**Lab 04 - Scanning the Target for Vulnerabilities**

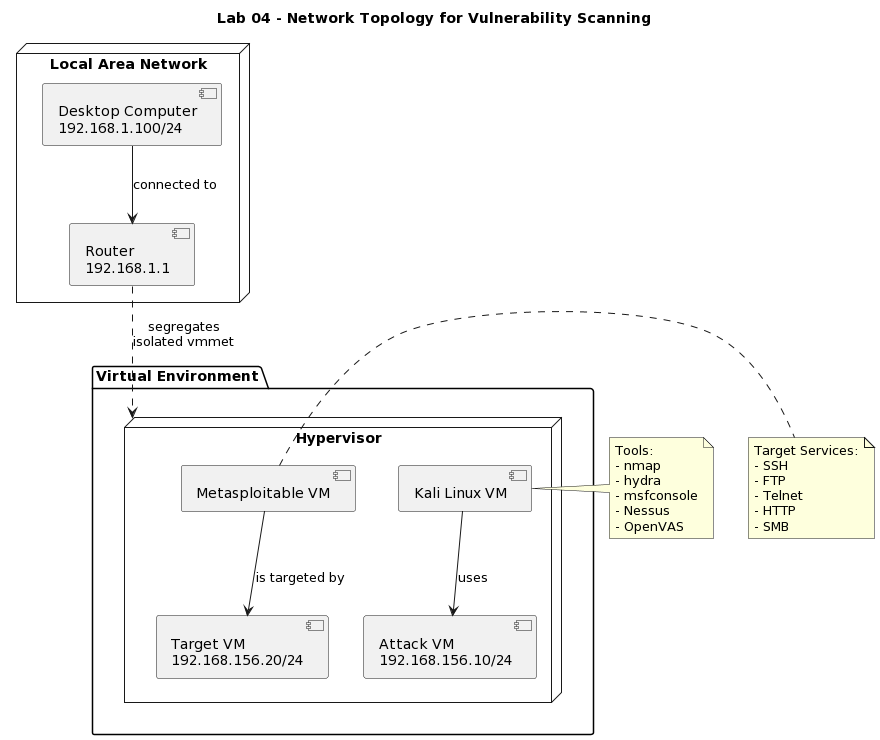
**Executive Summary**

This report outlines the methodology and findings from Lab 04, which focuses on the active discovery phase of penetration testing. Utilizing Kali Linux's suite of tools, we identified potential vulnerabilities within the Metasploitable2-Linux VM, assessing their exploitability for further penetration testing stages. Notable was the use of the Metasploit framework, which provides a comprehensive environment for testing system robustness against security breaches.

**Description**

The active discovery phase is crucial in penetration testing to pinpoint security weaknesses that can be leveraged for unauthorized access. The Kali Linux distribution, equipped with various security assessment tools, including the Metasploit framework, enables penetration testers to conduct effective security evaluations. Despite the challenges posed by false positives and negatives, the tools within Kali Linux offer up-to-date exploit databases and scanning capabilities necessary for identifying valuable targets.

**Topology/Diagram**



**Key Syntax:**

* **ping**: Verifies the connectivity between two machines.
* **ifconfig**: Displays the machine's IP address in the terminal.
* **nmap**: Scans the target machine for open ports and services.
* **hydra**: Conducts brute force password attacks.
* **msfconsole**: Launches the Metasploit framework for exploit execution.
* **set RHOSTS**: Designates the target machine's IP address.
* **exploit**: Executes a selected exploit against the target.
* **run**: Initiates a scripted attack sequence.
* **ssh**: Securely connects to a remote machine.
* **telnet**: Accesses a remote host interactively.
* **ftp**: Performs file transfers to and from a remote host.

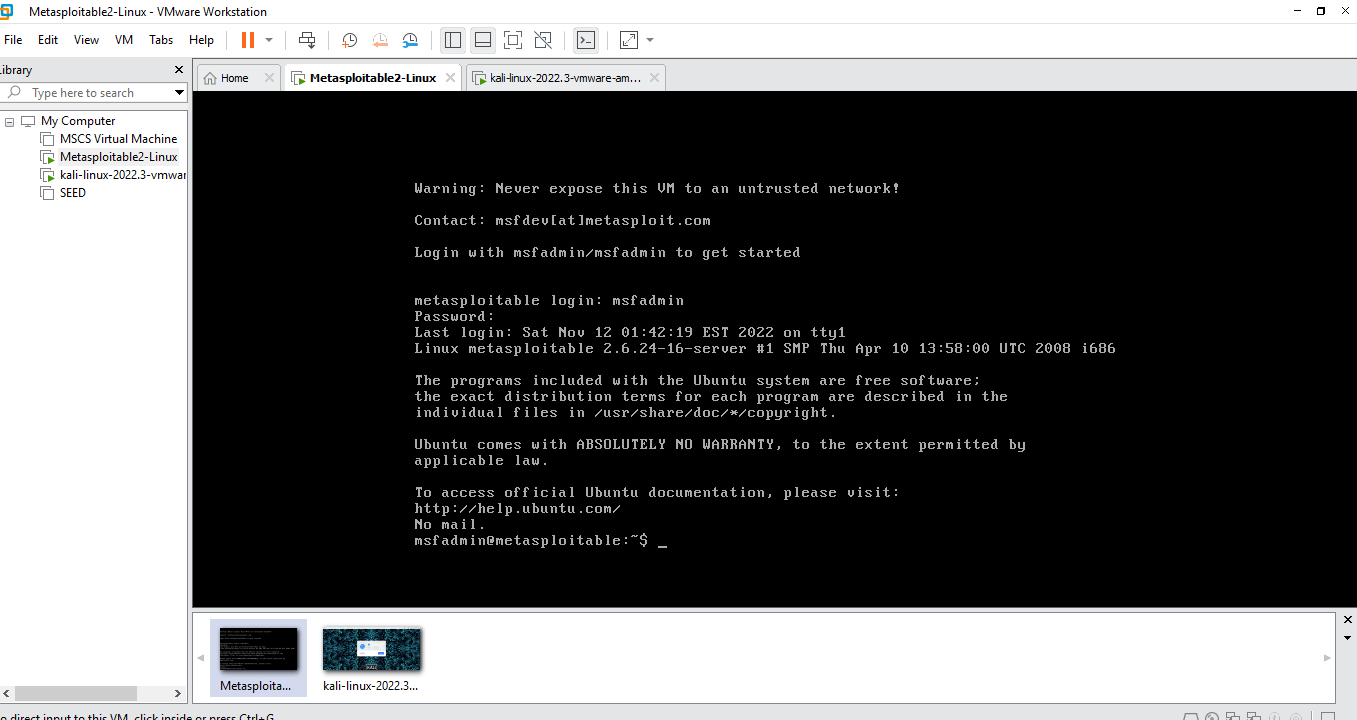
**Verification**

**Penetration Tools Utilized:**

* Metasploit for auxiliary and exploitation modules
* Hydra for credential brute-forcing
* Nmap for target scanning
* OpenVAS and Nessus for vulnerability scanning

