CA-3 Project

"Forensic Analysis of Networks using open source Software N-Map"

By:

Mohammad Musheer Anwar
11910270
Roll.No: 27

Submitted To:

Dr. Manjot Kaur

Index

Chapter 1
Introduction

What is computer forensics?

Computer forensics, also known as digital forensics, is the process of investigating and analyzing digital devices, such as computers, smartphones, and tablets, to uncover evidence related to a crime or security incident.

Computer forensics involves the collection, preservation, examination, and analysis of electronic data in a way that maintains its integrity and reliability for use in legal proceedings or other investigations. This includes recovering deleted files, examining internet history and email communications, and analyzing system logs and network traffic.

Computer forensics can be used in a variety of scenarios, including corporate investigations, law enforcement investigations, and civil litigation. It is an important tool in identifying and prosecuting cybercriminals and in ensuring the security and integrity of digital systems.

Why is computer forensics is important?

Computer forensics is important for several reasons:

1. Investigating cybercrime: With the rise of digital crimes such as hacking, identity theft, and fraud, computer forensics is crucial in investigating and prosecuting these crimes. Digital evidence can be used to identify perpetrators, determine the scope of the crime, and provide evidence for criminal prosecution.

2. Protecting corporate data: Companies rely on their digital systems to store sensitive data, and computer forensics can help identify and address security breaches. Forensic analysis can determine the cause of the breach and identify potential weaknesses in the system that need to be addressed.

3. Ensuring regulatory compliance: Many industries are subject to regulations that require the retention and protection of digital data. Computer forensics can help companies ensure compliance with these regulations and provide evidence in case of an audit or investigation.

4. Resolving disputes: Computer forensics can be used to resolve disputes related to intellectual property theft, employment law violations, and other legal matters. Digital evidence can provide proof of wrongdoing or exonerate individuals accused of wrongdoing

summary, computer forensics is important in protecting individuals and organizations from cybercrime, ensuring data security and regulatory compliance, and resolving legal disputes.

Types of computer forensics

There are several types of computer forensics, each with its own specialized focus:

1. **Disk Forensics:** This involves the analysis of physical storage devices such as hard drives, flash drives, and other storage media. Disk forensics includes the identification, preservation, and analysis of data on these devices, as well as the recovery of deleted or damaged data.

2. **Network Forensics:** This involves the analysis of network traffic to identify and investigate security incidents or policy violations. Network forensics involves capturing and analyzing network traffic, examining system logs, and analyzing communication patterns.

3. **Mobile Device Forensics**: This involves the analysis of data on mobile devices such as smartphones and tablets. Mobile device forensics includes the identification, preservation, and analysis of data on these devices, including text messages, call logs, photos, and other digital artifacts.

4. **Memory Forensics:** This involves the analysis of volatile memory, including RAM, to recover information that may not be stored on the disk. Memory forensics can be used to identify malware or other malicious software that is actively running on a system.

5. **Cloud Forensics:** This involves the analysis of data stored in cloud-based systems, such as email, file storage, and collaboration platforms. Cloud forensics involves the identification, preservation, and analysis of data stored in these systems, as well as the recovery of deleted or modified data.

Each type of computer forensics requires specialized tools and techniques, and may be used in different scenarios depending on the nature of the investigation.

Network Forensics

Network forensics is a type of computer forensics that involves the analysis of network traffic to identify and investigate security incidents or policy violations.

Network forensics involves the capture and analysis of network traffic, examination of system logs, and analysis of communication patterns. This process can help identify unauthorized access attempts, malware infections, data exfiltration attempts, and other security incidents.

Network forensic analysis involves the use of specialized tools and techniques to collect and analyze network traffic data. This can include packet capture and analysis tools, intrusion detection and prevention systems, and network flow analysis tools.

The goal of network forensics is to provide a complete picture of what happened on the network during a security incident. This includes identifying the source of the attack, the techniques used by the attacker, and the impact on the network and systems.

Network forensics is an important tool in identifying and mitigating cyber threats, and is used by security professionals in a variety of settings, including corporate security, law enforcement, and national security agencies.

1.1 **Objective of the Project**

Use any open source software to scan your network and discover everything connected to it, retrieve variety of information about what's connected, what services each host is operating, scan the hostname, list all the hosts in a text file, identify a host's operating system (OS).

1.2 **Description of the Project**

Scanning a network involves the process of examining a network to identify the active hosts, open ports, and running services. This can help identify potential vulnerabilities or security risks that need to be addressed. Network scanning can be performed using various tools, including Nmap.

