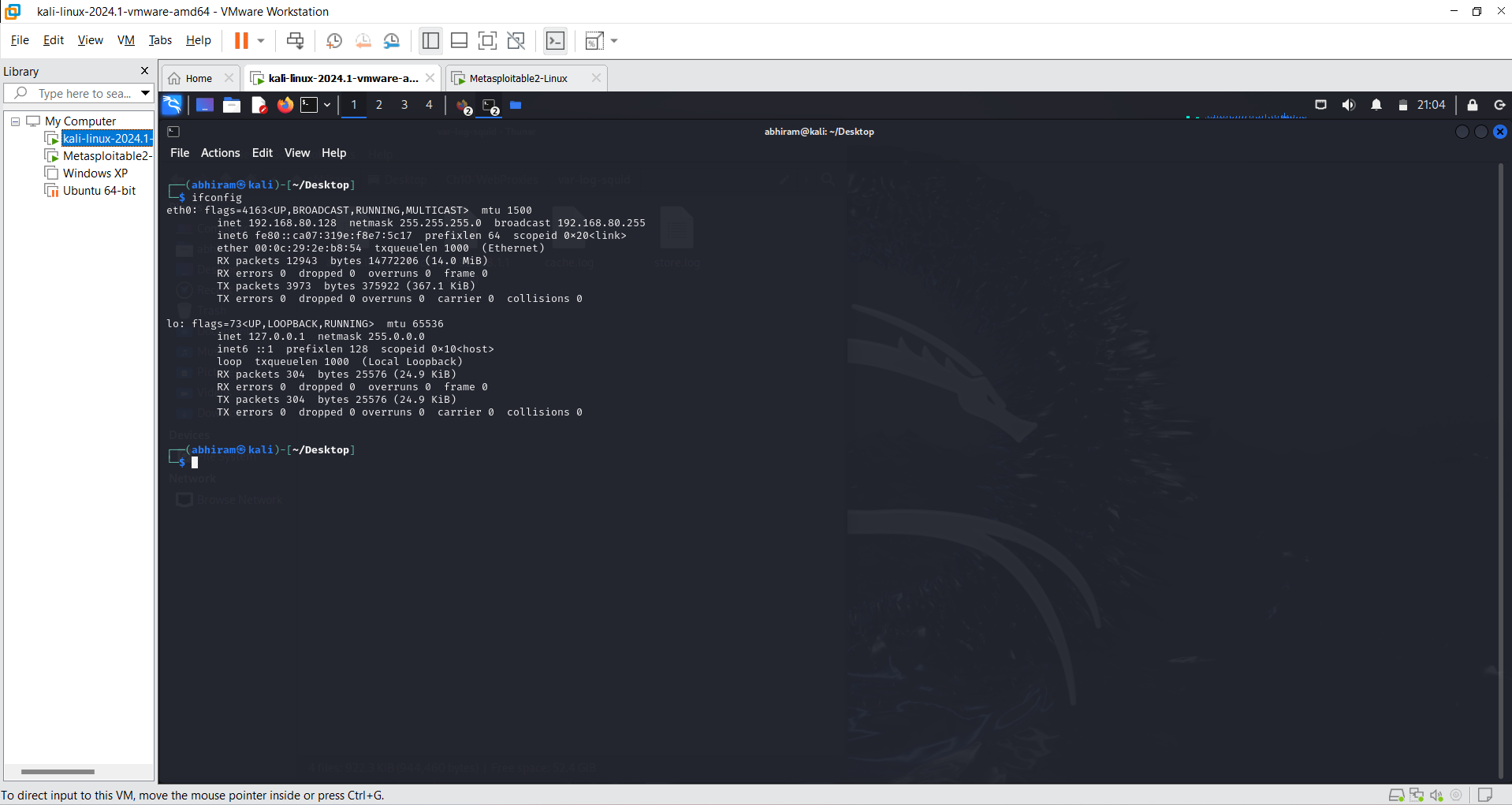
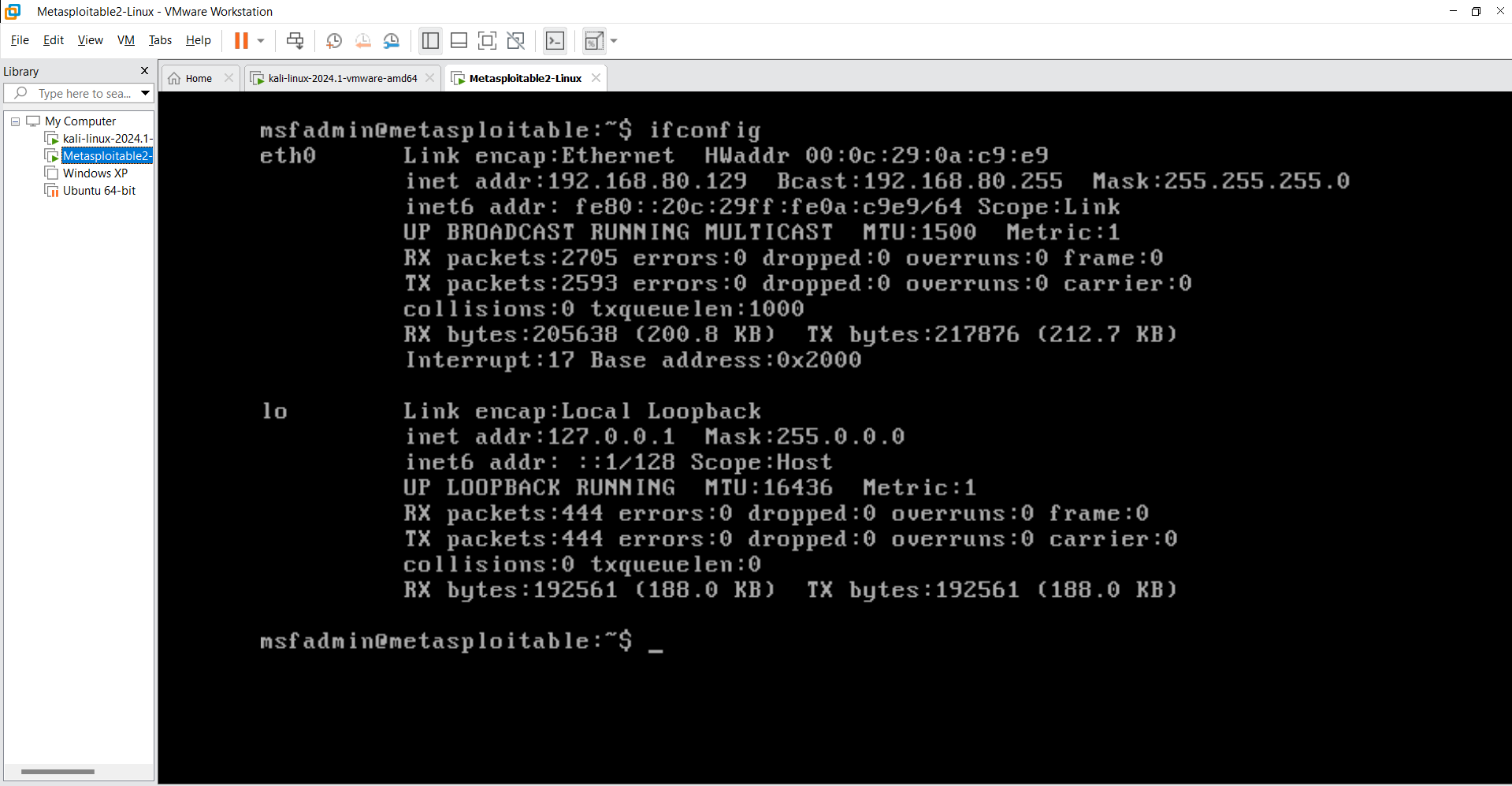
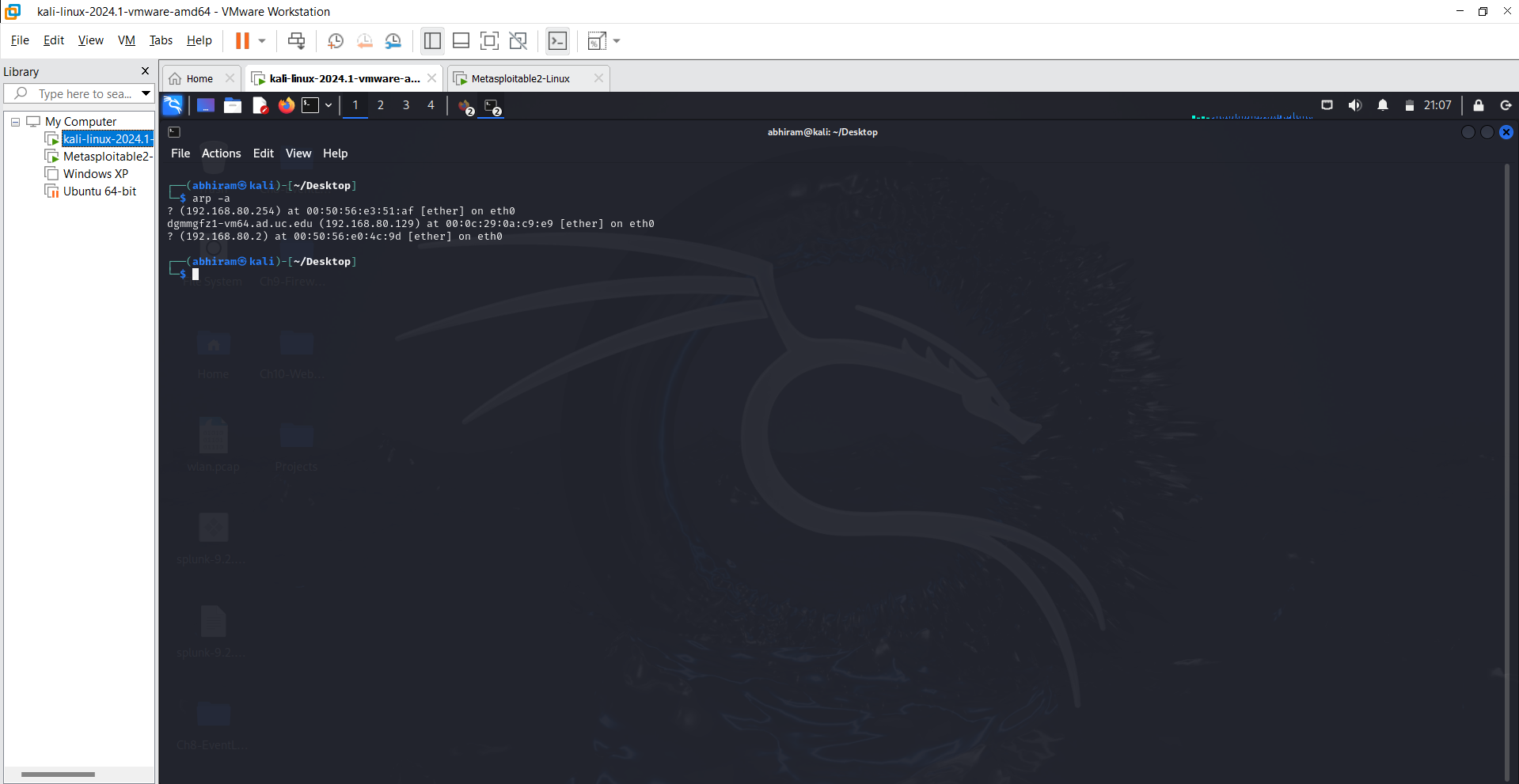
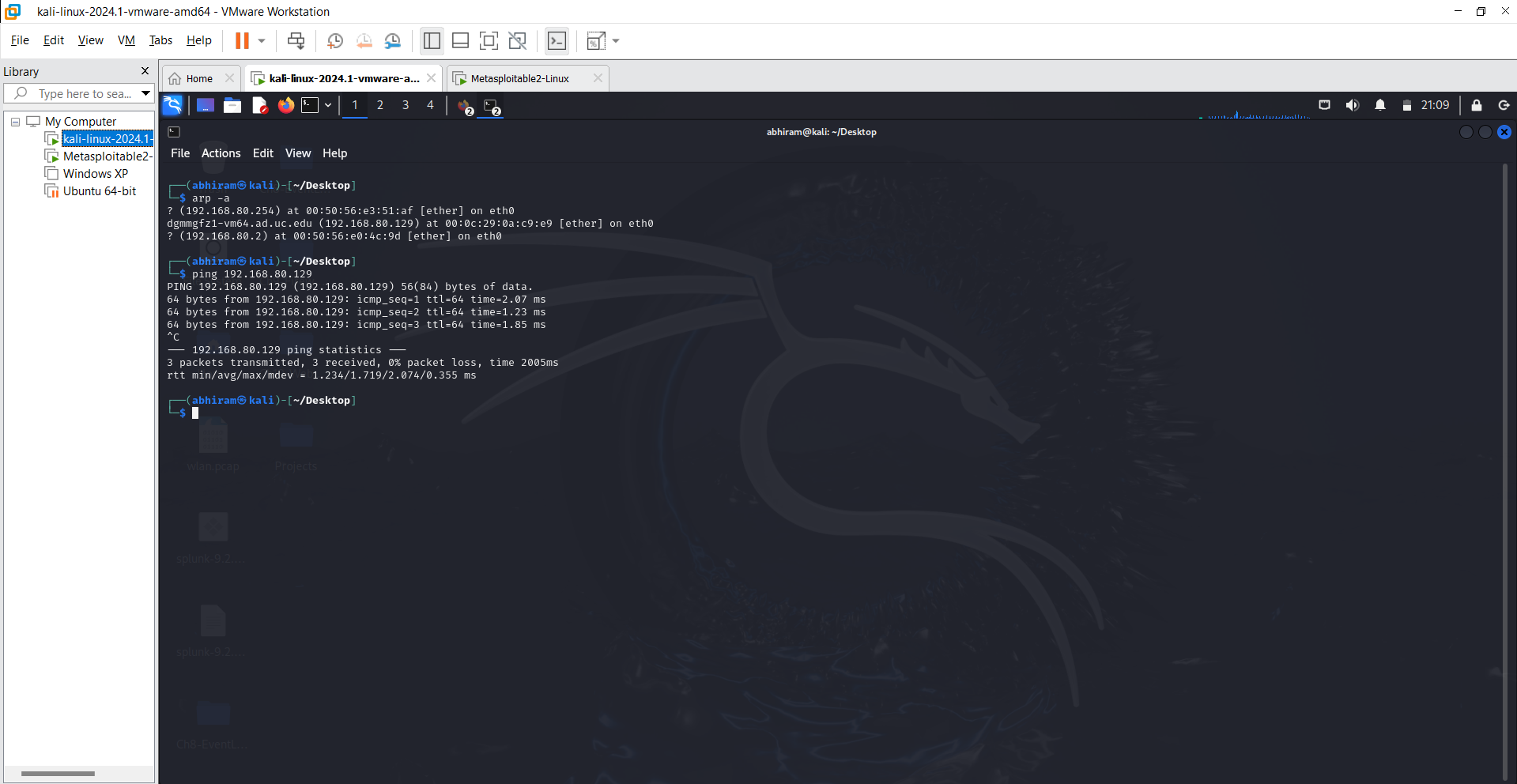
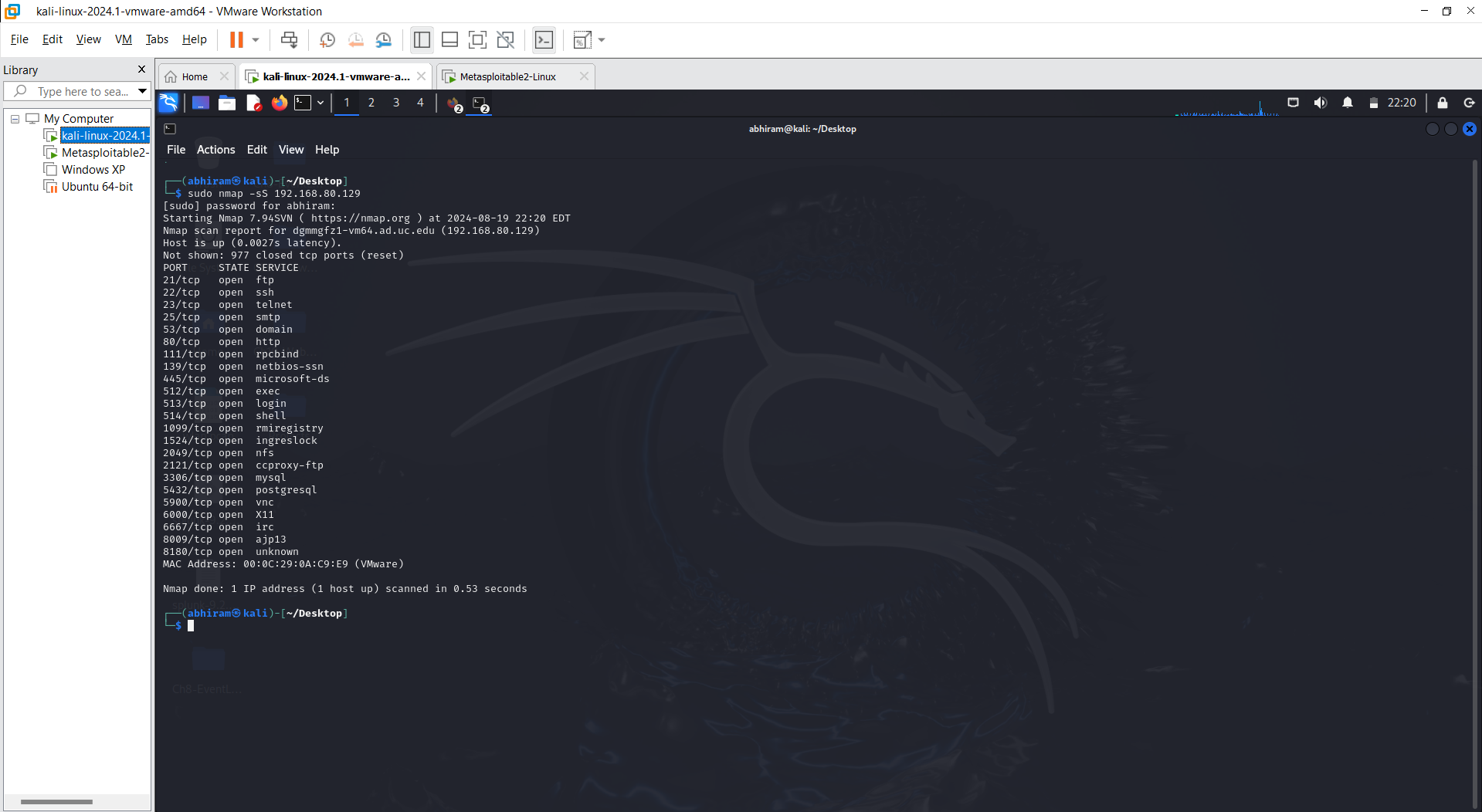
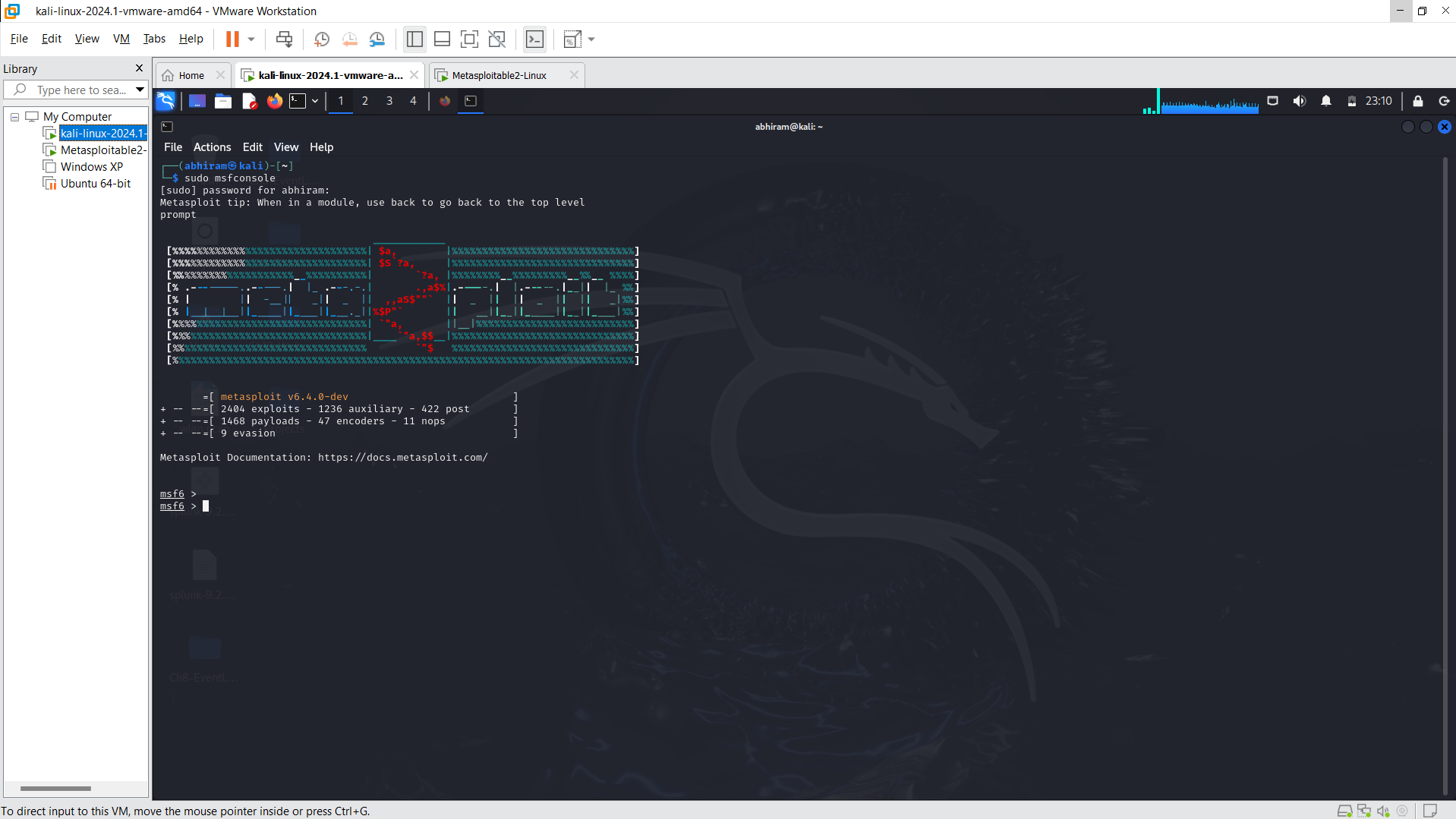