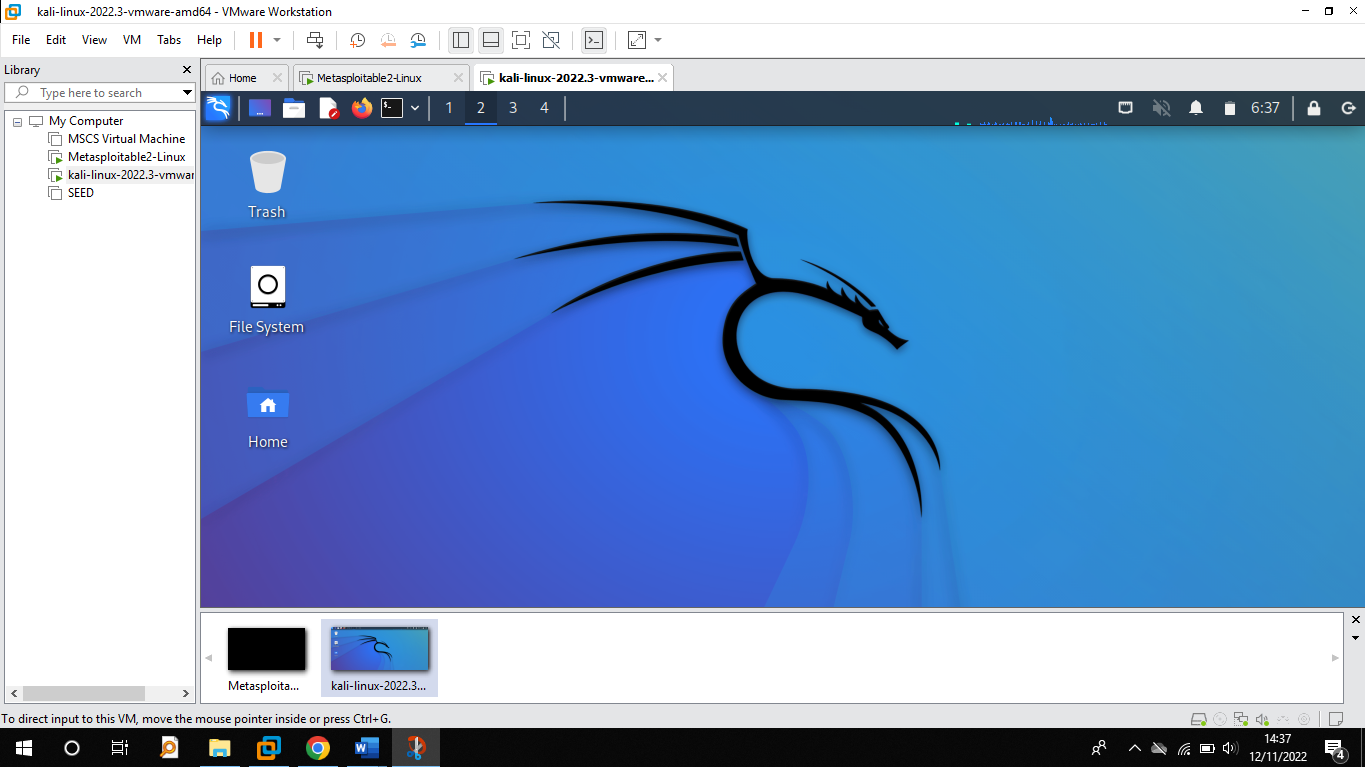
**Metasploitable2-Linux Installation**

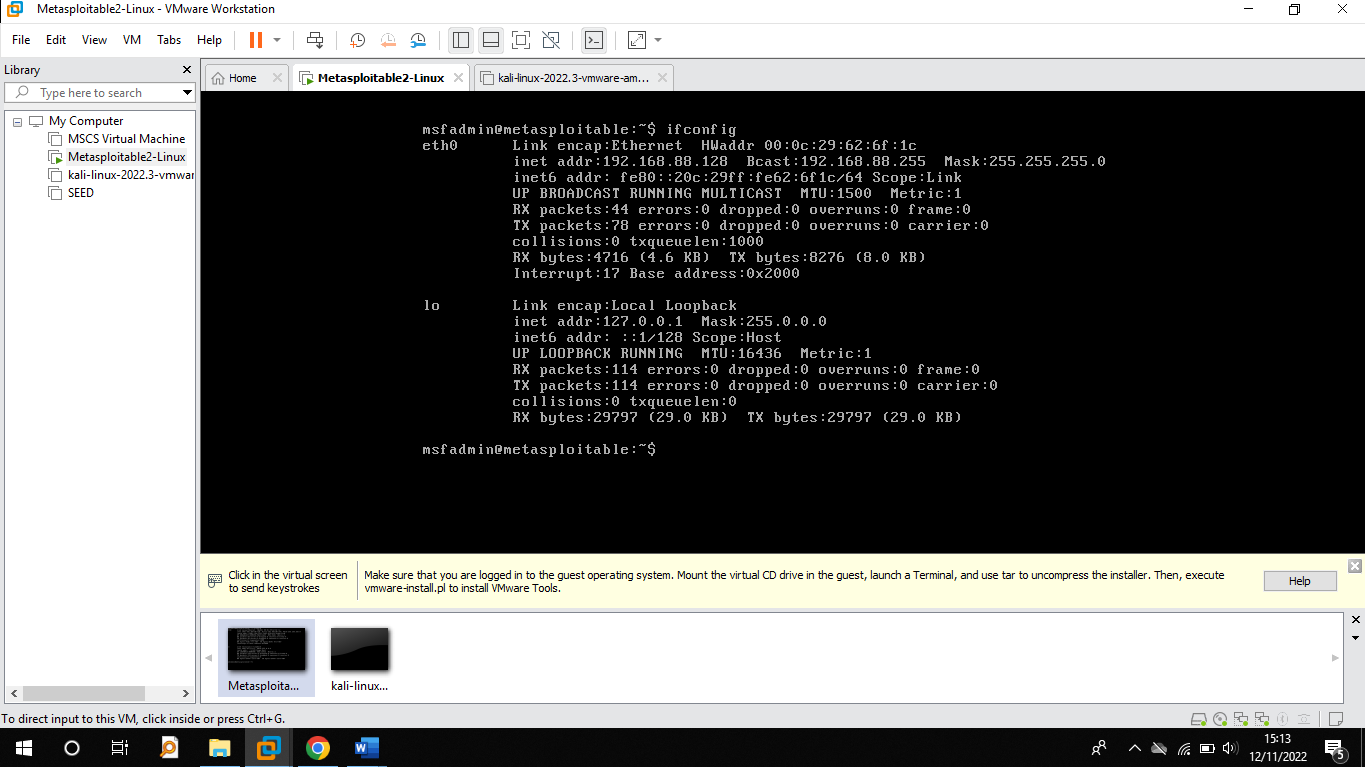
I started the lab environment setup by installing Metasploitable2-Linux on the VMware Workstation. This virtual machine serves as the target for penetration testing exercises.