Nmap (Network Mapper) is a free and open-source tool used for network exploration, security auditing, and network discovery. It is a command-line utility that runs on various operating systems, including Windows, Linux, and macOS.
Nmap can scan networks to determine which hosts and services are running, and can identify operating systems and software versions running on those hosts. This information can be used to identify vulnerabilities that could be exploited by attackers.
Nmap is highly configurable and can perform various types of scans, including ping scans to check if hosts are up, port scans to determine which services are running on hosts, and version detection scans to identify the software versions running on hosts.
Nmap is commonly used by network administrators, security professionals, and penetration testers to discover and secure networks. It is also used by attackers to identify potential targets and vulnerabilities, making it an important tool for both offensive and defensive purposes.

1.3 **Scope of the Project**

The scope of the Nmap project is to provide a free and open-source network exploration and security auditing tool that can be used by network administrators, security professionals, and penetration testers to discover and secure networks.

The Nmap project aims to provide a powerful and flexible tool that can perform various types of scans to identify active hosts, open ports, and running services on a network. It also aims to provide features for advanced network exploration, such as host fingerprinting, OS detection, and service version detection.

In addition to network scanning, the Nmap project also provides features for vulnerability scanning, scripting, and output customization. This allows users to identify potential vulnerabilities and security risks on their networks, as well as automate certain tasks related to network security.

The Nmap project is maintained by a community of developers and security professionals who contribute to its development, testing, and documentation. The project is constantly evolving to keep pace with changes in network security and new technologies.

Overall, the scope of the Nmap project is to provide a powerful and flexible tool that can be used to discover and secure networks, and to contribute to the development and advancement of network security practices.

Chapter 2

System Description

A system description is a document or set of documents that provide a detailed overview of a system, including its purpose, functions, architecture, and components. It is a key part of system design and development, and is used to communicate the system's specifications and requirements to stakeholders, including developers, users, and management.

A system description typically includes the following components:

1. Overview: This section provides an introduction to the system, including its purpose, scope, and objectives.

2. Functional Requirements: This section describes the functions that the system must perform to meet its objectives, and the performance requirements that must be met.

3. Architecture: This section provides an overview of the system's architecture, including its components, interfaces, and data flows.

4. Technical Requirements: This section describes the technical requirements of the system, including hardware, software, and network requirements.

5. Security Requirements: This section describes the security requirements of the system, including access control, authentication, and encryption requirements.

6. Testing Requirements: This section describes the testing requirements for the system, including the types of tests that will be performed, and the acceptance criteria that must be met.

A well-written system description is essential for ensuring that all stakeholders have a clear understanding of the system's requirements, and can help ensure that the system is developed and implemented successfully.

2.1 Target system description

A system description for network scanning using Nmap is a document that provides a detailed overview of the system used to perform network scanning using the Nmap tool. It is used to communicate the system's specifications and requirements to stakeholders, including developers, users, and management.

A system description for network scanning using Nmap typically includes the following components:

- Overview: This section provides an introduction to the system, including its purpose, scope, and objectives.

- Functional Requirements: This section describes the functions that the system must perform to meet its objectives, including the specific types of network scans that will be performed, and the performance requirements that must be met.

- Technical Architecture: This section provides an overview of the system's technical architecture, including the hardware and software components that make up the system.

- Nmap Configuration: This section describes the configuration of the Nmap tool that will be used for network scanning, including the specific command-line options that will be used, and any custom scripts or plugins that will be employed.

- Network Configuration: This section describes the network configuration of the system, including the IP addresses, subnets, and gateway settings that will be used for scanning.

- Testing Requirements: This section describes the testing requirements for the system, including the types of tests that will be performed, and the acceptance criteria that must be met.

By providing a detailed description of the system used for network scanning using Nmap, stakeholders can understand the capabilities and limitations of the system, and can ensure that the system is configured and used in a manner that meets their specific needs and requirements. The system description is a critical component of any network scanning project, and is used to ensure that the project is conducted in a thorough and effective manner.

2.2 Assumption and Dependencies

Assumptions and dependencies for using Nmap include the following:

- Network Access: Nmap assumes that the system conducting the scan has network access to the target network. This means that the system must be connected to the target network, either directly or through a remote access mechanism.
- Administrative Access: Nmap assumes that the system conducting the scan has administrative access to the target network. This is necessary to run scans that require privileged access to network resources.
- Operating System Compatibility: Nmap assumes that the system conducting the scan is compatible with the operating systems of the target network devices. This is important to ensure that the scans are effective and accurate.
- Firewall Configuration: Nmap assumes that the target network does not have any firewalls or other security measures that would prevent or limit access to the network. This is important because firewalls can block Nmap scans and prevent accurate results.
- Network Topology: Nmap assumes that the network topology of the target network is known and understood. This includes knowledge of the IP address ranges, subnet masks, and other network configuration details.

Dependencies for using Nmap include the following:

- Command Line Interface: Nmap is a command-line tool, which means that users must be familiar with command line interfaces in order to use the tool effectively.

