Password Cracking with Hydra

Introduction:

Hydra is a powerful tool used in cybersecurity for password cracking, specifically for performing brute-force attacks on various protocols and services. A brute-force attack is a method where a computer tries numerous combinations of passwords until it finds the correct one.

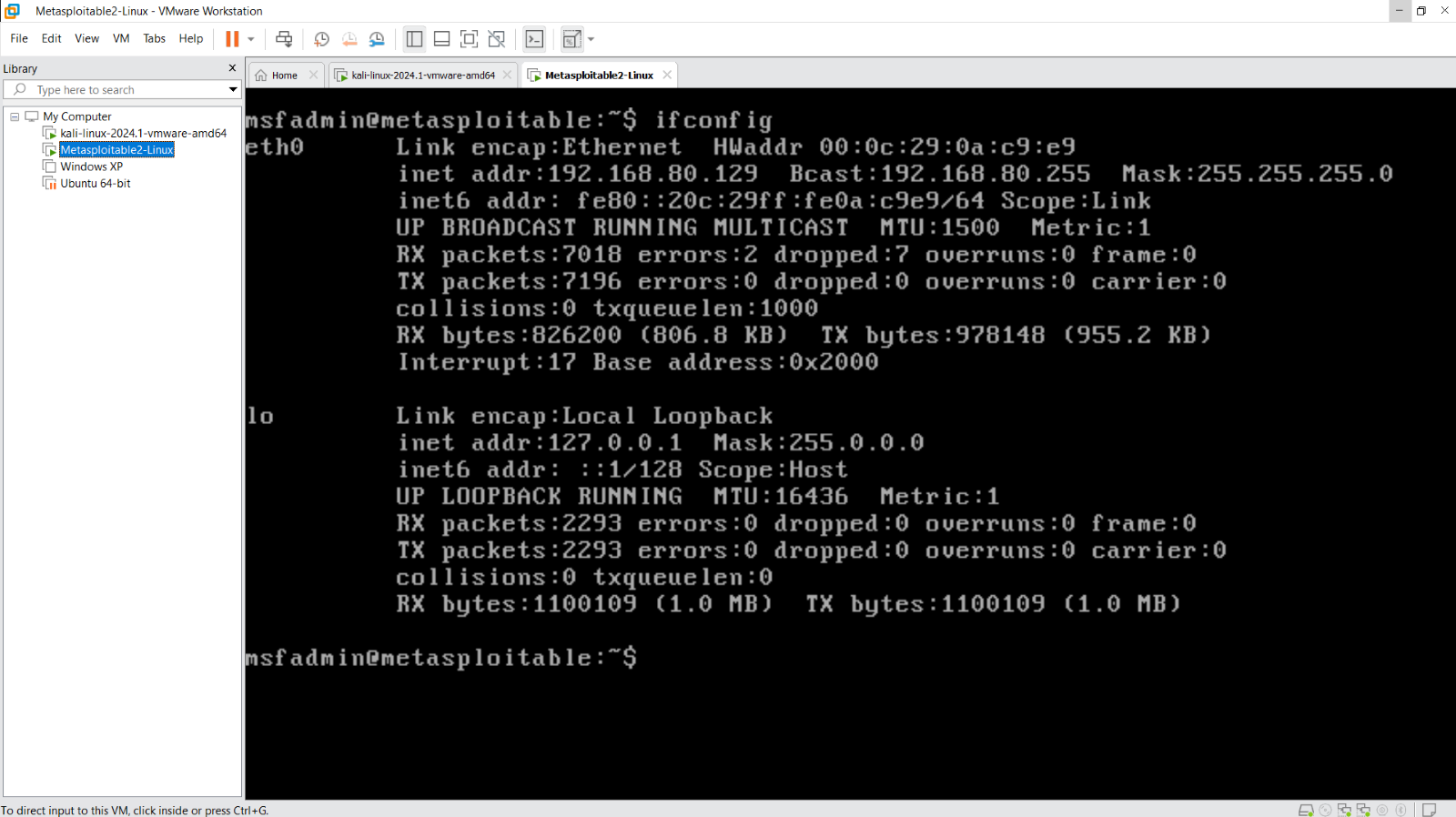
Hydra works by systematically trying different passwords from a list (called a wordlist) against a login interface, such as SSH, FTP, or a web form. If the correct password is in the list, Hydra will eventually find it and gain access to the targeted account.

