***Bandit – OverTheWire***

***Write-ups***

|  |  |  |
| --- | --- | --- |
| **Đề bài** | ***Tên*** | Bandit 1 |
| ***Loại*** | Command Linux |
| ***Lưu trữ*** |  |
| ***Cụ thể*** | The password for the next level is stored in a file called readme located in the home directory |
| **Quan sát đề bài** | |  |
| **Ý tưởng ban đầu** | | Kiếm tra thư mục và file ở máy chủ |
| **Công cụ thực hiện** | | Máy ảo chạy để điều hành Linux. Cụ thể ở đây mình sài Windows Subsystem for Linux (WSL 2) |
| **Giải** | ***Step 1*** | Kết nối đến máy chủ thông qua SSH    Pass: bandit0 |
| ***Step 2*** | Kiểm tra thư mục và file ở máy chủ bằng lệnh ls |
| ***Step 3*** | Đọc file readme bằng lệnh cat |
| ***Step 4*** |  |
| ***Step 5*** |  |
| ***Step 6*** |  |
| ***Step 7*** |  |
| ***Step 8*** |  |
| ***Step 9*** |  |
| **Flag** | |  |
| **Note** | | boJ9jbbUNNfktd78OOpsqOltutMc3MY1 |
| **Thực hiện** | | Đậu Hoàng Tài |

|  |  |  |
| --- | --- | --- |
| **Đề bài** | ***Tên*** | Bandit 2 |
| ***Loại*** | Command Linux |
| ***Lưu trữ*** |  |
| ***Cụ thể*** | The password for the next level is stored in a file called - located in the home directory |
| **Quan sát đề bài** | |  |
| **Ý tưởng ban đầu** | | Kiếm tra trong máy chủ có file – hay không |
| **Công cụ thực hiện** | | Máy ảo chạy để điều hành Linux. Cụ thể ở đây mình sài Windows Subsystem for Linux (WSL 2) |
| **Giải** | ***Step 1*** | Kết nối đến máy chủ của bandit 1 |
| ***Step 2*** | Kiểm tra thư mục và file ở máy chủ bằng lệnh ls |
| ***Step 3*** | Đọc file – bằng lệnh cat |
| ***Step 4*** |  |
| ***Step 5*** |  |
| ***Step 6*** |  |
| ***Step 7*** |  |
| ***Step 8*** |  |
| ***Step 9*** |  |
| **Flag** | | CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9 |
| **Note** | |  |
| **Thực hiện** | | Đậu Hoàng Tài |

|  |  |  |
| --- | --- | --- |
| **Đề bài** | ***Tên*** | Bandit 3 |
| ***Loại*** | Command Linux |
| ***Lưu trữ*** |  |
| ***Cụ thể*** | The password for the next level is stored in a file called spaces in this filename located in the home directory |
| **Quan sát đề bài** | |  |
| **Ý tưởng ban đầu** | | Kiếm tra file và thư mục trong máy chủ. Cụ thể là file spaces in this filename |
| **Công cụ thực hiện** | | Máy ảo chạy để điều hành Linux. Cụ thể ở đây mình sài Windows Subsystem for Linux (WSL 2) |
| **Giải** | ***Step 1*** | Kết nối đến máy chủ bandit2 qua giao thức SSH |
| ***Step 2*** | Kiểm tra file và thư mục ở máy chủ |
| ***Step 3*** | Đọc file bằng lệnh cat  Thêm dấu “\” trước mỗi dấu cách |
| ***Step 4*** |  |
| ***Step 5*** |  |
| ***Step 6*** |  |
| ***Step 7*** |  |
| ***Step 8*** |  |
| ***Step 9*** |  |
| **Flag** | | UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK |
| **Note** | |  |
| **Thực hiện** | | Đậu Hoàng Tài |

|  |  |  |
| --- | --- | --- |
| **Đề bài** | ***Tên*** | Bandit 4 |
| ***Loại*** | Command Linux |
| ***Lưu trữ*** |  |
| ***Cụ thể*** | The password for the next level is stored in a hidden file in the inhere directory. |
| **Quan sát đề bài** | |  |
| **Ý tưởng ban đầu** | | Kiểm tra các file bị ẩn |
| **Công cụ thực hiện** | | Máy ảo chạy để điều hành Linux. Cụ thể ở đây mình sài Windows Subsystem for Linux (WSL 2) |
| **Giải** | ***Step 1*** | Kết nối đến máy chủ bandit3 |
| ***Step 2*** | Kiểm tra file và thư mục ở máy chủ |
| ***Step 3*** | Di chuyển tới thư mục inhere bằng lệnh cd |
| ***Step 4*** | Kiểm tra file và thư mục có ở hiện tại bằng lệnh ls –la để xem quyền và các file ẩn |
| ***Step 5*** | Đọc file .hidden bằng lệnh cat |
| ***Step 6*** |  |
| ***Step 7*** |  |
| ***Step 8*** |  |
| ***Step 9*** |  |
| **Flag** | | pIwrPrtPN36QITSp3EQaw936yaFoFgAB |
| **Note** | |  |
| **Thực hiện** | | Đậu Hoàng Tài |

