



3

Lab

PHỤC VỤ MỤC ĐÍCH GIÁO DỤC
FOR EDUCATIONAL PURPOSE ONLY

Gather information & Vulnerability Scanning

Thực hành môn An toàn mạng

Tháng 9/2024

Lưu hành nội bộ

<Nghiêm cấm đăng tải trên internet dưới mọi hình thức>

A. TỔNG QUAN

1. Mục tiêu

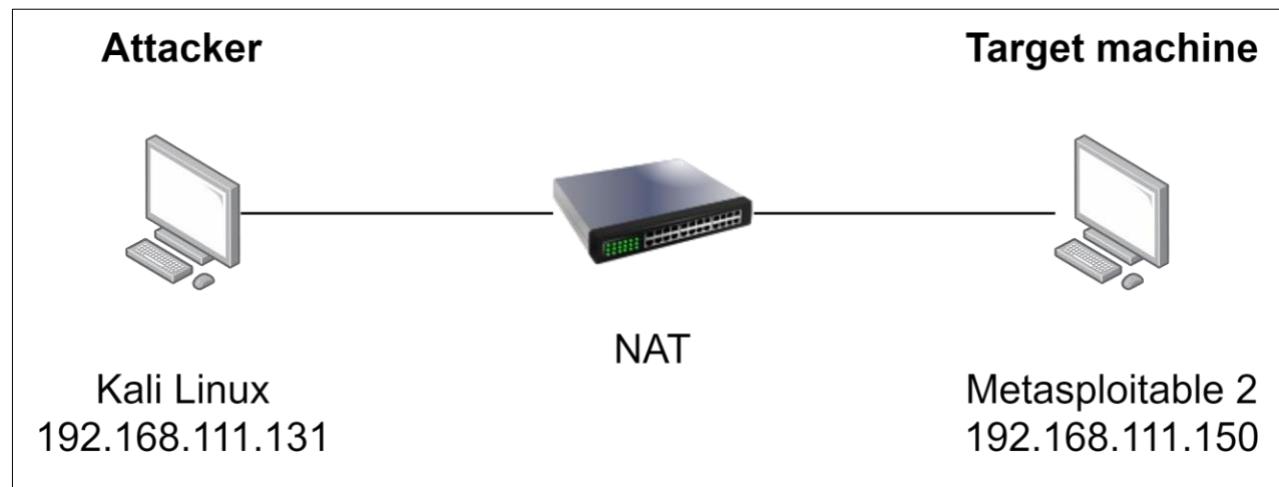
- Thu thập thông tin trên mạng
- Hiểu và sử dụng thành thạo các công cụ quét lỗ hổng tự động như Nessus, OpenVAS và Nmap.

2. Thời gian thực hành

- Thực hành tại lớp: 5 tiết tại phòng thực hành.
- Hoàn thành báo cáo kết quả thực hành: tối đa 13 ngày.

B. CHUẨN BỊ MÔI TRƯỜNG

- Cài đặt 2 máy ảo: Kali Linux và Metasploitable2 (Kali Linux: <https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/>. Metasploitable 2: <http://downloads.metasploit.com/data/metasploitable/metasploitable-linux-2.0.0.zip>)



Hình 1 Mô hình mạng bài thực hành

C. THỰC HÀNH

1. Thu thập thông tin thụ động (Passive Information Gathering)

Thu thập thông tin thụ động (hay còn gọi là Open-source Intelligence hay OSINT) là quá trình thu thập các thông tin về đối tượng thông qua các phương tiện công cộng như Internet, tạp chí, báo, ... mà không có bất kỳ sự tương tác trực tiếp nào đến đối tượng đó. Có 2 cách thu thập thông tin thụ động:

- Cách 1: Chúng ta sẽ không bao giờ tương tác trực tiếp với đối tượng. Ví dụ, chúng ta có thể dựa vào kết quả từ bên thứ 3 để có được thông tin mà không truy cập vào bất kỳ hệ thống hoặc máy chủ nào của đối tượng. Việc sử dụng phương pháp này giúp ta giữ được tính

bí mật về các hành động và ý định của mình, nhưng nhược điểm là có thể kết quả tìm kiếm sẽ bị giới hạn lại.

- Cách 2: Chúng ta có thể tương tác với đối tượng, nhưng chỉ như người dùng Internet bình thường. Ví dụ, nếu website của đối tượng cho phép chúng ta đăng ký tài khoản, chúng ta có thể thực hiện điều đó. Tuy nhiên, việc đánh giá website để tìm kiếm lỗ hổng sẽ không nằm trong giai đoạn này. Chúng ta sẽ thiết lập một VPN tunnel giữa một máy tính client và một gateway, cho phép máy tính có thể truy cập an toàn vào mạng riêng thông qua gateway. Mô hình của chúng ta sẽ gồm ít nhất là 3 máy ảo: VPN client (Host U), VPN Server (gateway) và một host V trong mạng riêng ảo.

a. Do thám website (Website Reconnaissance)

Nếu đối tượng có triển khai website, chúng ta có thể thu thập các thông tin cơ bản bằng cách truy cập vào website của đối tượng. Các tổ chức nhỏ có thể chỉ có duy nhất 1 website, trong khi các tổ chức lớn có thể có nhiều website. Vì vậy, việc thu thập thông tin các tổ chức lớn có thể mất khá nhiều thời gian, nhưng đổi lại thông tin có được về tổ chức đó sẽ nhiều hơn.