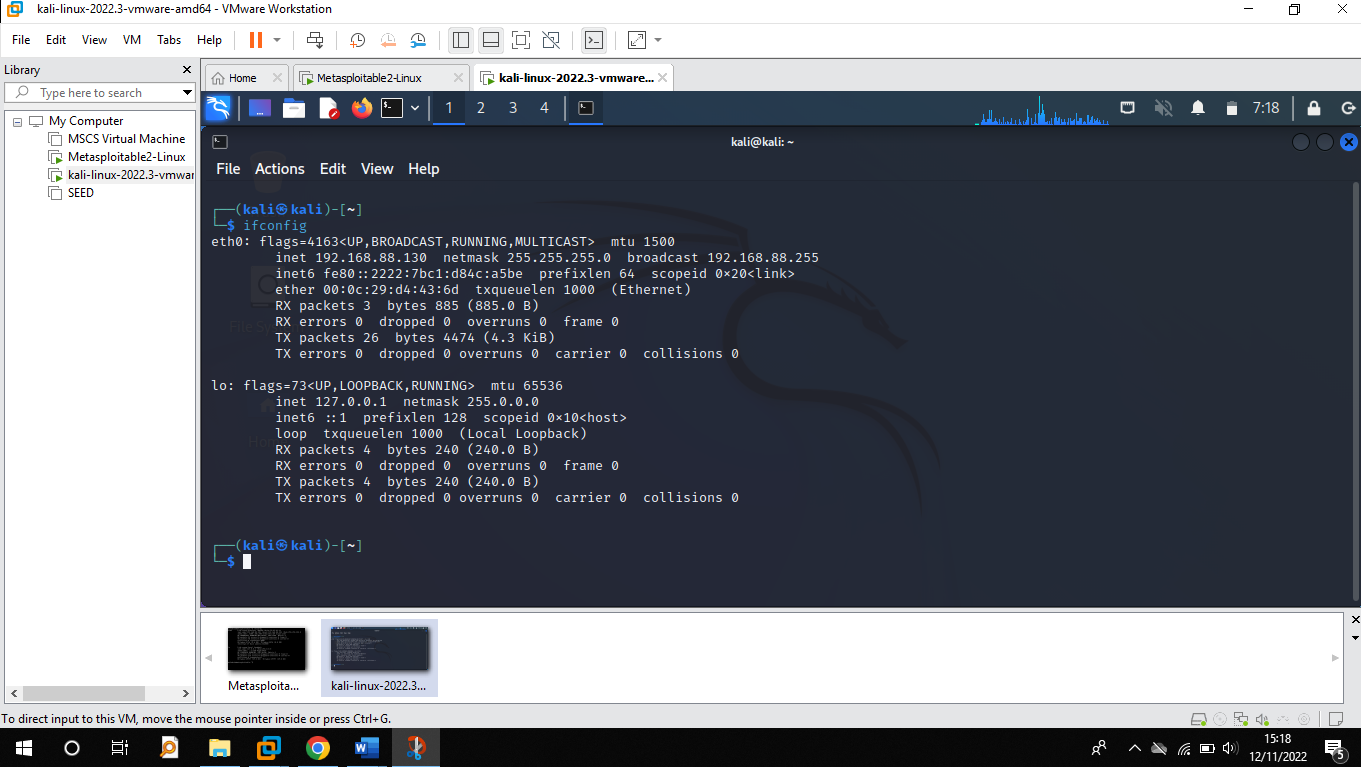


**Kali Linux Installation**

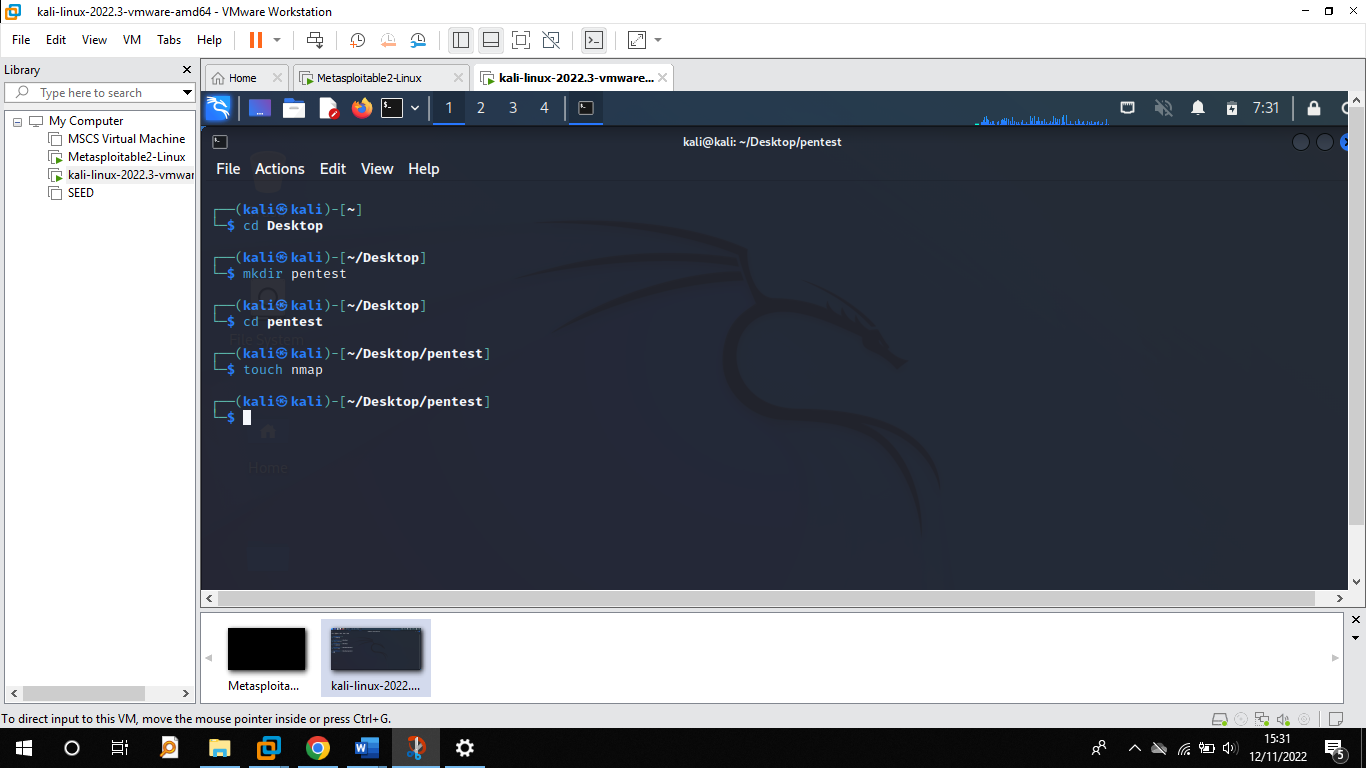
Following the setup of the target VM, Kali Linux was installed on the VMware Workstation. Kali Linux is equipped with a suite of tools for penetration testing and will function as the attack platform.

The IP address of the Metasploitable2-Linux VM was obtained by executing the **ifconfig** command within its terminal.

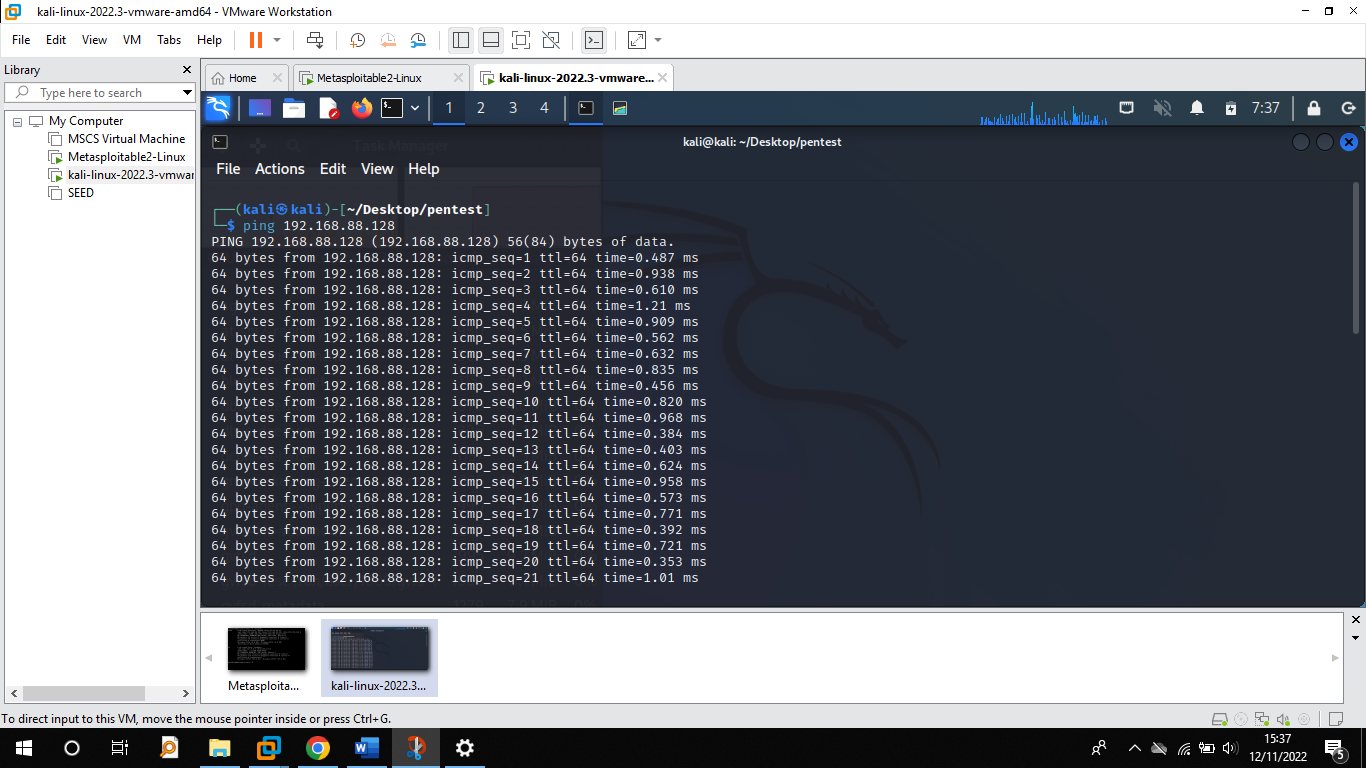


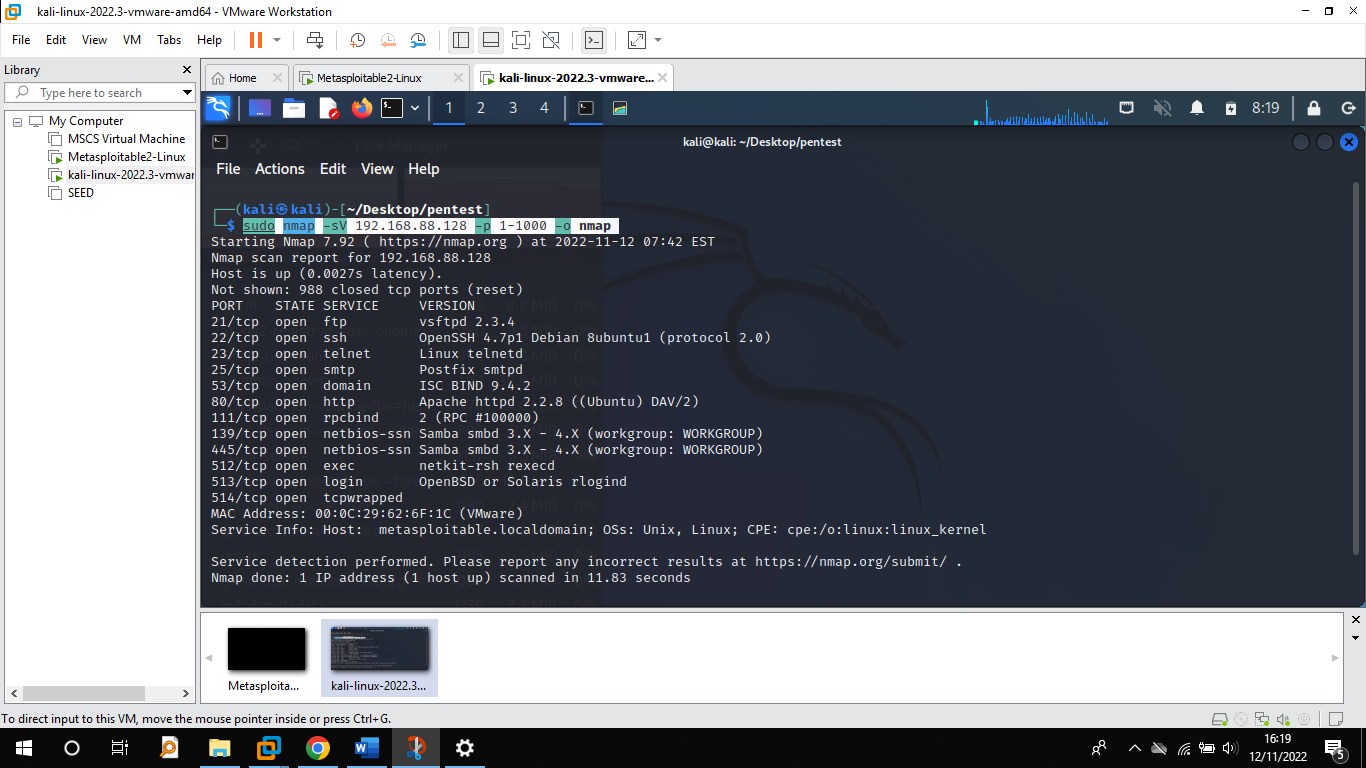
Similarly, ran the **ifconfig** command on the Kali Linux VM to get its IP address, ensuring network communication parameters were set for the upcoming penetration testing activities.