|  |  |  |
| --- | --- | --- |
| **Đề bài** | ***Tên*** | Bandit 5 |
| ***Loại*** | Command Linux |
| ***Lưu trữ*** |  |
| ***Cụ thể*** | The password for the next level is stored in the only human-readable file in the inhere directory |
| **Quan sát đề bài** | |  |
| **Ý tưởng ban đầu** | | Đọc những kí tự có thể đọc được trong bảng mã ASCII |
| **Công cụ thực hiện** | | Máy ảo chạy để điều hành Linux. Cụ thể ở đây mình sài Windows Subsystem for Linux (WSL 2) |
| **Giải** | ***Step 1*** | Kết nối đến máy chủ bandit4 bằng giao thức SSH |
| ***Step 2*** | Kiểm tra file và thự mục có trong máy chủ bằng lệnh ls |
| ***Step 3*** | Di chuyển đến file inhere bằng lệnh cd |
| ***Step 4*** | Kiểm tra quyền của file và thư mục ở inhere |
| ***Step 5*** | Đọc toàn bộ file có trong thư mục inhere bằng lệnh cat |
| ***Step 6*** |  |
| ***Step 7*** |  |
| ***Step 8*** |  |
| ***Step 9*** |  |
| **Flag** | | koReBOKuIDDepwhWk7jZC0RTdopnAYKh |
| **Note** | |  |
| **Thực hiện** | | Đậu Hoàng Tài |

|  |  |  |
| --- | --- | --- |
| **Đề bài** | ***Tên*** | Bandit 6 |
| ***Loại*** | Command Linux |
| ***Lưu trữ*** |  |
| ***Cụ thể*** | The password for the next level is stored in a file somewhere under the inhere directory and has all of the following properties:human-readable,1033 bytes in size,not executable |
| **Quan sát đề bài** | |  |
| **Ý tưởng ban đầu** | | Dùng lệnh find đề tìm kiếm file và thư mục đúng theo tiêu chuẩn của đề |
| **Công cụ thực hiện** | | Máy ảo chạy để điều hành Linux. Cụ thể ở đây mình sài Windows Subsystem for Linux (WSL 2) |
| **Giải** | ***Step 1*** | Kết nối đến máy chủ bandit5 qua giao thưc SHH |
| ***Step 2*** | Kiểm tra file và thư mục hiện tại và di chuyển đến thư mục đó |
| ***Step 3*** | Kiểm tra file và thư mục có ở inhere |
| ***Step 4*** | Theo đề ta sử dụng lệnh file để tìm kiếm file có tiêu chuẩn human-readable,1033 bytes in size,not executable. |
| ***Step 5*** | Đọc .file2 |
| ***Step 6*** |  |
| ***Step 7*** |  |
| ***Step 8*** |  |
| ***Step 9*** |  |
| **Flag** | | DXjZPULLxYr17uwoI01bNLQbtFemEgo7 |
| **Note** | |  |
| **Thực hiện** | | Đậu Hoàng Tài |

|  |  |  |
| --- | --- | --- |
| **Đề bài** | ***Tên*** | Bandit 7 |
| ***Loại*** | Command Linux |
| ***Lưu trữ*** |  |
| ***Cụ thể*** | The password for the next level is stored somewhere on the server and has all of the following properties:owned by user bandit7,owned by group bandit6  33 bytes in size |
| **Quan sát đề bài** | |  |
| **Ý tưởng ban đầu** | | Tìm kiếm file theo tiêu chuẩn của đề bằng lệnh find |
| **Công cụ thực hiện** | | Máy ảo chạy để điều hành Linux. Cụ thể ở đây mình sài Windows Subsystem for Linux (WSL 2) |
| **Giải** | ***Step 1*** | Kết nối tới máy chủ bandit6 qua giao thức SSH |
| ***Step 2*** | Kiểm tra file và thư mục ở máy chủ thì thấy không có file chứa password |
| ***Step 3*** | Ta tìm kiếm file theo đúng theo tiêu chuẩn của đề cho bằng lệnh find nhưng sẽ khác thử thách trước là phải tìm kiếm các tiêu chuẩn đó phù hợp ở trên toàn bộ thư mục của máy chủ    Kết trả về sẽ rất nhiều và ta lướt tìm bandit7 chứa password |
| ***Step 4*** | Đọc file bandit7.password |
| ***Step 5*** |  |
| ***Step 6*** |  |
| ***Step 7*** |  |
| ***Step 8*** |  |
| ***Step 9*** |  |
| **Flag** | | HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs |
| **Note** | |  |
| **Thực hiện** | | Đậu Hoàng Tài |

