CTF/BOOT2ROOT WALKTHROUGH

HACKTHETOWER - 08.05.2020

Giacomo Greci aka pepsy78

root@life:# whoami

- Commercialista fuori, Ingegnere informatico dentro (rev. 2019)
- Business Advisor & Auditor
- Forensics Fraud Examiner (2020)
- Master Digital Forensics in 2018 (ISF Milano)
- Master Cybersecurity in 2019 (UniPi)
- Love in IT & CTF & Pentesting
- Active on HTB, VulnHub, PentesterAcademy, TryHackMe
- Certification in progress: ePTS, ePTP
- Upcoming: OSCP, CEH, CHFI

- root@life:# uptime
- Long long time ago, there was a C64...and the story begun.

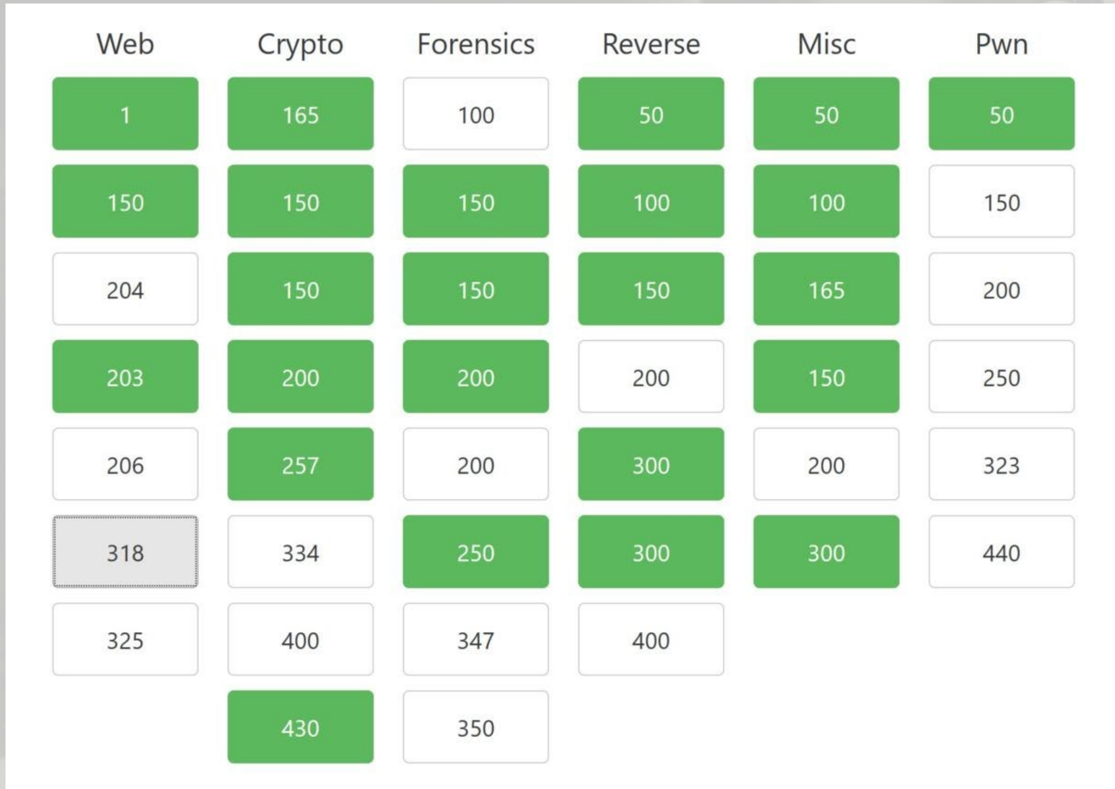
«LA MENTE DI UN CREATIVO, NON HA VICOLI CIECHI»

