**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA CÔNG NGHỆ THÔNG TIN**



Học phần: **An toàn mạng nâng cao**

Bài báo cáo

**Nghiên cứu**

**Giảng viên**: TS. Đặng Minh Tuấn

**Sinh viên thực hiện:** Nhóm 07

Nguyễn Tuấn Anh B17DCAT008

Tô Văn Quyền B17DCAT151

Nguyễn Thu Thảo B17DCAT170

Lê Tiến Đạt B17DCAT034

Nguyễn Văn Thanh B17DCAT166

Hà Nội 05/2021

MỤC LỤC

[MỤC LỤC 2](#_Toc71125216)

[DANH SÁCH CÁC THUẬT NGỮ TIẾNG ANH VÀ VIẾT TẮT 4](#_Toc71125217)

[DANH MỤC CÁC HÌNH ẢNH 5](#_Toc71125218)

[DANH MỤC BẢNG BIỂU 6](#_Toc71125219)

[CHƯƠNG 1. GIỚI THIỆU CÔNG CỤ NIKTO 7](#_Toc71125220)

[1.1. Tổng quan về Nikto 7](#_Toc71125221)

[CHƯƠNG 2. CƠ SỞ LÝ THUYẾT CỦA HÌNH THỨC TẤN CÔNG DOS 9](#_Toc71125222)

[2.1. Tổng quan lý thuyết về phương thức tấn công DOS 9](#_Toc71125223)

[2.1.1. Khái niệm phương thức tấn công DOS 9](#_Toc71125224)

[2.1.2. Lịch sử phương thức tấn công DOS 9](#_Toc71125225)

[2.1.3. Cách thức hoạt động của phương thức tấn công DOS 10](#_Toc71125226)

[2.1.4. Biểu hiện khi bị tấn công DOS 11](#_Toc71125227)

[2.2. Một số kỹ thuật tấn công DOS phổ biến 11](#_Toc71125228)

[2.2.1. SYN Flood 11](#_Toc71125229)

[2.2.2. UDP Flood 14](#_Toc71125230)

[2.2.3. Buffer overflow attacks 15](#_Toc71125231)

[2.2.4. ICMP flood 15](#_Toc71125232)

[2.2.5. Slowloris 15](#_Toc71125233)

[CHƯƠNG 3. MÔ HÌNH THỰC NGHIỆM TẤN CÔNG DOS 18](#_Toc71125234)

[3.1. Mô hình thực nghiệm tấn công DOS sử dụng công cụ UDP Flood 18](#_Toc71125235)

[3.1.1. Mô hình thực nghiệm 18](#_Toc71125236)

[3.1.2. Giới thiệu các phần mềm và công cụ được sử dụng 19](#_Toc71125237)

[3.1.2.1. Phần mềm Nmap 19](#_Toc71125238)

[3.1.2.2. Công cụ DOS UDP Flood 20](#_Toc71125239)

[3.1.2.3. Phần mềm Wireshark 20](#_Toc71125240)

[3.1.3. Quy trình thực nghiệm mô hình 21](#_Toc71125241)

[3.2. Mô hình thực nghiệm tấn công DOS sử dụng công cụ Tor’s Hammer 21](#_Toc71125242)

[3.2.1. Mô hình thực nghiệm 21](#_Toc71125243)

[3.2.2. Giới thiệu các phần mềm và công cụ được sử dụng 23](#_Toc71125244)

[3.2.2.1. Tor’s hammer 23](#_Toc71125245)

[3.2.2.2. Cách sử dụng 24](#_Toc71125246)

[CHƯƠNG 4. THỰC NGHIỆM VÀ ĐÁNH GIÁ 26](#_Toc71125247)

[4.1. Thực nghiệm và đánh giá mô hình tấn công DOS sử dụng công cụ UDP Flood 26](#_Toc71125248)

[4.1.1. Thực nghiệm tấn công 26](#_Toc71125249)

[4.1.1. Đánh giá kết quả thực nghiệm 32](#_Toc71125250)

[4.2. Thực nghiệm và đánh giá mô hình tấn công DOS sử dụng công cụ Tor’s Hammer 32](#_Toc71125251)

[4.2.1. Thực nghiệm tấn công 32](#_Toc71125252)

[4.2.1. Đánh giá kết quả thực nghiệm 35](#_Toc71125253)

[KẾT LUẬN 37](#_Toc71125254)

