VNCERT

MỤC LỤC

[DANH MỤC HÌNH VẼ 2](#_Toc131362156)

[I. TÓM TẮT VIỆC ĐÃ LÀM 3](#_Toc131362157)

[1.1. Bảng Nhiệm Vụ 3](#_Toc131362158)

[II. Module 2 Scanning Network 4](#_Toc131362159)

[2.1. Thu thập thông tin nguồn mở bằng Windows Command Line Utilities 4](#_Toc131362160)

[2.2. Tìm tên miền phụ của Công ty bằng Sublist3r 11](#_Toc131362161)

[III. Module 11 Sessions Hijacking 13](#_Toc131362162)

[3.1. Session Hijacking using the Zed Attack Proxy (ZAP) 13](#_Toc131362163)

[3.2. Perform sslstrip and Intercept HTTP Traffic through BetterCAP 19](#_Toc131362164)

[IV. Module 13 Hacking Web Servers 22](#_Toc131362165)

[4.1. Fingerprinting a Web Server 22](#_Toc131362166)

[4.1.1. Httprecon 22](#_Toc131362167)

[4.1.2. Uniscan 23](#_Toc131362168)

[4.2. Cracking Ftp 26](#_Toc131362169)

# DANH MỤC HÌNH VẼ

[Hình 2. 1 Lệnh ping để trích xuất địa chỉ IP cho www.certifiedhacker.com 4](#_Toc131362138)

[Hình 2. 2 Lệnh ping cho www.certifiedhacker.com với các tùy chọn –f –l 1500 4](#_Toc131362139)

[Hình 2. 3 Lệnh ping cho www.certifiedhacker.com với các tùy chọn –f –l 1300 5](#_Toc131362140)

[Hình 2. 4 Lệnh ping cho www.certifiedhacker.com với các tùy chọn –f –l 1464 5](#_Toc131362141)

[Hình 2. 5 Lệnh ping cho www.certifiedhacker.com với tùy chọn –i 5 6](#_Toc131362142)

[Hình 2. 6 Lệnh ping cho www.certifiedhacker.com với tùy chọn –i 3 6](#_Toc131362143)

[Hình 2. 7 Lệnh tracert cho www.certifiedhacker.com 7](#_Toc131362144)

[Hình 2. 8 Lệnh tracert cho www.certifiedhacker.com 7](#_Toc131362145)

[Hình 2. 9 Lệnh ping cho www.certifiedhacker.com với các tùy chọn –i 2 –n 1 8](#_Toc131362146)

[Hình 2. 10 Lệnh ping cho www.certifiedhacker.com với –i 17 –n 1 8](#_Toc131362147)

[Hình 2. 11 Dấu nhắc lệnh với lệnh nslookup 9](#_Toc131362148)

[Hình 2. 12 Trong lệnh nslookup, đặt type=a option 9](#_Toc131362149)

[Hình 2. 13 Trong lệnh nslookup, đặt tùy chọn type=cname 10](#_Toc131362150)

[Hình 2. 14 Ảnh chụp màn hình hiển thị trả về địa chỉ IP của máy chủ 10](#_Toc131362151)

[Hình 2. 15 Cài đặt sublist3r thông qua dòng lệnh 11](#_Toc131362152)

[Hình 2. 16 Lệnh trợ giúp Sublist3r 11](#_Toc131362153)

[Hình 2. 17 Sublist3r hiển thị các tên miền phụ duy nhất được tìm thấy 12](#_Toc131362154)

[Hình 2. 18 Sublist3r liệt kê tên miền phụ google.com với cổng 80 mở 12](#_Toc131362155)

[Hình 3. 1 Định cấu hình cài đặt proxy 14](#_Toc131362119)

[Hình 3. 2 Cấu hình proxy 14](#_Toc131362120)

[Hình 3. 3 Cấu hình địa chỉ ip của máy tấn công 15](#_Toc131362121)

[Hình 3. 4 Cài đặt OWASP ZAP 16](#_Toc131362122)

[Hình 3. 5 Chọn Break để yêu cầu ZAP bắt thông tin từ máy nạn nhân 16](#_Toc131362123)

[Hình 3. 6 Đặt địa chỉ ip của Windows Server 2016 17](#_Toc131362124)

[Hình 3. 7 Click Set break on all request and responses 17](#_Toc131362125)

[Hình 3. 8 Truy cập vào trình duyệt web Google Chrome 18](#_Toc131362126)

[Hình 3. 9 Các yêu cầu của máy nạn nhân 18](#_Toc131362127)

[Hình 3. 10 Nội dung server trả về 18](#_Toc131362128)

[Hình 3. 11 Nội dung sau khi sửa 19](#_Toc131362129)

[Hình 3. 12 Trang web trả về sau khi sửa nội dung 19](#_Toc131362130)

[Hình 3. 13 Khởi chạy bettercap 20](#_Toc131362131)

[Hình 3. 14 Kiểm tra các module đang hoạt động 20](#_Toc131362132)

[Hình 3. 15 Bật module arp.spoof và net.sniff 21](#_Toc131362133)

[Hình 3. 16 Kiểm tra các module đang hoạt động 21](#_Toc131362134)

[Hình 3. 17 Đăng nhập ở máy nạn nhân ở trang http 22](#_Toc131362135)

[Hình 3. 18 Máy tấn công bắt các gói tin từ máy nạn nhân 22](#_Toc131362136)

[Hình 3. 19 Thông tin đăng nhập ở máy nạn nhân 22](#_Toc131362137)

[Hình 4. 1 Giao diện website 23](#_Toc131362100)

[Hình 4. 2 kết quả sau khi giải nén 23](#_Toc131362101)

[Hình 4. 3 kết quả khi quét thông tin của website 24](#_Toc131362102)

[Hình 4. 4 kết quả khi quét thông tin 25](#_Toc131362103)

[Hình 4. 5 Thông tin của file report 25](#_Toc131362104)

[Hình 4. 6 kết quả khi quét với tùy chọn “-d” (1) 26](#_Toc131362105)

[Hình 4. 7 kết quả khi quét với tùy chọn “-d” (2) 26](#_Toc131362106)

[Hình 4. 8 Phần mềm cấu hình ftp 27](#_Toc131362107)

[Hình 4. 9 Cấu hình ứng dụng 27](#_Toc131362108)

[Hình 4. 10 Thêm tài khoản 28](#_Toc131362109)

[Hình 4. 11 Tạo folder ảo đồng thời cấp quyền 28](#_Toc131362110)

[Hình 4. 12 Kiểm tra các dịch vụ đang hoạt động 29](#_Toc131362111)

[Hình 4. 13 Tạo file userCustom.txt 29](#_Toc131362112)

[Hình 4. 14 Nội dung file userCustom.txt 29](#_Toc131362113)

[Hình 4. 15 Tạo file passCustom.txt 29](#_Toc131362114)

[Hình 4. 16 Nội dung file passCustom.txt 30](#_Toc131362115)

[Hình 4. 17 Dùng hydra để dò user, password 30](#_Toc131362116)

[Hình 4. 18 Dùng medusa để dò user, password 31](#_Toc131362117)

[Hình 4. 19 Tải wordlist trên internetư 31](#_Toc131362118)

# TÓM TẮT VIỆC ĐÃ LÀM

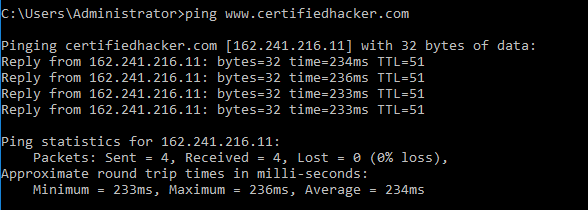
## Bảng Nhiệm Vụ

|  |  |  |
| --- | --- | --- |
| LÂM ANH | DUNG | ĐỨC |
| Module 13 | Module 11 | Module 2 |

# Module 2 Scanning Network

## Thu thập thông tin nguồn mở bằng Windows Command Line Utilities

Nhập ping www.certifiedhacker.com trong cửa sổ nhắc lệnh và nhấn Enter để tìm địa chỉ IP của nó. Phản hồi được hiển thị phải giống với phản hồi được hiển thị trong ảnh chụp màn hình sau.



