Chart, line chart

Description automatically generated

Hôm nay mk sẽ làm 1 bài mới có tên là “Road”. Bắt đầu thôi.

1. Dò quét

rustscan -b 500 -a 10.10.172.35

A screenshot of a computer

Description automatically generated with low confidence

Kết quả trả về vẫn 2 là port quen thuộc là 80 và 22. Chi tiết hơn

nmap -p 22,80 -sC -sV -v 10.10.172.35 -Pn

Text

Description automatically generated

2. Enum

Graphical user interface

Description automatically generated with medium confidence

Giao diện nhìn khá đẹp!!! Kéo xuống dưới mk tìm đc 1 thông tin đáng chú ý là skycouriers.thm. Mk add nó vào file /etc/hosts.

Graphical user interface, text, website

Description automatically generated

View page source tiếp thì tìm được 2 đường dẫn khá hay ho là /v2/admin/login.html và /v2/admin/track\_orders

Graphical user interface, text, application

Description automatically generated

Trước khi vào xem 2 đường dẫn đó mk tìm sub trước.

gobuster vhost -u skycouriers.thm -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -t 50

Bục mặt mà ko tìm thấy gì. Thế thì quay sang tìm hidden file/folder xem sao.

gobuster dir -u skycouriers.thm -w /usr/share/wordlists/dirb/big.txt -x html,php,txt -t 50

A screenshot of a computer

Description automatically generated with medium confidence

Thế này thì ghé vào “phpMyAdmin” thôi.

Graphical user interface, application

Description automatically generated

Thử 1 vài user/pass mặc định thì fail toàn tập. Hmm, mk quyết định quay trở lại với 2 đường dẫn tìm được ở phần trên.

Giống như ở page “phpMyAdmin” ở đây mk cũng test 1 vài user/pass đơn giản như root:root, admin:admin, admin:password,…..Kết quả cũng không khác gì ở trên. Fail.

Graphical user interface, chart

Description automatically generated

Nhìn “Register” thế này thì khả năng cao cách này ko hợp lý. Ý tưởng lúc này sẽ là mk đăng ký 1 tài khoản, rồi dùng tài khoản đó login vào hệ thống, rồi từ acc thường này sẽ tiến tới chiếm acc admin.

Graphical user interface

Description automatically generated with medium confidence

Với cái search form ở trên mk đã test nhưng ko bị dính sqli. Ở phần Profile mk tìm đc cái này

Graphical user interface, text, application, email

Description automatically generated

Mới đầu hí hửng tưởng file upload để get shell nên hì hục test. Xong ko có kết quả gì. Hmm, tuy fail nhưng mk cũng có đc thông tin quan trọng email của acc admin là [admin@sky.thm](mailto:admin@sky.thm). Thế là ngon rồi. Logout tài khoản hiện tại và register 1 tài khoản có username là [admin@sky.thm](mailto:admin@sky.thm) và pass là 123456.

Thành công, tài khoản đã được tạo.

Graphical user interface, application

Description automatically generated

Ơ mà ko login đc =)). Những lúc bế tắc ntn mk thường ra ngoài làm cốc nước lọc cho đầu óc đc thoải mái.

Quay trở lại với bài. Mk login lại bằng acc đã tạo ở phần trên là [bevuichoi@gmail.com](mailto:bevuichoi@gmail.com)

3. Khai thác

Graphical user interface, website

Description automatically generated

Đây rồi, reset password. Mk thấy phần Username đã bị disable, ko cho chỉnh sửa nhưng khả năng là người ta chỉ disable front-end thôi.

Graphical user interface, text, application

Description automatically generated

Mk xóa phần read-only đi. Lúc này username có thể chỉnh đc rồi. Thế này thì vui rồi. Thay username [bevuichoi@gmail.com](mailto:bevuichoi@gmail.com) bằng [admin@sky.thm](mailto:admin@sky.thm) để reset password thôi.

Graphical user interface, application

Description automatically generated

Submit và success. Lúc này mk login với acc admin.

Graphical user interface, text, application, email, website

Description automatically generated

Đến đây mk nhớ lại phần upload file ở phần trên (vì nó chỉ hoạt động với acc admin) nên khai thác vào điểm yếu đó. Mk quyết định “sắm” 1 con php reverse shell rồi upload thử xem sao.





