|  |  |
| --- | --- |
| Logo  Description automatically generated | BÀI TẬP KIỂM TRA 01  Khai thác lỗ hổng Website |

Họ và tên Sinh viên: Mã Sinh viên:

Nhóm học phần:

* Sinh viên tải file Word đề thi này về
* Đặt tên file (Tiếng Việt KHÔNG dấu): TenNhom-ATTT-MaSV.docx

Ví dụ: ***Nh20.12-ATTT-102334455.docx***

* Trình bày kết quả khai thác lổ hổng trong file và nộp lại theo LINK07
* Không công bố các kết quả trên mạng.

ĐỀ BÀI

Mỗi SV sử dụng các nội dung kiểm thử như dưới để thực hiện khai thác lổ hổng của Website do SV.

1) Trình bày các lệnh/các bước thao tác sử dụng các công cụ như dưới, chụp hình các kết quả thực hiện theo từng công cụ.

2) Phân tích/nhận xét kết quả.

*>> Lọc bỏ các thông tin chung, chọn các thông tin liên quan đến đối tượng khai thác.*

# Chuẩn bị

1. Tải hệ điều hành VMKaliLinux2023 hoặc VMKaliLinux2024 từ LINK03
2. Cài đặt VMware-workstation và chạy máy ảo
3. Tuy xuất ssh và sử dụng công cụ của Kali Linux để pentest địa chỉ của một Website do SV chọn
4. Tham khảo nội dung trong *Lab06 Khai thác các công cụ của Kali Linux*

# Quá trình Information Gathering

## Công cụ dmitry lấy thông tin Website

Lệnh thực hiện:

Hình 2.1. Kết quả

## Công cụ whois thu thập thông tin máy chủ

Hình 2.2. Kết quả ...

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

Hình 2.3. Kết quả ...

## Công cụ DNSenum thu thập thông tin DNS

Hình 2.4. Kết quả ...

## Các công cụ khác (nếu có)

# Quá trình Scanning

## Công cụ nmap

## Các công cụ khác (nếu có)

# Quá trình Vulnerability Analysis

## Công cụ uniscan quét lỗi bảo mật Website

## Công cụ nikto dò tìm lỗi website

## Công cụ skipfish

## Công cụ gobuster

## Công cụ sitadel

## Công cụ darkjumper

## Công cụ amap

## Các công cụ khác (nếu có)

# Quá trình Web application analysis

## Công cụ sqlmap phân tích lỗ hổng SQL

## Công cụ tlssled

## Công cụ xsser khai thác lỗi XSS

## Các công cụ khác (nếu có)

# Quá trình GUI Web application analysis

# Tổng hợp kết quả kiểm thử xâm nhập

....

|  |  |  |
| --- | --- | --- |
| **TT** | **Nội dung** | **Kết quả** |
|  | Tên miền & địa chỉ IPv4, IPv6 |  |
|  | Máy chủ |  |
|  | Các cổng dịch vụ và trạng thái |  |
|  | Các dịch vụ trên Server và phiên bản |  |
|  | Các lổ hổng |  |
|  | Thông tin tài khoản |  |
|  | Kết quả thăm dò tấn công |  |
|  | ... |  |

Nhận xét

1)

2)

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

Danh sách Website

|  |  |  |
| --- | --- | --- |
| **Mã SV** | **Họ và Tên** | **Website quét** |
|  |  | http://demo.testfire.net |
|  |  | http://php.testsparker.com |
|  |  | http://testasp.vulnweb.com |
|  |  | http://testphp.vulnweb.com |
|  |  | http://zero.webappsecurity.com |
|  |  | http://testhtml5.vulnweb.com |
|  |  | http://aspnet.testsparker.com |

MỤC LỤC

[1. Chuẩn bị 1](#_Toc176347632)

[2. Quá trình Information Gathering 1](#_Toc176347633)

[2.1 Công cụ dmitry lấy thông tin Website 1](#_Toc176347634)

[2.2 Công cụ whois thu thập thông tin máy chủ 1](#_Toc176347635)

[2.3 Công cụ sslscan liệt kê các bộ mã hóa và chứng chỉ trên máy chủ 2](#_Toc176347636)

[2.4 Công cụ DNSenum thu thập thông tin DNS 2](#_Toc176347637)

[2.5 Các công cụ khác (nếu có) 2](#_Toc176347638)

[3. Quá trình Scanning 2](#_Toc176347639)

[3.1 Công cụ nmap 2](#_Toc176347640)

[3.2 Các công cụ khác (nếu có) 2](#_Toc176347641)

[4. Quá trình Vulnerability Analysis 2](#_Toc176347642)

[4.1 Công cụ uniscan quét lỗi bảo mật Website 2](#_Toc176347643)

[4.2 Công cụ nikto dò tìm lỗi website 2](#_Toc176347644)

[4.3 Công cụ skipfish 2](#_Toc176347645)

[4.4 Công cụ gobuster 2](#_Toc176347646)

[4.5 Công cụ sitadel 2](#_Toc176347647)

[4.6 Công cụ darkjumper 2](#_Toc176347648)

[4.7 Công cụ amap 3](#_Toc176347649)

[4.8 Các công cụ khác (nếu có) 3](#_Toc176347650)

[5. Quá trình Web application analysis 3](#_Toc176347651)

[5.1 Công cụ sqlmap phân tích lỗ hổng SQL 3](#_Toc176347652)

[5.2 Công cụ tlssled 3](#_Toc176347653)

[5.3 Công cụ xsser khai thác lỗi XSS 3](#_Toc176347654)

[5.4 Các công cụ khác (nếu có) 3](#_Toc176347655)

[6. Quá trình GUI Web application analysis 3](#_Toc176347656)

[7. Tổng hợp kết quả kiểm thử xâm nhập 3](#_Toc176347657)

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