CYSE425

Mahish Mahendarkar

9/22/2021

Lab 2: Reconnaissance/Enumeration/Vulnerability Scan/Exploitation

Lab 2 purpose:

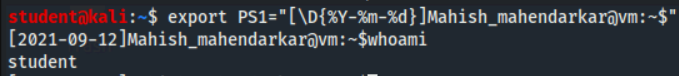
The purpose of this lab is to conduct malicious actions on a compromised target system. This lab 2 is a continuation of lab 1 in which an attack was conducted to yield a compromised system.

**Post-Exploitation**

The purpose of this section is to create a sshd server that allows for access to the compromised system. This allows for access without having to carry out the attack every time.

Pre-Lab configuration settings:

* A Virginia Cyber Range Virtual Machine is used for all Lab activities. This is logged into and hostname is changed as shown below. The specific machine name is “Cyber Range Cyber Basics (2020)”



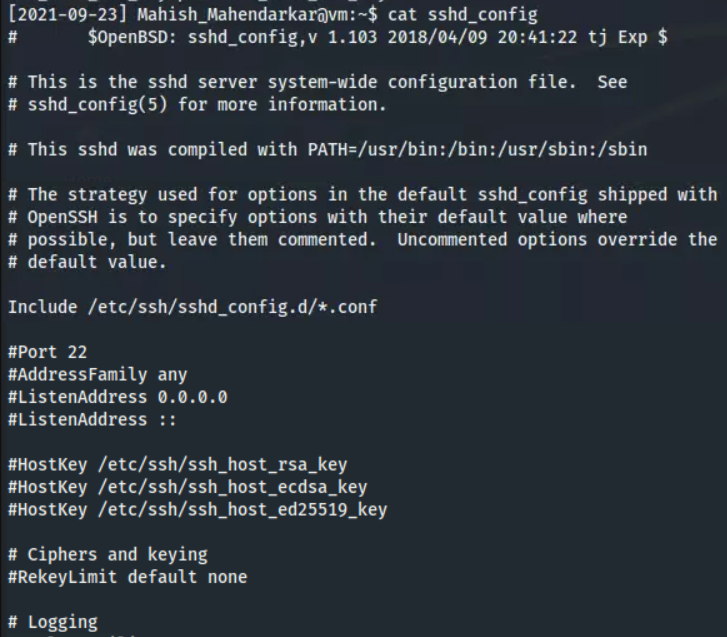
Lab tasks:

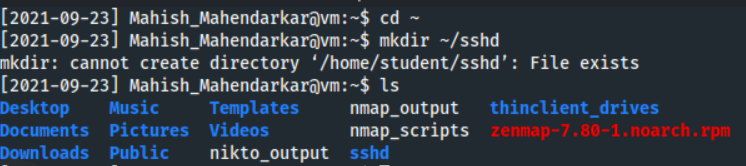
1. Copy the SSH server configuration from the target system

