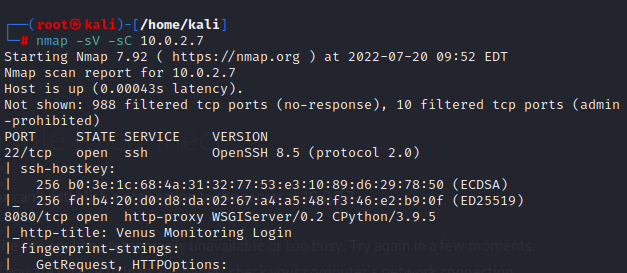
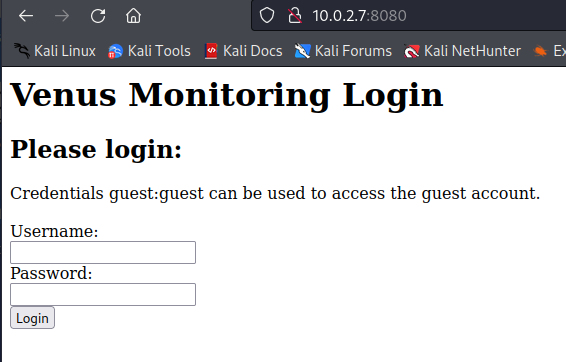
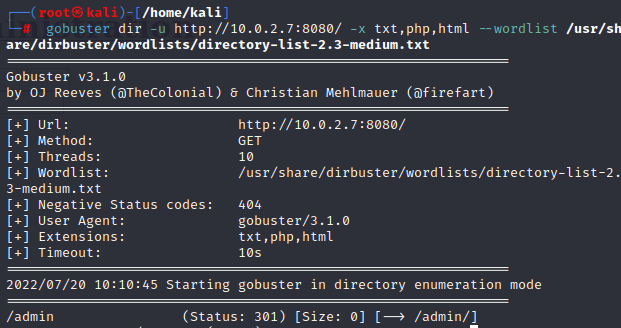
Scan ra



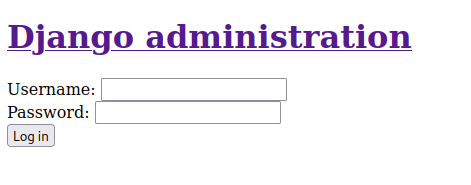
Vao xem



Dung gobuster: gobuster dir -u http://10.0.2.7:8080/ -x txt,php,html –wordlist /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt

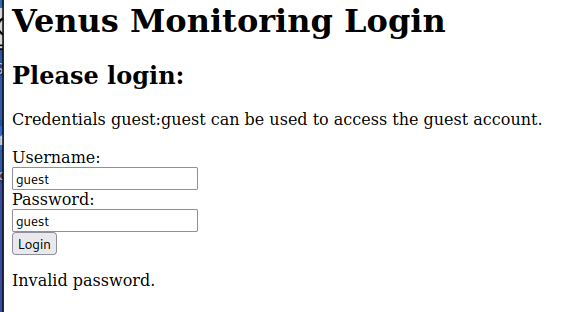


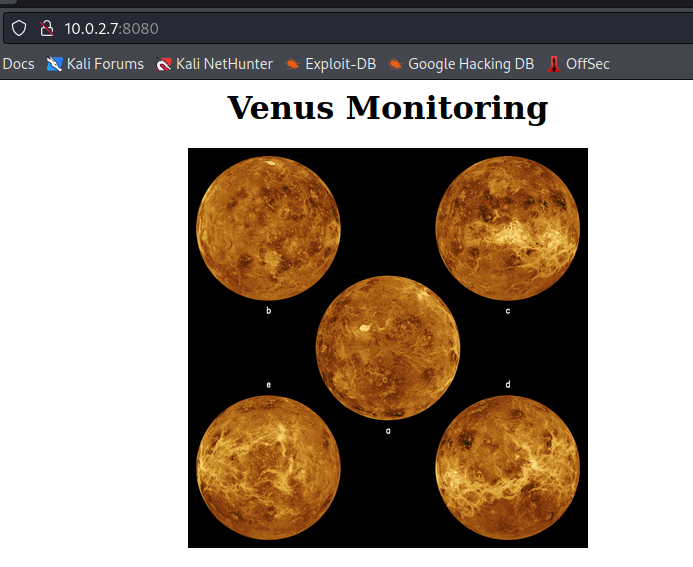
Vao xem thu, thay form login



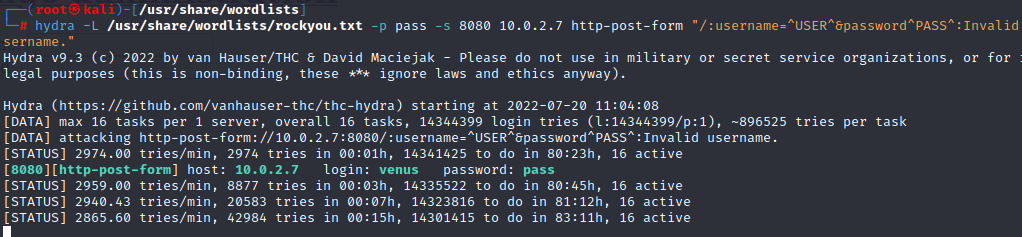
, nhap bua user: admin, pass: admin

-> hien loi 500. Bay gio back ve trang truoc

Nhap thu user: guest, pass: guest xem nao. Suprise!! Thu phat an luon

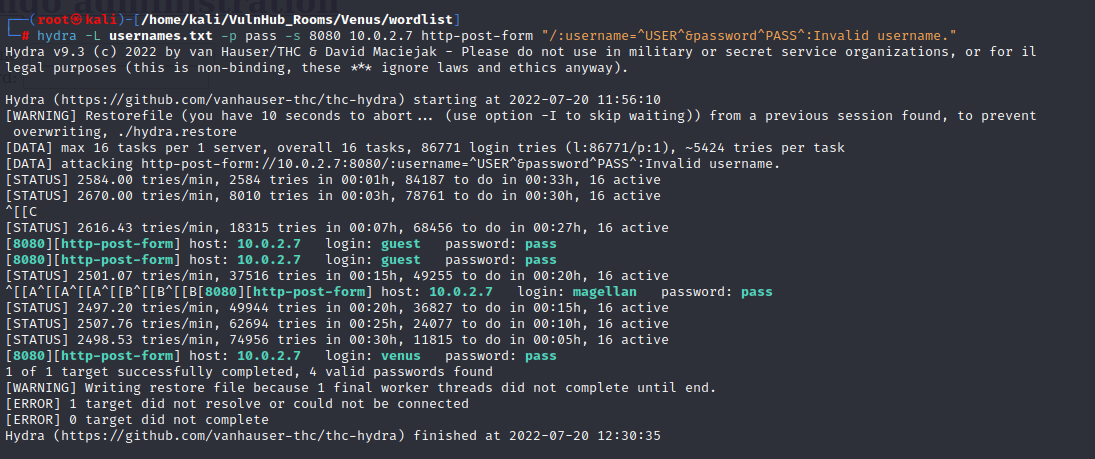


Thử dùng hydra để generate username va password xem sao. Ban dau minh dung rockyou.txt nhma lau qua.



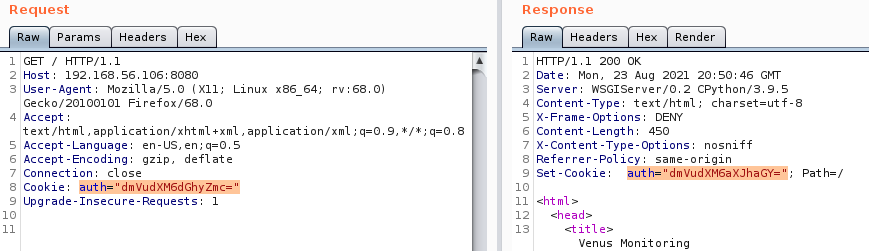
Sau 1 hoi mo mam tren internet, minh da bat gap 1 list usernames kha hay ho [**https://github.com/jeanphorn/wordlist/blob/master/usernames.txt**](https://github.com/jeanphorn/wordlist/blob/master/usernames.txt)**.** Bay gio wget ve va test lai xem nao

**hydra -L usernames.txt -p pass -s 8080 10.0.2.7 http-post-form "/:username=^USER^&password^PASS^:Invalid username."**



Du da nhanh hon nhieu nhung cung mat gan 30p :)))) va pass da duoc ma hoa (nhin account cua guest la biet ngay)

Dung burpsuite dang nhap lai tai khoan guest hoi nay vo tinh co pass xem



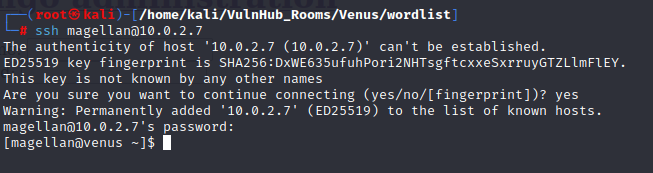
Day chac chan la base64 roi =))) decrypt ra xem

co duoc: **guest:thrfg**

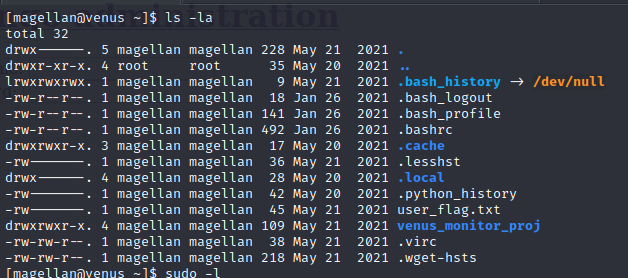
Dung pass nay + username truoc do => base64 xem sao. Surprise!!! Response da tu chuyen huong toi cookie can tim. Decrypt ra ta duoc tai khoan va mat khau lan luot la:

guest:guest  
venus:venus  
magellan:venusiangeology1989

Bay gio quay lai port 22 va ssh thu xem thoi nao! =)))