I a dedicated directory named 'pentest' on the desktop of the Kali Linux VM to organize the tools and outputs of the penetration testing exercises.



I conducted a connectivity test between the Kali Linux VM and the Metasploitable2-Linux VM by issuing a **ping** command from the Kali Linux terminal towards the Metasploitable2-Linux VM's IP address. The successful exchange of packets confirmed that the two machines were able to communicate over the network.

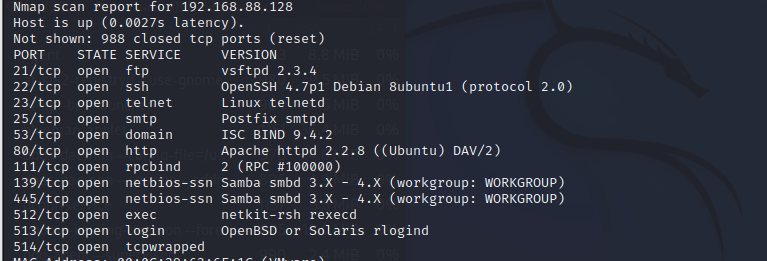
I initiated a scan on the target Metasploitable2-Linux VM using the **nmap** tool from the Kali Linux VM. The command **sudo nmap -sV 1922.168.88.128 -p 1-1000 -o nmap** was employed to perform a service version scan on the first 1000 ports. The results of the scan were directed to a file named 'nmap' within the previously created 'lab' directory on the Kali Linux desktop for future analysis and reporting.



Reviewed the nmap scan output, which indicated that the target system, Metasploitable2-Linux, is running a Unix/Linux operating system. This was determined from the service information section of the nmap results, where the operating system is identified by the Common Platform Enumeration (CPE) notation **cpe:/o:linux:linux\_kernel**.



The nmap scan results have identified multiple open ports on the target system, detailing the state, service, and version for each. Key services include FTP, SSH, Telnet, HTTP, and Samba, among others, which are potential points of entry for further penetration testing efforts.

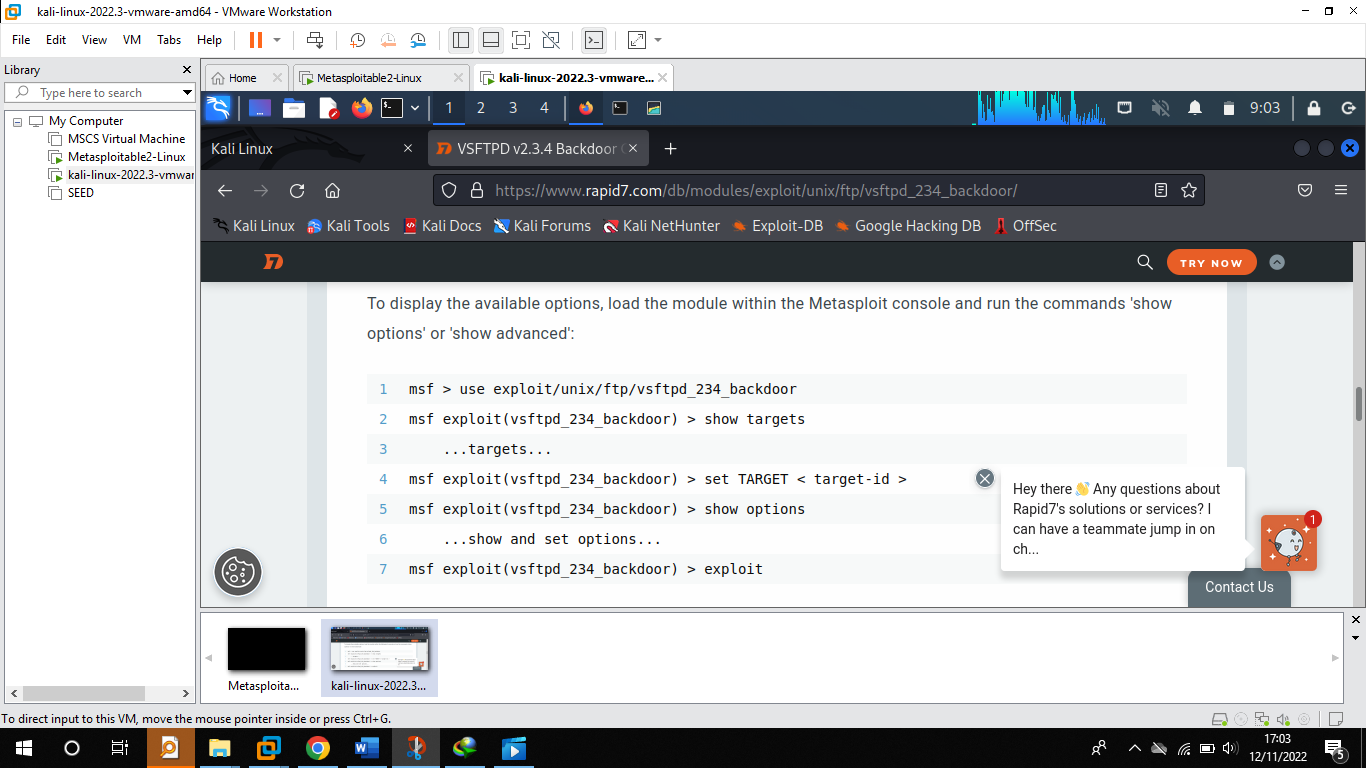


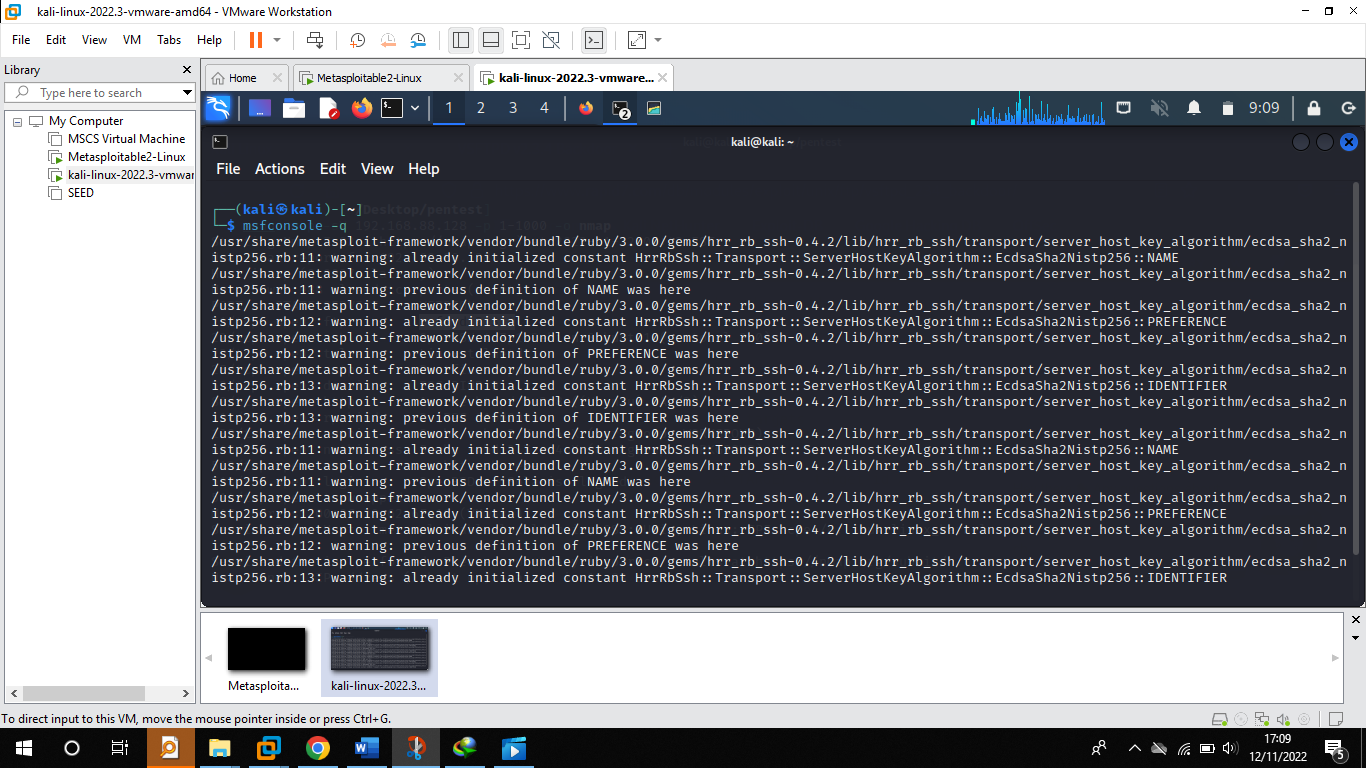
**Exploitation Focus**

The penetration testing will target specific services where vulnerabilities were discovered: FTP on port 21, SSH on port 22, Telnet on port 23, NetBIOS over SSN on port 445, and HTTP on port 80, aiming to exploit potential weaknesses identified during the scan.

