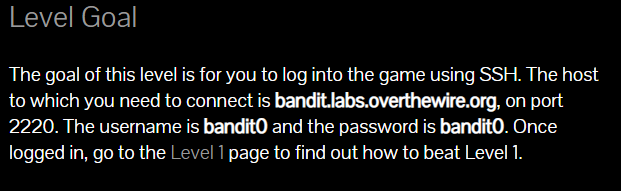
# Writeup

* Level 0



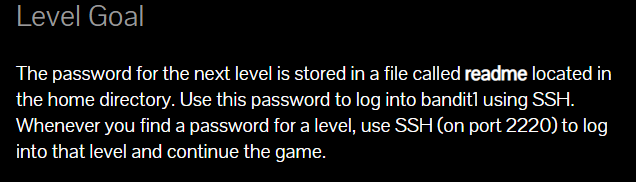
+ Level này yêu cầu ta kết nối vào game dùng SSH với dường dẫn và port đã được cung cấp

Ảnh có chứa văn bản

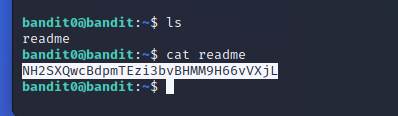
Mô tả được tạo tự động

+ Ta sử dụng user name và mật khẩu đã được cấp trong thử thách ở chế độ remote và dùng option -p để chỉ định port 2220 mà thử thách yêu cầu

* Level 0->1



+ Thử thách này ta thấy mật khẩu cho level tiếp theo được lưu trong 1 file gọi là readme



+ Sau khi dùng lệnh ls để xem các file thì ta thấy có file tên là readme

+ Ta dùng lệnh cat để xem nội dung của file readme và ta đã thấy mật khẩu

+ Mật khẩu cho level tiếp theo: NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL

* Level 1->2

Ảnh có chứa văn bản

Mô tả được tạo tự động

+ Ta sử dụng lại ssh để kết nối tới level1 với user name là level1

Ảnh có chứa văn bản

Mô tả được tạo tự động

+ Và pass đã tìm thấy ở trên

Ảnh có chứa văn bản

Mô tả được tạo tự động

+ Ta làm tương tự level ở trên dùng lệnh ls để xem các file

+ Nhưng ta thấy có 1 file với tên là “-“ ký tự đặc biệt

+ Để có thể đọc được file này ta dùng lệnh cat ./-

+ Và ta đã lấy được pass cho level tiếp theo: rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi

* Level 2->3

Ảnh có chứa văn bản

Mô tả được tạo tự động

+Mật khẩu cho level này nằm ở file tên là spaces in this file name

Ảnh có chứa văn bản

Mô tả được tạo tự động

+ Dùng lệnh ls để xem file tên ”spaces in this file name’

+ Ta không thể dùng lệnh cat với những file có dấu space trong tên

+ Để có thể cat file có dấu spaces thì ở mỗi khoảng trống trong tên ta têm ký tự ”\”

+ Ta tìm thấy mật khẩu cho level tiếp theo: aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG

* Level 3->4

Ảnh có chứa văn bản

Mô tả được tạo tự động

+ Pass cho level này nằm ở thư mục tên là “inhere”

Ảnh có chứa văn bản

Mô tả được tạo tự động

+ Khi vào được level ta dùng lệnh ls để xem các thư mục và file ta thấy được thư mục tên “inhere”

+ Dùng lệnh cd để di chuyển vào thư mục “inhere”

+ Nhưng khi dùng lệnh ls bình thường ta không thấy bất kỳ file hay thư mục nào khác

+ Ta dùng lệnh ls -a để xem tất cả các file kể cả file ẩn và thấy file tên “.hidden”

+ Ta dùng lệnh cat giống level 1 để đọc file có những ký tự đặc biệt

+ Ta tìm thấy pass cho level sau: 2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe

* Level 4->5

Ảnh có chứa văn bản

Mô tả được tạo tự động

+ Pass cho level này nằm trong thư mục tên “inhere” và ở dạng ký tự con người đọc được

