|  |  |
| --- | --- |
| **Mandatory** **Case** | Description: LogoBINUS-University |
| Programming for Penetration Testing H4 |
| **Periode Berlaku** Semester Ganjil 2020/2021  ***Valid on*** *Odd Semester Year 2020/2021* | **Software Laboratory Center**  **Assistant Recruitment 21-1** |

## Materi

*Material*

* Port Scanning
* Brute - Forcing Directories
* Web Scrapping
* Reverse TCP

## Soal

*Case*

**Bluejack CTF**

Here you go, the last Mandatory Case for your Core Training, let’s put everything that you’ve learnt to the test. You’ve made a promise to finish this case fully, 100% so I will give my all. You can **finish this task** if you have the **knowledge**, **research** **skill** and **might to become an Laboratory Assistant**. Tonight you have 7 deadly tasks that you need to complete. Here are the requirements:

* **Port Scanning**
* You are asked to make a python script to scan port with **FIN port scanning method** using **scapy** library.
* You need to make the program capable to receive arguments with **getopt**. Here are the list of parameters
  + **“-t”** or **“—target”**
    - You must pass the ip address of the target that you want to scan.
  + **“-s”** or **“—startPort”**
    - You must pass the starting port number.
  + **“-e”** or **“—endport”**
    - You must pass the ending port number.
* Turn off the verbose mode on scapy.

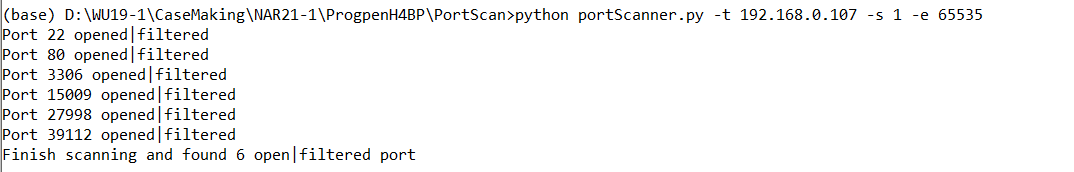
****

Figure 1. Port Scanning Example

* **Directory Listing and File**
* You are asked to make a python script to bruteforce directory or any web page that you can. The web application use PHP as backend languange.
* You need to make the program capable to receive arguments with **getopt**. Here are the list of parameters
  + **“-t”** or **“—target”**
    - You must pass the ip address of the target that you want to scan.
  + **“-p”** or **“—port”**
    - You must pass the port number.
* You can download the wordlist [here](https://github.com/daviddias/node-dirbuster/blob/master/lists/directory-list-2.3-medium.txt).

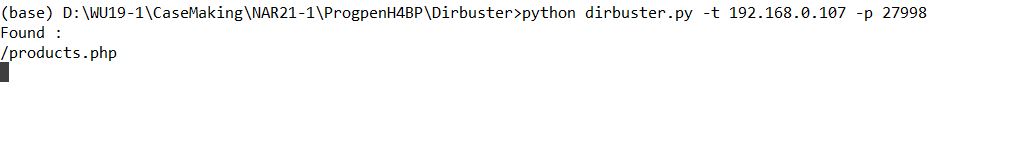
****

Figure 2. Dirbuster Example

* **Scrapping with GET Request**
* You are asked to make a python script to **scrap** one of the ports **after finding** out the URI.
* This specific web page has a list of products.
* You need to make the program capable to receive arguments with **getopt**. Here are the list of parameters
  + **“-t”** or **“—target”**
    - You must pass the ip address of the target that you want to scan.
  + **“-p”** or **“—port”**
    - You must pass the port number.
* You must display **total of items**, **sum** of all **prices**, and **average** of all **prices**.
* You must **clean** the **data first** because the website has 35% chance of generating trash.

