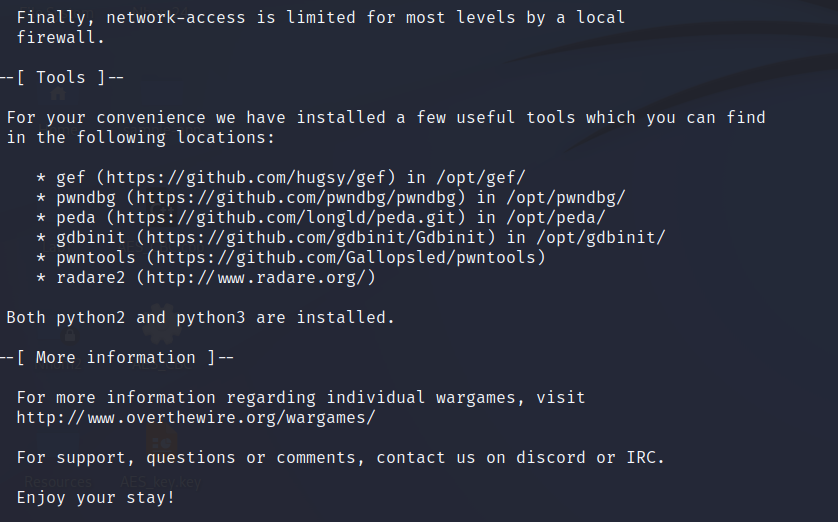
**WRITE-UP BANDIT**

**Level 0:**

Đăng nhập vào Bandit bằng ssh, nhưng ssh có port mặc định là 22 nên phải thay đổi port của bandit là 2220



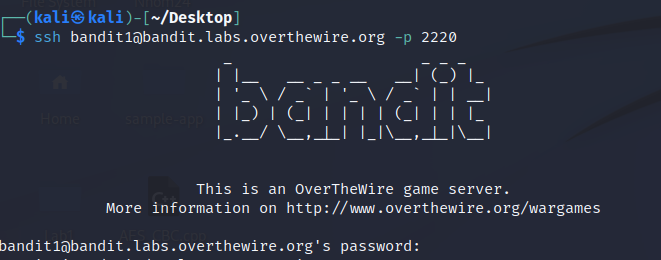
Nhập password là bandit0, đăng nhập thành công



**Level 0 - 1:**

Sử dụng lệnh cat để xem file readme, ta thu được password của lv1. Đăng nhập vào bandit như ở level 0 với username là bandit1 và password mới tìm được





**Level 1 - 2:**

Sử dụng lệnh ls để xem các tập tin hiện có, ta thấy chỉ có mỗi tập tin “-” và không thể dùng lệnh cat trực tiếp được



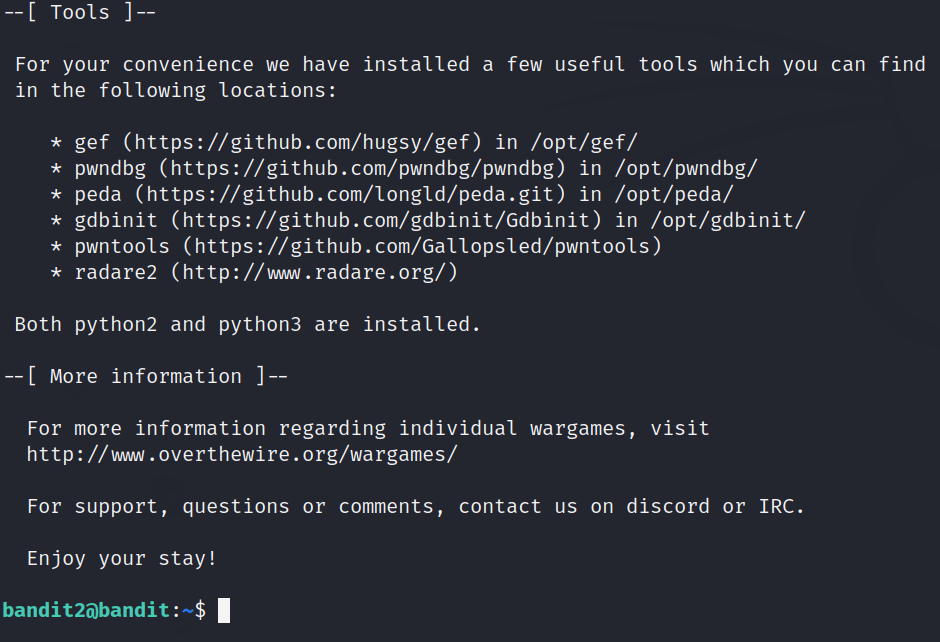
Trong Linux để xem thư mục “-” chúng ta có thể cat toàn bộ đường dẫn của tập tin này. Dùng lệnh pwd để xem đường dẫn của thư mục ta đang đứng.



Khi có path, ta cat tới tập tin “-” qua đường dẫn này

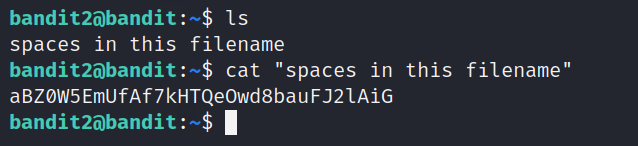


Với password vừa tìm được ta tiếp tục đăng nhập tới level 3 với username là bandit2

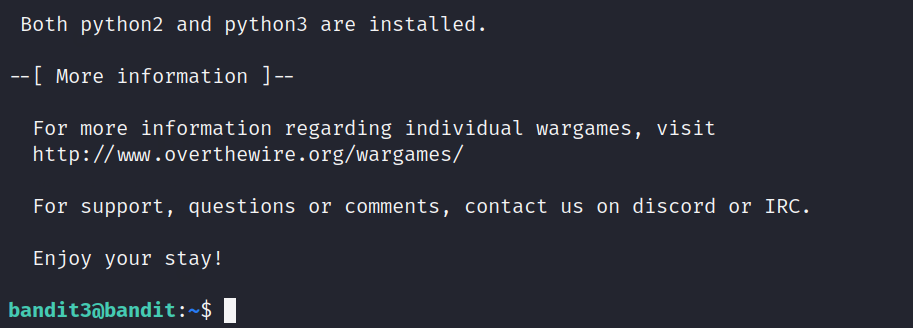


**Level 2 - 3**

Pass nằm trong tập tin spaces in this filename, ta xem thư mục này. Lưu ý để xem các file mà tên file có dấu cách thì thêm “ trước và sau tên

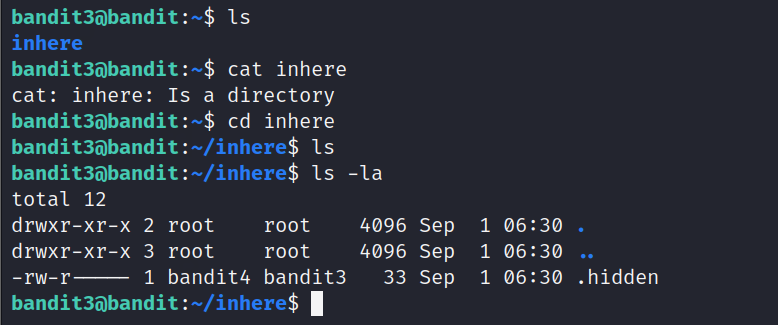


Tiếp tục đăng nhập với username là bandit3



**Level 3 - 4**

Ở level này, ta thấy thêm một thư mục inhere, cd vào thư mục này và không thấy bắt kì thứ gì nữa, có thể là các tập tin chứa pass đã bị ẩn. Ta dùng lệnh ls -la để xem các tập tin đã bị ẩn đó.



Ta thấy một tập tin .hidden bị ẩn, cat thử xem tập tin và ta thấy được pass nằm trong đó

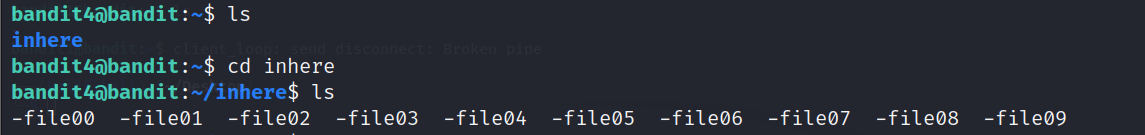


Tiếp tục đăng nhập với username là bandit4

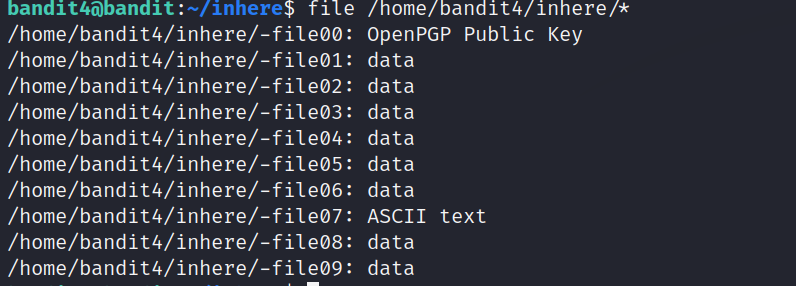
2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe

**Level 4 - 5**

Dùng lệnh cd để vào inhere sau đó ls để xem các file ở đây. Ta thấy tất cả các file đều có dấu “-” trong tên và ta không thể biết được file nào chứa pass



Hint của level này cho ta biết pass nằm trong tập tin *only human-readable.* Ta dùng lệnh file để tìm những tập tin *only human-readable* (lưu ý là do tên có dấu “-” nên phải dùng toàn bộ đường dẫn thư mục đang làm việc)



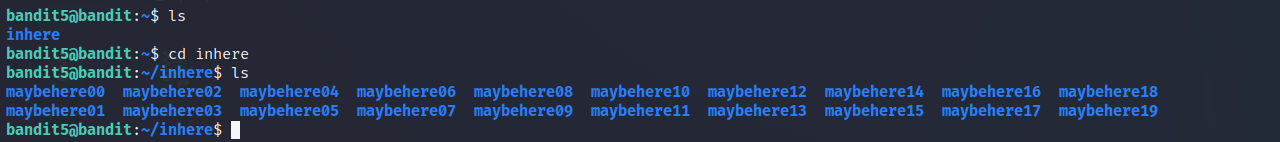
Ta thấy -file07 có dạng là ASCII text nên có thể pass nằm trong đó. Cat để xem và ta thấy được pass thật



Tiếp tục đăng nhập với username là bandit5

**Level 5 - 6**

Trong inhere ta thấy có rất nhiều thư mục và ta không thể biết chính xác là file chứa password nằm ở thư mục nào.