Hình 2. 1 Lệnh ping để trích xuất địa chỉ IP cho www.certifiedhacker.com

Domain’s ip address: 162.241.216.11

Tìm kích thước khung hình tối đa trên mạng:

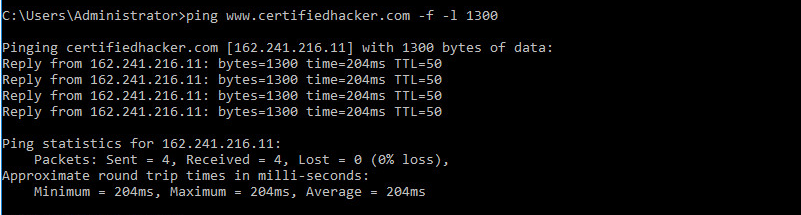


Hình 2. 2 Lệnh ping cho www.certifiedhacker.com với các tùy chọn –f –l 1500

Tùy chọn "-f" được sử dụng để đặt cờ Don't Fragment trong gói tin ping, điều này ngăn chặn gói tin bị chia nhỏ nếu kích thước quá lớn. Tùy chọn "-l 1500" được sử dụng để chỉ định kích thước của gói tin là 1500 byte.

Phản hồi, Gói cần được phân mảnh nhưng DF được đặt, có nghĩa là khung quá lớn để có trên mạng và cần được phân mảnh. Vì chúng tôi đã sử dụng công tắc -f với lệnh ping, gói không được gửi và lệnh ping đã trả về lỗi này.

Type ping www.certifiedhacker.com –f –l 1300

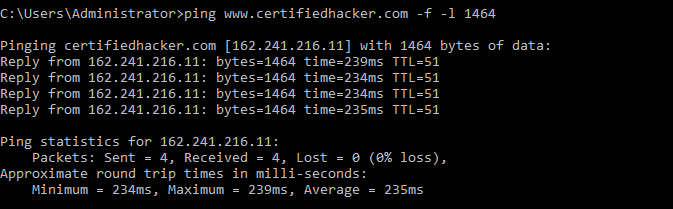


Hình 2. 3 Lệnh ping cho www.certifiedhacker.com với các tùy chọn –f –l 1300

Quan sát rằng kích thước gói tối đa nhỏ hơn 1500 byte và lớn hơn 1300 byte.

Bây giờ, hãy thử các giá trị khác nhau cho đến khi bạn tìm thấy kích thước khung hình tối đa. Chẳng hạn, ping www.certifiedhacker.com –f –l 1473 trả lời với Gói cần được phân mảnh nhưng DF được đặt và ping www.certifiedhacker.com –f –l 1464 trả lời bằng ping thành công. Nó chỉ ra rằng 1410 byte là kích thước khung hình tối đa trên mạng của máy này. Tùy máy khác nhau sẽ cho ra kết quả khác nhau

Lưu ý: Kích thước khung hình tối đa sẽ khác nhau tùy thuộc vào mạng mục tiêu



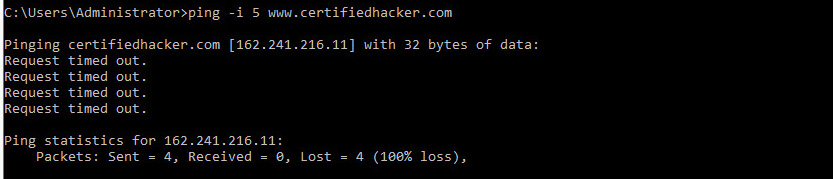
Hình 2. 4 Lệnh ping cho www.certifiedhacker.com với các tùy chọn –f –l 1464

Bây giờ, hãy tìm hiểu điều gì sẽ xảy ra khi TTL (Thời gian tồn tại) hết hạn. Mỗi khung trên mạng đã được xác định TTL. Nếu TTL đạt 0, bộ định tuyến sẽ loại bỏ gói. Cơ chế này ngăn chặn việc mất các gói tin.

TTL (Time to Live) của các gói tin được tính bằng số lượng các bước mạng mà gói tin có thể đi qua trước khi bị hủy bỏ. TTL được tính bằng số lượng các bước định tuyến (routing hops) mà gói tin đi qua trên đường đi tới đích. Khi một gói tin đi qua một bước định tuyến, giá trị TTL sẽ giảm đi một đơn vị, và nếu giá trị TTL của gói tin giảm xuống 0, gói tin sẽ bị hủy bỏ và không đến được đích. Việc giảm giá trị TTL giúp đảm bảo rằng các gói tin sẽ không lặp vô hạn trên các bước định tuyến nếu có lỗi xảy ra trong mạng.

Trong dấu nhắc lệnh, nhập ping www.certifiedhacker.com -i 5. Tùy chọn này đặt giá trị thời gian tồn tại TTL (-i) là 5. Điều này có nghĩa là lệnh ping sẽ gửi gói tin và chờ 5 giây trước khi gửi gói tin tiếp theo.

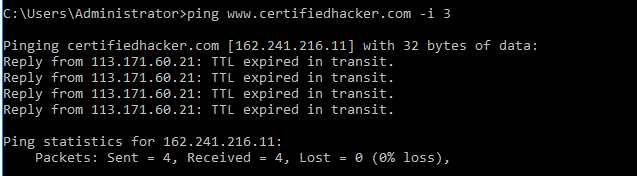
Lưu ý: Giá trị tối đa bạn có thể đặt cho TTL là 255.



Hình 2. 5 Lệnh ping cho www.certifiedhacker.com với tùy chọn –i 5

Khi bạn set giá trị TTL nhỏ hơn quãng đường đến đích, gói tin sẽ bị mất hoặc bị hủy bởi các thiết bị trung gian trên đường đi, do đó, bạn có thể nhận được thông báo lỗi "Request Timed Out" khi gói tin không thể truyền đến đích.

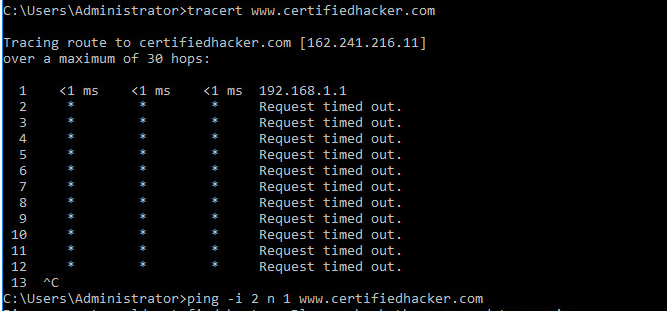
Đổi giá trị i thành 3



Hình 2. 6 Lệnh ping cho www.certifiedhacker.com với tùy chọn –i 3

Trả lời từ 162.241.216.11: TTL hết hạn trong quá trình truyền có nghĩa là bộ định tuyến (162.241.216.11) đã loại bỏ khung, vì TTL của nó đã hết hạn (đạt 0).

Tìm đường theo dõi từ PC của bạn đến www.certifiedhacker.com bằng cách sử dụng lệnh tracert. Lệnh này theo dõi thông tin cấu hình mạng của miền đích.