[DANH MỤC TÀI LIỆU THAM KHẢO 38](#_Toc71125255)

DANH SÁCH CÁC THUẬT NGỮ TIẾNG ANH VÀ VIẾT TẮT

|  |  |
| --- | --- |
| **Thuật ngữ viết tắt** | **Thuật ngữ đầy đủ** |
| CPU | Central Processing unit |
| DNS | Domain Name System |
| DOS | Denial of Service |
| FTP | File Tranfer Protocol |
| HTTP | Hypertext Transfer Protocol |
| ICMP | Internet Control Message Protocol |
| IP | Internet Protocol |
| LAN | Local Area Network |
| OWASP | The Open Web Application Security Project |
| ping | Packet Internet Grouper (Groper) |
| SQL | Structured Query Language |
| SYN | synchronization |
| TOR | The Onion Router |
| UDP | User Datagram Protocol |
| URL | Uniform Resource Locator |
| XSS | Cross-Site Scripting |
| XXE | XML External Entities |

DANH MỤC CÁC HÌNH ẢNH

[Hình 1.1. Minh hoạ hai hình thức tấn công DOS và DDOS 7](#_Toc57129283)

[Hình 2.1. Minh hoạ quá trình bắt tay ba bước của giao thức TCP thông thường 11](#_Toc57129284)

[Hình 2.2. Minh hoạ quá trình tấn công SYN flood 12](#_Toc57129285)

[Hình 2.3. Minh hoạ quá trình tấn công UDP flood 13](#_Toc57129286)

[Hình 2.4. Minh hoạc quá trình tấn công Slowloris Attack 15](#_Toc57129287)

[Hình 3.1. Mô hình thực nghiệm tấn công DOS UDP Flood 17](#_Toc57129288)

[Hình 3.2. Phần mềm Nmap 18](#_Toc57129289)

[Hình 3.3. Quá trình thực thi công cụ DOS UDP Flood 19](#_Toc57129290)

[Hình 3.4. Phầm mền Wireshark 19](#_Toc57129291)

[Hình 3.5. Mô hình tấn công sử dụng công cụ Tor’s hammer 21](#_Toc57129292)

[Hình 3.6. Mô tả mạng Tor 22](#_Toc57129293)

[Hình 3.7. Các tập tin của công cụ Tor's Hammer 23](#_Toc57129294)

[Hình 3.8. Thực thi công cụ Tor's Hammer 23](#_Toc57129295)

[Hình 3.9. Các tuỳ trọn của công cụ Tor's Hammer 24](#_Toc57129296)

[Hình 4.1. Mô hình thực nghiệm tấn công DOS UDP Flood 25](#_Toc57129297)

[Hình 4.2. Cửa sổ thực thi công cụ DOS UDP Flood 26](#_Toc57129298)

[Hình 4.3. Các gói tin được Wireshark trên luồng mạng. 27](#_Toc57129299)

[Hình 4.4. Trình quản lý tác vụ của máy nạn nhân 28](#_Toc57129300)

[Hình 4.5. Kết quả đo lưu lượng mạng trước khi bị tấn công 29](#_Toc57129301)

[Hình 4.6. Kết quả đo lưu lượng mạng khi bị tấn công 30](#_Toc57129302)

[Hình 4.7. Mô hình thực nghiệm tấn công DOS Tor’s Hammer 31](#_Toc57129303)

[Hình 4.8. Kết quả quét Nmap trên máy nạn nhân 32](#_Toc57129304)

[Hình 4.9. Cửa sổ thực thi công cụ Tor’s Hammer 33](#_Toc57129305)

[Hình 4.10. Trình quản lý tác vụ của máy nạn nhân 33](#_Toc57129306)

DANH MỤC BẢNG BIỂU

[Bảng 4.1. Ưu và nhược điểm của công cụ Tor's Hammer 35](#_Toc57129307)

CHƯƠNG 1. GIỚI THIỆU CÔNG CỤ NIKTO VÀ CÀI ĐẶT

* 1. Tổng quan về Nikto

Là một phần mềm mã nguồn mở với tính năng Web Server Scanner, tính năng kiểm tra các máy chủ Web. Bao gồm hơn 3200 phương thức nhận diện các file, lỗi logic nguy hiểm, hỗ trợ hơn 625 phiên bản Web Server, bao gồm những lỗi trên 230 Web Server khác nhau. Tính năng Scan kết hợp với các Plugins luôn được update tự động đảm bảo đưa ra kết quả đầy đủ và chính xác nhất. Là một công cụ rất hữu hiệu nhưng không được update thường xuyên. Các lỗi mới nhất thường được update chậm và không thể tìm thấy. Kiểm tra một host web để tìm các vấn đề tiềm năng và lỗ hổng bảo mật, bao gồm:

* Host và phần mềm cấu hình sai.
* Tập tin và các chương trình mặc định.
* Tập tin và các chương trình không an toàn.
* Các host và các chương trình lỗi thời.