Ảnh có chứa văn bản, thiết bị, đồng hồ đo

Mô tả được tạo tự động

+ Sau khi di chuyển vào thư mục “inhere” tao thấy có nhiều file tên ”-file0x”

+ Đọc thử 1 file ta được kết quả như trên

Ảnh có chứa văn bản

Mô tả được tạo tự động

+ Sau khi đọc tới file07 thì ta được pass của level sau

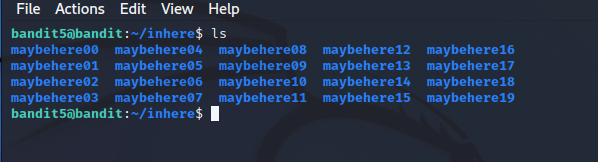
+ Pass cho level sau: lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR

* Level 5->6

Ảnh có chứa văn bản

Mô tả được tạo tự động

+ Pass nằm ở đâu đó trong thư mục “inhere” với những thuộc tính ký tự đọc được, 1033 byte kích thước và không thực thi được



+ Khi dùng lệnh ls ta thấy có rất nhiều foler “maybeherexx” nhưng ta không thể tìm hết được

+ Ta biết được file có kích thước 1033 byte



+ Ta dùng lệnh file với option -size để tìm file 1033 byte và thấy nó ở in thư mục “maybehere07” và tên”./file2”



+ Pass cho level tiếp theo: P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU

* Level 6->7

Ảnh có chứa văn bản

Mô tả được tạo tự động

+ Pass cho level này năm ở “somewhere on the server” và có các thuộc tính sở hữu bởi user bandit7, sở hữu bởi group bandit6 và kích thước 33 byte



+ Ta dùng lệnh find với option -user -group -size để kiếm





+ Ta thấy các thư mục khác đề không chó phép đọc chỉ có thư mục này ta truy cập vào đọc

+ Ta kiếm được pass cho level: z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S

* Level 7->8

Ảnh có chứa văn bản

Mô tả được tạo tự động

+ Pass cho level này năm ở dòng millionth



+ Ta cat thử file data.txt có rất nhiều dòng không thề tìm hết được



+ Ta dùng lênh grep để kiếm dòng có chứ từ “milionth”

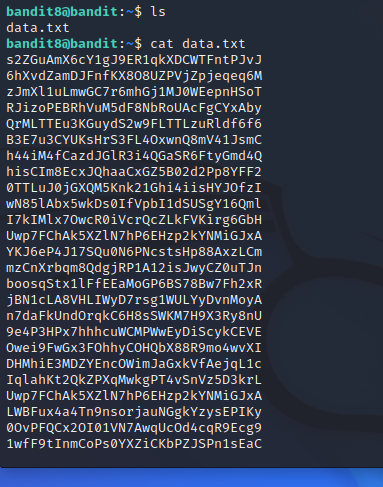
+ Pass cho level sau : TESKZC0XvTetK0S9xNwm25STk5iWrBvP

* Level 8->9

Ảnh có chứa văn bản

Mô tả được tạo tự động

+ Pass cho level nằm ở file data.txt và chỉ xuất hiện 1 lần



+ Ta cat file data.txt thì thấy có rất nhiều dòng

+ Ta chỉ lọc những dòng xuất hiện 1 lần

Ảnh có chứa văn bản

Mô tả được tạo tự động



+ Pass cho level sau: EN632PlfYiZbn3PhVK3XOGSlNInNE00t

* Level 9->10

Ảnh có chứa văn bản

Mô tả được tạo tự động

+ Pass nằm ở file data.txt và có thể đọc được

Ảnh có chứa văn bản

Mô tả được tạo tự động

+ Ta lướt qua các dòng thì thấy có dòng này có ký tự có thể đọc được

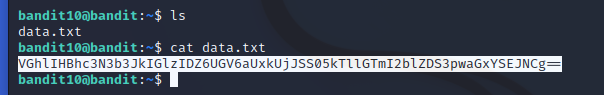
+ Pass cho level: G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s

