Lab 5

Bắt gói tin & dò tìm mật khẩu WPA/WPA2

Cracking WPA/WPA2 passwords

Thực hành Nhập môn Mạng máy tính

GVTH: Nguyễn Thanh Hòa

Học kỳ I – Năm học 2016-2017

Lưu hành nội bộ

(Dành cho Lớp PMCL2015.1)

A. TỔNG QUAN

1) Mục tiêu

- Tìm hiểu về bản distro Linux: Kali Linux 2016.
- Tìm hiểu về quá trình bắt tay 4 bước trong WPA/WPA2.
- Ứng dụng bắt gói tin và dò tìm mật khẩu Wifi theo phương pháp wordlist/brute-force sử dụng Kali Linux 2016.

Nội dung thực hành chỉ sử dụng cho mục đích học tập, nghiên cứu; không sử dụng với mục đích xấu ảnh hưởng đến bất kỳ tổ chức, cá nhân.

2) Nội dung chính

- Tìm hiểu về WPA/WPA2
- Tạo Kali Linux Live USB để sử dụng trực tiếp Kali Linux
- Ứng dụng Kali Linux trong khai thác password Wifi (WPA/WPA2)

3) Môi trường & công cụ

- Máy tính có card Wifi *(Laptop)* hoặc sử dụng USB Wifi
- 1 USB có dung lượng từ 4GB trở lên *(khuyến cáo USB 3.0)* để tạo Kali Live USB
- Bản cài đặt Kali Linux 2016.2 download tại https://www.kali.org/downloads/

Các phần mềm hỗ trợ tạo Kali Live USB:

- Phần mềm Universal USB Installer 1.9 để tạo Linux Live USB download tại https://www.pendrivelinux.com/universal-usb-installer-easy-as-1-2-3/

Lưu ý: *Sinh viên có thể cài song song Kali Linux cùng hệ điều hành hiện tại (nếu biết phương pháp) hoặc sử dụng các công cụ tương đương để tạo Kali Live USB.*

4) Kiến thức tổng quan

WEP, WPA/WPA2 là những chuẩn bảo mật phổ biến để bảo vệ mạng wifi, bảo đảm an toàn cho kết nối không dây. WEP là một giao thức bảo mật cũ với nhiều hạn chế về bảo mật và hiện tại đã được thay thế bởi 2 chuẩn WPA/WPA2 (WiFi Protected Access). WEP viết tắt của Wired Equivalent Privacy (Riêng tư tương tự mạng dây), WPA là Wireless Protected Area (vùng bảo vệ không dây). WPA2 là phiên bản thứ hai của chuẩn WPA.

