Text

Description automatically generated

Hôm nay mk sẽ trở lại với bài Watcher. Bài này mk làm cách đây khá lâu, bây giờ viết lại cách giải. Bắt đầu thôi.

1. Dò quét

nmap -T4 -v 10.10.78.20 -Pn

A screenshot of a computer

Description automatically generated with low confidence

Chi tiết hơn

nmap -sC -sV -v 10.10.78.20 -Pn

A screenshot of a computer

Description automatically generated with medium confidence

2. Enum

Do ftp ở đây là “vsftpd 3.0.3” mk ko tìm được lỗi nào nên quay sang port 80.

Graphical user interface, website

Description automatically generated

Khi mà “View page source” chúng ta sẽ thấy điều khá hay ở đây, đó là đoạn “post?=”. Thì với tình hình như này khả năng là lỗi lfi rồi

Graphical user interface, text, application, email

Description automatically generated

Text

Description automatically generated

Thành công. Để biết rõ hơn source code file post.php là ntn, thì các bạn có thể research với từ khóa “php lfi filter”.

Graphical user interface

Description automatically generated

Ở đây chúng ta có source code file “post.php” đã được encode base64 => Decode thôi



Sau khi decode thì chúng ta biết được lỗi phát sinh ở đoạn code này.

Với lfi thì ban đầu mk tìm các file id\_rsa của từng user như mat, will, toby nhưng đều không được. Mk chuyển qua tìm xem có file config.php, thì cũng ko thấy. Sau đó mk thử phương pháp “log poisoning” để RCE thì cũng ko thành công. Hmm, thế này phải tìm file/folder ẩn xem sao.

gobuster dir -u 10.10.78.20 -x php,txt -w /usr/share/wordlists/dirb/big.txt -t 50

A screenshot of a computer

Description automatically generated with medium confidence

“robots.txt”

Graphical user interface, text, application

Description automatically generated

/secret\_file\_do\_not\_read.txt. Chính là nó. Nhưng với cách thông thường thì chúng ta ko thể xem được

Graphical user interface

Description automatically generated with medium confidence

Với cách này chúng ta thành công.

Graphical user interface, text, application

Description automatically generated

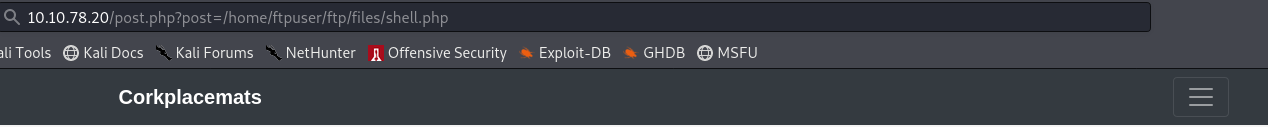
3. Khai thác

Login vào ftp với username/password ở trên.

Text

Description automatically generated

Mk upload 1 con shell viết bằng ngôn ngữ php. Vị trí của nó như chúng ta thấy ở trên, nằm ở thư mục /home/ftpuser/ftp/files. Lấy shell thôi.



Text

Description automatically generated

4. Leo thang đặc quyền

Với user “toby” khá đơn giản, sudo permission là ra

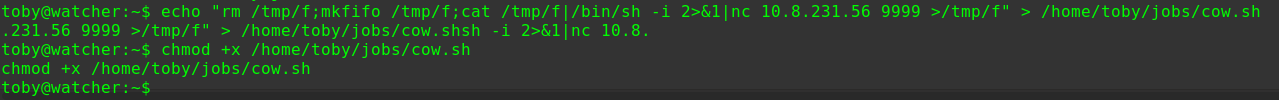
Text

Description automatically generated

Graphical user interface, text

Description automatically generated

Hãy để ý tới file “/home/toby/jobs/cow.sh” được chạy với danh nghĩa của user “mat”. Đơn giản thôi, chúng ta sửa file cow.sh là được.



nc -vlnp 9999, rồi chờ kết quả

A screenshot of a computer

Description automatically generated with medium confidence

Thành công, hiện tại đang là user “mat”.

Text

Description automatically generated

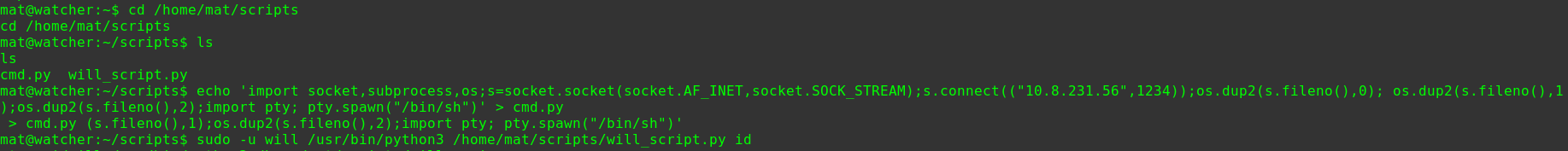
Kiểm tra file will\_script.py xem nó là gì.

Text

Description automatically generated

Import hay export thực chất là gọi/làm việc với file. “from cmd import get\_command” ở đây là gọi đến hàm get\_command trong file cmd.py. Và chúng ta thấy là chúng ta có thể sửa file cmd.py.

nc -vlnp 1234 rồi chờ.



Thành công, đã lên được user “will”.

A screenshot of a computer

Description automatically generated with medium confidence

Chúng ta thấy user Will thuộc group “adm”. Với những group đặc biệt ntn, các bạn có thể tham khảo <https://book.hacktricks.xyz/linux-unix/privilege-escalation/interesting-groups-linux-pe>.

Text

Description automatically generated

Thư mục “backups” đây rồi và chúng ta tìm được id\_rsa

Graphical user interface, text

Description automatically generated

Sử dụng id\_rsa này để login thôi.

Graphical user interface, text

Description automatically generated

Mission completed!