BÁO CÁO THỰC HÀNH

**Môn học: IDPS**

**Lab 3: Viết rule trên Snort**

*GVHD: Đỗ Hoàng Hiển*

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

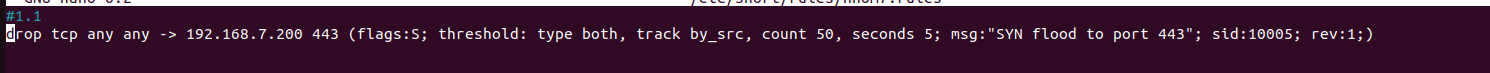
Lớp: NT204.N21.ATCL

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Hoàng Văn Anh Đức | 20520890 | 20520890@gm.uit.edu.vn |
| 2 | Nguyễn Mạnh Cường | 20520421 | 20520421@gm.uit.edu.vn |
| 3 | Lê Quang Minh | 20520245 | 20520245@gm.uit.edu.vn |

1. **NỘI DUNG THỰC HIỆN:[[1]](#footnote-1)**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Công việc** | **Thành viên thực hiện** | **Kết quả tự đánh giá** |
| 1 | 1.1 | Đức+Cường | 100% |
| 2 | 1.2 | Đức+Cường | 100% |
| 3 | 1.3 | Đức+Cường | 100% |
| 4 | 1.4 | Đức+Cường | 100% |
| 5 | 1.5.1 | Đức+Cường | 100% |
| 6 | 1.5.2 | Đức+Cường | 100% |

Text

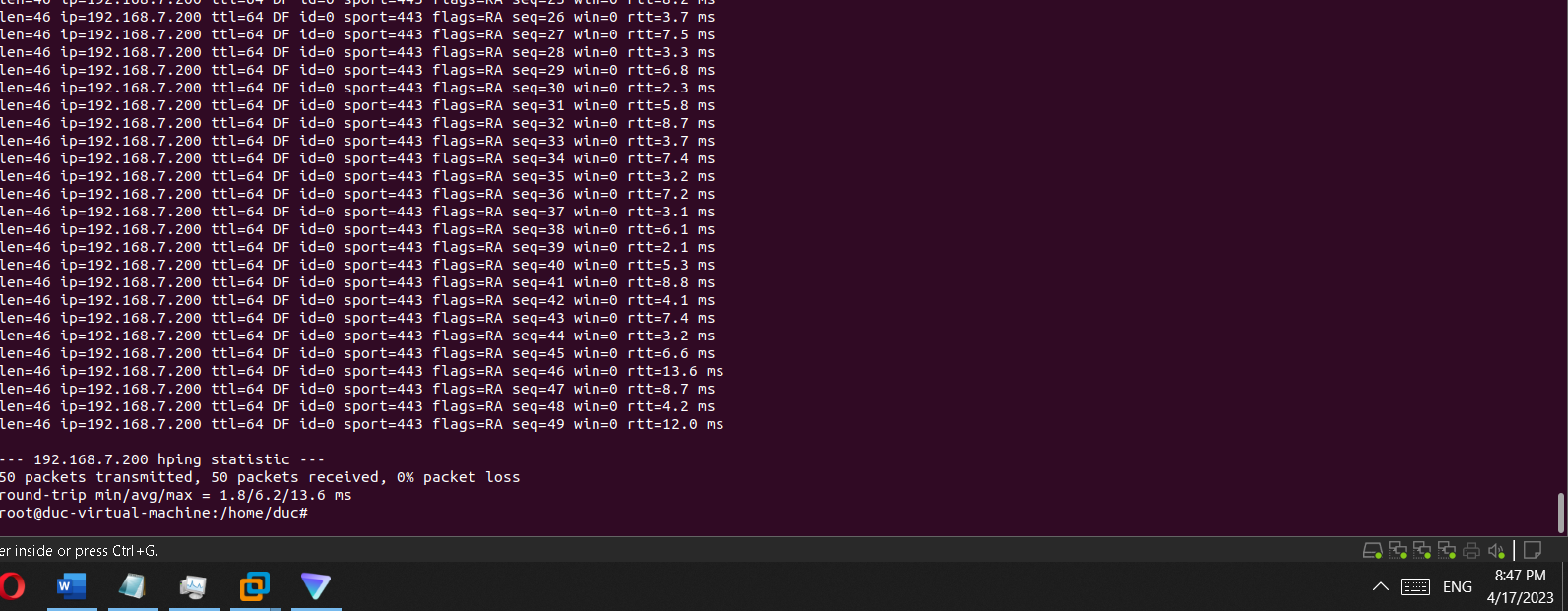
Description automatically generated

**drop tcp any any -> 192.168.7.200 443 (flags:S; threshold: type both, track by\_src, count 50, seconds 5; msg:"SYN flood to port 443"; sid:10005; rev:1;)**