Task 1: Thực hiện truy cập vào website của MegaCorp One tại (<https://www.megacorpone.com/>) và trả lời các câu hỏi sau:

- Từ trang web của MegaCorp One, hãy mô tả một chút về lĩnh vực hoạt động của công ty?
- Hãy liệt kê những thành viên đang làm việc cho MegaCorp One và một vài thông tin về những thành viên đó (địa chỉ email, chức vụ, tài khoản mạng xã hội)?
- Khi có được địa chỉ Email của các thành viên thuộc tổ chức, bạn có phát hiện ra
- được điều gì

b. Whois Enumeration

Whois là 1 dịch vụ TCP, công cụ, loại CSDL có thể cung cấp thông tin về tên miền như: Name servers (địa chỉ DNS đang trả về của tên miền), registrar (nhà quản lý tên miền, thường là các tổ chức, tập đoàn phân phối tên miền theo đuôi tên miền như Verisign, Mắt Bão, Namecheap, Godaddy, ...), ngày đăng ký tên miền... Chúng ta có thể thu thập các thông tin cơ bản về tên miền sử dụng công cụ whois.

```
root@kali:~# whois megacorpone.com
Domain Name: MEGACORPONE.COM
Registry Domain ID: 1775445745_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.gandi.net
Registrar URL: http://www.gandi.net
Updated Date: 2020-06-16T17:05:41Z
Creation Date: 2013-01-22T23:01:00Z
Registry Expiry Date: 2024-01-22T23:01:00Z
Registrar: Gandi SAS
Registrar IANA ID: 81
Registrar Abuse Contact Email: abuse@support.gandi.net
Registrar Abuse Contact Phone: +33.170377661
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferP
rohibited
Name Server: NS1.MEGACORPONE.COM
Name Server: NS2.MEGACORPONE.COM
Name Server: NS3.MEGACORPONE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2020-08-20T07:51:25Z <<<
For more information on Whois status codes, please visit https://icann.org/epp
NOTICE: The expiration date displayed in this record is the date the
```

Hình 2 Sử dụng whois trên tên miền megacorpone.com

Không phải tất cả dữ liệu đều có ích, nhưng chúng ta đã có thể lấy được một số thông tin có giá trị. Đầu tiên, kết quả whois cho ta biết được Alan Grofield là người đăng ký tên miền. Dựa vào trang giới thiệu công ty, ta biết được Alan là “IT and Security Director”.

```
The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: megacorpone.com
Registry Domain ID: 1775445745_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.gandi.net
Registrar URL: http://www.gandi.net
Updated Date: 2020-06-16T19:05:41Z
Creation Date: 2013-01-22T23:01:00Z
Registrar Registration Expiration Date: 2024-01-22T23:01:00Z
Registrar: GANDI SAS
Registrar IANA ID: 81
Registrar Abuse Contact Email: abuse@support.gandi.net
Registrar Abuse Contact Phone: +33.170377661
Reseller:
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Domain Status:
Domain Status:
Domain Status:
Domain Status:
Registry Registrant ID:
Registrant Name: Alan Grofield
Registrant Organization: MegaCorpOne
Registrant Street: 2 Old Mill St
Registrant City: Rachel
Registrant State/Province: Nevada
Registrant Postal Code: 89001
Registrant Country: US
Registrant Phone: +1.9038836342
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: 3310f82fb4a8f79ee9a6bfe8d672d87e-1696395@contact.gandi.net
Registry Admin ID:
Admin Name: Alan Grofield
```

Hình 3 Thông tin của người đăng ký tên miền

Ngoài ra, kết quả trả về của whois còn cho chúng ta biết được các name server của MegaCorp One. Name server là một trong những thành phần của DNS, và sẽ không được đề cập chi tiết trong bài thực hành này.

```
root@kali:~# whois megacorpone.com
Domain Name: MEGACORPONE.COM
Registry Domain ID: 1775445745_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.gandi.net
Registrar URL: http://www.gandi.net
Updated Date: 2020-06-16T17:05:41Z
Creation Date: 2013-01-22T23:01:00Z
Registry Expiry Date: 2024-01-22T23:01:00Z
Registrar: Gandi SAS
Registrar IANA ID: 81
Registrar Abuse Contact Email: abuse@support.gandi.net
Registrar Abuse Contact Phone: +33.170377661
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: NS1.MEGACORPONE.COM
Name Server: NS2.MEGACORPONE.COM
Name Server: NS3.MEGACORPONE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
```

Hình 4 Các name server đang quản lý tên miền megacorpone.com

Task 2: Sử dụng công cụ whois trả lời các câu hỏi sau:

- a. Xác định các name server của MegaCorp One.
- b. Có thể tìm kiếm các thông tin của trường Đại học Công nghệ Thông tin (uit.edu.vn) có được không? Giải thích?
- c. Thu thập thông tin về tên miền uit.edu.vn và hãy cho biết các thông tin như: Ngày đăng ký tên miền, Ngày hết hạn tên miền, Chủ sở hữu tên miền, Các name server của tên miền

c. Google Hacking

Thuật ngữ “Google Hacking” trở nên phổ biến bởi Jonny Long vào năm 2001. Ông ấy đã chỉ ra cách sử dụng các search engine như Google có thể lấy được các thông tin, lỗ hổng quan trọng các website cấu hình sai.

Hãy thử một vài từ khóa cơ bản. Từ khóa **site** chỉ thực hiện tìm kiếm trên một tên miền nhất định.