Nikto được xây dựng trên LibWhisker và có thể chạy trên bất kỳ nền tảng trong đó có môi trường Perl. Nó hỗ trợ SSL, proxy, xác thực, mã hóa tấn công và nhiều hơn nữa. Nó có thể được cập nhật tự động từ dòng lệnh.

* 1. Lịch sử

Nikto 1.00 Beta được phát hành vào ngày 27 Tháng Mười Hai năm 2001, (gần như ngay sau đó phát hành 1,01). Trong suốt hai năm Nikto là phần mềm kiểm thử miễn phí phát triển nhất. Phiên bản 2.0 được phát hành trong tháng mười một năm 2007. Hiện tại phiên bản mới nhất là 2.1.6.

Nikto được viết và duy trì bởi Chris Sullo và David Lodge. LibWhisker được viết và duy trì bởi Jeff Forristal (Rain Forrest Puppy).

* 1. Cài đặt

1. Yêu cầu:

Bất kỳ hệ thống nào hỗ trợ Perl cơ bản đều cho phép cài đặt Nikto. Nó đã được thử nghiệm rộng rãi trên:

* + Windows (sử dụng ActiveState Perl và Strawberry Perl). Một số tính năng POSIX, chẳng hạn như các lệnh tương tác có thể không làm việc với Windows.
  + Mac OSX.
  + Và một số hệ điều hành khác như Linux và Unix (bao gồm cả RedHat, Solaris, Debian, Ubuntu, Backtrack, vv).

b) Cài đặt:

- Tải chương trình Nikto về:

# wget <https://cirt.net/nikto/nikto-2.1.5.tar.gz>

Ta tiếp tục tiến hành giải nén và chạy chương trình Nikto:

# tar zxvf nikto-2.1.5.tar.gz

# cd nikto-2.1.5

# perl nikto.pl

- Trên máy tính đang chạy kali linux hoặc các phiên bản phân phối khác của Kali.

Truy cập theo thứ tự Kali Linux -> Vulnerability Analysis -> Misc Scanners -> nikto.

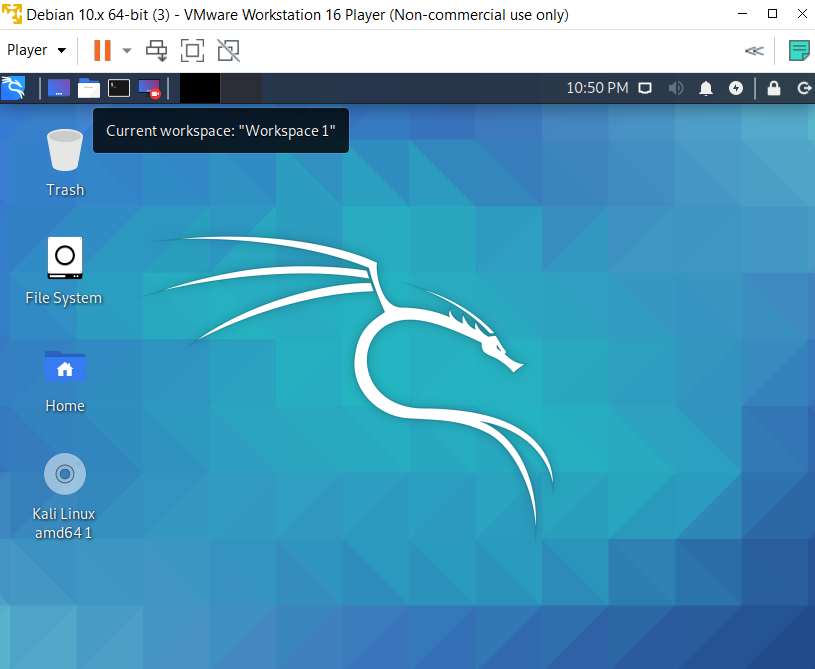
CHƯƠNG 2. Tổng hợp LAB

2.1. Lab 1: Http scanning with Nikto (Lê Tiến Đạt)

Case Study:Sử dụng Nikto trên Kali Linux để quét các lỗ hổng bảo mật của trang web <http://www.sieuthinhua.vn/> trên cổng TCP 80.