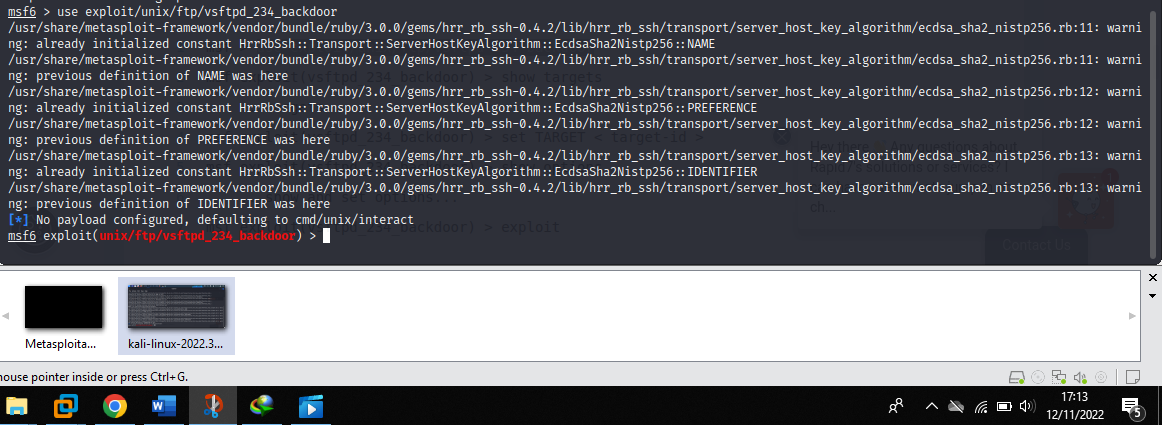
**Investigation of FTP Service on Port 21**

Upon identifying the FTP service version on port 21 from the nmap scan, the next step is to research potential vulnerabilities associated with this version for exploitation opportunities.

Research through a web browser confirmed a vulnerability in the FTP service, which is exploitable using Metasploit. Subsequently, Metasploit was launched in quiet mode through a new terminal window to prepare for the exploitation of the identified vulnerability.

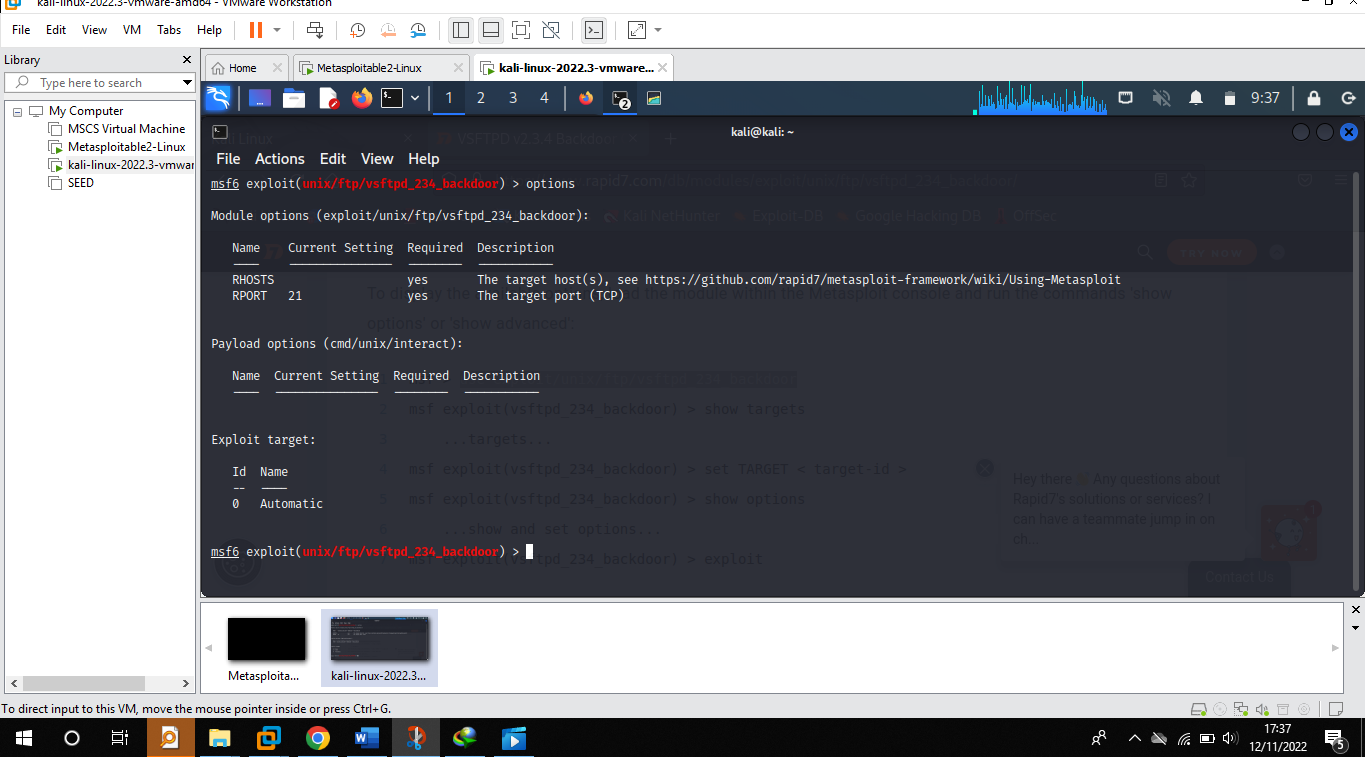


With Metasploit operational, the relevant exploitation module was loaded into the framework to proceed with the attack on the vulnerable FTP service.



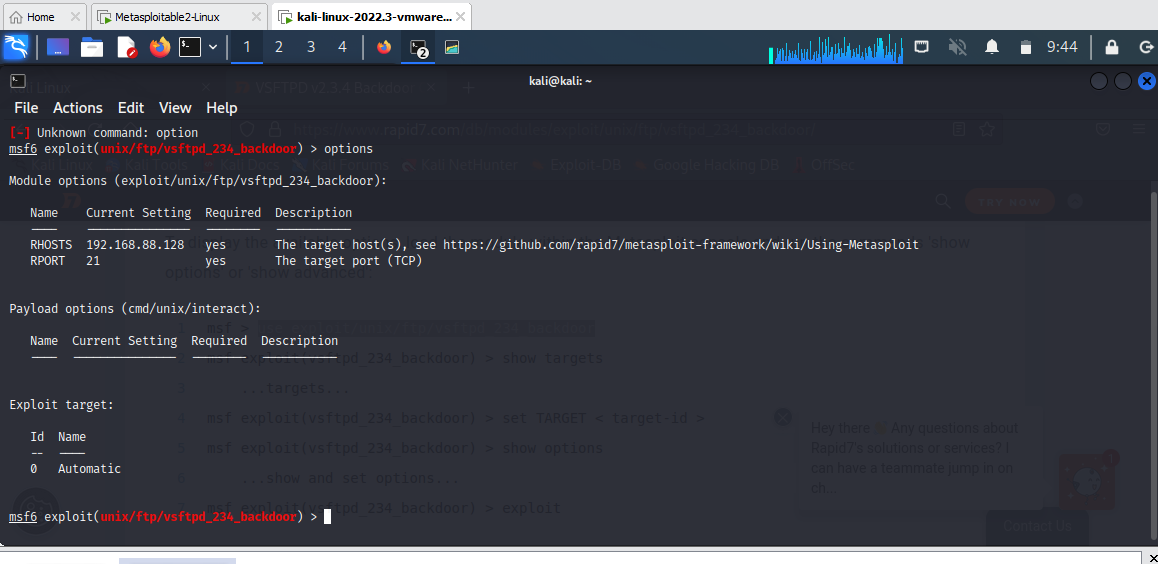
The module for the FTP service vulnerability was successfully loaded in Metasploit, as indicated by the command prompt above ready to receive further instructions for exploitation.

Executed the **options** command within Metasploit to review and configure the necessary parameters for the loaded FTP exploit module.



The IP address and port number of the target machine were configured in the module's settings to align the exploit with our specific Metasploitable2-Linux VM.