Dùng lệnh find để tìm kiếm với các option như mô tả.



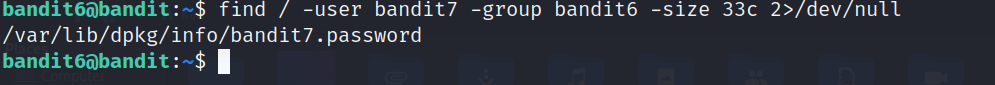
Với -type là kiểu của file và -size là kích thước file cần tìm, ta thấy chỉ có file nằm ở ./maybehere07/.file2 được tìm thấy. Xem thử file này và ta thu được password.



Tiếp tục đăng nhập vào level tiếp theo với username là bandit6

**Level 6 - 7**

Tiếp tục sử dụng lệnh find để tìm kiếm các tập tin theo hint



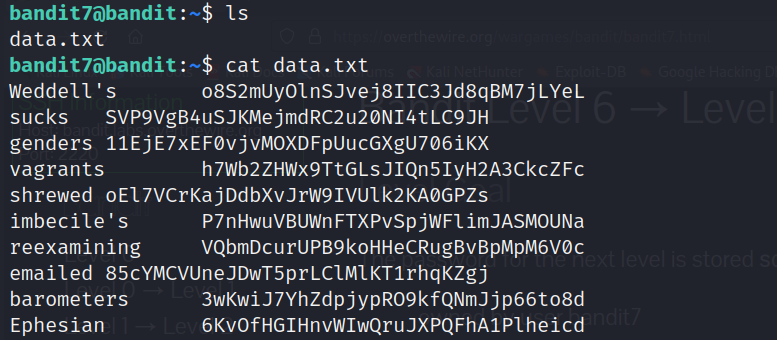
Trong đó -user chỉ định người dùng, -group chỉ định nhóm, -size là kích thước còn 2>/dev/null là chuyển hướng thông báo lỗi đến thùng rác. Ta tìm được 1 tập tin, thử xem với toàn bộ đường dẫn.



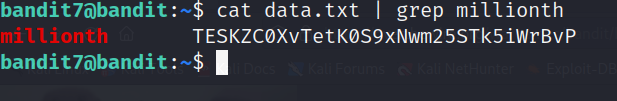
Tìm được pass, tiếp tục đăng nhập với username là bandit7

**Level 7 - 8**

Xem thử file data.txt



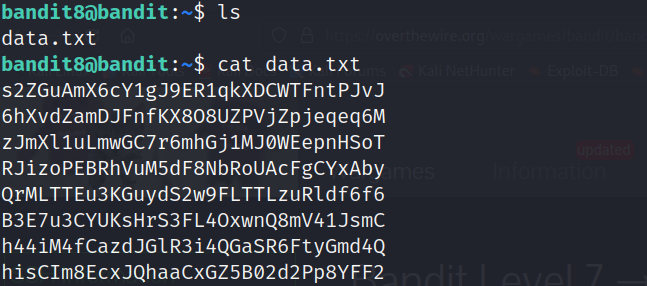
Có thể thấy có rất nhiều thông tin trong data.txt, theo hint thì pass nằm cạnh từ millionth, sử dụng grep millionth



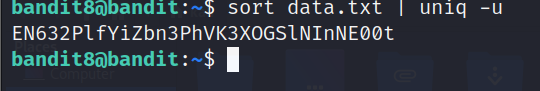
Đã có được pass ta tiếp tục đăng nhập với username là bandit8

**Level 8 - 9**

Như level trên, có rất nhiều dữ liệu trong data.txt. Theo hint thì pass chỉ xuất hiện 1 lần duy nhất

 \

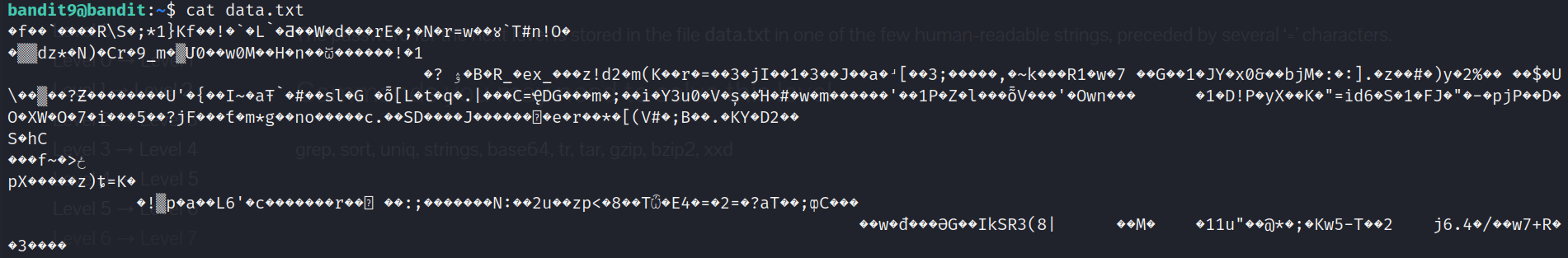
Thử sắp xếp các dòng trong file theo thứ tự alphabet và hiển thị dòng xuất hiện 1 lần duy nhất



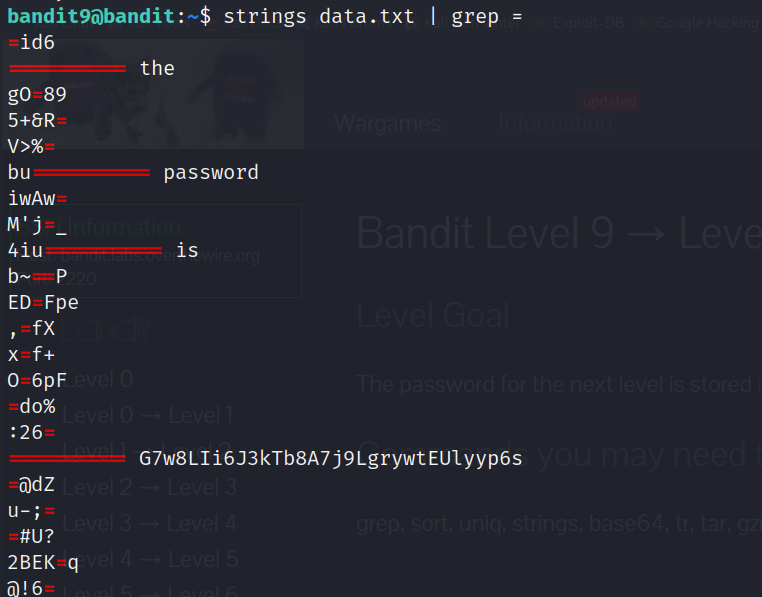
Đã tìm thấy pass tiếp tục đăng nhập với username là bandit9

**Level 9 - 10**

Ta thấy data.txt chứa nội dung không thể đọc được, vậy thử dùng lệnh strings để xuất ra các dòng cá thể đọc được kèm thêm grep =



Ta tìm thấy 1 dòng có thể là pass



Thử đăng nhập vào level tiếp theo bằng pass này với username là 10. Thành công.

**Level 10 - 11**

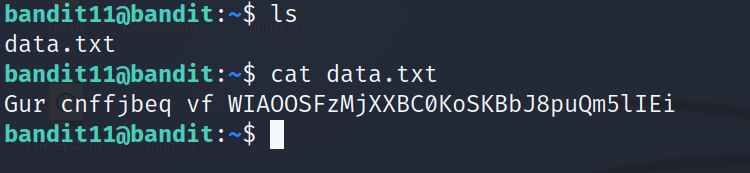
Theo hint thì đoạn pass nằm trong data.txt đã được mã hóa base64. Cat data.txt cũng với giải mã đoạn pass



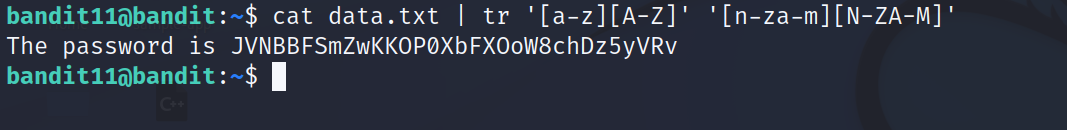
Ta có được đoạn pass, đăng nhập với username là bandit11

**Level 11 - 12**

Như đã thấy, pass được mã hóa bằng cách thay đổi các chữ cái.