* **Flags**: S: chỉ xử lý các gói có cờ SYN được đặt
* **threshold**: type both, track by\_src, count 50, seconds 5;: đặt ngưỡng giới hạn 50 gói trong 5 giây
* **type both**: giới hạn số lượng gói cho cả inbound và outbound traffic

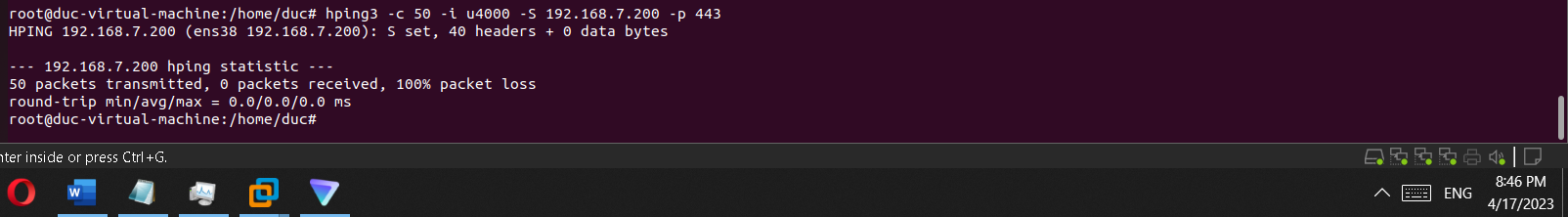
TRƯỚC :

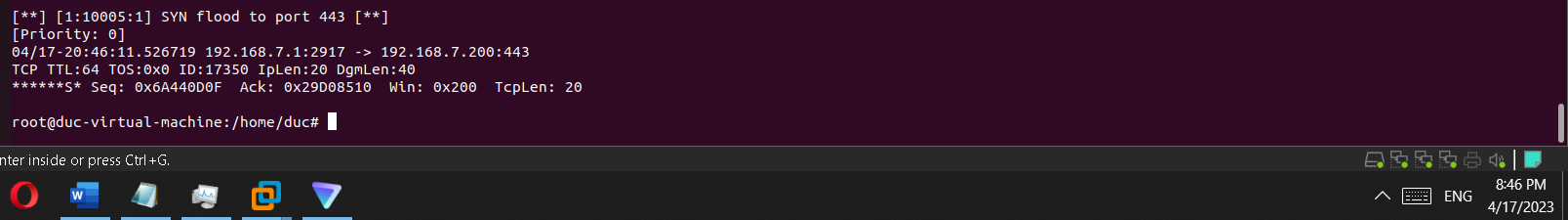
Tấn công hping3 bình thường



SAU :

Không tấn công được nữa





Text

Description automatically generated

A picture containing background pattern

Description automatically generated

Trước :

Nmap port nào cũng đc

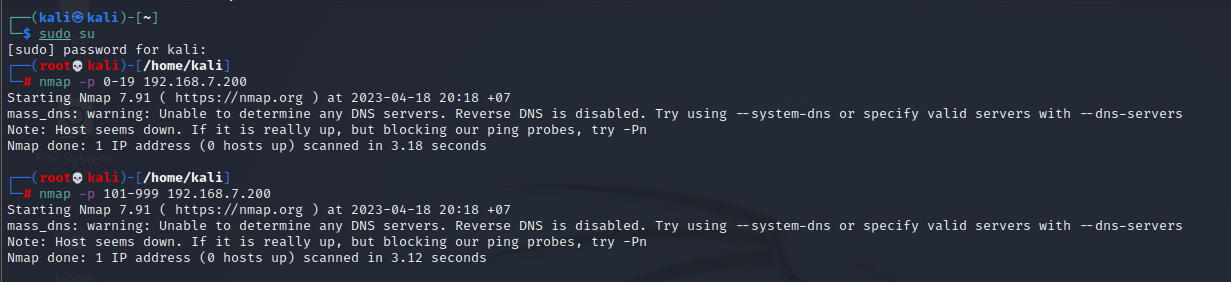
Text

Description automatically generated with low confidence

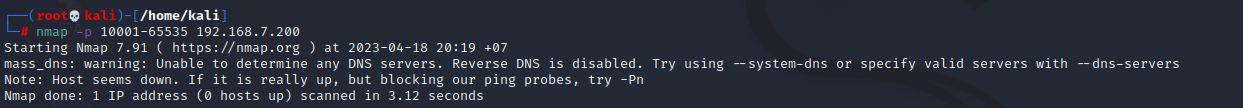
Sau :

