**Những Tool Dành Cho Hệ Điều Hành Kali Linux**

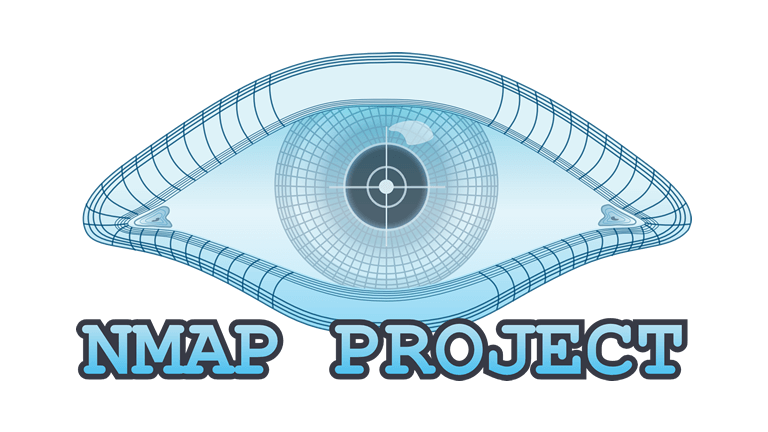
1. **Metasploit :**



Là Framework dùng để phát triển lỗi khai thác, shellcodes, fuzzing tool, payloads. Bộ Framework này có rất nhiều công cụ khai thác được tích hợp. Framework có sẵn trên nhiều hệ điều hành phổ biến như Mac OSX, Windows, Linux và được cài đặt sẵn trong Kali Linux. Nó thường được dùng để các hacker mũ trắng tấn công vào hạ tầng mạng của họ, từ đó tìm ra những lỗi bảo mật để sửa chữa kịp thời.

Ngoài ra Metasploit còn được dùng để nhắm đến các mục tiêu như ứng dụng web, mạng và server… Giao diện của Metasploit có cả đồ họa và command line. Sẽ có 2 phiên bản miễn phí và Metasploit Pro trả phí.

1. **Nmap (Network Mapper) :**



Nmap được dùng để scan cả hệ thống và tìm ra các port nào đang được mở. Với hacker mũ trắng, công cụ này được dùng để phát hiện máy tính nào đang online, và khảo sát bảo mật, các cổng đang mở cũng như service nào đang được chạy. Công cụ sử dụng các gói tin IP để biết host nào đang hoạt động trên hệ thống mạng, cổng nào đang mở cũng như các dịch vụ chạy trên nó.

Tool có 2 giao diện GUI và command line. Zenmap là giao diện người dùng được khuyến khích sử dụng dành cho newbie, lần đầu tiên tiếp xúc với command line, và sau đó chuyển qua GUI nếu bạn thấy tự tin.

1. **Armitage :**

Armitage là một công cụ quản lý tấn công mạng đồ họa, cung cấp giao diện GUI, giúp người dùng dễ tiếp cận và sử dụng. Nếu bạn thực sự muốn nắm vững về cơ bản cũng như các tính năng nâng cao trong tấn công mạng, Armitage sẽ là lựa chọn phù hợp nhất với các tính năng dò tìm, truy cập, khai thác…

Ngoài ra, nếu bạn đang làm việc cùng với nhóm, phần mềm còn có nhiều chế độ hữu ích để chia sẻ cho các thành viên khác cùng làm việc :

* Cùng sử dụng phiên.
* Share host bị tấn công, dữ liệu thu được, download file…
* Hỗ trợ giao tiếp cùng nhau thông qua một share log.
* Chạy boot tự động thực hiện công việc.