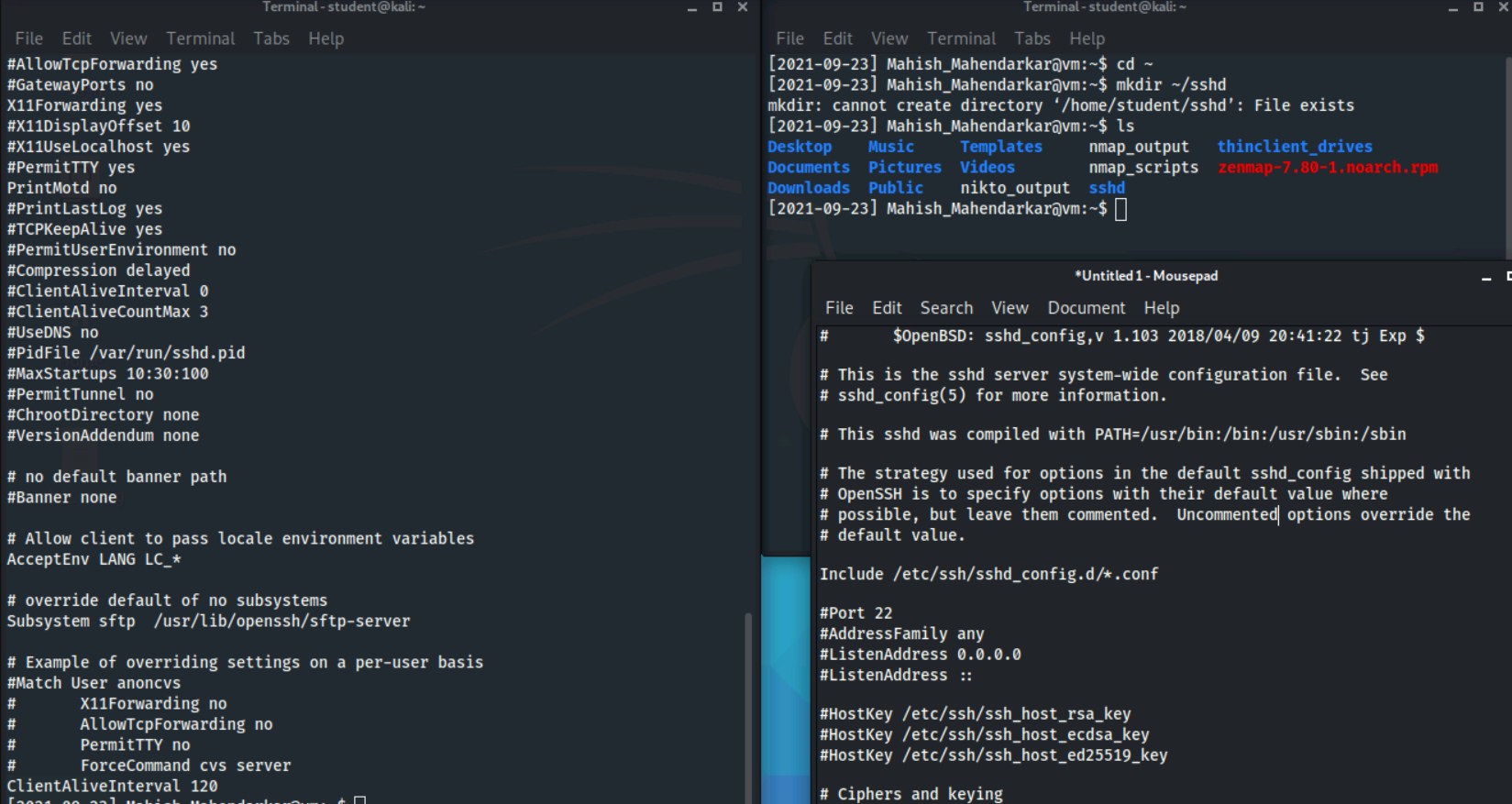
This task dealt with the creation of a new sshd\_config file and a new sshd directory at the path ~/.

**A screenshot of a computer

Description automatically generated with medium confidence**

****

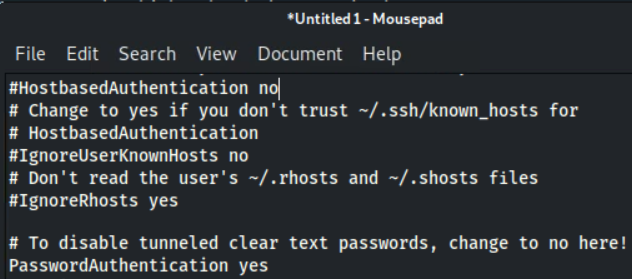
****

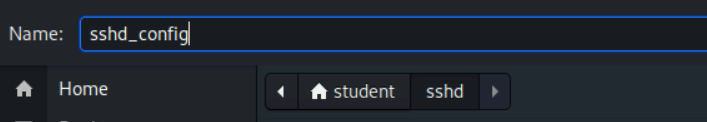
****

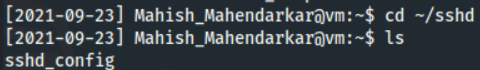
Observations: This task had no issues or errors. The second file has been setup and changes to it can be made via a separate text editor instead of vi.