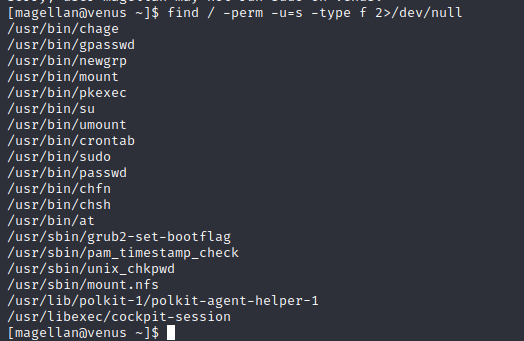


Ls –la



Sudo –l < khong duoc vi magellan khong nam trong sudoers >

find / -perm -u=s -type f 2>/dev/null

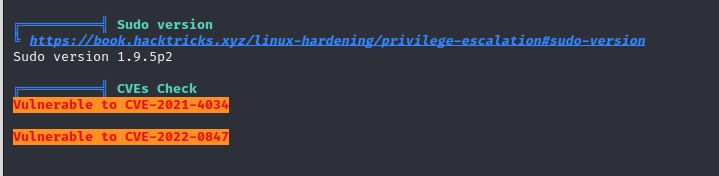


Toi day tu nhien minh nho ra Linpeash :)))) ehehe va dieu gi den cung phai den 😆

╔══════════╣ CVEs Check

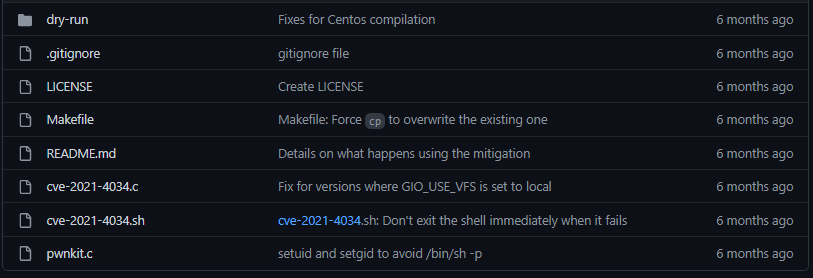
Vulnerable to CVE-2021-4034

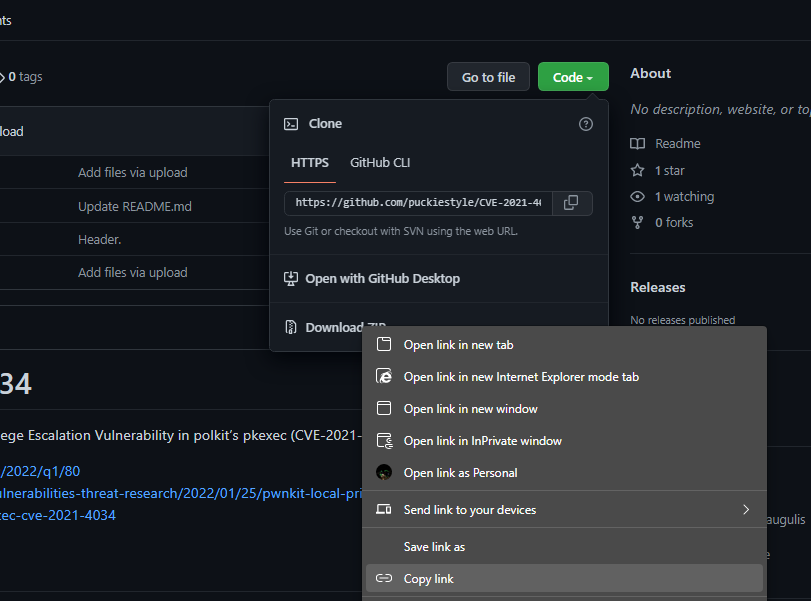
Vulnerable to CVE-2022-0847



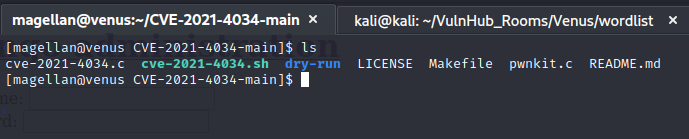
Sau khi search google ve CVE tren, minh da tim duoc thu hay ho nay :

[GitHub - berdav/CVE-2021-4034: CVE-2021-4034 1day](https://github.com/berdav/CVE-2021-4034) no bao gom cac file sau

 va chung ta se dung wget +url file zip cua git nay tren github bang cach



Ok, bay gio giai nen ra va test thoi nao



De y readme.md cua github nhe 😆 

Day la cac cau lenh chung ta se can dung toi

vagrant@ubuntu-impish:~/CVE-2021-4034$ make

vagrant@ubuntu-impish:~/CVE-2021-4034$ ./cve-2021-4034

Xong roi #whoami phat de biet minh la ai :)))))