Hình 2. 7 Lệnh tracert cho www.certifiedhacker.com

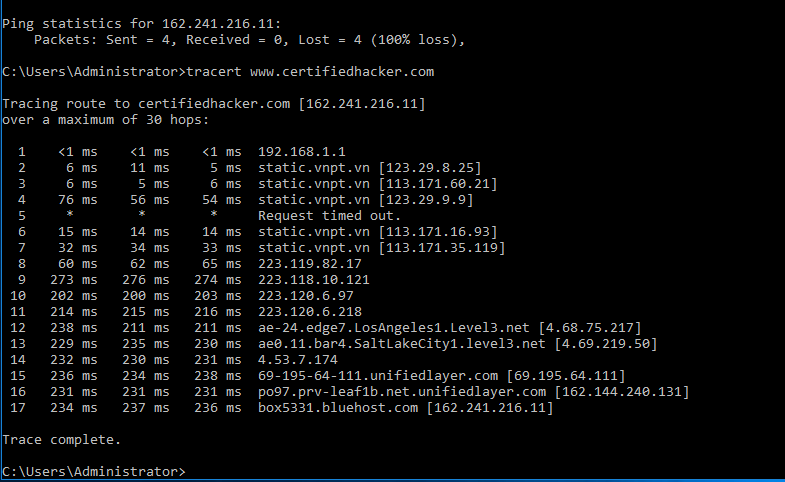
"Request timed out".

Miền bị chặn hoặc bảo vệ: Có thể các hệ thống tường lửa (tường lửa) hoặc các bộ lọc mạng khác đã cấm truy cập vào miền mà bạn đang cố gắng truy cập, dẫn đến lệnh tracert không thể kết nối và trả về kết quả. kết quả "Hết thời gian yêu cầu".

Các bước nhảy trên đường truyền không phản hồi: Có thể các thiết bị trung gian trên đường truyền không hoạt động hoặc không phản hồi yêu cầu từ lệnh tracert, dẫn đến kết quả "Hết thời gian yêu cầu" trên các bước nhảy đó.

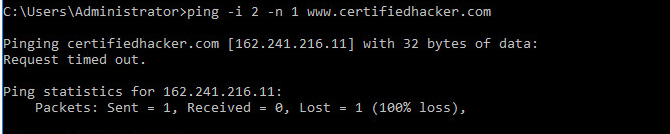
Truy cập từ xa bị chặn: Nếu đang truy cập từ xa vào miền (ví dụ: thông qua VPN hoặc từ một quốc gia khác), có thể đã bị chặn truy cập vào miền do giới hạn địa lý hoặc chính sách bảo mật.

Thực hiện đổi mạng và thử lại, ta sẽ có kết quả:



Hình 2. 8 Lệnh tracert cho www.certifiedhacker.com

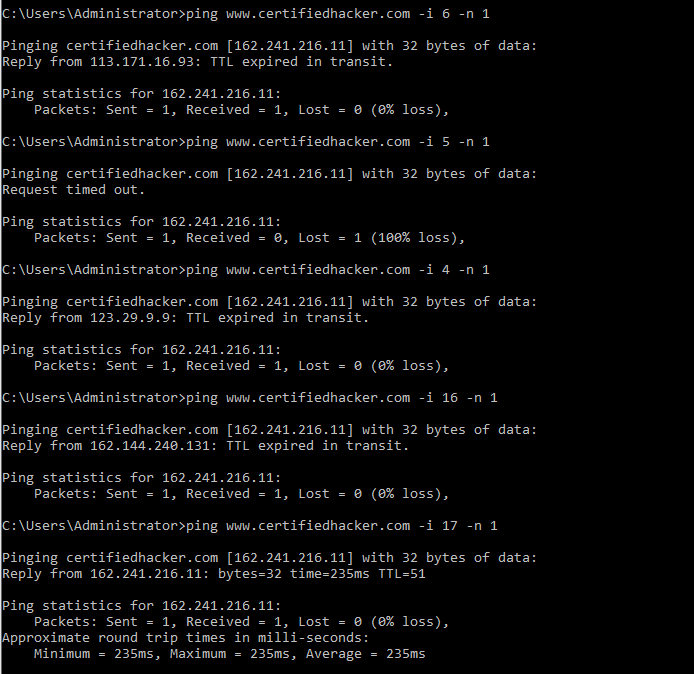
Thu nhỏ dấu nhắc lệnh được hiển thị ở trên và khởi chạy một dấu nhắc lệnh mới. Trong cửa sổ nhắc lệnh, nhập ping www.certifiedhacker.com -i 2 –n 1. Điểm khác biệt duy nhất so với lệnh ping trước đó là chúng tôi đang đặt TTL thành hai trong nỗ lực kiểm tra tuổi thọ của gói tin.



Hình 2. 9 Lệnh ping cho www.certifiedhacker.com với các tùy chọn –i 2 –n 1

Quan sát rằng có một phản hồi đến từ địa chỉ IP 162.241.216.11 và không có gói bị mất.

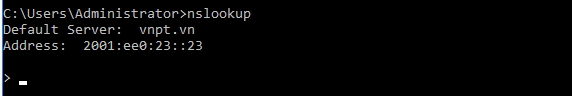
Ở đây, ping thành công để truy cập www.certifiedhacker.com là 17 bước nhảy. Đầu ra sẽ tương tự như kết quả theo dõi lộ trình.



Hình 2. 10 Lệnh ping cho www.certifiedhacker.com với –i 17 –n 1

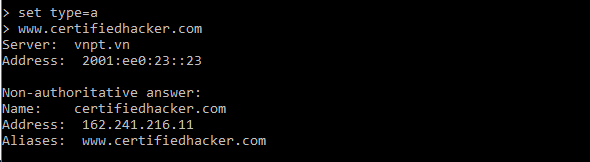
Điều này nói rằng, tại thời điểm có giá trị trực tiếp là 17, phản hồi được nhận từ máy chủ đích (162.241.216.11).

Khởi chạy dấu nhắc lệnh mới, nhập nslookup và nhấn Enter. Điều này sẽ hiển thị máy chủ mặc định và địa chỉ của nó được gán cho máy Windows Server 2016.



Hình 2. 11 Dấu nhắc lệnh với lệnh nslookup

Trong chế độ tương tác nslookup, nhập set type=a và nhấn Enter. Đặt loại là cấu hình nslookup để truy vấn địa chỉ IP của một miền nhất định. Nhập tên miền mục tiêu www.certifiedhacker.com và nhấn Enter. Điều này giải quyết địa chỉ IP và hiển thị kết quả như sau:



Hình 2. 12 Trong lệnh nslookup, đặt type=a option

Set type=a được sử dụng để chỉ định kiểu bản ghi (record type) sẽ được tìm kiếm trong tên miền (domain name). Khi sử dụng set type=a, nslookup sẽ tìm kiếm bản ghi loại A (Address) của tên miền đã chỉ định. Bản ghi A chứa địa chỉ IP của tên miền đó.

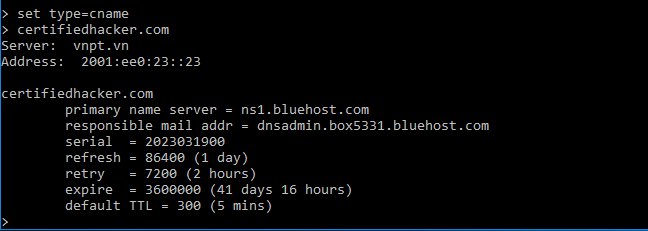
Hai dòng đầu tiên trong kết quả là:

vnpt.vn và 2001:ee0:23::23

Điều này xác định rằng kết quả được chuyển hướng đến máy chủ mặc định được lưu trữ trên máy cục bộ (Windows Server 2016) giải quyết miền được yêu cầu của bạn.

Do đó, nếu phản hồi đến từ máy chủ của máy cục bộ của bạn (vnpt), chứ không phải máy chủ lưu trữ miền hợp pháp www.certifiedhacker.com, nó được coi câu trả lời non-authoritative. Vì kết quả trả về non-authoritative nên bạn cần lấy máy chủ định danh authoritative của miền.

