Sam Holroyd
CYBE 467
PT 1
3/7/24

Pen Test 1

Executive Summary

This Pen Test was conducted on the target machine cybe467ctf2.1 from a kali VM. The goal of the test was to discover security weaknesses and extract important data (8 flags) back to the kali VM.

Findings and Recommendations

Open SSH - The ssh service currently running lacks basic security features. The SSH server should not allow password authentication. It should only allow connection if the user has the proper ssh key.

Apache web server - The web server that is currently running on the target machine produces an error when submitting the form on the landing page. Once the form is submitted a database problem occurs because of invalid credentials. This will cause an error message that displays sensitive information about the system.

User Passwords - The user passwords on this machine are compromised. The users brown and huggins have very insecure passwords that can found on the rockyou password list. User passwords should be changed regularly and follow a password rule scheme.

File Directory permissions - Certain directories such as /var can be accessed by non privileged users. This can lead to large data breaches or in this case privilege escalation.

Employee training - Sensitive data can be found in some users personal directories. Including but not limited to Trash, Music, Download directories. Users should be educated on how to properly delete sensitive data when finished with it.

All sensitive data was able to be viewed (not encrypted) easily by a non root user once the data has been copied out of its original location. It is highly recommended to use encryption to secure important data files.

Introduction

Pen test 1 will be conducted on the CSSP instance cybe467ctf2.1. The goal of this pen test is to gain access to the system and capture eight flags. To gain more information about the machine passive reconnaissance will be completed and the target website will be examined. The purpose of this pen test is to capture eight files or “flags” that are placed into the target machine. The goal is to gain access, establish a backdoor, and exfiltrate the flags to the kali vm where the pen test will be performed.

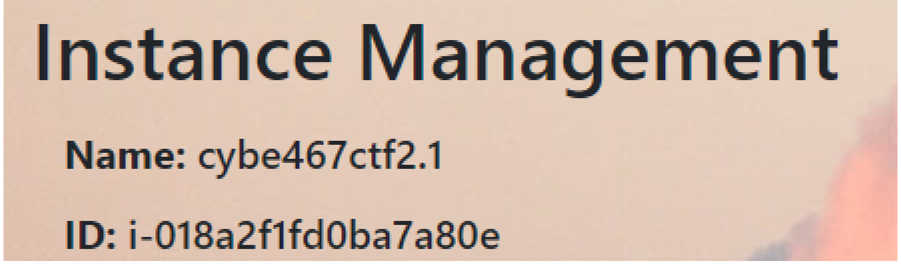
Scope

The scope of this penetration testing assignment is focused on the cybe476ctf2.1 machine and its associated services. The pen test aims to identify vulnerabilities and potential security weaknesses within the target machine and its hosted website. All services will remain active during the duration of the test. All web applications hosted on the target machine will be scanned and could be exploited. All accessible network services, such as ssh,https, etc. will be scanned and analyzed for vulnerabilities. It is intended to thoroughly explore the file systems and attempt to escalate privileges, including attempting to log in as the root user if the password can be discovered. Password cracking software will be used to gain an initial foothold on the machine. Existing user passwords will not be changed or modified in any way. Additional users can be created to help aid in the testing process. Any files in the system will be looked at but not modified. Some select files, the flags, will be transferred to an external machine to be examined further. Log files that are created due to the pen test will be deleted. These actions are essential for identifying potential security weaknesses and vulnerabilities within the target system.

Methodology

Setup

The target machine for the pen test is the cybe467ctf2.1, hosted on the cssp website. You will see multiple different IP addresses used throughout the screen shots. This is because of the hour and a half time limit per instance. For the attacker machine, a standard kali Vm will be used.



