

Department of

Bachelor of Computer Applications

**Ethical Hacking Fundamentals**

Lab File – CA 09

**Subject Code:** 19BCA4C02L

**Class:** IInd Year IInd Semester

**Prepared By:**

Suman Garai

20BCAR0246

**Aim :**

Practical to perform enumerating services on user network using Nmap [Any 5 scan].

**Requirements :**

* Virtualisation Software
* Kali Linux 2021.4a
* Basics of Nmap
* Internet Connection

**Objectives :**

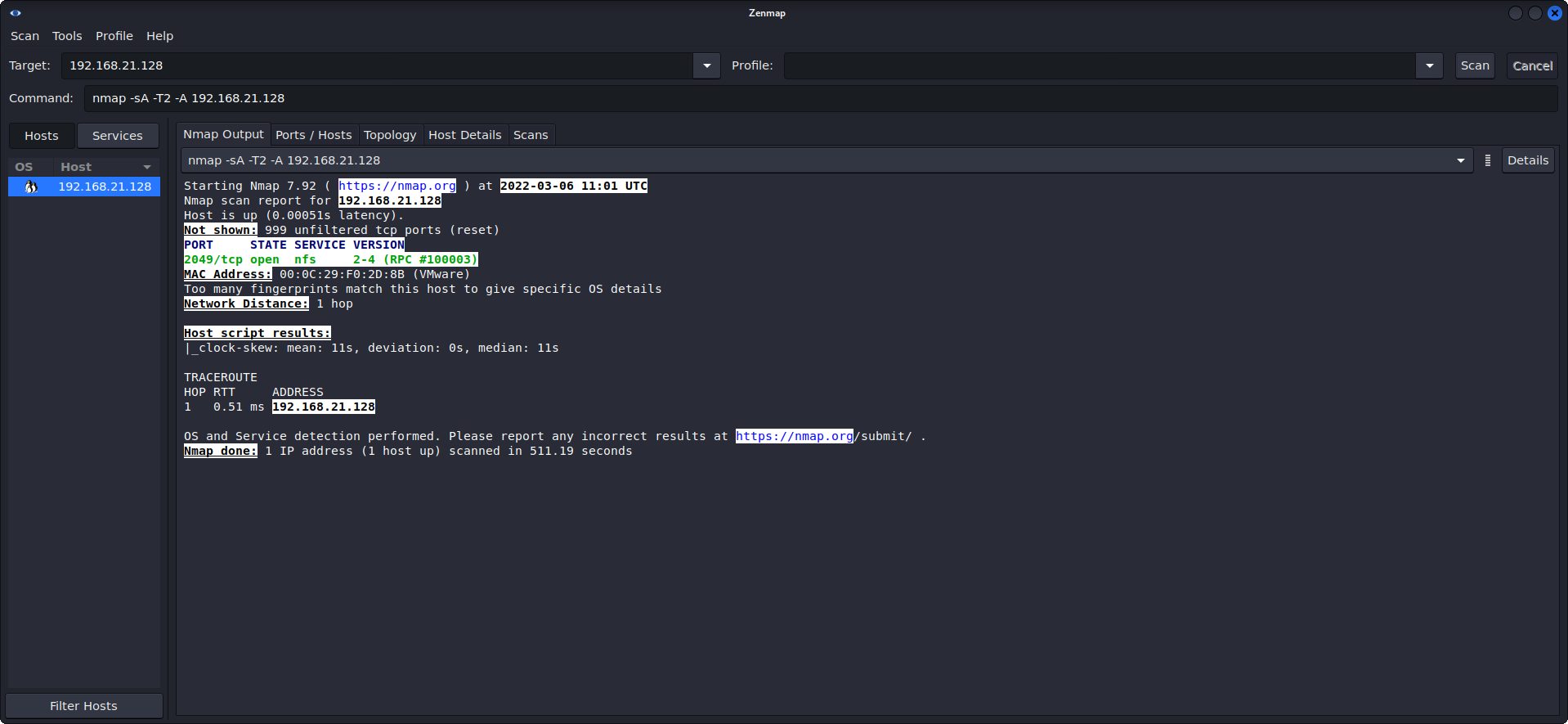
To Run different scans :