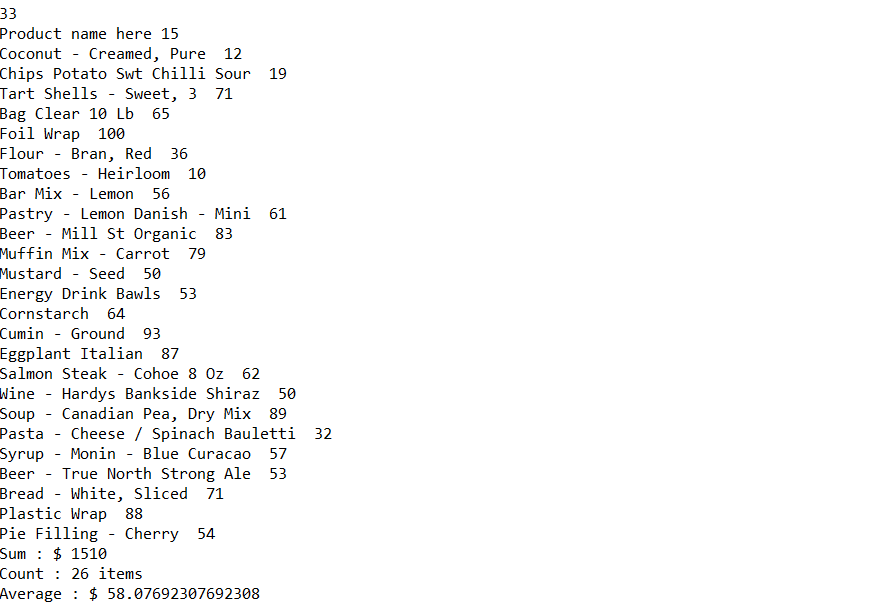


Figure 3. Scrapping Result

* **Scrapping with GET Request and POST Request**
* You are asked to make a python script to **scrap** one of the ports **after finding** out the URIs.
* This specific web page has a list of flags and you need to submit the flags and find out the correct flag, there are 5 of them.
* You need to make the program capable to receive arguments with **getopt**. Here are the list of parameters
  + **“-t”** or **“—target”**
    - You must pass the ip address of the target that you want to scan.
  + **“-p”** or **“—port”**
    - You must pass the port number.
* You must display **all the flags** and the response from the **flag** after being **submitted**.

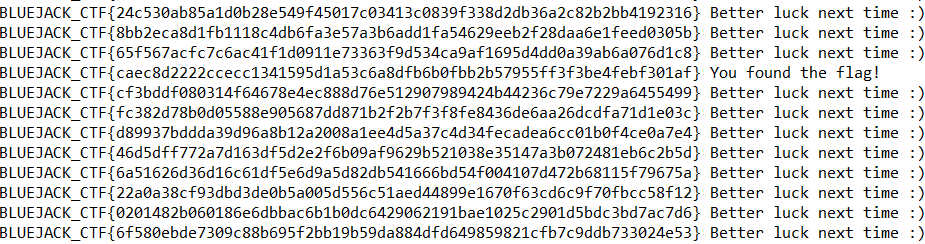


Figure 4. Scrapping Result with GET and POST

* **Reverse TCP (Victim)**
* You are asked to make a python script that can be used as a **backdoor** to the **server** via **file** **upload**.
* You need to upload the file to one of the page that contains file upload.
* **Reverse TCP (Atttacker)**
* You are asked to make a python script to **connect** to the **Server** via **python** **file** that you have **uploaded**.
* You need to make the program capable to receive arguments with **getopt**. Here are the list of parameters
  + **“-t”** or **“—target”**
    - You must pass the ip address of the target that you want to scan.
  + **“-p”** or **“—port”**
    - You must pass the port number.
* The script is capable to run **any command and receive and display the result of the command**.
* The script must be capable of **changing directory** and display **current working directory**.

