|  |  |
| --- | --- |
| **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 Enumeration Utility

## Subtopics

* Port Scanning using Python with Various Methods (NMAP equivalent)
* Reverse TCP using Python (Netcat equivalent)
* File Exfiltration via TCP

## Soal

*Case*

**The Hammer**

**The Hammer** refers to a tool equivalent of **Network Mapper** (**nmap**) that can **check** if a **port** is **opened or not** with some various methods. In this practicum case, you need to make the tool with specific requirements with **Python Programming Language**, they are:

Port Scanner:

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. | -s | --startPort | The starting port |
| 3. | -e | --endPort | The end port |
| 4. | -t | --thread | Set the thread value (thread has 3 threads by default) |
| 5. | - | --xmas | Use XMAS Scan Method |
| 6. | - | --fin | Use FIN Scan Method |
| 7. | - | --null | Use NULL Scan Method |
| 8. | - | --syn | Use SYN Scan Method (Full SYN) |
| 9. | - | --stealthsyn | Use Stealth SYN Scan Method (Half SYN) |

1. Print out the ports that are filtered (received ICMP Error type 3 with code 0, 1, 2, 3, 9, 10, 13) ([rfc1812 (ietf.org)](https://datatracker.ietf.org/doc/html/rfc1812#section-5.2.7.1), [rfc1122 (ietf.org)](https://datatracker.ietf.org/doc/html/rfc1122#page-39)) or opened (depends on the port scanning method).