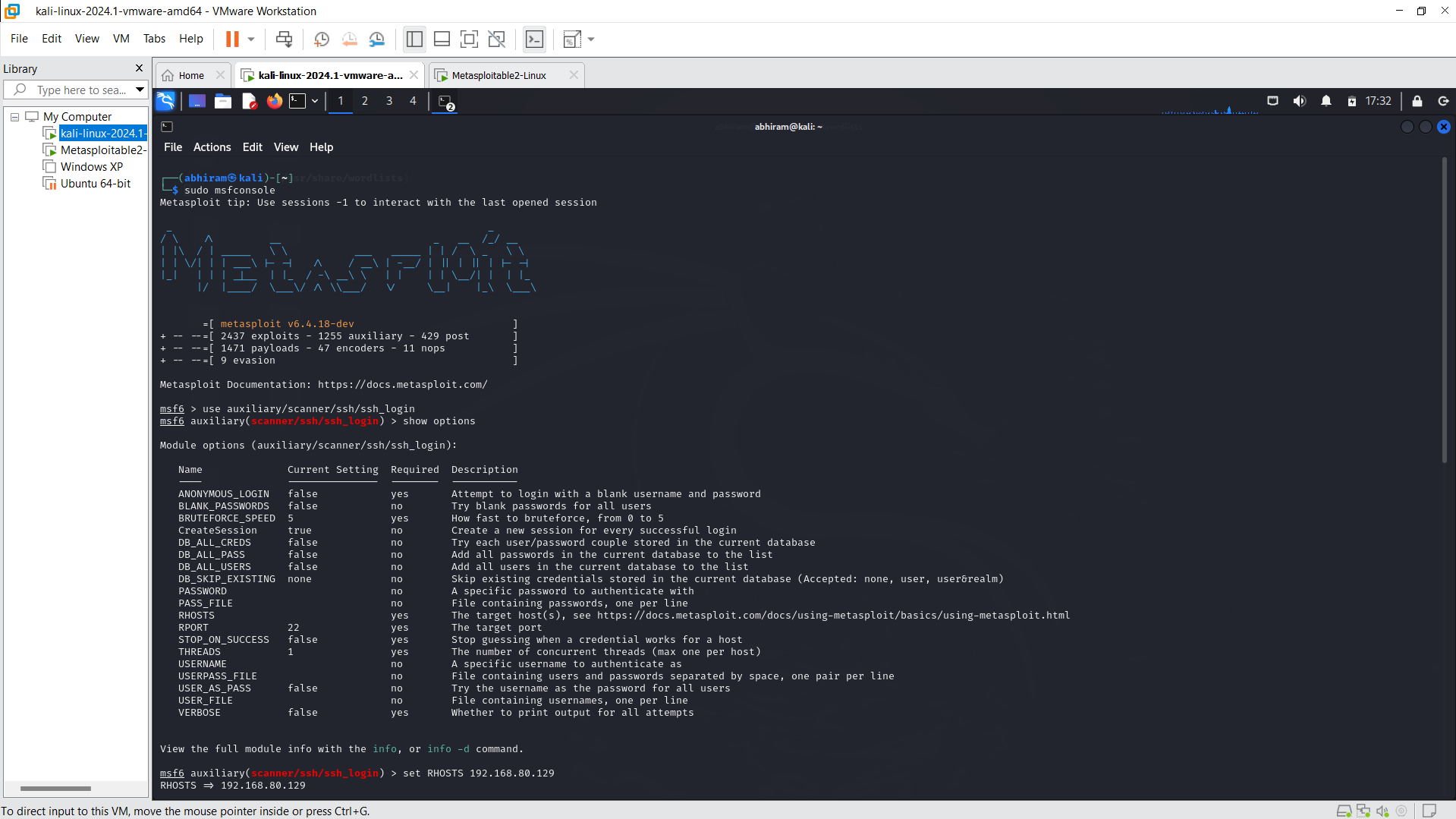
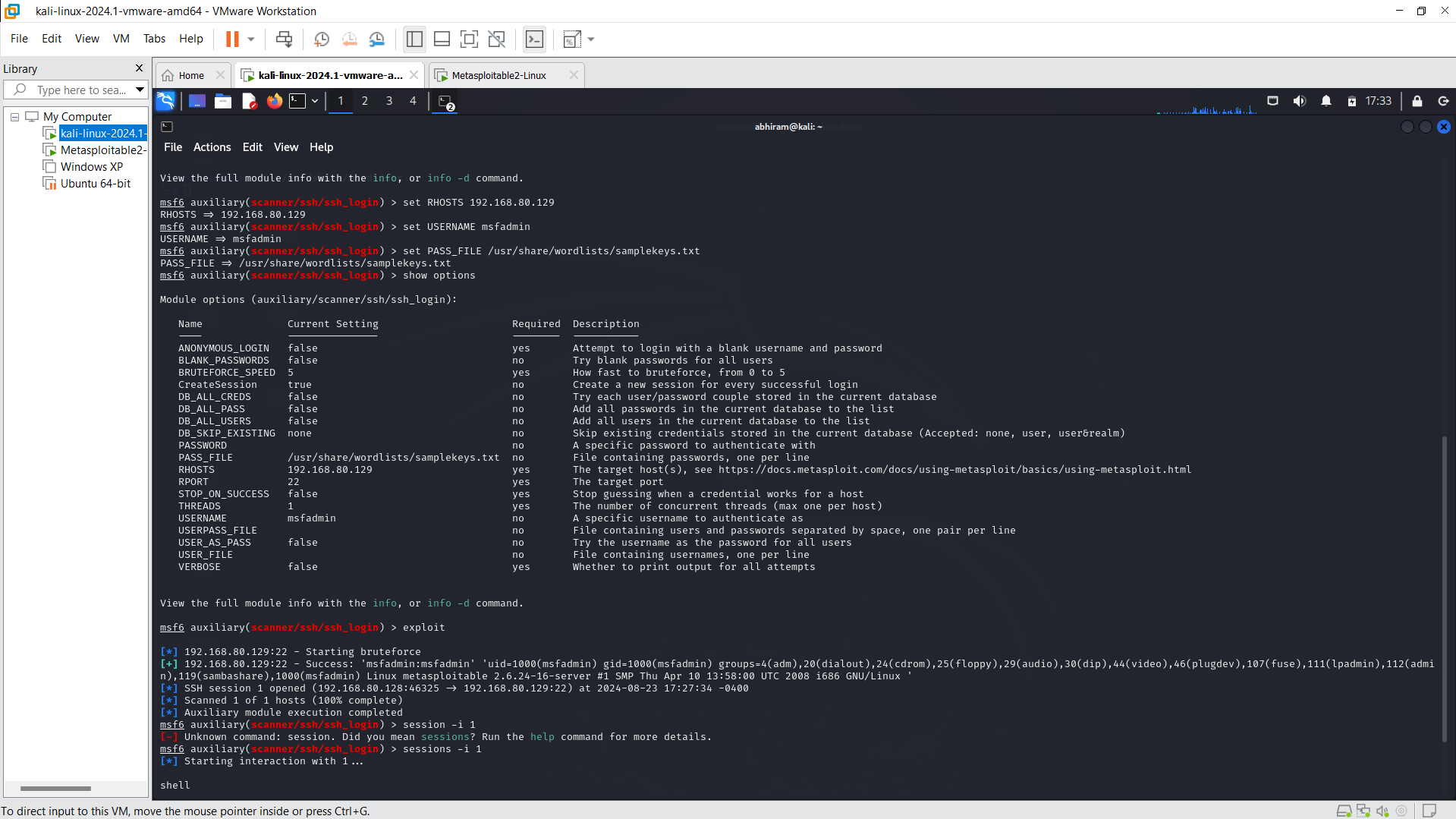
Penetration testing on Metasploitable Machine

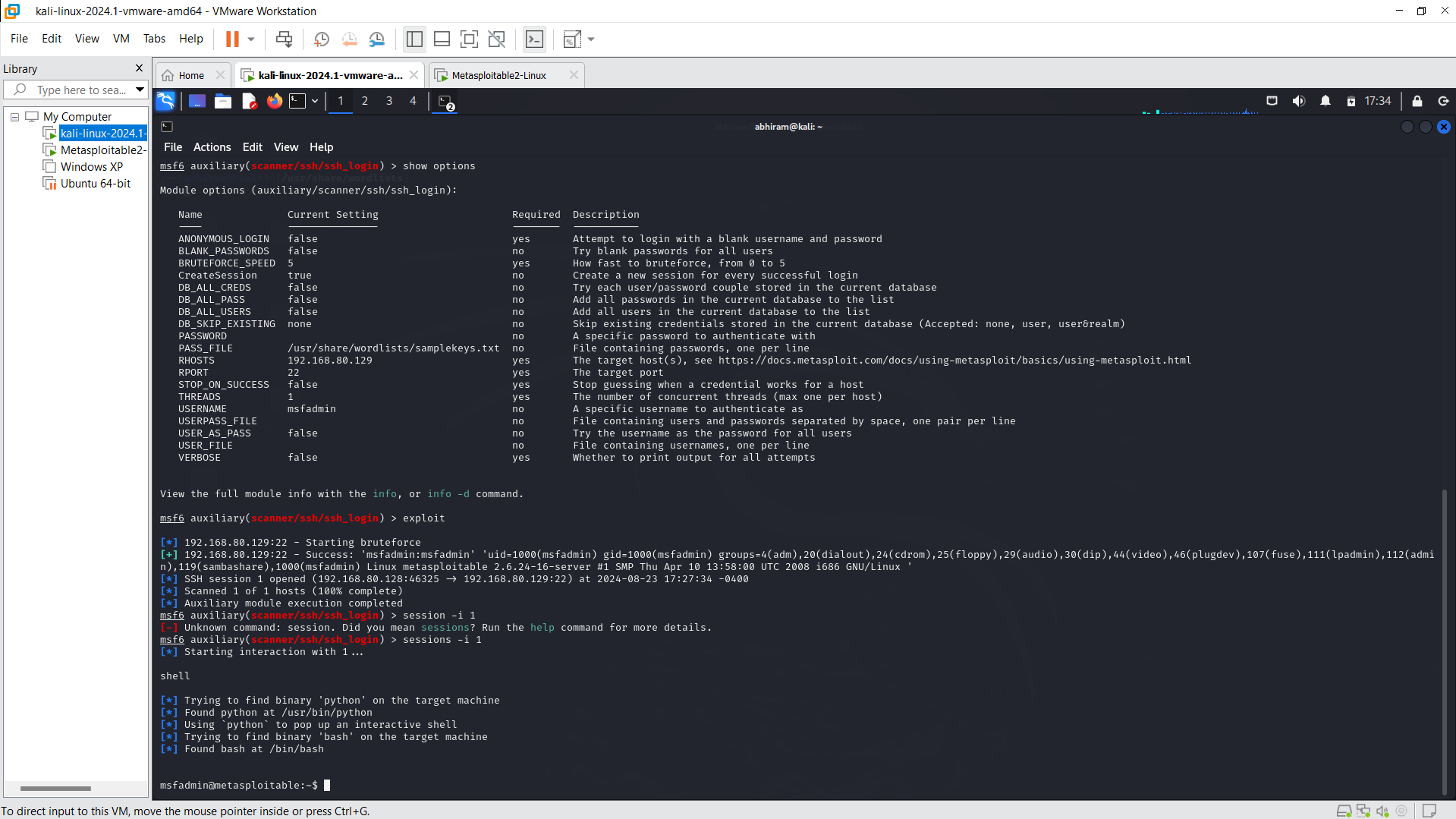
1. Created a Virtual Environment containing