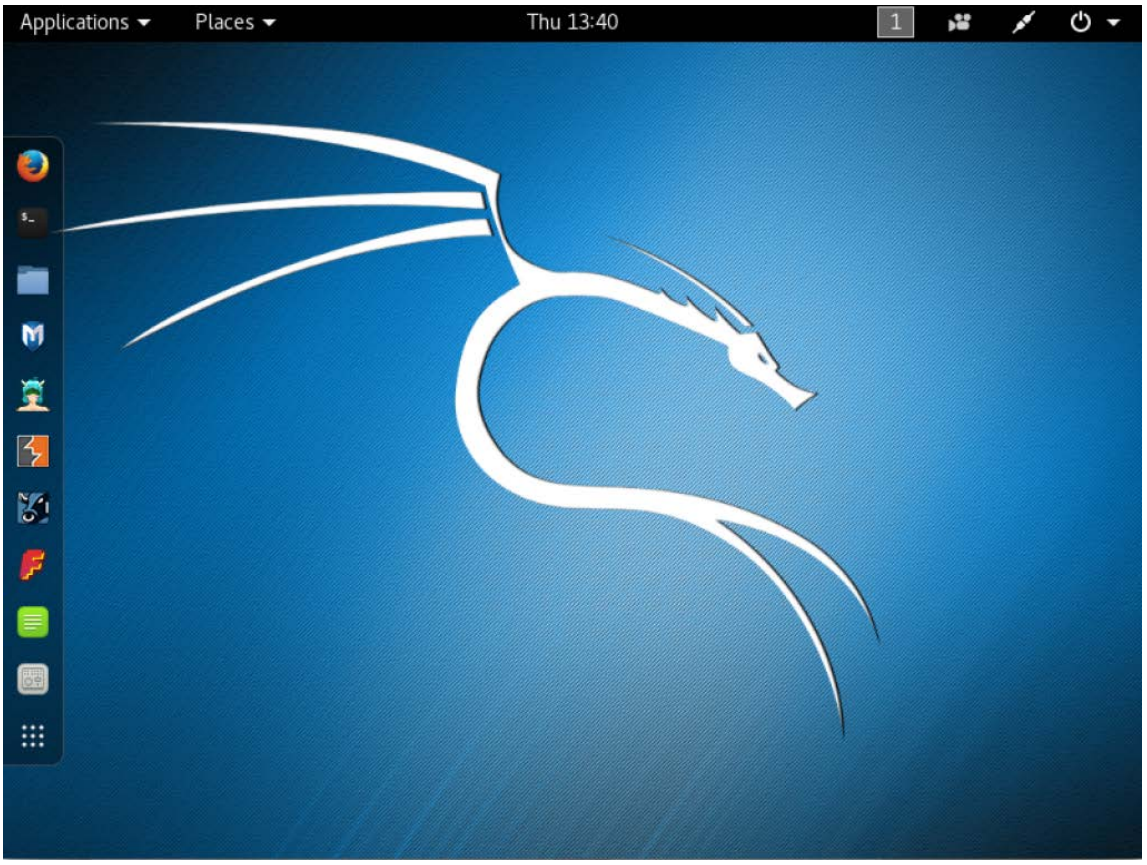
B. THỰC HÀNH

BÀI I. CHUẨN BỊ MÔI TRƯỜNG KALI LINUX 2016

1) Chuẩn bị

Kali Linux là một phiên bản Linux nhân Debian rất hữu ích đối với những chuyên gia đánh giá bảo mật, tập hợp và phân loại gần như tất cả các công cụ thiết yếu mà bất kỳ một chuyên gia đánh giá bảo mật nào cũng cần sử dụng đến khi tác nghiệp – tấn công thử nghiệm (Penetration Testing – pentest)

Phiên bản mới nhất của Kali Linux hiện tại là **Kali Linux 2016.2** (tháng 12/2016) có dung lượng ~ 2.9GB và được cung cấp miễn phí tại https://www.kali.org/downloads/



Hình 1. Hệ điều hành Kali Linux 2016.2

2) Thực hành

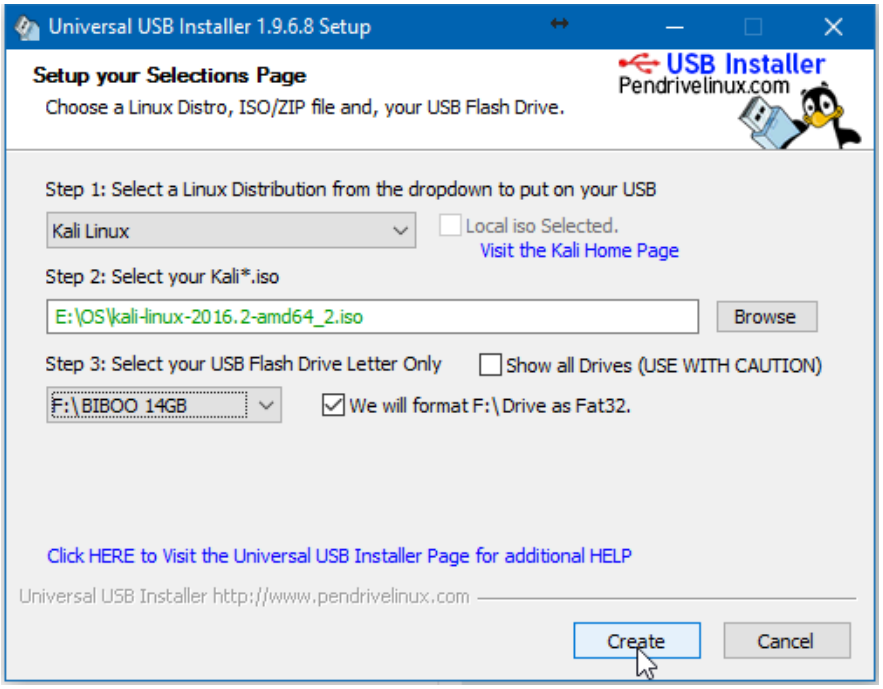
a) Tạo Kali Linux Live USB:

Phương pháp này sẽ tạo nhanh chóng Kali Linux Live USB để có thể sử dụng Kali Linux trực tiếp qua USB ở nhiều máy tính khác nhau mà không cần cài đặt.

- **Bước 1:** Chuẩn bị file iso Kali Linux 2016.2 ~ 2.9GB (có thể download tại trang chủ https://www.kali.org/downloads/ hoặc sinh viên có thể chép trực tiếp bản cài đặt Kali Linux từ GVTH vào buổi thực hành).

- **Bước 2:** Sử dụng phần mềm Universal USB Installer (UUI) 1.9 để tạo Kali Live USB. Lựa chọn bản Kali Linux và chọn đúng file iso cài đặt Kali Linux 2016, chọn USB để cài đặt Kali.

Lưu ý: *USB cần được định dạng FAT32 và nên có dung lượng tối thiểu từ 4GB, khuyến cáo USB 3.0 để có tốc độ đọc ghi tốt.*



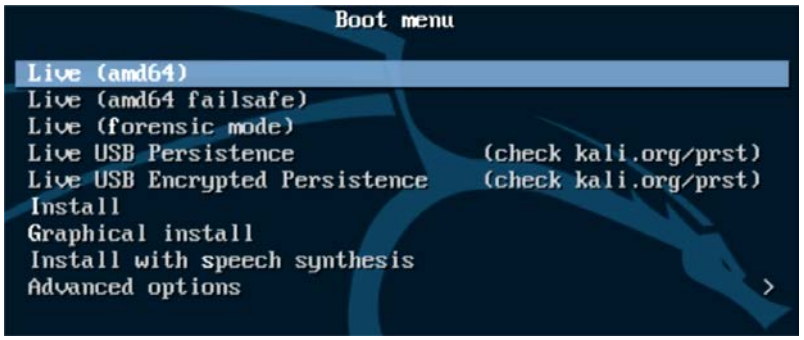
Hình 2. Tạo Kali Linux Live USB bằng UUI

Chọn Yes ở hộp thoại tiếp theo để đồng ý ghi và chờ quá trình tạo hoàn tất.
Lưu ý: Đánh dấu chọn We will format …. As Fat32, USB sẽ được format lại.

- **Bước 3:** Khởi động lại máy tính và chọn tùy chỉnh Boot vào USB đầu tiên.

Lưu ý: Tùy từng dòng máy mà cách vào menu boot sẽ khác nhau.

- **Bước 4:** Sau khi đã boot từ USB, ở màn hình Boot menu, chọn Live (amd64) để sử dụng Kali Linux trực tiếp.



Hình 3. Chọn Live (amd64) để có thể sử dụng ngay Kali Linux

- **Bước 5:** Đăng nhập vào Kali Linux với tài khoản là **root** và mật khẩu mặc định của tài khoản root là **toor**

Hình 4. Đăng nhập với username root và mật khẩu toor

Quá trình chuẩn bị môi trường hoàn tất.

Trong môi trường Kali Linux, vẫn có thể truy xuất dữ liệu đến các ổ đĩa trong máy tính bằng cách mở **Files** > chọn thẻ **Other Locations** > danh sách các ổ đĩa thật sẽ xuất hiện, đồng thời có thể mở file PDF bình thường bằng công cụ có sẵn. Trình duyệt được cài đặt sẵn là Firefox.

Kali Linux có hỗ trợ sẵn chức năng quay phim màn hình bằng công cụ EasyScreenCast với nhiều tùy biến khác nhau thuận tiện trong việc ghi nhận quá trình thực hành để làm báo cáo.

Hình 5. Chức năng quay phim màn hình có sẵn trong Kali Linux

BÀI II. SỬ DỤNG KALI LINUX CRACK WIFI PASSWORD VỚI AIRCRACK-NG

1) Tổng quan

AIRCRACK-NG [1] là bộ công cụ mạnh mẽ trong Kali Linux phục vụ cho quá trình đánh giá bảo mật mạng Wifi. Bộ công cụ này gồm nhiều công cụ với các chức năng như:

- **airmon-ng** – Dùng để chuyển card Wireless sang chế độ monitor *(chế độ theo dõi và thu thập tín hiệu Wifi).*
- **airodump-ng** – dùng để phát hiện các điểm phát sóng và bắt các gói tin 802.11.
- **aireplay-ng** – tạo ra dòng tín hiệu tác động đến mạng.
- **aircrack-ng** – tìm ra mã khóa WEP.

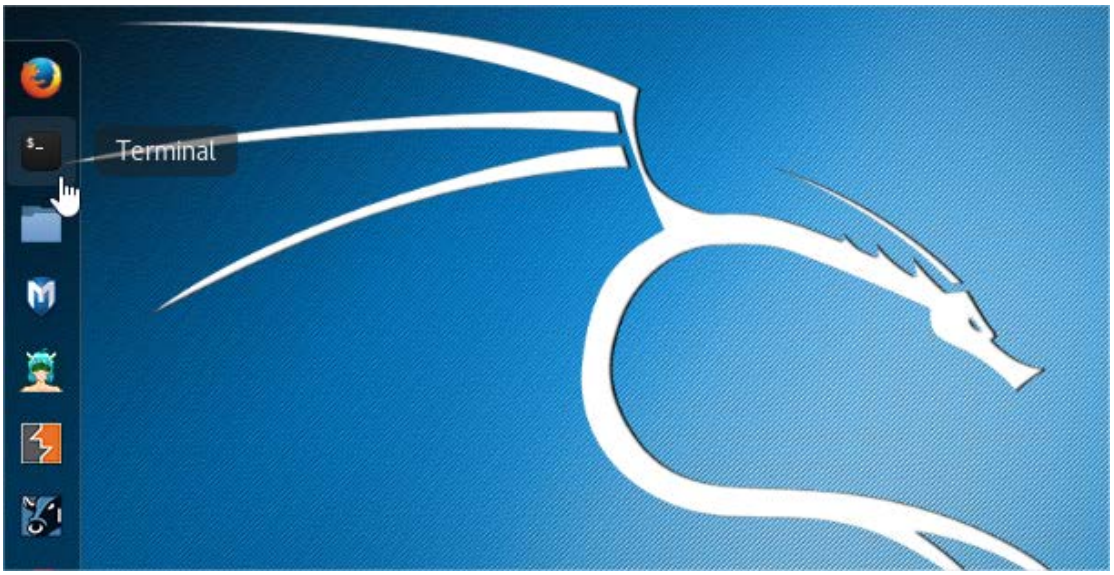
Bộ Aircrack-ng còn khá nhiều công cụ khác phục vụ cho việc khai thác mạng Wifi có thể tham khảo tại [1] .

Crunch[2] là công cụ tạo Wordlist (danh sách các mật khẩu theo quy tắc đã định nghĩa) tự động và rất nhanh chóng, phục vụ cho việc dò tìm mật khẩu, có sẵn trong Kali Linux.