* TCP ACK Port Scan
* TCP Connect Scan
* TCP Maimon Scan
* Version Detection Scan
* Fin Scan

**Procedure :**

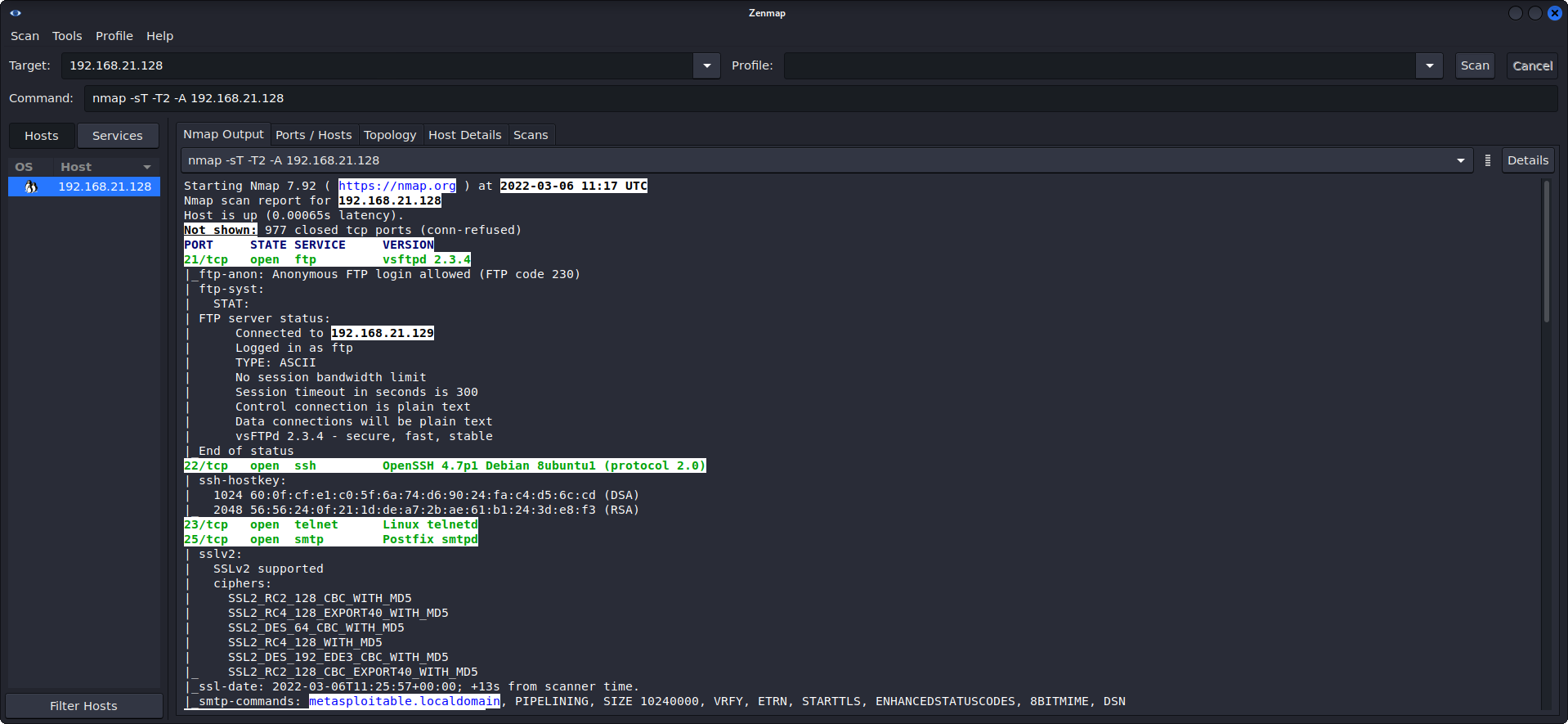
TCP ACK Port Scan

Command: nmap -sA -T2 -A <IP Address>



TCP Connect Scan

