**WEB APPLICATION PENTESTING**

**GROUP – 2.10**

MEMBERS OF GROUP

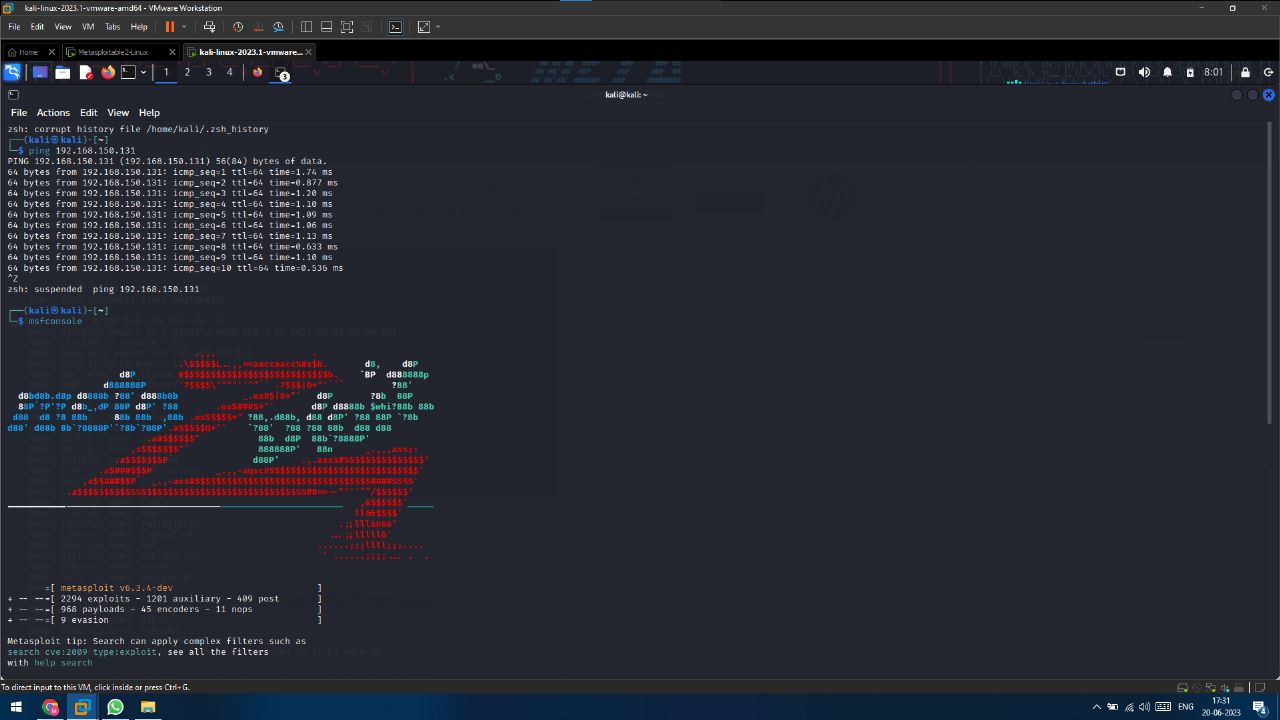
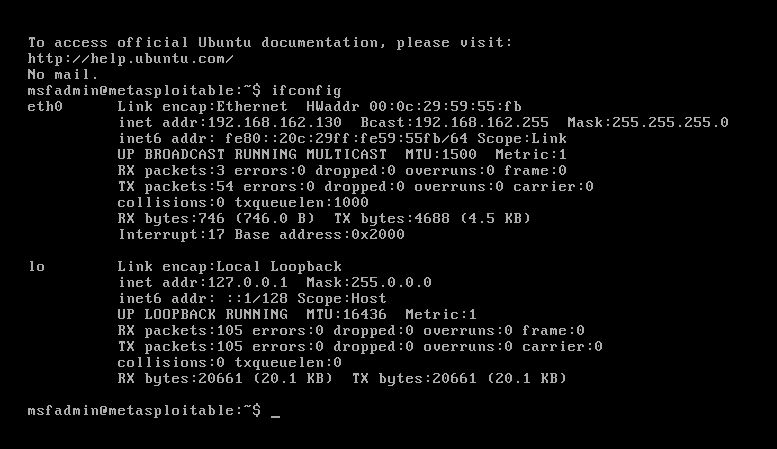
MALLA SRIRAJ – 20BCN7117