Hình 5 Tìm kiếm với từ khóa site

Từ khóa **filetype** (hoặc **ext**) để chỉ hiển thị các kết quả có phần mở rộng của tập tin theo chỉ định.



google.com/search?sxsrf=ALeKk03uT6obnwl76d2eo0ltTWiZc1ymAg%3A1598067131092&ei=u5FAX82nBdP4wAP1_LcQ&q=sit

site:megacorpone.com filetype:html

All Images News Shopping More Settings Tools

3 results (0.16 seconds)

[www.megacorpone.com › about](#)
About Us - MegaCorp One
Chief Executive Officer, Joe Sheer, has been featured in the Journal of NanoTimes stating: Our team is creating the building blocks of modern society, where ...

[www.megacorpone.com › jobs](#)
Nanotechnology Is the Future - MegaCorp One
IT Positions. Citrix Administrator. Maintain, secure, and expand the MegaCorp One Citrix installation. Applicant must be well versed with remote work conditions ...

[www.megacorpone.com › contact](#)
Contact Us - MegaCorp One
Name: Joe Sheer. Title: CEO Email: joe@megacorpone.com. Name: Mike Carlow. Title: VP Of Legal Email: mcarlow@megacorpone.com. Name: Alan Grofield.

Hình 6 Sử dụng từ khóa filetype để hiển thị các kết quả có phần mở rộng của tập

Có thể thêm ký tự “-” để loại bỏ các kết quả tìm kiếm không mong muốn.



site:megacorpone.com -filetype:html

All Images News Shopping More Settings Tools

About 20 results (0.17 seconds)

[www.megacorpone.com › assets](#)

Index of /assets - MegaCorp One

Name · Last modified · Size · Description. [DIR], Parent Directory, -, [DIR], css/, 21-Aug-2016 11:21, -, [DIR], fonts/, 21-Aug-2016 11:21, -, [DIR], img/, 03-Oct-2017 ...

[www.megacorpone.com](#)

400 Bad Request

Bad Request. Your browser sent a request that this server could not understand. Reason: You're speaking plain HTTP to an SSL-enabled server port.

[www.megacorpone.com › assets › img](#)

Index of /assets/img - MegaCorp One

Name · Last modified · Size · Description. [DIR], Parent Directory, -, [IMG], agency.jpg, 21-Aug-2016 11:21, 166K. [IMG], browser.png, 21-Aug-2016 11:21, 211K.

[www.megacorpone.com › assets](#)

Index of /assets/js - MegaCorp One

Name · Last modified · Size · Description. [DIR], Parent Directory, -, [], bootstrap.min.js, 21-Aug-2016 11:21, 28K. [], custom.js, 21-Aug-2016 11:21, 368. [] ...

Hình 7 Sử dụng thêm ký tự “-” để loại bỏ các mục không mong muốn

Những ví dụ cơ bản trên chỉ là một số từ khóa thông dụng. Google Hacking Database (<https://www.exploit-db.com/google-hacking-database>) chứa nhiều từ khóa thường được sử dụng trong giai đoạn thu thập thông tin của đối tượng.

Google Hacking Database

Show 15

Date Added Dork

Date	Dork Query	Category	Author
2020-08-21	intext:admin ext:sql inurl:admin	Files Containing Juicy Info	Anshul T
2020-08-21	intitle:"NVR LOGIN"-inurl:"nvr com www net"	Pages Containing Login Portals	Sibi Mathew George
2020-08-21	inurl:'view.shtml' "Network Camera"	Various Online Devices	Alexandros Pappas
2020-08-20	ext:log intext:NetworkManager "systemd"	Files Containing Juicy Info	Mayank Sharma
2020-08-20	inttitle:Tuxedo Connected Controller	Various Online Devices	Alexandros Pappas
2020-08-20	inurl:/config/cam_portal.cgi "Panasonic"	Various Online Devices	Alexandros Pappas
2020-08-20	site:*/piwik "Sign in" "Matomo"	Pages Containing Login Portals	Alexandros Pappas
2020-08-19	inurl:~/login?csrfkey= intitle:cisco email security"	Pages Containing Login Portals	Adithya Chandra
2020-08-17	inurl: *eservices/login	Various Online Devices	Jitendra Kumar Tripathi
2020-08-17	intitle:axigen webadmin	Pages Containing Login Portals	Edwyn Sanders
2020-08-17	"EMAIL_HOST_PASSWORD" ext:yaml ext:env ext:txt ext:log	Files Containing Passwords	Alexandros Pappas

Hình 8 Google Hacking Database (GHDB)