*Procedure:*

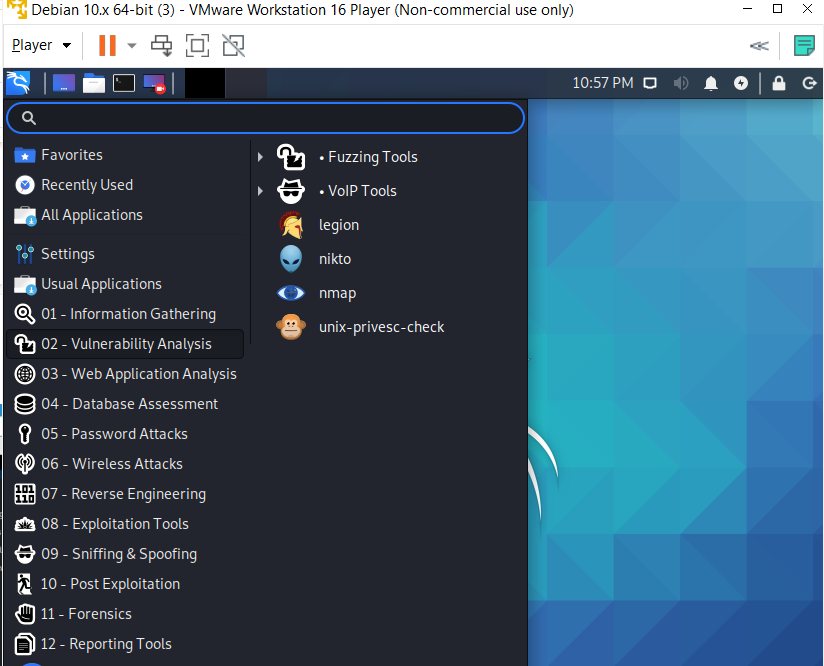
- Bước1: Đăng nhập vào Kali linux sau đó sẽ chuyển qua giao diện chính của hệ điều hành