Nothing is impossible,
you just have to find one way for it

CTF: Capture The Flag

- Jeopardy
- Attack/Defense
- Boot2Root

CTF: Capture The Flag

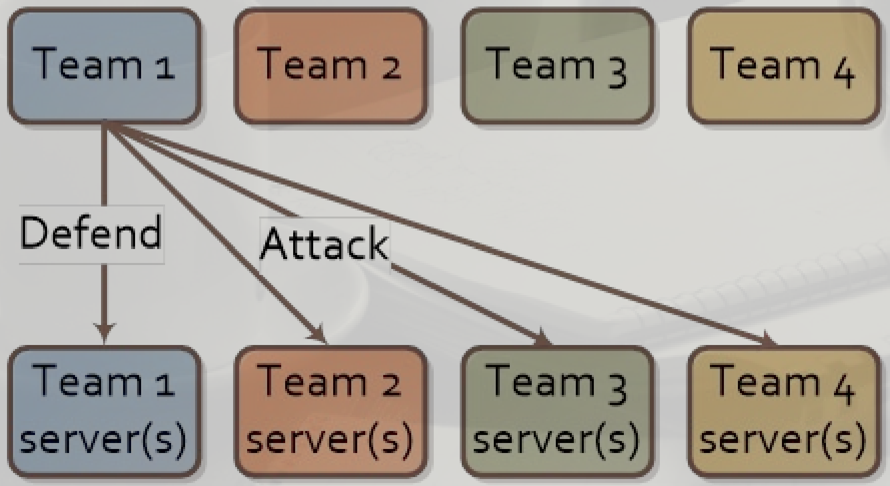


Web	Crypto	Forensics	Reverse	Misc	Pwn
1	165	100	50	50	50
150	150	150	100	100	150
204	150	150	150	165	200
203	200	200	200	150	250
206	257	200	300	200	323
318	334	250	300	300	440
325	400	347	400		
	430	350			

Jeopardy

https://ctftime.org/event/list/upcoming

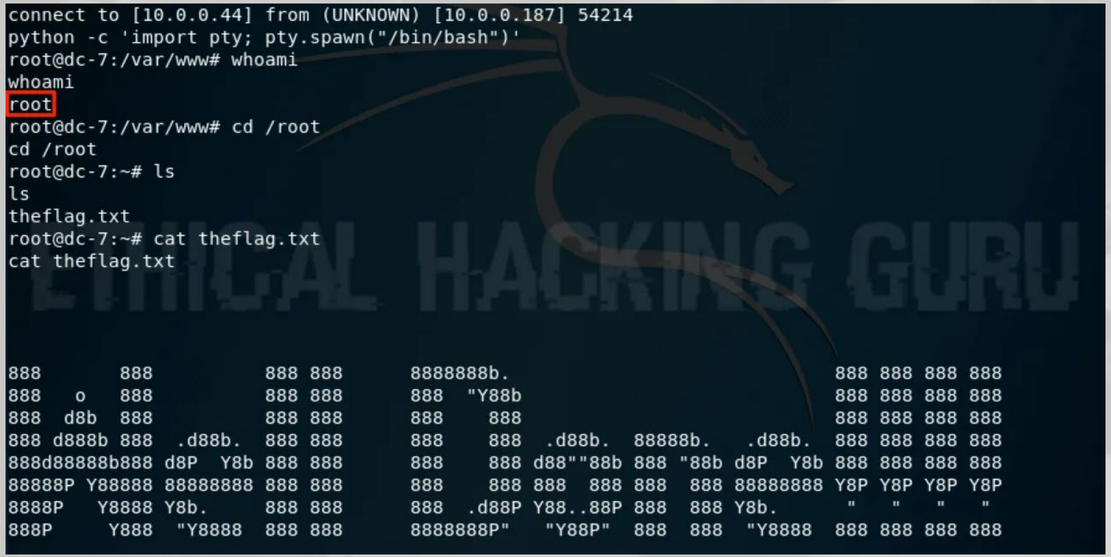
CTF: Capture The Flag



Team 1
Team 2
Team 3
Team 4
Defend
Attack
Team 1 server(s)
Team 2 server(s)
Team 3 server(s)
Team 4 server(s)

Attack/Defense

CTF: Capture The Flag



```
connect to [10.0.0.44] from (UNKNOWN) [10.0.0.187] 54214
python -c 'import pty; pty.spawn("/bin/bash")'
root@dc-7:/var/www# whoami
whoami
root
root@dc-7:/var/www# cd /root
cd /root
root@dc-7:~# ls
ls
theflag.txt
root@dc-7:~# cat theflag.txt
cat theflag.txt


888       888          888 888      8888888b.                             888 888 888 888
888   o   888          888 888      888  "Y88b                            888 888 888 888
888  d8b  888          888 888      888    888                            888 888 888 888
888 d888b 888  .d88b.  888 888      888    888  .d88b.  88888b.   .d88b.  888 888 888 888
888d88888b888 d8P  Y8b 888 888      888    888 d88""88b 888 "88b d8P  Y8b 888 888 888 888
88888P Y88888 88888888 888 888      888    888 888  888 888  888 88888888 Y8P Y8P Y8P Y8P
8888P   Y8888 Y8b.     888 888      888  .d88P Y88..88P 888  888 Y8b.      "   "   "   "
888P     Y888  "Y8888  888 888      8888888P"   "Y88P"  888  888  "Y8888  888 888 888 888
```

Boot2Root

Today's Boot2Root

recon: 1

https://www.vulnhub.com/entry/recon-1,438/

DevRandom CTF: 1.1

https://www.vulnhub.com/entry/devrandom-ctf-11,450/

Q&A

recon: 1

Roadmap:

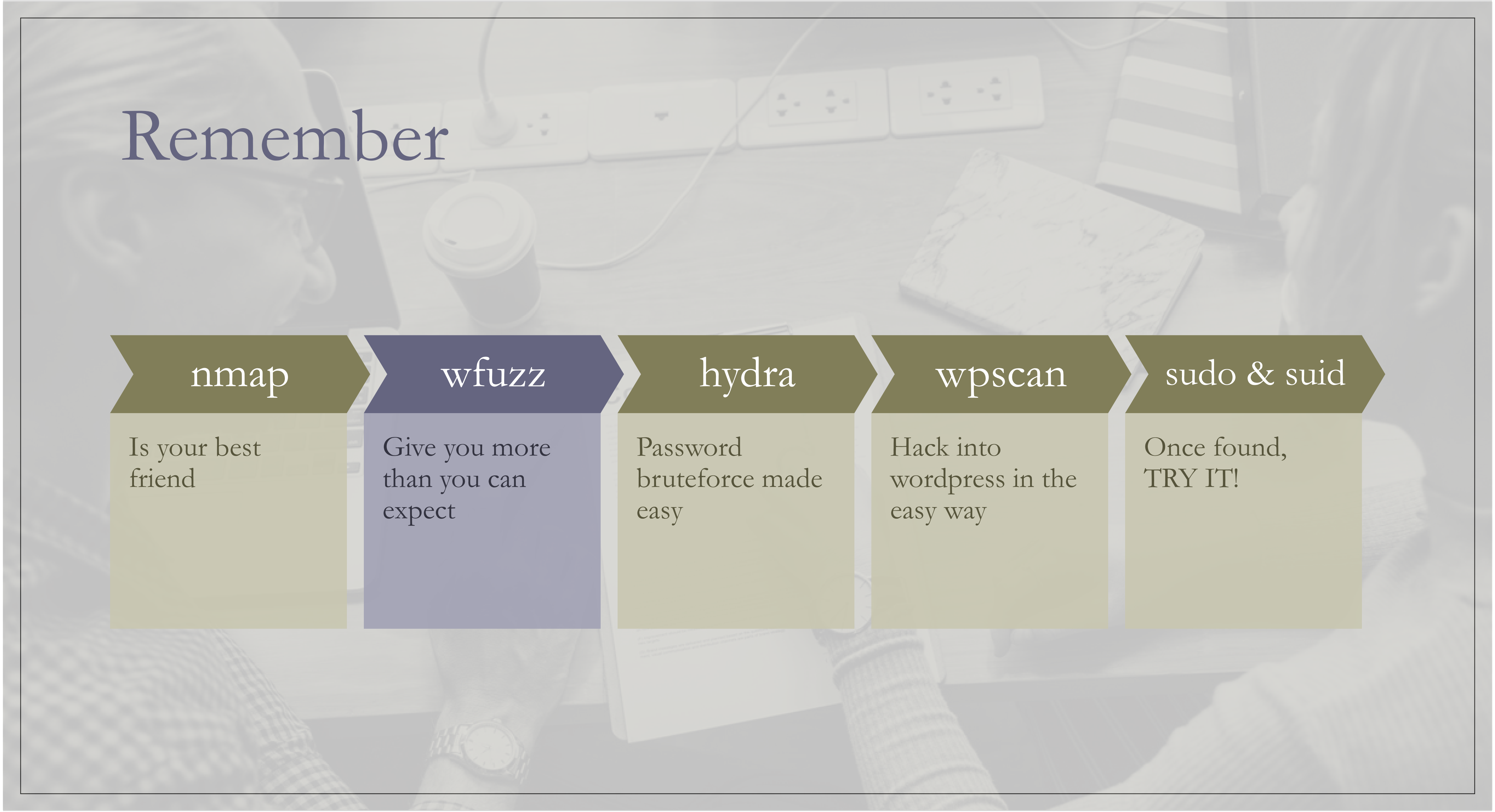
- nmap
- dirb o wfuzz
- wpscan
- Hack the Wordpress Plugin!
- LinEnum
- sudo
- docker

DevRandom CTF

Roadmap:

- nmap
- wfuzz
- Log Injection through PHP Include
- hydra
- setuid is my friend
- sudo!

Remember



nmap

Is your best friend

wfuzz

Give you more than you can expect

hydra

Password bruteforce made easy

wpscan

Hack into wordpress in the easy way

sudo & suid

Once found, TRY IT!

Docker?

Be a bad boy, and use it for your way out!

Think that….

(root) NOPASSWD:
better no than yes

WordPress:
keep updated and
password strong!

PHP Include:
may expose you
badly

Think that….

comment:
plz no on production services!

suid:
yes with moderation

docker:
keep in mind the environment

What’s next….

- TRY TRY TRY TRY
- KEEP TRING
- Think out of the box!!!
- Break it!
- Have fun!
- Take a Beer

THAT'S ALL FOLKS!

Just my 2c back to community