --- |
| **Your search query** [1 marks] |
|  |
| **Explain the purpose of your search query** [2 marks] |
|  |
| **Please express your views on the pros and cons of expose the RDP services to the public internet** [5 marks] |
|  |
| **Screenshots of your search results** [1 marks] |
|  |

Give another example how to use Shodan to conduct information gathering (e.g. vulnerable machines and IoT devices).

|  |
| --- |
| **Your search query** [1 marks] |
|  |
| **Explain the purpose of your search query and what kind of information you are able to find** [3 marks] |
|  |
| **Screenshots of your search results** [1 marks] |
|  |
| **Please express your views on the impact of Shodan on the cybersecurity industry (do NOT copy directly from the websites) and cite the references you refer to** [10 marks] |
|  |