# GIỚI THIỆU

CTF (Capture the Flag) - là loại hình thi đấu dành riêng cho cộng đồng bảo mật máy tính. Các đội chơi tham gia sẽ tìm kiếm “cờ” (flag) được giấu trong hệ thống, trong các ứng dụng hoặc các file đã được bảo vệ. Mỗi cờ là một chuỗi ký tự đặc biệt và các đội chơi phải tìm cách truy cập và chiếm cờ đó.

Để chơi CTF, người tham gia cần có các kiến thức về mã hóa, an ninh mạng, phân tích mã độc, kỹ năng lập trình. CTF chia thành các mảng chính:

* **Web exploit** (Khai thác lỗ hổng web): Các thử thách tập trung vào lỗ hổng bảo mật của ứng dụng web.
* **Reverse engineering** (Dịch ngược): Các thử thách tập trung vào phân tích và giải mã các phần mềm , tệp tin.
* **Crypto** (Mật mã): Các thử thách tập trung vào các thuật toán mã hóa và giải mã.
* **Pwnable** (Khai thác lỗ hổng): Các thử thách tập trung vào khai thác các lỗ hổng bảo mật trong hệ thống hoặc phần mềm.
* **Forensics** (Truy vết): Các thử thách tập trung vào việc thu thập và phân tích các dữ liệu số.

Leviathan của OverTheWire là một tập hợp các bài thi CTF dành cho người mới với độ khó 1/10

# WRITEUP

## Tổng quan

Leviathan có tổng cộng 8 level (gồm cả level 0). Server Bandit có thể kết nối thông qua Secure Shell (SSH). Thông tin đăng nhập được cấp từ level 0, và mỗi level sẽ có một flag là chuỗi password của level tiếp theo. Có nhiều cách để truy cập vào tệp password, ta chỉ cần làm đúng một cách là đủ.

Link tham gia: [OverTheWire: Leviathan](https://overthewire.org/wargames/leviathan/)

## Leviathan0

ssh leviathan.labs.overthewire.org -p 2223 -l leviathan0

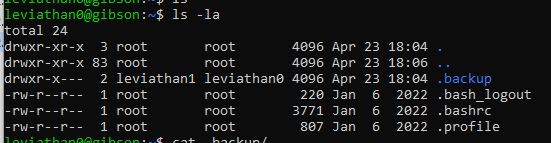
password để đăng nhập: leviathan0

## Leviathan0->1

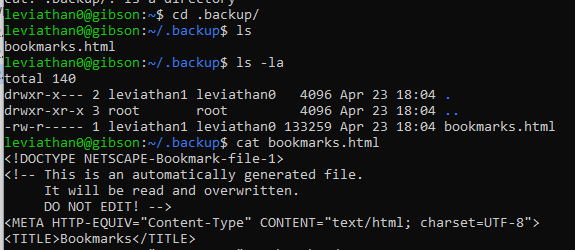
Yêu cầu: tìm flag ở đường dẫn home. Các mật khẩu cho từng level sẽ được lưu trữ ở /etc/leviathan\_pass

Đầu tiên ta kiểm tra các tệp/thư mục ở home thông qua

ls -la

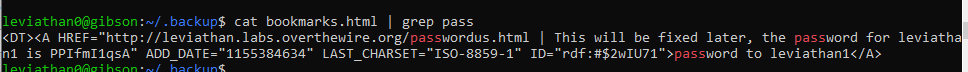


Phát hiện thư mục ẩn .backup, ta mở thư mục này ra và thấy tệp bookmarks.html



Tệp bookmarks.html này là 1 tệp chứa nội dung HTML. Dự đoán flag có thể giấu ở trong các dòng lệnh này, ta sử dụng grep để lọc nội dung. Từ khóa có thể gặp là: “pass”, “password”, “leviathan1”, “secret”