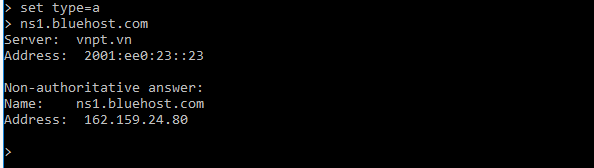
Nhập set type=cname và nhấn Enter. Việc tra cứu CNAME được thực hiện trực tiếp với máy chủ định danh authoritative của miền và liệt kê các bản ghi CNAME cho một miền. Điều này trả về tên máy chủ của miền mà có thẩm quyền, cùng với địa chỉ máy Email



Hình 2. 13 Trong lệnh nslookup, đặt tùy chọn type=cname

Bản ghi CNAME là một bản ghi phân giải tên miền, nó cho phép bạn chỉ định một tên miền phụ (alias) cho một tên miền chính (canonical name). Khi máy chủ DNS nhận được yêu cầu truy vấn cho tên miền alias, nó sẽ trả về địa chỉ IP của tên miền chính.

Vì bạn đã có được máy chủ định danh có thẩm quyền, bạn sẽ cần xác định địa chỉ IP của máy chủ định danh. Đưa ra lệnh set type=a và nhấn Enter. Nhập ns1.bluehost.com (hoặc máy chủ định danh chính được hiển thị trong môi trường phòng thí nghiệm của bạn) rồi nhấn Enter. Điều này trả về địa chỉ IP của máy chủ

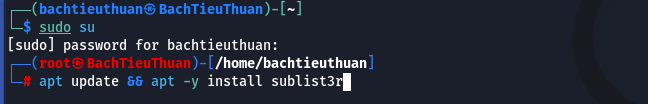


Hình 2. 14 Ảnh chụp màn hình hiển thị trả về địa chỉ IP của máy chủ

Tên máy chủ có thẩm quyền lưu trữ các bản ghi được liên kết với miền. Vì vậy, nếu kẻ tấn công có thể xác định một máy chủ tên có thẩm quyền (primary nameserver) và có được địa chỉ IP được liên kết của nó, thì kẻ đó có thể cố gắng khai thác máy chủ để thực hiện các hành động nguy hiểm. Cuộc tấn công bao gồm DoS, DDoS, Chuyển hướng URL, v.v.

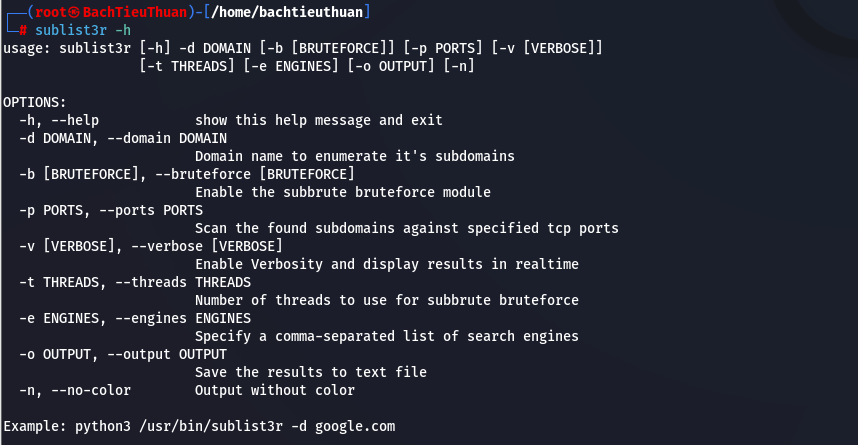
## Tìm tên miền phụ của Công ty bằng Sublist3r

Cài đặt Sublist3r. Để cài đặt Sublist3r, hãy nhập apt update && apt -y install sublist3r và nhấn Enter.



Hình 2. 15 Cài đặt sublist3r thông qua dòng lệnh

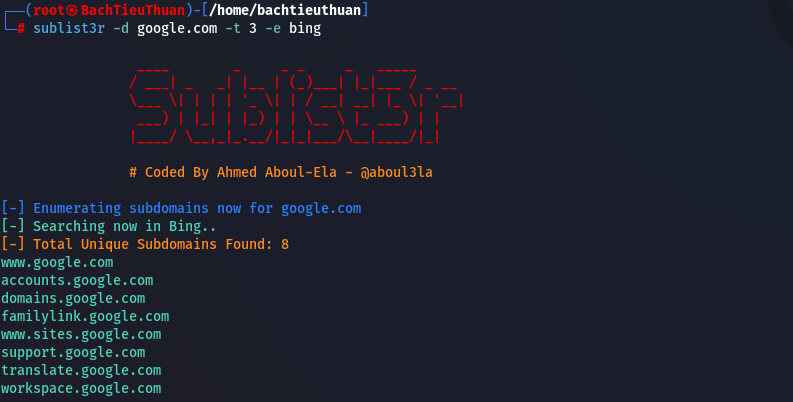
Khi quá trình cài đặt hoàn tất, hãy nhập sublist3r -h và nhấn Enter. Lệnh này in tổng quan về tất cả các tùy chọn có sẵn cho chúng tôi kèm theo mô tả.



Hình 2. 16 Lệnh trợ giúp Sublist3r

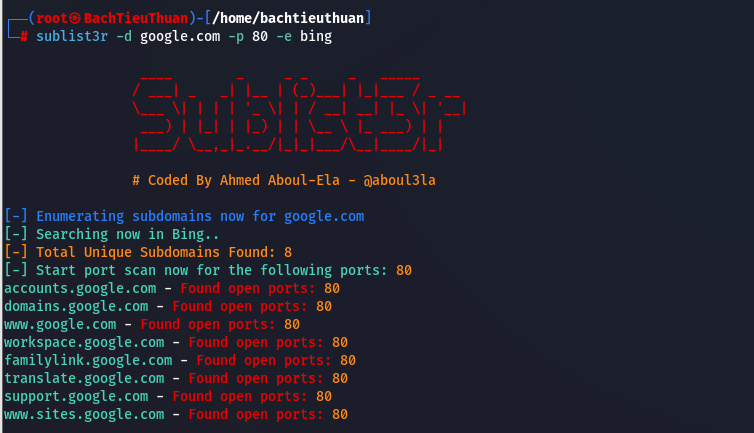
Nhập sublist3r -d google.com -t 3 -e bing và nhấn Enter. Ở đây -d là để tìm kiếm các tên miền phụ, -t 3 với 3 luồng và -e bing là để tìm kiếm trong bing.

Chúng ta đã tìm thấy các Tên miền phụ có trong google.com, như được hiển thị trong ảnh chụp màn hình.



Hình 2. 17 Sublist3r hiển thị các tên miền phụ duy nhất được tìm thấy

Bây giờ, hãy tìm cổng tên miền phụ 80 đang mở trong google.com. Nhập sublist3r -d google.com -p 80 -e bing và nhấn Enter. Sublist3r sẽ liệt kê tất cả các tên miền phụ của google.com với cổng 80 mở như trong ảnh chụp màn hình.



Hình 2. 18 Sublist3r liệt kê tên miền phụ google.com với cổng 80 mở

# Module 11 Sessions Hijacking

## Session Hijacking using the Zed Attack Proxy (ZAP)

Định cấu hình cài đặt proxy trong máy nạn nhân (Windows 10). Khởi chạy trình duyệt Chrome, chọn Setting => vào phần System , click vào Open your computer’s proxy settings để cấu hình proxy

Graphical user interface, text, application, email

Description automatically generated

Hình 3. 1 Định cấu hình cài đặt proxy

Cấu hình Proxy

Graphical user interface, text, application, email

Description automatically generated

Hình 3. 2 Cấu hình proxy

Vào Internet Properties -> Connections -> LAN settings. Nhập địa chỉ ip của máy tấn công (Windows Server 2016: 192.168.174.128) và cổng 8080

Graphical user interface, text, application

Description automatically generated

Hình 3. 3 Cấu hình địa chỉ ip của máy tấn công

Như vậy là đã định cấu hình proxy ở máy tấn công. Bây giờ cài đặt OWASPZAP (Zed Attack Proxy) ở máy Windows Server 2016, lưu ý khi cài đặt OWASPZAP cần cài đặt Java (*https://download.oracle.com/java/20/latest/jdk-20\_windows-x64\_bin.exe*) , sau đó tiến hành cài đặt OWASPZAP.