Here's a basic overview of how Hydra works:

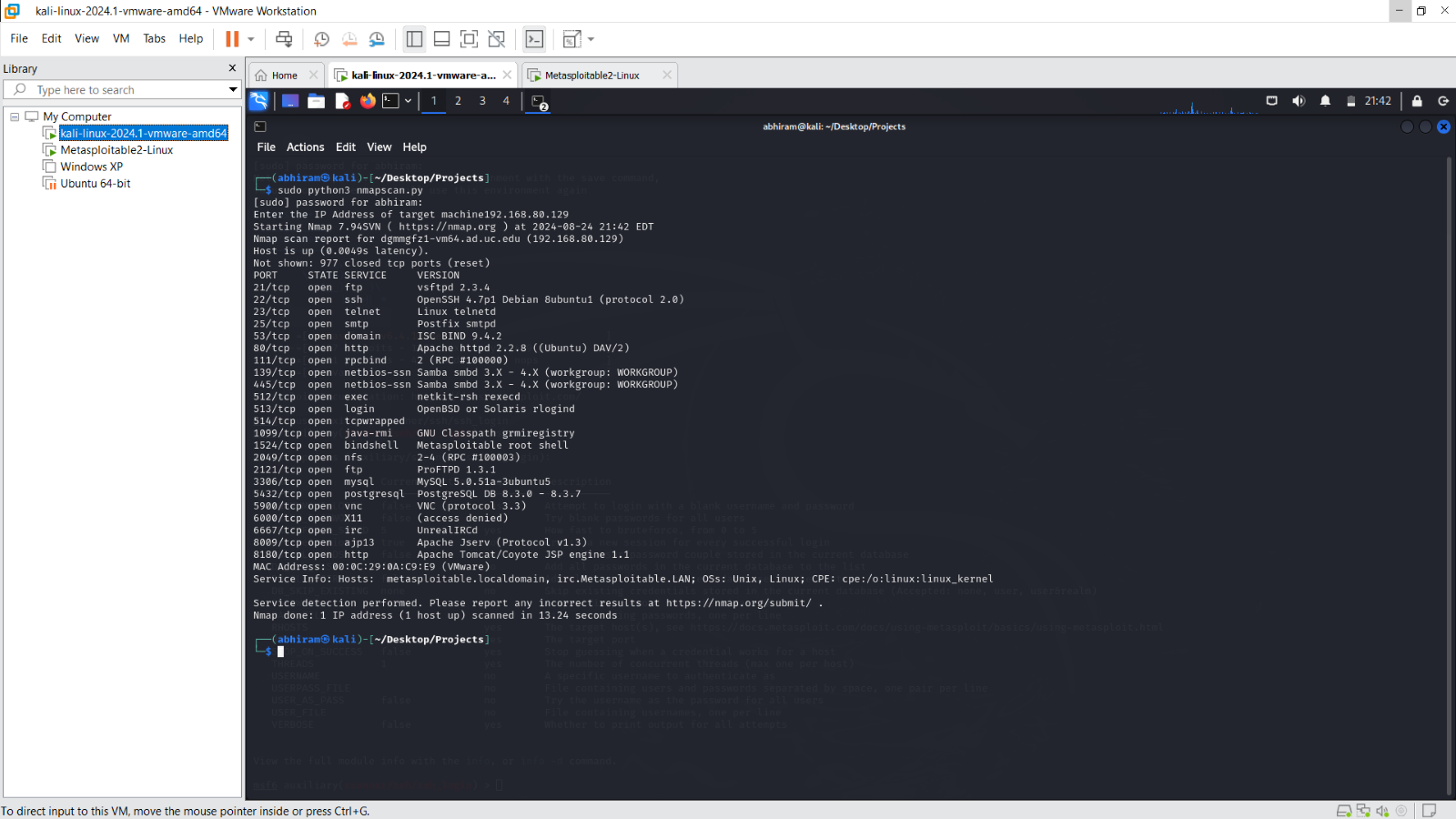
1. **Select Target**: Identify the service or protocol you want to attack (e.g., SSH, FTP, HTTP).
2. **Choose Wordlist**: Use a list of potential passwords that Hydra will try. This list can be customized or chosen from pre-existing ones.
3. **Run Hydra**: Hydra systematically tries each password in the list against the target until it finds a match or exhausts the list.