Instance Management

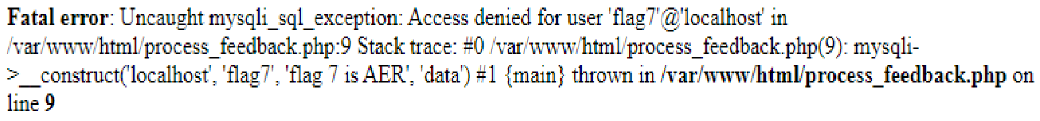
Name: cybe467ctf2.1

ID: i-018a2f1fd0ba7a80e

Information Gathering

- Passive reconnaissance

The target machine is hosting an Apache web server that can be accessed by searching the public IP of the target machine. Upon visiting the website, an about us page is displayed. From the about us page, potential usernames can be extracted. Five names are mentioned on the page. Chatgpt assisted with the creation of a username list based on the names: Gordon Gee, Bob Huggins, Neal, Brown, Dr Devine, and Kro. The website also allows for feedback to be submitted to wvu. Completing the form causes an error with the php service. The error message provides details about where the php service files are located.

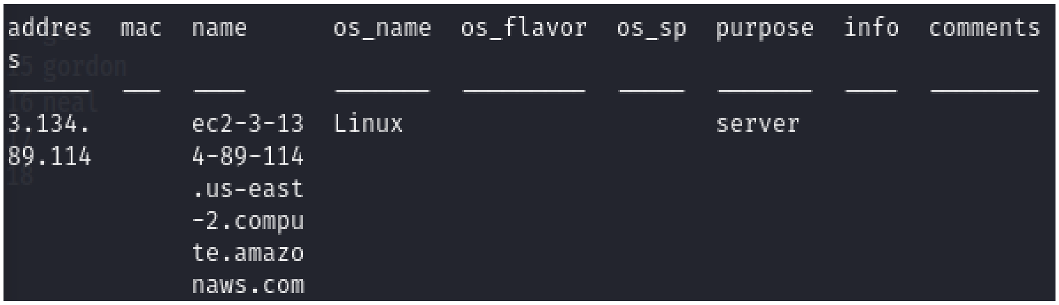


```
Fatal error: Uncaught mysqli_sql_exception: Access denied for user 'flag7'@'localhost' in /var/www/html/process_feedback.php:9 Stack trace: #0 /var/www/html/process_feedback.php(9): mysqli->__construct('localhost', 'flag7', 'flag 7 is AER', 'data') #1 {main} thrown in /var/www/html/process_feedback.php on line 9
```

- Active reconnaissance

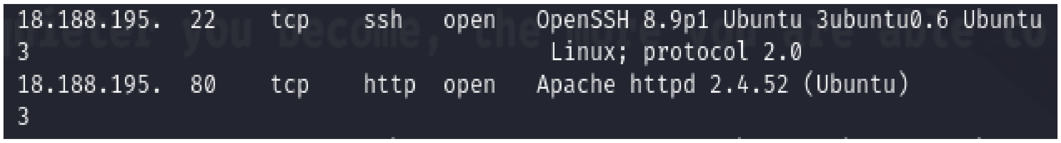
The metasploitable framework 6 will be used to conduct active probing of the target system. A standard nmap scan is performed using: db_nmap -sV 18.188.195.3

OS: Linux



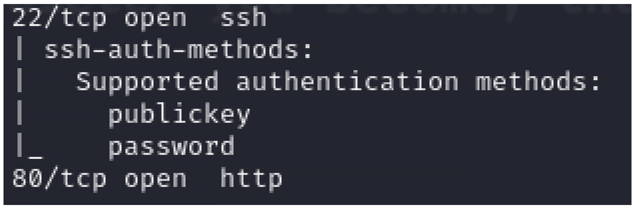
```
addres  mac  name      os_name  os_flavor  os_sp  purpose  info  comments
s
______  ___  ____      _______  _________  _____  _______  ____  ________
3.134.       ec2-3-13  Linux                      server
89.114       4-89-114
             .us-east
             -2.compu
             te.amazo
             naws.com
```

Services: OpenSSH and Apache httpd



```
18.188.195.  22    tcp    ssh   open   OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 Ubuntu
3                                       Linux; protocol 2.0
18.188.195.  80    tcp    http  open   Apache httpd 2.4.52 (Ubuntu)
3
```

The OpenSSH server is configured to use password authentication. To prove that password authentication is on, the nmap scan : nmap --script ssh-auth-methods 18.188.195.3 is used.