* Level 10->11

Ảnh có chứa văn bản

Mô tả được tạo tự động

+ Pass nằm trong file data.txt và ở dạng base64 encode



+ cat file data.txt tao thấy pass ở dạng base64

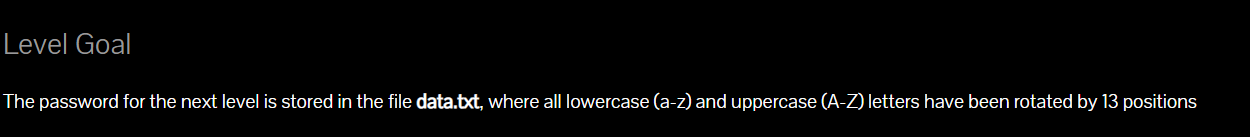
+ Ta dùng base64 encoding để lấy pass

Ảnh có chứa văn bản

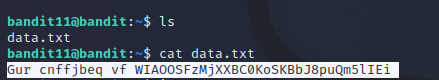
Mô tả được tạo tự động

+ Pass cho level: 6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM

* Level 11->12



+ Pass nằm trong file data.txt đã bị mã hóa thay thế bằng ROT13



+ ta cat xem thử file data.txt thì thấy pass đã bị thay thế bởi ROT13 cipher

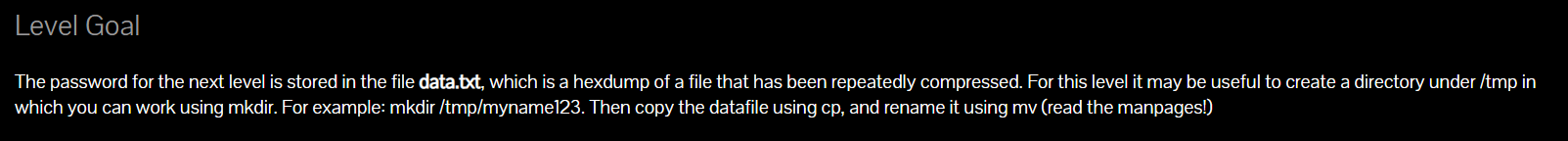
+ Lên cypherchef để giải mã

Ảnh có chứa văn bản

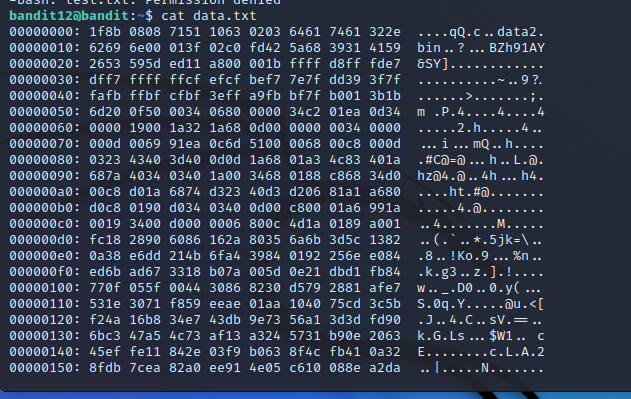
Mô tả được tạo tự động

+ Pass cho level: JVNBBFSmZwKKOP0XbFXOoW8chDz5yVRv

* Level 12->13



+ Pass cho level sau ở file data.txt đã bị nén liên tục và trở thành hexdump



+ File data.txt là 1 file hex đã được nén nhiều lần

Ảnh có chứa văn bản

Mô tả được tạo tự động

+ ta dùng lệnh xxd -r để chuyển đổi file hexdump thành file bin

+ Sau đó dùng lệnh file để xem nó là dạng file gì

+ Sau đó biết nó là file gzip

+ Sáu đó dùng lệnh gzip để giải nén và đè lên lại file data

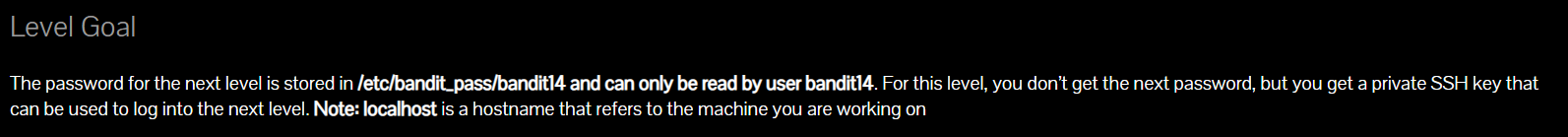
+ Ta cú làm lại nhiều lần và sẽ thấy có 1 file ascii

