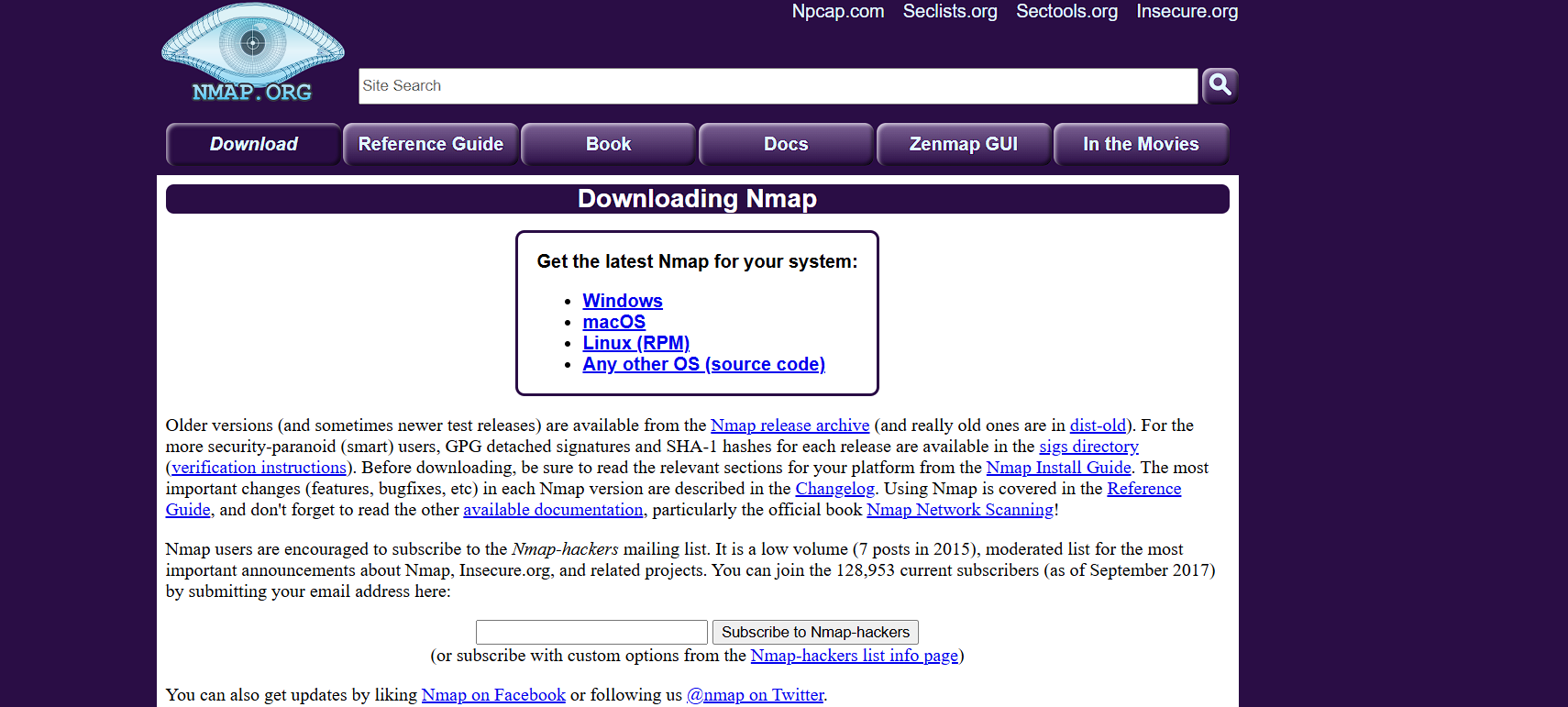
DAY-1 TASK

NMAP SCAN



A screenshot of a computer

AI-generated content may be incorrect.

A screen shot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

|  |  |  |  |
| --- | --- | --- | --- |
| **Port** | **Protocol** | **Service** | **Description** |
| 135 | TCP | MS RPC | Common Windows RPC service, used by DCOM |
| 139 | TCP | NetBIOS-SSN | NetBIOS session service (file sharing) |
| 445 | TCP | Microsoft-DS | SMB over TCP – used for Windows shares |
| 9013 | TCP | Unknown | Likely custom/third-party service |
| 49670 | TCP | Dynamic Port | Windows ephemeral port (high-range) |
| 49666 | TCP | Dynamic Port | Likely related to system or RPC services |
| 49664 | TCP | Dynamic Port | Possibly RPC/DCOM or WMI |
| 49671 | TCP | Dynamic Port | Dynamic/private service |
| 49665 | TCP | Dynamic Port | Ephemeral (used by RPC/WMI) |
| 49663 | TCP | Dynamic Port | Same as above |
| 7680 | TCP | Delivery Optimization | Windows Update file sharing |
| 502 | TCP | Modbus | Common in ICS/SCADA (if detected, unusual) |
| 49152 | TCP | Dynamic Port | RPC/Ephemeral port (Windows) |
| 49672 | TCP | Dynamic Port | Ephemeral, possibly RPC |
| 49667 | TCP | Dynamic Port | Ephemeral |

