EXAMPLE REPORT

By Martin Martinez

DISCLAIMER

This document is just to expose my communication skills, in it I show my pentesting skills by hacking a TryHackMe platform machine.

In it there will not be any step by step to hack the machine, it is rather a report for an imaginary company.

Executive summary

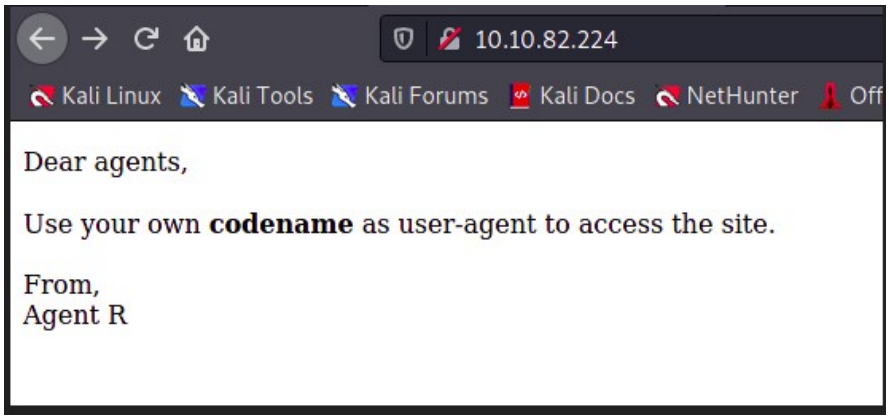
In this test I obtained total control of the server, in a very simple way I could obtain information such as:

- users
- passwords
- documents with sensitive information

This could allow an attacker to steal information about the clients, among this information could be bank details, addresses, users, etc.
To achieve this, the attacker should have a medium level of knowledge, so it is really easy to breach your system,

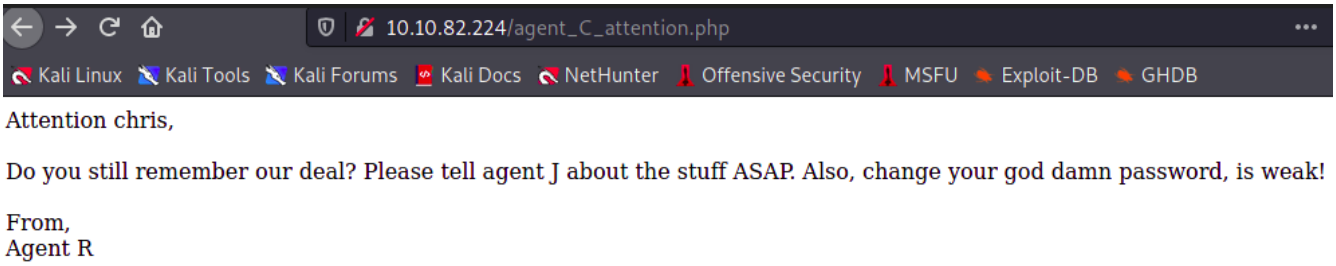
Technical summary

In the test conducted I found very simple ways to obtain information about users in the system, since by accessing the web page you can find a message:



Thanks to this message, an attacker can intercept the request, modify it and gain access to the page, which is really very simple.

Also the message lets me know that each user has a code in his user, so it is really easy to make a dictionary and get more information about the user.
Thanks to the dictionary created I gained access to a secret page that has even more information:



Thanks to this message I know that there is a user called chris, which is agent C, also there is an agent R and J, in the message you can see that the password is very easy to obtain, so a very simple brute force attack is possible.

By scanning the IP address I was granted I know that there are 3 services open and without any protection, so the brute force attack is even easier to execute.

Once I got access to the system, thanks to the information that was saved in files I was able to get access to the system through SSH and the user james, finally to get the maximum privileges of the system I only had to get information about **CVE-2019-14287**.

Assessment results

The problems that were discovered during the test are:

1.- Weak credentials: Weak passwords are a very common issue in companies, due to not having a good password policy, as well as using patterns, such as name.Lastname@company.com

Thanks to this problem is that I was able to get even more information about the users, so to correct this it is recommended:

- Use a password manager, KeePassXC is my recommendation.
- Create a good password policy:
- Do not create patterns
- Use passwords of minimum 20 to 30 characters.
- Do not use important dates

2.- Old version in "sudo":

CVE-2019-14287, is a vulnerability found in versions **prior to 1.8.28** in which an attacker can bypass certain restrictions and **execute commands as root.**

Thanks to this vulnerability I was able to obtain the maximum privileges, but by executing the command "**sudo -l**" I was able to execute this attack.

My recommendations are:

- Update sudo
- Restrict the commands that can show information about the system.
- Follow the law of least privilege

3. Information Desclousure

Thanks to a simple nmap scan I was able to obtain information about the software versions running on the different ports, this could reveal vulnerabilities in the software.

To fix this it is advisable to remove the banners from the services.