Ảnh có chứa văn bản

Mô tả được tạo tự động

+ Pass cho level: wbWdlBxEir4CaE8LaPhauuOo6pwRmrDw

* Level 13->14



+ Pass cho level lưu ở 1 thư mục mà chỉ có thể được truy cập bởi user bandit14. Nhưng ta có thể truy cập vào level sau bằng localhost với ssh key private



+ Ta thấy có file sshkey.private chứa key dùng để xác thực

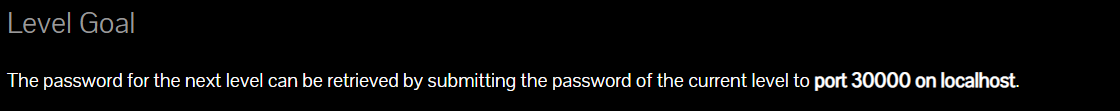
Ảnh có chứa văn bản

Mô tả được tạo tự động

+ Ta dùng lệnh ssh option -i để xác thực public key dùng private key

+ Và Pass để dùng cho level sau được lưu trong /etc/bandit\_pass\_bandit14: fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq

* Level 14->15

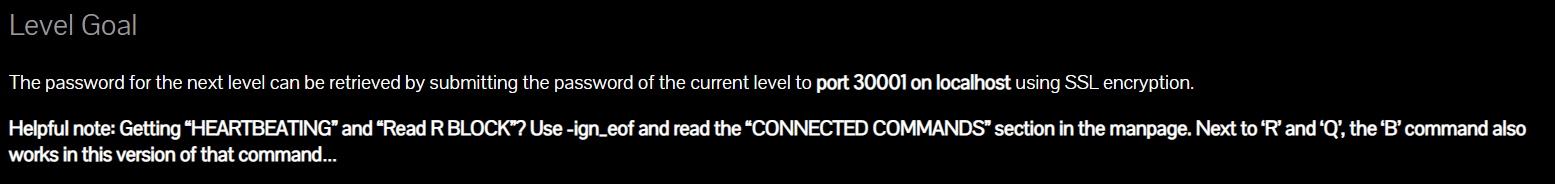


+ Pass cho level có thể lấy bằng cách submit pass lấy được ở level trên nhưng không dùng vào localhost port 30000

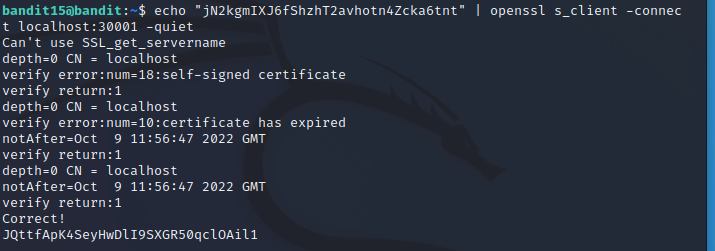


+ Pass : jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt

* Level 15->16



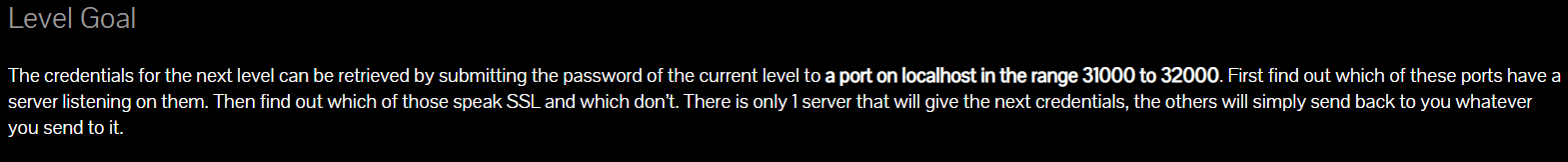
+ Pass cho level có thể lấy bằng cách submit pass của level hiện tại vào localhost port 30001 dùng SSL encryption