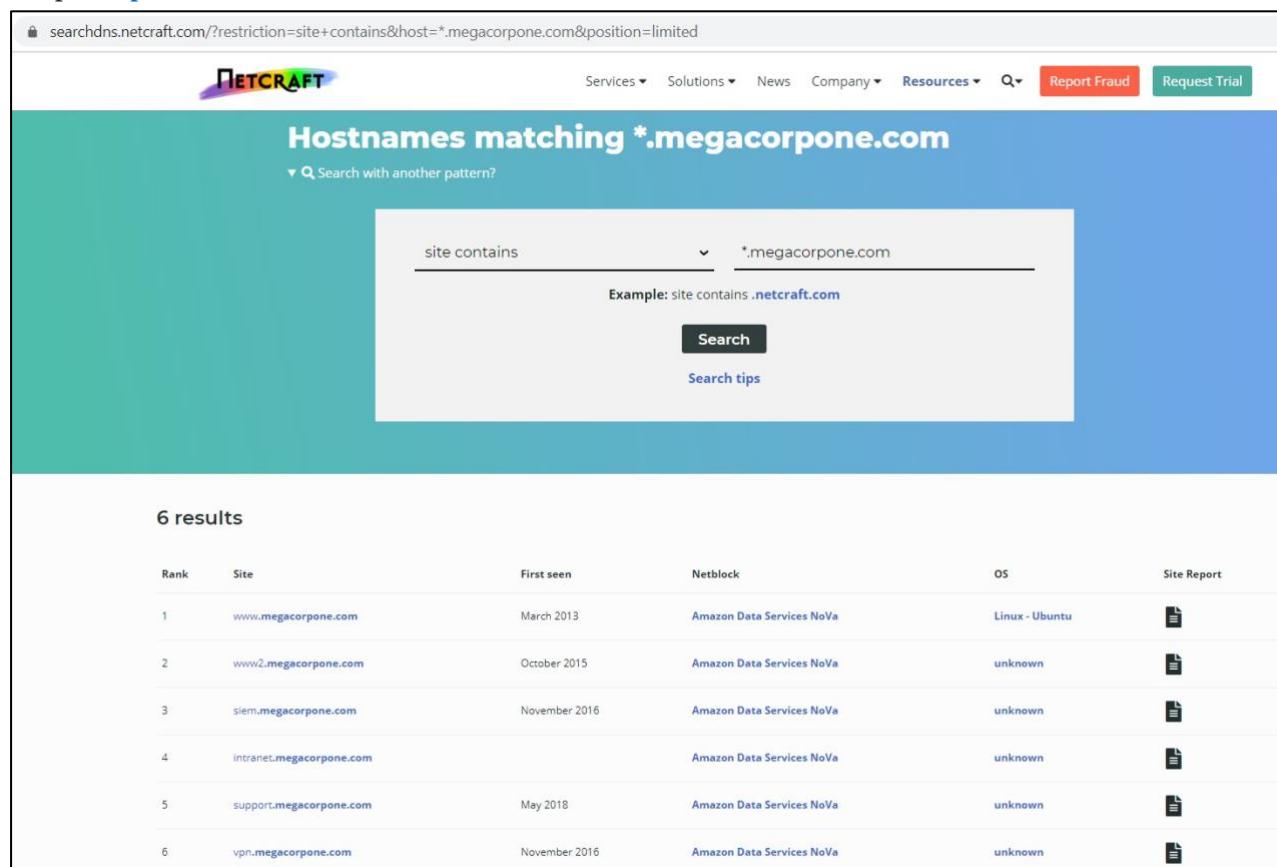
Task 3: Trả lời các câu hỏi sau:

- Ai là Phó chủ tịch Pháp lý (Vice President of Legal) của MegaCorp One và địa chỉ email của họ là gì?
- Bạn có thể tìm kiếm thêm các nhân viên khác của MegaCorp One mà không được liệt kê trên trang web www.megacorpone.com?
- Liệt kê một vài từ khóa thường gặp trên Google và cho ví dụ? (Yêu cầu: ít nhất 5 từ khóa)
- Thực hiện tìm kiếm các tài liệu thú vị của Trường Đại học Công nghệ Thông tin mà được công bố trên Internet mà theo bạn là không nên được công bố?

d. Netcraft

Netcraft là một công ty dịch vụ trên Internet có trụ sở tại Anh, cung cấp một cổng thông tin miễn phí thực hiện các chức năng thu thập thông tin khác nhau. Sử dụng các dịch vụ như Netcraft cung cấp được coi là một kỹ thuật thu thập thông tin thụ động vì chúng ta không bao giờ tương tác trực tiếp với đối tượng của mình.

Ví dụ: Netcraft cung cấp dịch vụ tìm kiếm thông tin DNS liên quan đến tên miền cần thu thập (<https://searchdns.netcraft.com/>).



The screenshot shows the Netcraft search interface. In the search bar, the query "site contains *.megacorpone.com" is entered. Below the search bar, there are 6 results listed in a table. The columns include Rank, Site, First seen, Netblock, OS, and Site Report. The results are as follows:

Rank	Site	First seen	Netblock	OS	Site Report
1	www.megacorpone.com	March 2013	Amazon Data Services NoVa	Linux - Ubuntu	Report
2	www2.megacorpone.com	October 2015	Amazon Data Services NoVa	unknown	Report
3	siem.megacorpone.com	November 2016	Amazon Data Services NoVa	unknown	Report
4	intranet.megacorpone.com		Amazon Data Services NoVa	unknown	Report
5	support.megacorpone.com	May 2018	Amazon Data Services NoVa	unknown	Report
6	vpn.megacorpone.com	November 2016	Amazon Data Services NoVa	unknown	Report

Hình 9 Kết quả tìm kiếm các hostname chứa *.megacorpone.com

Ứng với mỗi máy chủ được tìm thấy, chúng ta có thể xem các thông tin bổ sung và lịch sử về máy chủ bằng cách sử dụng tính năng “Site Report”.