Hình 1: Lab 1-Giao diện chính của Kali Linux

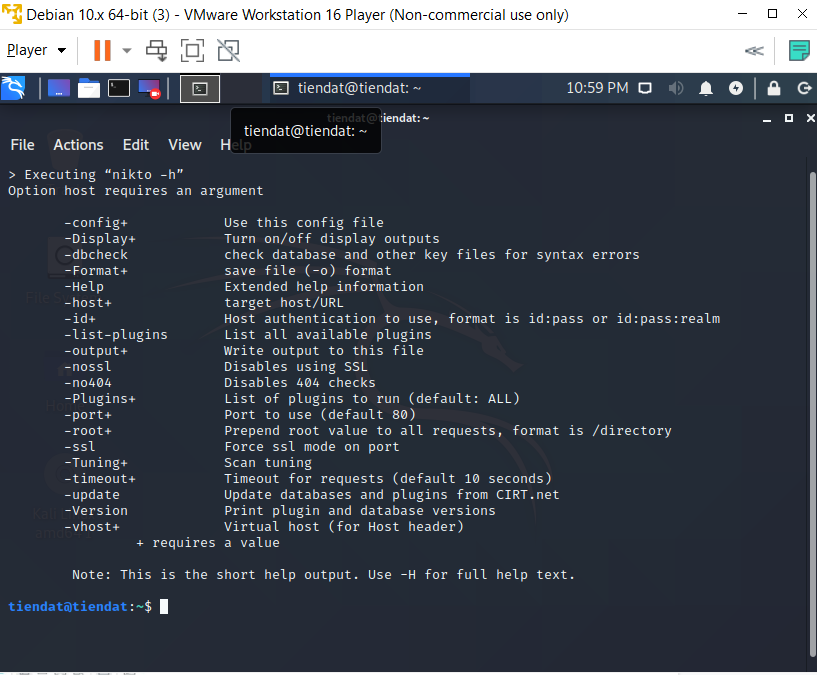
- Bước 2: Khởi động Nikto

Application Vulnerability Analysis Nikto



Hình 2: Lab 1-Khởi động Nikto

- Ứng dụng Nikto hiển thị các Option

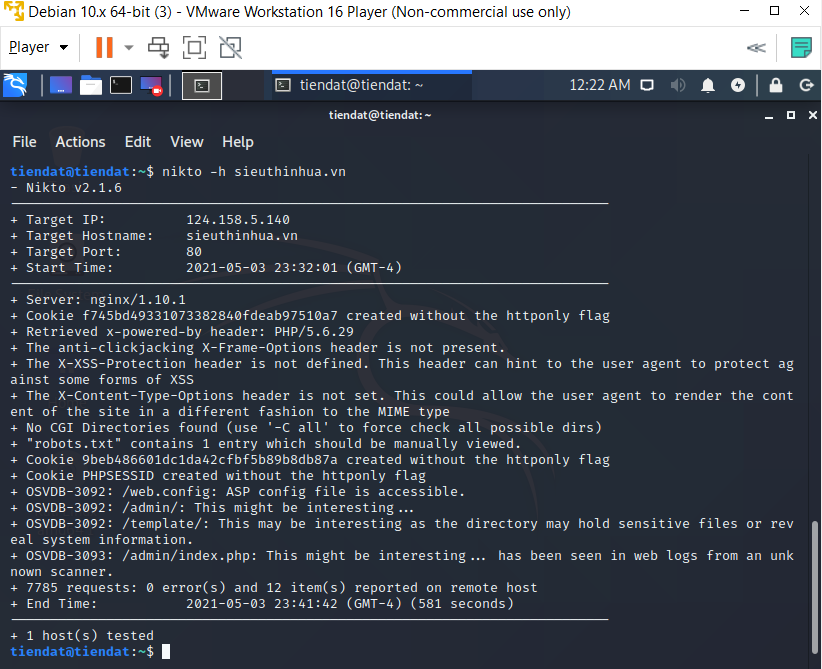


Hình 3: Lab 1-Giao diện tùy chọn của Nikto

- Bước 3: Tiến hành quét tìm

Tìm lỗ hổng của trang web <http://www.sieuthinhua.vn/>

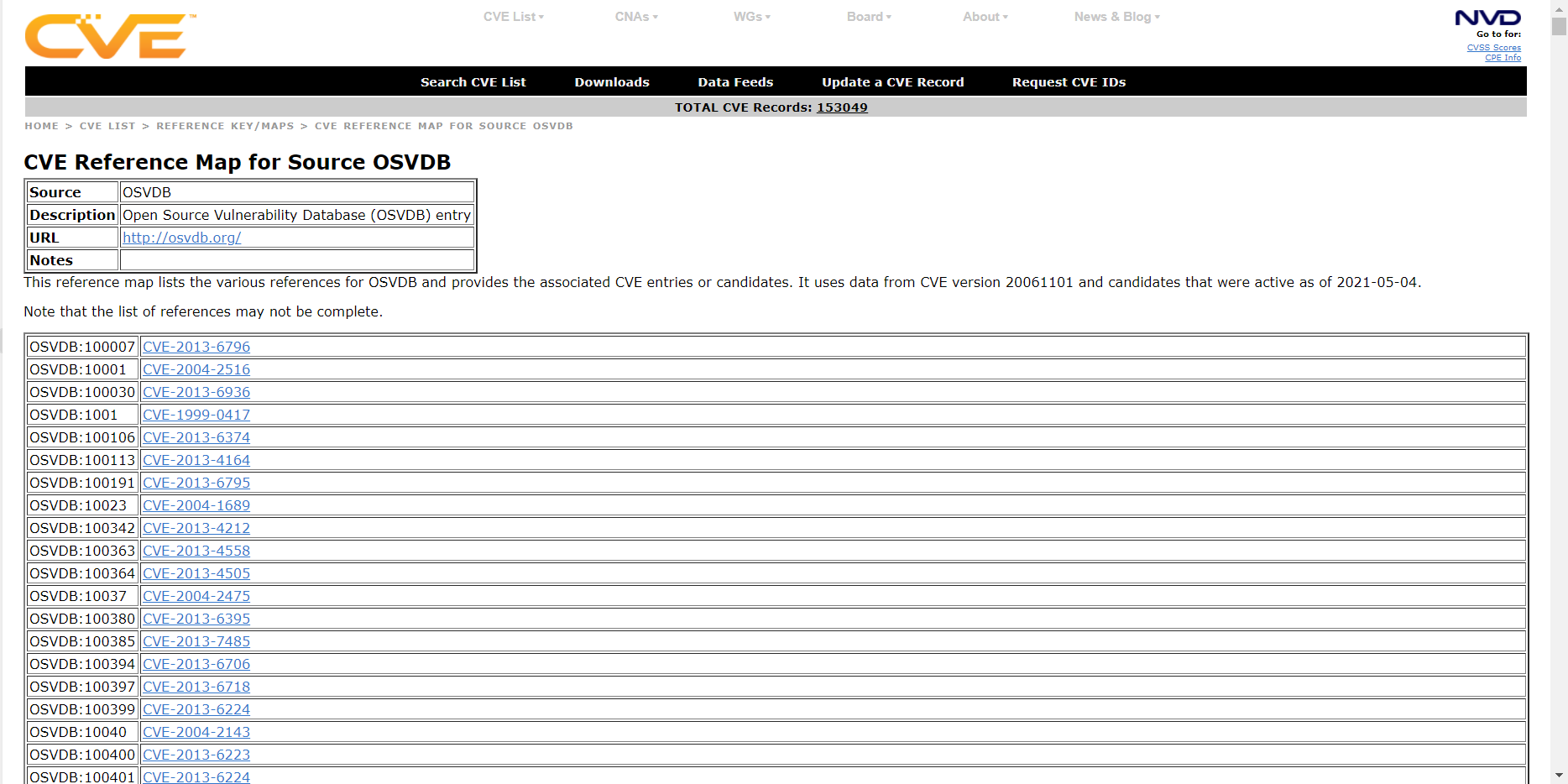
* Nginx Web Server
* Phiên bản PHP/5.6.29
* Phát hiện các lỗi OSVDB: [OpenSourceVulnerabilitiesDatabase](http://osvdb.org/)