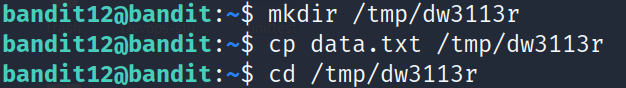
Ta sử dụng thuật toán ROT13 giải mã đoạn văn bản



Có được pass ta đăng nhập vào level tiếp theo bằng username là bandit12

**Level 12 - 13**

Do không có quyền chỉnh sửa ở thư mục hiện tại nên ta copy data.txt vào thư mục có đường dẫn /tmp/dw3113r để chỉnh sửa, sau đó ta thử reverse data.txt

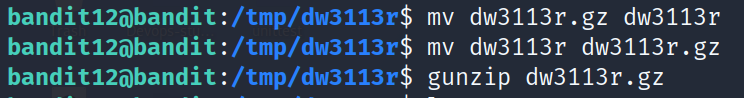




Xem thử dw3113r là loại file gì



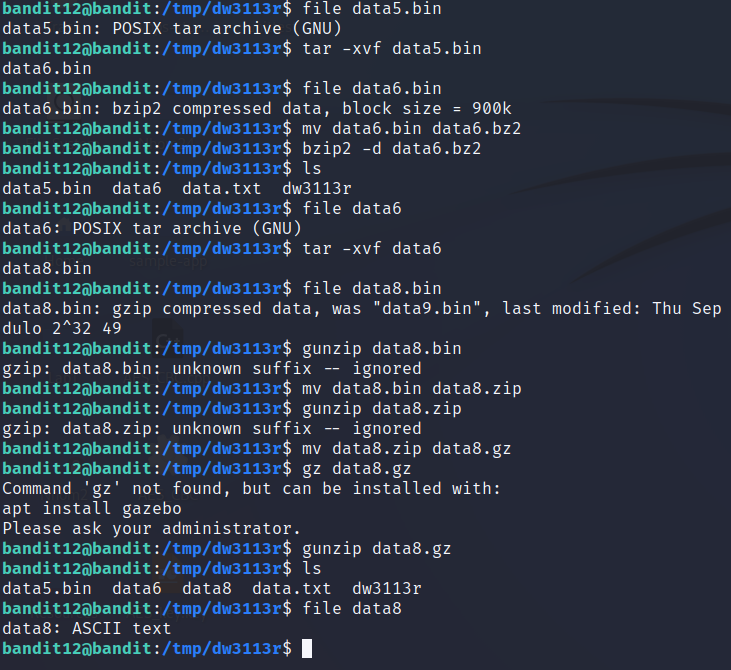
Đây là một file gzip, hãy đổi tên và giải nén nó



Xem tiếp dw3113r là gì



Tiếp tục đổi tên và giải nén các file, cuối cùng ta thu được 1 file ASCII text



Xem thư file này ta thấy được password

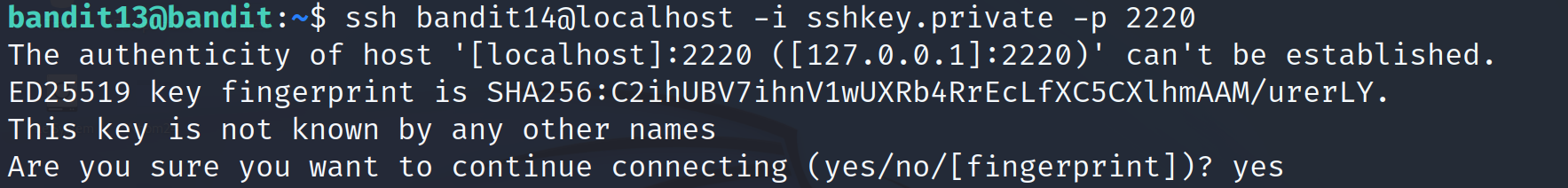


Đăng nhập vào level tiếp theo với username là bandit13

wbWdlBxEir4CaE8LaPhauu0o6pwRmrDw

**Level 13 - 14**

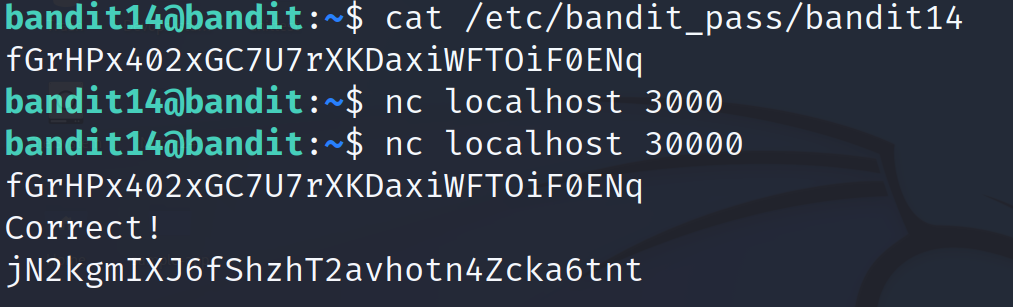
Để đăng nhập vào level tiếp theo, sử dụng file sshkey.private như là password



Đăng nhập thành công vào level tiếp theo

**Level 14 - 15**

Ta xem password của lv14 tại đường dẫn /etc/bandit\_pass/banditX (đường dẫn chứa pass của các level), sau đó dùng netcat để truy cập tới port 30000 để lấy pass của lv tiếp theo



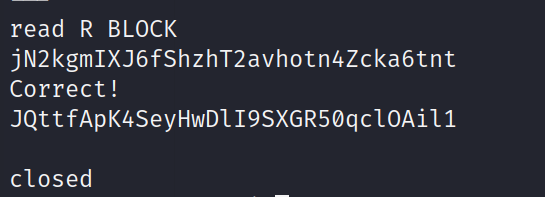
Sau khi có được pass ta đăng nhập vào lv tiếp theo

**Level 15 - 16**

Level này cũng giống level trước, ta sẽ gửi password của level hiện tại tới localhost qua port 30001 sử dụng mã hóa SSL.

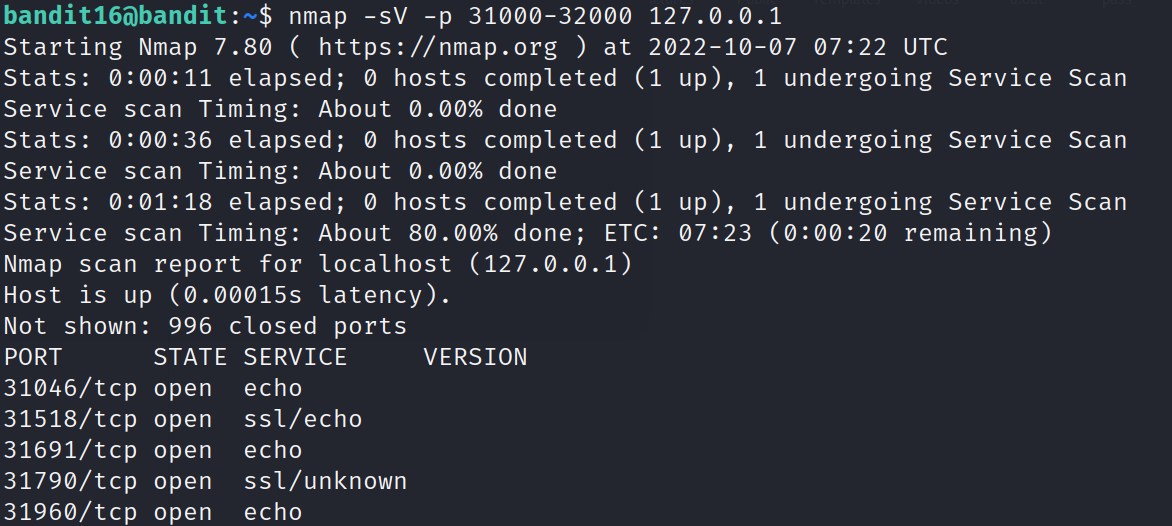


Dùng openssl với s\_client để kết nối tới SSL, sau đó chúng ta nhập password của lv này và nhận được pass của lv tiếp theo

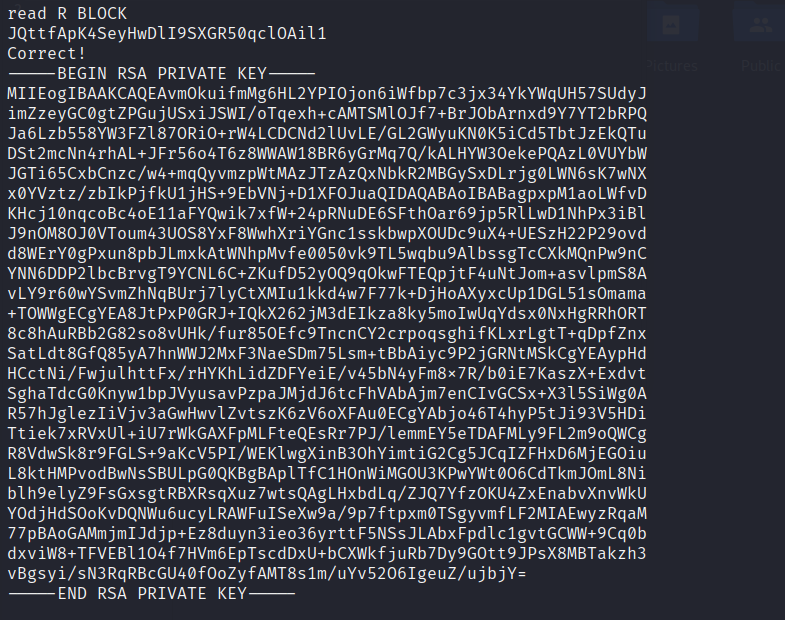


**Level 16 - 17**

Level này cũng giống như 2 level trước, thuy nhiên chúng ta cần tìm ra port đang được listen và cho kết nối SSL



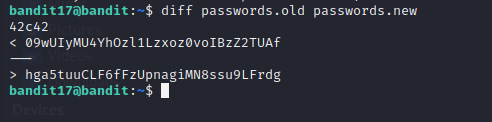
Sử dũng nmap để quét các port trong đó -sV là các service có port đang mở, -p là khoảng port cần quét. Ta thấy có 2 port là 31518 và 31790 có kết nối SSL nhưng 31515 có echo như các port khác nên ta sẽ kết nối tới port 31790.



Nhập password của lv này ta sẽ nhận được RSA key, sử dụng RSA key này như password cho lv tiếp theo.

**Level 17 - 18**

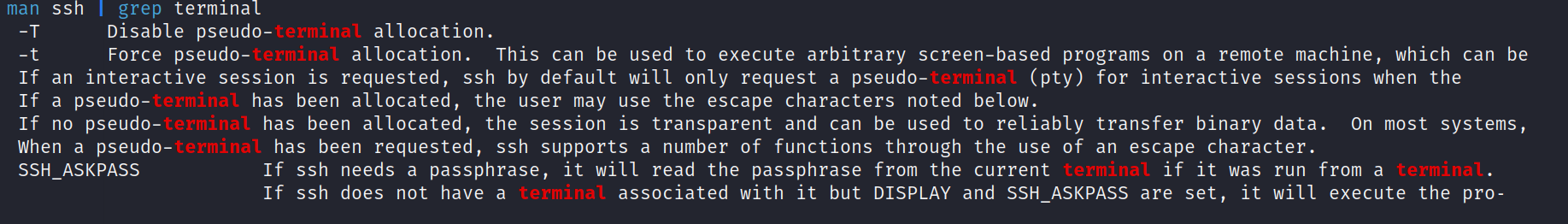
Level này yêu cầu ta tìm ra sự thay đổi duy nhất của file password.new so với password.old



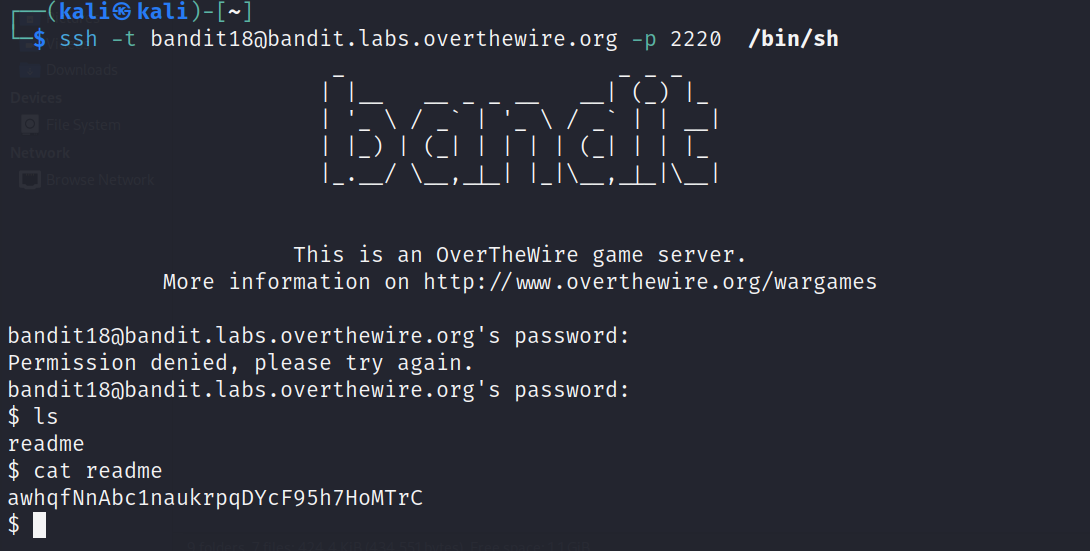
Dòng < là chỗ bị thay đổi, dòng > là được thay thế vào cũng chính là pass cho lv tiếp theo

**Level 18 - 19**

Tuy đã có password nhưng ta vẫn không thể kết nối vào ssh bởi có người đã chỉnh sủa .bashrc để ta tự động log out khi đăng nhập vào. Tuy nhiên lệnh ssh có flag -t, công dụng của nó được hiểu như sau.



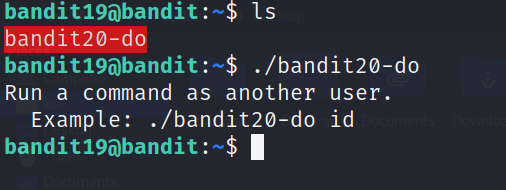
Sử dụng flag này để kết nối với ssh



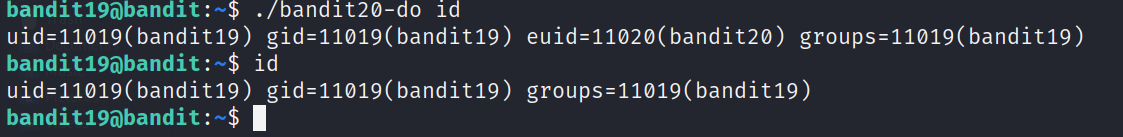
Sau khi kết nối thành công ta chỉ cần cat readme là đã có pass cho lv tiếp theo

**Level 19 - 20**

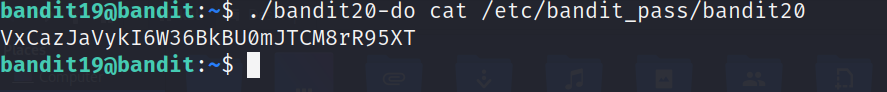
Ở level này ta thấy 1 file nhị phân, thử chạy nó. Có thể hiểu khi thực thi file này ta có thể dùng những lệnh với tư cách là user bandit20 .



Thử với ví dụ



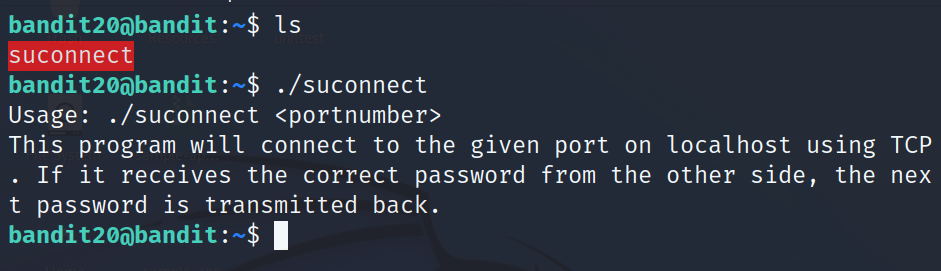
Ta thấy so với id thì xuất hiện thêm euid, vậy ta có thể đọc password bởi bandit20-do. Truy cập vào thư mục chứa pass và đọc nó.



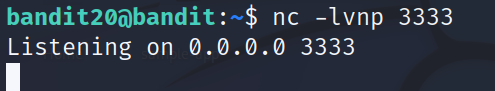
Ta đã có password của lv tiếp theo.

**Level 20 - 21**

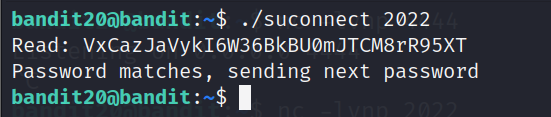
Có một file setuid như level trên, giúp kết nối tới localhost ở port ta truyền vào khi thực thi file setuid. Sau khi kết nối nó sẽ đọc 1 dòng text, nếu là password của level trước thì sẽ đưa lại password của level tiếp theo

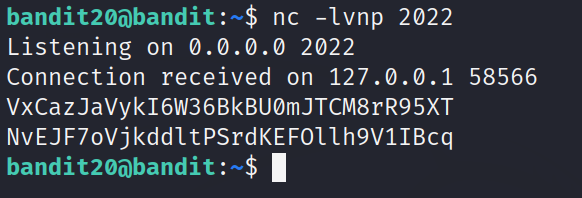


Dùng netcac để tạo 1 listener với 1 port bất kì



Sau đó dùng file suconnect và truyền vào port dùng ở netcac

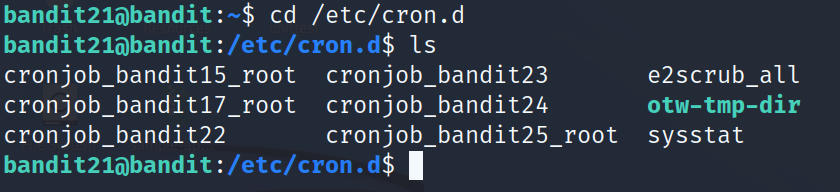




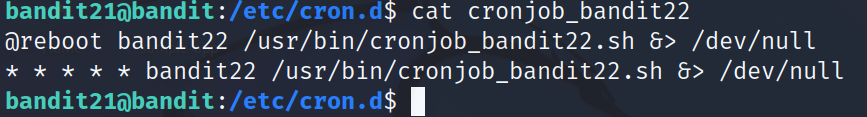
Ta đã có được password của level tiếp theo

**Level 21 - 22**

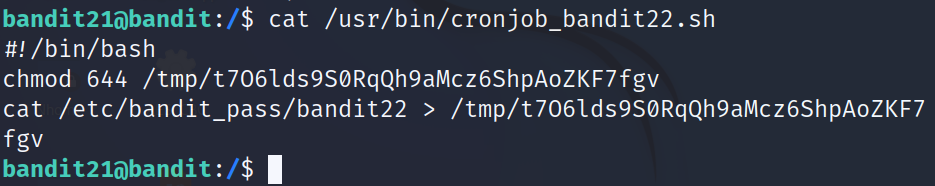
Cron là một chức năng giúp lên lịch tự động giúp thực hiện 1 công việc nào đó. Thử xem đường dẫn mà bài cho có gì



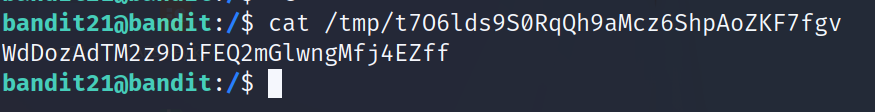
Có rất nhiều file trong đây nhưng thứ ta cần quan tâm là cronjob\_bandit22. Xem thử file này



Ta sẽ coi thử đoạn script /usr/bin/cronjob\_bandit22.sh là gì.



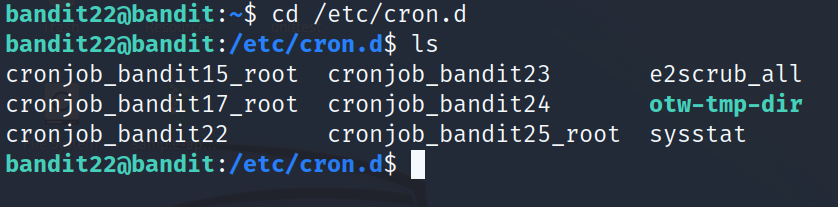
Đọc qua sẽ thấy nó sẽ cấp quyền 644 cho /tmp/t7O6lds9S0RqQh9aMcz6ShpAoZKF7fgv và /etc/bandit\_pass/bandit22 sẽ ghi đè vào /tmp/t7O6lds9S0RqQh9aMcz6ShpAoZKF7fgv. Thử xem /tmp/t7O6lds9S0RqQh9aMcz6ShpAoZKF7fgv có password không.



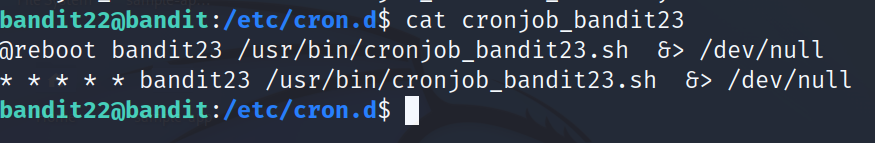
Chính xác, đây là password của level tiếp theo.