cat bookmarks.html | grep pass



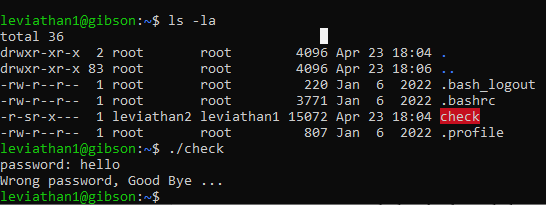
Ta thu được flag: PPIfmI1qsA

## Leviathan1->2

ssh leviathan.labs.overthewire.org -p 2223 -l leviathan1

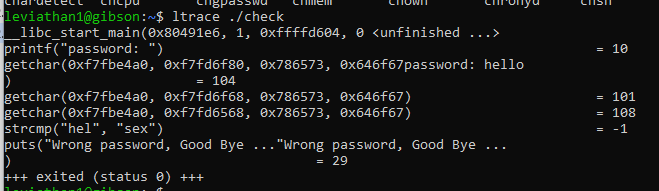
Ta kiểm tra các tệp/thư mục ở home:

ls -la



Nhận thấy 1 tệp thực thi là check, ta chạy thử thì tệp này sẽ cho phép nhập vào một chuỗi kí tự, và có vẻ tệp này sẽ kiểm tra mật khẩu của chuỗi kí tự này có đúng với một giá trị chuỗi nào đó cho trước hay không. Không đúng thì in ra màn hình “Wrong password, Good Bye...”, khả năng là nếu đúng sẽ in ra flag.

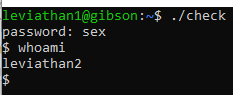
Ta sẽ kiểm tra tệp thực thi này sẽ gọi những hàm nào trong thư viện bằng câu lệnh ltrace



Nhìn vào luồng hoạt động, có thể thấy chương trình này thực hiện lần lượt:

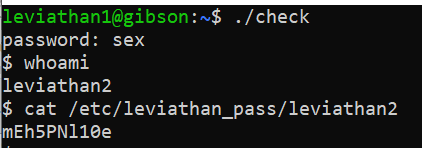
* In ra chuỗi “password: “
* Cho người dùng nhập chuỗi thông qua 3 hàm getchar(), tức là lấy 3 kí tự đầu tiên của chuỗi đã nhập
* So sánh 3 chuỗi đó với từ “sex”, và vì 2 chuỗi này khác nhau nên in ra “Wrong password...”

Vậy ta thử nhập chữ “sex” xem có đúng mật khẩu hay không:



Sau khi nhập, nhận thấy hiển thị một subshell, ta kiểm tra subshell này được sử dụng với user nào. Ta thấy ta đang sử dụng subshell với quyền của leviathan2.

Ta tìm password của leviathan2 ở tệp /etc/leviathan\_pass/leviathan2

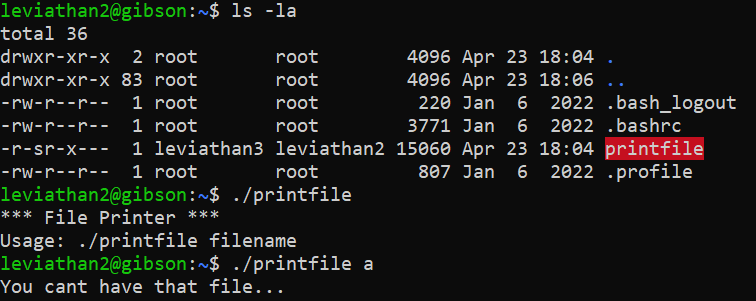


Thu được flag: mEh5PNl10e

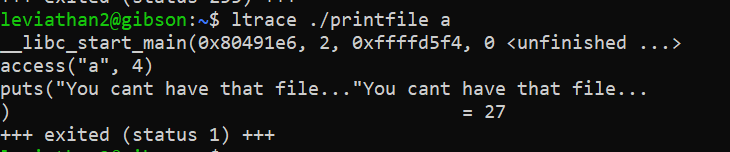
## Leviathan2->3

ssh leviathan.labs.overthewire.org -p 2223 -l leviathan2

Kiểm tra đường dẫn thư mục gốc, ta thấy một tệp là printfile. Tệp này có vẻ sẽ in thông tin một tệp (print một file) bằng cách truyền tham số tên file đó vào:



Thử phân tích tệp:



Nhận thấy tệp sẽ nhận đối số tên file (a) và kiểm tra khả năng truy cập của file này bằng access("a",4). Và khả năng vì không thể truy cập file này nên in ra chuỗi “You cant have that file...”.