- Technical Knowledge: Nmap requires technical knowledge of network protocols, scanning techniques, and security vulnerabilities. Users must be familiar with these concepts in order to use Nmap effectively.
- Data Analysis: Nmap produces large amounts of data, which must be analyzed and interpreted in order to identify security vulnerabilities and other issues. Users must be able to analyze this data effectively to make informed decisions.

By understanding the assumptions and dependencies for using Nmap, users can ensure that the tool is used effectively and accurately to identify security vulnerabilities and other issues on target networks.

Chapter 3

Analysis Report

3.1 Devices connected to network

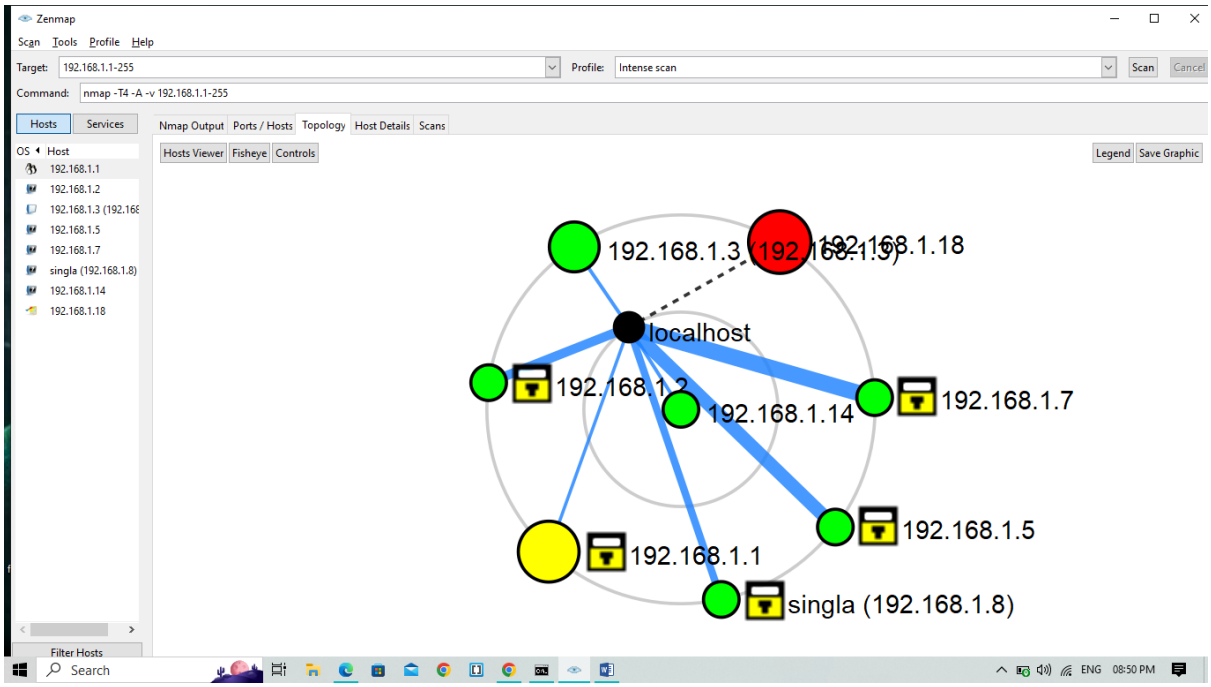

Figure.1 Topology of connected devices to network.

In Figure.1 there is the topology of the devices connected to the local network of my area. At the time of scanning, there are eight (8) devices found to be connected to the network. The IP addresses of each devices are shown above in the topology.

The topology of networks in Nmap can vary depending on the type of network being scanned, as well as the scanning techniques used by the tool. In general, however, the topology of a network in Nmap will include a range of IP addresses, as well as information about which hosts are alive and responsive, which ports are open, and which operating systems are being used. By using this information to build a map of the network topology, users can identify potential security vulnerabilities and other issues, and can take steps to address them.