Top of Form

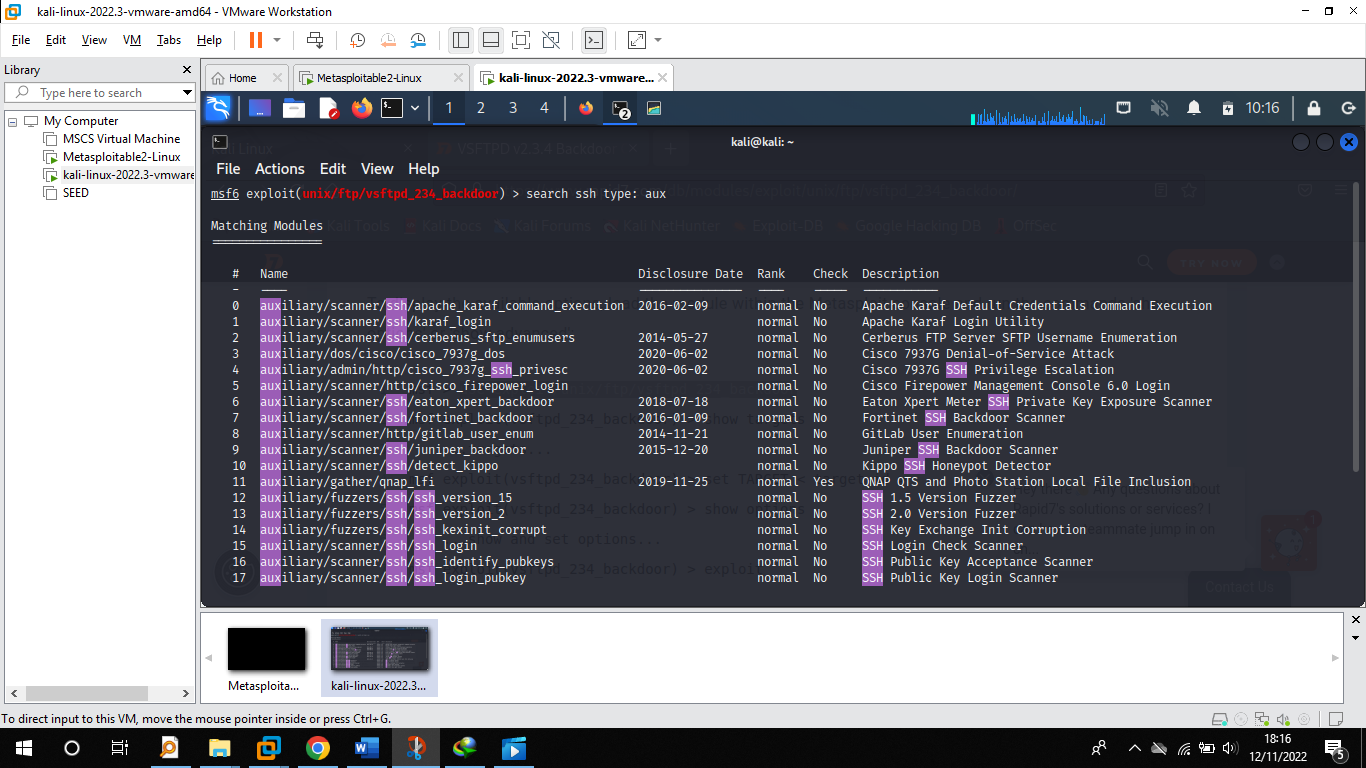


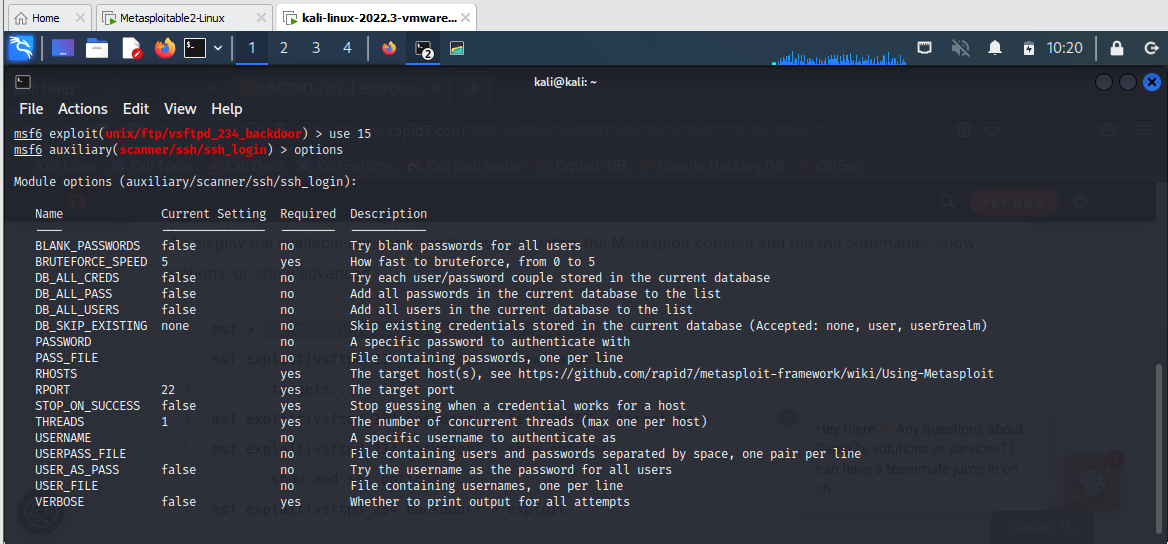
To start the module, the **exploit** command was entered. Upon successful execution, we gained a shell on the target machine, indicating that the exploit had achieved its intended effect and access was obtained.

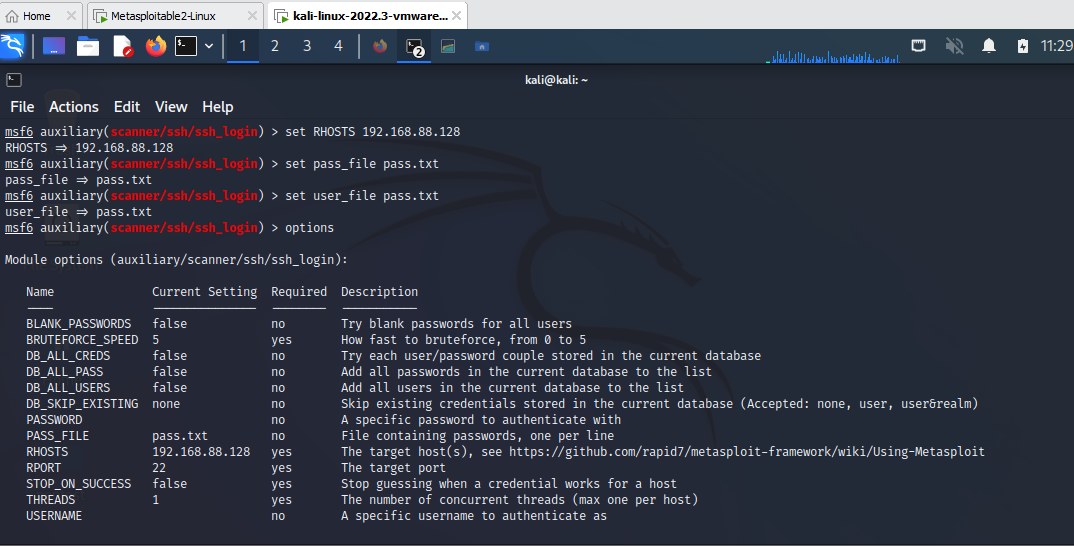
Top of Form

**Investigation of SSH Service on Port 22**

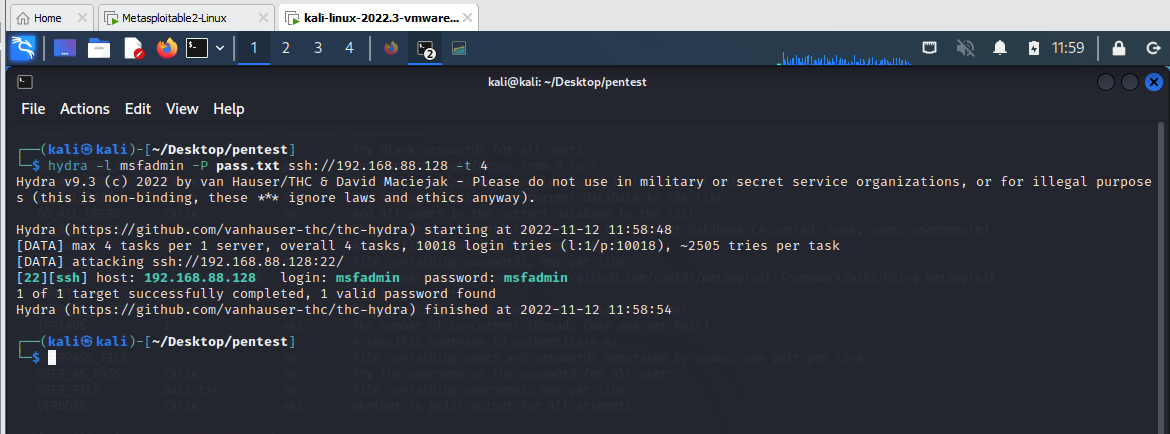
For port 22 (SSH), we prepared to perform a brute force attack by searching for the appropriate auxiliary module in Metasploit with the command **search ssh**.



Selected the auxiliary module number 15, **auxiliary/scanner/ssh/ssh\_login**, designed to gather SSH credentials, and input the **options** command to display and configure the necessary parameters for the module. 

We verified the visibility of the newly set variables to ensure they were correctly configured for the SSH credential gathering module.

**Using Hydra Tool**

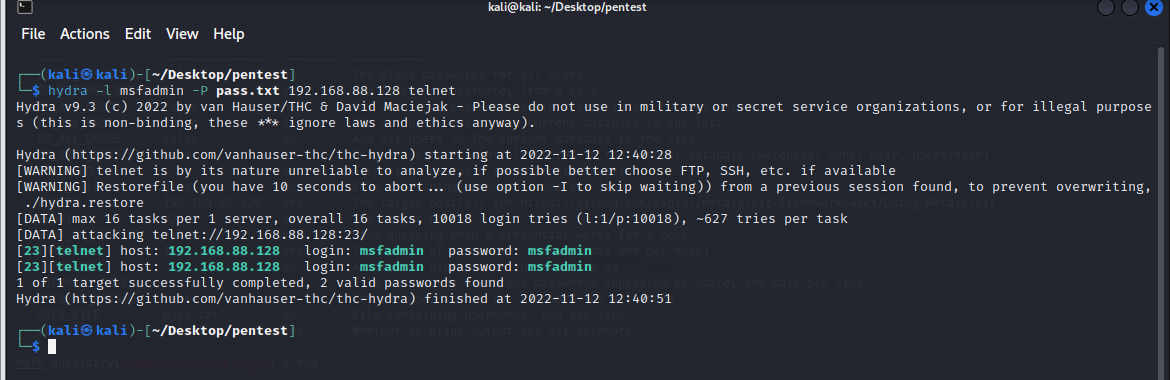
After configuring the necessary variables, the **run** command was issued to initiate the brute force process with the tool Hydra targeting the SSH service. Top of Form

The brute force attack executed by Hydra successfully retrieved SSH login credentials, specifically the username 'msfadmin' with the password 'msfadmin'.