+ Ta dùng lênh openssl s\_client Để kết nối dùng SSL, option conect để kết nối với host và port. -quiet để không in ra các chứng chỉ

+ Pass cho level: JQttfApK4SeyHwDlI9SXGR50qclOAil1

* Level 16->17



+ Lấy thông tin xác thực bằng cách submit pass ở level hiện tại tới 1 trong những port trong khoảng 31000-32000 và prot nào sử dụng SSL

Ảnh có chứa văn bản

Mô tả được tạo tự động

+ Ta dùng nmap để quét các cổng để xem cổng nào mở

+ Ảnh có chứa văn bản

Mô tả được tạo tự động

+ Sau đó ta thử từng cổng và có cổng 31790 là đúng và phản hồi lại

Ảnh có chứa văn bản

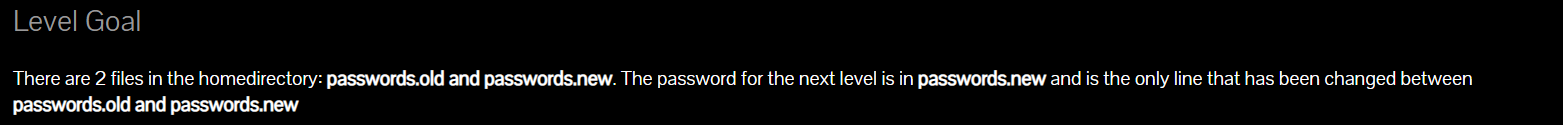
Mô tả được tạo tự động

+ Ta lưu private key này và dùng nó để kết nối localohost với user của level tiếp theo và dùng SSH

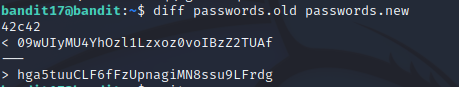
Ảnh có chứa văn bản

Mô tả được tạo tự động

* Level 17->18



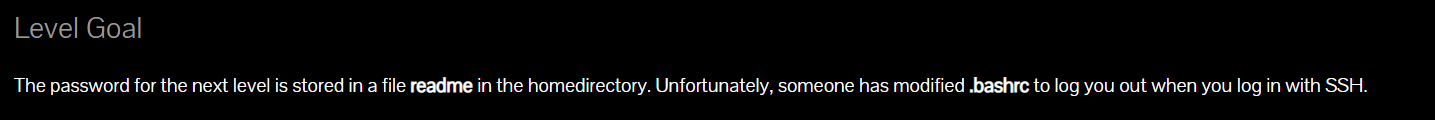
+ Có 2 pass là old và new và pass nằm ở trong new mà có dòng đã được thay đổi so với file old



+ Ta dùng lệnh diff để kiểm tra

+ Pass cho level : hga5tuuCLF6fFzUpnagiMN8ssu9LFrdg

* Level 18->19



+ Pass trong file readme nhưng nó được modified để log out khi mình cố truy cập vào

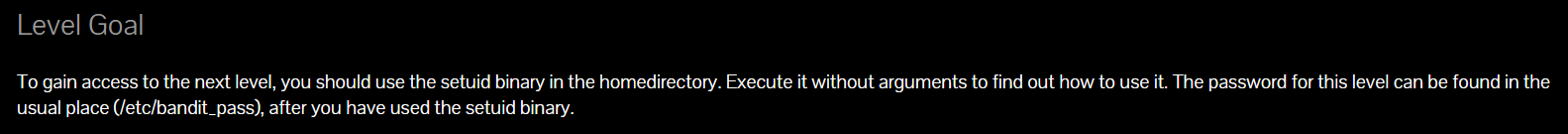
+ Ảnh có chứa văn bản

Mô tả được tạo tự động

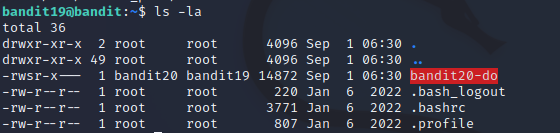
+ Ta có thể truyền lệnh muốn thực thi vào SSH nếu như không thể đăng nhập vào