Hết Nmap luôn

0-19 , 101-999



10001-65535

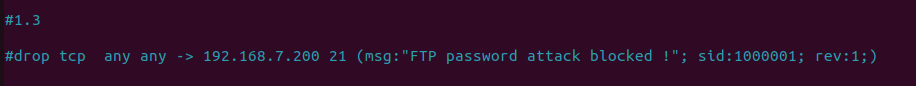
****

**A picture containing rectangle

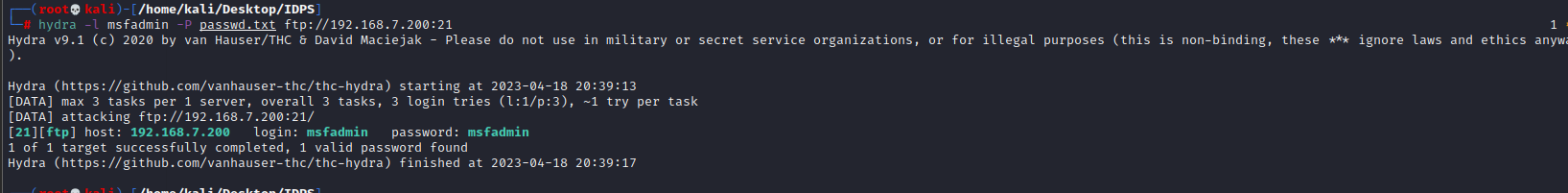
Description automatically generated**

**Text

Description automatically generated**

****

**TRƯỚC:**

****

Quét cổng 21 (d vụ ftp trên máy victim) và lấy đc passwd

Sử dụng hydra

**SAU :**

Hết quét luôn

Text

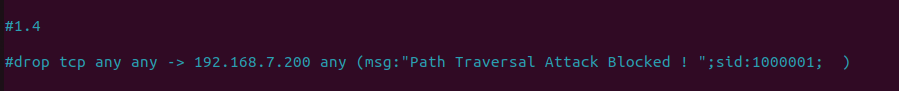
Description automatically generated with medium confidence