1. Edit SSH server configuration on the Kali system

This task creates a modified sshd\_config file and places it into a directory called sshd.



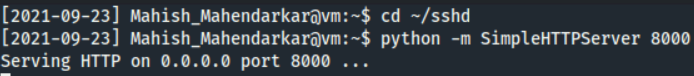


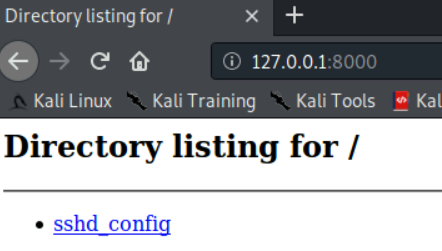


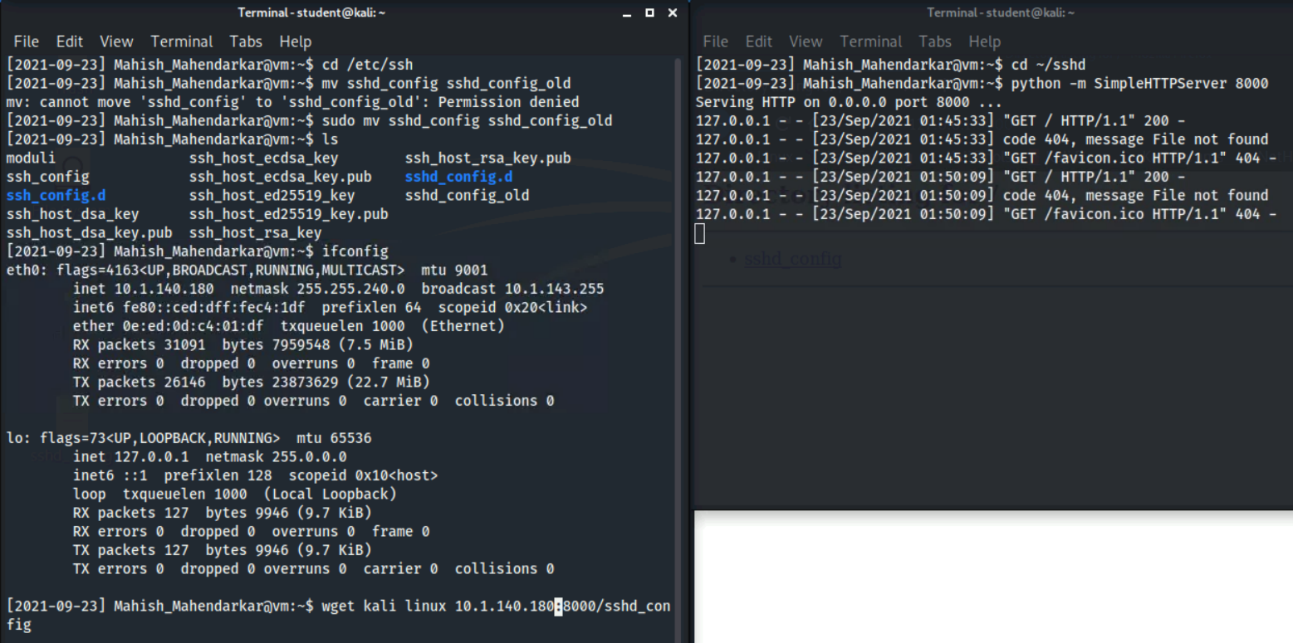
Observations: This task was had no issues. The file modifications and save location were completed successfully.

