

Chào các bạn, lâu lắm rồi mk ko viết writeup thì hôm nay mk trở lại với 1 bài mới đc ra mắt có tên là “Hacker vs Hacker”. Bắt đầu thôi

1. Dò quét

rustscan -b 500 -a 10.10.152.95

A picture containing text, clock

Description automatically generated

Vẫn là 2 cổng quen thuộc là 80 và 22.

nmap -p 22,80 -sC -sV -v -T4 10.10.152.95 -Pn

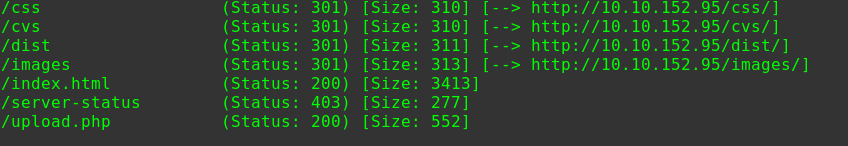
Text

Description automatically generated

1. Enum

Trước tiên ta tìm hidden file/folder:

gobuster dir -u 10.10.152.95 -w /usr/share/wordlists/dirb/big.txt -t 75 -x html,php,txt



Trong số các kết quả tìm được thì “cvs” và “upload.php” là 2 thứ mk thấy là thú vị nhất.

Graphical user interface, text, application

Description automatically generated

Với đoạn code trên thì chỉ cần đặt tên file là “shell.pdf.php” là bypass được rồi. => upload thôi

Trên website của target có phần upload mà chúng ta đang tìm và file thì được lưu ở thư mục “cvs”.

Graphical user interface, application, website

Description automatically generated

Tới đây mk nghĩ ngay tới “File upload vulnerability”. Ko đắn đo, mk up 1 con shell và kết quả là: thật bất ngời =)).

Graphical user interface, text, application, website

Description automatically generated

Ở folder “cvs” cũng ko khá hơn

Graphical user interface, text, application

Description automatically generated

Bị filter rồi. Sau đó mk có dùng rất nhiều cách để bypass mà vẫn chưa đc. Từ shell.pdf.php, shell.pdf.phtml, shell.php%00.pdf,….. Nghe vẻ hơi khó nhai rồi.

Đến đây thì mk cũng loay hoay hơn 90 phút để tìm đường, thì bất chợt trong đầu lóe lên ý nghĩ rằng: có khi nào file mk up nó đã đc lưu trên server rồi chăng. Thế là mk thử các file mà mk đã upload

Graphical user interface, text, application, email

Description automatically generated

Nhưng đến “shell.pdf.php” thì thật bất ngờ

Graphical user interface, text, application

Description automatically generated

Wow, quá bất ngờ, đây chính là cái mà mk đang tìm.

**Cảm tạ Thượng Đế là Đấng đã ban sự may mắn và khôn ngoan này cho chúng ta.**

1. Exploitation

Mk thấy rằng file này ko phải file mk đã upload mà đây là file do attacker đã up (theo gợi ý cũng như tiêu đề thì chúng ta đoán đc điều đó). Nó là 1 con webshell. Thường thì những con webshell cho phép chúng ta chạy lệnh trên đó. Hãy thử với 1 vài parameter như: cmd, c, command,….

Graphical user interface, text, application, email

Description automatically generated

OS command injection thì khá quen thuộc rồi.

Text

Description automatically generated

1. Leo thang đặc quyền

Graphical user interface, text

Description automatically generated

Dễ dàng thấy được password của “Lachlan” là “thisistheway123”

Text

Description automatically generated

Sau 1 hồi lục lọi đủ các thứ, thậm chí dùng đến cả linpeas mà chưa thấy gì thì mk bắt đầu lại theo hướng mà attacker trước đó đã làm

Text

Description automatically generated with medium confidence

Nhìn hướng mà attacker đã đi thì khả năng là kernel hoặc có 1 chương trình nào đó bị lỗi. Thế là mk hì hục lục lọi tiếp. Hơn 1 tiếng tiếp theo trôi qua, thử rất nhiều đoạn exploit rồi enum đi enum lại vẫn chưa thành công.

Sau 1 hồi mới ngớ ra là chưa xem file “/etc/cron.d/persistence” nó có nd ntn.

A picture containing text

Description automatically generated

File backup.sh run với quyền user root nhưng bị comment mất rồi. Nhưng, khoan đã, “pkill” họ ko dùng đường dẫn tuyệt đối. Về lỗi này các bạn có thể tham khảo: <https://www.hackingarticles.in/linux-privilege-escalation-using-path-variable/>

Sau đó bạn sẽ lấy được shell của user root