Vulnerability Penetration Test Report

v.2.0

Khashika S@khashikas.ece2021@citchennai.net

CONTENTS

1.INTRODUCTION:

This assessment contains all items that were used to do penetration testing on the target machine i.e. academy machine .

2.OBJECTIVE:

The main objective of this assessment is to perform an internal penetration test against the academy machine.Our goal is to find the root flag.

3.RECOMMENDATIONS:

Before switching on the VM it is recommended to check both the attacker machine and target machine were in Bridged network.If not edit the VM and change the network settings to Bridged

4.STEPS FOLLOWED:

- Login to the academy machine by using username and password in the root password.txt file.
- By default this virtual machine's network settings were disabled ,so there won't be any ip addresses.
- Next step is to find the ip address of the academy machine.It is done by following procedures:
    1. Search ens33 no ip address in the browser and enter No ip address on VMware running centos.
    2. Run the following command
       `ip link set dev ens33` `up-used to set up ens33`
       `dhclient -v ens33`-it is used to request an ip address from DHCP server to the network interface ens33.
    3. Now check the ip address of the academy machine.My ip address is found to be 192.168.1.107.
- To configure SIEM cloud instances in this machine install splunk forwarder and configure it with our splunk cloud so that any malicious activity can be monitored and tracked.Follow these steps.

1.Open command prompt in windows. to copy the spl file to the academy VM. using command.

scp splunkclouduf.spl root@[academy ip]

2.Download the splunk universal forwarder in academy using command

wget -O splunkforwarder-9.2.0.1-d8ae995bf219-linux-2.6-amd64.

3. To install and configure splunk universal forwarder use the following commands,

dpkg -i splunkforwarder-9.2.0.1-d8ae995bf219-linux-2.6-amd64.deb

export SPLUNK_HOME=”/opt/splunkforwarder”