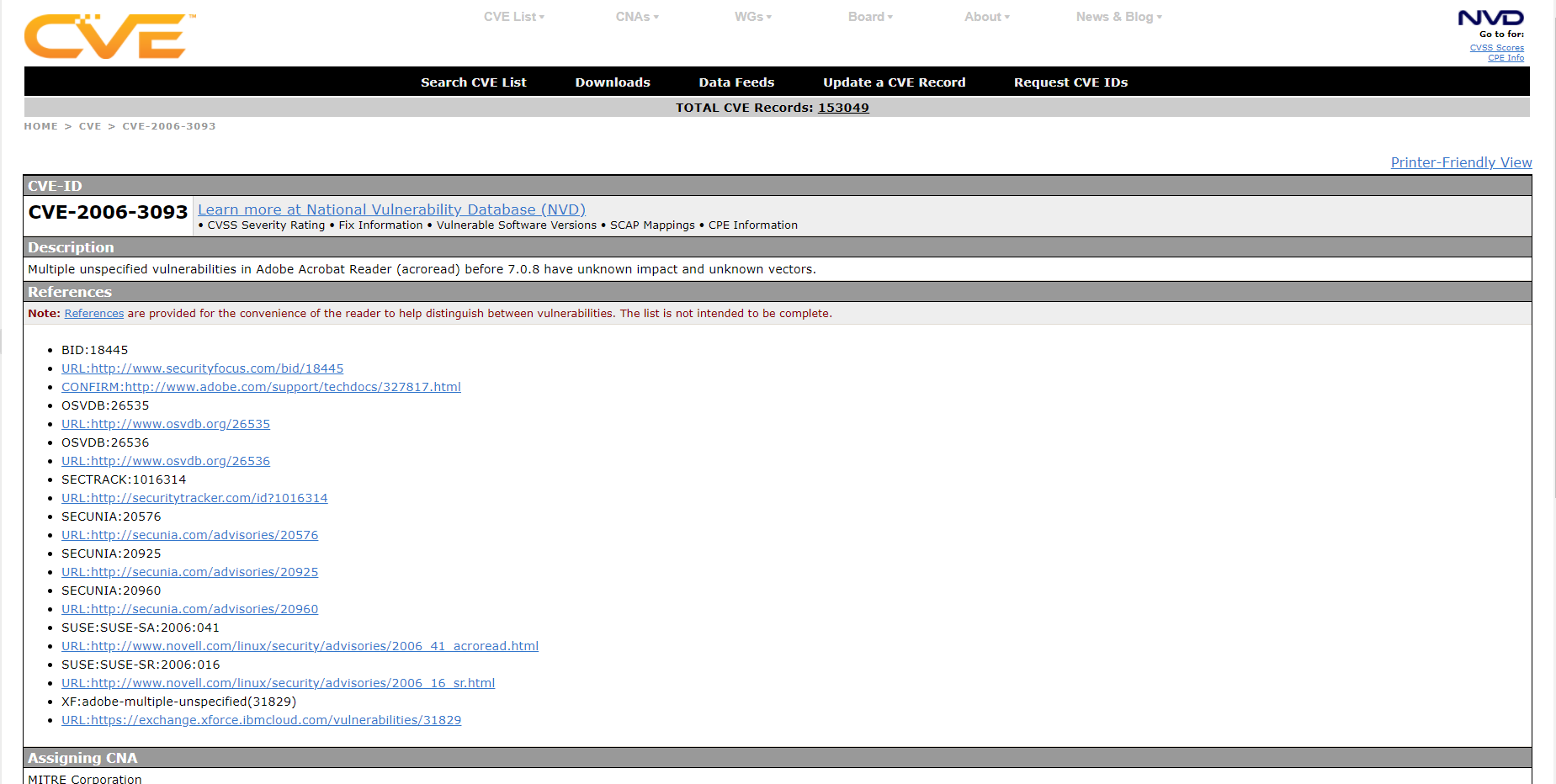
Hình 4: Lab1-Scanning Website http://www.sieuthinhua.vn/

