Lab Session 1 (L1)

Information Gathering & OSINT

Objectives

The objectives of L1 are:

- To know about common information gathering tools beyond the concepts already explained in theory lectures.
- To perform some exercises using a set of information gathering tools with the objective to retrieve information from vulnerable targets.
- To perform first steps of vulnerability exploitation (reconnaissance) of a well-known CVE. To gain practice in searching about potential exploits.

Statement

Open a text document titled **L1_D1**, that will be the report that will contain the answers to the questions asked in the ongoing tasks. Recall that you can use the slides about information gathering (see the slides of T2 session) as supporting material.

Note: The tools that are going to be used in this task are: Google Dork, GHDB, WHOIS, SHODAN, crt.sh and Wappalyzer. You will need to choose the tool (or combination of tools) to use at every step. Some of the tools will require login and can only be used with limited features in their free version. Use of active scanning tools, such as nmap, and brute-force attacks are forbidden.

Preliminaries

Read about exploit-db (https://www.exploit-db.com/about-exploit-db) and in particular, about Google Hacking DB (GHDB).

Task 1: Finding Vulnerabilities (4 points)

Let us start our exercise by performing an advanced search. The following command is proposed:

intitle:"index of" /etc/shadow

1) Explain in detail what is the objective of this search. What the operator does? What is the purpose of the string “index of”? Why is the objective of the parameter etc/shadow? Is there any malicious purpose by executing this dork?
2) Run the command in Google Search bar, and take a look to the search results. Explain what you can see.
3) Let us focus on the url

   https://shrishikshayatancollege.org/etc/shrishikshayatancollege.org

   Enumerate the files you can see and describe the type of contents that you can find in “passwd” and “shadow” files

4) Let us get some additional information about the main site https://shrishikshayatancollege.org

   Using the aforementioned tools, provide the following information:

   a. Registrant contact information
   b. IP address of the domain
   c. Internet service provider
   d. Cloud service provider
   e. Open ports (Do **NOT** use nmap)
   f. Web Technologies

5) Now, play the role of a *black hat*, and **describe** (not perform):
   a. A vulnerability/weakness you detected
   b. Potential actions to exploit such vulnerability

   You can propose using additional tools and making assumptions for those aspects that you cannot know with the obtained information.

6) Come back to point 2), and select another different domain. Repeat points 4) and 5); if possible, select a different vulnerability and/or potential actions to perform.

Task 2: Exploiting a CVE (2 points)

For this task we focus on a CVE clearly identified (CVE-2021-42013):

https://nvd.nist.gov/vuln/detail/CVE-2021-42013

1) Explain in your own words, your understanding on this vulnerability.
2) Search in exploit-db one identified exploit for this vulnerability. Briefly explain how the exploit works (do not execute any code)
3) Which tool would you use (and how) to list the servers that are affected by this vulnerability? Write the results
4) Is there any site affected by the vulnerability that is exposing port 22 (ssh)?[1]

[1] Hint: By default, many servers expose their software name and version in the “Server” HTTP response header. “<software>/<version>” like “nginx/1.18.0”

Task 3: Information Gathering Tool Analysis (4 points)

For this last part, select one of the information gathering tools presented during this practical or during theory lecture about this topic. Some of the tools that you can select are (not restricted to):

- WHOIS/Reverse WHOIS
- Wayback Machine
- NSLookup
- Shodan
- TheHarvester (passive modules)

Explain in detail what the tool does, how it works, write execution examples and put results (captures, screenshots). Put several examples (as nice as possible) to show the functionalities and flexibility of the tool. Explain what are the main benefits for a white hat (or pen tester) to use the tool. And explain whether a black hat hacker can get different benefits and/or opportunities. If you choose a tool used in this lab session, highlight those features/functionalities that have not been explored during the different tasks.

The format is free, be as didactic as possible. Do not exceed 4-5 pages for this task.

Delivery

Zip the document **L1_D1** in a compressed file with name **L1_[your_group_number].zip**. Submit the file to **RACO (Practicals/L1**).

Deadline: October 17th

Supporting Material

Information gathering slides available in RACO.