A picture containing rectangle

Description automatically generated

Graphical user interface, text, application

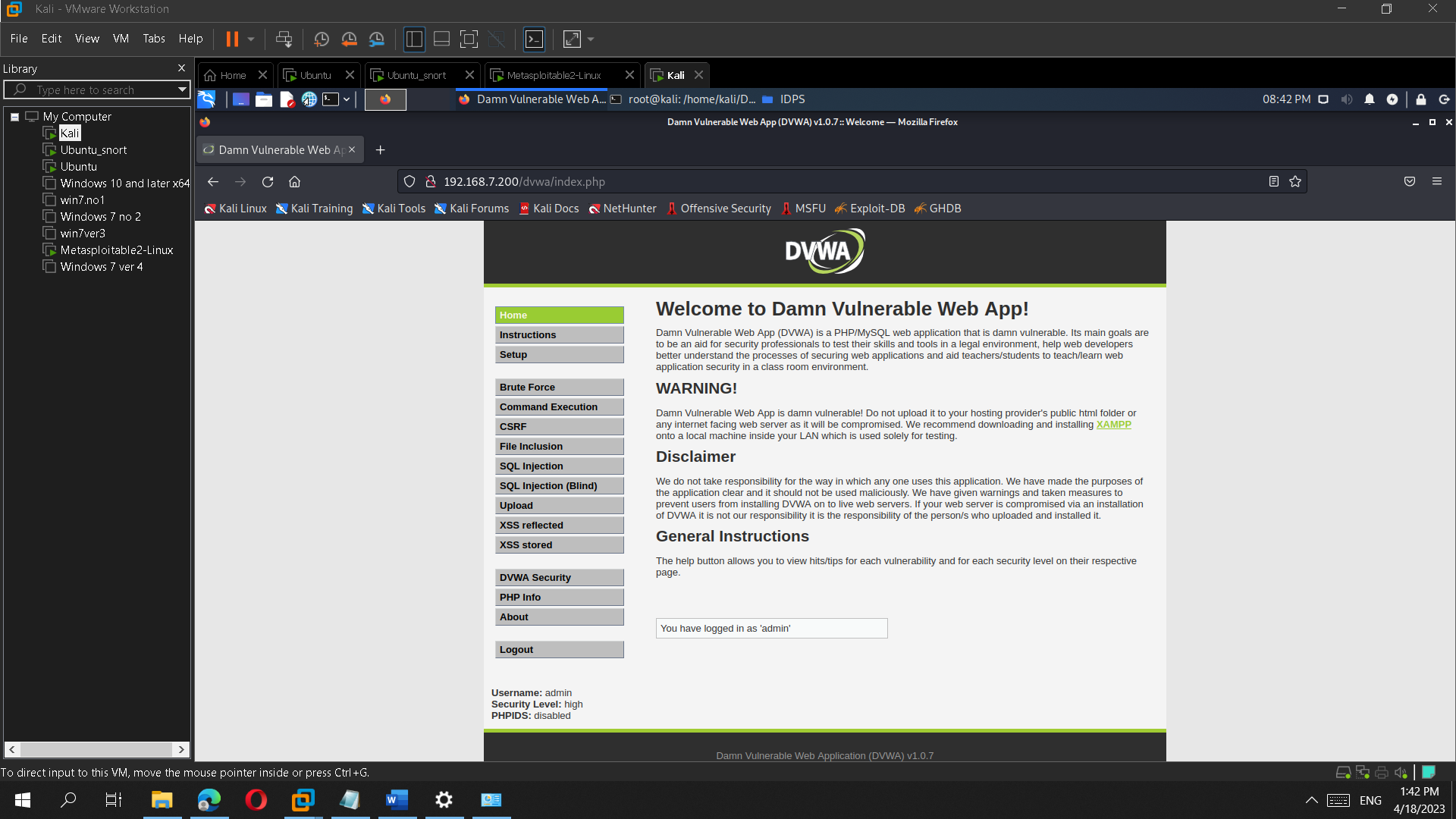
Description automatically generated