MALLIDI VISWA TEJA REDDY – 20BCN7022

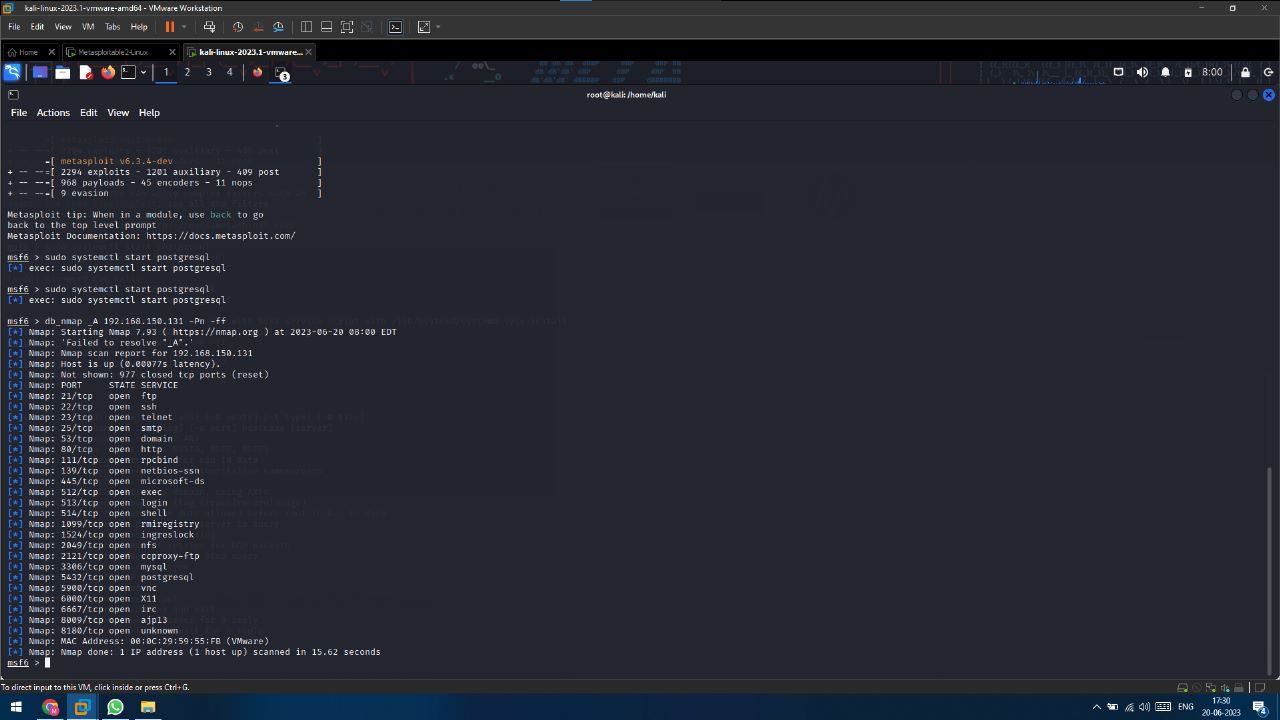
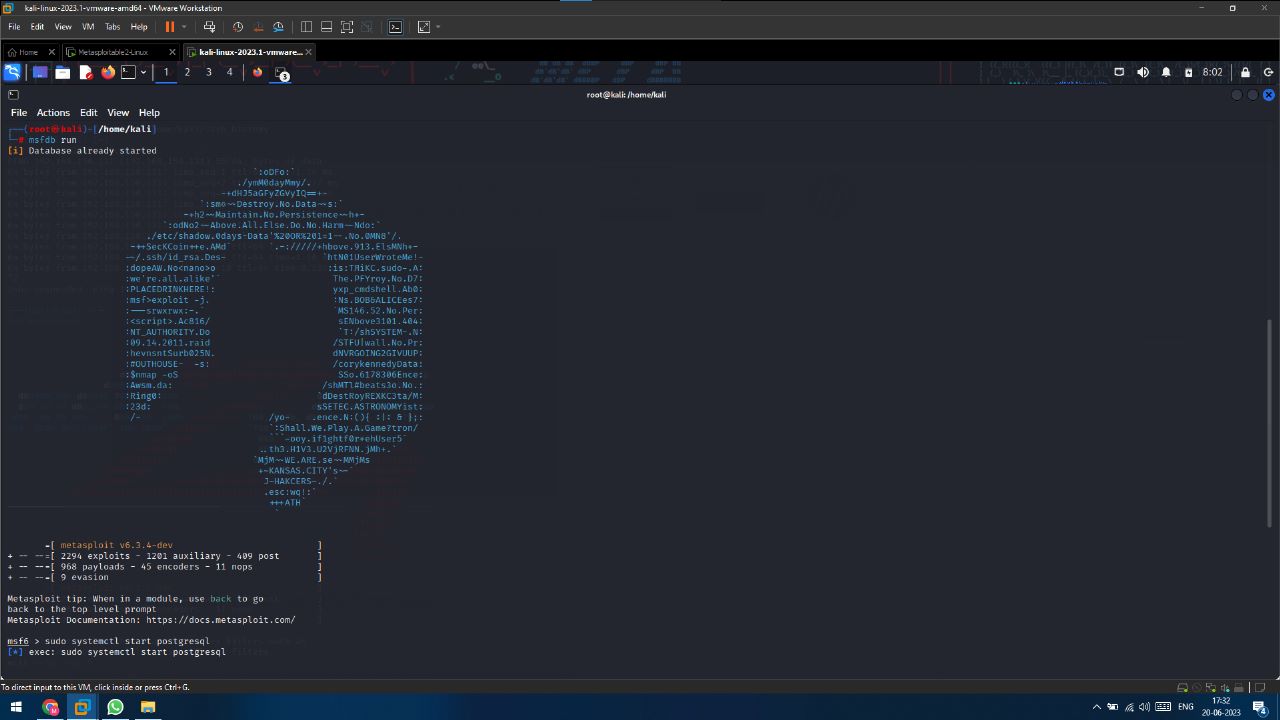
J V S MANIDEEP – 20BCN7164