+ Pass cho level sau: awhqfNnAbc1naukrpqDYcF95h7HoMTrC

* Level 19->20



+ Pass cho level nằm trong /etc/bandit\_pass. Ta dùng seyuid trong homedirectory và thực thi nó mà không dùng đối số



+ File bandit20-do có 1 trường s nghĩa là setuid. Nghĩa là file chỉ được thực thi dưới sự cho phép của chủ sở hữu.

+ Bất kỳ commandline nào chạy dưới dandit20-do sẽ như là user bandit 20



+ Pass cho level: VxCazJaVykI6W36BkBU0mJTCM8rR95XT

* Level 20->21

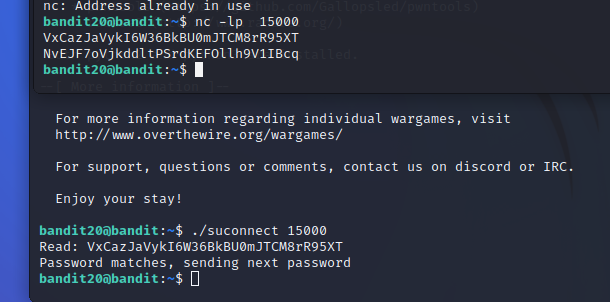
Ảnh có chứa văn bản

Mô tả được tạo tự động

+ Ở level này ta cần mở 2 terminal cùng kết nối vào level 20

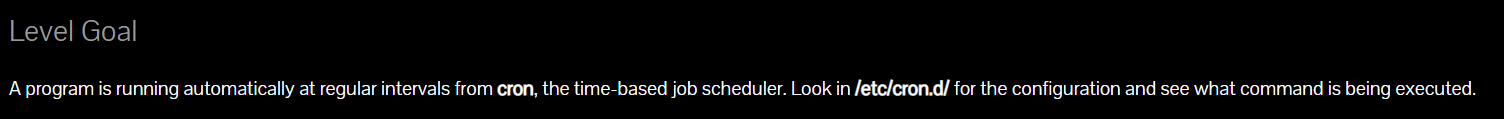
+ Sau đó thực thi file suconnect ở 1 trong 2 terminal với port bất kỳ

+ Ở terminal còn lại ta cần dùng nc để kết nối và lắng nghe từ terminal còn lại ở cùng port sau đó gửi pass của level thì nó sẽ trả về pass của level



+ Pass của level: NvEJF7oVjkddltPSrdKEFOllh9V1IBcq

* Level 22



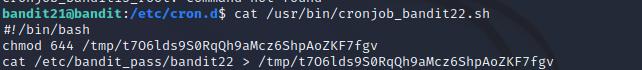


+ Ta thấy có file cronjob\_bandit22 có thể sẽ là file ta cần xem

+ Ta xem thử file này có gì



+ Ta xem trong /usr/bin/cronjob\_bandit22.sh có gì



+ Ta thấy nó tạo 1 file trong thư mục tmp sau đó cat pass cho level sau

+ Nên ta cat có thể dủng cat để xem trong tmp/t7O6lds9S0RqQh9aMcz6ShpAoZKF7fgv để có pass