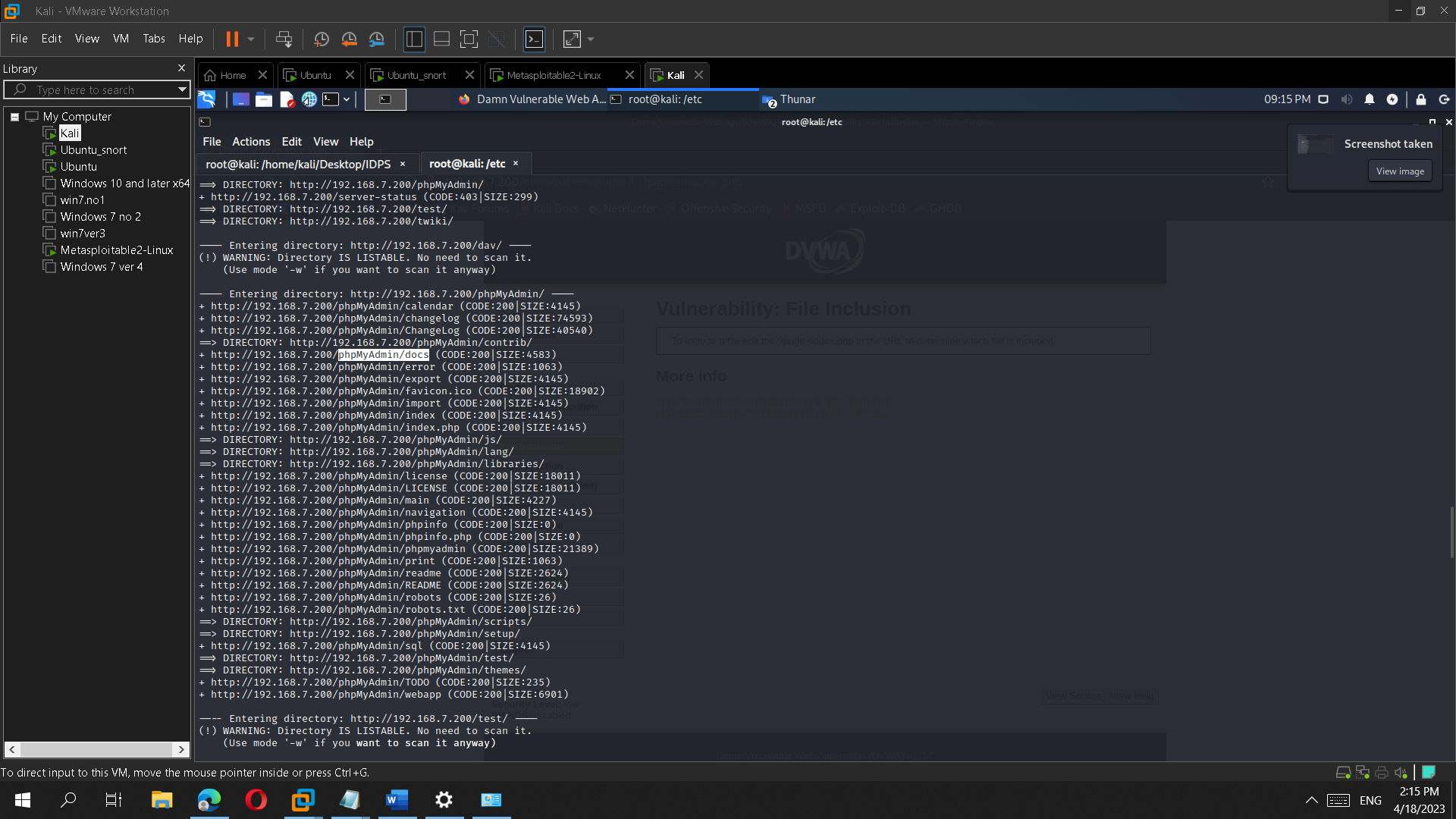
**Trước**

Đăng nhập vào web của metasploitable và xem thông tin bình thường





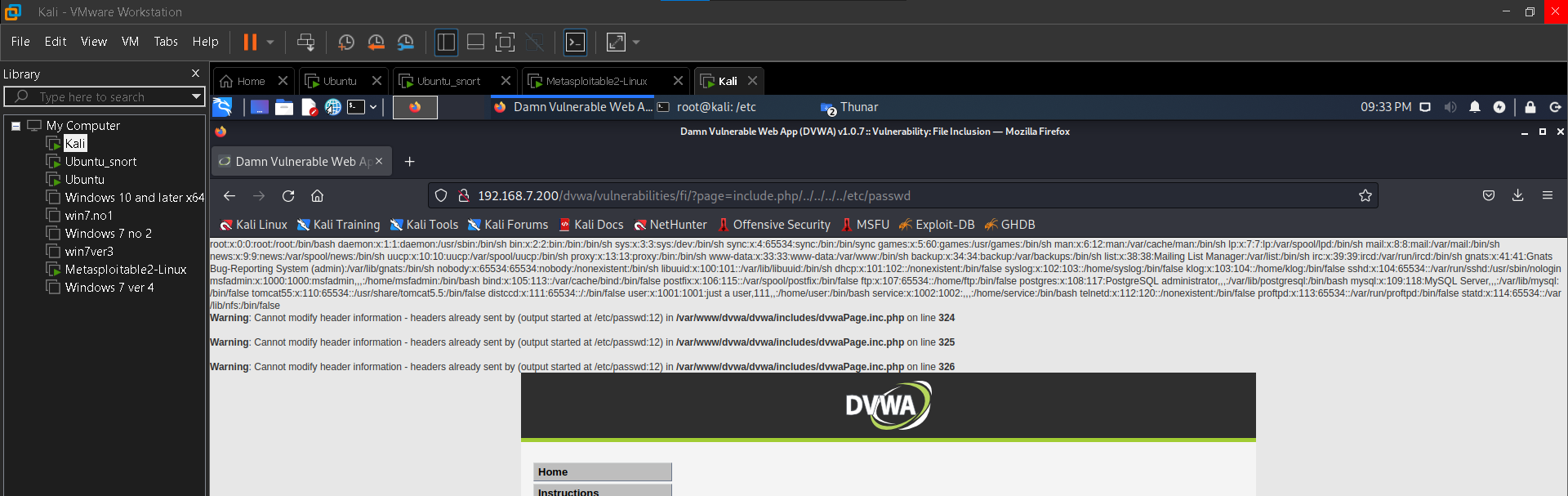
Dirb <http://192.168.7.200/> để xem các file có trên web