PRANAV DATT – 20BCE2722

**METASPLOITABLE**:



OPEN PORTS:



**Port number 21** is commonly associated with the File Transfer Protocol (FTP), a standard network protocol used for transferring files between a client and a server. When a server listens on port 21, it indicates that it is running an FTP server and is ready to accept incoming FTP connections. FTP relies on a control connection established on port 21, through which commands and responses between the client and server are exchanged. The actual file transfers occur over a separate data connection on dynamically allocated ports. While port 21 is the default for FTP, alternative ports can be used. It's important to exercise caution when opening port 21 or any other port, as it can introduce security risks. Secure alternatives like FTPS or SFTP are recommended for enhanced security.

**Port number 22** is associated with the Secure Shell (SSH) protocol, which is widely used for secure remote administration and file transfers. When a server listens on port 22, it signifies that it is running an SSH server and ready to accept incoming SSH connections. SSH establishes a secure encrypted channel between a client and server, ensuring confidential communication and secure remote access. Port 22 allows users to securely log into remote systems and execute commands remotely. However, it is important to implement strong security measures to protect against potential unauthorized access, as port 22 is a common target for hackers. By following best practices, opening port 22 can provide convenient and secure remote access to systems for effective administration and file transfers.

**Port number 23** is commonly associated with the Telnet protocol, which enables remote terminal access and command-line control of a remote computer. When a server listens on port 23, it indicates that it is running a Telnet server and ready to accept incoming Telnet connections. However, Telnet poses significant security risks as it transmits data and commands in plain text, making it vulnerable to eavesdropping and unauthorized access. Consequently, the use of Telnet has diminished in favor of more secure alternatives like SSH (Secure Shell) that operate on port 22. It is advisable to keep port 23 closed or limited to controlled environments with appropriate security measures to mitigate the risks associated with plaintext transmission.