2) Thực hành

a) Sử dụng Aircrack-ng để crack mật khẩu Wifi (WPA/WPA2)

- **Bước 1:** Mở Terminal để thực hiện các câu lệnh (tương tự Command Prompt trong Windows)



Hình 6. Khởi động Terminal

[1] http://tools.kali.org/wireless-attacks/aircrack-ng
[2] http://tools.kali.org/password-attacks/crunch

- **Bước 2:** Kiểm tra tên card Wireless đang sử dụng bằng lệnh **iwconfig**, thông thường là card wlan0. Nếu card wireless chưa được bật (không thể kết nối wifi) thì có thể bật bằng lệnh **ifconfig wlan0 up**

- **Bước 3:** Chuyển card mạng Wifi sang chế độ monitor (chế độ theo dõi toàn bộ các tín hiệu trong mạng) bằng airmon-ng.

Kiểm tra tên card Wifi với lệnh iwconfig hay airmon-ng, thông thường là wlan0.
Chuyển card wlan0 sang chế độ monitor bằng công cụ **airmon** với lệnh:

airmon-ng start wlan0

Hình 7. Kích hoạt chế độ Monitor trên card wlan0

Lúc này, kiểm tra bằng ifconfig ta sẽ thấy có card wlan0mon

- **Bước 4:** Sử dụng airodump để theo dõi hoạt động các mạng wifi hiện tại qua card wlan0mon (card wlan0 ở chế độ monitor)

airodump-ng wlan0mon

- **Bước 5:** Xác định mạng wifi mục tiêu và sử dụng airodump để bắt gói tin và chỉ theo dõi duy nhất mạng mục tiêu đó:

airodump-ng -c [channel] **-w** [tập tin] **--bssid** [BSSID của mạng] **wlan0mon**

Ví dụ: *airodump-ng -c 9 -w wifi-sniff --bssid C4:6E:1F:F6:34:B8 wlan0mon*

Trong đó:

+ Quan sát trường CH để xác định Channel của điểm phát sóng
+ -w [tập tin]: xác định đường dẫn để lưu tập tin bắt được (định dạng .cap)
+ bssid: Xem trường BSSID (địa chỉ MAC của access point)

- **Bước 6:** Thu thập gói tin bắt tay WPA handshake (bắt tay 4 bước) trong quá trình đăng nhập để dựa vào đó dò tìm mật khẩu.

Có 2 cách:

+ Chờ người dùng nào đó đăng nhập vào Wifi đang theo dõi.

+ Sử dụng aireplay để tạo tín hiệu deauth (kích các người dùng đang sử dụng mạng thoát ra và đăng nhập lại liên tục. Cú pháp:

aireplay-ng --deauth [số lệnh deauth] **-a** [BSSID của mạng] **wlan0mon**

Ví dụ: *aireplay-ng --deauth 5 -a C4:6E:1F:2D:D6:B8 wlan0mon (có thể thay –deauth thành -0, khi muốn gửi không giới hạn lệnh deauth có thể đặt thông số là 0)*

- **Bước 7:** Thực hiện chờ hoặc dùng aireplay như bước 6 đến khi nhận được gói tin WPA handshake của mạng mục tiêu tương ứng, ta dừng quá trình bắt gói tin (Ctrl+C) và tiến hành dò tìm mật khẩu dựa vào file .cap đã bắt được.

Hình 8. Ví dụ đã nhận được gói tin WPA Handshake của mạng C4:6E:1F:2D:D6:B8

Có thể sử dụng phương pháp dò tìm theo Wordlist hay thực hiện Brute-force để dò tìm mật khẩu.

- Phương pháp dùng Wordlist (danh sách các từ có sẵn)

Trong Kali cung cấp sẵn một số Wordlist thông dụng tại thư mục /usr/share/wordlist. Nổi bật là wordlist rockyou.txt với thư viện khoảng 10 triệu mật khẩu thông dụng. Ngoài ra, có thể dùng Crunch để tự tạo Wordlist tùy ý.