ZAP là một công cụ kiểm thử bảo mật ứng dụng web được sử dụng để phân tích các yêu cầu và phản hồi giữa máy khách và máy chủ, và tìm kiếm các lỗ hổng bảo mật trong ứng dụng web.

Bằng cách sử dụng ZAP trên máy tấn công, kẻ tấn công có thể bắt các yêu cầu được gửi từ máy nạn nhân đến máy chủ, và sau đó phân tích các yêu cầu này để tìm kiếm các lỗ hổng bảo mật.

Graphical user interface, text, application, email

Description automatically generated

Hình 3. 4 Cài đặt OWASP ZAP

Nhấp vào biểu tượng dấu “+” ở khung bên phải, chọn Break

Tab Break cho phép bạn sửa đổi phản hồi hoặc yêu cầu khi ZAP bắt được phản hồi đó. Cho phép sửa đổi một số yếu tố mà bạn không thể sửa đổi thông qua trình duyệt của mình; bao gồm các: Tiêu đề, Trường ẩn, Các trường bị vô hiệu hóa, Các trường sử dụng JavaScript để lọc các ký tự không hợp lệ.

Graphical user interface, logo

Description automatically generated

Hình 3. 5 Chọn Break để yêu cầu ZAP bắt thông tin từ máy nạn nhân

Vào Tools => Options => Network => Local Servers/Proxies nhập địa chỉ ip của máy tấn công (Windows Server 2016)

Graphical user interface, text, application

Description automatically generated

Hình 3. 6 Đặt địa chỉ ip của Windows Server 2016

Click vào *Set break on all requests and responses* (nút hình tròn màu xanh) trên thanh công cụ ZAP, *Set break on all requests and responses* sẽ tự động chuyển từ màu xanh sang màu đỏ. Nút này dùng để đặt và bỏ đặt điểm dừng chung sẽ bẫy và hiển thị phản hồi hoặc yêu cầu tiếp theo trong tab Break từ máy của nạn nhân.

Graphical user interface, application

Description automatically generated

Hình 3. 7 Click Set break on all request and responses

Bây giờ, vào máy Windows 10. Nhập https://sec.vnpt.vn/2023/01/ky-thuat-attacking-kerberos-as-rep-roasting/ vào trình duyệt web Google Chrome

Graphical user interface, text, application

Description automatically generated

Hình 3. 8 Truy cập vào trình duyệt web Google Chrome

Tiếp tục, vào máy tấn công Windows Server 2016 để xem các yêu cầu của máy nạn nhân (Windows 10) từ ZAP proxy.

Graphical user interface, text, application, email

Description automatically generated

Hình 3. 9 Các yêu cầu của máy nạn nhân

Đoạn mã này là một thông báo yêu cầu HTTP được gửi đến máy chủ tại sec.vnpt.vn. Yêu cầu được thực hiện bằng phương thức GET và URL đích là " <https://sec.vnpt.vn/2023/01/ky-thuat-attacking-kerberos-as-rep-roasting/> ".

Graphical user interface, text, application

Description automatically generated

Hình 3. 10 Nội dung server trả về

Bây giờ, sửa đổi nội dung của server trả về

Graphical user interface, application, Word

Description automatically generated

Hình 3. 11 Nội dung sau khi sửa

Graphical user interface, text, application, email

Description automatically generated

Hình 3. 12 Trang web trả về sau khi sửa nội dung

**Kết luận:** Session Hijacking using the Zed Attack Proxy (ZAP) là một cuộc tấn công mà kẻ tấn công sử dụng một máy tấn công (Windows Server 2016) để bắt các thông tin yêu cầu ở trình duyệt web Google Chrome của máy nạn nhân (Windows 10) thông qua công cụ ZAP.

## Perform sslstrip and Intercept HTTP Traffic through BetterCAP

Sử dụng BetterCAP để bắt thông tin tên đăng nhập và mật khẩu

BetterCAP là một công cụ bảo mật mạng dùng để thực hiện các cuộc tấn công MITM (Main-in-the-middle), kiểm tra và phân tích các thông tin mạng,… Bettercap có thể sửa đổi, thay đổi hoặc chèn thêm các gói tin trong lưu lượng mạng HTTP, HTTPS,…

Sau khi cài đặt bettercap thì đăng nhập vào máy Kali Linux và sử dụng dòng lệnh *sudo bettercap* để khởi chạy bettercap.

A screenshot of a computer

Description automatically generated

Hình 3. 13 Khởi chạy bettercap

Dùng lệnh *help* để kiểm tra xem các modules nào đang hoạt động

Graphical user interface, text

Description automatically generated

Hình 3. 14 Kiểm tra các module đang hoạt động

Bật module arp.spoof và net.sniff bằng lệnh *arp.snoof on, net.sniff on.*

ARP spoofing là kỹ thuật giả mạo địa chỉ MAC của một thiết bị trong mạng, với mục đích để tấn công mạng hoặc theo dõi các thông tin được truyền qua mạng.

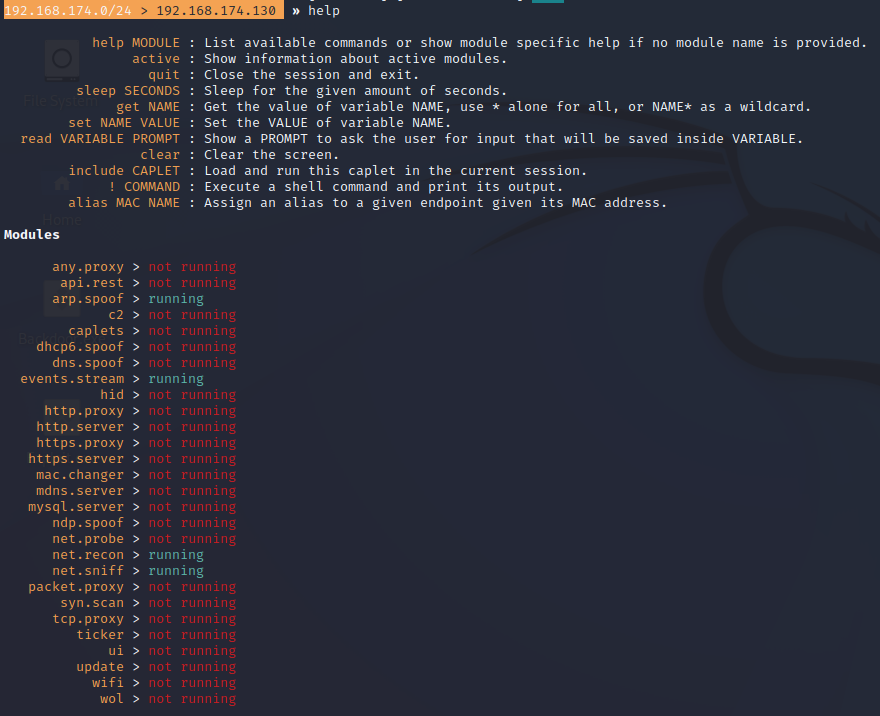
Net sniffing là kỹ thuật giám sát các gói tin mạng khi chúng đi qua một thiết bị. Khi kích hoạt net sniffing, kẻ tấn công có thể theo dõi và phân tích các gói tin mạng để tìm kiếm các thông tin như tên đăng nhập và mật khẩu.

A screenshot of a computer

Description automatically generated with medium confidence

Hình 3. 15 Bật module arp.spoof và net.sniff

Kiểm tra lại xem module arp.spoof và net.sniff đã được bật chưa



Hình 3. 16 Kiểm tra các module đang hoạt động

Truy cập vào máy nạn nhân (Windows Server 2016) và đăng nhập vào một trang web http

Graphical user interface, application

Description automatically generated

Hình 3. 17 Đăng nhập ở máy nạn nhân ở trang http

Máy tấn công đang bắt các thông tin từ máy nạn nhân như đang gởi yêu cầu truy cập vào trang ocsenshop.com và kết quả trả về là thông tin đăng nhập bao gồm: username:kdung@gmail.com, password: 1234 và gửi yêu cầu Đăng nhập.