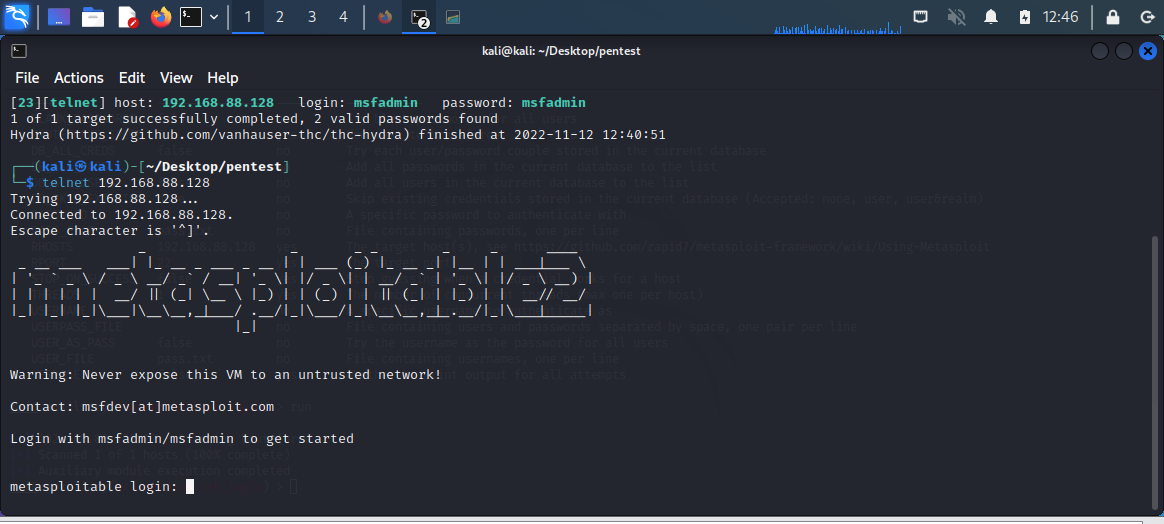
**Investigation of Telnet Service on Port 23**

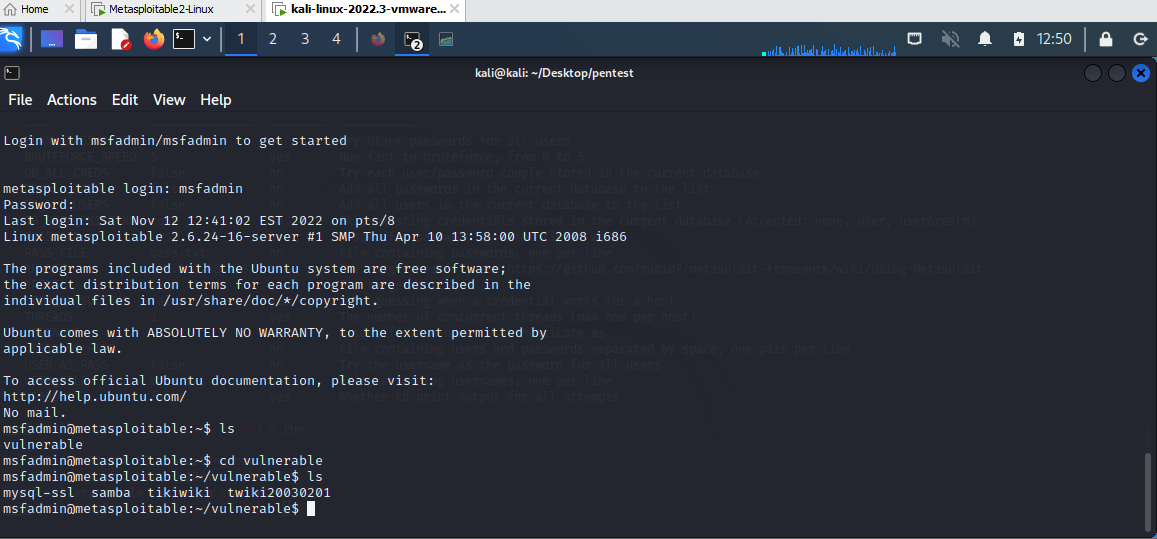
We targeted the Telnet service on port 23, similar to SSH but without secure encryption, using Hydra to brute force and acquire login credentials.

Hydra's brute force attack yielded two valid login credentials for the target system as shown below.



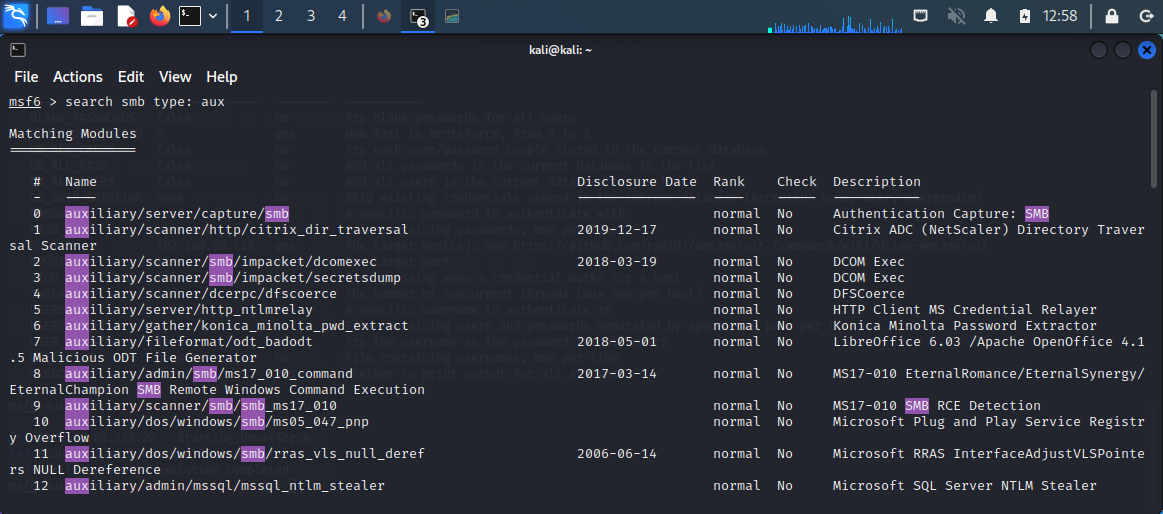
These credentials were then utilized to successfully log in to the system via Telnet, granting command-line access to the Metasploitable VM.



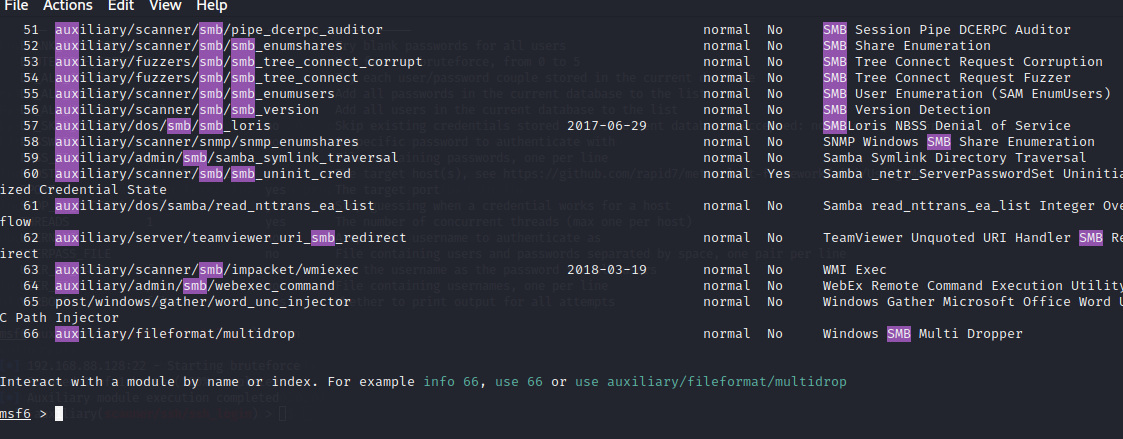
Utilizing the credentials retrieved by Hydra, we logged into the target machine via Telnet. This granted us access to the system's resources, confirming the effectiveness of the credential harvesting.