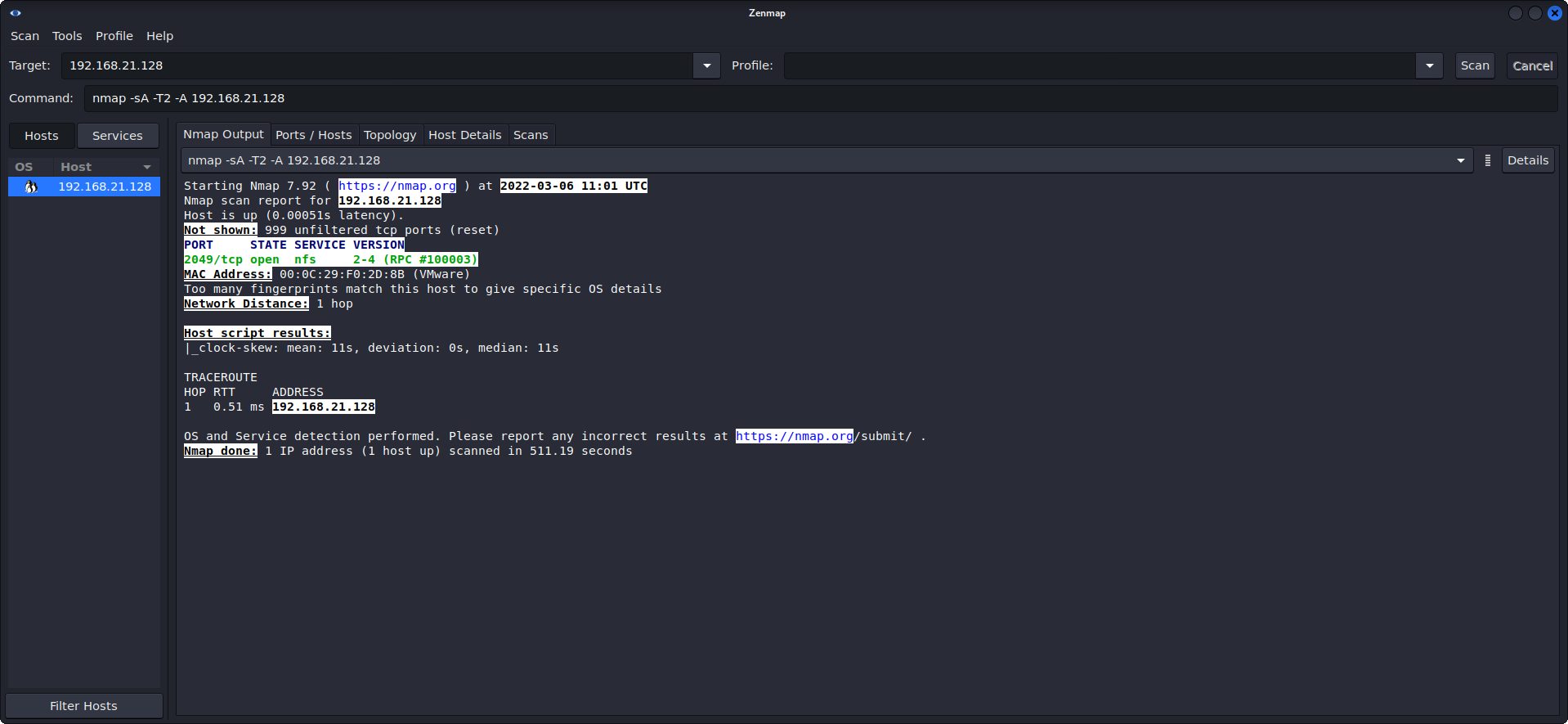
Command: nmap -sT -T2 -A <IP Address>



NOTE: For more details regarding the information obtained, head over to: <https://drive.google.com/file/d/1mDal9rrzByahercesW7C4yndI8LZS7FD/view?usp=sharing>