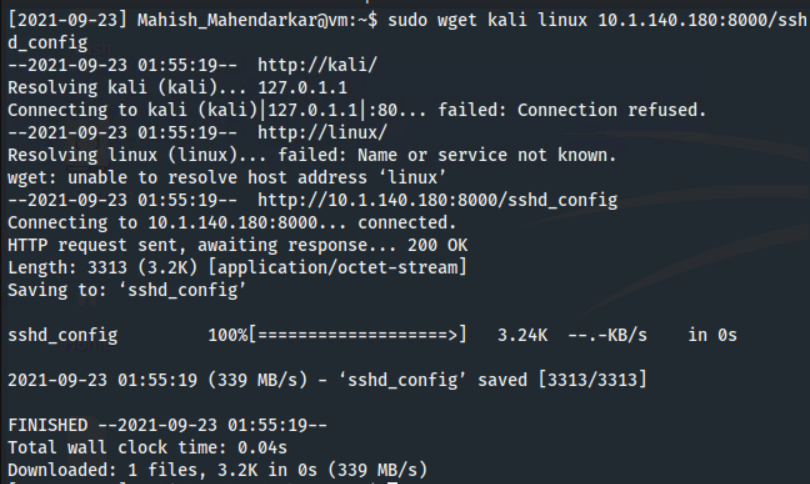
1. Put the modified SSH server configuration back on the target system

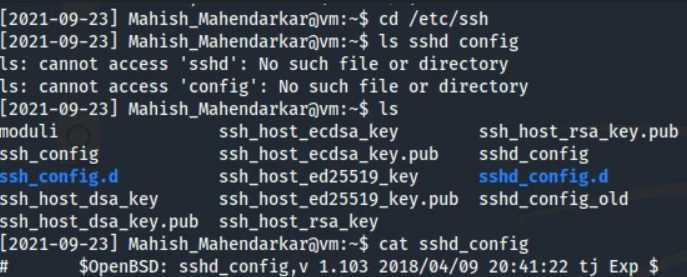
This task brings the modified config file to the target system and the sshd service is restarted effectively loading the new config file settings.









Text

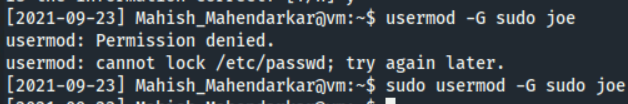
Description automatically generated

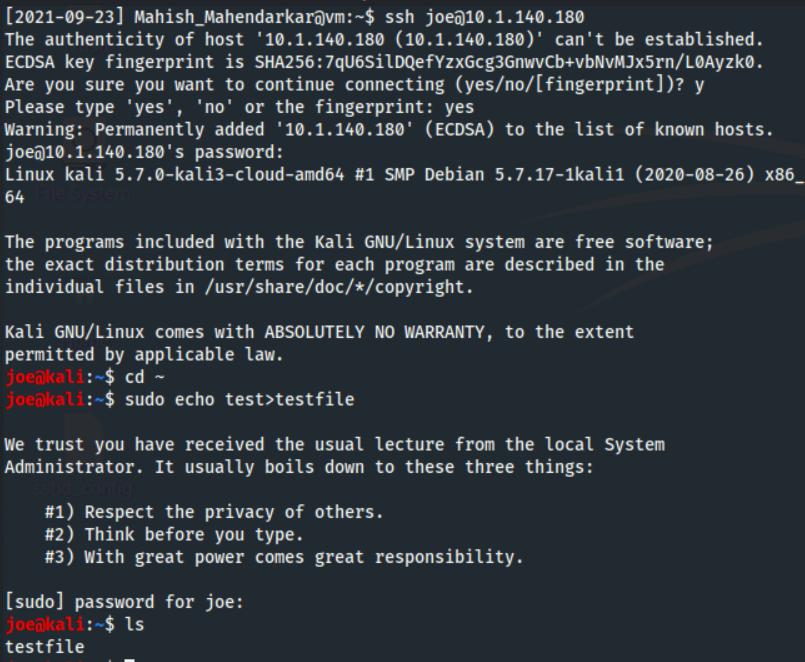
Observations: This task had no issues or errors. The wget command was successful after adding sudo. The file was moved into the new sshd directory created earlier.

