|  |  |
| --- | --- |
| **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 Authentication Attack

## Subtopics

* Python SSH Module
* Brute-force SSH Authentication
* Read and Permutate Credential Wordlist with Python Threading

## Soal

*Case*

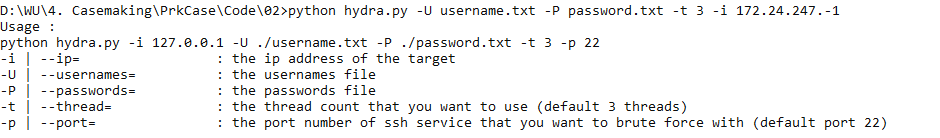
**Hydra**

Hydra is a login cracker that supports multiple protocols, one of the protocols that you are going to brute force is SSH. You need to make the “Hydra” like program with **Python Programming Language** and **paramiko library** with the following specification:

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

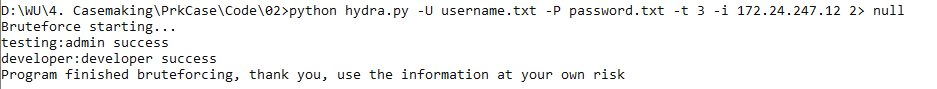
|  |  |  |  |
| --- | --- | --- | --- |
| No. | Short Args | Long Args | Description |
| 1. | -i | --ip | The ip address of the target |
| 2. | -U | --usernames | The usernames file |
| 3. | -P | --passwords | The passwords file |
| 4. | -t | --thread | The thread count that you want to use (default 3 threads) |
| 5. | -p | --port | The port number of ssh service that you want to brute force with (default port 22) |

1. Brute force the ssh service and only display the correct credentials only. Output the result.
2. If the program validation fails, output the usage of the program, and simply exit the program.



**Figure 1. Invalid Argument**

1. The brute force needs to use Threading and Events.



**Figure 2. Result of the Program**