Task-1: The first step is to find the IP address of each Virtual Machine (Kali and Metasploitable 2). Use the appropriate command on each VM and find out each VM’s IP Address.

* Using the necessary command line tools, the IP addresses for both VMs were successfully retrieved. These IP addresses are distinct and belong to the same network, enabling networked communication and interaction between virtual computers. This configuration is required for a variety of network-dependent operations, such as data exchange, service configuration, and security testing, in order to ensure effective network performance within the virtualized environment.

1. Kali:

IP Address: 192.168.56.101

A screenshot of a computer

Description automatically generated

1. Metasploitable2:

IP Address: 192.168.56.102

A screenshot of a computer

Description automatically generated

Task-2: Verify that the two VMs can communicate with each other by using the **ping** command to ping each other’s IP Address. (You can quit the pings after about 10-15s using CTRL+C in each VM).

* The 'ping' command was used to show effective two-way communication between the two virtual machines (VMs). This critical network diagnostic tool has proven their ability to correctly send and receive data packets amongst each other. This successful 'ping' test demonstrates that the VMs are correctly setup and integrated, allowing them to exchange data and interact across the network easily. This capacity is critical for a variety of network-dependent tasks such as data sharing, remote access, and VM collaboration, all of which contribute to the overall usefulness and efficiency of the virtualized environment.

1. Kali:

A screenshot of a computer

Description automatically generated

1. Metasploitable2:

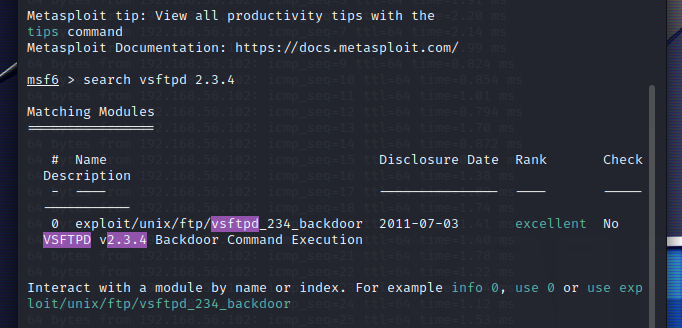
A screenshot of a computer

Description automatically generated

Task-3: From your Kali VM, start up Metasploit and issue the command:

search vsftpd 2.3.4

* Launching the Metasploit framework and executing the'search vsftpd 2.3.4' command in Kali Linux commences a search for Metasploit modules, exploits, and payloads associated with the particular vsftpd version 2.3.4. This command is used in ethical hacking and penetration testing to find flaws in the popular FTP server software vsftpd. The huge database of Metasploit provides information on potential exploits and payloads, which helps cybersecurity experts identify system vulnerabilities and prepare for ethical hacking activities. Users may use this search to find relevant exploit modules that can be used to evaluate the security of systems running vsftpd 2.3.4, therefore contributing to strong network defence and mitigation measures.



Task-4: Still within your Kali VM, issue the command:

use exploit/unix/ftp/vsftpd\_234\_backdoor

* Within Kali Linux's Metasploit framework, the command 'use exploit/unix/ftp/vsftpd\_234\_backdoor' picks the specific exploit module designed to target the vsftpd 2.3.4 FTP server backdoor vulnerability. This module is useful for ethical hackers and penetration testers since it allows them to exploit a known vulnerability in version 2.3.4 of vsftpd. When this module is selected, it may be further configured with the necessary settings and options to conduct an attack against a susceptible FTP server, potentially providing unauthorized access to the target system. It demonstrates Metasploit's ability to discover and exploit security flaws, enabling security experts in bolstering network defences.

A screenshot of a computer screen

Description automatically generated

Task-5: Still within your Kali VM, issue the command:

show options.

* The'show options' command is a critical component of the Metasploit framework, giving users a detailed view of the current configuration and settings for the selected exploit module. When executed in the Metasploit terminal of Kali Linux, it shows a list of possible parameters, along with their default settings and explanations. These options often contain parameters such as 'RHOST' (remote host), 'RPORT' (remote port), 'LHOST' (local host), and 'LPORT' (local port), which are important for tailoring the exploit's behaviour to the details of the target system. The’ show options' command enables ethical hackers and security experts in constructing exploits and payloads precisely, ensuring effective and controlled penetration testing and vulnerability assessment.

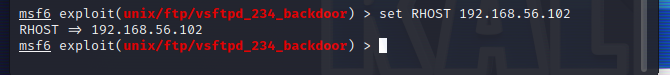
A screenshot of a computer

Description automatically generated

Task-6: Still within your Kali VM, issue the command:

set RHOST {IP Address of Metasploitable 2 VM}

* The Metasploit framework’s ‘set RHOST' command is used to configure the 'RHOST' option, setting the target's IP address. This crucial step guarantees that the exploitation attempt is directed to the proper location, in accordance with the aims of ethical hacking and penetration testing. Setting the 'RHOST' option correctly is critical to the success of the penetration test, allowing security experts to target the attack on the specified susceptible system and precisely analyze its security posture.



Task-7: Still within your Kali VM, issue the command:

Exploit

* The Metasploit framework's 'exploit' command is the final step in conducting an attack against the given target using a selected exploit module. When issued in Kali Linux's Metasploit interface, it launches the exploit against the specified target, seeking to exploit vulnerabilities and obtain unauthorized access. The real penetration test or ethical hacking activity is started with this command. By simulating real-world attack situations, the 'exploit' command aids security experts in identifying and correcting vulnerabilities before bad actors can exploit them. It represents a methodical and proactive approach to network defence and risk reduction.

A screen shot of a computer

Description automatically generated

Task-8

1. What worked well for you?

Ans. Throughout this project, I discovered that my ability to explore and use numerous cybersecurity tools and frameworks, such as Metasploit, really increased. This encounter enhanced my grasp of network penetration testing methodologies and improved my ability to operate in virtualized systems. Furthermore, I was able to apply theoretical information to real-world settings, which improved my problem-solving abilities in the subject of cybersecurity.

1. What didn’t work well and how you resolved the issue(s)

Ans. During the assignment, I experienced difficulties with exploit settings and target identification. These difficulties were wonderful learning opportunities since they forced me to go into the intricacies of the exploited vulnerabilities and comprehend the subtleties of various network settings. To overcome these obstacles, I conducted significant study, read necessary material, and enlisted the help of online groups and mentors. This not only assisted me in resolving the difficulties, but it also improved my research and troubleshooting skills.

1. What is one thing that you were able to learn or accomplish through this Assignment that you did not know prior to starting.

Ans. One notable accomplishment with this work was obtaining a better understanding of the significance of ethical hacking and responsible disclosure. I understood that ethical hacking is more than simply exposing flaws; it is also about raising awareness and ensuring that corporations solve security concerns appropriately. This assignment emphasized the need of ethical hackers in detecting and mitigating possible issues before criminal actors may exploit them. It underlined the ethical and legal duties connected with cybersecurity, an important component of my area that I may not have completely comprehended before to beginning this task.

Reference:

[1] *The best way to learn cybersecurity skills online*. Cybrary. (n.d.). https://www.cybrary.it/

[2] Infosec &amp; Cybersecurity training. OffSec. (2023, August 22). https://www.offsec.com/

[3] Dive into anything. Reddit. (n.d.). https://www.reddit.com/r/AskNetsec/?rdt=54862

[4] Where developers learn, share, &amp; build careers. Stack Overflow. (n.d.). https://stackoverflow.com/

[5] Explore the worldof cyber security. OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation. (n.d.). https://owasp.org/