mkdir $SPLUNK_HOME

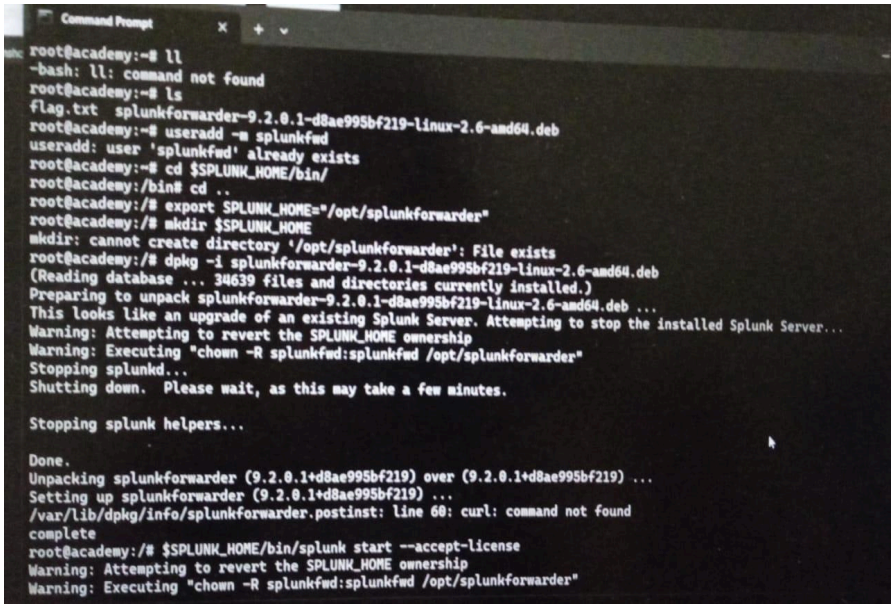
cd /opt/splunkforwarder/bin

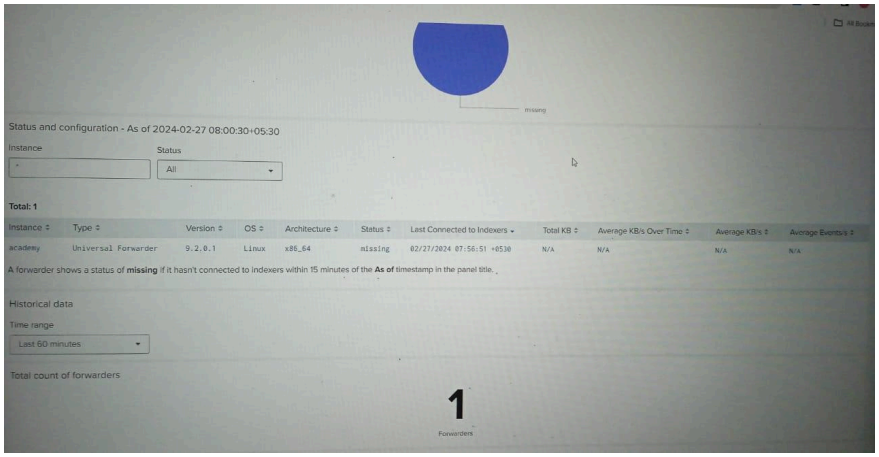
./splunk start –accept-license

./splunk install app/splunkclouduf.spl

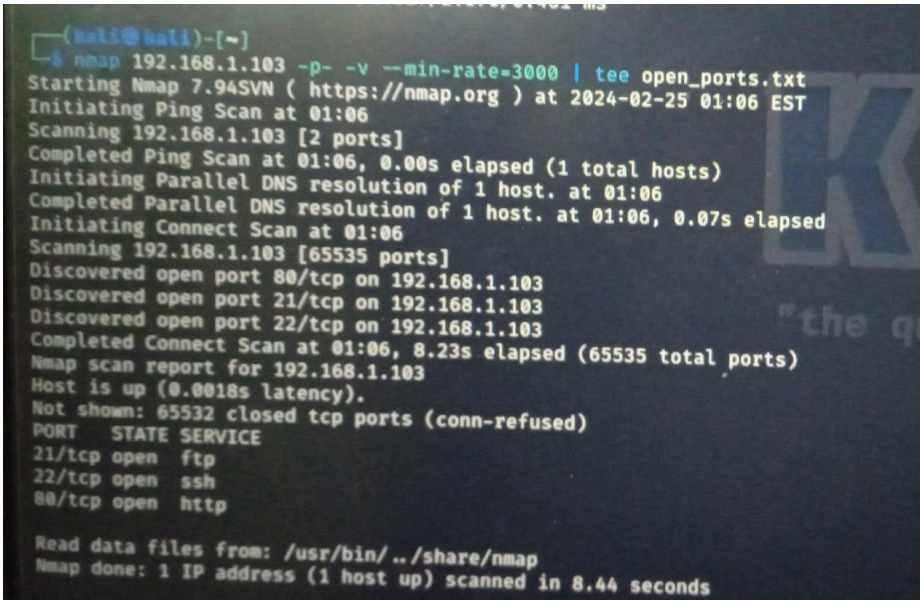
./splunk add forward-server username:port(used to add forward server in splunk for forwarding logs)

./splunk add monitor /var/log(used to monitor logs in splunk)





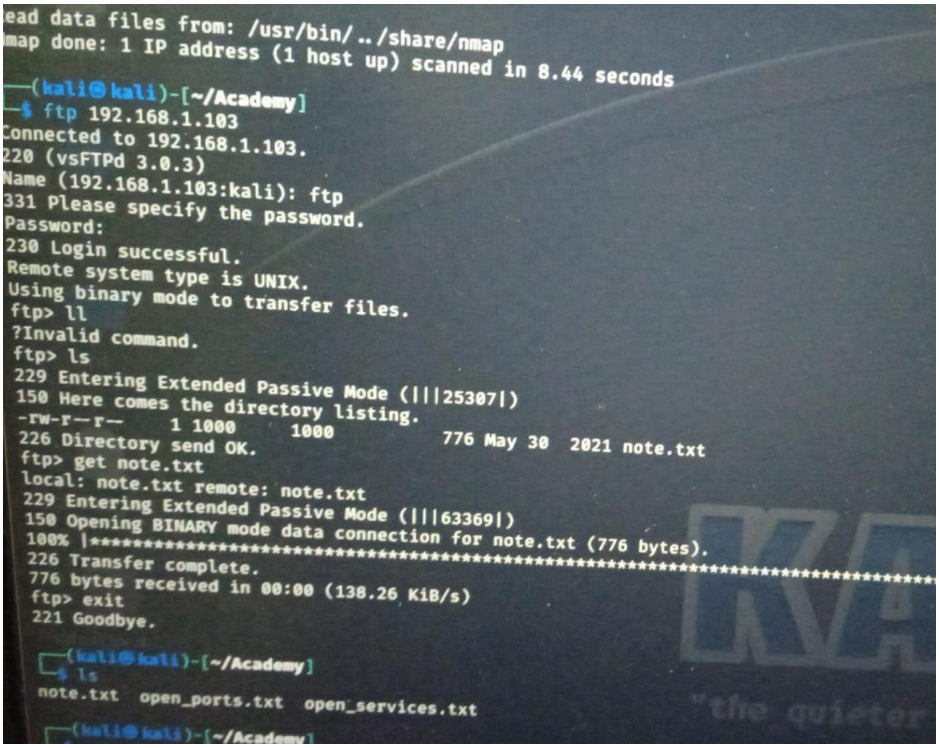
- To find the login page follow these steps:
    1. Ping kali with academy.
    2. nmap is done with minimum rate =3000 and the results are stored in open_ports.txt

