**TASK- 1**

**Basic Network Scanning with Nmap**

* **Port 135 (Microsoft RPC - msrpc):** Port 135 is used by Microsoft’s Remote Procedure Call (RPC) services, which are crucial for network communication between Windows-based systems. This service helps applications communicate across a network or the internet. However, it has a history of being targeted by attackers due to vulnerabilities that can allow remote code execution. For example, the infamous Blaster worm exploited RPC on port 135. On systems where RPC services are not required externally, it is highly recommended to restrict this port using a firewall.
* **Port 139 (NetBIOS Session Service - netbios-ssn):** Port 139 is associated with NetBIOS over TCP/IP, used for Windows file and printer sharing over a local network. It is typically used in older versions of Windows to allow shared access to files and printers. While useful in internal networks, exposing this port to the internet can make the system vulnerable to NetBIOS enumeration and SMB-based attacks. Disabling NetBIOS or filtering this port on public-facing interfaces is considered good practice for securing Windows systems.
* **Port 445 (Microsoft Directory Services - microsoft-ds):** Port 445 is used by the SMB (Server Message Block) protocol to provide shared access to files, printers, and serial ports. It plays a central role in Windows networking. However, it is also one of the most attacked ports due to its association with several critical vulnerabilities, such as EternalBlue, which was used in the WannaCry and NotPetya ransomware outbreaks. For non-enterprise users, it’s strongly advised to block or disable port 445 on systems not requiring it for local network functionality.
* **Port 554 (RTSP - Real-Time Streaming Protocol):**Port 554 typically runs the Real-Time Streaming Protocol (RTSP), used for streaming audio and video media. The presence of this port may suggest that the host is capable of media streaming or is running a camera, media server, or surveillance software. RTSP can also be exploited if not properly secured, especially if default credentials or open access are allowed. Since the version is uncertain in the scan result, further validation is required to confirm its exact usage and ensure no unauthorized streaming service is enabled.
* **Port 2869 (Microsoft HTTPAPI httpd 2.0):** This port is commonly used for the Universal Plug and Play (UPnP) framework on Windows. UPnP allows devices like printers, routers, or other IoT systems to automatically discover and communicate with each other. The HTTPAPI httpd 2.0 service indicates that the system is running a mini web server for UPnP-related communication. While convenient for home networking, UPnP has been criticized for security issues and should be disabled or restricted in sensitive or enterprise environments to avoid unauthorized access.
* **Port 5357 (Microsoft HTTPAPI httpd 2.0):** Similar to port 2869, port 5357 is also used for UPnP and Web Services for Devices (WSD) on Windows platforms. It allows device discovery and service announcements across the network. Attackers have exploited these ports in the past to perform local network reconnaissance. If the device is not actively using this functionality, disabling it reduces unnecessary network exposure and prevents potential misuse by malicious actors or malware inside the network.
* **Port 10243 (Microsoft HTTPAPI httpd 2.0):** Port 10243 is another port linked with UPnP and used by the "HomeGroup Listener" service in Windows. It allows systems to communicate and share files within a trusted home network group. However, this feature is largely deprecated in newer Windows versions and can be safely disabled on many systems. Keeping it open unnecessarily might give attackers another entry point for lateral movement within a local network.
* **Port 5040 (Unknown Service - Possibly VirtualBox Virtual NIC):** Port 5040 did not return a recognizable service or version, but based on the device MAC vendor (PCS Systemtechnik GmbH), it is likely associated with virtualization software like Oracle VirtualBox. This may be a virtual NIC (network interface card) or a local service related to virtualization features. Even though it may be harmless, unknown services should be examined closely. It is advised to investigate further using manual banner grabbing or deeper scans to ensure this port is not exposing sensitive services.