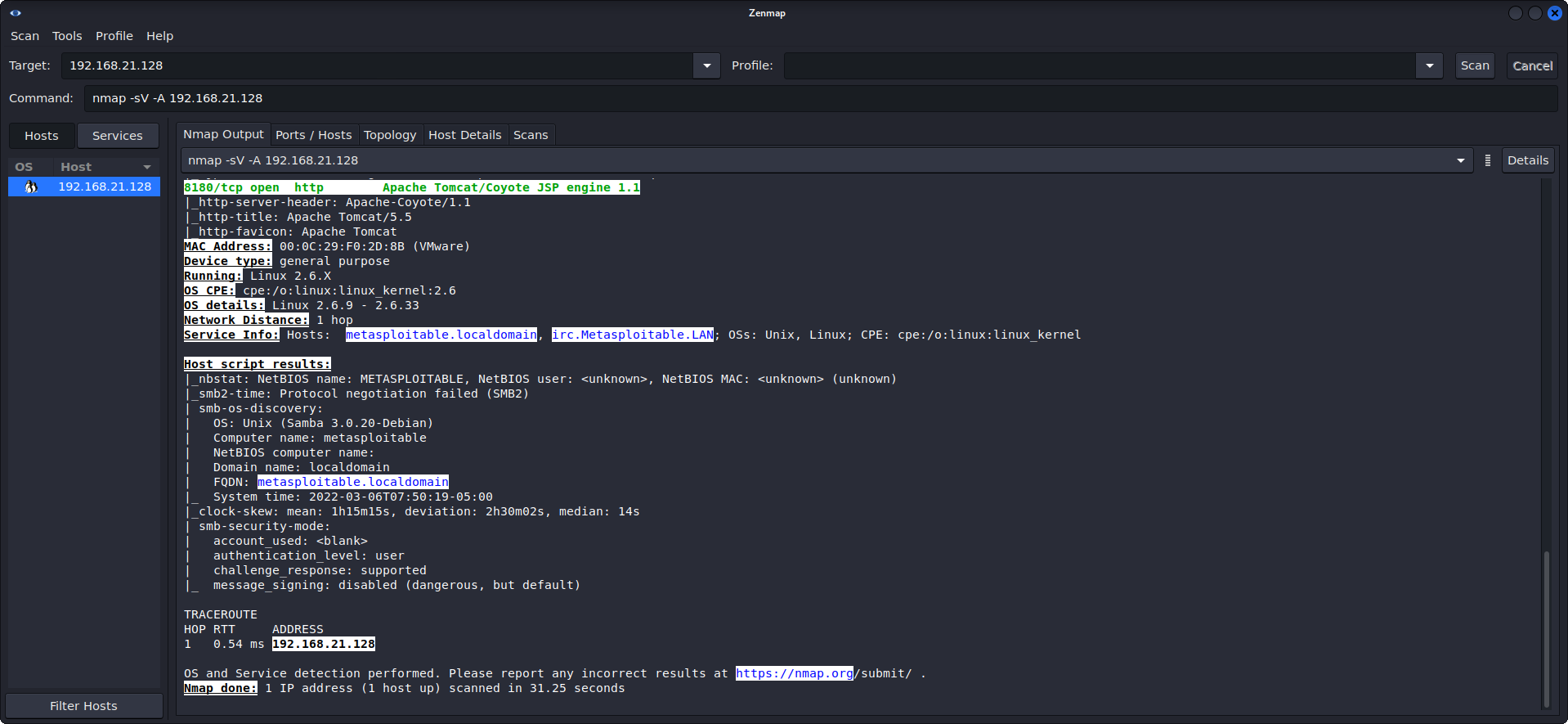
TCP Maimon Scan

Command: nmap -sM -T3 -A <IP Address>



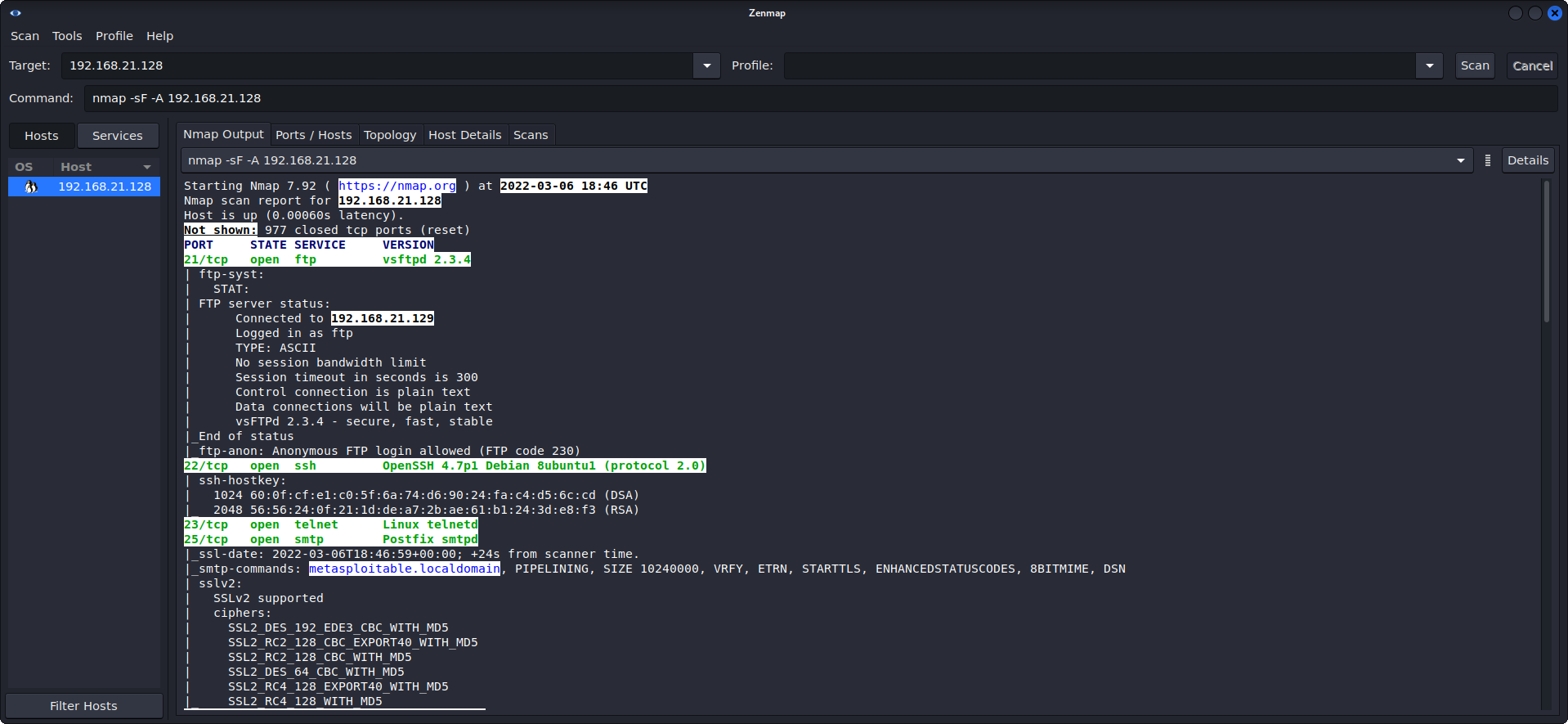
Version Detection Scan

Command: nmap -sV -A <IP Address>



Fin Scan

Command: nmap -sF -A <IP Address>



NOTE: For more details regarding the information obtained, head over to: <https://drive.google.com/file/d/11yLVgHPBsjzDnhssDW7Iq9l2rxzZMhLT/view?usp=sharing>

**Conclusion :**

Nmap is a network scanner tool available both in CLI and GUI interfaces. Nmap is used to discover hosts and services on a computer network by sending packets and analysing the responses. Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection. These features are extensible by scripts that provide more advanced service detection. Tools used in this practical are Metasploitable and Linux CLI nmap. NMAP is used for identifying the available ports on the target machine. Further, using the available ports, we can exploit the available ports by identifying their exploits.