1. Create a user with sudo access on the target system

This task involves logging in via ssh to the newly created super user.







Observations: This task had no issues. The user was created and logged into with no issues and the testfile is present within the home directory.

**Exfiltration**

Lab tasks:

1. Access the target system via SSH

This task was accomplished in the previous lab section..

Observations: This task worked as expected. The user was logged into with the password joe.

1. Copy the passwd and shadow files

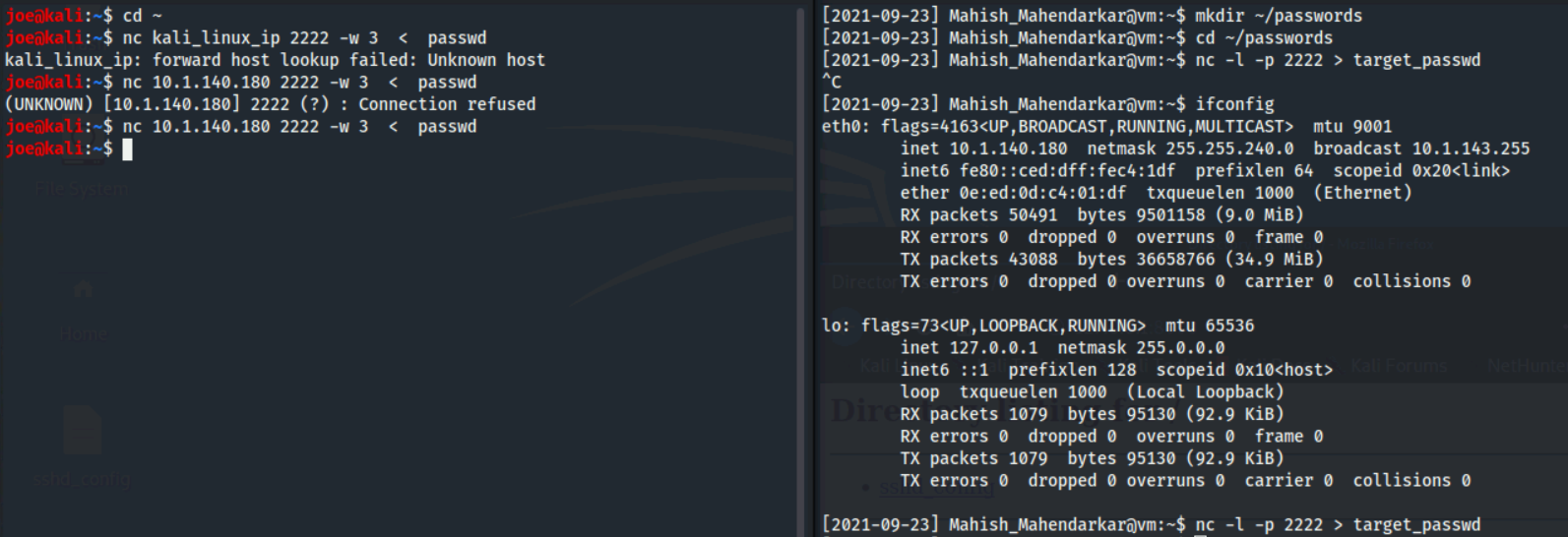
This task is focused on moving files and ownership.