3.2 List of hosts

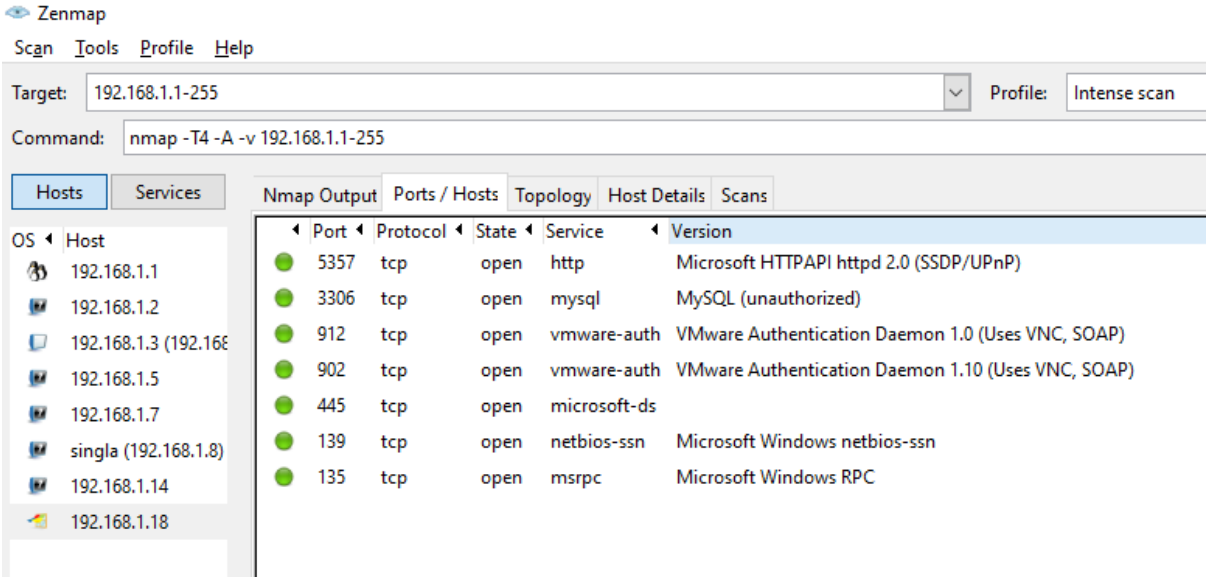

Figure.2 Shows the number of Hosts.

3.3 Scan Output

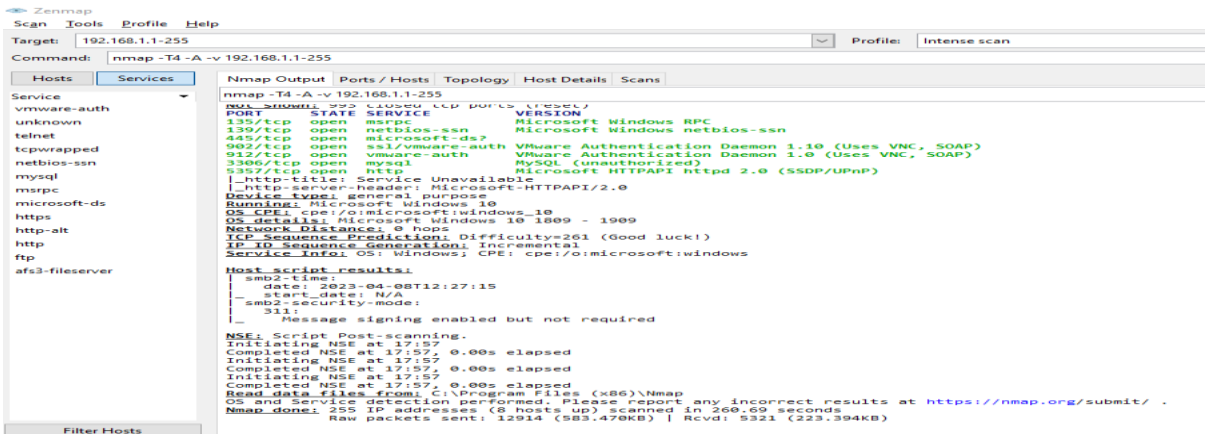

Figure.3 Output of the Deep Scan

In the above figure.3 it shows the details of the deep scan, includes number of hosts, numbers of services like https, ftp, afs3-filesserver, http-alt etc. It also shows the number of ports and the services running

through these ports. Also shows, the device type, OS CPE, OS details, network distance, TCp sequence prediction and service information.

