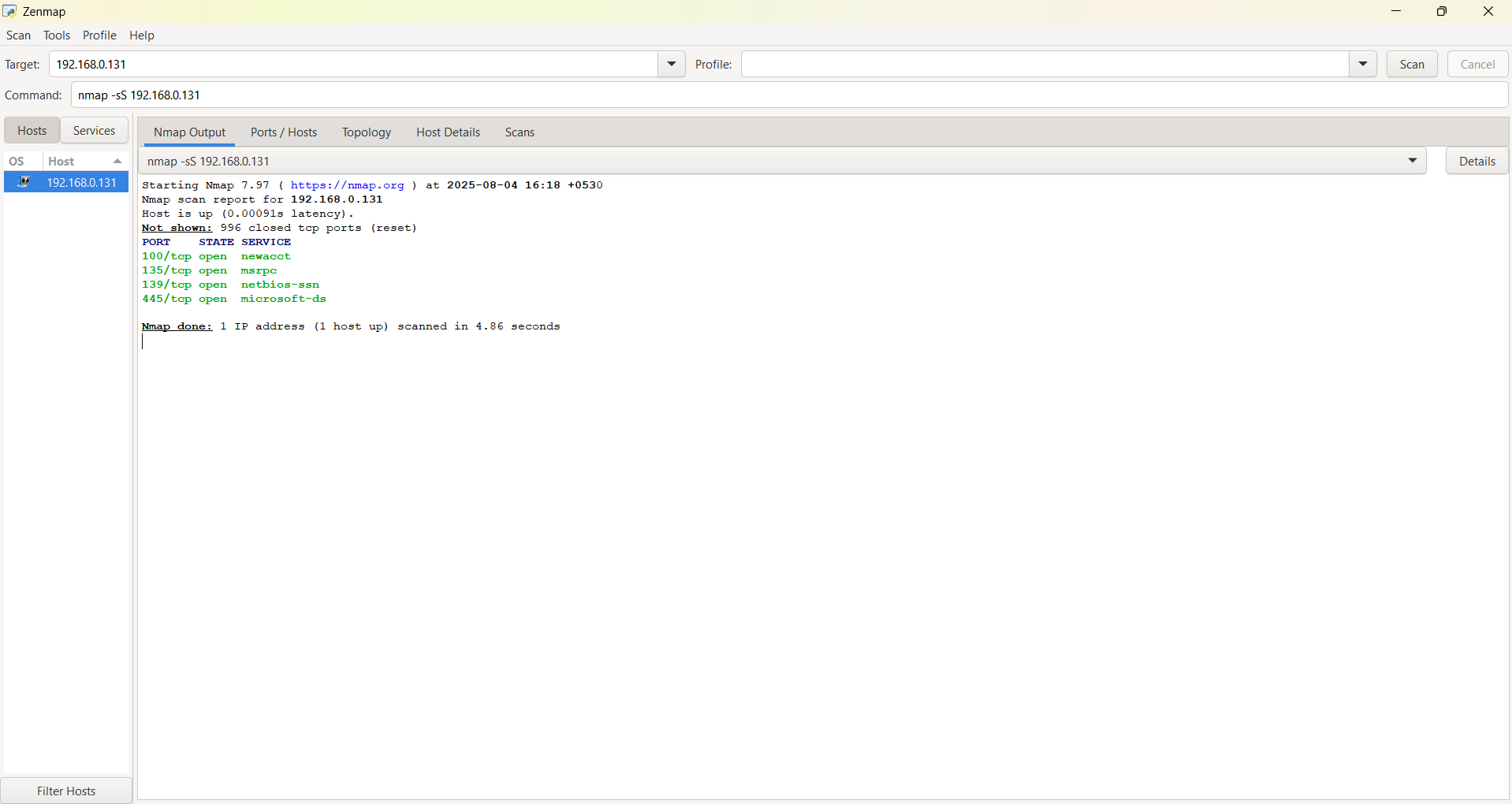
**TASK 1**

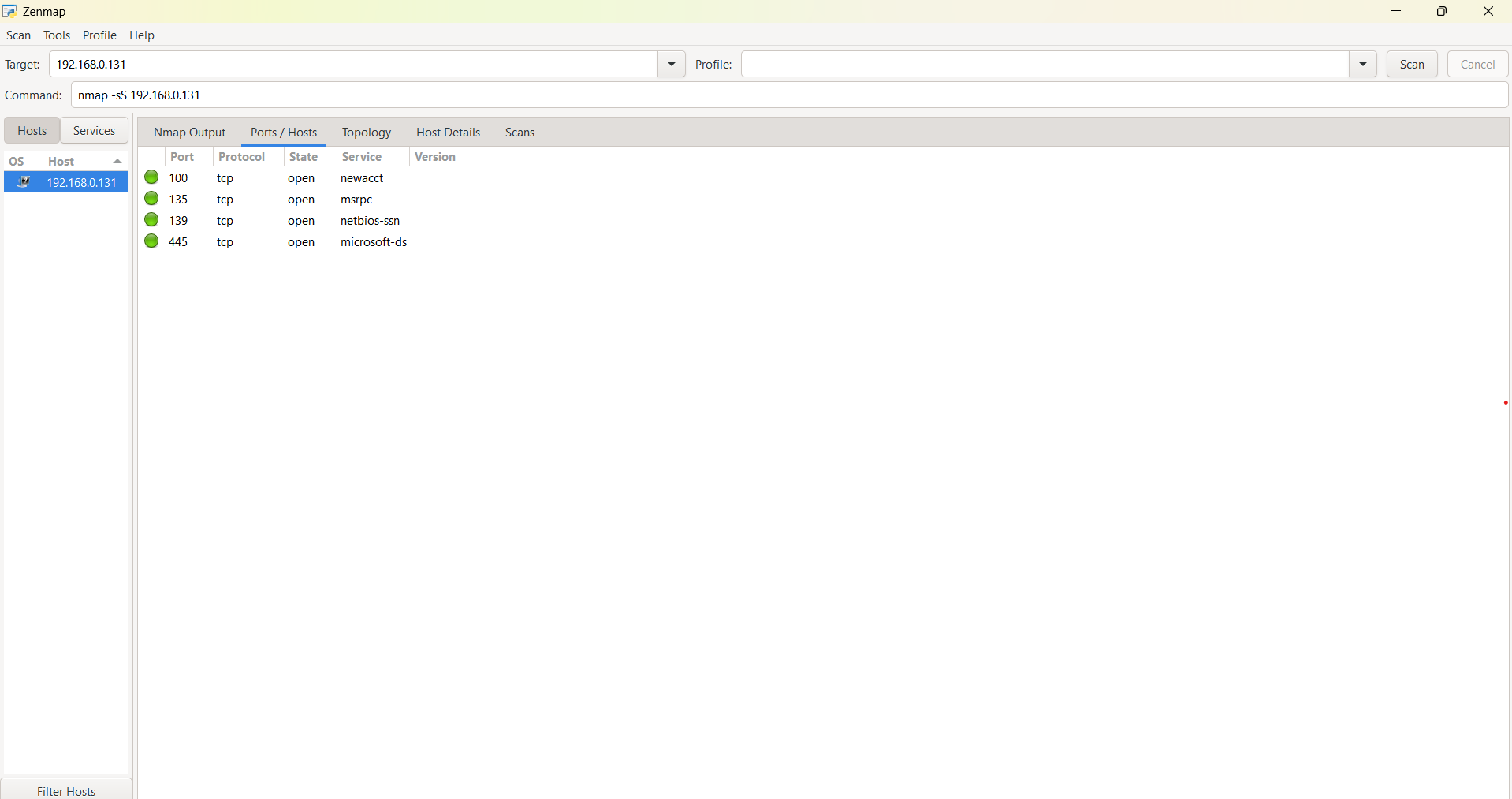
****

The image shows the Zenmap graphical user interface (GUI) for the Nmap network scanner.

Here's a description of what is happening:

* **Tool:** The application is **Zenmap**, a front-end for Nmap.
* **Target:** The user has targeted the IP address 192.168.0.131.
* **Command:** The Nmap command being run is nmap -sS 192.168.0.131. The -sS flag indicates a TCP SYN scan, which is a fast and stealthy type of scan.
* **Scan Report:** The scan report for 192.168.0.131 is displayed.
  + **Host Status:** The report indicates that the host is "up" with a very low latency (0.00019s).
  + **Port Status:** Nmap has identified 996 closed TCP ports. This is a common finding for a host that is not running many services.
  + **Open Ports:** Four ports are listed as open:
    - **Port 100/tcp:** Service is identified as newacct.
    - **Port 135/tcp:** Service is identified as msrpc. This is a common port for Microsoft Remote Procedure Call.
    - **Port 139/tcp:** Service is identified as netbios-ssn. This is a NetBIOS Session Service port.
    - **Port 445/tcp:** Service is identified as microsoft-ds. This is the SMB (Server Message Block) port, often used for file and printer sharing on Windows systems.
* **Duration:** The scan completed in 4.06 seconds.
* **Tabs:** The interface shows several tabs:
  + Hosts
  + Nmap Output (the current tab)
  + Ports / Hosts
  + Topology
  + Host Details
  + Scans

The image depicts a Zenmap scan of a single host (192.168.0.131), revealing that it is online and has four specific TCP ports open, likely indicating it is a Windows machine due to the services (msrpc, netbios-ssn, microsoft-ds) running on those ports.



Based on the Nmap output and general cybersecurity knowledge:

**Port 100:** **Protocol tcp, Service newacct**

* **Description**: Port 100 is a "well-known port". These ports, from 0 to 1023, are typically used by system processes that provide network services. This port is not officially assigned by the Internet Assigned Numbers Authority (IANA). The "newacct" service name is often associated with unauthorized or custom applications. There are no standard, legitimate uses for this port.
* **Protocol**: TCP (Transmission Control Protocol) is a reliable, connection-oriented protocol that ensures data is delivered correctly and in the proper order.
* **State**: The state "open" means that a service on the target device is actively listening for and accepting connections on this port.
* **Service**: The service name "newacct" is what Nmap has identified as running on this port. However, the Nmap service file itself marks this port as "[unauthorized use]". This suggests that "newacct" is not a standard, officially registered service for port 100. In some contexts, "newacct" may be used by specific companies or systems, but it is not a universally defined service.