Để đọc thêm thông tin về các lỗi bảo mật OSVDB ta truy cập trang web:

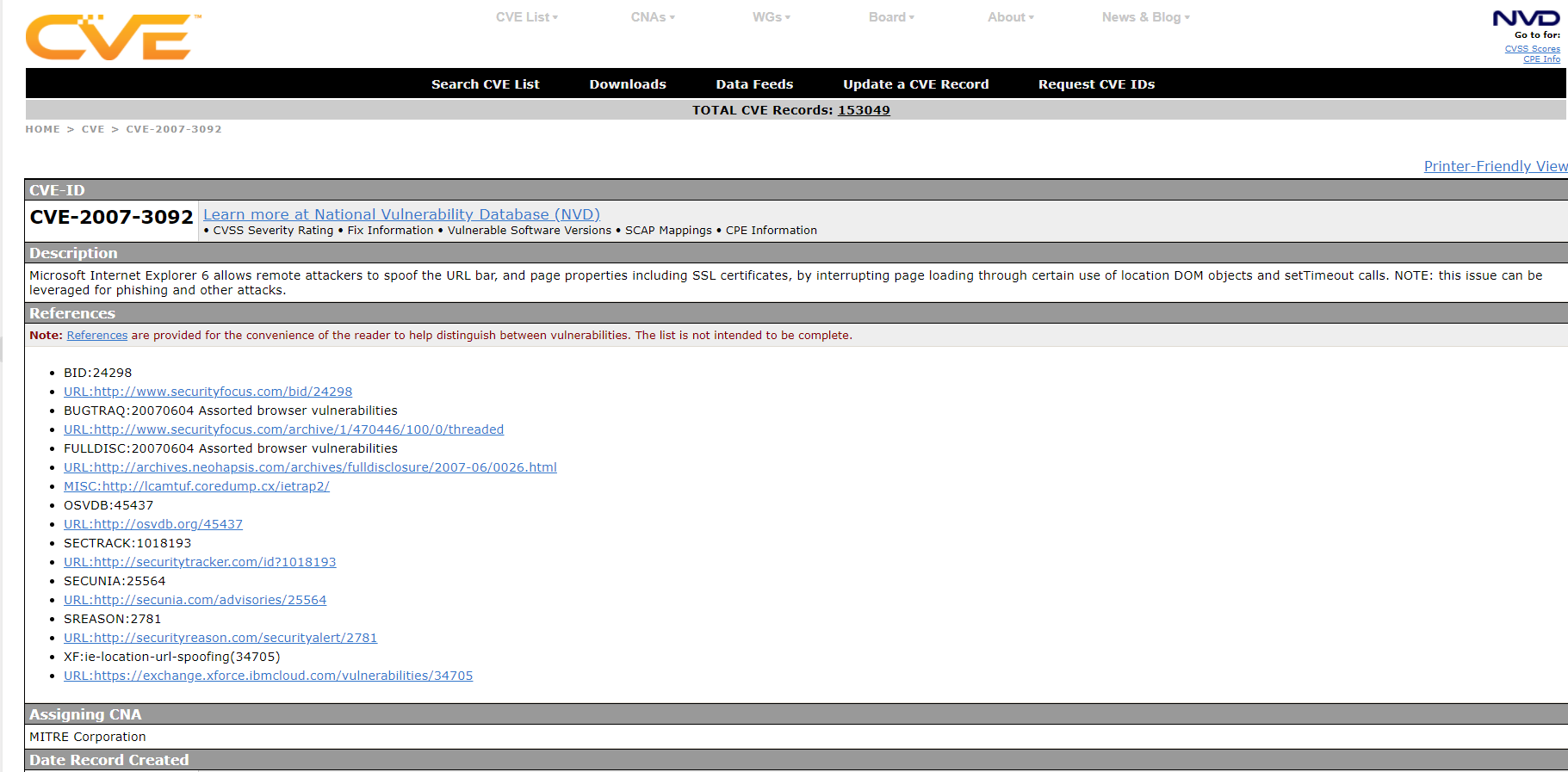
<https://cve.mitre.org/data/refs/refmap/source-OSVDB.html>