|  |  |  |
| --- | --- | --- |
| **Đề bài** | ***Tên*** | Bandit 8 |
| ***Loại*** | Command Linux |
| ***Lưu trữ*** |  |
| ***Cụ thể*** | The password for the next level is stored in the file data.txt next to the word millionth |
| **Quan sát đề bài** | |  |
| **Ý tưởng ban đầu** | | Tìm kiếm file data.txt và đọc nó |
| **Công cụ thực hiện** | | Máy ảo chạy để điều hành Linux. Cụ thể ở đây mình sài Windows Subsystem for Linux (WSL 2) |
| **Giải** | ***Step 1*** | Kết nối máy chủ bandit7 qua giao thức SSH |
| ***Step 2*** | Kiểm tra file và thư mục có ở máy chủ |
| ***Step 3*** | Đọc file data.txt với lọc từ khóa là millionth bằng lệnh cat và grep |
| ***Step 4*** |  |
| ***Step 5*** |  |
| ***Step 6*** |  |
| ***Step 7*** |  |
| ***Step 8*** |  |
| ***Step 9*** |  |
| **Flag** | | cvX2JJa4CFALtqS87jk27qwqGhBM9plV |
| **Note** | |  |
| **Thực hiện** | | Đậu Hoàng Tài |

|  |  |  |
| --- | --- | --- |
| **Đề bài** | ***Tên*** | Bandit 9 |
| ***Loại*** | Command Linux |
| ***Lưu trữ*** |  |
| ***Cụ thể*** | The password for the next level is stored in the file data.txt and is the only line of text that occurs only once |
| **Quan sát đề bài** | |  |
| **Ý tưởng ban đầu** | | Đọc file data.txt và kiếm dòng text chỉ xuất hiện 1 lần trong file |
| **Công cụ thực hiện** | | Máy ảo chạy để điều hành Linux. Cụ thể ở đây mình sài Windows Subsystem for Linux (WSL 2) |
| **Giải** | ***Step 1*** | Kết nối đến máy chủ bandit8 qua giao thức SSH |
| ***Step 2*** | Kiểm tra file và thư mục có trong máy chủ |
| ***Step 3*** | Đọc file data.txt và tìm kiếm dòng text chỉ xuất hiện một lần bằng lệnh cat và uniq và loại bỏ các bản sao trùng lặp bằng sort |
| ***Step 4*** |  |
| ***Step 5*** |  |
| ***Step 6*** |  |
| ***Step 7*** |  |
| ***Step 8*** |  |
| ***Step 9*** |  |
| **Flag** | | UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR |
| **Note** | |  |
| **Thực hiện** | | Đậu Hoàng Tài |

|  |  |  |
| --- | --- | --- |
| **Đề bài** | ***Tên*** | Bandit 10 |
| ***Loại*** | Command Linux |
| ***Lưu trữ*** |  |
| ***Cụ thể*** | The password for the next level is stored in the file data.txt in one of the few human-readable strings, preceded by several ‘=’ characters. |
| **Quan sát đề bài** | |  |
| **Ý tưởng ban đầu** | | Đọc file data.txt và lọc theo từ khóa “=” |
| **Công cụ thực hiện** | | Máy ảo chạy để điều hành Linux. Cụ thể ở đây mình sài Windows Subsystem for Linux (WSL 2) |
| **Giải** | ***Step 1*** | Kết nối đến máy chủ bandit9 qua giao thức SSH |
| ***Step 2*** | Kiểm tra file và thư mục có trong máy chủ |
| ***Step 3*** | Vì file data.txt này được lưu dưới dạng file nhị phân nên chúng ta không thể đọc file như thông thường bằng lệnh cat |
| ***Step 4*** | Đọc file data.txt bằng lệnh strings và lọc theo từ khóa “=” |
| ***Step 5*** |  |
| ***Step 6*** |  |
| ***Step 7*** |  |
| ***Step 8*** |  |
| ***Step 9*** |  |
| **Flag** | | truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk |
| **Note** | |  |
| **Thực hiện** | | Đậu Hoàng Tài |

|  |  |  |
| --- | --- | --- |
| **Đề bài** | ***Tên*** | Bandit 11 |
| ***Loại*** | Command Linux |
| ***Lưu trữ*** |  |
| ***Cụ thể*** | The password for the next level is stored in the file data.txt, which contains base64 encoded data |
| **Quan sát đề bài** | |  |
| **Ý tưởng ban đầu** | | Đọc file data.txt và giải mã base64 nội dung file đó |
| **Công cụ thực hiện** | | Máy ảo chạy để điều hành Linux. Cụ thể ở đây mình sài Windows Subsystem for Linux (WSL 2) |
| **Giải** | ***Step 1*** | Kết nối đến máy chủ bandit10 qua giao thức SSH |
| ***Step 2*** | Kiểm tra các file và thư mục có trong máy chủ |
| ***Step 3*** | Đọc file data.txt bằng lệnh cat |
| ***Step 4*** | Chúng ta thấy nội dung của file bị encode bởi base64. Dấu hiệu nhận biết sẽ là có “==” ở cuối chuỗi. Vì vậy chúng ta phải decode chuỗi đó bằng lệnh base64 –d hoặc sử dụng các trang web decode online |
| ***Step 5*** |  |
| ***Step 6*** |  |
| ***Step 7*** |  |
| ***Step 8*** |  |
| ***Step 9*** |  |
| **Flag** | | IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR |
| **Note** | |  |
| **Thực hiện** | | Đậu Hoàng Tài |