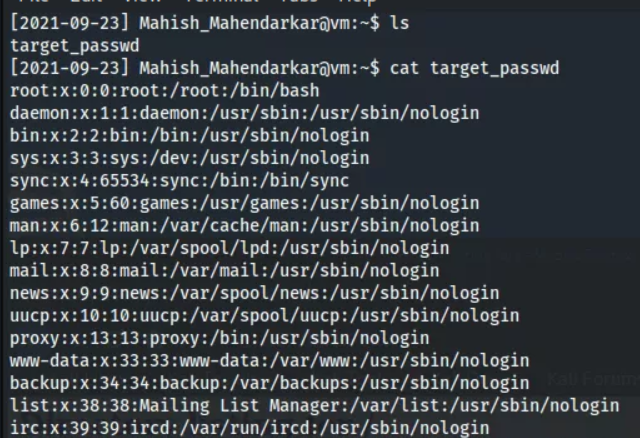


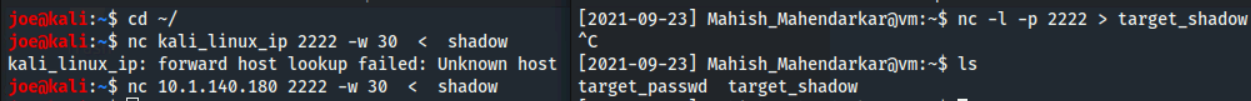
Observations: This task was straightforward. No issues occurred.

1. Exfiltrate the passwd and shadow files

This task pulls the passwd and shadow files via netcat and a new directory for the swiped files.







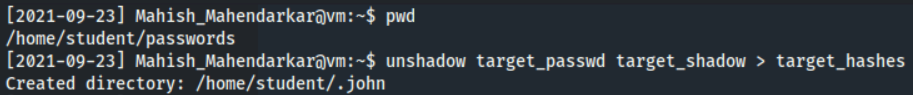
Observations: This task failed a few times because I did not get the listener and sender netcat in the correct order. The last screenshot shows a successful transfer of the shadow file and the first one shows the transfer of the passwd file.

**Password Cracking**

Lab tasks:

1. Merge the passwd and shadow files

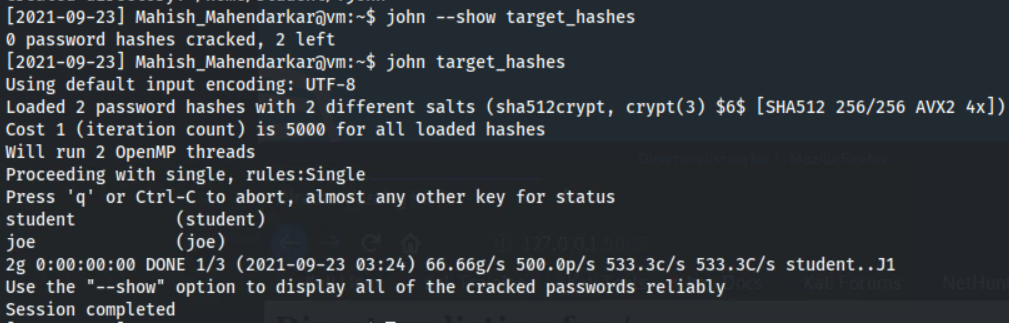
This task merges two files and unshadows both transferred files.



Observations: This task had no issues.

1. Crack the passwords

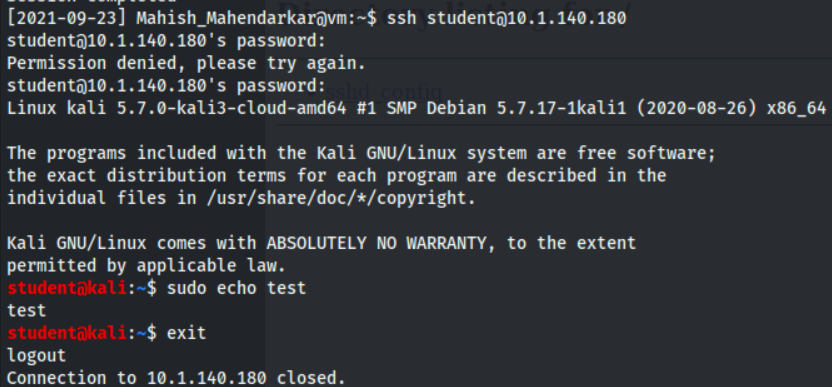
This task uses John the Ripper to crack password.