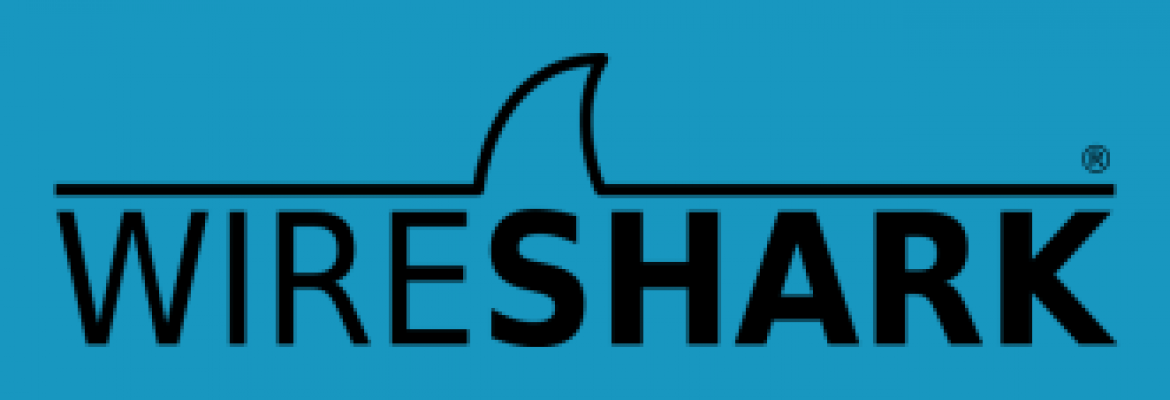
1. **Jhon The Ripper (JTR) :**



Jhon The Ripper là công cụ phổ biến để phá Password, được biết đến nhiều hơn với tên viết tắt JTR. Jhon The Ripper sử dụng những text file, còn được gọi là “wordlist”, file này chứa những password thông dụng và những password đã từng bị phá, sau đó công cụ sẽ lần lượt thử từng password cũng như những tổ hợp các text để tìm ra password nạn nhân.

Về phương pháp, Jhon The Ripper khá tương tự với THC Hydra, tuy nhiên JTR được dùng để crack password offline thì THC Hydra lại được dùng để crack password các service online.

1. **Wireshark :**



Wireshark là công cụ mã nguồn mở, được dùng để phân tích mạng, traffic của hệ thống, các gói tin… Với tên gọi cũ là Ethereal, Wireshark có thể chặn lưu lượng mạng, từ những thông tin kết nối đến từng bit của gói tín hiệu. Tất cả tác vụ này được thực hiện trong thời gian thực và hiển thị cho người dùng ở định dạng có thể đọc được.

Trong nhiều năm qua, Wireshark đã có nhiều sự thay đổi, nâng cấp đáng giá như là các bộ lọc, màu sắc các gói tin… việc này đã giúp ích nhiều cho nhà quản trị mạng quản lý và phân tích được những gì đang diễn ra trong hệ thống mạng của họ.

1. **THC Hydra :**



Như đã trình bày ở trên, THC Hydra là tool để crack password và cùng với Jhon The Ripper là 2 tool được cấu hình thủ công. THC Hydra còn được biết đến với tên rút gọn là Hydra, là công cụ hack password thông dụng, được dùng để hack Password login qua mạng, sử dụng cả 2 phương pháp [Brute Force Attack](https://anninhmang.edu.vn/thu-thap-ssh-username-password-voi-brute-force-attack/) và Dictionary Attack tại trang đăng nhập. Phần mềm hỗ trợ tấn công nhiều giao thức mạng phổ biến như SSH, Mail (POP3, IMAP), Database, SMB, VNC, LDAP…

1. **Burp Suite :**



Burp Suite là một ứng dụng nền Web, giúp kiểm tra khả năng thâm nhập. Phần mềm là công cụ mạnh mẽ, có nhiều tính năng hacking mà có thể bạn đang tìm kiếm. Dưới đây là danh sách các thành phần tính năng của Burp Suite :

**Intercepting Proxy** : tính năng này cho phép kiểm tra và chỉnh sửa tất cả các gói tin yêu cầu và phản hồi trả về của trình duyệt.

**Spider** : công cụ tiện dụng dùng để liệt kê tất cả các thư mục và tập tin trên máy chủ.

**Web Scanner** : phát hiện các lỗ hổng đang hiện hiện trên Website.

**Intruder** : tính năng cho phép tạo và tùy chỉnh các cuộc tấn công để tìm và khai thác các lỗi không mong muốn.

**Repeater** : chỉnh sửa và gửi trả lại bất cứ gói tin request riêng lẻ nào.

**Sequencer** : kiểm tra tính ngẫu nhiên của các token (csrf , authenticity\_token ).

**Extensions** : cho phép người dùng viết và add plugin tự phát triển này vào gói công cụ, hoặc download các bản plugin có sẵn để add thêm, giúp đa dạng hơn trong các cuộc tấn công.

Bản Pro cũng cho phép người dùng Donate những plugin này.