Background	Value	Network	Value
Site title	MegaCorp One - Nanotechnology Is the Future	Date first seen	March 2013
Site rank	104647	Netcraft Risk Rating	Not Present
Description	Not Present	Primary language	English
Network			
Site	http://www.megacorpone.com	Domain	megacorpone.com
Netblock Owner	Amazon Data Services NoVa	Nameserver	ns1.megacorpone.com
Hosting company	Amazon - US East (Northern Virginia) datacenter	Domain registrar	gandi.net
Hosting country	us	Nameserver organisation	whois.gandi.net
IPv4 address	3.220.87.155 (VirusTotal)	Organisation	MegaCorpOne, Rachel, 89001, United States
IPv4 autonomous systems	AS14618	DNS admin	admin@megacorpone.com
IPv6 address	Not Present	Top Level Domain	Commercial entities (.com)
IPv6 autonomous systems	Not Present	DNS Security Extensions	unknown
Reverse DNS	ec2-3-220-87-155.compute-1.amazonaws.com		

Hình 10 Site Report đối với máy chủ www.megacorpone.com

Task 4: Sử dụng Netcraft để xác định máy chủ ứng dụng (application server) đang chạy trên www.megacorpone.com

e. Recon-ng

Recon-ng là một nền tảng theo module cho mục đích thu thập thông tin dựa trên web. Recon-ng hiển thị kết quả trên terminal hoặc CSDL. Điểm mạnh của recon-ng là có thể đưa kết quả từ module này làm đầu vào cho module khác, cho phép chúng ta nhanh chóng mở rộng phạm vi thu thập thông tin của mình. Để sử dụng, thực hiện lệnh **recon-ng**.

Hình 11 Khởi động recon-ng

Theo như kết quả sau khi khởi động recon-ng, chúng ta cần cài đặt thêm module để có thể sử dụng recon-ng. Chúng ta có thể thêm các module từ “Marketplace”. Sử dụng lệnh **marketplace search** để tìm kiếm các module của recon-ng.

```
[recon-ng][default] > marketplace search github
[*] Searching module index for 'github'...

+-----+
|          Path          | Version | Status    | Updated   | D | K |
+-----+
| recon/companies-multi/github_miner | 1.1     | not installed | 2020-05-15 |   | * |
| recon/profiles-contacts/github_users | 1.0     | not installed | 2019-06-24 |   | * |
| recon/profiles-profiles/profiler | 1.0     | not installed | 2019-06-24 |   |   |
| recon/profiles-repositories/github_repos | 1.1     | not installed | 2020-05-15 |   | * |
| recon/repositories-profiles/github_commits | 1.0     | not installed | 2019-06-24 |   | * |
| recon/repositories-vulnerabilities/github_dorks | 1.0     | not installed | 2019-06-24 |   | * |
+-----+
D = Has dependencies. See info for details.
K = Requires keys. See info for details.
```

Hình 12 Tìm kiếm các module chưa từ khóa github

Dựa vào Hình 12, lưu ý cột “K”, chúng ta thấy có một số module được đánh dấu *. Các module này yêu cầu cung cấp thông tin đăng nhập hoặc API key cho các nhà cung cấp bên thứ 3. Một vài key sẽ được miễn phí nếu đăng ký tài khoản, trong khi sẽ có một vài key yêu cầu trả phí.

Sử dụng lệnh **marketplace info** để biết thông tin của module.

```
[recon-ng][default] > marketplace info recon/companies-multi/github_miner
+---+
| path      | recon/companies-multi/github_miner
| name      | GitHub Resource Miner
| author    | Tim Tomes (@lanmaster53)
| version   | 1.1
| last_updated | 2020-05-15
| description | Uses the Github API to enumerate repositories and member profiles associated with a company search string. Updates the respective tables with the results.
| required_keys | ['github_api']
| dependencies | []
| files     | []
| status    | not installed
+---+
```

Hình 13 Thông tin về module có yêu cầu key

```
[recon-ng][default] > marketplace info recon/domains-hosts/google_site_web
+---+
| path      | recon/domains-hosts/google_site_web
| name      | Google Hostname Enumerator
| author    | Tim Tomes (@lanmaster53)
| version   | 1.0
| last_updated | 2019-06-24
| description | Harvests hosts from Google.com by using the 'site' search operator. Updates the 'hosts' table with the results.
| required_keys | []
| dependencies | []
| files     | []
| status    | not installed
+---+
```

Hình 14 Thông tin về module không cần key

Sử dụng lệnh **marketplace install** để thực hiện cài đặt module.

```
[recon-ng][default] > marketplace install recon/domains-hosts/netcraft
[*] Module installed: recon/domains-hosts/netcraft
[*] Reloading modules...
[recon-ng][default] >
```

Hình 15 Cài đặt module

Sau khi cài đặt module, sử dụng lệnh **modules load** để sử dụng module đó. Sau đó dùng lệnh **info** để hiển thị thông tin chi tiết về module và các tham số yêu cầu.

```
[recon-ng][default] > modules load recon/domains-hosts/netcraft
[recon-ng][default][netcraft] > info

    Name: Netcraft Hostname Enumerator
    Author: thrapt (thrapt@gmail.com)
    Version: 1.1

Description:
    Harvests hosts from Netcraft.com. Updates the 'hosts' table with the results.

Options:
Name   Current Value  Required  Description
-----  -----  -----  -----
SOURCE  default        yes      source of input (see 'info' for details)

Source Options:
default      SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
<string>     string representing a single input
<path>       path to a file containing a list of inputs
query <sql>   database query returning one column of inputs

[recon-ng][default][netcraft] > 
```