3.4 Hosts and their Services

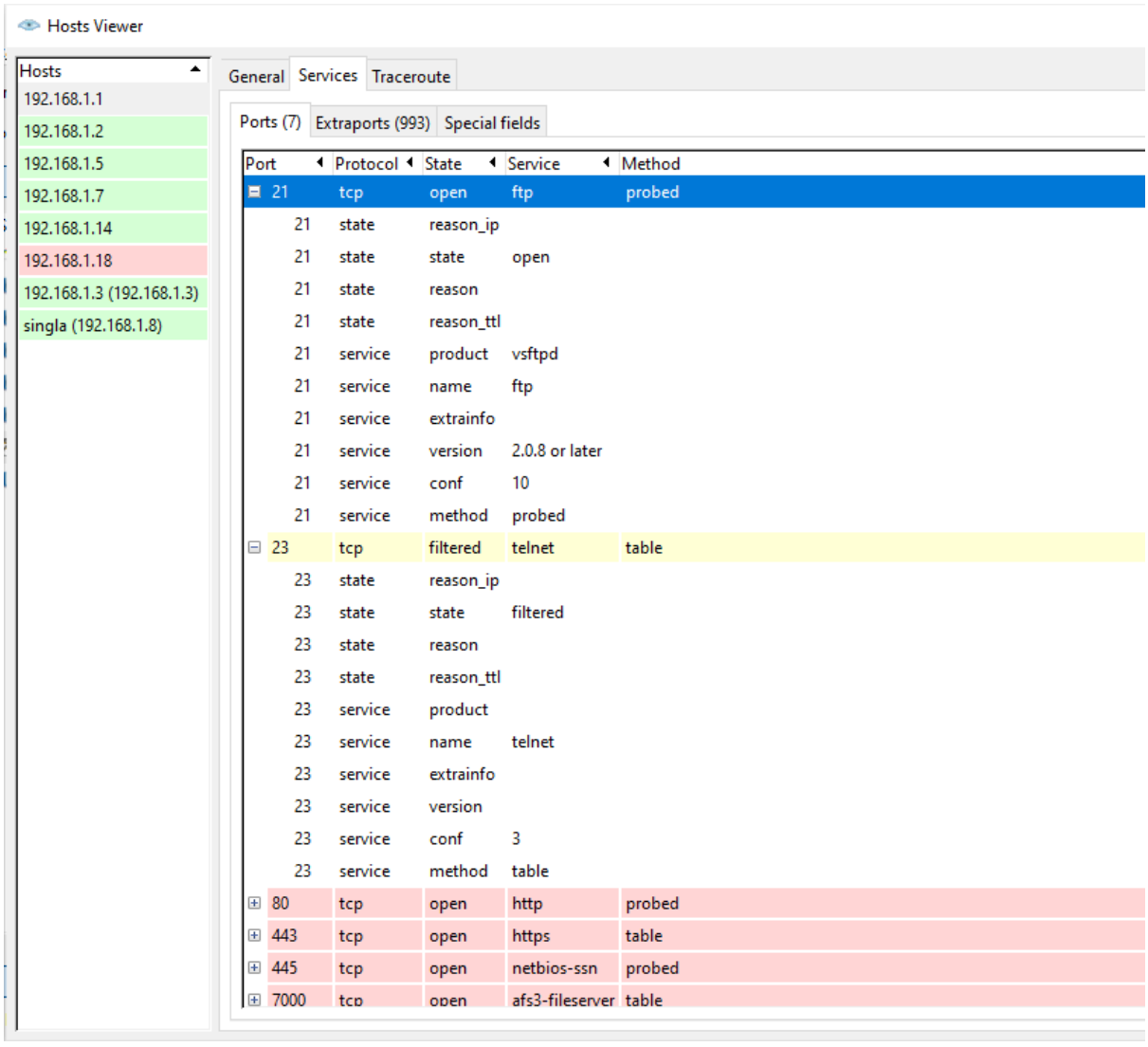

Figure.4 Services provides by the each hosts.