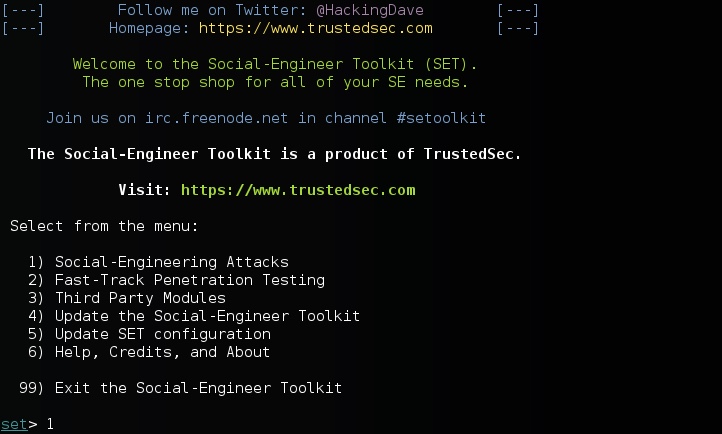
1. **OWASP Zed** :



OWASP Zed Attack Proxy ( ZAP ) được biết đến như một công cụ Proxy, có thể dự phòng khá tốt cho công cụ Burp Suite, ưu điểm của ZAP là miễn phí và mã nguồn mở.

Công cụ được phát triển với mục đích tìm những lổ hỗng trong ứng dụng Web. Với cộng đồng người dùng rộng lớn có tên OWASP security Community, người mới làm quen có thể dễ dàng sử dụng cũng như nhận được sự hỗ trợ khá tốt. Bạn có thể dùng OWASP Zed Attack Proxy để scan đối tượng, thực hiện các chiến dịch Scan tự động, tìm ra các lổ hỗng, thực hiện test thủ công…

1. **Social Engineering Toolkit** :



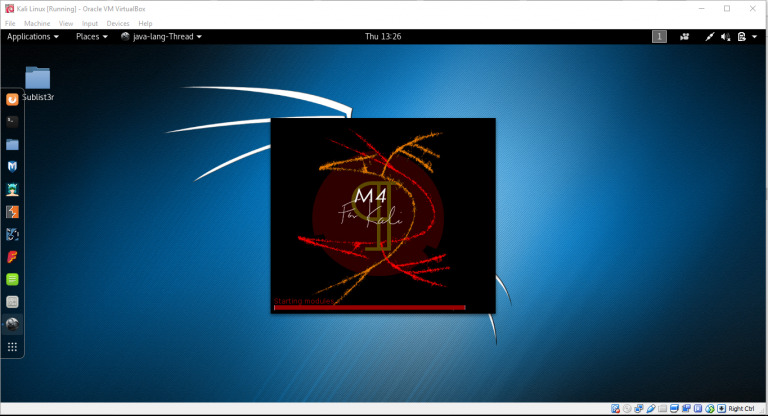
The Social-Engineering Toolkit còn được biết đến với tên thông dụng hơn là SET là công cụ hữu ích để thực hiện các cuộc tấn công nhắm vào yếu tố con người hơn là hệ thống. Công cụ có nhiều tính năng cho phép hacker gửi email, trong đó có kèm các backdoor Java applet. Phần mềm có giao diện command line và có thể chạy trên các hệ điều hành Linux, Mac OS X và Windows.

1. **Aircrack-ng** :



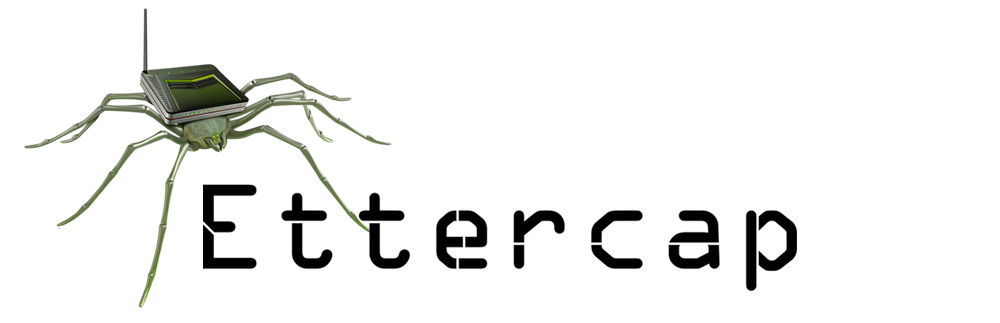
Thêm một tool để crack password, tuy nhiên đặc biệt hơn, Aircrack-ng được thiết kế để crack password Wifi. Đối với những người mới lần đầu tiếp xúc với phần mềm này, Aircrack-ng có thể phá các loại pass wifi theo chuẩn 802.11 WEP và WPA-PSK. Cơ chế hoạt động của Tool sẽ capture các gói tin có chứa password, sau đó thực hiện giải mã chúng. Aircrack-ng được xem là một trong những Tool hàng đầu trong việc bẻ khóa Password Wifi.