A picture containing graphical user interface

Description automatically generated

Hình 3. 18 Máy tấn công bắt các gói tin từ máy nạn nhân

Graphical user interface

Description automatically generated

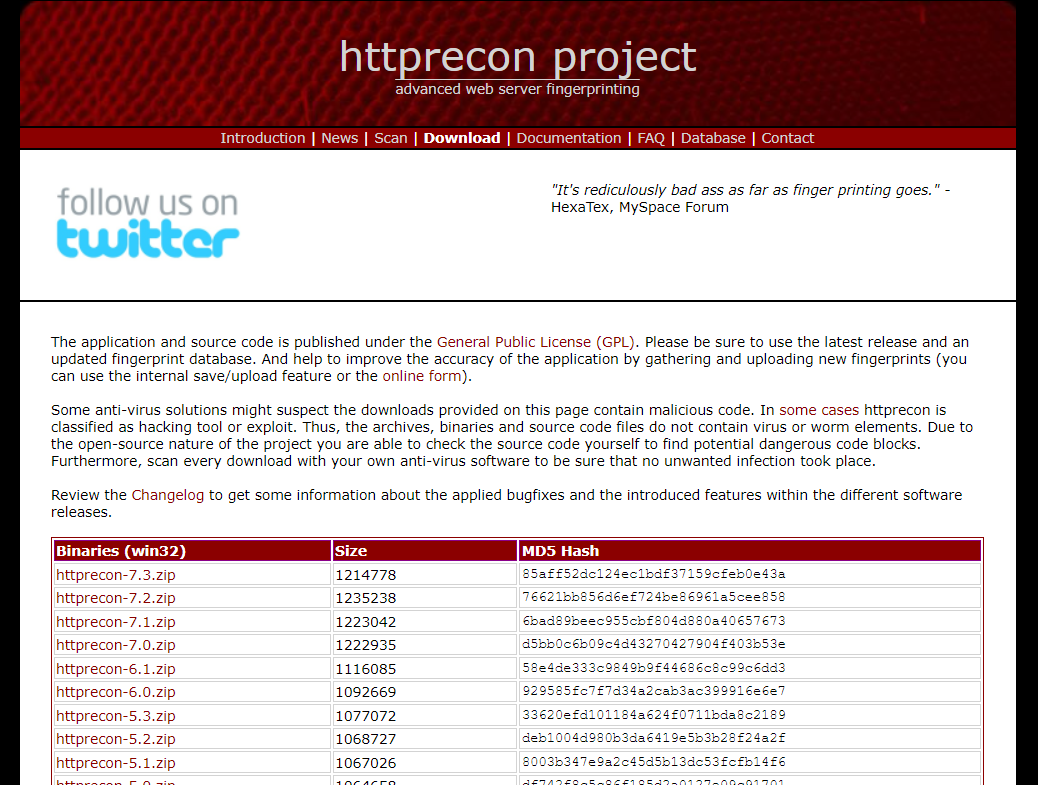
Hình 3. 19 Thông tin đăng nhập ở máy nạn nhân

# Module 13 Hacking Web Servers

## Fingerprinting a Web Server

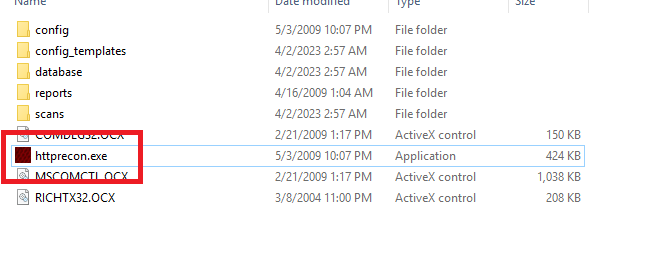
### Httprecon

Truy cập vào website: <https://www.computec.ch/projekte/httprecon/> để tải về phần mềm httprecon



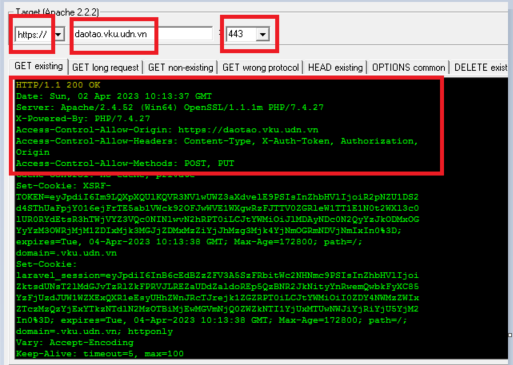
Sau khi giải nén thư mục tải về chúng ta sẽ có được một phần mềm “httprecon.exe”

Hình 4. 1 Giao diện website



Hình 4. 2 kết quả sau khi giải nén

Chúng ta tiến hành quét thông tin của website “https://daotao.vku.udn” và do sử dụng ssl nên cổng mặc định thường là 443.



Hình 4. 3 kết quả khi quét thông tin của website

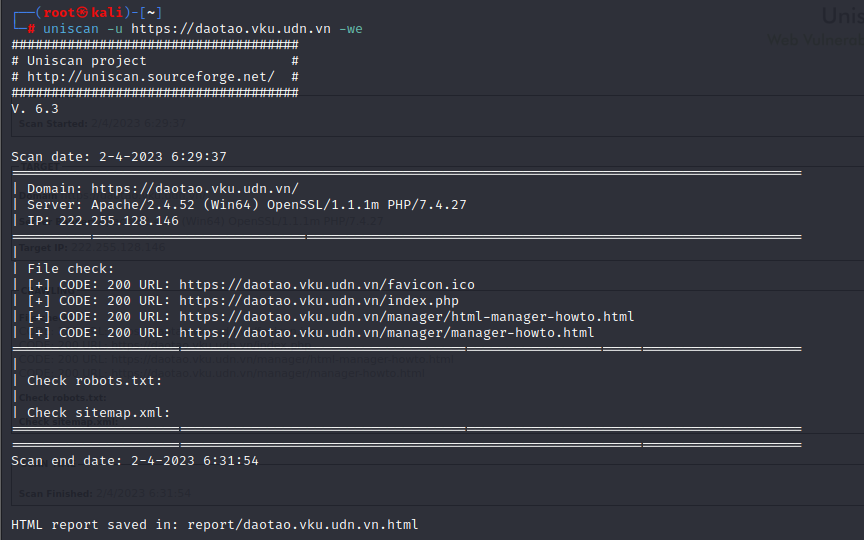
### Uniscan

Tùy chọn -we trong Uniscan được sử dụng để chỉ định phạm vi quét của công cụ. Khi sử dụng tùy chọn này, Uniscan sẽ chỉ quét các tài nguyên nằm trong phạm vi của trang web được chỉ định.