3.5 Host's Operating System

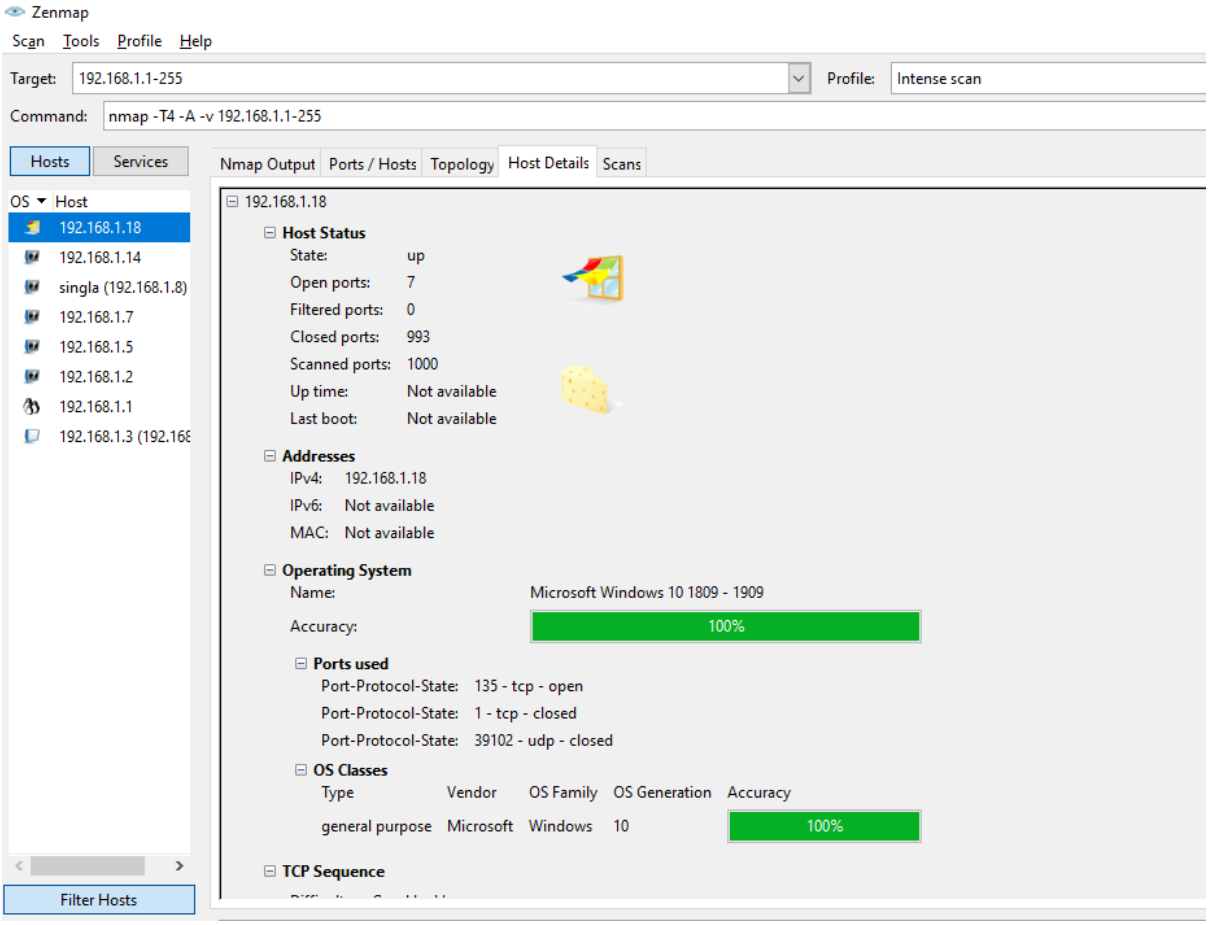

Figure.5 Shows the OS of each Host.

In the above figure.5, it shows the operating system of each hosts with various details like, state of the host, number of open ports, number of scnnned ports, differents addresses IPv4, IPV5, MAC. It also shows the accuracy of predicting the operating system of the host etc.

3.6 Number of Ports of each Host.

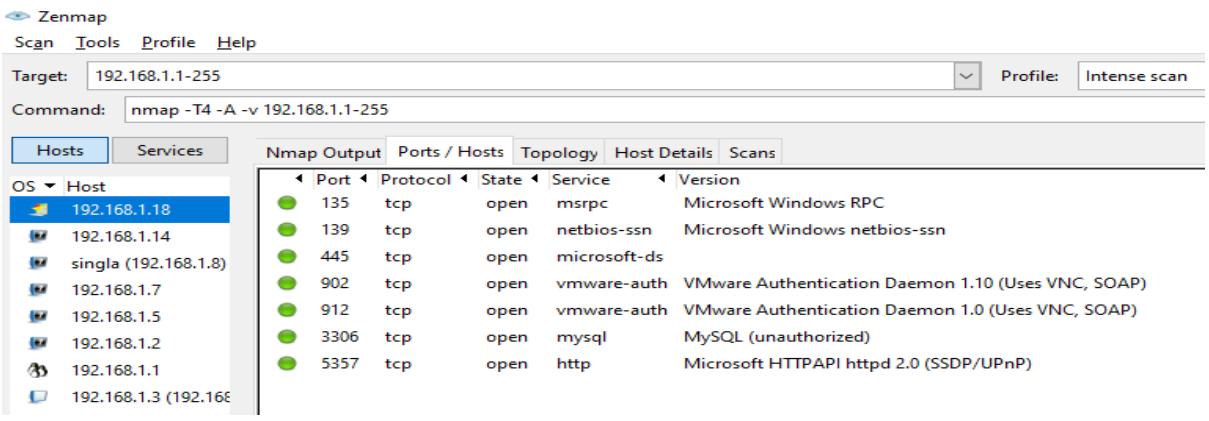

Figure.6 Ports and service of host1.