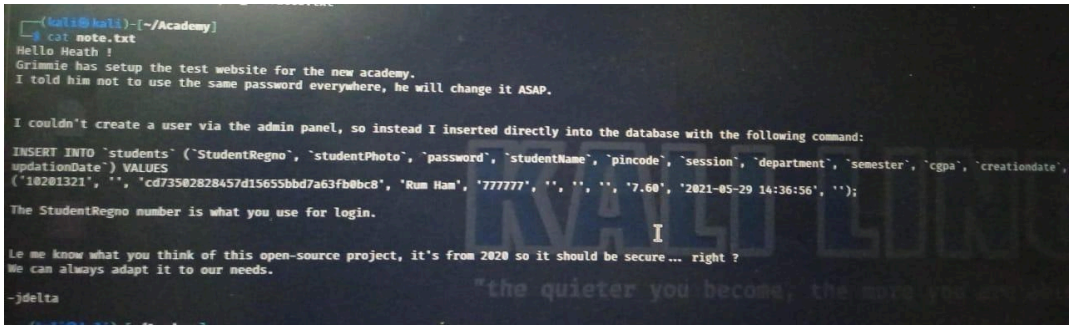


3. Port scan reports:

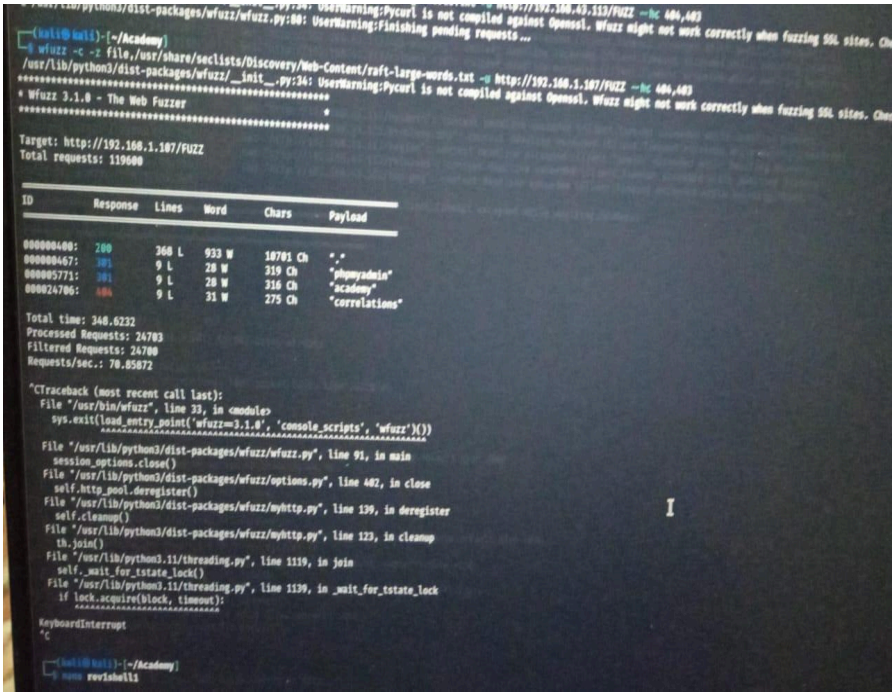
IP Address	**Ports Open**
192.168.1.107	**FTP**: 21 **SSH**:22 **HTTP**:80