Ví dụ, nếu chúng ta muốn quét các tài nguyên nằm trong thư mục "/admin" của trang web "example.com", bạn có thể sử dụng lệnh sau:

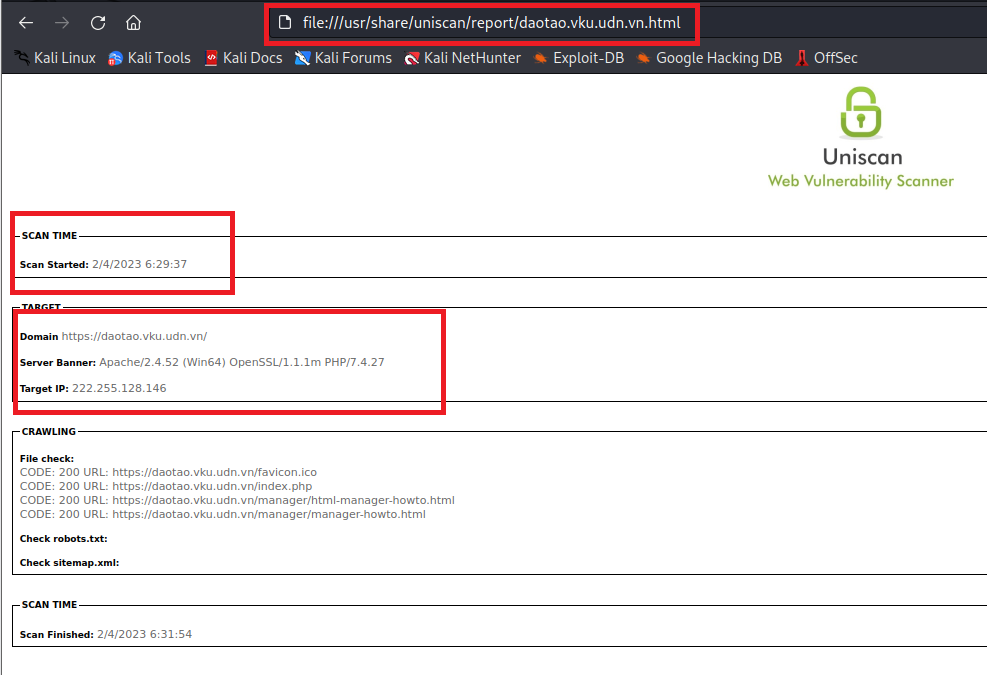
uniscan -d example.com -we /admin

Khi sử dụng tùy chọn -we, Uniscan sẽ chỉ quét các tài nguyên nằm trong thư mục "/admin" trên trang web "example.com". Nếu bạn không sử dụng tùy chọn này, Uniscan sẽ quét toàn bộ trang web được chỉ định.

**

Hình 4. 4 kết quả khi quét thông tin

Khi đã quét được các thông tin chúng ta sẽ truy cập vào folder chứa file report ở “/usr/share/uniscan/report/”

**

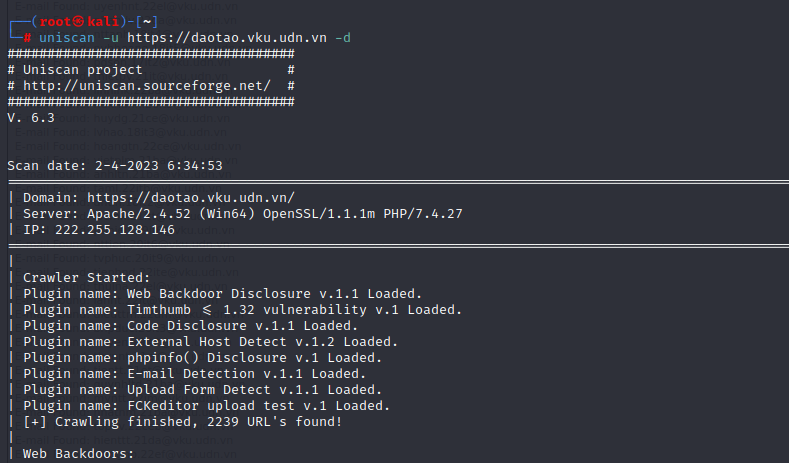
Hình 4. 5 Thông tin của file report

Tùy chọn -d được sử dụng để chỉ định tên miền mục tiêu. Khi sử dụng tùy chọn này, Uniscan sẽ chỉ quét mục tiêu đã được chỉ định thay vì quét tất cả các mục tiêu trên một trang web.

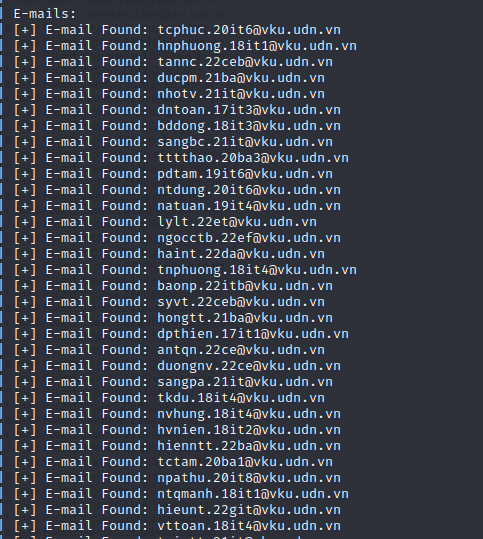
Nếu chúng ta muốn quét lỗ hổng trên trang web "example.com", bạn có thể sử dụng lệnh sau:

*“uniscan -d example.com”*

Khi sử dụng tùy chọn -d, Uniscan chỉ sẽ quét các tài nguyên (file và thư mục) thuộc miền "example.com".

**

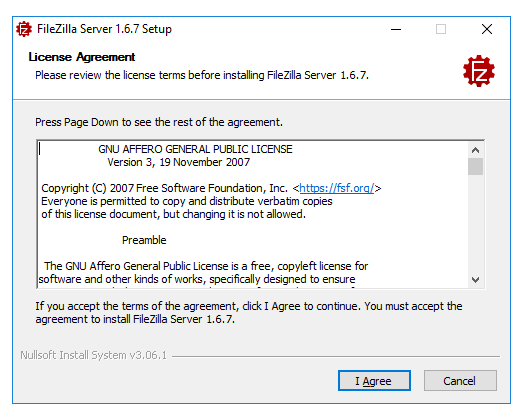
Hình 4. 6 kết quả khi quét với tùy chọn “-d” (1)

**

Hình 4. 7 kết quả khi quét với tùy chọn “-d” (2)

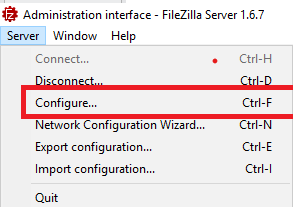
## Cracking Ftp

Cấu hình ftp server trên windows 2016.



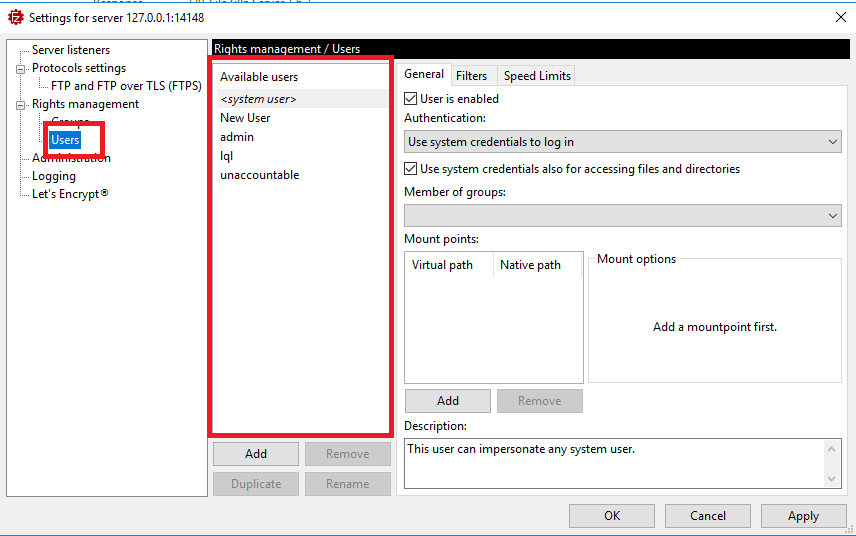
Hình 4. 8 Phần mềm cấu hình ftp

Tiến hành cấu hình fpt server.