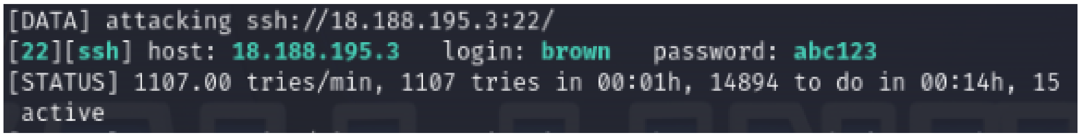


```
22/tcp open  ssh
| ssh-auth-methods:
|   Supported authentication methods:
|     publickey
|_    password
80/tcp open  http
```

In order to gain access to the target system using OpenSSH a username and password is required. Metasploit was used for user enumeration on the SSH service, but no users were found using this method.

Exploitation

Since the OpenSSH service is running on the target machine and port 22 is open, hydra password cracker was used to brute force ssh passwords. With the data found from the information gathering step a list of possible usernames was created for hydra. All names found were on the About US section on the target's website. Hydra was able to crack the password for the user brown by providing hydra with the userlist and the first 1000 lines of the rockyou password list.

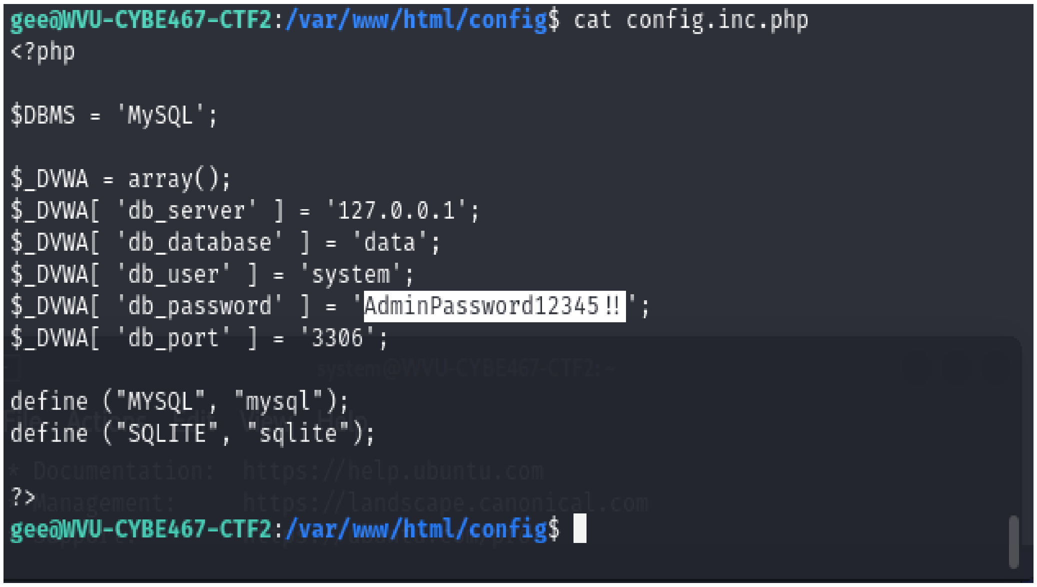


```
[DATA] attacking ssh://18.188.195.3:22/
[22][ssh] host: 18.188.195.3   login: brown   password: abc123
[STATUS] 1107.00 tries/min, 1107 tries in 00:01h, 14894 to do in 00:14h, 15
 active
```

Since couch brown’s username and password has been cracked, ssh was used to connect to the target machine. Once a shell is obtained, privilege escalation can begin.

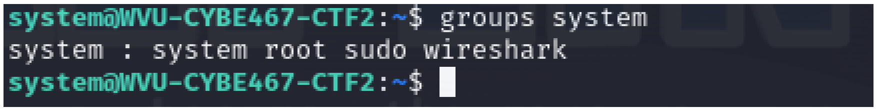
Establish Persistence

With the information from the webpage after submitting a form, A flag is located in the /var/www/html/proccess_feedback.php file. The var directory should only be able to be accessed by privileged users, but the user brown can. Using this misconfiguration the files for the website can be examined. Upon examination of a file called config.inc.php a password can be found for the system user.