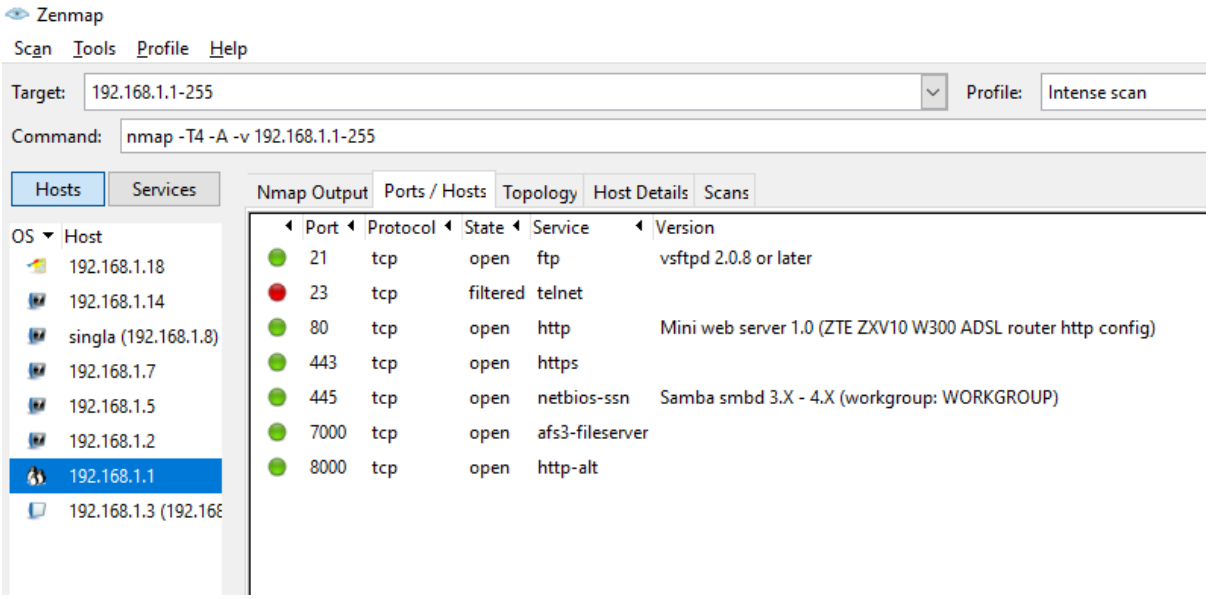

Figure.7 Ports and service of host2.

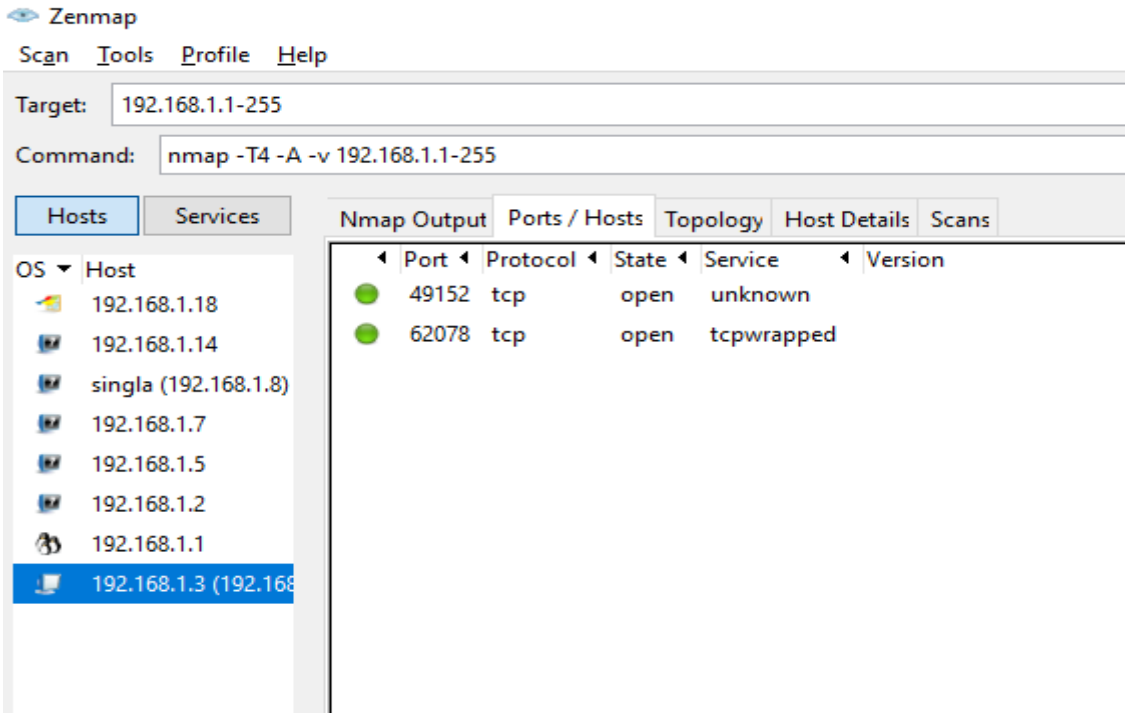

Figure.8 Ports and services of host3.

In the above figure6, figure7 and figure8, shows the number of ports running through each host and number of different services of provided by each hosts. Also shows the state of each port and the protocol used in every services.