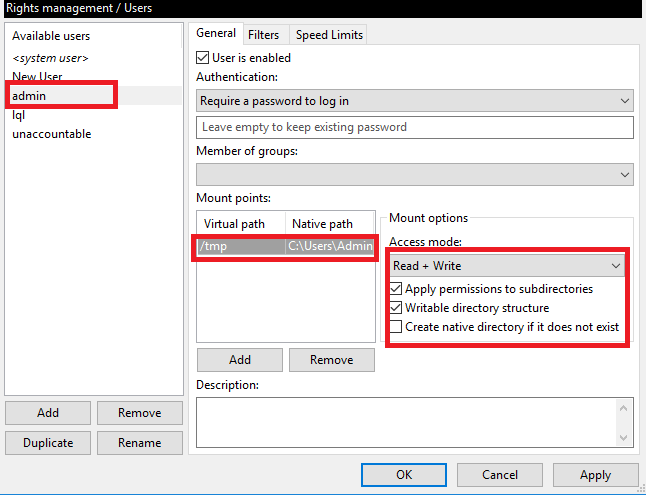
Hình 4. 9 Cấu hình ứng dụng

Thêm tài khoản để các máy khách có thể truy cập vào ftp trên windows 2016.



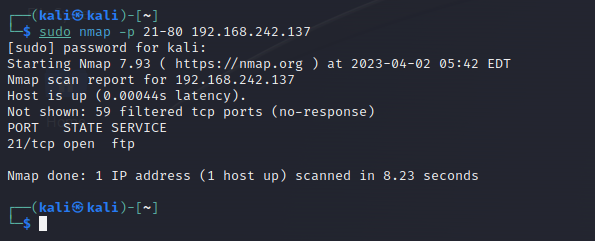
Hình 4. 10 Thêm tài khoản

Với tài khoản admin chúng ta sẽ tạo một virtual path là “/tmp” và đường dẫn tới vị trí thật trong ổ đĩa là “C:\Users\Administrator\Downloads”.



Hình 4. 11 Tạo folder ảo đồng thời cấp quyền

Trước tiên chúng ta sẽ kiểm tra các cổng đang mở trên windows server 2016



Hình 4. 12 Kiểm tra các dịch vụ đang hoạt động

Khi đã có thông tin chúng ta tiến hành Brute Force tài khoản mật khẩu của ftp trên kali linux bằng hydra và medusa, trước tiên chúng ta giả sử là có một file txt có chứa các dãy tài khoản dùng để brute force tài khoản.



Hình 4. 13 Tạo file userCustom.txt

Trong file userCustom.txt bao gồm các tài khoản dùng để brute force.

Graphical user interface, website

Description automatically generated

Hình 4. 14 Nội dung file userCustom.txt

Tiếp theo chúng ta tạo ra một file passCustom dùng để chứa các mật khẩu để phục vụ cho việc dò mật khẩu.



Hình 4. 15 Tạo file passCustom.txt

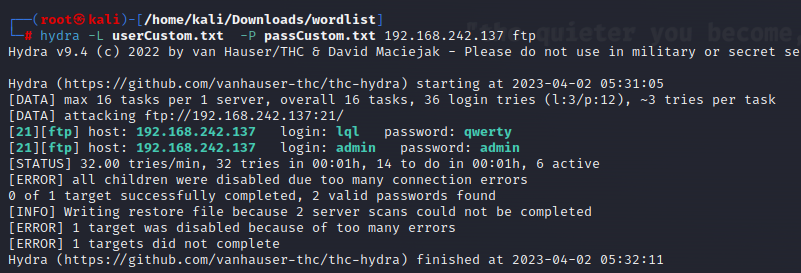
Nội dung của file passCustom dùng để dò mật khẩu.

Graphical user interface, text, application, chat or text message

Description automatically generated

Hình 4. 16 Nội dung file passCustom.txt

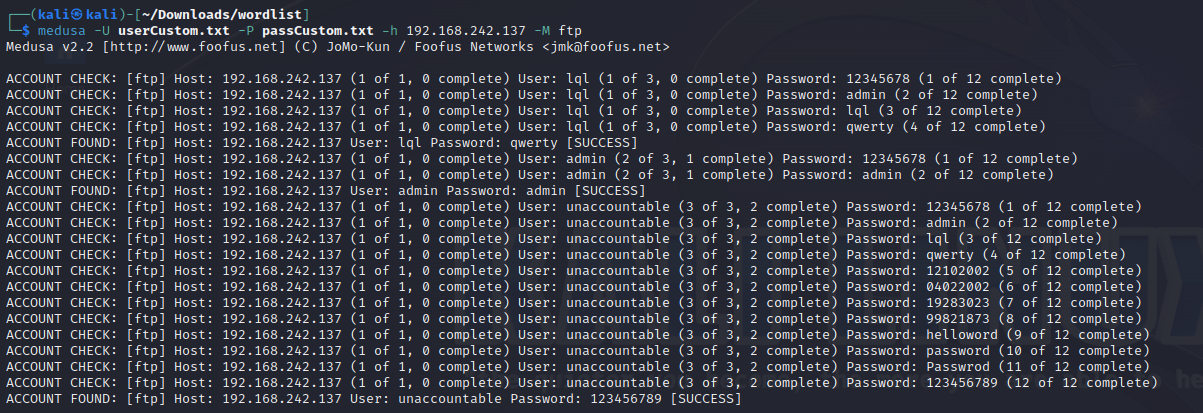
Chúng ta sẽ sử dụng lệnh *“hydra -L userCustom.txt  -P passCustom.txt 192.168.242.137 ftp”* với ý nghĩa là sẽ sử các tài khoản trong userCustom.txt và mật khẩu trong passCustom.txt tới ip của máy mục tiếu với dịch vụ là ftp.



Hình 4. 17 Dùng hydra để dò user, password

Như chúng ta thấy hydra có thể dò được 2/3 tài khoản mà chúng ta thiết lập lúc ban đầu, nhưng có thông báo lỗi khi mà số lượng kết nối lỗi trả về quá nhiều.

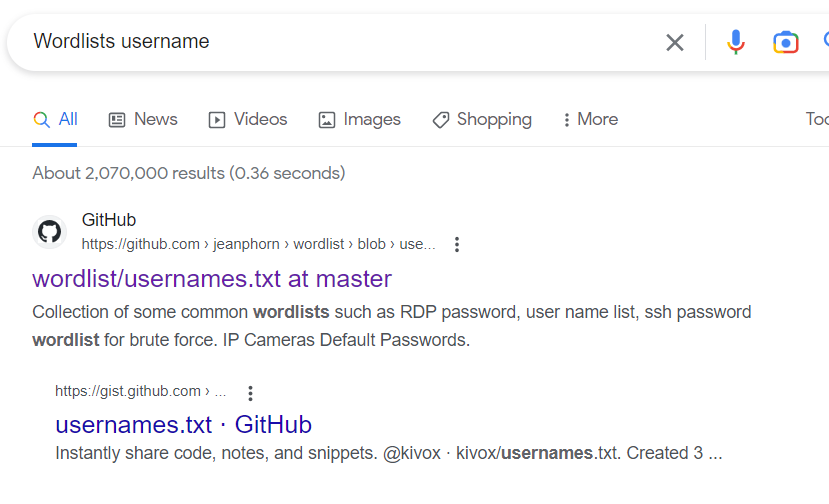
Tiếp theo chúng ta sẽ sử dụng medusa để brute force bằng lệnh sau *“medusa -U userCustom.txt -P passCustom.txt -h 192.168.242.137 -M ftp”* với ý nghĩa giống như hydra.



Hình 4. 18 Dùng medusa để dò user, password

Khi sử dụng tool này nó có thể quét hết các tài khoản mật khẩu trong file userCustom.txt mà ta đã liệt kê với mật khẩu tương ứng.

LƯU Ý: với file userCustom và passCustom chúng ta giả sử các tài khoản mật khẩu vì chúng ta là người thiết lập ftp server trong thực tế chúng ta có thể tải các wordlist ở trên github.



Hình 4. 19 Tải wordlist trên internetư

Tương tự vậy chúng ta có thể tìm wordlist với password.