Steps:

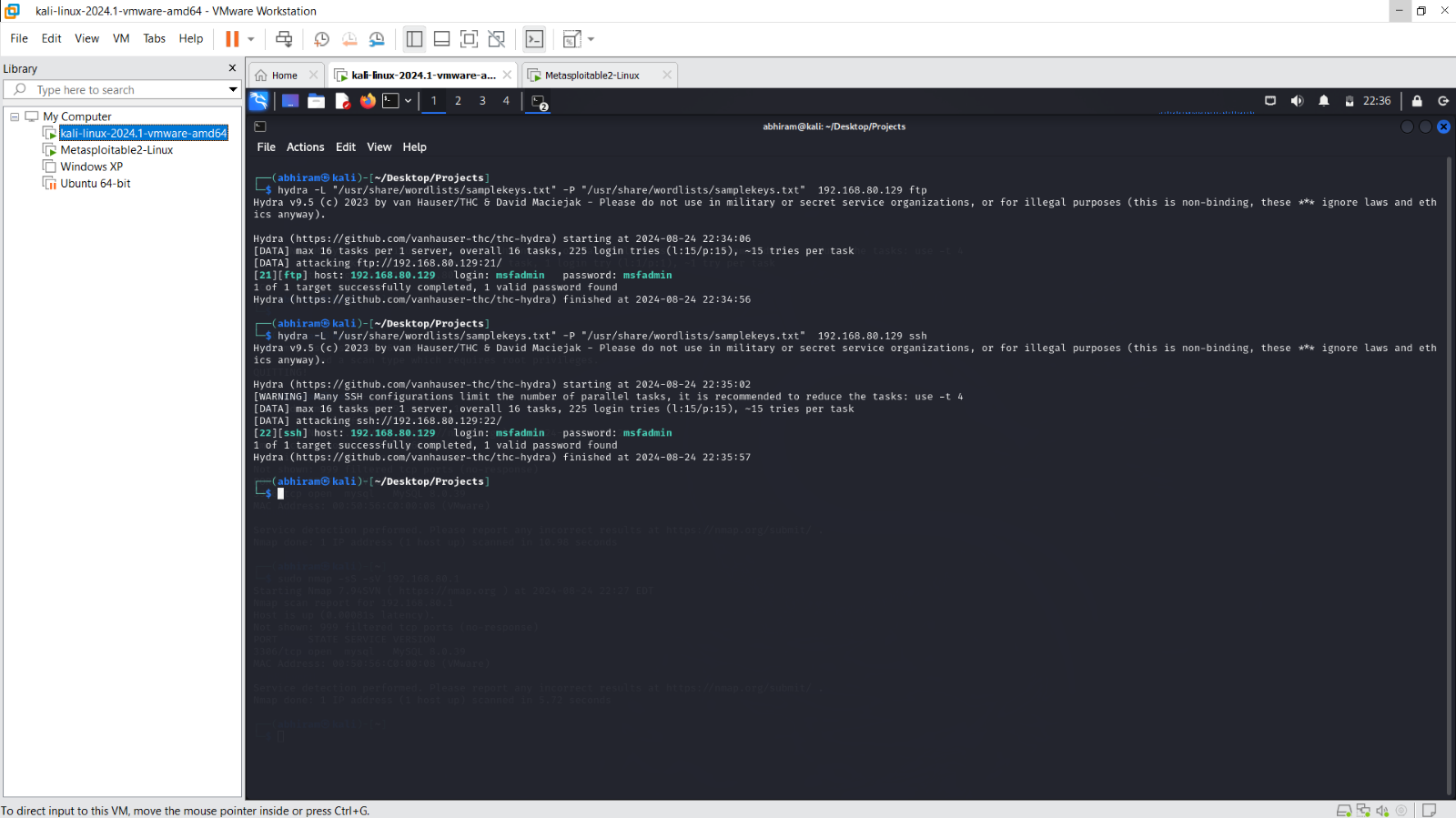
1. Displaying the IP of metasploitable machine as shown below:



1. Using nmap tool to scan the open ports, which can be used to exploit the target machine.



1. Using Hydra tool to crack the password using brute force as show on vulnerable services (open ports).



1. Developed Python script to automate the password cracking password.