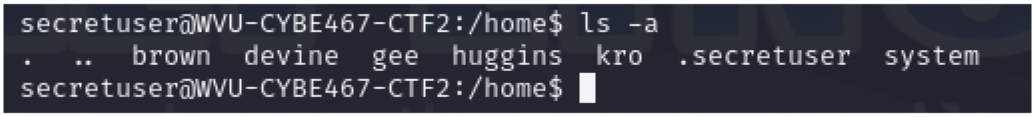
```
gee@WVU-CYBE467-CTF2:/var/www/html/config$ cat config.inc.php
<?php

$DBMS = 'MySQL';

$_DVWA = array();
$_DVWA[ 'db_server' ] = '127.0.0.1';
$_DVWA[ 'db_database' ] = 'data';
$_DVWA[ 'db_user' ] = 'system';
$_DVWA[ 'db_password' ] = 'AdminPassword12345!!';
$_DVWA[ 'db_port' ] = '3306';

define ("MYSQL", "mysql");
define ("SQLITE", "sqlite");

?>
gee@WVU-CYBE467-CTF2:/var/www/html/config$
```

Once logged in as the system, the group's command is used to see the privileges of the user.

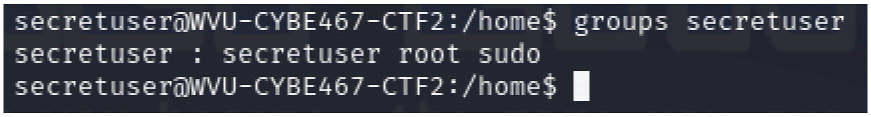


```
system@WVU-CYBE467-CTF2:~$ groups system
system : system root sudo wireshark
system@WVU-CYBE467-CTF2:~$
```

From the screen shot, the system user is in the sudo and root groups. This user will allow access to the sudo -i command to obtain a root shell. Once a root shell is obtained a secretuser can be created. The secretuser's home directory can be prefixed with a period to hide the directory. The secretuser is also added to the sudo group so that sudo access is granted.



```
secretuser@WVU-CYBE467-CTF2:/home$ ls -a
.  ..  brown  devine  gee  huggins  kro  .secretuser  system
secretuser@WVU-CYBE467-CTF2:/home$ 
```

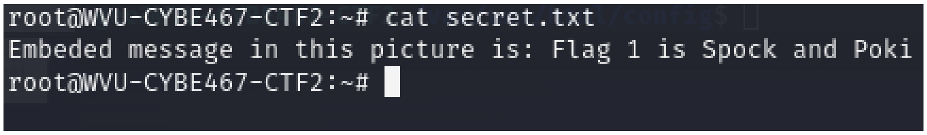


```
secretuser@WVU-CYBE467-CTF2:/home$ groups secretuser
secretuser : secretuser root sudo
secretuser@WVU-CYBE467-CTF2:/home$ 
```

Exfiltration

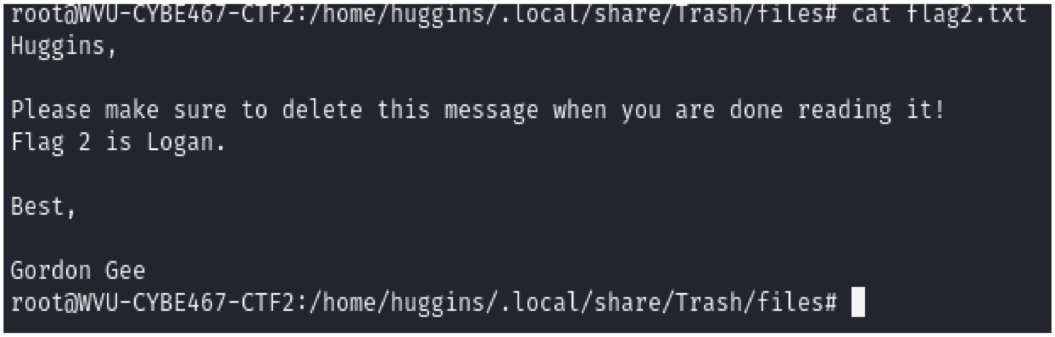
Now that a privileged user has been obtained, the search for the flags begins.

- Flag 1 - Spock and Poki
  In the root directory a file named secret.txt can be found. Using that cat command the following flag is found.