3.7 Detail view of Devices Connected

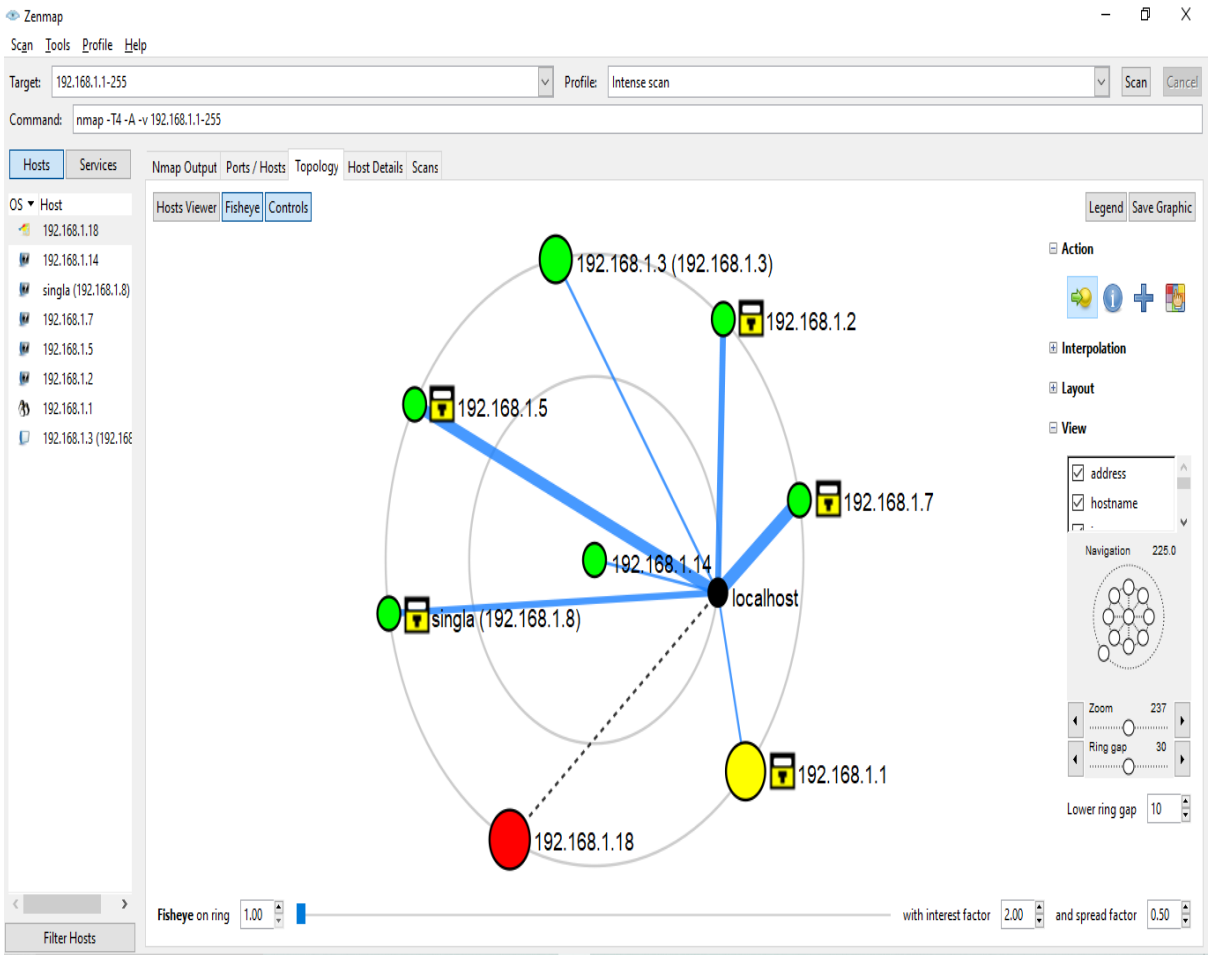

Figure.9 Fisheye view of connected devices.

In the above figure.9, it is the fisheye view of the topology of connected devices through local network at the time of scanning. In this figure.9 we can also notice that wether connected devices are proctected by password or not. It can be easily observe by the lock symbol mention infront of the devices along with their IP addresses.

References/Bibliography

[1]. https://www.techtarget.com/searchsecurity/definition/computer-forensics

[2]. https://www.devry.edu/online-programs/area-of-study/technology/what-is-computer-forensics.html

[3]. https://www.geeksforgeeks.org/introduction-of-computer-forensics/

[4]. https://link.springer.com/article/10.1007/s11896-022-09566-y#:~:text=In%20criminal%20cases%2C%20especially%20based,or%20innocence%20of%20the%20accused.

[5]. https://nmap.org/download.html

[6]. https://www.redhat.com/sysadmin/use-cases-nmap#:~:text=Using%20Nmap,%2Dopen)%2C%20and%20FTP.

[7]. https://www.upguard.com/blog/how-to-use-nmap

[8]. https://en.wikipedia.org/wiki/Nmap

[9]. https://www.dnsstuff.com/network-scanning#:~:text=The%20purpose%20of%20network%20scanning,protect%20the%20network%20from%20attacks.

[10]. https://www.ajer.org/papers/v5(06)/G050603842.pdf

Github-Link

https://github.com/Musheer-Anwar/CA-3-Project