***Team no :*  2.13**

**Date:21-06-23**

**Team members:**

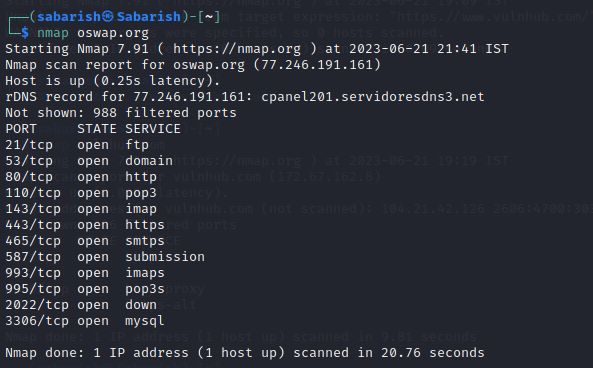
Yerramsetty Sai Naga Sabarish-20BCE2370

Jayasree N -20MIS0370

Satya Harika- 20BKT0131

Nikitha AR-20MIA1025

**TARGET WEBSITE:** Owasp.org



**OPEN PORTS:**

1. **FTP:** FTP (File Transfer Protocol) is a standard network protocol used for transferring files between a client and a server on a computer network. By default, FTP uses two ports:

* port 21 for control and port 20 for data transfer. Here are the details of these two ports:Port 21 (Control Port): This port is used for sending commands and receiving responses between the FTP client and server. It handles the control flow of the FTP session, including authentication, file listing, and commands for file transfer.
* Port 20 (Data Transfer Port): This port is used for the actual transfer of data files between the FTP client and server. When a file transfer request is made, the data channel is established on port 20 to transfer the file content.

1. **HTTP** (Hypertext Transfer Protocol) is the primary protocol used for transmitting data over the World Wide Web. It operates over TCP (Transmission Control Protocol) and typically uses port 80 for communication. Here are the details of an open HTTP port:

* Port 80 (Default HTTP Port): This port is the default port for serving HTTP traffic. When a client makes an HTTP request to a server, it establishes a connection on port 80 to send the request and receive the response. The server listens on this port for incoming HTTP connections.

1. **Pop3** (Post office protocol version 3),which is a widely used Internet protocol that email clients utilise to get email from a mail server. Users can download their email from the server to local devices using this TCP/IP-based system.

* Port 110 (Default Pop3 port): This is associated with the Post Office Protocol version 3 (POP3), used for email retrieval from a mail server. It operates over TCP/IP and listens for incoming POP3 requests. While considered an older email protocol, it may still be used by some mail servers and clients for accessing email messages.

1. **IMAPS** (Internet Message Access Protocol over SSL) is a secure protocol used for retrieving email messages from a remote mail server. It operates over TCP and typically uses port 993 for communication. Here are the details of an open IMAPS port:

* Port 993 (Default IMAPS Port): This port is the default port for establishing a secure IMAP connection using SSL/TLS encryption. When a client connects to an email server over IMAPS, it establishes a connection on port 993 to securely retrieve email messages.

1. **SMTPS** (Simple Mail Transfer Protocol Secure) is a secure version of the SMTP protocol used for sending email messages. It operates over TCP and typically uses port 465 for communication. Here are the details of an open SMTPS port:

* Port 465 (Default SMTPS Port): This port is the default port for establishing a secure SMTP connection using SSL/TLS encryption. When a client wants to send an email using SMTPS, it establishes a connection on port 465 to securely communicate with the mail server.SMTPS provides enhanced security by encrypting the communication between the email client and the mail server, protecting the integrity and confidentiality of the email content, as well as any sensitive information, such as usernames and passwords.

1. **Submission port** is an alternative SMTP (Simple Mail Transfer Protocol) port used for email submission by mail clients. It is primarily designed for email clients to send outgoing mail to mail servers.

* Port 587 is commonly used with encryption and authentication mechanisms, ensuring secure transmission of email messages. It helps prevent issues related to ISP blocking of port 25, the default SMTP port.