Ta thử tạo một tệp và cấp quyền truy cập đầy đủ cho tệp đó rồi chạy lại ltrace:



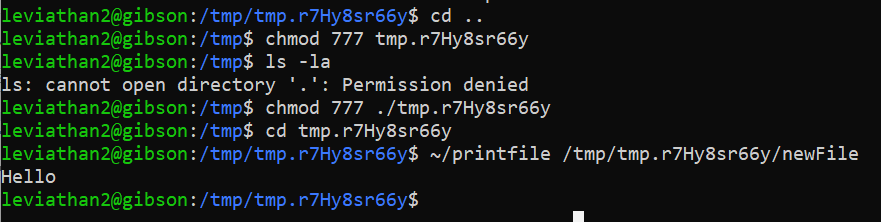
Chương trình printFile đã chạy thêm đòng snprintf(“/bin/cat newFile”, 511, “/bin/cat %s”, “newFile”). Dòng này có nghĩa là sử dụng câu lệnh cat lên file có giá trị ta vừa truyền vào, lưu câu lệnh đó vào bộ nhớ đệm. Dòng này chỉ thực hiện khi access thành công, tức là có quyền truy cập đến newFile.

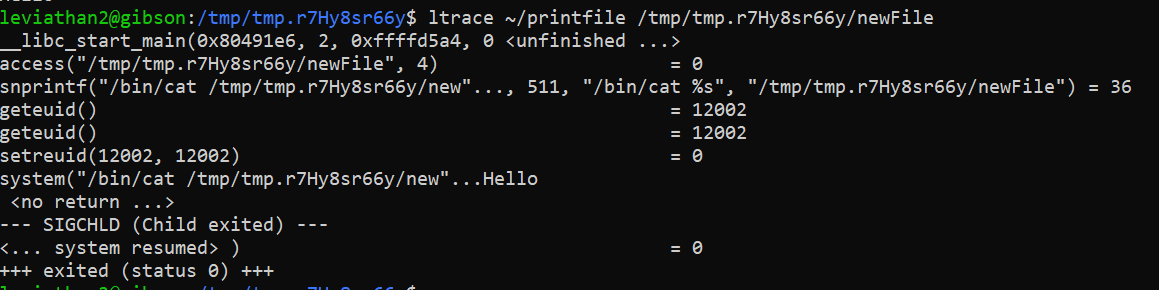
Sau đó câu lệnh system(“/bin/cat newFile”) khả năng cao là câu lệnh system() và truyền vào đối số là các giá trị trong bộ nhớ đệm của ta (lúc này là /bin/cat newFile).

Khi chạy chương trình thực tế, câu lệnh in ra là:



Permission denied là do ta chưa cấp quyền truy cập cho thư mục tạm tmp.r7Hy8sr66y. Ta thực hiện cấp quyền truy cập cho mọi user/group vào thư mục này và thử thực hiện lại đoạn lệnh trên.



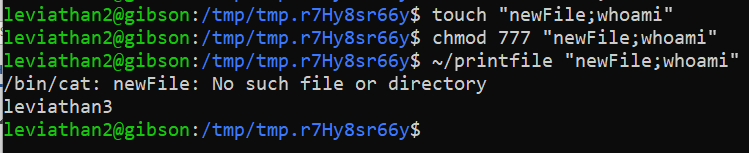


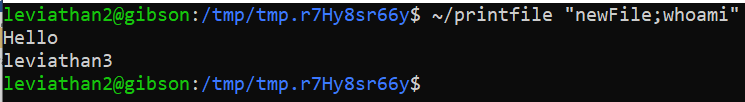
Ta nhận thấy câu lệnh system(“/bin/cat ...”) tức là sử dụng lệnh cat lên một tệp nào đó, mà tệp này chính là tệp ta đưa vào thông qua tham số khi sử dụng /printfile.