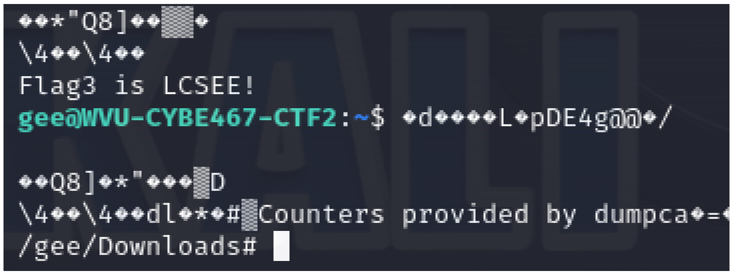
```
root@WVU-CYBE467-CTF2:~# cat secret.txt
Embeded message in this picture is: Flag 1 is Spock and Poki
root@WVU-CYBE467-CTF2:~# 
```

- Flag 2 - Logan
  Located in huggins's trash bin, an old email from gee was left. In the email Flag 2 can be found.



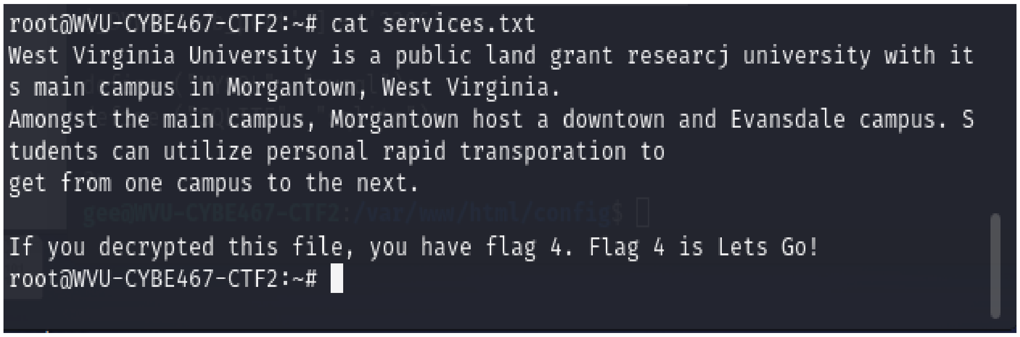
```
root@WVU-CYBE467-CTF2:/home/huggins/.local/share/Trash/files# cat flag2.txt
Huggins,

Please make sure to delete this message when you are done reading it!
Flag 2 is Logan.

Best,

Gordon Gee
root@WVU-CYBE467-CTF2:/home/huggins/.local/share/Trash/files# 
```

- <u>Flag 3 - LCSEE!</u>
  A packet capture file can be found in gee’s downloads folder. When using the cat command flag 3 is found.



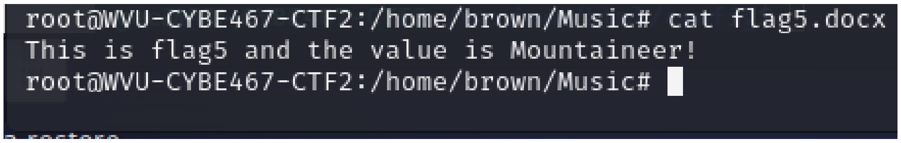
```
��*"Q8]��▒�
\4��\4��
Flag3 is LCSEE!
gee@WVU-CYBE467-CTF2:~$ �d����L�pDE4g@@�/

��Q8]�*"���▒D
\4��\4��dl�*�#▒Counters provided by dumpca�=�
/gee/Downloads# █
```

- <u>Flag 4 - Lets Go!</u>
  This flag is located in the services.txt file found in the root directory. When the contents of the file are displayed flag 4 is found.



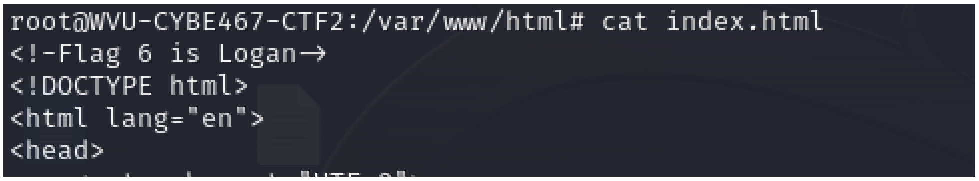
```
root@WVU-CYBE467-CTF2:~# cat services.txt
West Virginia University is a public land grant researcj university with it
s main campus in Morgantown, West Virginia.
Amongst the main campus, Morgantown host a downtown and Evansdale campus. S
tudents can utilize personal rapid transporation to
get from one campus to the next.

If you decrypted this file, you have flag 4. Flag 4 is Lets Go!
root@WVU-CYBE467-CTF2:~# █
```

- <u>Flag 5 - Mountaineer!</u>
  A file named Flag5.docx can be found in brown’s music directory.