1. **Maltego** :



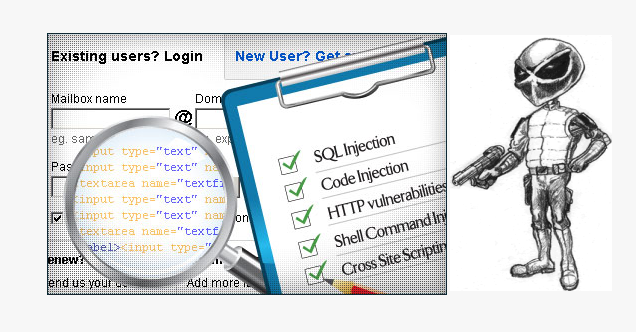
Tool này thu thập mọi dữ liệu của đối tượng từ internet như Email, Dns record… công cụ có thể thu thập dữ liệu cả cá nhân và network…

1. **Ettercap** :



Phần mềm mã nguồn mở này được cung cấp miễn phí, và thường được dùng để thực hiện các cuộc tấn công trong mạng Lan. Ettercap được dùng để phân tích các Protocol mạng và theo dõi an ninh hệ thống. Hiện phần mềm có mặt ở hầu hết các hệ điều hành như Windows, Unix, Linux BSD, và các distro khác.

1. **Nikto Website Vulnerability Scanner** :



Nikto là phần mềm mã nguồn mở, scan và tìm ra các lỗ hổng trên Web Server. Hệ thống search dựa vào cơ sở dữ liệu 6800 file / chương trình có ẩn chứa nguy hiểm, kiểm tra các hệ thống chưa được cập nhật bản vá.

Metasploit - Công cụ khai thác lỗ hổng

1. Giới thiệu Metasploit

Metasploit Framework là một môi trường dùng để kiểm tra, tấn công và khai thác lỗi của các service. Metasploit được xây dựng từ ngôn ngữ hướng đối tượng Perl, với những component được viết bằng C, assembler, và [Python](https://quantrimang.com/python). Metasploit có thể chạy trên hầu hết các hệ điều hành: [Linux](https://quantrimang.com/linux), Windows, [MacOS](https://quantrimang.com/mac-os-x). Bạn có thể download chương trình tại metasploit.com.

Metasploit có thể tự động update bắt đầu từ version 2.2 trở đi, sử dụng script **msfupdate.bat** trong thư mục cài đặt

## 2. Các thành phần của Metasploit

Metasploit hỗ trợ nhiều giao diện với người dùng:

* **Console interface:** Dùng msfconsole.bat. Msfconsole interface sử dụng các dòng lệnh để cấu hình, kiểm tra nên nhanh hơn và mềm dẻo hơn
* **Web interface:** Dùng msfweb.bat, giao tiếp với người dùng thông qua giao diện web
* **Command line interface:** Dùng msfcli.bat

Environment:

* **Global Environment:** Được thực thi thông qua 2 câu lệnh setg và unsetg, những options được gán ở đây sẽ mang tính toàn cục, được đưa vào tất cả các module exploits.
* **Temporary Environment:** Được thực thi thông qua 2 câu lệnh set và unset, environment này chỉ được đưa vào module exploit đang load hiện tại, không ảnh hưởng đến các module exploit khác.

Bạn có thể lưu lại environment mình đã cấu hình thông qua lệnh save. Môi trường đó sẽ được lưu trong /.msf/config và sẽ được load trở lại khi user interface được thực hiện.

Những options nào mà chung giữa các exploits module như là: LPORT, LHOST, PAYLOAD thì bạn nên được xác định ở Global Environment.

Ví dụ:



## **3. Cách sử dụng Metasploit framework**

**3.1. Chọn module exploit:**

Lựa chọn chương trình, dịch vụ lỗi mà Metasploit có hỗ trợ để khai thác.

* **show exploits:** Xem các module exploit mà framework có hỗ trợ
* **use exploit\_name:** Chọn module exploit
* **info exploit\_name**: Xem thông tin về module exploit

Bạn nên cập nhật thường xuyên các lỗi dịch vụ trên metasploit.com hoặc qua script msfupdate.bat

**3.2. Cấu hình module exploit đã chọn:**

* **show options:** Xác định những options nào cần cấu hình
* **set**: Cấu hình cho những option của module đó

Một vài module còn có những advanced options, bạn có thể xem bằng cách gõ dòng lệnh **show advanceds**

**3.3. Xác nhận những option vừa cấu hình:**

* **check:** Kiểm tra xem những option đã được set chính xác chưa.

**3.4. Lựa chọn mục tiêu:**

Lựa chọn hệ diều hành muốn thực hiện.