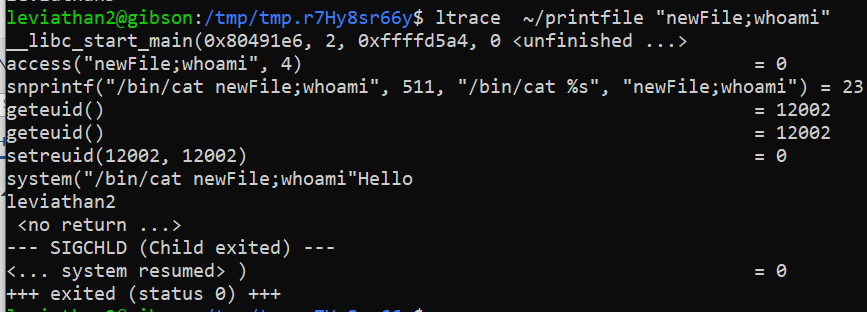
Như vậy nếu ta đặt tên tệp này là newFile;whoami, câu lệnh sẽ thành:

/bin/cat newFile;whoami

Thử thực hiện, ta thấy:







Ở đây ta nhận thấy ta nhập vào chuỗi nào thì tất cả chuỗi đó sẽ được kiểm tra access (quyền truy cập), và nếu có quyền thì thực thi thông qua câu lệnh system("/bin/cat chuỗi\_vừa\_nhập"). Do đó nếu chuỗi vừa nhập ta sử dụng thêm dấu ; để phân định các câu lệnh, và tiêm vào 1 đoạn lệnh sau dấu ; thì chương trình sẽ thực thi 2 việc:

/bin/cat newFile

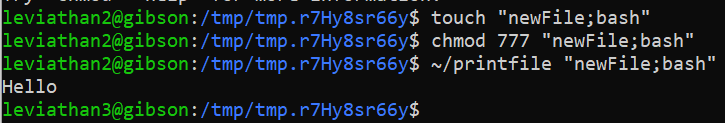
whoami

Ta sẽ tiêm đoạn lệnh thứ 2, thay thế whoami bằng lệnh gọi ra subshell bash dưới quyền của leviathan3 bằng việc:

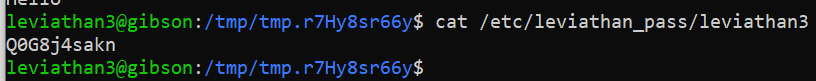
Tạo tệp newFile;bash

Cấp quyền truy cập cho file trên

Thực thi file printfile với tham số newFile;bash



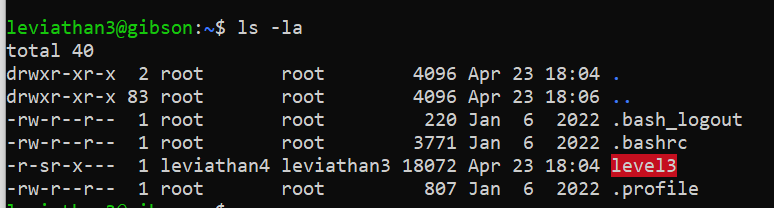
Nhận thấy ta đã truy cập vào subshell dưới quyền leviathan3, ta tìm mật khẩu trong thư mục /etc/leviathan\_pass/leviathan3



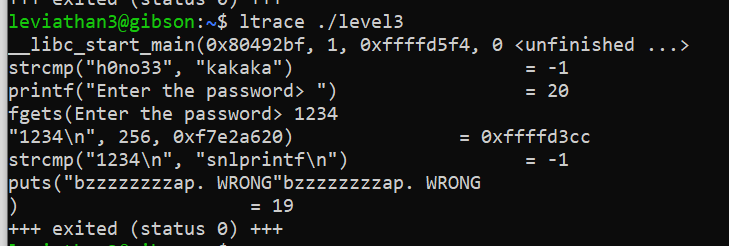
Thu được: Q0G8j4sakn

## Leviathan3->4

ssh leviathan.labs.overthewire.org -p 2223 -l leviathan3

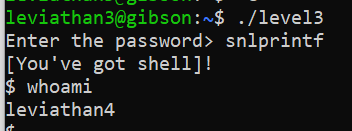


Tương tự như các level trước, ta ltrace ./level3



Đoạn strcmp đầu tiên chỉ để gây nhiễu, không có tác dụng gì cụ thể.