4. After scanning the ftp note.txt file is found.Student regno and hash code are found from this file.

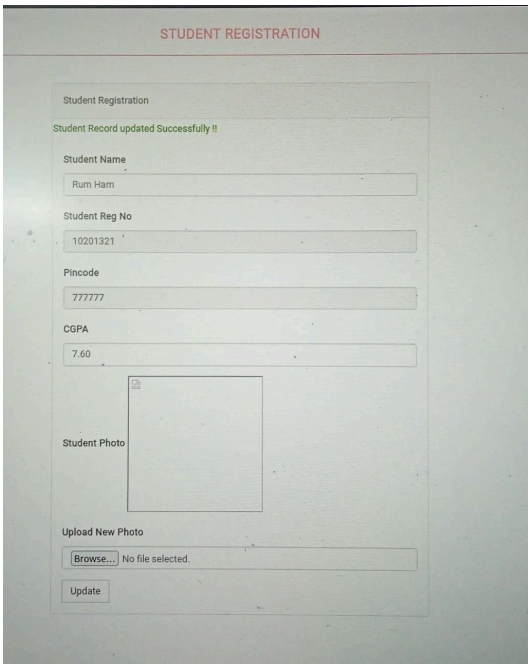




5. Use MD5 centre to crack the password.The password is found to be “student”.
6. In the website there is a default Apache web page.To find other web pages.wfuzz is used.