Kali-Linux and Metasploitable machine using VMware Workstation 17 Pro. Their IPs are displayed as shown using “ifconfig” command.   
     
   
2. I used arp command to check that they are on the same network as shown below:  
   
3. Checking if the Kali-Linux VM has network connectivity with the metasploitable IP with ping command and can see that ICMP echo requests are being transmitted between them as shown:  
   
4. Performed a stealth scan on Metasploitable IP address to find the open ports and services running on it.  
   
5. I observed that most of the ports are open and can be used to exploit the Metasploitable IP in many ways like using ssh (22), ftp (21), smtp (25) etc...
6. Using Metasploit framework to exploit the vulnerabilities in target metasploitable machine identified through open ports obtained by nmap command.
7. Using brute force ssh login in Metasploit framework:



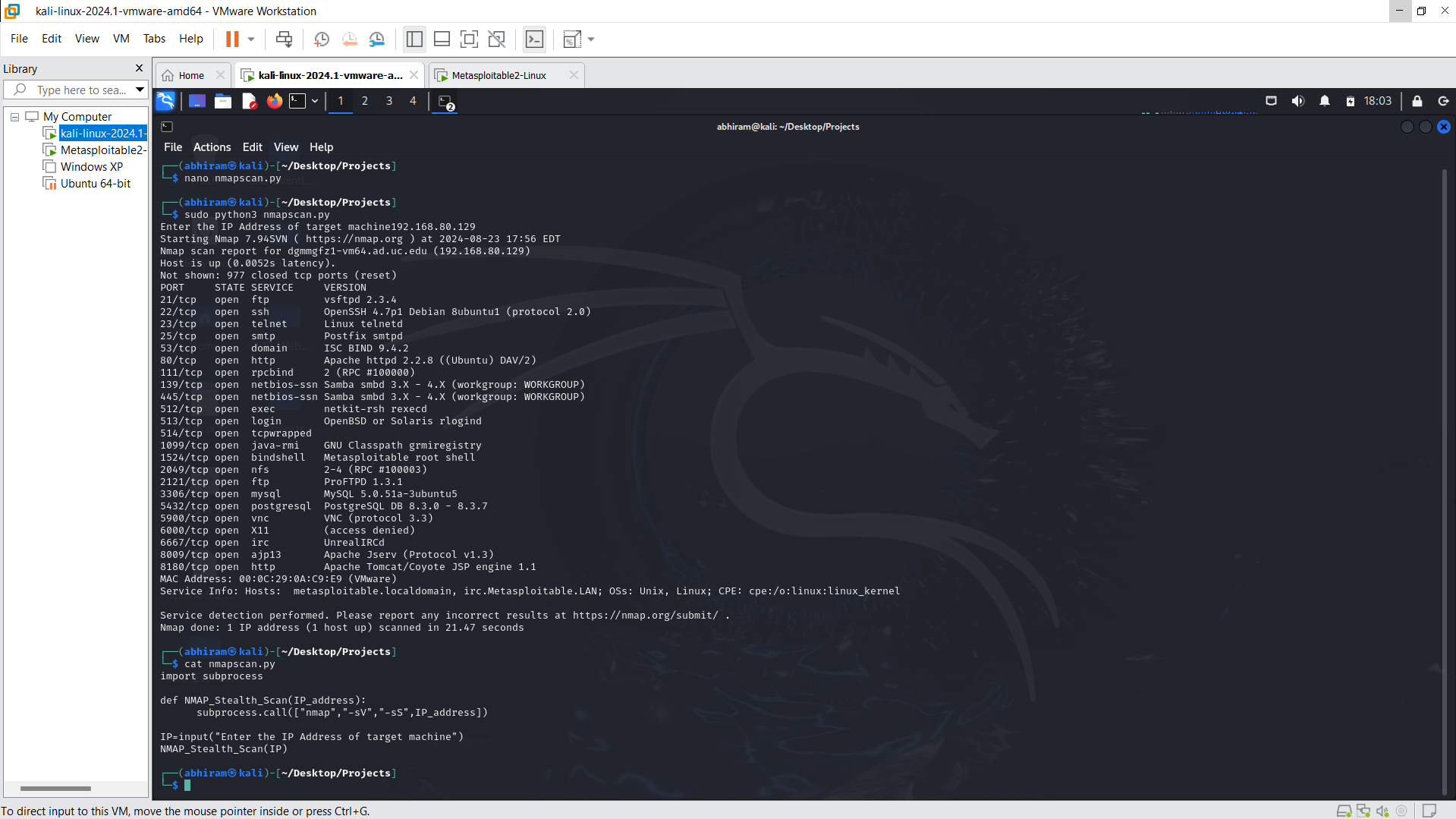
1. Searching for SSH\_LOGIN exploit and using that module:



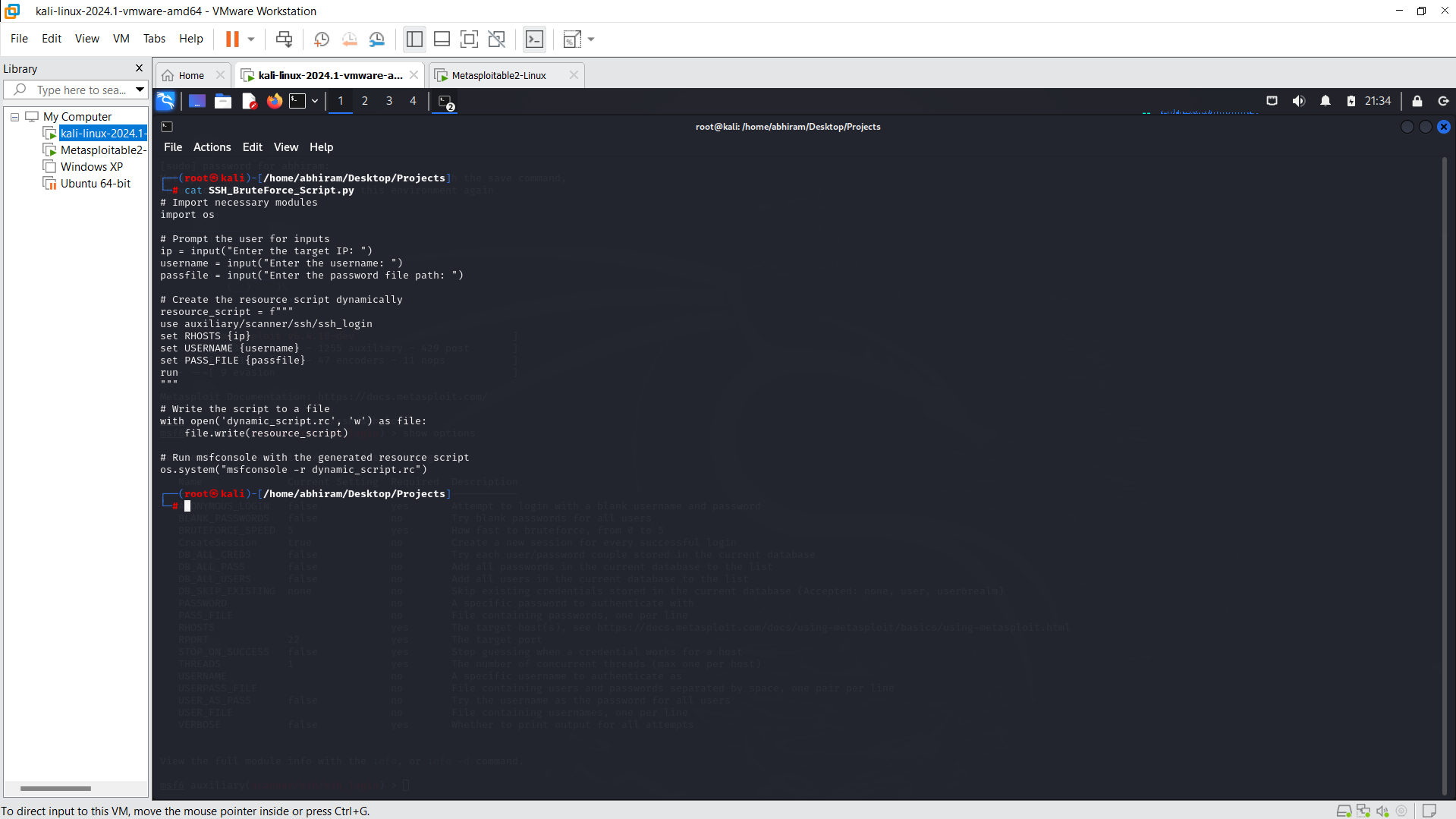




1. Using automated python script that takes IP address as input and performing nmap stealth scan.



1. Using an automated script and resource script for metasploit command execution to take necessary inputs like RHOSTS, USERNAME, PASS\_FILE and performing ssh\_login brute force attack.



1. Running the automated python script:

