**bandit0**

ssh bandit0@bandit.labs.overthewire.org -p 2220

**bandit1: NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL**

**bandit2**

Muốn lấy được mật khẩu của bandit2, chúng ta phải giải được bandit1.

dashed-filename: bắt đầu với - là những tên tệp bị ẩn trong Linux vì chúng không được hiển thị bình thường khi dùng lệnh ls. Vì dash ở đầu tên tệp được thông dịch là 1 lựa chọn của shell.

Cách đọc dash file:

cat < -samplefile

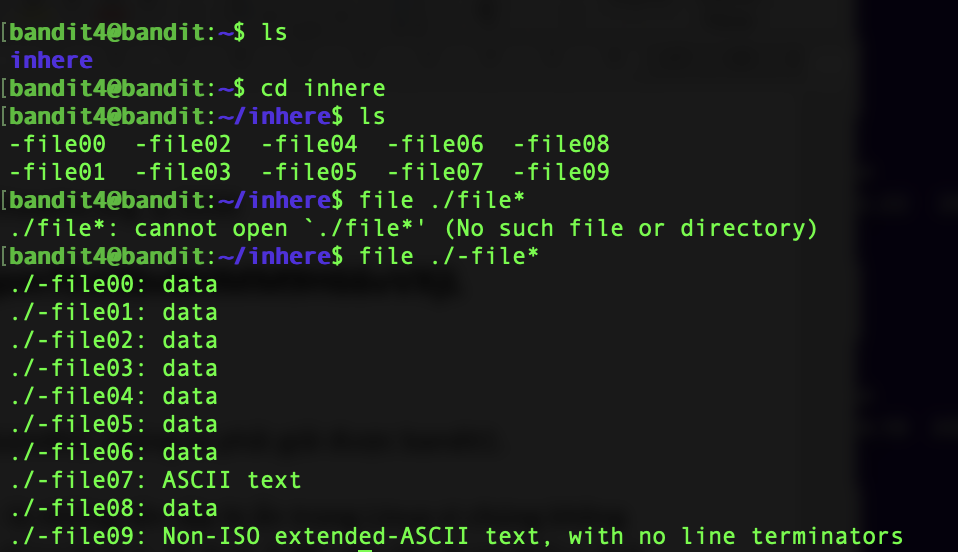
**bandit2: rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi**

**bandit3: aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG**

**bandit4: 2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe**

**bandit5:**

Cách kiểm tra file có định dạng human-readable:

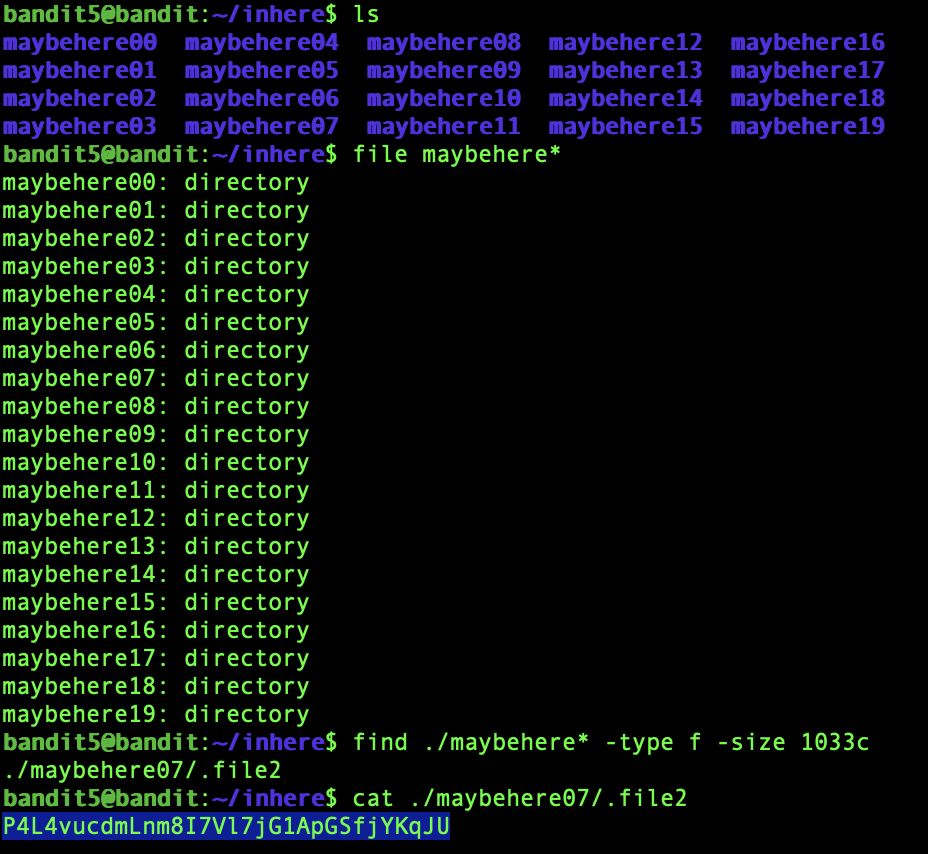


**bandit5: lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR**

**bandit6**

Tìm file trong thư mục inhere và có những thuộc tính sau:

* human-readable
* 1033 bytes in size
* not executable

****

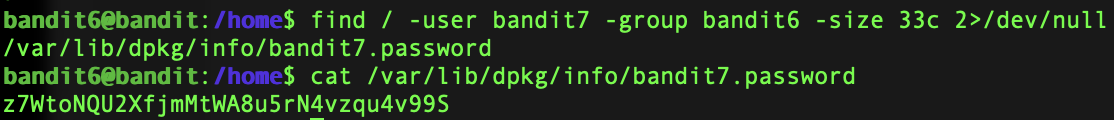
find ./ -type f -size 1033c ! -executable

**bandit6: P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU**

**bandit7**

Tìm file trong máy chủ có những thuộc tính sau:

* Làm chủ bởi user bandit7
* Làm chủ bởi group bandit6
* Kích thước 33 bytes



**bandit7: z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S**

**bandit8**

Mật khẩu cho cấp độ tiếp theo được lưu trong tệp data.txt kế bên từ millionth

cat data.txt | grep millionth

**bandit8: TESKZC0XvTetK0S9xNwm25STk5iWrBvP**

**bandit9**

Mật khẩu cho cấp độ kế tiếp được lưu ở tệp data.txt và là dòng chữ duy nhất chỉ xuất hiện 1 lần



uniq mặc định nó sẽ hiện ra những dòng bị lặp lại và không lặp lại

Lệnh uniq phải kết hợp với sort mới hoạt động tốt

* uniq -u: hiển thị những dòng không lặp lại
* uniq -c: hiển thị số lần dòng đó lặp lại

**bandit9: EN632PlfYiZbn3PhVK3XOGSlNInNE00t**

**bandit10**

Mật khẩu ở cấp độ tiếp theo được lưu ở tệp data.txt ở 1 trong các chuỗi mà con người có thể đọc được, trước có một số kí tự “=”

strings data.txt

**bandit10: G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s**

**bandit11**

Mật khẩu ở cấp độ tiếp theo được lưu ở tệp data.txt, được mã hóa base64

base64 -d data.txt

The password is 6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM

**bandit11: 6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM**

**bandit12**

Mật khẩu ở cấp độ tiếp theo được lưu ở tệp data.txt, tất cả chữ thường (a-z) và chữ hoa (A-Z) đã được xoay 13 vị trí.

Gợi ý: Rot13

Cách giải mã rot13:

cat data.txt | tr 'N-ZA-Mn-za-m' 'A-Za-z'

**bandit12: JVNBBFSmZwKKOP0XbFXOoW8chDz5yVRv**

**bandit13**

Mật khẩu cho cấp độ tiếp theo được lưu trong tệp data.txt, là 1 file hexdump đã được nén nhiều lần.

**Hex dump là gì?**

Có 1 chương trình hello world viết bằng ngôn ngữ C:

#include<stdio.h>

int main(){

printf(“hello World”);

}

Sau khi biên dịch bằng gcc nó sẽ thành 1 file nhị phân ELF. Ta sẽ dùng hexdump để xem các giá trị hexa trong file.

Hexa dump thường được dùng để debug 1 phần mềm.

Đầu tiên nó cho mình 1 file hexdump ở thư mục /home/bandit12. Mình chỉ có quyền đọc nên phải đưa nó đến thư mục /tmp:

cd /tmp

mkdir sec (tạo 1 thư mục sec ở /tmp)

cp /home/bandit12/data.txt ./

Mình dùng lệnh xxd để reverse hex dump thành 1 file nhị phân.

xxd -r data.txt > data

Mình kiểm tra thì thấy data là file gzip

file data

Muốn giải nén được data thì phải thêm cho file data một suffix .gz

mv data data.gz

gzip -d data.gz

Mình kiểm tra tiếp thì thấy data là file bzip2

Thêm suffix .bz

mv data data.bz

bzip2 -d data.bz

Mình kiểm tra tiếp thì thấy data là file tar

Thêm suffix .tar

mv data data.tar

tar -xf data.tar

Làm tương tự cho đến khi kiểu file là Ascii.

**bandit13: wbWdlBxEir4CaE8LaPhauuOo6pwRmrDw**

**bandit14**

Ta đang ở bandit13.

Mật khẩu cho cấp độ tiếp theo được lưu trong /etc/bandit\_pass/bandit14 và chỉ có thể đọc được bởi bandit14. Với level này bạn không có mật khẩu kế tiếp nhưng bạn có 1 private ssh key có thể được dùng để đăng nhập cấp độ tiếp theo.

Để ssh đến máy chủ từ xa bằng private key:

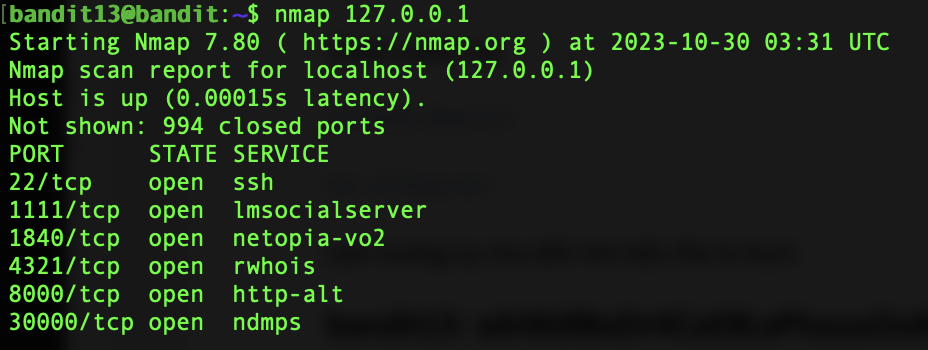
ssh -i sshkey.private bandit14@bandit.labs.overthewire.org -p 2220

**bandit14: fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq**

**bandit15**

Mật khẩu cho cấp độ tiếp theo có thể được lấy bằng cách gửi mật khẩu của level hiện tại đến cổng 30000 trên localhost

Quét xem localhost đang chạy những dịch vụ gì:

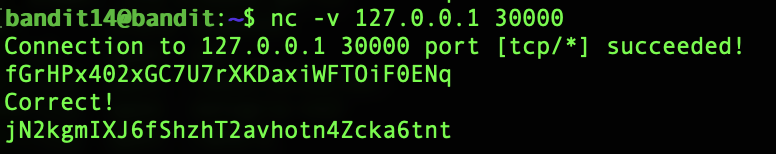


Dịch vụ ndmps đang chạy ở cổng 30000 (network data management protocol)

Tiếp theo chúng ta cần gửi mật khẩu của bandit14 đến localhost ở cổng 30000.

nc hay netcat là 1 lệnh cho phép đọc và ghi dữ liệu qua kết nối mạng. Nó có thể được dùng cho các kết nối TCP hoặc UDP.

* Để kết nối đến 1 dịch vụ trên mạng, cú pháp của lệnh là nc <host> <port>
* Để tạo 1 máy chủ lắng nghe những gói tin đang đến, cú pháp của lệnh là nc -l <port>



**bandit15: jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt**

**bandit16**

Mật khẩu cho cấp độ tiếp theo có thể được truy suất bằng cách gửi mật khẩu của level hiện tại đến cổng 30001 trên localhost bằng ssl encryption.

**Tìm hiểu về openssl**

Openssl là 1 thư viện các thuật toán về mã hóa (kể cả thuật toán cổ điển) , nó giúp bạn tạo được các cipher text.

echo -n 'secret' | openssl dgst -sha256

Tại sao phải echo -n?

echo 'secret' mặc định sẽ thêm newline vào sau chuỗi secret, secret\n. Khi bạn thêm flag -n, thì chỉ có secret

openssl s\_client là 1 thực thi của máy khách kết nối đến máy chủ bằng SSL/TLS.

Vì mật khẩu có thể được truy suất bằng ssl encryption, tôi kết nối đến localhost ở cổng 30001 với OpenSSL client và gửi mật khẩu của level này. Máy chủ sẽ gửi mật khẩu của cấp độ kế tiếp

openssl s\_client -connect localhost:30001

…

jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt

Correct!

JQttfApK4SeyHwDlI9SXGR50qclOAil1

**bandit16: JQttfApK4SeyHwDlI9SXGR50qclOAil1**

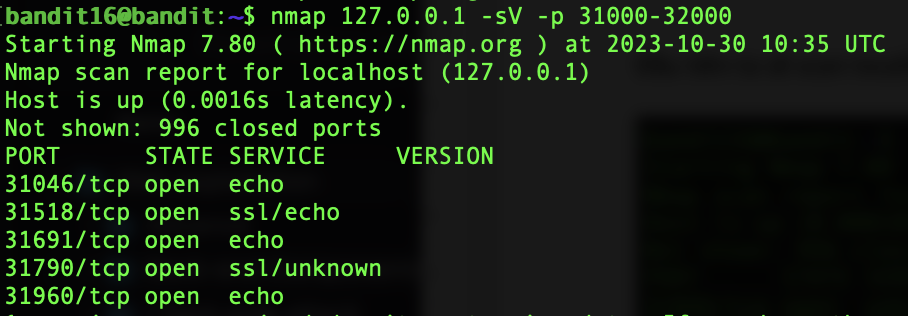
**bandit17**

Thông tin đăng nhập cho cấp độ tiếp theo có thể được truy suất bằng cách gửi mật khẩu của level hiện tại đến 1 cổng trên localhost trong phạm vi 31000 đến 32000. Đầu tiên hãy tìm ra những port máy chủ đang lắng nghe. Sau đó tìm ra những port nói SSL và những port không. Chỉ có 1 máy chủ sẽ đưa mật khẩu, những ports khác chỉ gửi lại cho bạn những gì bạn gửi cho nó

Đầu tiên ta sẽ scan localhost ở port trong phạm vi 31000 đến 32000:



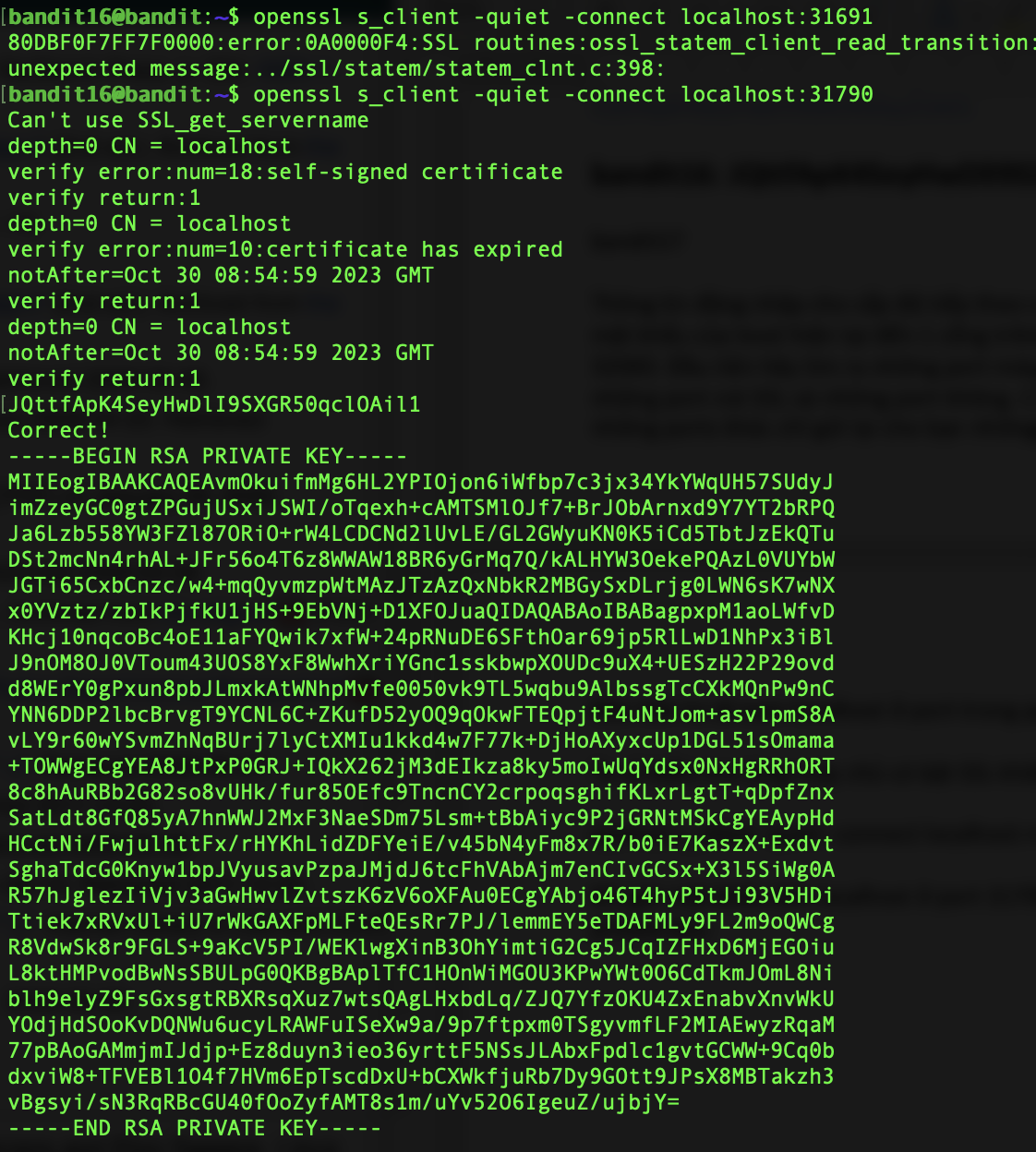
Nếu bạn muốn biết cổng đó đang chạy dịch vụ nào:



Như vậy, ta chỉ cần kiểm tra 2 port là 31518 và 31790:

openssl s\_client -quiet -connect localhost:<port>

Khi gửi mật khẩu đến localhost ở port 31790, nó báo Correct! và cho mình 1 private key:



Chúng ta cần lưu key trong 1 file có thể được dùng để ssh đến máy chủ ở level tiếp theo. Nhưng ta không có quyền ghi trong thư mục hiện tại nên sẽ lưu nó ở tmp.

mkdir /tmp/secret

cd /tmp/secret

vim private.key (sao chép private key bỏ vào file này)

Kết nối đến máy chủ bandit17 bằng private key:

ssh -i private.key bandit17@bandit.labs.overthewire.org -p 2220

Nó báo lỗi:

Permissions 0664 for 'private.key' are too open.

It is required that your private key files are NOT accessible by others.

This private key will be ignored.

Load key "private.key": bad permissions

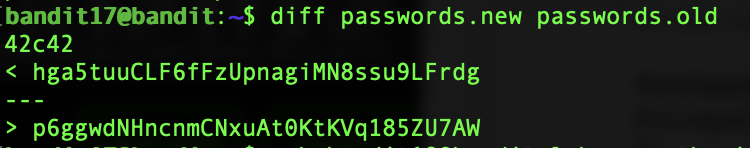
Mình mới nhớ ra permission của private key là 0600/-rw------ (không ai có thể truy cập file này trừ người dùng)

chmod 600 private.key

Kết nối lại lần nữa 🡪 Thành công

**bandit18**

Có 2 files trong thư mục home: passwords.old và passwords.new. Mật khẩu của level tiếp theo ở trong passwords.new và là dòng duy nhất khác nhau được thay đổi giữa passwords.old và passwords.new



Lưu ý: nếu bạn giải được level này và thấy “Byebye!’ khi cố gắng đăng nhập bandit18, điều này sẽ liên quan đến level tiếp theo, bandit19.

**bandit18: hga5tuuCLF6fFzUpnagiMN8ssu9LFrdg**

**bandit19**

Mật khẩu cho cấp độ tiếp theo được lưu trong file readme. Không may mắn, một người đã điều chỉnh .bashrc để ngăn chặn bạn đăng nhập SSH.

Shell mặc định của Linux là bash. Khi bạn đăng nhập bandit18, sẽ thấy “Byebye!”

Cách làm:

ssh -t bandit18@bandit.labs.overthewire.org -p 2220 /bin/sh

Flag -t: cho phép bạn thực thi chương trình trên máy từ xa, có thể rất hữu ích. Không cần phiên tty.