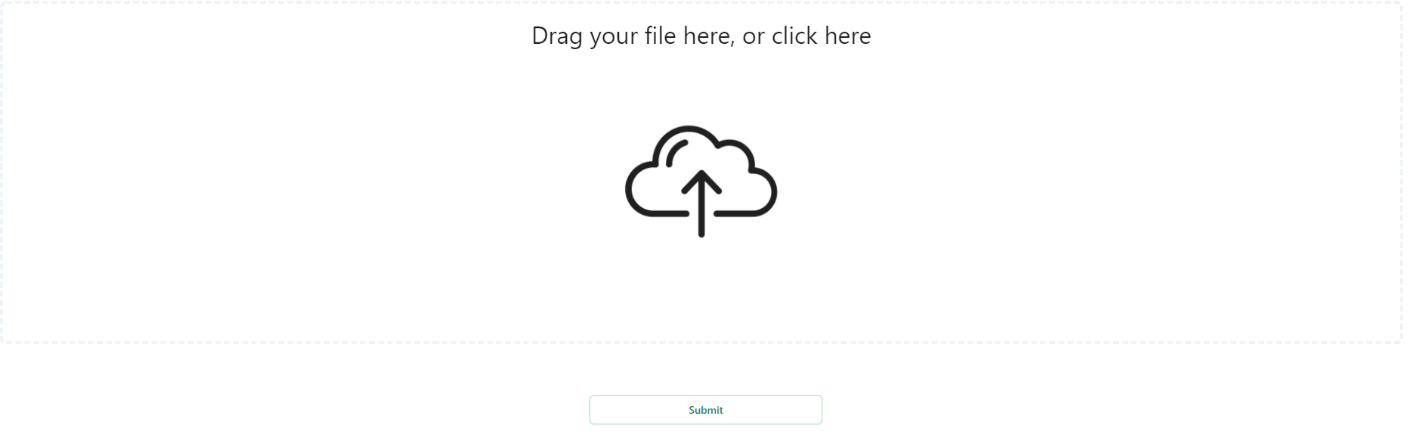
****

Figure 5. Uploading python file

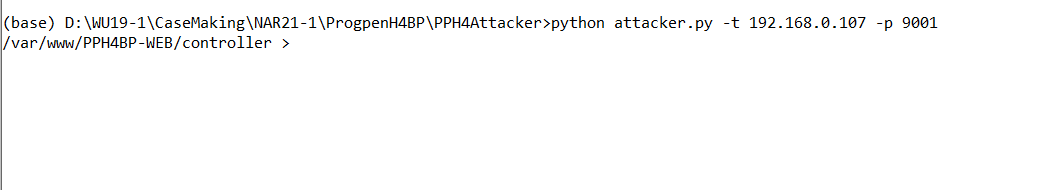


Figure 6. Successful Reverse TCP

* **Penetration Testing Scenario**

Here is the case, you are a cyber security division member in a police department. One day a case has arrived that there is a suspicion that there is a suspicous anonymous party who sponsors a **Capture The Flag** Event which is held by **Bluejacket Allstar Group**. There is a suspicion that this anonymous party want to do **money laundering** by sponsoring this event. You need to find **who sponsored it** and **how much money** does this anonymous party gave. Luckily for you, your partner have done some of the hard work, you need to make the proof of concept and execute everything based on this instructions.

* Step 1

Do the **Reverse** **TCP** to access the **server**.

* Step 2

Find the **configuration** file for the server to **access** the **database**.

* Step 3

Retrieve the **username** and **password** for the **database**.

* Step 4

Use any method to access the **database** **service** (ex. Use **phpmyadmin**).

* Step 5

There is an table called **users** find out what’s in it.

* Step 6

**Access** the **Server** using **any info that you find** from the user’s table.

* Step 7

**Gain root access** and **search** for the **home** **directory** for any suspicious file.

* Step 8

If you find any **suspicious file** that can be used as evidence, **exfiltrate** it and **retrieve** it **by** **any** **means** **necesarry**.

## Note

*Catatan*

* You don’t have to use **threading** for the **dirbuster**.
* There is no **Firewall** or any **IDS** **installed** in this Machine.
* You need to provide **“writeup”** for the **Penetration Testing Scenario**
* All request must contains **Browser User-Agent**, you can copy it from your browser and append it to your request header.
* Restart the machine if the server **refused to connect** (for **dirbuster**).
* After you are in **the** **machine**, **do not** **screw the configuration** file for the web server (in this case, I am using Apache2).
* You need to install and start **npcap service** for using scapy.
* You **can use** the tools in **Kali Linux** first before **make your own tools**. (**Except for scrapping**)
* If you found the answer but you **didn’t make the python script**, your **scored for that script** will be **zeroed**.

## Component

*Components*

|  |  |  |
| --- | --- | --- |
| No. | Criteria | Percentage |
| 1 | FIN Port Scanner Script | 20% |
| 2 | Dirbuster Script | 10% |
| 3 | Scrapping Products Script | 10% |
| 4 | Scrapping Flags Script | 10% |
| 5 | Reverse TCP Client’s Script | 10% |
| 6 | Reverse TCP Attacker’s Script | 10% |
| 7 | Penetration Testing Scenario | 12.5% |
| 8 | Penetration Testing Proof | 12.5% |
| 9 | Argument Parser on All Script | 5% |