7. By using academy we enter a login page .By entering username as student regno and password “student”.

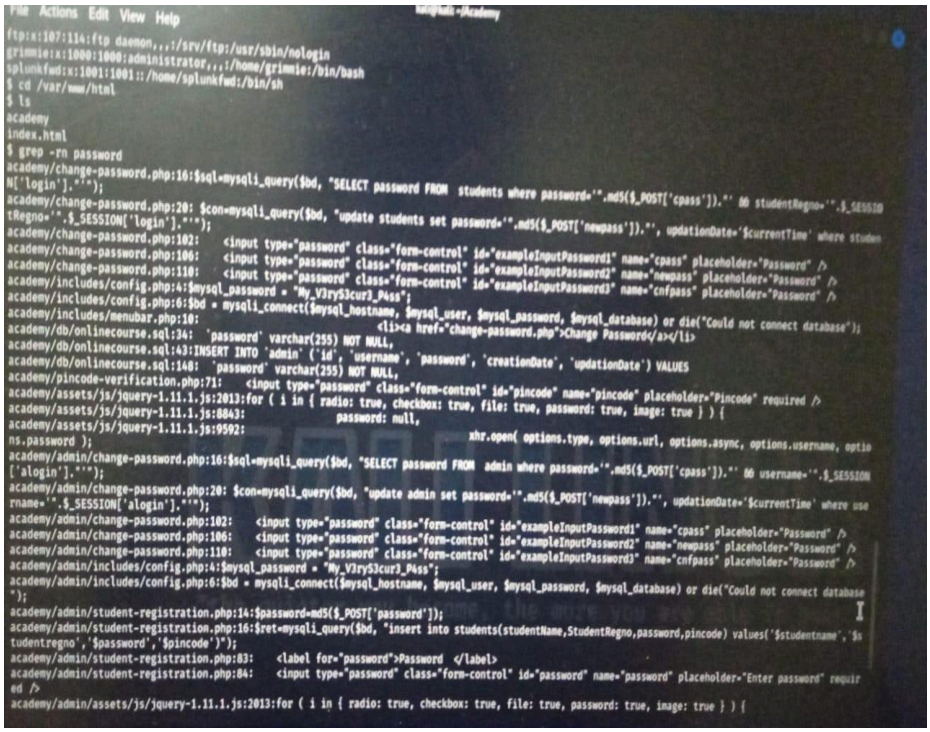


- To perform file upload vulnerability reverse shell is used.It is done by

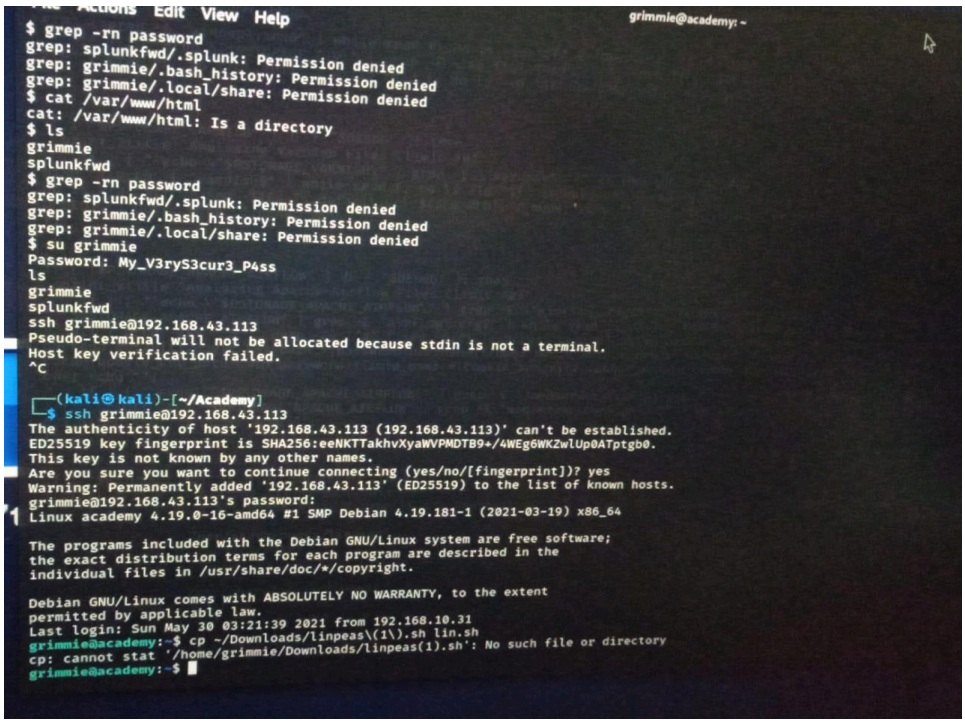
1. Go to revshells.com
2. Enter the port number and kali/windows ip address
3. Select PHP Pentest and copy the code
4. Create a file .php extension[revshell.php] and save the code.
5. Use -nc lvnp [portnumber] to gain access to the target machine.
6. After this in the student profile page ,on student photo upload revshell.php and update.
7. To trigger the reverse shell right click on the photo and open this in new page.
8. Wait for some time to gain access to the machine ,whoever clicks our link.
9. After obtaining the access our next step is to find the usernames in the machine for this use,