Nếu sử dụng Wordlist rockyou.txt có sẵn, ta thực hiện các lệnh sau:

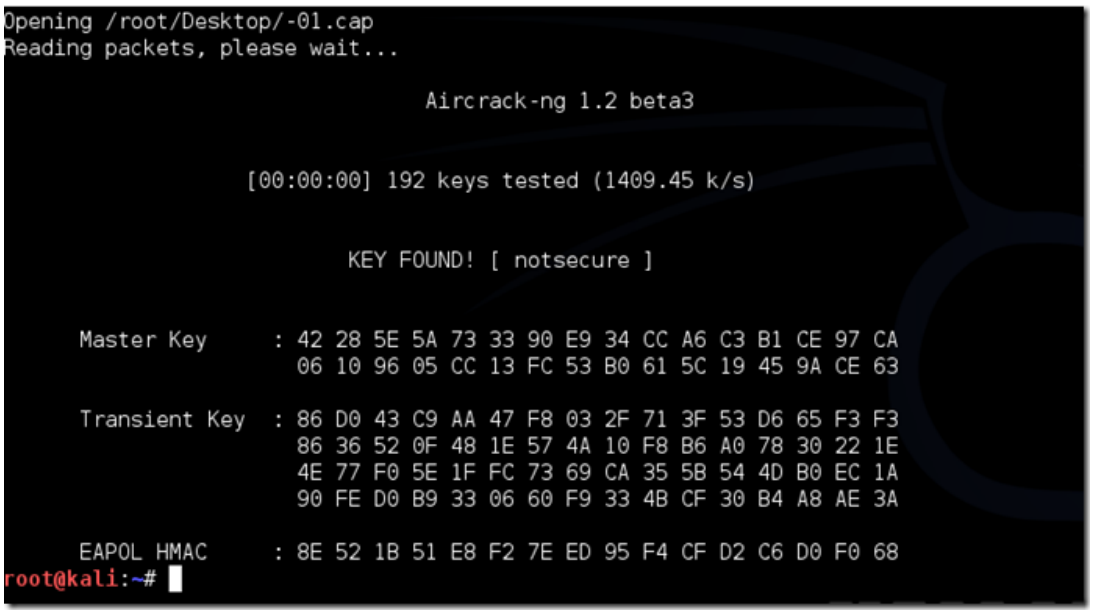
cp /usr/share/wordlists/rockyou.txt.gz /root/Desktop → Copy file nén chứa rockyou.txt ra Desktop để thuận tiện sử dụng

gzip –d /root/Desktop/rockyou.txt.gz → Giải nén file rockyou.txt.gz

Sau khi đã có file rockyou.txt đã giải nén, sử dụng lệnh sau để dò tìm password:

aircrack-ng -w [đường dẫn file Wordlist] [đường dẫn file .cap đã thiết lập ở bước 5]

Ví dụ: aircrack-ng –w /root/Desktop/rockyou.txt wifi-sniff-01.cap



Hình 9. Ví dụ quá trình dò tìm mật khẩu từ Wordlist

- Phương pháp kết hợp tool **Crunch** để brute-force (dò tìm vét cạn) không cần dùng Wordlist có sẵn

Cú pháp để sử dụng Crunch:

crunch [min] [max] [charset] **-t** [pattern] **-o** [path file] với:

- [min]: số kí tự tối thiểu
- [max]: số kí tự tối đa
- [charset]: danh sách kí tự có trong mật khẩu
- [pattern]: mẫu mật khẩu & các ký tự đã biết, ký tự chưa biết ký hiệu %
- [path file]: đừng dẫn file Wordlist được tạo

Thực hiện lệnh với cú pháp như sau:

crunch [min] [max] [danh sách các ký tự có có trong chuỗi] **–t** [mẫu định dạng mật khẩu] | **aircrack-ng -w-** [tập tin đã capture.cap] **–bssid** [địa chỉ MAC của mục tiêu]

Ví dụ: Dự đoán mật khẩu có 10 ký tự là 1 số điện thoại có đầu số 091, mật khẩu gồm các số từ 0-9 có thể dò tìm vét cạn tất cả các dãy 091xxxxxxx như sau:

crunch 10 10 0123456789 –t 091%%%%%%% | aircrack-ng –w- wifi-sniff.cap –bssid C4:6E:1F:2D:D6:B8

- **Bước 8:** Sau khi đã tìm được mật khẩu, tắt chế độ monitor của card wlan0 để có thể sử dụng lại Wifi bằng lệnh

airmon-ng stop wlan0mon

Dùng mật khẩu vừa dò tim để truy cập thử Wifi.