Security Risk Assessment

1. **Ports 135, 139, 445 (Windows Services and File Sharing):**  
   These ports are used for communication between Windows computers. But if they are open to unknown networks (like the internet), they can be very dangerous. Hackers have used these in the past to spread viruses like WannaCry
2. **Ports in the 49600+ range and 49152 (Temporary Ports):**  
   These are temporary ports used by Windows to run services. They are usually safe inside your network, but attackers can use them to move from one system to another if they get in.
3. **Port 7680 (Windows Update Sharing):**  
   This port lets your computer share Windows updates with others, like a peer-to-peer system. While it helps save internet data, it may expose your system.

**Security Recommendations**

Firewall Restrictions

Disable Unused Services

Audit Unknown Services

Update WebSocket Library

Harden Windows Host

interview

**1. What is an open port?**

An open port is simply a door that allows data to flow into or out of a device over a network. If a service or application is running on your system (like a web server or file sharing), it needs a port to communicate. So, when a port is open, it means something is actively listening on that port and ready to connect with other systems. While open ports are needed for communication, they can also expose systems to risks if not managed properly.

**How does Nmap perform a TCP SYN scan?**

Nmap uses a clever trick called a TCP SYN scan to check if ports are open. It sends a SYN (synchronization) packet to the target, which is the first step in a normal TCP handshake. If the target replies with a SYN-ACK, Nmap knows the port is open. But instead of finishing the handshake, Nmap stops right there by sending a reset (RST), which means the connection was never fully established. This makes the scan faster and less likely to be noticed by the system.

**What risks are associated with open ports?**

Open ports can be useful, but they also create opportunities for attackers. If a port is open and running an outdated or vulnerable service, a hacker could exploit it to break into the system. Even unused open ports can be risky because they could be accidentally misconfigured or used as a backdoor. That’s why it’s important to keep only the necessary ports open and secure the services behind them.

**What is the difference between TCP and UDP scanning?**

The main difference lies in how the two protocols work.  
**TCP scanning** involves a handshake—it checks if the other side wants to talk by going through a connection process. It’s more reliable because you get clear responses.  
**UDP scanning**, on the other hand, is more unpredictable. Since UDP doesn’t need a handshake, you might not get any response at all, even if the port is open. That makes UDP scans slower and harder to interpret, but sometimes necessary for services that only use UDP (like DNS or DHCP).

**. How can open ports be secured?**

To secure open ports, the first step is to close the ones that aren’t needed. For the ones that must stay open, it’s important to use firewalls to control who can access them. You should also make sure the services running on those ports are updated and properly configured. Monitoring tools and regular scans can help spot anything unusual, and techniques like VPNs or port knocking can add extra layers of security.

**What is a firewall’s role regarding ports?**

A firewall works like a security guard—it decides which ports are allowed to communicate and which aren’t. It can block or allow traffic based on rules, like only allowing a certain port from a trusted IP address. For example, if port 22 (SSH) is open, a firewall can make sure only the system admin’s device can access it. This helps prevent unwanted or harmful traffic from getting in or out.

**What is a port scan and why do attackers perform it?**

A port scan is like knocking on all the doors of a house to see which ones are open. Attackers use it to find out which ports are open and what services are running behind them. Once they know that, they can plan their next steps—like looking for weaknesses or trying to exploit known vulnerabilities. But it’s not just attackers—ethical hackers and security professionals also use port scans to test and secure networks.

**How does Wireshark complement port scanning?**

While tools like Nmap show you which ports are open, Wireshark goes deeper and shows you what’s actually happening on those ports. It captures real network traffic so you can see which data is flowing in and out. This helps you confirm if a service is behaving normally or if something suspicious is going on. Together, Nmap and Wireshark give a complete picture—Nmap tells you what’s exposed, and Wireshark tells you what’s really happening.