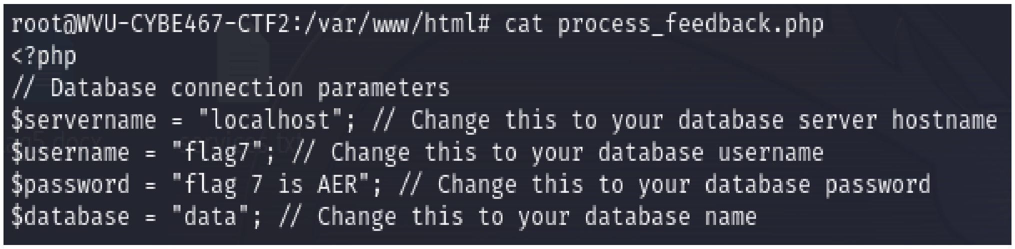
```
root@WVU-CYBE467-CTF2:/home/brown/Music# cat flag5.docx
This is flag5 and the value is Mountaineer!
root@WVU-CYBE467-CTF2:/home/brown/Music# █
```

- <u>Flag 6 - Logan</u>
  This flag can be found in the html directory for the apache web server. The file name is index.html



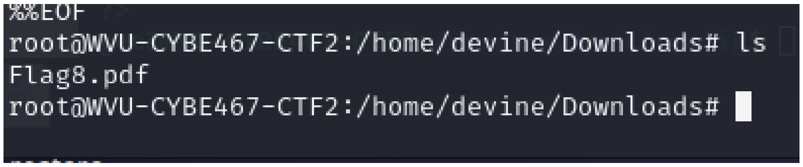
```
root@WVU-CYBE467-CTF2:/var/www/html# cat index.html
<!-Flag 6 is Logan→
<!DOCTYPE html>
<html lang="en">
<head>
```

- Flag 7 - AER
  This flag can originally be seen by submitting the form on the target machine's website and will display an error message containing the flag. The file for the flag can be found in the html directory named process_feedback.php



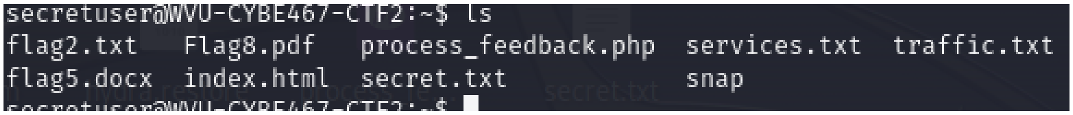
```
root@WVU-CYBE467-CTF2:/var/www/html# cat process_feedback.php
<?php
// Database connection parameters
$servername = "localhost"; // Change this to your database server hostname
$username = "flag7"; // Change this to your database username
$password = "flag 7 is AER"; // Change this to your database password
$database = "data"; // Change this to your database name
```

- Flag 8 - Phishing
  This flag can be found in devine's download folder. The file is named Flag8.pdf and contains a QR code. The QR code was scanned using an Iphone and the riddle "what's a favorite hackers season?" is found. The answer of course being phishing.

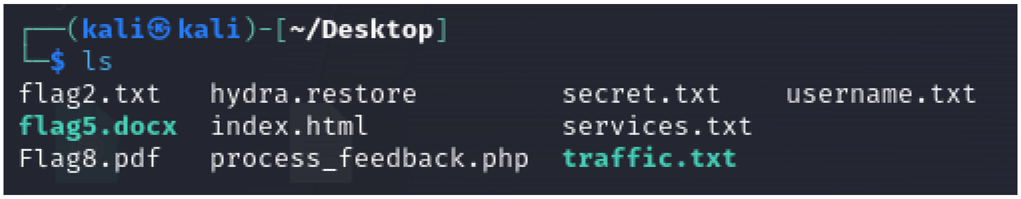


```
%%EOF
root@WVU-CYBE467-CTF2:/home/devine/Downloads# ls
Flag8.pdf
root@WVU-CYBE467-CTF2:/home/devine/Downloads# █
```

Once a flag is located it is copied into the home directory of the secretuser. From there the flags can be exfiltrated using scp to the kali machine. Flags 3 and 5 need their permissions changed so that the secret user has the privilege to copy it to the kali machine.