1. **Pop3s** (Post Office Protocol version 3 Secure) is an extension of POP3 that adds encryption and security features to the protocol. It operates over a secure SSL/TLS connection.

* Port 995: It is commonly used for retrieving email messages securely from a mail server. By default, POP3 over port 995 ensures that data transmitted between the mail client and server is encrypted, adding an extra layer of security.

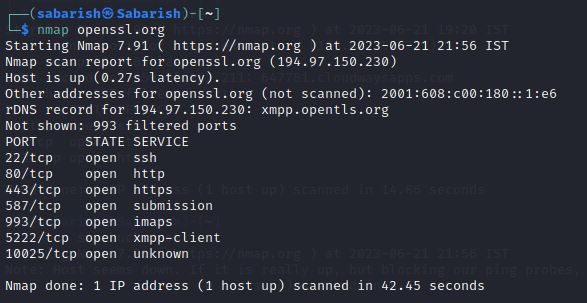
1. **Down :** When a port is reported as "down," it means that there is no service actively listening on that port.

* Port 2022: An open port status on port 2022 may indicate that there is no service running or listening on that specific port. This could be intentional, as the port might be unused or reserved for future use, or it could be due to a misconfiguration or firewall blocking the port.

1. **Mysql: It** is typically associated with the MySQL database management system. It allows communication between clients and the MySQL server for database operations. It's crucial to secure this port by implementing proper authentication mechanisms and firewall rules to protect against unauthorized access and potential vulnerabilities. Regular security updates and best practices should be followed to ensure the integrity and confidentiality of the MySQL database.

* Port 3306 is commonly used for MySQL, a popular open-source database management system.It's important to secure this port to prevent unauthorized access and protect the confidentiality and integrity of the database.

**MAIN WEBSITE** : Openssl.org



**OPEN PORTS:**

1. **SSH** (Secure Shell) is a secure network protocol used for establishing encrypted connections and providing secure remote access to systems. It operates over TCP and typically uses port 22 for communication. Here are the details of an open SSH port:

* Port 22 (Default SSH Port): This port is the default port for establishing SSH connections. When a client wants to connect to a remote system using SSH, it establishes a connection on port 22 to securely communicate with the SSH server.
* SSH provides strong encryption and authentication mechanisms, ensuring the confidentiality and integrity of data transmitted between the client and the server. It allows users to securely log into remote systems, execute commands, transfer files, and perform other administrative tasks.

1. **The Submission port,** also known as the "Message Submission Agent" (MSA) port, is used for email submission by mail clients to a mail server. It operates over TCP and typically uses port 587 for communication. Here are the details of an open Submission port:

* Port 587 (Default Submission Port): This port is the default port for email submission. When a mail client wants to submit an email message to a mail server for delivery, it establishes a connection on port 587 to communicate with the server.
* The Submission port is designed to provide a secure and authenticated method for mail clients to submit outgoing email messages to the mail server. It is often used in scenarios where the mail client is outside the local network or when the standard SMTP port 25 is blocked or restricted.

1. **Xmpp-client** (Extensible Messaging and Presence Protocol) :This is used for encrypted communication with the XMPP server. An open port for XMPP client enables communication between clients and servers using the XMPP protocol, facilitating instant messaging, presence information, and other real-time communication features.

* Port 5222 is an open technology for real-time communication. It is used for instant messaging, presence information, and establishing client-server connections for various applications. Port 5222 is the default port for XMPP client-to-server connections, providing secure and encrypted communication for XMPP-based services.

1. **Unknown :** An open port with an unknown service running can indicate a potential security concern or a misconfiguration. It is essential to investigate and identify the service running on the port to determine its purpose and assess any associated risks. Further analysis and network monitoring may be required to ensure the security and integrity of the system.

* Port 10025 is commonly associated with the Simple Mail Transfer Protocol (SMTP) submission. It is used for email submission from email clients to mail servers. It operates over TCP/IP and provides a secure and authenticated method for sending outgoing email messages. It is often used in conjunction with port 587 for email submission.