**Level 22 - 23**

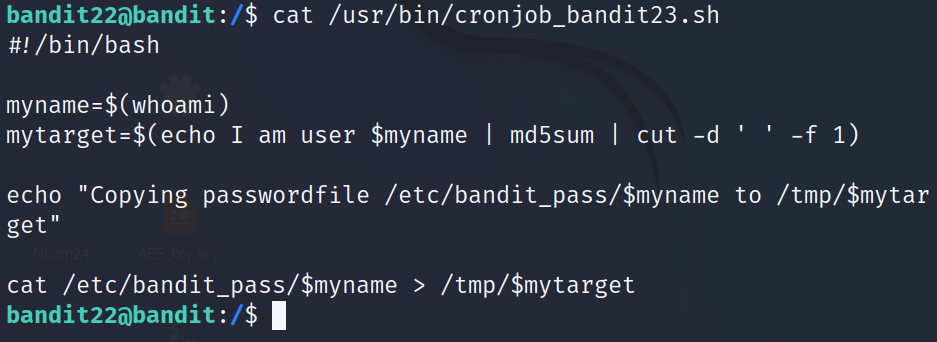
Vẫn tiếp tục xem trong /etc/cron.d có gì



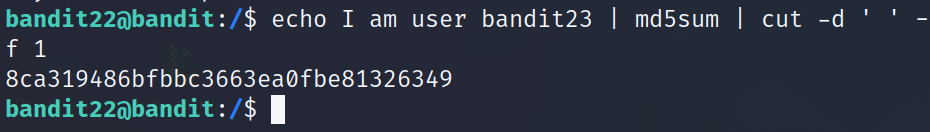
Tiếp tục xem trong cronjob-bandit23 có gì



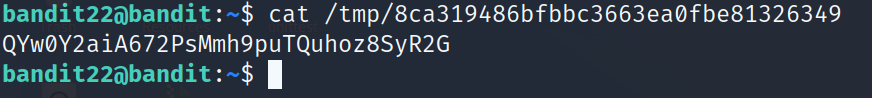
Xem thử script trong đường dẫn được reboot



Output của mytarget sẽ giúp ta tìm ra password. Thử chạy script này với myname là bandit23



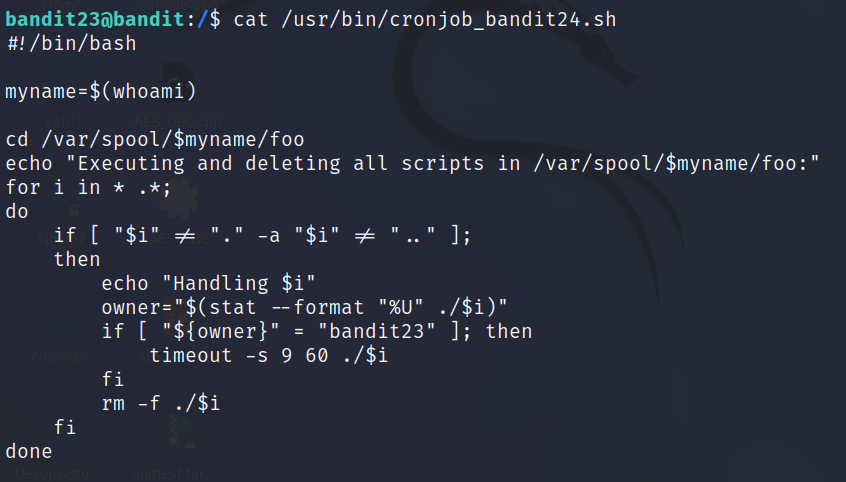
Giờ xem thử /tmp/$mytarget là gì với output vừa tìm được



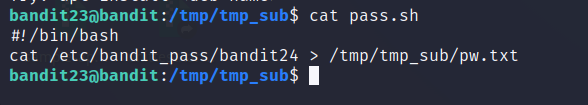
Ta có được pass của level tiếp theo

**Level 23 - 24**

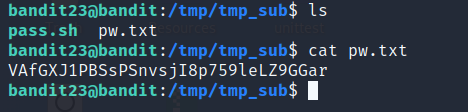
Lại là 1 bài cron job,ta vẫn tiếp tục đọc /usr/bin/cronjob\_bandit24.sh



Viết 1 file script có nội dung ghi đè passwd vào pw.txt ở một thư mục bên ngoài nào đó

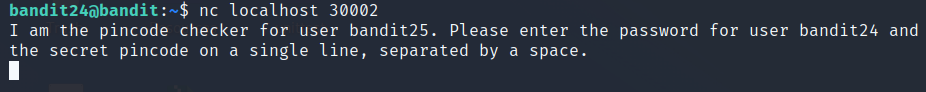


Chờ 1 tí để script thực thi, sau đó ta có được file pw.txt chứa passcua3 level tiếp theo

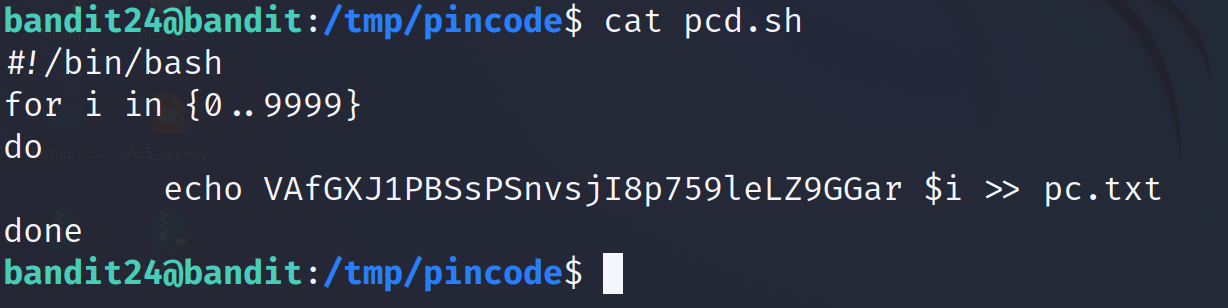


**Level 24 - 25**

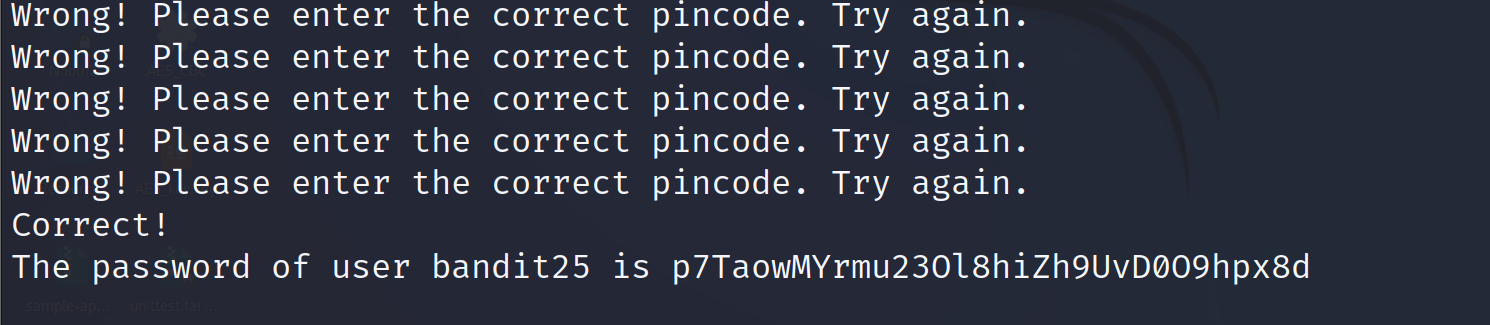
Level này cho ta biết daemon đang lắng nghe port 30002 và nếu ta đưa password của level trước thì sẽ trả lại ta passwd của level này và pincode với 4 chữ số. Thử xem kết nối của daemon



Kết nối này bảo ta phải nhập lần lượt cả password và pincode thì mới trả passwd của level tiếp theo cho ta. Vậy hãy viết 1 script nhỏ để nhập password và pincode chạy từ 0000 tới 9999 truyền vào nc.



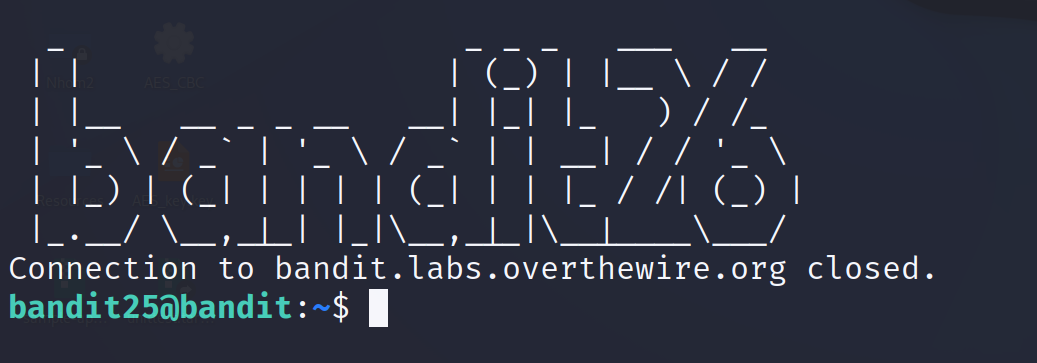
Thực thi pcd.sh sau đó truyền pc.txt vào nc để dò được password



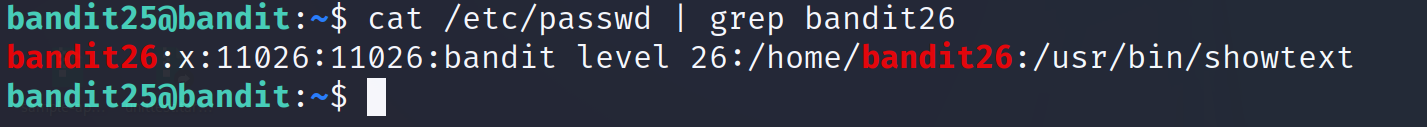
Ta có được password của lv tiếp theo

**Level 25 - 26**

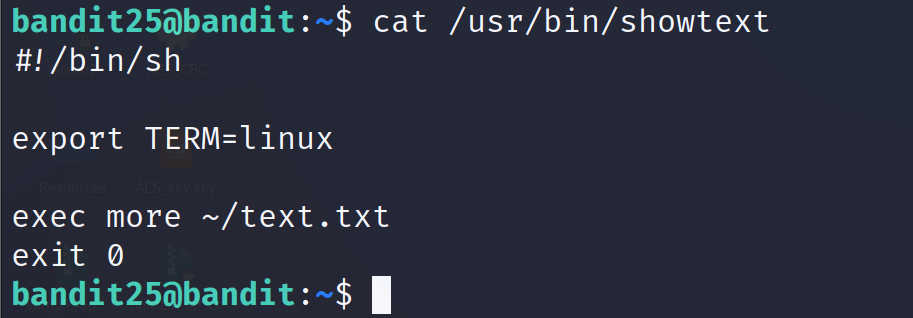
Thử sử dụng file sshkey như là password cho level tiếp theo

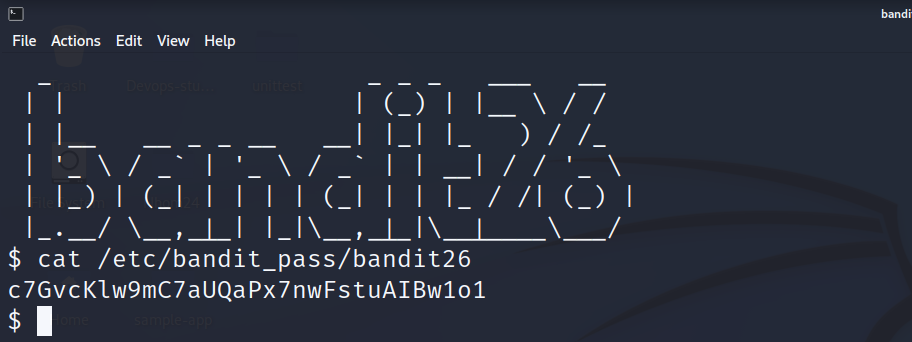


Tuy nhiên, level đã đá ta ra khỏi. Thử xem trong /etc/passwd có gì

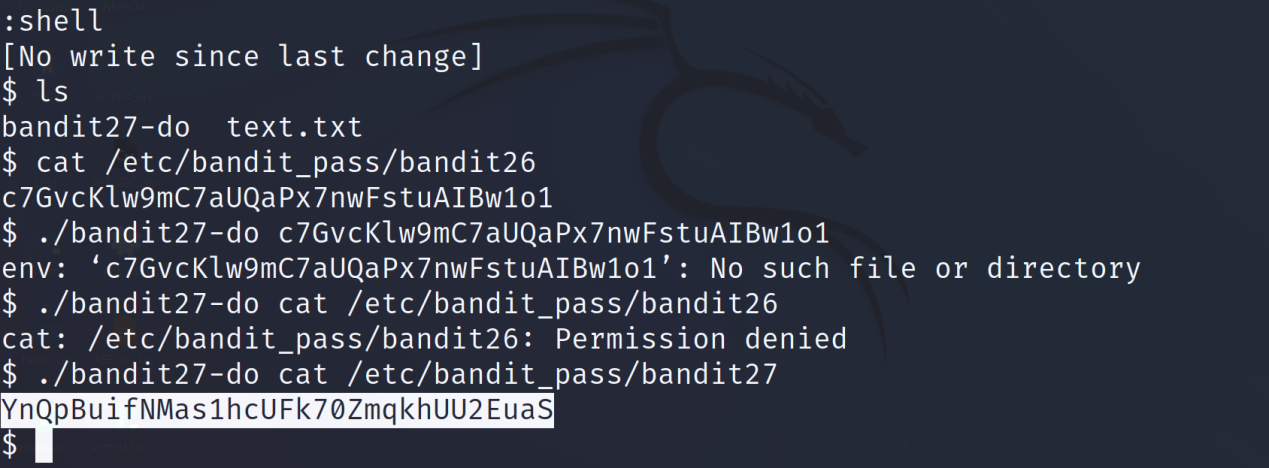


Tiếp tục xem trong /usr/bin/showtext có gì



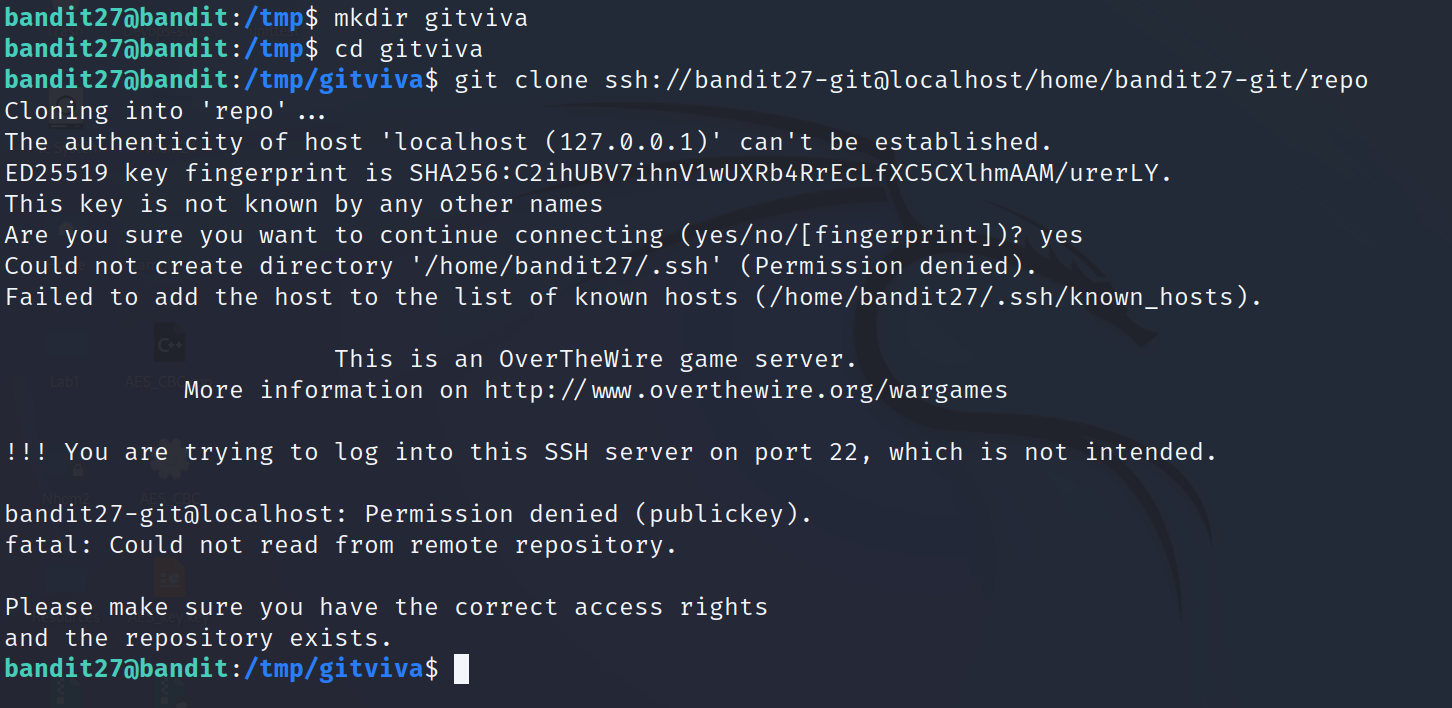


**Level 26 - 27**

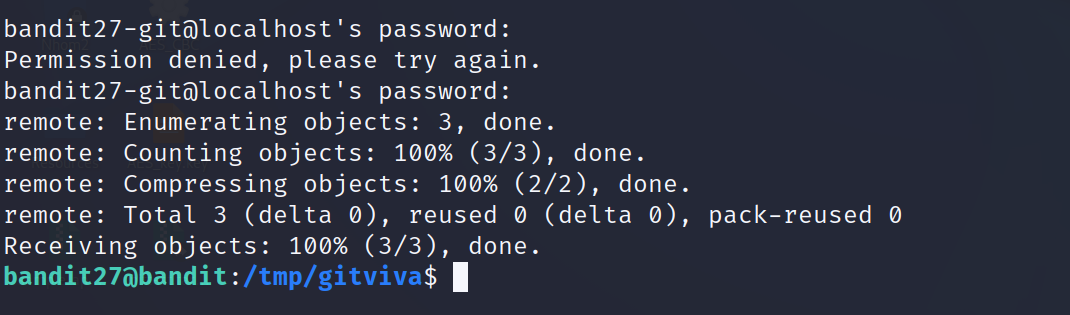


**Level 27 - 28**

Đề cho ta 1 link repo và ta sẽ clone nó về trong 1 thư mục ở /tmp



Kết quả là không kết nối được do đang dùng port mặc định là 22 nên ta sẽ thêm port 2220 vào và thử lại

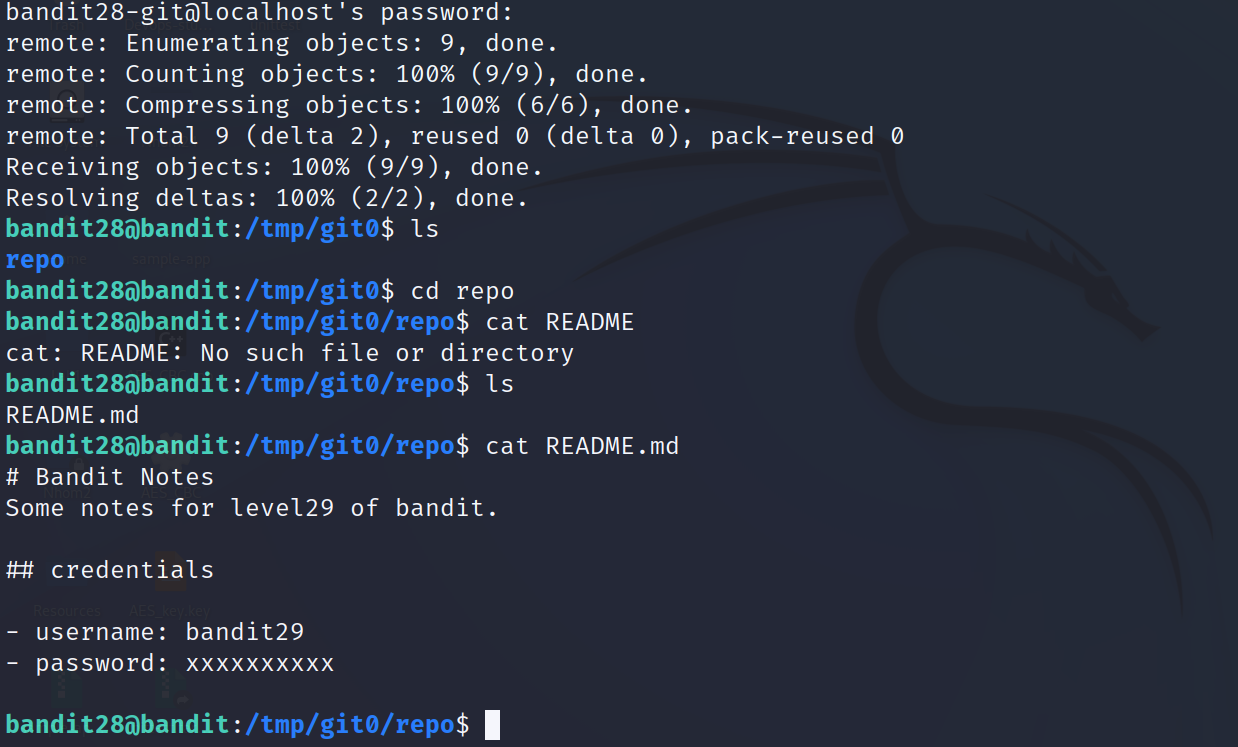


Sử dụng password của level này ta đã clone thành công, giờ thì xem trong đây có gì và đọc nó

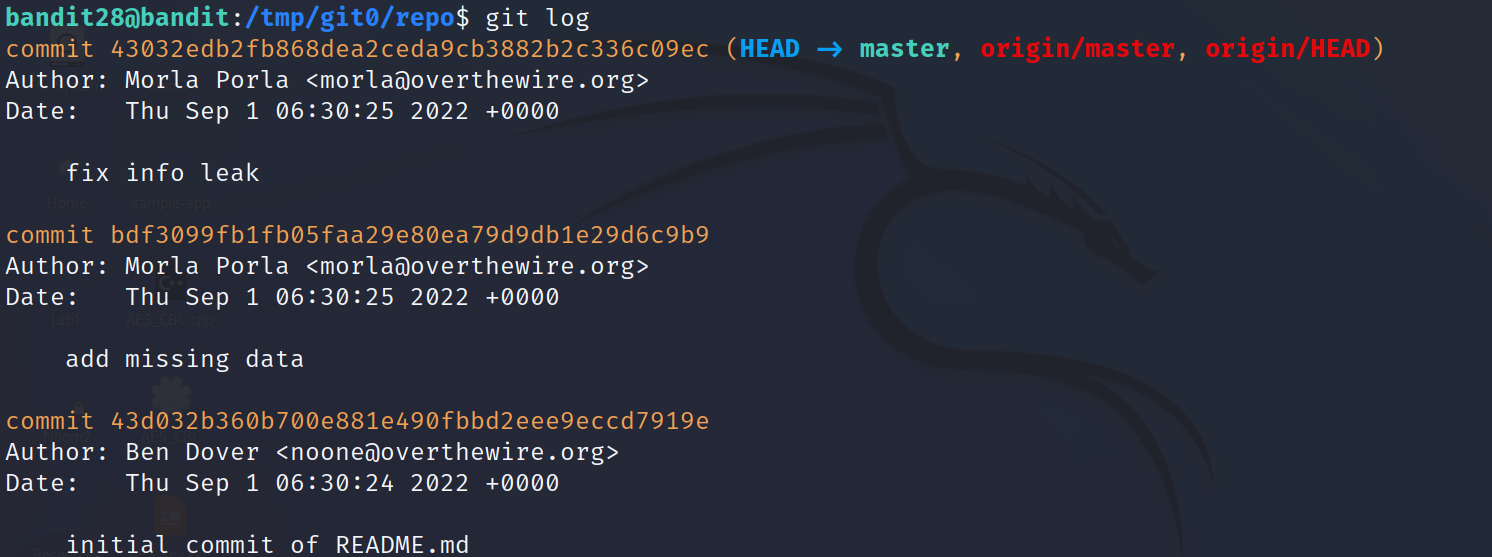


**Level 28 - 29**

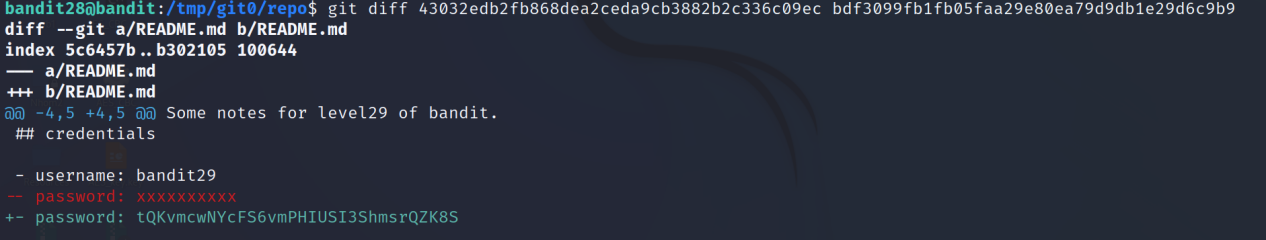
Tiếp tục tải về repo và xem thử trong đó chứa gì



Xem ra password đã bị ẩn, thử xem git log



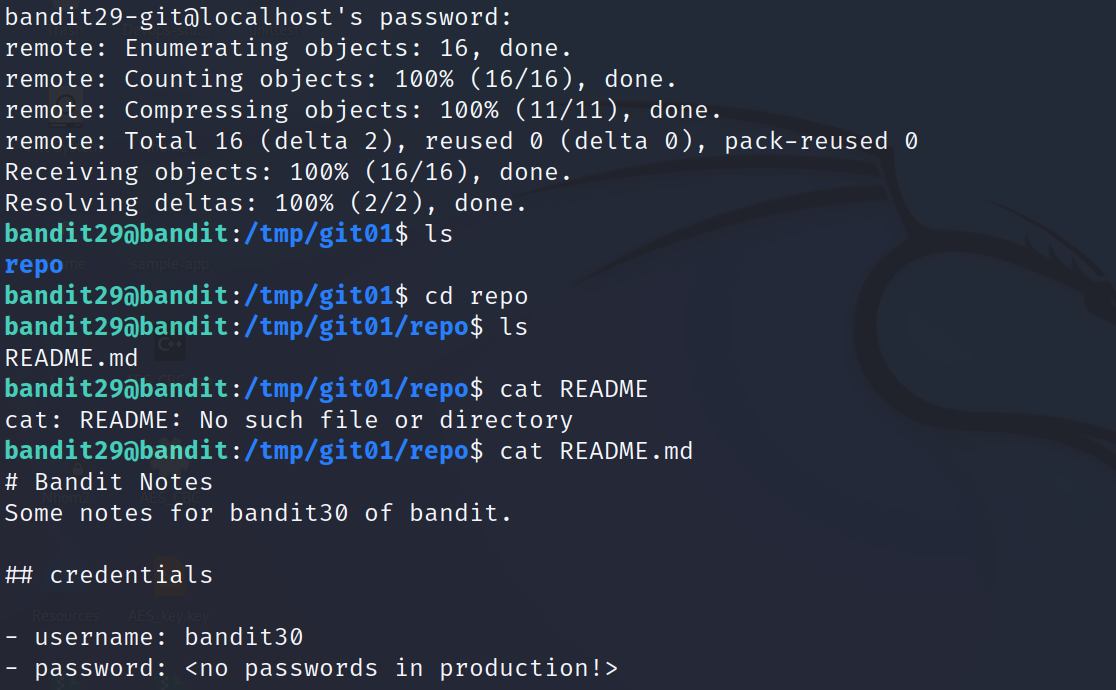
Ta thấy đã có sự chỉnh sửa gì đó thử so sánh 2 cái commit gần nhất nào



Tìm được password của level tiếp theo.

**Level 29 - 30**

Vẫn tải repo về và xem nó



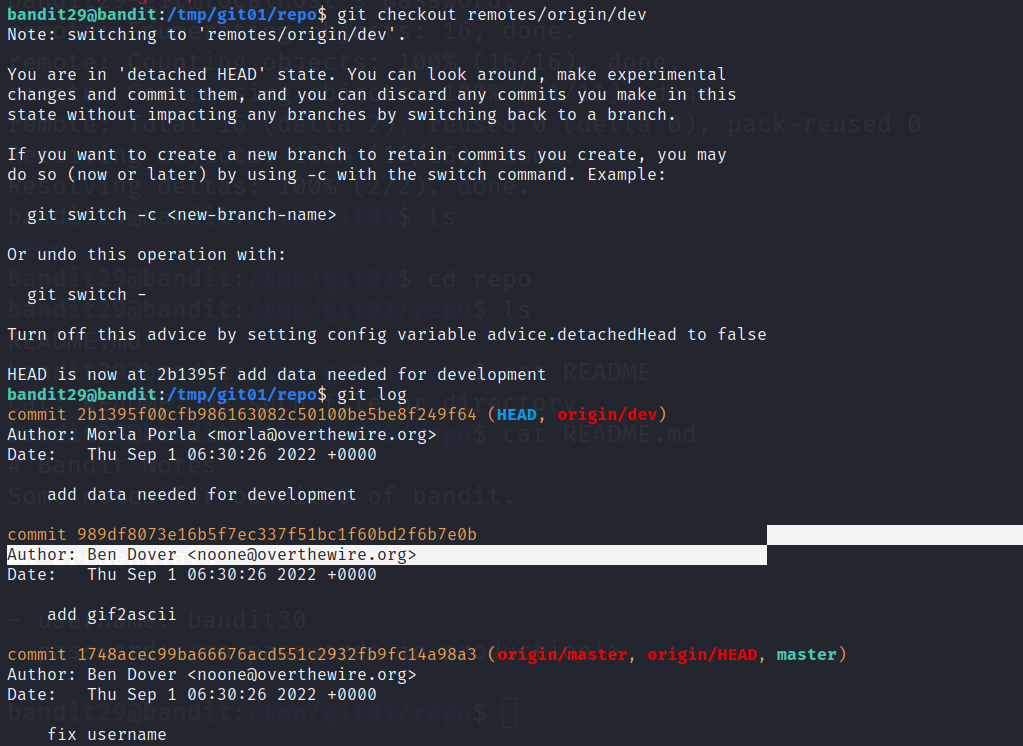
Không thấy gì ở password thử xem git log



