Graphical user interface, text, application

Description automatically generated

Lâu lắm rồi ko làm thì hn mk trở lại với bài “Chocolate Factory”. Bài này cũng khá dễ thôi. Let’s go

1. Dò quét

nmap -T4 -v 10.10.83.7 -Pn

Text

Description automatically generated

Rất nhiều cổng đang mở. Chúng ta nên bđ từ những port quen thuộc như 21, 22, 80.

1. Enum

ftp cho phép chúng ta anonymous login

Text

Description automatically generated with medium confidence

Có 1 file ảnh gum\_room.jpg.

A picture containing text

Description automatically generated

Về nd thì ko có gì ngoài mấy thanh kẹo cao su =)).

Graphical user interface, text

Description automatically generated

Nothing.

Graphical user interface

Description automatically generated

Trong file ảnh người ta giấu trong đó file text b64.txt đã đc encode ở dạng base64 => Decode xem nd nó là gì

Graphical user interface, text

Description automatically generated with medium confidence

Chính là nó. Chúng ta có được hash của user Charlie. Sau khi đợi crack thì ta thu được password là “cn7824”

Mk login với ssh và ftp thì đều ko thành công. Hmm chuyển qua web xem có gì ko

Diagram

Description automatically generated with low confidence

Nó để login cho cái này và thành công

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

Description automatically generated

Lấy shell thôi.

Text

Description automatically generated

Text

Description automatically generated

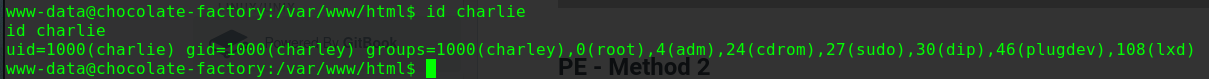
1. Leo thang đặc quyền

Khá buồn cười khi www-data lại thuộc group root và sudo. Với việc thuộc group sudo chúng ta có thể đọc file /etc/sudoers

Text

Description automatically generated

Ở đây chúng ta phát hiện được user Charlie có thể chạy lệnh vi bằng quyền root mà ko cần password. Khá ngon.

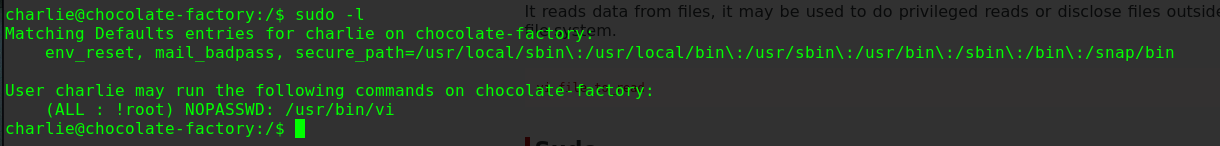


Ở trong /home/charlie tìm được file teleport (thực ra nó là id\_rsa)

Graphical user interface, text

Description automatically generated

Login bằng key tìm được thôi



Mk có thử với lxd để leo thang nhưng ko thành công.

A screenshot of a computer

Description automatically generated