Hình 16 Sử dụng module `recon/domains-hosts/netcraft`

Dựa vào kết quả Hình 16, module này yêu cầu tham số đầu vào là `source`, là đối tượng mà chúng ta cần thu thập thông tin. Trong trường hợp này, sử dụng lệnh `options set SOURCE megacorpone.com` để thiết lập tên miền của mục tiêu.

```
[recon-ng][default][google_site_web] > options set SOURCE megacorpone.com
SOURCE => megacorpone.com
[recon-ng][default][google_site_web] >
```

Hình 17 Thiết lập mục tiêu cần thu thập thông tin

Chạy lên `run` để khởi chạy module.

```
[recon-ng][default][netcraft] > run
-----
[MEGACORPONE.COM]
-----
[*] URL: http://searchdns.netcraft.com/?restriction=site%2Bends%2Bwith&host=megacorpone.com
[*] Country: None
[*] Host: www.megacorpone.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] Country: None
[*] Host: vpn.megacorpone.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] Country: None
[*] Host: siem.megacorpone.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] Country: None
[*] Host: www2.megacorpone.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] Country: None
[*] Host: intranet.megacorpone.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] Country: None
[*] Host: support.megacorpone.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[SUMMARY]
-----
[*] 6 total (6 new) hosts found.
[recon-ng][default][netcraft] >
```

Hình 18 Chạy module

Sử dụng lệnh **show hosts** để xem lịch sử các host đã được tìm thấy.

```
[recon-ng][default][netcraft] > back
[recon-ng][default] > show hosts

+-----+
| rowid | host | ip_address | region | country | latitude | longitude | notes | module |
+-----+
| 1 | www.megacorpone.com | | | | | | netcraft |
| 2 | vpn.megacorpone.com | | | | | | netcraft |
| 3 | siem.megacorpone.com | | | | | | netcraft |
| 4 | www2.megacorpone.com | | | | | | netcraft |
| 5 | intranet.megacorpone.com | | | | | | netcraft |
| 6 | support.megacorpone.com | | | | | | netcraft |
+-----+
[*] 6 rows returned
```

Hình 19 Xem lịch sử các host

Task 5:

- Thực hiện sử dụng module có thể giúp phân giải tên miền ở Hình thành địa chỉ IP tương ứng.
- Sử dụng một số module khác có trong recon-ng để thu thập thông tin về UIT nhiều nhất có thể.

f. Open-Source Code

Một trong những nơi để thu thập thông tin là ở những nơi lưu trữ mã nguồn mở, tập trung như GitHub, GitLab, SourceForge.

Truy cập vào GitHub của MegaCorp One (<https://github.com/megacorpone>), sử dụng từ khóa `file:users` để tìm kiếm các tập tin có chứa từ khóa “users”.

Hình 20 Tìm kiếm tập tin trong GitHub

Truy cập vào GitHub của MegaCorp One (<https://github.com/megacorpone>), sử dụng từ khóa `file:users` để tìm kiếm các tập tin có chứa từ “users”.

Kết quả tìm kiếm chỉ trả về một tập tin duy nhất – xampp.users. Tuy nhiên, lưu ý XAMPP là môi trường phát triển ứng dụng web, vì vậy có thể xem đây là 1 phát hiện khá có ích.

The screenshot shows a GitHub search interface. At the top, there's a search bar with the query 'user:megacorpone filename:users'. Below the search bar are navigation links: Pull requests, Issues, Marketplace, and Explore. On the left, there's a sidebar with repository statistics: Repositories (2), Code (1), Commits (0), Issues (1), Discussions (Beta, 0), Packages (0), Marketplace (5K), Topics (721K), Wikis (0), and Users (1). The main area displays the search results with the title '1 code result'. It shows a single file named 'xampp.users' from the repository 'megacorpone/xampp.users'. The file was last indexed on 11 Jul, 2018. Below the results are links for Advanced search and Cheat sheet.

Hình 21 Kết quả trả về sau khi tìm kiếm trên GitHub

Kiểm tra nội dung của tập tin này. Tập tin này chứa tên đăng nhập và mật khẩu (dưới dạng mã hash), sẽ rất có ích trong các giai đoạn sau.

The screenshot shows a GitHub repository page for 'xampp.users'. The repository is owned by 'megacorpone.com / megacorpone'. It has 1 contributor and 1 line of code. The code content is: 'trivera:\$apr1\$A0vSKwao\$GV3sgGAj53j.c3GkS4oUC0'. This is a password hash.

Hình 22 Nội dung tập tin xampp.users chứa username và password (dạng hash)

Tuy nhiên, hướng tiếp cận này sẽ hoạt động tốt nhất đối với các repository nhỏ. Đối với các repo lớn hơn, chúng ta có thể sử dụng thêm các công cụ để giúp tự động tìm kiếm như Gitrob (<https://github.com/michenriksen/gitrob>), Gitleaks (<https://github.com/zricethezav/gitleaks>).

Task 6: Sử dụng 1 trong 2 công cụ Gitrob hoặc Gitleaks để tìm kiếm các thông tin nhạy cảm bị rò rỉ đối với các trường đại học thành viên trong ĐHQG

2. Thu thập thông tin chủ động

a. DNS Enumeration

Hệ thống tên miền (Domain Name System – DNS) là một trong những hệ thống quan trọng nhất trên Internet và là một cơ sở dữ liệu phân tán chịu trách nhiệm chuyển đổi tên miền thành địa chỉ IP.