C. YÊU CẦU

Sinh viên sử dụng bộ công cụ Aircrack-ng như đã hướng dẫn để thực hành crack mật khẩu Wifi được phát sóng tại buổi thực hành hoặc tự phát sóng 1 wifi với mật khẩu không quá phức tạp để có thể brute-force nhanh chóng và ghi nhận quá trình thực hiện của mình bằng Video quay lại quá trình thực hiện (upload lên Google Drive và nộp link chia sẻ) **hoặc** báo cáo quá trình thực hiện của mình trên file Word/PDF.

Sinh viên có thể tìm hiểu các phương pháp, công cụ khác để thực hiện việc crack mật khẩu Wifi trong các công cụ Kali Linux cung cấp.

D. MỞ RỘNG

Tạo phân vùng Persistence để lưu dữ liệu làm việc với Kali Linux trên USB

Khi sử dụng Kali Linux boot trực tiếp từ USB mặc định khi khởi động lại hệ thống thì toàn bộ dữ liệu của phiên làm việc trước đều bị mất đi và reset lại như ban đầu. Để có thể lưu trữ các dữ liệu trong quá trình làm việc với Kali trên USB, ta cần tạo phân vùng **Persistence** [3].

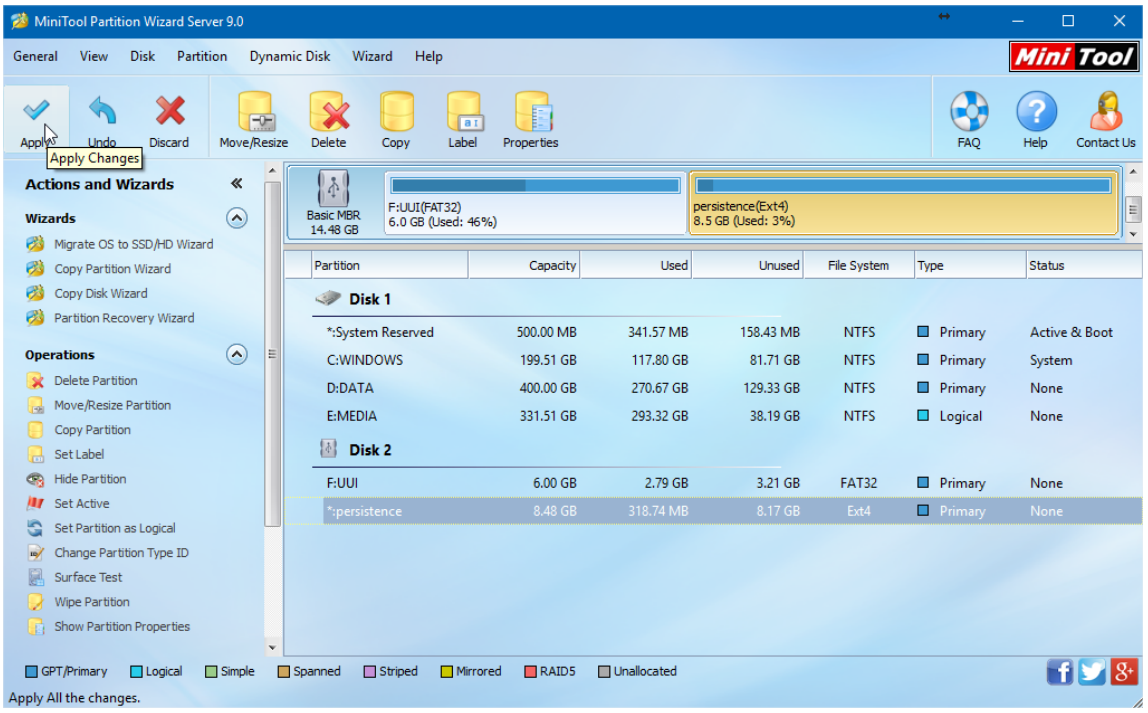
- **Bước 1:** Tạo phân vùng Persistence trên USB để Kali Linux lưu trữ file