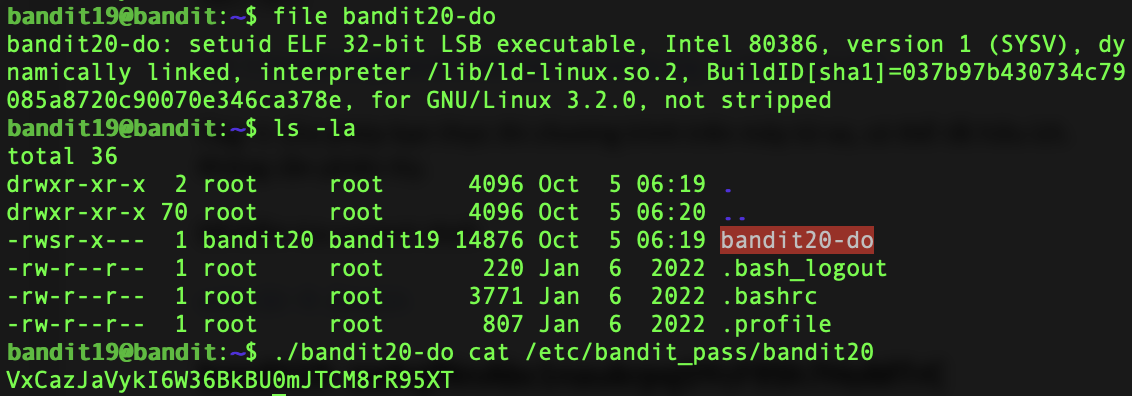
Để kiểm tra current shell:

echo $0 🡪 /bin/sh

**bandit19: awhqfNnAbc1naukrpqDYcF95h7HoMTrC**

**bandit20**

Bạn nên dùng file nhị phân setuid trong thư mục home. Mật khẩu của level tiếp theo có thể được tìm thấy trong /etc/bandit\_pass.



./bandit20-do cat /etc/bandit\_pass/bandit20

**bandit20: VxCazJaVykI6W36BkBU0mJTCM8rR95XT**

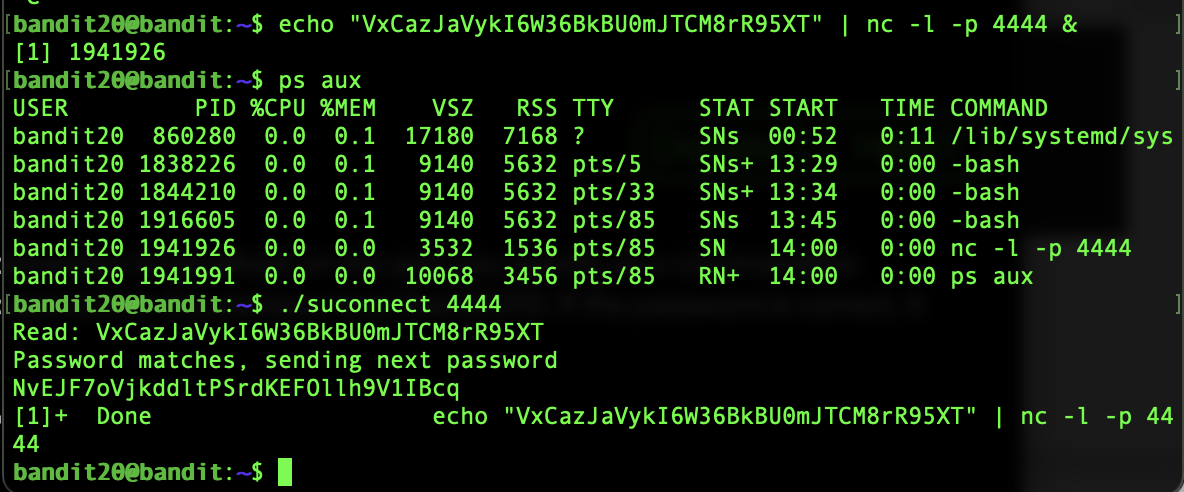
**bandit21**

Có 1 file nhị phân setuid trong thư mục home: nó tạo kết nối đến localhost trên port bạn chỉ định làm đối số dòng lệnh. Sau đó nó đọc 1 dòng dữ liệu từ kết nối và so sánh nó với mật khẩu của bandit20. Nếu mật khẩu đúng, nó sẽ chuyển cho bạn mật khẩu của bandit21

Lưu ý: cố gắng kết nối đến mạng daemon của bạn để xem

Đầu tiên, chúng ta lắng nghe kết nối ở cổng 4444 và để quá trình này chạy ở background

Tiếp theo, thực thi file nhị phân suconnect để kết nối đến localhost:



**bandit21: NvEJF7oVjkddltPSrdKEFOllh9V1Ibcq**