# Hadaiq Ahmad

BSCS-4A

cms#112807

NS Gp-1

# Lab 06: OS Fingerprinting and Port Scanning

**CLO4: Compare, investigate and evaluate different security mechanisms to protect network resources.**

**Date: 16th October 2017**

**Time: 9am to 11:50 am**

# Instructor: Ms. Haleemah Zia

**Lab Tasks**

1. What computers did you find running on the local network? [1 Mark]

|  |
| --- |
| Solution |
| nmap -sP -PT80 192.168.56.\* |

1. What is the operating System of your target machine? [1 Mark]

|  |
| --- |
| Solution |
| nmap -O -v 192.168.56.1 |
|  |

1. What ports are open on the machine that you scanned? [1 Mark]

|  |
| --- |
| Solution |
| nmap -sT 10.3.34.135 |

1. What is the difference between a TCP-connect scan and a SYN scan? [1.5 Mark]

|  |
| --- |
| Solution |
| TCP-connect scan is port scanning while SYN scan is stealth scanning  In TCP connect scan , logs are maintained while scanning at the host device  In SYP scan,it does not allow to build up the logs |

1. What is the purpose of the –sP command line switch? [1 Mark]

|  |
| --- |
| Solution |
| -sP stands for “sweet ping”,  The purpose of this command is to scan all the devices that are discovered to be connected with network device |

1. What is the purpose of the –sS command line switch? [1 Mark]

|  |
| --- |
| Solution |
| While using –sT command scanning can be easily detected.  The –sS command which is basically Stealth port scanning is used to avoid logs being ceated of your scanning activity. The targeted computer doesn’t log the connection because the 3-way TCP handshake never finishes.  Instead of finishing the handshake, the attacker sends an RST (reset command) flag to disconnect the connection instead of acknowledging the connection. |

1. After you have run the “–sS –v <Victim IP Address>”, take a look at the other tabs. What information was disclosed by this scan?

[1 Mark]

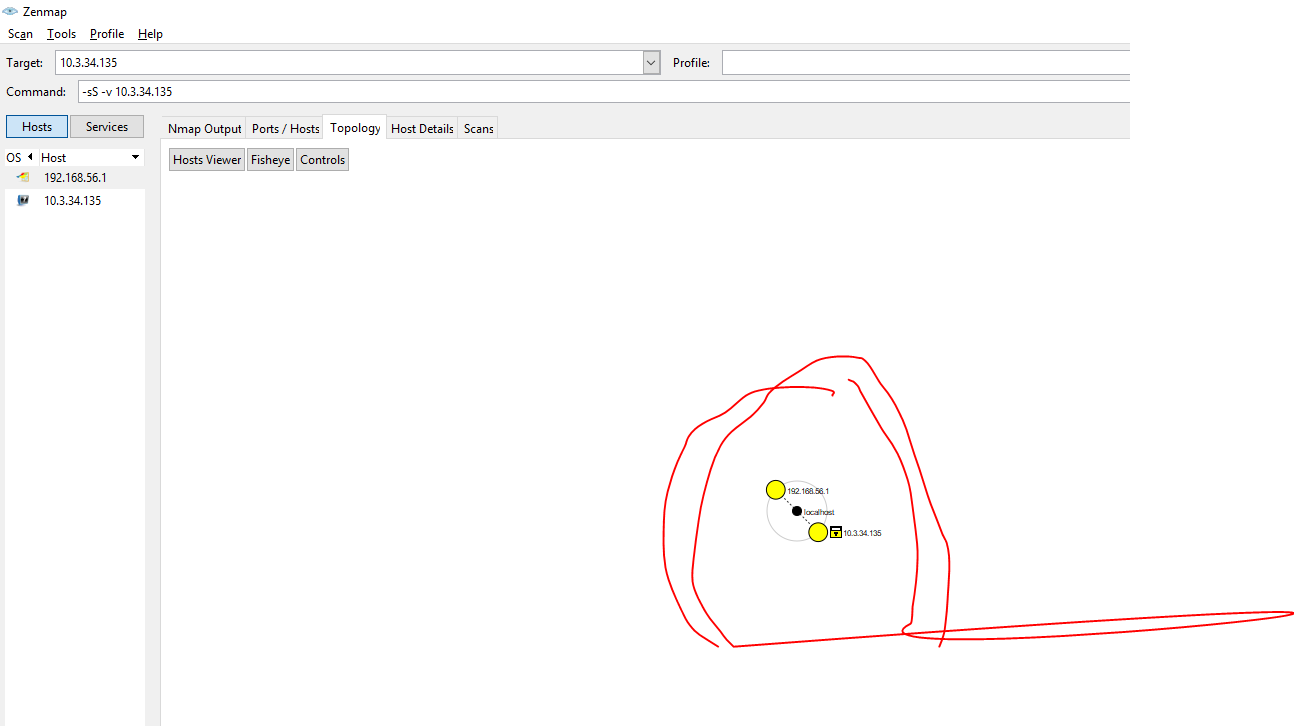
|  |
| --- |
| Solution |
| Ports Tab:  It shows the open ports at target ip address |