|  |  |  |
| --- | --- | --- |
| **Đề bài** | ***Tên*** | Bandit 12 |
| ***Loại*** | Command Linux |
| ***Lưu trữ*** |  |
| ***Cụ thể*** | The password for the next level is stored in the file data.txt, where all lowercase (a-z) and uppercase (A-Z) letters have been rotated by 13 positions |
| **Quan sát đề bài** | |  |
| **Ý tưởng ban đầu** | | Đề bài có nhắc đến dữ liệu đã được xoay 13 vị trí nên mình nghĩ đến có thể là đọc dữ liệu và sử dụng ROT13 để decode |
| **Công cụ thực hiện** | | Máy ảo chạy để điều hành Linux. Cụ thể ở đây mình sài Windows Subsystem for Linux (WSL 2) |
| **Giải** | ***Step 1*** | Kết nối đến máy chủ bandit11 qua giao thức SSH |
| ***Step 2*** | Kiểm tra file và thư mục có ở máy chủ |
| ***Step 3*** | Đọc file text data.txt bằng lệnh cat |
| ***Step 4*** | Ta thử decode theo Rot13 như ý tưởng ban đầu. Có thể sử dụng các trang web online về decode rot13 |
| ***Step 5*** |  |
| ***Step 6*** |  |
| ***Step 7*** |  |
| ***Step 8*** |  |
| ***Step 9*** |  |
| **Flag** | | 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu |
| **Note** | |  |
| **Thực hiện** | | Đậu Hoàng Tài |

|  |  |  |
| --- | --- | --- |
| **Đề bài** | ***Tên*** | Bandit 13 |
| ***Loại*** | Command Linux |
| ***Lưu trữ*** |  |
| ***Cụ thể*** | The password for the next level is stored in the file data.txt, which is a hexdump of a file that has been repeatedly compressed |
| **Quan sát đề bài** | |  |
| **Ý tưởng ban đầu** | | Như yêu cầu đề thì mình sẽ reverse hashdump |
| **Công cụ thực hiện** | | Máy ảo chạy để điều hành Linux. Cụ thể ở đây mình sài Windows Subsystem for Linux (WSL 2) |
| **Giải** | ***Step 1*** | Kết nối đến máy chủ bandit12 qua giao thức SSH |
| ***Step 2*** | Kiểm tra file và thư mục có trong máy chủ |
| ***Step 3*** | Mở file data.txt bằng lệnh cat |
| ***Step 4*** | Như chúng ta thấy ở bước 3 thì file data.txt chứa nội dùng có mã đã được hexdump vì vậy đọc lại đề bài thì thấy tác giả cho gợi ý “For this level it may be useful to create a directory under /tmp in which you can work using mkdir”  Vì vậy chúng ta làm theo gợi ý của tác giả là tạo ra 1 folder tên “bandit13” nằm trong /tmp bằng lệnh mkdir  Sau đó copy file data.txt vào thư mục mình vừa tạo bằng lệnh cp  Tiếp tục di chuyển đến thư mục “bandit13” mà mình đã tạo và kiểm tra file data.txt đã được copy đến chưa |
| ***Step 5*** | Ta convert file data.txt qua file .bin bằng lệnh xxd  Sau đó kiểm tra file đó có thuộc tính gì và chúng ta sẽ convert theo thuộc tính đó lúc nào nó trở thành file ASCII text thì dừng lại và đọc  Và như theo đề bài thì file đã bị nén nhiều lần vì vậy chúng sẽ sẽ nén nó vào 1 file zip và unzip nó nhiều lần |
| ***Step 6*** | Chúng ta thấy file data đã thành bzip2 vì vậy lại tiếp tục nén nó thành bzip2 |
| ***Step 7*** | Tiếp tục là file gzip    Kiểm tra file vừa unzip thì thấy là file tar |
| ***Step 8*** | Tiếp tục chuyển file data5.bin vô data5.tar và untar nó |
| ***Step 9*** | Tiếp tục những bước còn lại |
| **Flag** | | 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL |
| **Note** | |  |
| **Thực hiện** | | Đậu Hoàng Tài |