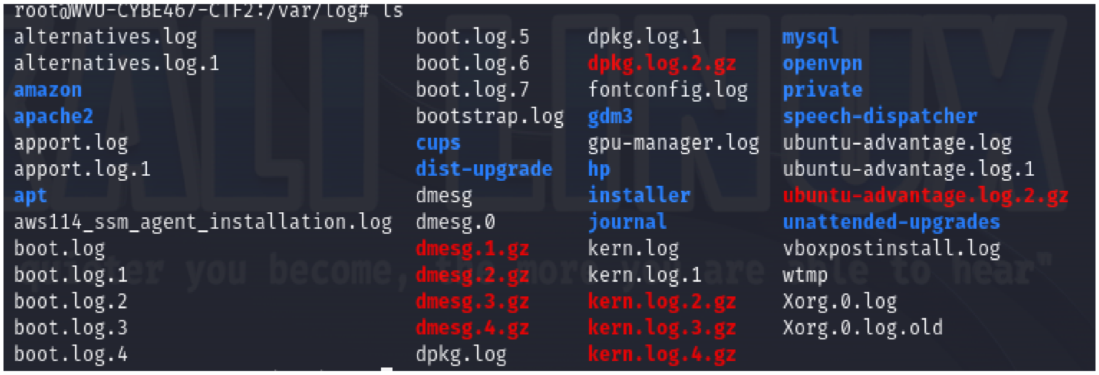
```
secretuser@WVU-CYBE467-CTF2:~$ ls
flag2.txt   Flag8.pdf   process_feedback.php  services.txt  traffic.txt
flag5.docx  index.html  secret.txt            snap
secretuser@WVU-CYBE467-CTF2:~$ █
```



```
┌──(kali㉿kali)-[~/Desktop]
└─$ ls
flag2.txt   hydra.restore         secret.txt    username.txt
flag5.docx  index.html            services.txt
Flag8.pdf   process_feedback.php  traffic.txt
```

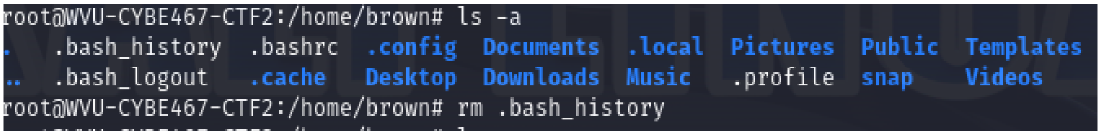
Cover Your Tracks

Now that all flags have been exfiltrated to the kali vm, the log files and command history need to be deleted to cover any tracks made during the process of the pen test. To start the ssh logs need to be deleted. They will show all login attempts from hydra and my login attempts with the secretuser. In the /var/log directory the following files are deleted: syslog, syslog.1 , lastlog, btmp , btmp.1, auth.log, auth.log.1, auth.log.2, auth.log.3 auth.log.4. To delete the bash history we need to go into each of the users that we ran a command on to delete the bash history. This will be for the users, brown , gee, system, and root.