**Risks and Disadvantages**

The primary risk is that having any open port increases the network's "attack surface". Since the "newacct" service is not a standard service and is noted for "unauthorized use" by Nmap, its purpose and security are unknown, which could be a significant vulnerability. Attackers often target open ports to exploit known vulnerabilities, misconfigurations, or other security flaws in the underlying service. Without knowing what the service is or what it does, you cannot properly assess the security risks.

**Advantages**

There are no known general advantages to having the "newacct" service running on an open port. An open port is only considered an "advantage" if the service it provides is necessary for a device's functionality and is properly secured. Given that this service is not a standard one, its necessity is questionable.

**Port 135: MSRPC (Microsoft Remote Procedure Call)**

* **Description**: Port 135 is used by Microsoft RPC (Remote Procedure Call) services. It acts as an "endpoint mapper," allowing a client device to connect and ask for the port number of a specific RPC service it wants to use. This is essential for remote communication and management in Windows environments, including services like Windows Management Instrumentation (WMI) and Active Directory (AD).
* **Advantages**: This port is crucial for the functionality of Windows networks. It enables remote administration, which is a key component of managing a large number of systems. It is necessary for services like file sharing, printing, and authentication to work properly.
* **Disadvantages & Risks**: MSRPC services, and by extension port 135, have a history of vulnerabilities. If left exposed to the internet, it can be a significant security risk. Attackers can exploit it for:
  + **Malware Exploitation**: Many worms and viruses, such as WannaCry and the Blaster worm, have specifically targeted vulnerabilities in RPC services on port 135 to spread rapidly across networks.
  + **Remote Code Execution (RCE)**: Vulnerable RPC services can be exploited to execute malicious commands on a remote system, giving an attacker unauthorized access.
  + **Denial-of-Service (DDoS)**: Attackers can overwhelm the port with excessive requests, causing a denial of service and system crashes.
  + **Lateral Movement**: Once an attacker compromises one system, they can use port 135 to move laterally and compromise other systems on the network.

**Port 139: NetBIOS-SSN (NetBIOS Session Service)**

* **Description**: This port is associated with the NetBIOS Session Service, which is an older protocol primarily used for file and printer sharing in Windows environments. It allows for connection-oriented communication between two computers and supports the Server Message Block (SMB) protocol. While it has been largely superseded by directly-hosted SMB on port 445, it may still be active on networks with legacy systems or specific configurations.
* **Advantages**: Its primary advantage is enabling file and print sharing on older Windows networks. It provides a way for devices to communicate and share resources using NetBIOS names.
* **Disadvantages & Risks**: Port 139 is a well-known vulnerability and a prime target for attacks when exposed.
  + **Ransomware and Worms**: Ransomware like WannaCry and other worms have historically scanned for and exploited open port 139 to propagate and encrypt files.
  + **Unauthorized Access**: Attackers can exploit the service to gain unauthorized access to file shares, even without credentials.
  + **Information Disclosure**: Unencrypted NetBIOS traffic can be intercepted in a man-in-the-middle attack, allowing an attacker to steal data and credentials.
  + **Legacy Technology**: Since NetBIOS is an older protocol, it has inherent security weaknesses and higher network overhead compared to modern alternatives.

**Port 445: Microsoft-DS (SMB over TCP/IP)**

* **Description**: Port 445 is used by newer versions of the Server Message Block (SMB) protocol for direct TCP/IP communication. Unlike port 139, it does not rely on the older NetBIOS layer. This is the modern standard for file and print sharing in Windows networks, and is a foundational part of intra-network communication.
* **Advantages**: Port 445 is essential for modern Windows file and printer sharing, as well as for remote management tasks. It is more efficient and scalable than the older NetBIOS method on port 139 and can operate over the internet.
* **Disadvantages & Risks**: Despite being the modern standard, port 445 is a high-risk port if not properly secured. Its exposure to the internet is a major security liability.
  + **Ransomware and Malware**: Like port 139, port 445 has been famously exploited by ransomware like WannaCry, which targeted vulnerabilities in SMBv1 to spread.
  + **Remote Code Execution**: Known SMB vulnerabilities can be used for remote code execution and lateral movement within a network.
  + **Information Disclosure and Credential Theft**: Attackers can use SMB relay attacks to steal user credentials.
  + **Lateral Movement**: Attackers can use SMB to move between systems on a network, making a breach more widespread.

To mitigate these risks, it is a best practice to block these ports at the perimeter firewall, especially if they are not needed for external communication. For internal use, ensure that systems are fully patched and services are configured with strong access controls and authentication.