|  |  |  |
| --- | --- | --- |
| **Đề bài** | ***Tên*** | Bandit 14 |
| ***Loại*** | Command Linux |
| ***Lưu trữ*** |  |
| ***Cụ thể*** | The password for the next level is stored in /etc/bandit\_pass/bandit14 and can only be read by user bandit14. |
| **Quan sát đề bài** | |  |
| **Ý tưởng ban đầu** | | Kết nối đến máy chủ bandit14 dựa vào private key như gợi ý tác giả cho “you get a private SSH key that can be used to log into the next level.” |
| **Công cụ thực hiện** | | Máy ảo chạy để điều hành Linux. Cụ thể ở đây mình sài Windows Subsystem for Linux (WSL 2) |
| **Giải** | ***Step 1*** | Kết nối tới máy chủ bandit13 qua giao thức SSH |
| ***Step 2*** | Kiếm tra file và thư mục có ở máy chủ    Như gợi ý của tác giả thì bây giờ chúng ta đã thấy có file sshkey.private  Vậy bây giờ kết nối đến máy chủ bandit14 dựa vào file đó thôi |
| ***Step 3*** |  |
| ***Step 4*** | Đọc file flag theo đề cho ở “/etc/bandit\_pass/bandit14” |
| ***Step 5*** |  |
| ***Step 6*** |  |
| ***Step 7*** |  |
| ***Step 8*** |  |
| ***Step 9*** |  |
| **Flag** | | 4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e |
| **Note** | |  |
| **Thực hiện** | | Đậu Hoàng Tài |

|  |  |  |
| --- | --- | --- |
| **Đề bài** | ***Tên*** | Bandit 15 |
| ***Loại*** | Command Linux |
| ***Lưu trữ*** |  |
| ***Cụ thể*** | The password for the next level can be retrieved by submitting the password of the current level to port 30000 on localhost. |
| **Quan sát đề bài** | |  |
| **Ý tưởng ban đầu** | | Như đề bài cho sau khi kết đối được máy chủ bandit14 thì chúng ta sẽ necat đến host và post của tác giả cho. |
| **Công cụ thực hiện** | | Máy ảo chạy để điều hành Linux. Cụ thể ở đây mình sài Windows Subsystem for Linux (WSL 2) |
| **Giải** | ***Step 1*** | Kết nối đến máy chủ bandit14 qua giao thức SSH |
| ***Step 2*** | Kiểm tra file và thư mục có trong máy chủ  Như vậy không có file nào được tác giả cho ở đây vì vậy ta sẽ làm theo đề bài là kết nối đến host và port mà tác giả cho. |
| ***Step 3*** | Kết nối đến hort: localhost và port: 30000    Sau đó nhập pass của bandit14 chúng ta đã tìm được ở thử thách trên |
| ***Step 4*** |  |
| ***Step 5*** |  |
| ***Step 6*** |  |
| ***Step 7*** |  |
| ***Step 8*** |  |
| ***Step 9*** |  |
| **Flag** | | BfMYroe26WYalil77FoDi9qh59eK5xNr |
| **Note** | |  |
| **Thực hiện** | | Đậu Hoàng Tài |

|  |  |  |
| --- | --- | --- |
| **Đề bài** | ***Tên*** | Bandit 16 |
| ***Loại*** | Command Linux |
| ***Lưu trữ*** |  |
| ***Cụ thể*** | The password for the next level can be retrieved by submitting the password of the current level to port 30001 on localhost using SSL encryption |
| **Quan sát đề bài** | |  |
| **Ý tưởng ban đầu** | | Như đề bài cho là sử dụng SSL nên mình đã nghĩ đến sử dụng openssl để kết nối đến host và port như tác giả cho |
| **Công cụ thực hiện** | | Máy ảo chạy để điều hành Linux. Cụ thể ở đây mình sài Windows Subsystem for Linux (WSL 2) |
| **Giải** | ***Step 1*** | Kết nối đến máy chủ bandit15 qua giao thức SSH |
| ***Step 2*** | Kiểm tra file và thư mục có ở máy chủ |
| ***Step 3*** | Chúng ta thử sử dụng openssl như đã nêu ở ý tưởng ban đầu    Chúng ta kết nối tới được và nhập pass của bandit15 chúng ta đã giải quyết ở trên và kết quả nhận được pass của bandit16 |
| ***Step 4*** |  |
| ***Step 5*** |  |
| ***Step 6*** |  |
| ***Step 7*** |  |
| ***Step 8*** |  |
| ***Step 9*** |  |
| **Flag** | | cluFn7wTiGryunymYOu4RcffSxQluehd |
| **Note** | |  |
| **Thực hiện** | | Đậu Hoàng Tài |