* **show targets:** những target được cung cấp bởi module đó.
* **set**: xác định target nào

Ví dụ:



Exploit sẽ liệt kê ra những target như: winxp, winxp SP1, win2000, win2000 SP1

**3.5. Lựa chọn payload:**

Payload là đoạn code mà sẽ chạy trên hệ thống máy tính được điều khiển từ xa.

* **show payloads:** Liệt kê ra những payload của module exploit hiện tại
* **info payload\_name:** Xem thông tin chi tiết về payload đó
* **set PAYLOAD payload\_name:** Xác định payload module name.Sau khi lựa chọn payload nào, dùng lệnh show option để xem những option của payload đó
* **show advanced:** Xem những advanced option của payload đó.

**3.6. Thực thi exploit:**

* **exploit:** Lệnh dùng để thực thi payload code. Payload sau đó sẽ cung cấp cho bạn những thông tin về hệ thống được khai thác.

## 4. **Giới thiệu payload meterpreter**

Meterpreter, viết tắt từ Meta-Interpreter là một advanced payload có trong Metasploit framework. Muc đích của nó là để cung cấp những tập lệnh để khai thác, tấn câng các máy remote computers. Nó được viết từ các developers dưới dạng shared object (DLL) files. Meterpreter và các thành phần mở rộng được thực thi trong bộ nhớ, hoàn toàn không được ghi lên đĩa nên có thể tránh được sự phát hiện từ các phần mềm chống virus.

Meterpreter cung cấp một tập lệnh để chúng ta có thể khai thác trên các remote computer:

* **Fs:** Cho phép upload và download files từ các remote machine
* **Net:** Cho phép xem thông tin mạng của remote machine như IP, route table
* **Process:** Cho phép tạo các processes mới trên remote machine
* **Sys:** Cho phép xem thông tin hệ thống của remote machine

**Sử dụng câu lệnh:**

* use -m module1,module2,module3 [ -p path ] [ -d ]: Câu lệnh use dùng để load những module mở rộng của meterpreter như: Fs, Net, Process.
* loadlib -f library [ -t target ] [ -lde ]: Câu lệnh cho phép load các thư viện của remote machines.
* read channel\_id [length]: Lệnh read cho phép xem dữ liêu của remote machine trên channel đang kết nối.
* write channel\_id: Lệnh write cho phép ghi dữ liệu lên remote machine.
* close channel\_id: Đóng channel mà đã kết nối với remote computer.
* interact channel\_id: Bắt đầu một phiên làm việc với channel vừa thiết lập với remote machine.
* initcrypt cipher [parameters]: Mã hoá dữ liệu được gửi giữa host và remote machine.

**Sử dụng module Fs:** Cho phép upload và download files từ các remote machine.

* cd directory: Giống lệnh cd của [command line](https://quantrimang.com/nhung-lenh-dos-pho-bien-trong-cmd-118351)
* getcwd: Cho biết thư mục đang làm việc hiện tại
* ls [filter\_string]: liệt kê các thư mục và tập tin
* upload src1 [src2 ...] dst: Upload file
* download src1 [src2 ...] dst: Download file

**Sử dụng module Net:**

* ipconfig
* route: Xem bảng định tuyến của remote machine.
* portfwd [ -arv ] [ -L laddr ] [ -l lport ] [ -h rhost ] [ -p rport ] [ -P ]: Cho phép tạo port forward giữa host và remote machine.

**Sử dụng module Process:**

* execute -f file [ -a args ] [ -Hc ]: Câu lệnh execute cho phép bạn tạo ra một process mới trên remote machine và sử dụng process đó để khai thác dữ liệu
* kill pid1 pid2 pid3: Huỷ những process đang chạy trên máy remote machine
* ps: Liệt kê những process của remote machine.

**Sử dụng module Sys:**

* getuid: Cho biết username hiện tại của remote machine
* sysinfo: Cho biết thông tin về tên máy tính, hệ điều hành.

[**https://quantrimang.com/tat-tan-tat-ve-nmap-157752**](https://quantrimang.com/tat-tan-tat-ve-nmap-157752)

[**https://cuongquach.com/nmap-la-gi-cong-cu-quet-mang.html**](https://cuongquach.com/nmap-la-gi-cong-cu-quet-mang.html)

[**https://www.mystown.com/2016/03/huong-dan-su-dung-nmap-e-scan-port-tren.html**](https://www.mystown.com/2016/03/huong-dan-su-dung-nmap-e-scan-port-tren.html)

[**https://123doc.org/document/4003918-do-an-tot-nghiep-danh-gia-bao-mat-he-thong-mang-cong-cu-kali-linux.htm**](https://123doc.org/document/4003918-do-an-tot-nghiep-danh-gia-bao-mat-he-thong-mang-cong-cu-kali-linux.htm)