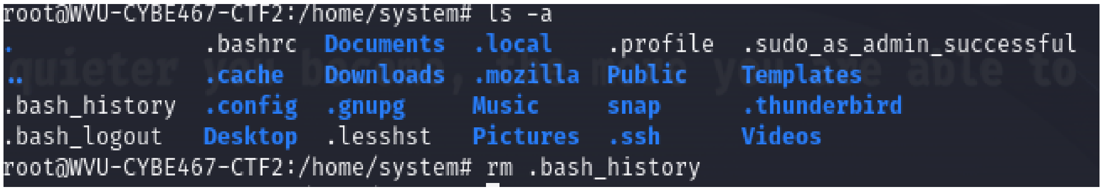
```
root@WVU-CYBE467-CTF2:/var/log# ls
alternatives.log                  boot.log.5       dpkg.log.1       mysql
alternatives.log.1                boot.log.6       dpkg.log.2.gz    openvpn
amazon                            boot.log.7       fontconfig.log   private
apache2                           bootstrap.log    gdm3             speech-dispatcher
apport.log                        cups             gpu-manager.log  ubuntu-advantage.log
apport.log.1                      dist-upgrade     hp               ubuntu-advantage.log.1
apt                               dmesg            installer        ubuntu-advantage.log.2.gz
aws114_ssm_agent_installation.log dmesg.0          journal          unattended-upgrades
boot.log                          dmesg.1.gz       kern.log         vboxpostinstall.log
boot.log.1                        dmesg.2.gz       kern.log.1       wtmp
boot.log.2                        dmesg.3.gz       kern.log.2.gz    Xorg.0.log
boot.log.3                        dmesg.4.gz       kern.log.3.gz    Xorg.0.log.old
boot.log.4                        dpkg.log         kern.log.4.gz
```

/var/log directory after deleting the log files.



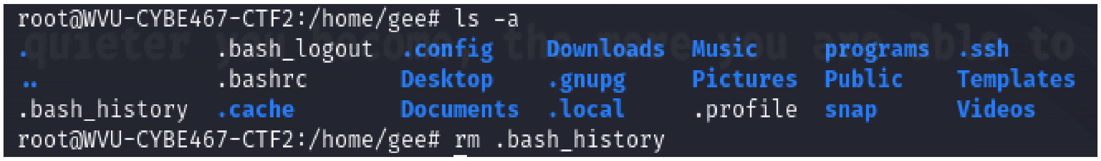
```
root@WVU-CYBE467-CTF2:/home/brown# ls -a
.   .bash_history  .bashrc  .config  Documents  .local  Pictures  Public  Templates
..  .bash_logout   .cache   Desktop  Downloads  Music   .profile  snap    Videos
root@WVU-CYBE467-CTF2:/home/brown# rm .bash_history
```

Deleting brown’s bash history



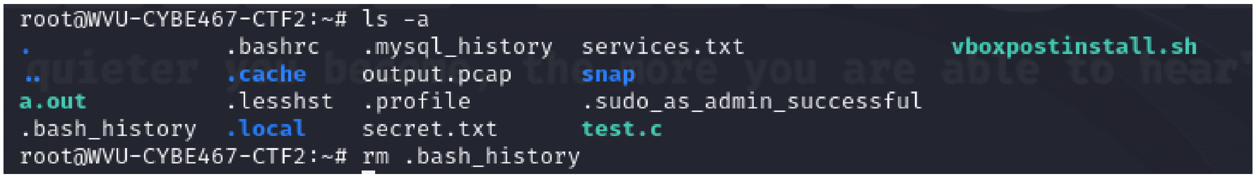
```
root@WVU-CYBE467-CTF2:/home/system# ls -a
.              .bashrc  Documents  .local    .profile  .sudo_as_admin_successful
..             .cache   Downloads  .mozilla  Public    Templates
.bash_history  .config  .gnupg     Music     snap      .thunderbird
.bash_logout   Desktop  .lesshst   Pictures  .ssh      Videos
root@WVU-CYBE467-CTF2:/home/system# rm .bash_history
```

Deleting system’s bash history



```
root@WVU-CYBE467-CTF2:/home/gee# ls -a
.              .bash_logout  .config    Downloads  Music     programs  .ssh
..             .bashrc       Desktop    .gnupg     Pictures  Public    Templates
.bash_history  .cache        Documents  .local     .profile  snap      Videos
root@WVU-CYBE467-CTF2:/home/gee# rm .bash_history
```

Deleting gee’s bash history



```
root@WVU-CYBE467-CTF2:~# ls -a
.               .bashrc   .mysql_history  services.txt               vboxpostinstall.sh
..              .cache    output.pcap     snap
a.out           .lesshst  .profile        .sudo_as_admin_successful
.bash_history   .local    secret.txt      test.c
root@WVU-CYBE467-CTF2:~# rm .bash_history
```

Deleting root’s bash_history