cat /etc/passwd

10. We found two users: root and grimmie.



- **Horizontal privilege escalation: (www->grimmie)**

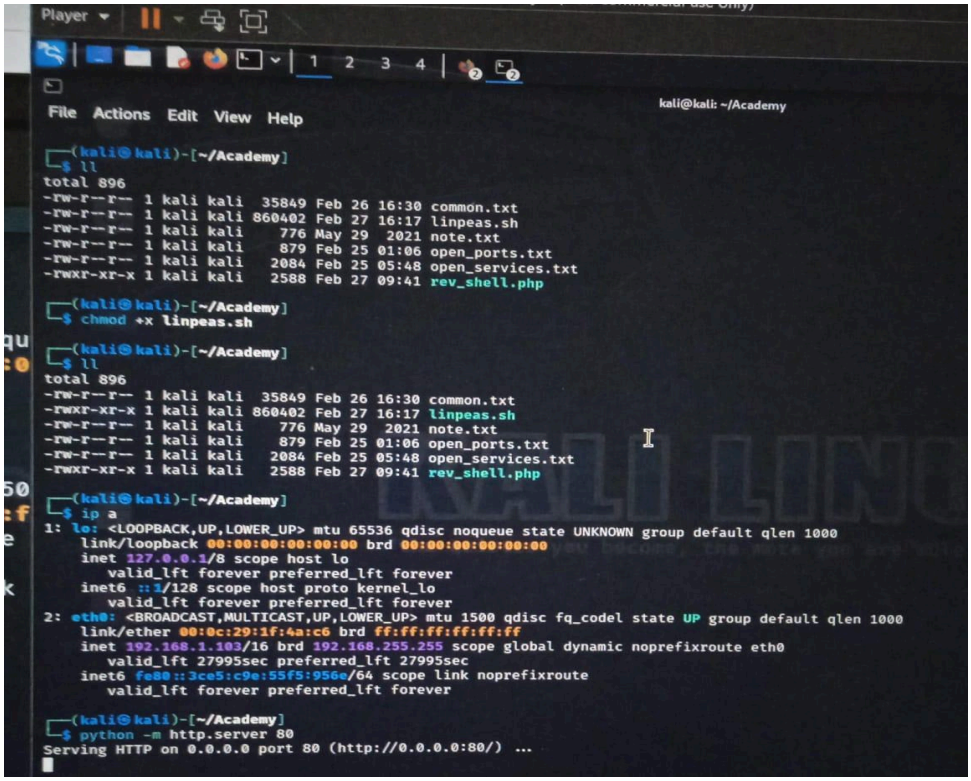


1.Now go to the website using default path /var/www/html.Two websites academy and index.html were found.

2.grep -rn password command is used to get all the passwords.From this we can find the password for grimmie as “My_V3ryS3cur3_P4ss”.

3.Switch the user to grimmie and enter password.

- **Vertical privilege escalation: (grimmie ->root)**

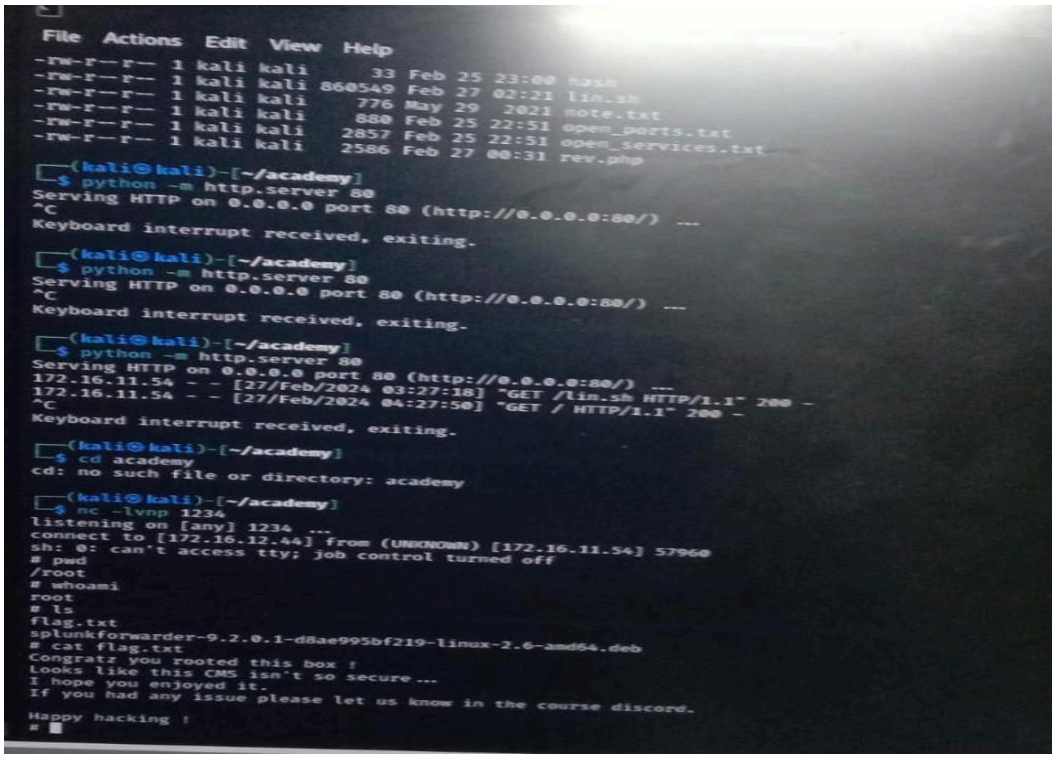


1.First download linpeas.sh(Linux privilege escalation used to search paths for suitable privilege escalation in linux) from github ans save it in academy .

2.Give the execute permission for linpeas.sh.

3.To transfer all the files in this particular academy folder use command,

python -m http.server 80



4.After transferring go to grimmie user, download these files in linpeas directory.

5.In grimmie user go to home and do ll ,two files were found: backup.sh and academy.

6.Read backup.sh copy and paste it in a new file called backup.sh .Now again go to reverse shell generator, enter port number and kali ip address,copy the bash code.

7.Once again listening is done and now we have access to the root,we have found our target file flag.txt.

8.After reading the flag file ,our message is found to be **“Happy Hacking” !**