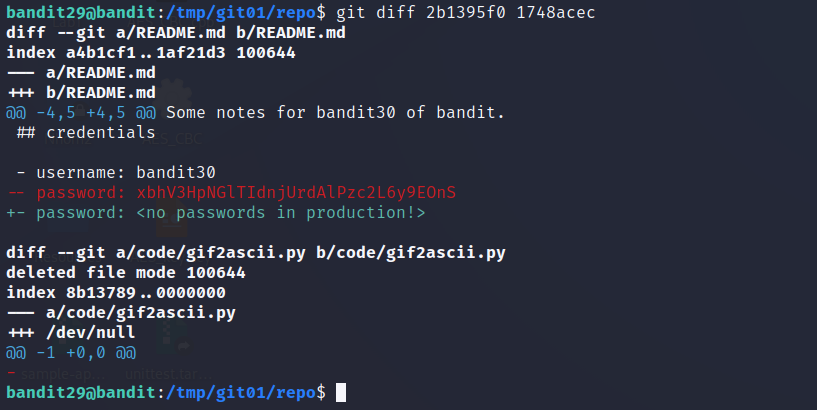
Git log cũng chả có gì liên quan, tuy nhiên nên nhớ chúng ta chỉ đang làm việc trên nhánh master, thử tìm kiếm các nhánh khác



Khá là nhiều branch khác, thử checkout đến từng branch và xem git log



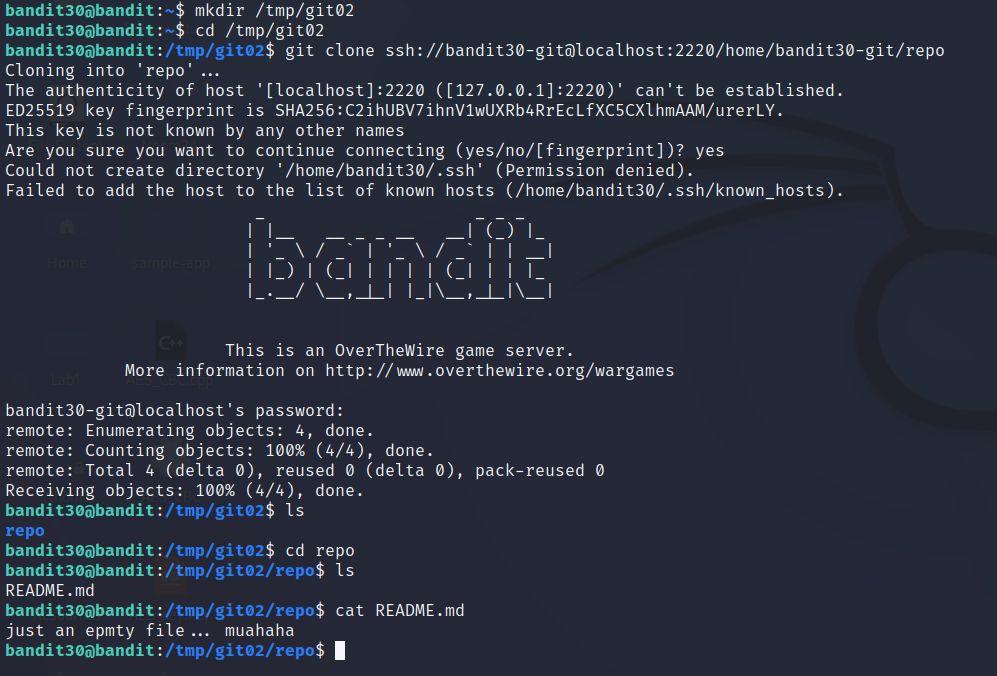
Ở branch đầu tiên ta thấy khá nhiều commit thử diff 2 commit gần nhất xem



Thử đoạn pass vừa xuất hiện, thành công.

**Level 30 - 31**

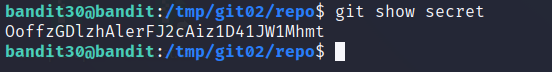
Vẫn tiếp tục là tải repo về và xem nó



Hmm, có lẽ đây chỉ là 1 file rỗng, thử kiểm tra các branch khác nhưng không thấy gì. Sau khi tìm hiểu, git còn 1 thứ gọi là tag thử sử dụng nó xem có gì không.



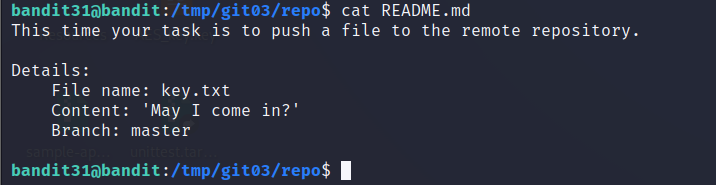
Xuất hiện thêm một tag là secret, thử show nó xem



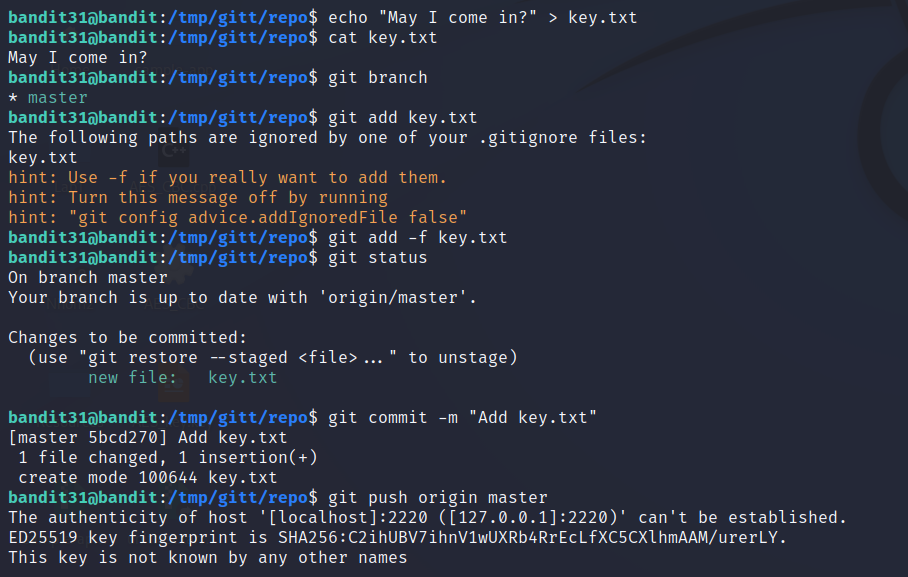
Ta đã có được pass của level tiếp theo

**Level 31 - 32**

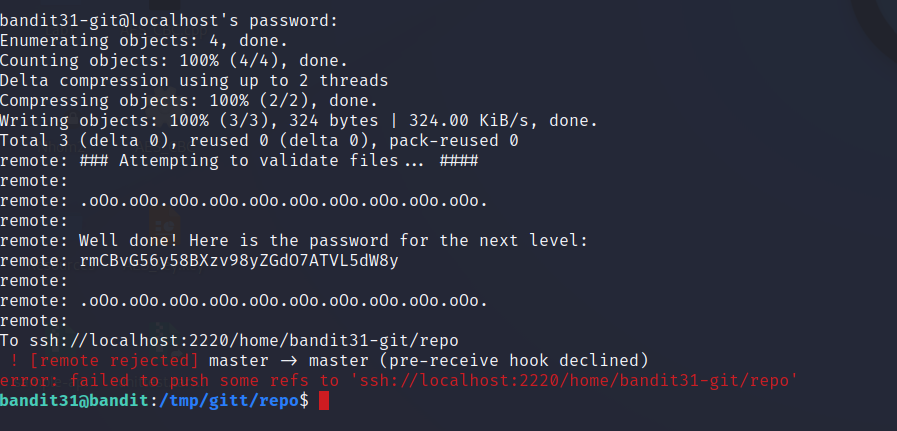
Vẫn tiếp tục làm các bước như các level trên, ta thấy file txt có nội dung như sau



Thử làm các yêu cầu này xem

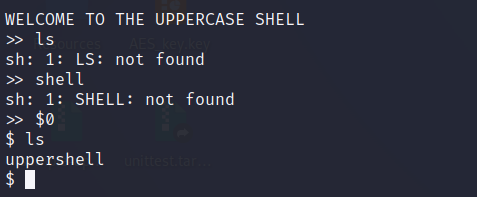


Do .gitignore sẽ chặn add các file .txt lên nên ta sẽ -f để ép add key.txt. Kết quả sau khi push ta thu được password của level tiếp theo

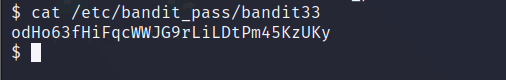


**Level 32 - 33**

Ở level này mọi câu lệnh chúng ta nhập vào sẽ tự động viết hoa. Sau khi tìm hiểu thì chỉ có lệnh $0 sẽ không thể chuyển đổi được chúng ta thử xem.



Chúng ta đã thoát khỏi chế dộ uppercase trở về với chế độ thường dùng, sau đó xem thử pass của level tiếp theo trong /etc/bandit\_pass nào



Dễ dàng tìm được key của level tiếp theo

**Level 33 - 34**