Hình 5: Lab 1-Truy cập vào CVE Reference Map for Source OSVDB



Hình 6: Lab 1-Thông tin về lỗi bảo mật OSVDB-3093



Hình 7: Thông tin về lỗi bảo mật OSVDB-3093

2.2. Lab 2: CGI Scanning with Nikto (Nguyễn Thu Thảo)

Case Study:Sử dụng Nikto trên Kali Linux để quét các lỗ hổng bảo mật của trang web <http://www.sieuthinhua.vn/> trên cổng TCP 80.

*Procedure:*

DANH MỤC TÀI LIỆU THAM KHẢO

[1] “Tình hình an ninh mạng qua những số liệu mới nhất,” *CyStack Resources*, Oct. 19, 2018. https://resources.cystack.net/tinh-hinh-an-ninh-mang/ (accessed Nov. 23, 2020).

[2] S. User, “Continuity Central.” https://www.continuitycentral.com/ (accessed Nov. 23, 2020).

[3] “Understanding Denial-of-Service Attacks | CISA.” https://us-cert.cisa.gov/ncas/tips/ST04-015 (accessed Nov. 18, 2020).

[4] “Distributed Denial of Service Attacks - The Internet Protocol Journal - Volume 7, Number 4 - Cisco,” Aug. 26, 2019. https://web.archive.org/web/20190826143507/https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-30/dos-attacks.html (accessed Nov. 18, 2020).

[5] “Denial-of-service attack,” *Wikipedia*. Nov. 16, 2020, Accessed: Nov. 18, 2020. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Denial-of-service\_attack&oldid=989006172.

[6] “Article: What is... Denial-of-Service (DoS) | F-Secure.” https://www.f-secure.com/v-descs/articles/denial-of-service.shtml (accessed Nov. 19, 2020).

[7] “SYN flood,” *Wikipedia*. Sep. 24, 2020, Accessed: Nov. 19, 2020. [Online]. Available: https://en.wikipedia.org/w/index.php?title=SYN\_flood&oldid=980118288.

[8] “UDP Flood DDoS Attack,” *Cloudflare*. https://www.cloudflare.com/learning/ddos/udp-flood-ddos-attack/ (accessed Nov. 19, 2020).

[9] “Denial-of-Service (DoS) Attacks — Web-based App Security,” *Spanning*, Jun. 16, 2020. https://spanning.com/blog/denial-of-service-attacks-web-based-application-security-part-7/ (accessed Nov. 19, 2020).

[10] “What is an ICMP Flood Attack?,” *NETSCOUT*. https://www.netscout.com/what-is-ddos/icmp-flood (accessed Nov. 19, 2020).

[11] “Slowloris DDoS Attack,” *Cloudflare*. https://www.cloudflare.com/learning/ddos/ddos-attack-tools/slowloris/ (accessed Nov. 19, 2020).

[12] “Leeon123/TCP-UDP-Flood,” *GitHub*. https://github.com/Leeon123/TCP-UDP-Flood (accessed Nov. 19, 2020).