Có thể dùng **MiniTool Partition Wizard 9** để thực hiện việc này:

Phần mềm MiniTool Partition Wizard 9 để định dạng, phân vùng ổ cứng download tại https://www.partitionwizard.com/partition-magic-free.html

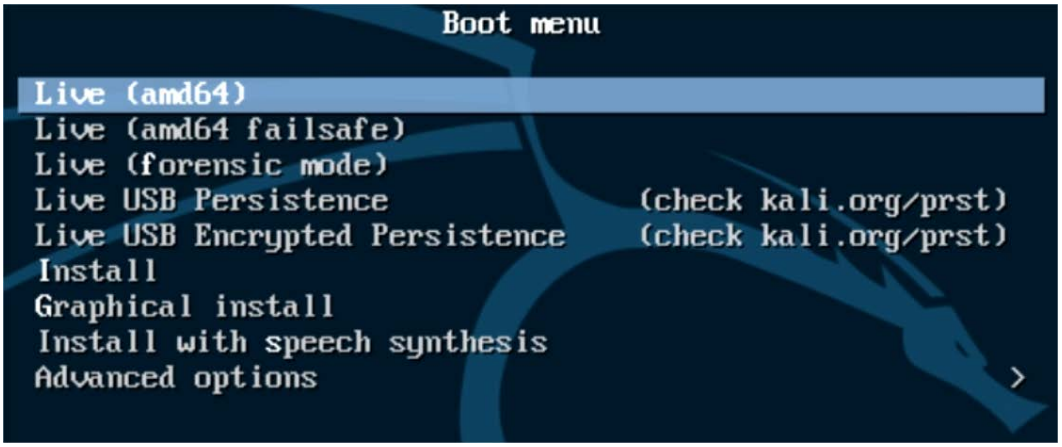
- Resize vùng đang chứa hệ điều hành trên USB còn trống khoảng từ 1GB.
- Tạo phân vùng tại vùng trống còn lại trên USB theo loại **Primary**, định dạng file system là **ext4** và tên **persistence**

[3] http://docs.kali.org/downloading/kali-linux-live-usb-persistence



Hình 10. Sau khi đã thiết lập phân vùng, nhấn Apply để áp dụng.

- **Bước 2:** Khởi động lại máy, chọn chế độ Boot vào USB (tùy từng loại máy sẽ có cách vào menu Boot khác nhau). Chọn khởi động ở chế độ Live bình thường.



Hình 11. Lưu ý không chọn chế độ Persistence ở giai đoạn này.

- **Bước 3:** Thực hiện việc cấu hình như sau sau khi khởi động Kali Linux:

Mở Terminal, thực hiện các lệnh sau

- **fdisk –l**: liệt kê tất cả ổ đĩa trong máy để kiểm tra tên phân vùng persistence
- **mkdir -p /mnt/UUI**: tạo thư mục trong filesystem để mount USB
- **mount** /dev/sdb2 **/mnt/UUI**: mount phân vùng persistence (/dev/sdb2) trên USB vào thư mục vừa tạo

- **echo "/ union"> /mnt/UUI/persistence.conf**: Tạo file cấu hình kích hoạt Persistence
- **umount /dev/sdb2 && reboot**: Unmount phân vùng và khởi động lại máy.

Quá trình cấu hình và tạo phân vùng Persistence hoàn tất và khi khởi động lại ta có thể sử dụng chế độ Live USB Persistence.

E. THAM KHẢO

[1] Cracking WPA: https://www.aircrack-ng.org/doku.php?id=cracking_wpa

HẾT