A screenshot of a computer

Description automatically generated

Truy cập vào /etc/passwd trên máy exsploitable2 bằng cách thực hiện tấn công Path Traversal



Text

Description automatically generated

**SAU :**

Khỏi vào web luôn

A picture containing background pattern

Description automatically generated

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

1.5

Kịch bản 1: Sử dụng payload để thực hiện mã độc

Khởi động các dịch vụ web để victim khi truy cập vào web thì sẽ tải payload về

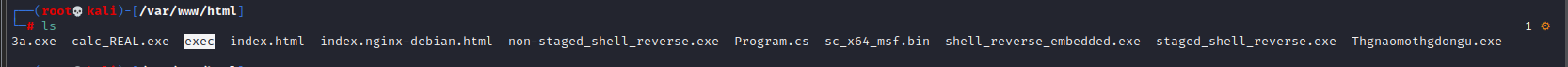


Tạo payload có chứa câu lệnh attack muốn victim muốn thực thi

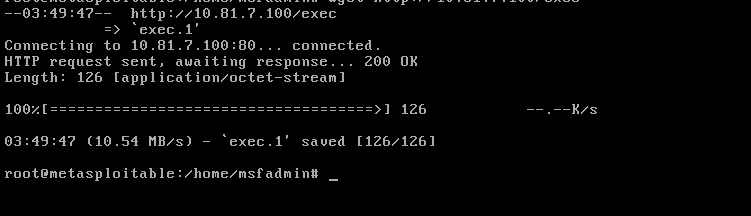
A screenshot of a computer

Description automatically generated

Đưa lên web



Victim tải và thực thi



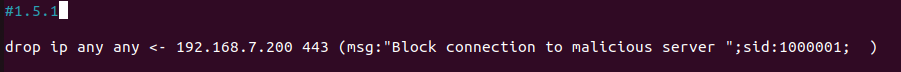
(cái này em nhấn tải 2 lần nên nó ra exec.1)

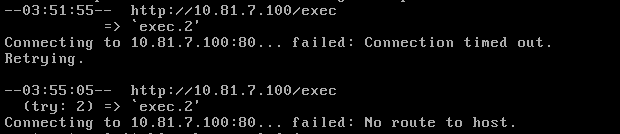
Kết quả : mã độc đã được thực hiện

A picture containing text

Description automatically generated

**SAU:** Hết truy cập vào web và tải được luôn

****

****

**1.5.2 :** **Khai thác cổng 21: FTP**

**Dùng search vsftpd trong metasploit**

**Text

Description automatically generated**

* Chọn một exploit để tấn công một hệ thống Unix qua lỗ hổng trong dịch vụ FTP của phần mềm vsftpd phiên bản 2.3.4. Lỗ hổng này cho phép tin tặc thực hiện tấn công từ xa để kiểm soát máy chủ mục tiêu.

**Text

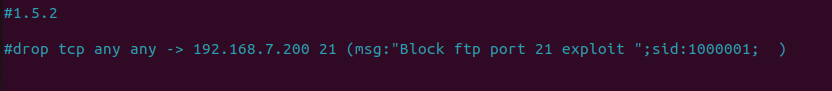
Description automatically generated**

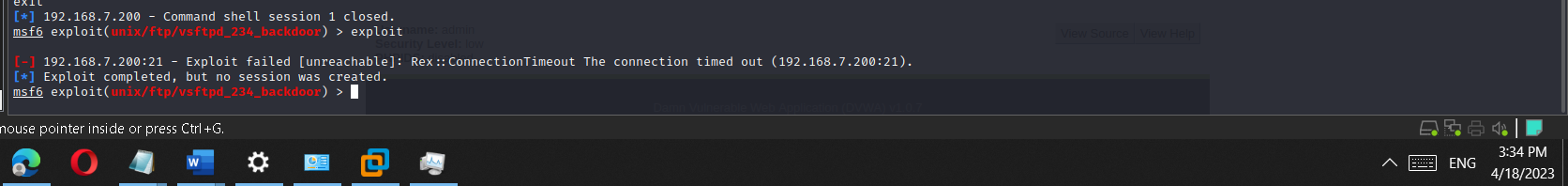
* Khai thác lỗ hổng và thực hiện những gì mình muốn với victim

**Graphical user interface, text

Description automatically generated**

SAU : Hết exploit đc luôn





A picture containing rectangle

Description automatically generated

1. Ghi nội dung công việc, các kịch bản trong bài Thực hành [↑](#footnote-ref-1)