|  |  |  |
| --- | --- | --- |
| **Đề bài** | ***Tên*** | Bandit 17 |
| ***Loại*** | Command Linux |
| ***Lưu trữ*** |  |
| ***Cụ thể*** | The credentials for the next level can be retrieved by submitting the password of the current level to a port on localhost in the range 31000 to 32000 |
| **Quan sát đề bài** | |  |
| **Ý tưởng ban đầu** | | Như đề bài cho thì có lẽ chúng ta sẽ phải quét cổng xem cổng nào đang mở và chứa pass của bandit17 ở đây mình sử dụng công cụ đó là nmap |
| **Công cụ thực hiện** | | Máy ảo chạy để điều hành Linux. Cụ thể ở đây mình sài Windows Subsystem for Linux (WSL 2) |
| **Giải** | ***Step 1*** | Kết nối đến máy chủ bandit16 qua giao thức SSH |
| ***Step 2*** | Kiểm tra file và thư mục có ở máy chủ  Không có file hay thư mục nào ở đây |
| ***Step 3*** | Tiếp theo chúng ta thử quét cổng bằng công cụ nmap như mình đã nêu ở ý tưởng ban đầu    Kết quả chỉ có 5 cổng cho phép dịch vụ |
| ***Step 4*** | Bây giờ chúng ta đi kiểm tra 5 cổng đó,cổng nào được cấu hình chấp nhận kết nối bình thường hay bị hạn chế kết nối SSL. Và chúng ta kiểm tra chúng bằng netcat |
| ***Step 5*** | Như chúng ta thấy ở bước 4 thì chỉ có 2 port là “31518” và “31790” là ghi mình nhập vào nó không in ra màn hình chuỗi mình nhập vào => đúng với yêu cầu của đề. Vì vậy bây giờ mình tập trung vào 2 port đó. Đầu tiên thử openssl tới port “31518”  Mình sử dụng echo để nó tự nhập chuỗi mình truyền vào khi nó gặp input của openssl để khỏi phải nhập tay  Kết quả thấy được port 31518 không in ra gì đặc biệt ngoài pass cũ của bandit16. Vậy nê ta tiếp tục với port còn lại là “31790”  Kết quả chúng ta nhận được một private key |
| ***Step 6*** | Sau khi nhận được private key nó khá giống với thử thách mình đã giải quyết trước đó nên chúng ta lưu vào một file và sử dụng ssh như trước.  Đầu tiên ta tạo một thư mục c ó tên savekey ở /tmp vì không thể tạo ở home hiện tại vì không có quyền |
| ***Step 7*** | Sử dụng trình soạn thảo nano hoặc vim để lưu RSA key ở trên vào file privatekey.private |
| ***Step 8*** | Kết nối ssh qua privatekey đó |
| ***Step 9*** | Đọc pass của bandit 17 ở /etc/bandit\_pass/bandit17 |
| **Flag** | | xLYVMN9WE5zQ5vHacb0sZEVqbrp7nBTn |
| **Note** | |  |
| **Thực hiện** | | Đậu Hoàng Tài |

|  |  |  |
| --- | --- | --- |
| **Đề bài** | ***Tên*** | Bandit 18 |
| ***Loại*** | Command Linux |
| ***Lưu trữ*** |  |
| ***Cụ thể*** | There are 2 files in the homedirectory: passwords.old and passwords.new. The password for the next level is in passwords.new and is the only line that has been changed between passwords.old and passwords.new |
| **Quan sát đề bài** | |  |
| **Ý tưởng ban đầu** | | So sánh nội dung của 2 file xem có những đoạn text nào khác nhau |
| **Công cụ thực hiện** | | Máy ảo chạy để điều hành Linux. Cụ thể ở đây mình sài Windows Subsystem for Linux (WSL 2) |
| **Giải** | ***Step 1*** | Kết nối đến máy chủ bandit17 qua giao thức SSH |
| ***Step 2*** | Kiểm tra file và thư mục có ở máy chủ |
| ***Step 3*** | So sánh nội dùng hai file xem có những đoạn text nào khác nhau bằng lệnh diff |
| ***Step 4*** | Chúng ta thấy có 2 đoạn text khác nhau ở trong 2 file nhưng không thể biết đoạn text nào mà mật khẩu cho thử thách tiếp theo vậy nên chúng ta đọc lại gợi ý mà tác giả cho “NOTE: if you have solved this level and see ‘Byebye!’ when trying to log into bandit18, this is related to the next level, bandit19” |
| ***Step 5*** | Chúng ta thử mật khẩu đầu tiên vào máy chủ bandit18 nếu hiện “Byebye” thì đó mà mật khẩu chính xác. |
| ***Step 6*** |  |
| ***Step 7*** |  |
| ***Step 8*** |  |
| ***Step 9*** |  |
| **Flag** | | kfBf3eYk5BPBRzwjqutbbfE887SVc5Yd |
| **Note** | |  |
| **Thực hiện** | | Đậu Hoàng Tài |