Tương tác với máy chủ DNS

Mỗi tên miền có thể sử dụng các loại bản ghi DNS khác nhau. Một số bản ghi DNS phổ biến nhất bao gồm:

- **NS** – Bản ghi Nameserver chứa tên của máy chủ có thẩm quyền (authoritative server) lưu trữ các bản ghi DNS cho một tên miền nào đó.
- **A** – Còn được gọi là bản ghi host, dùng để phân giải Host ra một địa chỉ 32-bit IPv4. Dùng để trỏ tên website như www.domain.com đến một Server Hosting website đó.
- **MX** – Bản ghi Mail Exchange chứa tên của các máy chủ có nhiệm vụ xử lý email cho tên miền. Một tên miền có thể chứa nhiều bản ghi MX
- **PTR** – Bản ghi Pointer được sử dụng trong reverse lookup zones và được sử dụng để tìm kiếm các hostname tương ứng với địa chỉ IP muốn tìm kiếm.
- **CNAME** – Bản ghi Canonical Name được sử dụng để tạo các bí danh (alias) cho các bản ghi host,
- **TXT** – Các bản ghi Text có thể chứa các dữ liệu bất kỳ và có thể được sử dụng cho các mục đích khác nhau, chẳng hạn như chứng nhận quyền sở hữu tên miền.

Do có rất nhiều thông tin được chứa bên trong DNS, nó thường là mục tiêu trong giai đoạn thu thập thông tin chủ động.

Sử dụng lệnh **host** để tìm địa chỉ IP của www.megacorpone.com

```
root@kali:~# host www.megacorpone.com
www.megacorpone.com has address 3.220.87.155
```

Hình 23 Sử dụng lệnh host để tìm A record cho tên miền www.megacorpone.com

Mặc định, lệnh **host** sẽ tìm kiếm bản ghi A, nhưng chúng ta có thể yêu cầu các bản ghi khác, như TXT hoặc MX. Sử dụng tùy chọn **-t** để chỉ định loại bản ghi muốn tìm kiếm.

```
root@kali:~# host -t txt megacorpone.com
megacorpone.com descriptive text "Try Harder"
megacorpone.com descriptive text "google-site-verification=U7B_b0HNeBtY4qYGQZNsEYXfCJ32hMNV3GtC0wWq5pA"
root@kali:~# host -t mx megacorpone.com
megacorpone.com mail is handled by 50 mail.megacorpone.com.
megacorpone.com mail is handled by 60 mail2.megacorpone.com.
megacorpone.com mail is handled by 20 spool.mail.gandi.net.
megacorpone.com mail is handled by 10 fb.mail.gandi.net.
```

Hình 24 Sử dụng lệnh host để tìm kiếm các bản ghi TXT và MX cho tên miền megacorpone.com

Task 7:

- Ngoài các bản ghi kể trên, hãy liệt kê các bản ghi khác của DNS.
- Sử dụng lệnh host để tìm kiếm các bản ghi TXT, MX cho tên miền uit.edu.vn

Tra cứu tự động (Automation Lookups)

Bây giờ chúng ta đã thu thập được một số thông tin từ tên miền megacorpone.com, chúng ta có thể tiếp tục sử dụng thêm các truy vấn DNS để tìm kiếm các hostname và địa chỉ IP cùng thuộc một tên miền.

Sử dụng lại lệnh host đối với máy chủ www.megacorpone.com.

```
root@kali:~# host www.megacorpone.com
www.megacorpone.com has address 3.220.87.155
root@kali:~#
```

Hình 25 Sử dụng lệnh host cho hostname hợp lệ

Bây giờ, kiểm tra xem liệu megacorpone.com có máy chủ với hostname tên là “noexist”. Theo dõi sự khác nhau giữa các kết quả trả về.

```
root@kali:~# host noexist.megacorpone.com
Host noexist.megacorpone.com not found: 3(NXDOMAIN)
root@kali:~#
```

Hình 26 Sử dụng lệnh host cho hostname không hợp lệ

Trong Hình 25, chúng ta đã truy vấn một hostname hợp lệ và đã nhận được địa chỉ phân giải IP tương ứng. Ngược lại, ở Hình 26, kết quả báo lỗi hostname không tìm thấy cho ta biết bản ghi DNS không tồn tại đối với hostname này. Bây giờ chúng ta đã hiểu được cách tìm kiếm các hostname hợp lệ, chúng ta có thể tự động hóa quá trình này.

Task 8: Sử dụng lệnh host cho các hostname không tồn tại trong tên miền uit.edu.vn (idontexist, noexist, baithuchanhso2). Có nhận xét gì về kết quả trả về hay không? Giải thích?

Forward Lookup Brute Force

Brute Force là kỹ thuật tìm kiếm thông tin hợp lệ, bao gồm các thư mục trên máy chủ web, các kết hợp username và password, hoặc trong trường hợp này, các bản ghi DNS hợp lệ. Bằng cách sử dụng danh sách chứa các hostname thông dụng, chúng ta có thể sử dụng để đoán các bản ghi DNS và kiểm tra kết quả trả về cho các hostname hợp lệ. Đầu tiên, tạo danh sách các hostname thường gặp.

```
root@kali:~/Desktop# cat list.txt
www
ftp
mail
owa
proxy
router
admin
www2
firewall
mx
pop3
dns
ca
root@kali:~/Desktop#
```

