Lab 2

In this lab, you are asked to read the scenario and answer the related questions/tasks. This lab is designed to increase your familiarity with honeypot deployment and data collection from attackers using honeypots.

Scenario

You are working for a cybersecurity firm as a cybersecurity analyst. Your manager is interested in investigating cyberattacks towards Elasticsearch servers without authentication. You are asked to deploy selected Elasticsearch honeypots to your remote servers. Two different honeypot projects are selected:

1. Elastichoney: https://github.com/jordan-wright/elastichoney
2. ElasticPot: https://github.com/bontchev/elasticpot

You can improve or change honeypot pages to increase likelihood of attacks.

Questions/Tasks

Task 1: You are asked to deploy the Elastichoney honeypot to port 9200 and the Elasticpot honeypot to 9300. Once honeypots are deployed, you should be able to see the honeypots' home pages by navigating to the corresponding [SERVER_IP]:[PORT] combination using your web browser.

You are expected to provide a report. In your report, explain how you managed to install & deploy both of these honeypots. Show and explain the Linux commands used to set up the honeypots. Your explanations should contain screenshots. Make sure that you also include screenshots of the honeypots' home page from your browser.

In the report, please clearly mention which honeypot installation you are working on (explain them in separate sections, one for Elastichoney and one for Elasticpot). Your report should be clear and precise. Your report should contain many screenshots to explain your installation process. Each of these screenshots must be sufficiently explained in words. We will not accept reports containing screenshots solely. If the explanation is missing some key parts, then we will reduce points. Your report should contain your remote server's IP address.

Note: If you could not successfully deploy the honeypots, please explain what went wrong in your report so we can give you partial points.

Also please include your entire Linux history using the Linux history command.

You can use this command as follows: "`history > [location_you_want]/[filename]`" (e.g. you can use the command "`history > ~/history.txt`" to create a text file named "history.txt" containing history in the current user's home directory) and then pull this from your server and include it in your submission.

You can pull this created file via secure copy (SCP). The basic usage of SCP is as follows: "`scp [username]@[server_ip]:[target_file_path] [destination_file_path]`" (e.g. you can use "`scp root@[server_ip]:~/history.txt history.txt`" to copy the file called "history.txt" which is on the root's home directory to current directory of the target machine).

Here is some hint:

You might need a command called *screen*. The basic usage can be seen here: https://linuxize.com/post/how-to-use-linux-screen/

Task 2: Test your honeypots with the queries provided. In this task, you are asked to perform all queries given below, on each of the deployed honeypots.

Queries:

1. /_cat/indices

   Aim: Listing all the available indices in a cluster. Also providing high level information about them. Query example for browser: [SERVER_IP]:9200/_cat/indices & [SERVER_IP]:9300/_cat/indices

   https://www.elastic.co/guide/en/elasticsearch/reference/current/cat-indices.html#cat-indices-api-request

2. /_cat/nodes

   Aim: Returns information about a cluster's nodes.

   https://www.elastic.co/guide/en/elasticsearch/reference/current/cat-nodes.html

3. /StudentID/Surname (no Turkish characters, e.g. çetin -> cetin)

   This is a special query. In a normal Elasticsearch server, this will result in an error message indicating the requested content is not found.

What is required for this task :

1. The log files created by the honeypots. These log files should include all the queries made by you.
2. In your report please include screenshots coming from your remote session displaying your honeypot logs that contain the queries above. You should explain which log file (created by which of the honeypots) you would prefer to work with in the future if you have to capture any attacks towards Elasticsearch servers. Also why you would prefer this! Please use sections for each of the honeypots while doing this part.
3. The IP address which was used by you to query the honeypots.
4. Again in your report, please mention how log files can be improved. What else can be added in terms of improving usability and honeypots' monitoring capabilities (gathering meaningful data using Elasticsearch honeypots)?

To summarise, you are expected to provide screenshots of Elastichoney (containing queries), screenshots of Elasticpot (containing queries), explanation regarding which one you prefer (Please provide your explanation criteria –ease of understanding attacks, informativeness, usability).

Task 3 : Please complete the following survey after answering the following questions (You will not be able to retake it).

Link to the survey: http://206.189.4.53/