|  |  |  |
| --- | --- | --- |
| **Đề bài** | ***Tên*** | Bandit 19 |
| ***Loại*** | Command Linux |
| ***Lưu trữ*** |  |
| ***Cụ thể*** | The password for the next level is stored in a file readme in the homedirectory. Unfortunately, someone has modified .bashrc to log you out when you log in with SSH. |
| **Quan sát đề bài** | |  |
| **Ý tưởng ban đầu** | | Đọc đề thấy tác giả nói về phiên của ssh bị kết thúc trước khi mình đăng nhập ssh nên vì vậy mình đã nghĩ đến mở giả một pseudo-tty trong phiên bằng cách này chúng ta có thể chạy trước một lệnh trước khi kết nối bị đóng |
| **Công cụ thực hiện** | | Máy ảo chạy để điều hành Linux. Cụ thể ở đây mình sài Windows Subsystem for Linux (WSL 2) |
| **Giải** | ***Step 1*** | Kết nối đến máy chủ bandit18 qua giao thức SSH và cùng lúc đó cat file readme như đề yêu cầu |
| ***Step 2*** |  |
| ***Step 3*** |  |
| ***Step 4*** |  |
| ***Step 5*** |  |
| ***Step 6*** |  |
| ***Step 7*** |  |
| ***Step 8*** |  |
| ***Step 9*** |  |
| **Flag** | | IueksS7Ubh8G3DCwVzrTd8rAVOwq3M5x |
| **Note** | |  |
| **Thực hiện** | | Đậu Hoàng Tài |

|  |  |  |
| --- | --- | --- |
| **Đề bài** | ***Tên*** | Bandit 20 |
| ***Loại*** | Command Linux |
| ***Lưu trữ*** |  |
| ***Cụ thể*** | To gain access to the next level, you should use the setuid binary in the homedirectory. Execute it without arguments to find out how to use it. The password for this level can be found in the usual place (/etc/bandit\_pass), after you have used the setuid binary. |
| **Quan sát đề bài** | |  |
| **Ý tưởng ban đầu** | | Đề gợi ý bạn nên sử dụng setuid nên ban đầu mình phải đi google mà đọc về nó. Cơ bản setuid là một loại đặc quyền file có thể cho phép user tạm có quyền thức thi file bằng chính quyền của người sở hữu. |
| **Công cụ thực hiện** | | Máy ảo chạy để điều hành Linux. Cụ thể ở đây mình sài Windows Subsystem for Linux (WSL 2) |
| **Giải** | ***Step 1*** | Kết nối đến máy chủ bandit19 qua giao thức SSH |
| ***Step 2*** | Kiếm tra file và thư mục có trong máy chủ    Chúng ta có một file là “bandit20-do” và chưa biết nó là file gì và người dùng ở đây không có quyền đọc thực thi và ghi vào nó |
| ***Step 3*** | Kiểm tra file “bandit20-do” là file gì bằng lệnh file |
| ***Step 4*** | Chúng ta thấy file đó là file binary và có setuid nên vì vậy ta có quyền tạm thời đọc file đó như chính người sở hữu |
| ***Step 5*** |  |
| ***Step 6*** |  |
| ***Step 7*** |  |
| ***Step 8*** |  |
| ***Step 9*** |  |
| **Flag** | | GbKksEFF4yrVs6il55v6gwY5aVje5f0j |
| **Note** | |  |
| **Thực hiện** | | Đậu Hoàng Tài |

|  |  |  |
| --- | --- | --- |
| **Đề bài** | ***Tên*** | Bandit 21 |
| ***Loại*** | Command Linux |
| ***Lưu trữ*** |  |
| ***Cụ thể*** | There is a setuid binary in the homedirectory that does the following: it makes a connection to localhost on the port you specify as a commandline argument. It then reads a line of text from the connection and compares it to the password in the previous level (bandit20). If the password is correct, it will transmit the password for the next level (bandit21). |
| **Quan sát đề bài** | |  |
| **Ý tưởng ban đầu** | | Đọc qua đề bài thì có lẽ chúng ta phải scan port của máy chủ xem những port nào đang mở trên máy chủ sau đó tạo một máy chủ. Sau đó thiết lập một trình lắng nghe bằng port của mình không trùng với những port đang mở ở máy chủ. Cuối cùng chạy file binary đó với port của mình mở. Nếu trùng với password mình đang lắng nghe thì có pass của bandit21 |
| **Công cụ thực hiện** | | Máy ảo chạy để điều hành Linux. Cụ thể ở đây mình sài Windows Subsystem for Linux (WSL 2) |
| **Giải** | ***Step 1*** | Kết nối đến máy chủ bandit20 qua giao thức SSH |
| ***Step 2*** | Kiểm tra file và thư mục có trong máy chủ |
| ***Step 3*** | Chúng ta không thể mở file subconnect như thử thách trên |
| ***Step 4*** | Bây giờ ta kiểm tra các cổng đã mở trên máy chủ |
| ***Step 5*** | Chúng ta thử lắng nghe port 40000 của riêng mình không trùng với tất cả các port đang mở trên máy chủ của nó |
| ***Step 6*** | Bật 1 tab mới và connect tới port của mình đang mở nếu trùng với pass mình đang để ở bước trên thì nó sẽ gửi cho chúng ta pass của bandit21 |
| ***Step 7*** | Kết quả    Chúng ta có pass của bandit21 |
| ***Step 8*** |  |
| ***Step 9*** |  |
| **Flag** | | gE269g2h3mw3pwgrj0Ha9Uoqen1c9DGr |
| **Note** | |  |
| **Thực hiện** | | Đậu Hoàng Tài |