Ta thấy sau khi nhập password (1234), chương trình so sánh với chuỗi snlprintf. Như vậy ta thử nhập password là snlprintf xem sao:

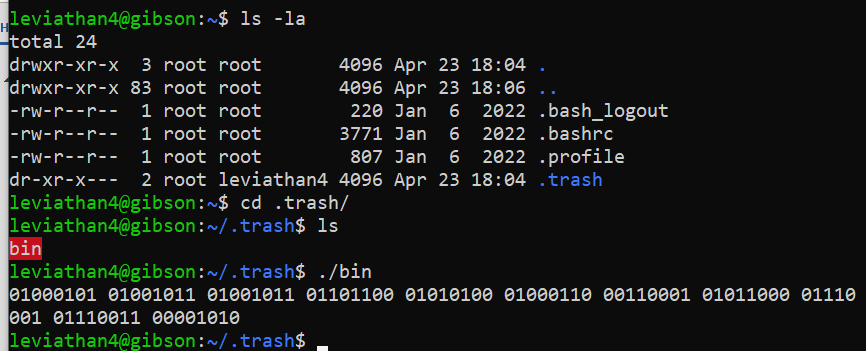


Ta đã truy cập vào subshell với quyền leviathan4, tiếp tục vào tệp chứa mật khẩu để tìm flag, thu được: AgvropI4OA

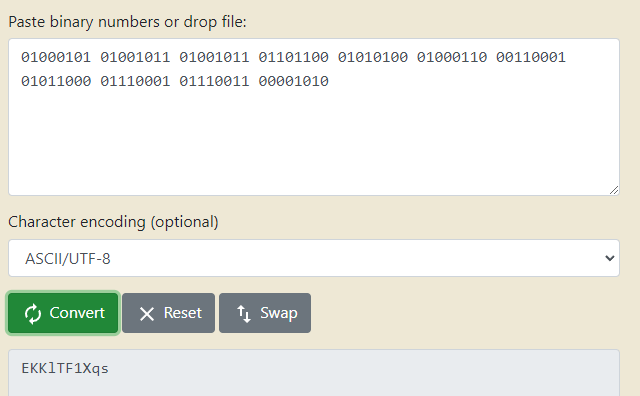


## Leviathan4->5

ssh leviathan.labs.overthewire.org -p 2223 -l leviathan4



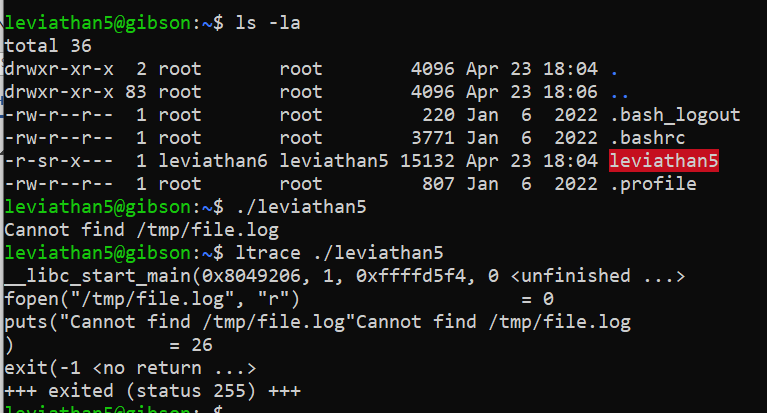
Tệp ./bin in ra một loạt các chuỗi nhị phân, ta thử convert về chuỗi ascii:



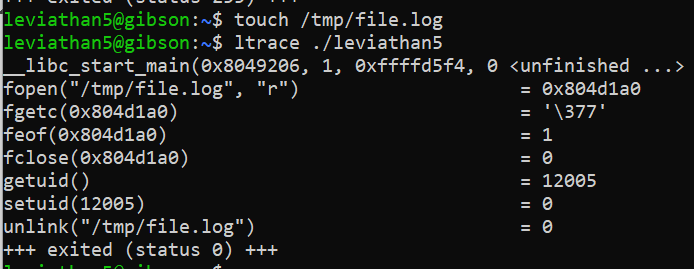
Thu được: EKKlTF1Xqs

## Leviathan5->6

ssh leviathan.labs.overthewire.org -p 2223 -l leviathan5

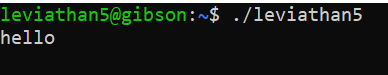


Tệp ./leviathan5 sẽ mở tệp /tmp/file.log (thông qua fopen), ta thử tạo tệp trên:



Ở đây có dòng lệnh unlink() đáng chú ý. unlink là một lệnh dòng lệnh dùng để xóa bỏ liên kết đến một tập tin hoặc thư mục. Nếu tập tin đó không có liên kết nào khác, thì nó sẽ bị xóa khỏi hệ thống.