Observations: This task failed initially but after modifying the command to run john the ripper the passwords were cracked and shown.

1. Test the cracked account

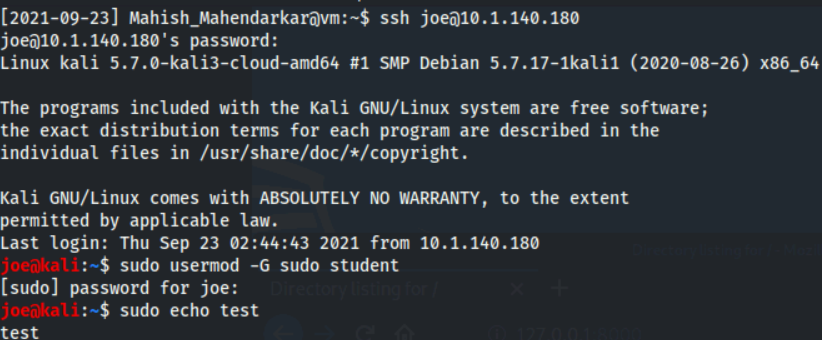
This task attempts to ssh into the target system.



Observations: This shell was accessed and then exited with full sudo ability which was unexpected. The connection was able to close successfully.

1. Upgrade the cracked account

This task involves upgrading the previously made student account that was successfully logged into.



Observations: This task involved using sudo user joe to upgrade the student user. This is how an acceleration of privilege attack is actually conducted.

**Creating a Backdoor**

The purpose of this reconnaissance

Lab tasks:

1. Setup a backdoor with netcat

This task created a cache with sudo credentials stored for backdoor purposes in the future.

Graphical user interface

Description automatically generated with medium confidence

Observations: This task was successful and no issues occurred.

1. Verify the backdoor with netstat

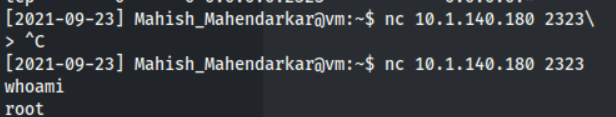
This task verifies the existence of the previous backdoor using detail netcat commands.



Observations: This task shows an active connection corresponding to the port that is associated with the backdoor.

1. Connect to the backdoor with netcat

This task connects to the target using the backdoor previously created.



Observations: The backdoor was used and full root privileges were verified, a success!

**Cleaning Up**

Lab tasks:

1. Remove the user account you created



Observations: This task was straightforward

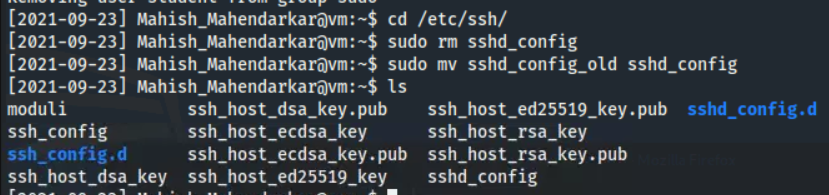
1. Remove the student account from the sudo group



Observations: This task was successful.

1. Put the original sshd\_config file back

This task involves moving of files to maintain the original system settings.



Observations: This task was successful; the files are verified as well in the last commands results.

1. Restart the ssh server





Observations: This task was successful. No errors were thrown during the restart.

1. Backout of the backdoor

Observations: Exit command was typed and the terminal and associated ssh shells all closed, A successful lab!

---------------------------------------------------------------------------------------------------------------------