Thay “127.0.0.1” bằng IP của mk. Upload!! Phần thông báo thành công tắt khá nhanh. Điều quan trọng bây giờ là tìm làm sao đc đường dẫn tới shell.php mà chúng ta vừa upload. Hmm mặc dù upload thành công nhưng avatar vẫn ko đổi. Mk có đổi sang 1 file ảnh khác thì kết quả vẫn tương tự. Mk quyết định brute force tiếp để tìm file/folder ẩn

gobuster dir -u http://skycouriers.thm/v2 -w /usr/share/wordlists/dirb/big.txt -x html,php,txt -t 50

Đợi 1 lúc lâu là ko có kết quả gì. Thử với các wordlist khác nhau cũng ko ăn thua. Lúc này bắt đầu nản =)). Mk lại ra ngoài 1 lúc trong nhẹ đầu.

Haizz, “cờ bí dí tốt” còn ko tìm đc file/folder thì ta view page source vậy. Mk bắt đầu từ <http://skycouriers.thm/v2/index.php> đến <http://skycouriers.thm/v2/ResetUser.php> và cuối cùng tìm được ở <http://skycouriers.thm/v2/profile.php>

Text

Description automatically generated

/v2/profileimages/ đây chính là thư mục chứa ảnh avatar mà cũng là nơi shell.php mà mk vừa upload đc lưu ở đây.

A picture containing text, clock, mounted, dark

Description automatically generated

Graphical user interface

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Thành công. Đã lấy được shell

4. Leo thang đặc quyền

Graphical user interface, text, application

Description automatically generated

Như vậy ngoài user root ra thì chỉ có thêm 1 user khác là webdeveloper. User này đặc biệt ở chỗ là nó ở trong group sudo

Graphical user interface, text, application

Description automatically generated

Login vào mysql nhưng ko tìm đc gì. Mk có thử password này với các user khác nhau đều không thành công. Đến lúc này, mk vẫn như cũ tìm các SUID, schedule, sudo permission, id\_rsa, kernel exploit….thì đều ko đc. Khi theo dõi các tiến trình và đặc biệt là các tiến trình mạng thì mk phát hiện

A screenshot of a computer

Description automatically generated with medium confidence

Những port bật trên local: mysql 3360, port 9000 rất khả nghi có thể là http, còn port 27017 thì là port gì mk cũng biết. Research vậy

Graphical user interface, text, application, email

Description automatically generated

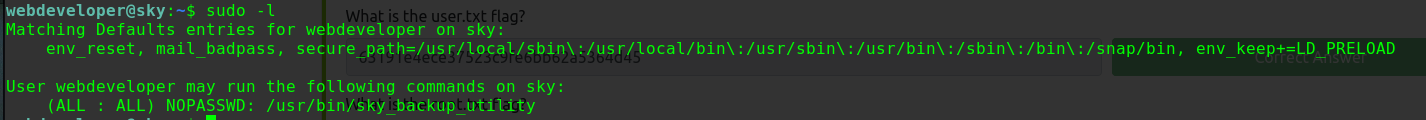
Thì ra là MongoDB. Mk chưa xài cái này bh nên phải tham khảo cách sử dụng ở đây <https://www.youtube.com/watch?v=SY_9zwb29LA>

Text

Description automatically generated

Đến đây thì password của webdeveloper chắc chắn là “BahamasChapp123!@#”. Login ssh thôi.

ssh webdevloper@10.10.172.35 -p 22



Khá vui “/usr/bin/backup\_utility”. Kiểm tra xem nó thực hiện những gì.

strings /usr/bin/sky\_backup\_utility

A screenshot of a computer

Description automatically generated with medium confidence

# Với lệnh tar như thế kia thì mk nảy ra 2 ý tưởng có thể sử dụng PATH variable hoặc Exploiting Wildcard (<https://www.hackingarticles.in/exploiting-wildcard-for-privilege-escalation/>) để leo thang đặc quyền. Nhưng mk quyết định tận dụng sudo group =)) (vì ở phần trên chúng ta đã phát hiện webdeveloper thuộc sudo group). Link tham khảo <https://book.hacktricks.xyz/linux-unix/privilege-escalation/interesting-groups-linux-pe>

# PE 1 ko dùng được mk chuyển qua PE 2. Với PE 2 thì phải mở thêm 1 sessions ssh nữa.

# Text Description automatically generated

# Graphical user interface, text, application, email Description automatically generated

# Mk làm theo như hướng dẫn ở đây. Và thành công lấy được quyền root trên hệ thống.

# A screenshot of a computer Description automatically generated with medium confidence

# Text Description automatically generated