|  |  |  |
| --- | --- | --- |
| **Đề bài** | ***Tên*** | Bandit 22 |
| ***Loại*** | Command Linux |
| ***Lưu trữ*** |  |
| ***Cụ thể*** | A program is running automatically at regular intervals from cron, the time-based job scheduler. Look in /etc/cron.d/ for the configuration and see what command is being executed. |
| **Quan sát đề bài** | |  |
| **Ý tưởng ban đầu** | | Ở thử thách này dễ hơn mấy thử thách trước chỉ cần như gợi ý của tác giả. Điều hướng đến thư mục /etc/cron.d/ và tìm kiếm tệp nào có tên là bandit22 |
| **Công cụ thực hiện** | | Máy ảo chạy để điều hành Linux. Cụ thể ở đây mình sài Windows Subsystem for Linux (WSL 2) |
| **Giải** | ***Step 1*** | Kết nối đến máy chủ bandit21 qua giao thức SSH |
| ***Step 2*** | Kiểm tra file và thư mục có trong máy chủ |
| ***Step 3*** | Như ý tưởng ban đầu bây giờ chúng ta điều hướng đến “/etc/cron.d/” |
| ***Step 4*** | Kiểm tra file và thư mục có ở địa chỉ đó thì thấy được có bandit22 sau đó ta mở file “cronjob\_bandit22” |
| ***Step 5*** | Kết quả hiển thị bandit2 nằm ở “/usr/bin/cronjob\_bandit22.sh” vậy nên ta lại cat ở địa chỉ đó |
| ***Step 6*** | Kết quả cuối cùng nhận được pass của bandit22 nằm ở địa chỉ “/tmp/t7O6lds9S0RqQh9aMcz6ShpAoZKF7fgv” và chúng ta cat ở đó và có flag |
| ***Step 7*** |  |
| ***Step 8*** |  |
| ***Step 9*** |  |
| **Flag** | | Yk7owGAcWjwMVRwrTesJEwB7WVOiILLI |
| **Note** | |  |
| **Thực hiện** | | Đậu Hoàng Tài |

|  |  |  |
| --- | --- | --- |
| **Đề bài** | ***Tên*** | Bandit 23 |
| ***Loại*** | Command Linux |
| ***Lưu trữ*** |  |
| ***Cụ thể*** | A program is running automatically at regular intervals from cron, the time-based job scheduler. Look in /etc/cron.d/ for the configuration and see what command is being executed. |
| **Quan sát đề bài** | |  |
| **Ý tưởng ban đầu** | | Bài này chúng ta cũng sẽ điều hướng đến đường dẫn /etc/cron.d/ |
| **Công cụ thực hiện** | | Máy ảo chạy để điều hành Linux. Cụ thể ở đây mình sài Windows Subsystem for Linux (WSL 2) |
| **Giải** | ***Step 1*** | Kết nối đến máy chủ bandit22 qua giao thức SSH |
| ***Step 2*** | Kiểm tra file và folder có trong máy chủ |
| ***Step 3*** | Chúng ta điều hướng đến đường dẫn như tác giả cho |
| ***Step 4*** | Kiểm tra file và folder có trong đường dẫn /etc/cron.d thì chúng ta thấy có file cronjob\_bandit23. Sau dó chúng ta thử mở file đó |
| ***Step 5*** | Chúng ta đọc file cronjob\_bandit23.sh ở đường dẫn /usr/bin như hiện ra ở màn hình. |
| ***Step 6*** | Chúng ta thấy sau khi đọc file cronjob\_bandit23.sh thì nó hiện ra một đoạn code đơn giản. Folow của code này đơn giản chỉ là biến myname sẽ được gán bằng id hiện tại của máy chủ. Mytarget sẽ được gán với một câu lệnh echo.  Sau đó sẽ coppy file password từ /etc/bandit\_pass/$myname qua /tmp/$mytarget  Cuối cùng nó đọc file /etc/bandit\_pass/$myname vào file /tmp/$mytarget |
| ***Step 7*** | Vậy chúng ta chỉ cần đổi biến myname bằng id của bandit 23 sẽ tìm kiếm được pass của bandit 23 |
| ***Step 8*** | Cuối cùng đọc file đó ở /tmp |
| ***Step 9*** |  |
| **Flag** | | jc1udXuA1tiHqjIsL8yaapX5XIAI6i0n |
| **Note** | |  |
| **Thực hiện** | | Đậu Hoàng Tài |