+ Pass cho level sau: WdDozAdTM2z9DiFEQ2mGlwngMfj4EZff

* Level 22->23

Ảnh có chứa văn bản

Mô tả được tạo tự động

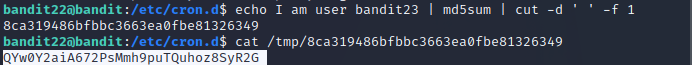
Ảnh có chứa văn bản

Mô tả được tạo tự động

+ Tương tự như level trước

+ Nhưng trong file sh chỗ lưu pass đã thay đổi bằng giá trị của câu lệnh echo

+ Vì vậy ta chỉ cần in giá tri của câu lệnh là được



+ Pass cho level : QYw0Y2aiA672PsMmh9puTQuhoz8SyR2G

* Level 23->24

Ảnh có chứa văn bản

Mô tả được tạo tự động

Ảnh có chứa văn bản

Mô tả được tạo tự động

+ Tương tự như level trước

+ Các file trong /var/spool/bandit24/foo sau khi thưv5 thi thì sẽ bị xóa

+ Vì vậy ta cần tạo 1 script để lưu pass vào 1 thư mục mà ta có thể đọc được





+ Sau đó copy vào thư mục var/spool/bandit24/foo

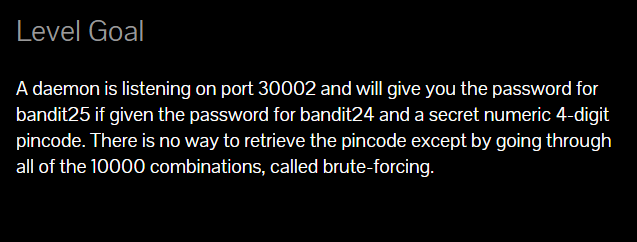
+ Thì trong thư mục hiện tại sẽ xuất hin65 1 file và cat file đó sẽ có pass

Ảnh có chứa văn bản

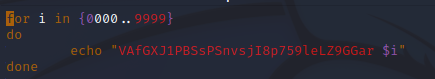
Mô tả được tạo tự động

+ Pass: VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar

* Level 24->25



+ Ta kết nối vào localhost port 30002 và nó sẽ yêu cầu pass là của bandit24 + 4 số từ 0000 đến 9999 nếu cũng pincode thì nó sẽ trả về mật khẩu



Ảnh có chứa văn bản

Mô tả được tạo tự động

+ Ta lưu output vào file bruteforce sau đó đưa đầu vào file này vào lệnh nc

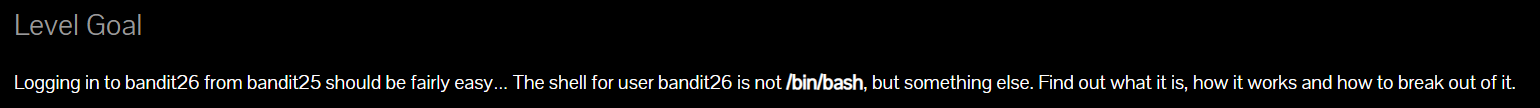
+ Output lệnh nc đưa vào file pass25.txt

+ Kết quả



+ Pass: p7TaowMYrmu23Ol8hiZh9UvD0O9hpx8d

* Level 25->26





+ Có key ta thử dùng cách truy cập như những level ở trên



+ Nhưng thất bại

+ Shell dùng trong level này không phải bin/bash

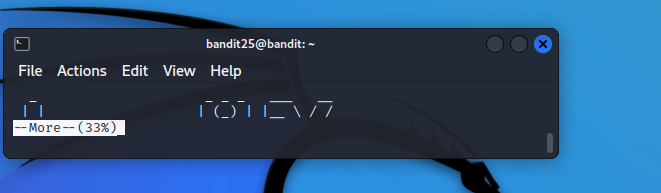


+ Vào /etc/passwd để tìm shell của bandit26. Nó là 1 showtext

Ảnh có chứa văn bản

Mô tả được tạo tự động

+ Ta thấy shell đọc với lệnh more sau đó thoát. Vì nội dung kích thước không đủ dài nên ta cần giảm kích thước của terminal xuống



+ Sau đó ấn v để vào vim

+ Sau đó gõ lệnh

:set shell=/bin/bash

Sau đó gõ :shell



+ Ta đã vào được shell bandit 26

* Level 26->27

Ảnh có chứa văn bản

Mô tả được tạo tự động

Ảnh có chứa văn bản, tấm

Mô tả được tạo tự động

+ Giống level 20 ở trên

+ Pass cho level: YnQpBuifNMas1hcUFk70ZmqkhUU2EuaS

* Level 27->28
* Level 29
* Level 30
* Level 31
* Level 32
* Level 33