**Port number 111** is commonly associated with the Remote Procedure Call (RPC) protocol. When a server listens on port 111, it indicates that it is running an RPC server and ready to handle incoming RPC requests. RPC enables programs on different computers to communicate and share resources over a network, allowing the execution of procedures on remote systems. However, it is important to note that RPC implementations have historically had vulnerabilities, making them potential targets for attackers. Therefore, maintaining the security of RPC servers is crucial, involving regular updates, proper configurations, and security measures such as firewall rules and access restrictions. Exposing port 111 without necessary precautions can expose systems to potential risks, so it's important to be vigilant and follow best practices to safeguard against unauthorized access and potential security threats.

**Port number 139** is commonly associated with the NetBIOS Session Service, which facilitates file and printer sharing on Windows networks. When a server listens on port 139, it signifies that it is running the NetBIOS Session Service and ready to establish NetBIOS connections. However, port 139 and the associated NetBIOS protocol have well-known security vulnerabilities and are susceptible to attacks. As a result, it is recommended to disable or block port 139 in modern network environments. The use of port 445, which is associated with the more secure Server Message Block (SMB) protocol, is preferred for file and printer sharing. If port 139 must remain open for specific legacy applications, it is essential to implement robust security measures, including firewalls, access controls, and regular updates, to mitigate potential risks and safeguard against unauthorized access and potential security threats.

**Port number 445** is associated with the Server Message Block (SMB) protocol, which enables file and printer sharing on Windows networks. When a server listens on port 445, it indicates that it is running an SMB server and is ready to accept incoming SMB connections. SMB facilitates seamless access to shared files, directories, and printers on a network. Over the years, SMB has undergone improvements to address security concerns and enhance functionality. Modern implementations, like SMB version 3, incorporate stronger security features such as encryption, signing, and authentication mechanisms to safeguard against unauthorized access and data interception. However, it is important to be vigilant as port 445 has been targeted by malware in the past. To mitigate potential risks, it is crucial to implement robust security measures such as firewalls, access controls, and regular updates. By adopting proper security practices, organizations can ensure the integrity and security of their file and printer sharing services while leveraging the capabilities provided by port 445.

**Port number 1099** is commonly used for the Java Remote Method Invocation (RMI) registry. When a server is configured to listen on port 1099, it signifies that an RMI registry is running and prepared to handle incoming RMI requests. RMI is a feature in Java that allows different Java Virtual Machines (JVMs) to communicate with one another over a network. The RMI registry acts as a central repository for remote Java objects, enabling clients to locate and invoke methods on these objects. By opening port 1099, the RMI registry can receive and respond to remote method invocation requests. It is important, however, to exercise caution when opening this port, as it could expose vulnerabilities if not properly secured. Implementing appropriate security measures, such as authentication, encryption, and access controls, is essential to protect against unauthorized access or potential exploits. By adhering to best practices, opening port 1099 for the RMI registry can facilitate efficient communication between Java applications while ensuring the overall security of the network environment.

**Port number 2121** does not have a well-known or standardized service associated with it. Its usage can vary depending on the specific configuration or application in which it is employed. In some cases, it may be utilized as an alternative port for the File Transfer Protocol (FTP) control connection when the default port 21 is unavailable. However, the use of port 2121 for FTP is not widely recognized or supported by all FTP clients and servers. Additionally, other custom or proprietary applications may also use port 2121 for their specific communication needs. If you encounter an open port 2121 on a network, it is important to investigate and determine the specific application or service utilizing it to ensure it aligns with your intended usage and security considerations.

**Port number 8180** does not have a designated standard service associated with it. However, it is commonly used as an alternative or custom port for web applications. In particular, port 8180 is often employed as an HTTP or HTTPS port for hosting web services. It can be chosen to avoid conflicts with the default ports (80 for HTTP and 443 for HTTPS) or as a specific configuration choice for a particular web application. If you come across an open port 8180, it is important to investigate further to determine the specific web application or service utilizing it. This will help ensure that the usage aligns with your intended purpose and that appropriate security measures are in place to protect the application and its data.