Links of support:

- https://nvd.nist.gov/vuln/detail/CVE-2019-14287
- https://www.onelogin.com/learn/least-privilege-polp
- https://keepassxc.org/
- https://www.whitesourcesoftware.com/resources/blog/new-vulnerability-in-sudo-cve-2019-14287

https://password.jcu.edu/public/passphrase.php

In the following section I will describe how I got root to the system, as well as show screenshots and describe the process step by step.

Information about the target:

- IP: 10.10.82.224

Enumeration:

To get information about the system I like to run the two step scan:

- one to get the open ports.
- another to get more information about the open ports.

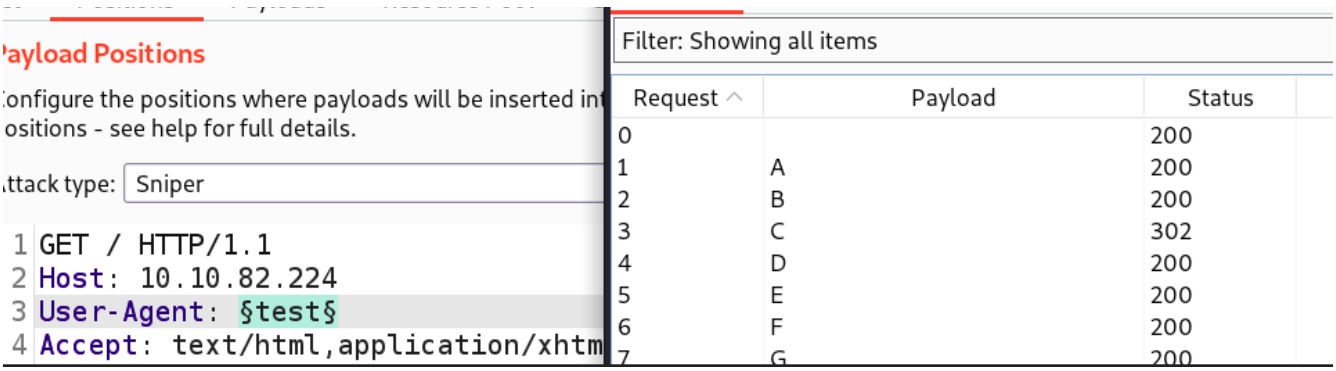
```
# Nmap 7.91 scan initiated Fri Oct 22 12:40:40 2021 as: nmap -sC -sV -p 21,22,80 -Pn -n -oA nmap/deep/deepScan
0.10.82.224
Nmap scan report for 10.10.82.224
Host is up (0.31s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 ef:1f:5d:04:d4:77:95:06:60:72:ec:f0:58:f2:cc:07 (RSA)
|   256 5e:02:d1:9a:c4:e7:43:06:62:c1:9e:25:84:8a:e7:ea (ECDSA)
|_  256 2d:00:5c:b9:fd:a8:c8:d8:80:e3:92:4f:8b:4f:18:e2 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Annoucement
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Oct 22 12:40:59 2021 -- 1 IP address (1 host up) scanned in 18.93 seconds
```

When I entered the website I got information about the users and worse, a description on how to access the "secret" website, I think that this information should only be known by the employees.

So to access the system I decided to create a dictionary with the alphabet and use burpsuite intruder to perform my attack, I got the following results.



As you can see in the image I got the code 302, this code indicates "redirection", so I entered the secret page and got much more information.

In which I was able to get more information, thanks to that message I used hydra to get the password, I used the list rockyou.txt and the user chris.

```
┌──(kali㉿kali)-[~/TryHackMe/agent-sudo]
└─$ hydra -l chris -P /usr/share/wordlists/rockyou.txt ftp://10.10.82.224 -t 50
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in milita
ations, or for illegal purposes (this is non-binding, these *** ignore laws and ethi

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-10-22 13:01:05
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waitin
found, to prevent overwriting, ./hydra.restore
[DATA] max 50 tasks per 1 server, overall 50 tasks, 14344399 login tries (l:1/p:1434
k
[DATA] attacking ftp://10.10.82.224:21/
[STATUS] 183.00 tries/min, 183 tries in 00:01h, 14344221 to do in 1306:24h, 50 activ
[21][ftp] host: 10.10.82.224   login: chris   password: crystal
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 5 final worker threads did not complete until
[ERROR] 5 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-10-22 13:03:00
```

I connected via FTP and there I was able to get even more information, I used a stegcracker to get the message that was hidden in an image and I got another user "james:hackerrules!" and so I used SSH to enter the system.

```
└─$ cat To_agentJ.txt
Dear agent J,

All these alien like photos are fake! Agent R stored the real picture inside your directory. Your login password
 is somehow stored in the fake picture. It shouldn't be a problem for you.

From,
Agent C
```

```
└─$ cat cute-alien.jpg.out
Hi james,

Glad you find this message. Your login password is hackerrules!

Don't ask me why the password look cheesy, ask agent R who set this password for you.

Your buddy,
```

To become the user I had to exploit the vulnerability explained above, so it was really easy.