|  |  |
| --- | --- |
| **Practicum Case** |  |
| COMP6548  Programming for Penetration Testing |
| **Cyber Security** | **<Case Code>** |
| ***Valid on*** *[Odd/Even/Compact] Semester Year 9999/9999* | **Revision 00** |

## Learning Outcomes

* Socket Network Program for Penetration Testing
* Web Vulnerability with Programming
* Additional tools for Penetration Testing

## Topic

* Server Post-exploitation I

## Subtopics

* Establish Connection
* File Retrieval through Reverse TCP
* Execute Arbitrary Command through Reverse TCP

## Soal

*Case*

**The Scalpel**

**The Scalpel** refers to a tool that **split open** and **extract** the **information** and/or **execute command** on the **victim’s machine** and **get** the **result back** with **Reverse Shell Method**. In this practicum case, you need to make this tool with specific requirements with **Python Programming Language**, they are:

Reverse Shell:

1. The program contains argument parser with **getopt** **library** with the following specification:

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Short Args | Long Args | Description |
| 1. | -i | --ip | The ip address of the target (default ip 127.0.0.1) |
| 2. | -l | --listen | Set the program to listening mode |
| 3. | -e | --exfiltrate | Specify that the program will exfiltrate a file. It depends on the machine that runs with listen option or not. |
| 4. | -h | --help | Print the help menu |
| 5. | -p | --port | The port number of ssh service that you want to brute force with (default port 1234) |

1. If the program does not run on the exfiltrate mode, the program will run Reverse TCP attack.
   1. The program with “**listen**” option

The program will **create** a **socket** and **listen** on the **ip and port** specified by the user. Any message **that was received** by the **socket** that **was listening** at the time will **execute** the **command** and **send back** the **result**.

If the program receive “**cd**” command (or **Change Directory** command) the program will **execute** the “**cd**” command and **change the current working directory** to the directory that was **received**.

* 1. The program without “**listen**” option

The program will **create a socket** and **try** to **connect** to the **ip and port** specified by the user. The program will **send** a **command** and **receive** the **result back**.

If the program receive the “**exit**” command, the program will **terminate** the **socket’s connection** and **exit the program**.

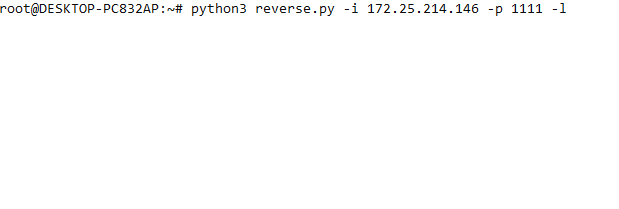


Figure . The Program with Listen Mode On

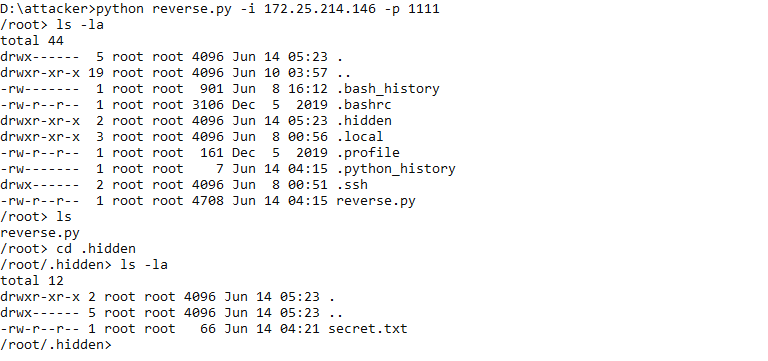


Figure . The Program with Listen Mode On (with cd and other command)

1. If the exfiltrate option was specified, the **program will exfiltrate** the **file** that was specified by the **listening program** and send it over the **socket**. The file will be written by the program that is listening.

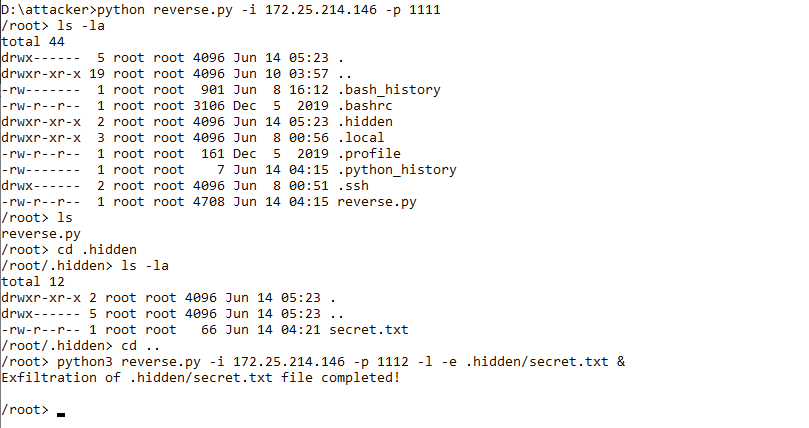


Figure . The Attacker with Reverse TCP Execute the Program with Exfiltrate Option



Figure . The Attacker Received the File with Another Command Prompt Opened

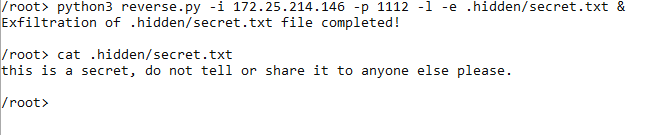


Figure . The Result and the Content of "secret.txt" in ".hidden" Directory

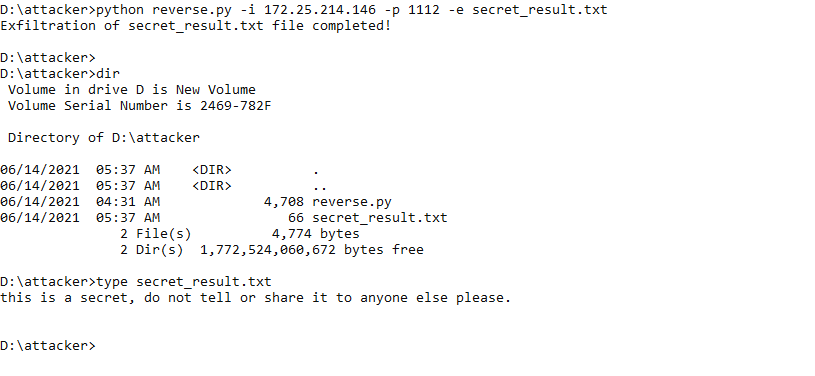


Figure . The Extracted File from the Victim