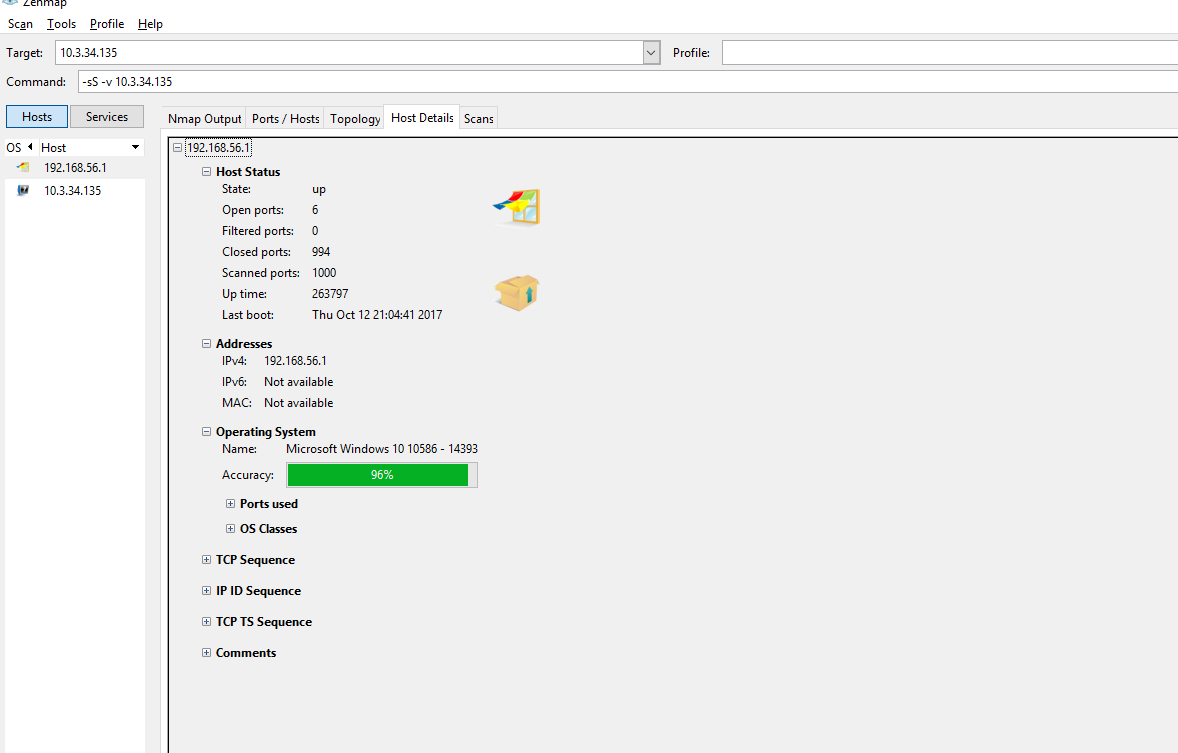
Topology Tab:

It shows the network topology for target ip address.

Host Details:

It shows the details for host address including open ports, mac address etc





1. What are the three main functions of Nmap? [1 Mark]

|  |
| --- |
| Solution |
| Three main functions of Nmap are following  1. Port scanning 2. Host or device detection 3. Service detection 4. OS fingerprinting |
|  |

1. What is the purpose of “nmap –sA –v <Victim IP Address>”? [1.5 Mark]

|  |
| --- |
| Solution |
| The purpose of this command is to send a tcp handshake request to the target ip address. Upon receiving acknowledgement it marks the host as up.I tried multiple times. But it is showing the same response. |

**Deliverables**

Compile a single Word document by filling in the solution/answer part (as directed) along with the snapshots. Name your submission file as given below and submit this Word file on LMS before the deadline.

**Name – Registration No. – Section**

**Grade Criteria**

This lab is graded. Min marks: 0. Max marks: 10.

|  |  |  |
| --- | --- | --- |
| **Activity** | **Minimum** | **Maximum** |
| Documentation with clearly defined understanding of the lab task and approach | Fail | Pass |
| Lab Tasks | 0 | 10 |