**Investigation of netbios-ssn Service on Port 445**

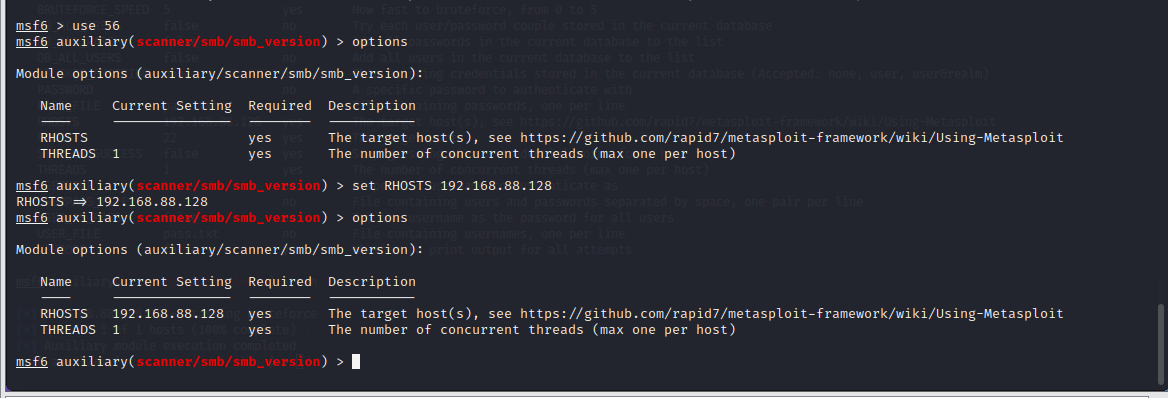
We first examine the auxiliary service we are going to apply in the metasploit module



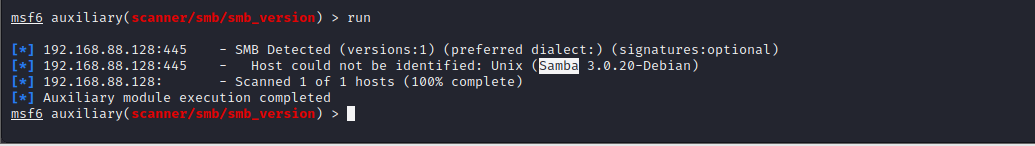
We are going to utilize the auxiliary service number 56 which is auxiliary/scanner/smb/smb\_version



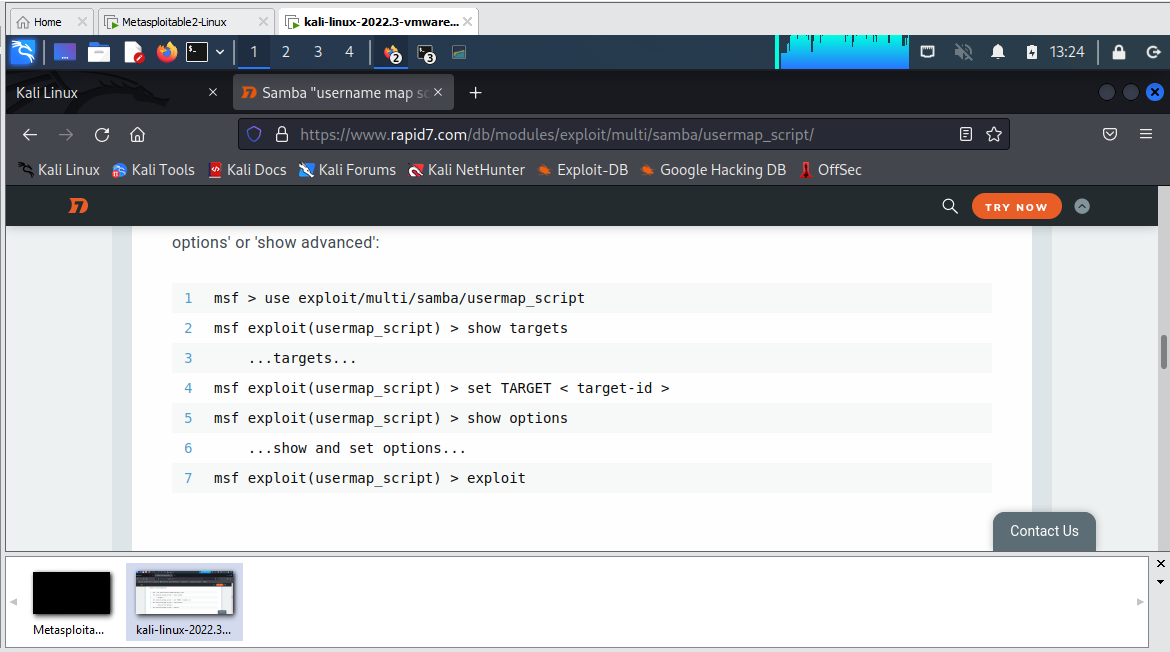
Checking and setting up the required variables before running the auxiliary module



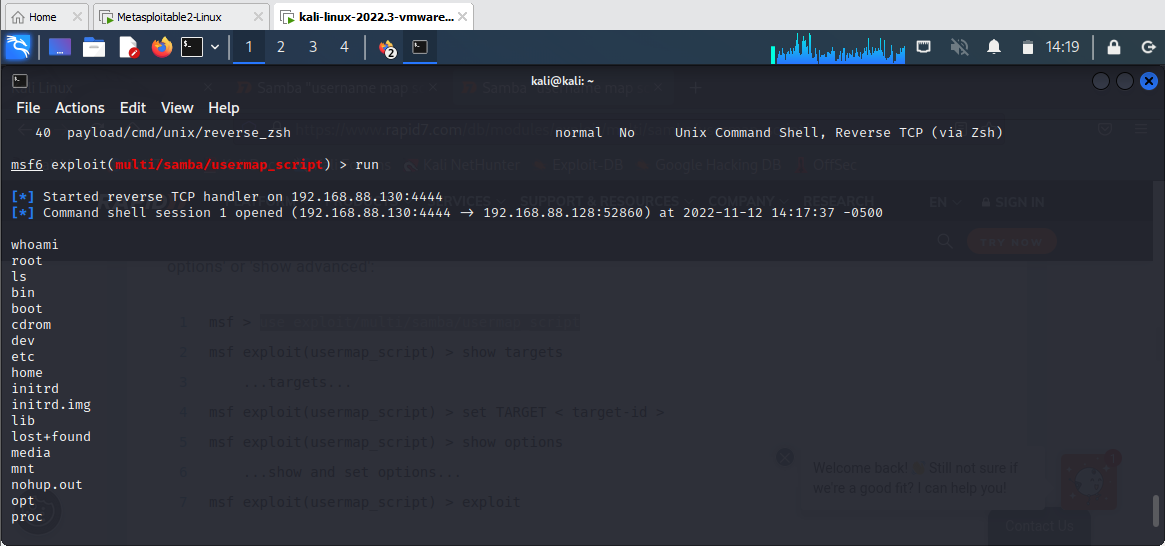
Next we load the module by typing run



From the above output, we take samba 3.0.20-Debian and use the browser to search for the exploit relate to it.



We copy the first module and paste it into metasploit

We set the **RHOSTS** parameter to the target's IP address and executed the module. This opened a command shell connected to the target machine, where we verified our access level with the **whoami** command and confirmed root privileges, allowing us to traverse the target's directories.

**Recommendations**

Based on the findings from Lab 04, it is clear that regular and thorough vulnerability scanning is paramount to identify and mitigate potential security weaknesses. The Metasploitable2-Linux VM demonstrated several exploitable services, highlighting the importance of keeping software up to date with the latest patches and security measures. The lab underscores the need for strong, unique passwords to resist brute-force attacks and the importance of secure communication protocols to replace inherently insecure ones like Telnet.

Organizations should consider the following actions:

1. Implement regular update and patch management protocols to address known vulnerabilities.
2. Use strong, complex passwords and consider multi-factor authentication to enhance security.
3. Replace insecure protocols such as Telnet with secure alternatives like SSH.
4. Conduct regular penetration testing and security training to stay ahead of potential attackers.
5. Isolate critical systems and segment networks to limit the impact of any single compromised point.

**Conclusion**

The active discovery phase in penetration testing, as conducted in Lab 04, is vital in identifying and understanding vulnerabilities within a system. Our exercises with tools like Nmap, Hydra, and the Metasploit framework revealed several critical vulnerabilities, especially on services running on ports 21 (FTP), 22 (SSH), 23 (Telnet), 445 (NetBIOS-SSN), and 80 (HTTP). These vulnerabilities were exploited, providing unauthorized access to the system, which illustrates the risks faced by organizations when security best practices are not followed.

The successful completion of this lab demonstrated the ease with which an attacker could compromise systems that are not properly secured. As such, this report should serve as a call to action for organizations to assess their cybersecurity posture and implement the recommended measures to protect their assets and data effectively.

**References**

1. *Metasploitable 2 Exploitability Guide | Metasploit Documentation*. (n.d.). <https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/>
2. <https://cyberlab.pacific.edu/courses/comp178/labs/lab-1-kali-metasploitable2>
3. Timchenko, M., & Starobinski, D. (2015). A Simple Laboratory Environment for Real-World Offensive Security Education. *Proceedings of the 46th ACM Technical Symposium on Computer Science Education*. <https://doi.org/10.1145/2676723.2677225>
4. Oriental Monkey. (2022, January 18). *Exploiting Vulnerabilities in Metasploitable 2* [Video]. YouTube. https://www.youtube.com/watch?v=vAwQFr4YDaw