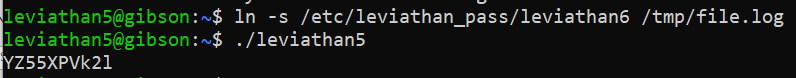
Ta thử tạo lại tệp trên với nội dung “hello” ở trong và thực hiện lại lệnh ./leviathan5



Tức là đoạn lệnh ở chương trình trên sẽ in ra nội dung trong tệp /tmp/file.log. Sau đó sử dụng unlink() để xóa liên kết/xóa file trên.

Như vậy nếu ta link file này với tệp mật khẩu cho level tiếp theo thì khi thực thi lệnh ./leviathan5, câu lệnh sẽ in ra nội dung mật khẩu trong tệp /etc/leviathan\_pass/leviathan6. Thực hiện link bằng câu lệnh:

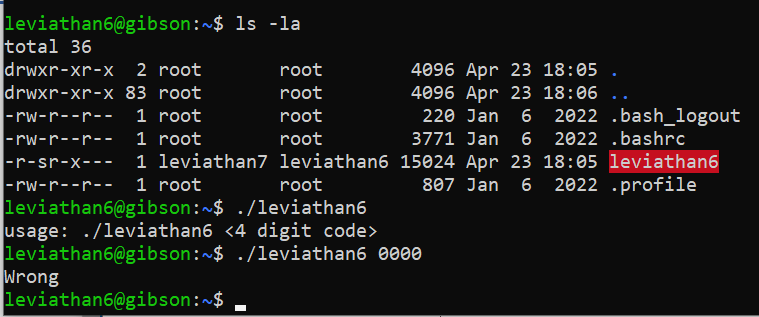
ln -s /etc/leviathan\_pass/leviathan6 /tmp/file.log



Thu được flag: YZ55XPVk2l

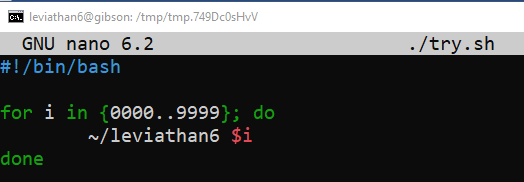
## Leviathan6->7

ssh leviathan.labs.overthewire.org -p 2223 -l leviathan6

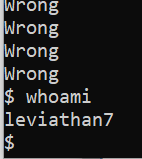


Có vẻ chương trình leviathan6 này sẽ nhận một số 4 chữ số, so sánh với mã PIN đúng.

Ta sẽ vét cạn bằng cách thực thi toàn bộ các câu lệnh leviathan6 $i, với $i chạy từ 0000 đến 9999. Viết file bash ở thư mục /tmp để hỗ trợ chạy đoạn lệnh trên:



Thực hiện mở subshell dưới quyền leviathan7 thành công



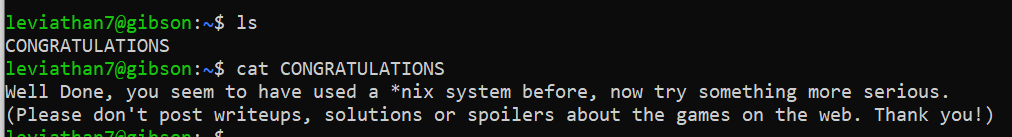
Ta tìm mật khẩu trong thư mục leviathan\_pass:



Thu được: 8GpZ5f8Hze

## Leviathan7->8

ssh leviathan.labs.overthewire.org -p 2223 -l leviathan7



Chúc mừng anh em đã phá đảo thành công.