Hình 27 Danh sách các hostname thông dụng

Sử dụng Bash script để phân giải mỗi hostname có trong danh sách.

```
root@kali:~/Desktop# for ip in $(cat list.txt); do host $ip.megacorpone.com; done
www.megacorpone.com has address 3.220.87.155
Host ftp.megacorpone.com not found: 3(NXDOMAIN)
mail.megacorpone.com has address 3.220.61.179
Host owa.megacorpone.com not found: 3(NXDOMAIN)
Host proxy.megacorpone.com not found: 3(NXDOMAIN)
router.megacorpone.com has address 3.220.61.179
admin.megacorpone.com has address 3.220.61.179
www2.megacorpone.com has address 3.220.61.179
Host firewall.megacorpone.com not found: 3(NXDOMAIN)
Host mx.megacorpone.com not found: 3(NXDOMAIN)
Host pop3.megacorpone.com not found: 3(NXDOMAIN)
Host dns.megacorpone.com not found: 3(NXDOMAIN)
Host ca.megacorpone.com not found: 3(NXDOMAIN)
```

Hình 28 Sử dụng Bash script để brute force forward DNS name

Task 9: Sử dụng wordlist thông dụng khác (rockyou, seclists) để tìm kiếm các hostname hợp lệ khác của megacorpone.com

Reverse Lookup Brute Force

Ngoài dãy IP (3.220.X.Y) đã được tìm kiếm ở trên, tổ chức MegaCorp One còn dãy IP 38.100.193.X. Nếu quản trị viên của megacorpone.com cấu hình các bản ghi PTR cho teen miền này, chúng ta có thể quét địa chỉ IP trong dãy IP đó để tìm ra hostname thuộc MegaCorp One.

Chúng ta sẽ quét địa chỉ IP từ 38.100.193.50 đến 38.100.193.100. Sử dụng lệnh `grep -v` để loại bỏ các hostname không hợp lệ.

```
root@kali:~/Desktop# for ip in $(seq 50 100); do host 38.100.193.$ip;done | grep -v "not found"
66.193.100.38.in-addr.arpa domain name pointer syslog.megacorpone.com.
69.193.100.38.in-addr.arpa domain name pointer beta.megacorpone.com.
70.193.100.38.in-addr.arpa domain name pointer ns1.megacorpone.com.
72.193.100.38.in-addr.arpa domain name pointer admin.megacorpone.com.
73.193.100.38.in-addr.arpa domain name pointer mail2.megacorpone.com.
76.193.100.38.in-addr.arpa domain name pointer www.megacorpone.com.
77.193.100.38.in-addr.arpa domain name pointer vpn.megacorpone.com.
80.193.100.38.in-addr.arpa domain name pointer ns2.megacorpone.com.
84.193.100.38.in-addr.arpa domain name pointer mail.megacorpone.com.
85.193.100.38.in-addr.arpa domain name pointer snmp.megacorpone.com.
89.193.100.38.in-addr.arpa domain name pointer siem.megacorpone.com.
90.193.100.38.in-addr.arpa domain name pointer ns3.megacorpone.com.
91.193.100.38.in-addr.arpa domain name pointer router.megacorpone.com.
root@kali:~/Desktop#
```

Hình 29 Sử dụng Bash script để brute force reverse DNS name

Chúng ta có thể thấy, kết quả cho ta biết thêm các hostname hợp lệ khác như snmp, siem, mail2...

DNS Zone Transfers

Zone Transfer là một bản sao cơ sở dữ liệu giữa các máy chủ DNS liên quan trong đó tập tin zone được sao chép từ máy chủ DNS chính (Master DNS Server) sang máy chủ DNS phụ (Slave DNS Server). Tập tin zone chứa danh sách tất cả các tên DNS được cấu hình cho zone đó. Zone transfer chỉ được cho phép đối với các máy chủ DNS phụ có ủy quyền, nhưng nhiều quản trị viên cấu hình sai các máy chủ DNS và trong trường hợp này, bất kỳ ai yêu cầu bản sao của zone thường sẽ nhận được kết quả trả về.

Điều này chẳng khác nào đưa cho hacker danh sách các tên miền đầy đủ của tổ chức. Tất cả tên, địa chỉ và chức năng của máy chủ có thể bị lộ ra ngoài.

Việc chuyển vùng thành công không trực tiếp dẫn đến rò rỉ thông tin mạng, mặc dù nó là tiền đề, tạo điều kiện thuận lợi cho kẻ xấu.

Cú pháp lệnh host thực hiện zone transfer như sau:

```
host -l <domain-name> <dns server address>
```

Như đã biết ở trên, chúng ta biết được có 3 máy chủ DNS đang quản lý tên miền

megacorpone.com: ns1, ns2 và ns3.

Thử thực hiện zone transfer của mỗi máy chủ này. Sử dụng lệnh **host -l** (liệt kê các zone) để thực hiện zone transfer:

```
root@kali:~/Desktop# host -l megacorpone.com ns1.megacorpone.com
Using domain server:
Name: ns1.megacorpone.com
Address: 3.220.61.179#53
Aliases:

Host megacorpone.com not found: 5(REFUSED)
; Transfer failed.
root@kali:~/Desktop#
```

Hình 30 Thực hiện zone transfer ở nameserver ns1 thất bại

Đáng tiếc, nameserver đầu tiên, ns1, không cho phép thực hiện DNS zone transfer, vì vậy chúng ta thất bại. Thực hiện tương tự với nameserver kế tiếp, ns2.

```
root@kali:~/Desktop# host -l megacorpone.com ns2.megacorpone.com
Using domain server:
Name: ns2.megacorpone.com
Address: 3.211.51.86#53
Aliases:

megacorpone.com name server ns1.megacorpone.com.
megacorpone.com name server ns2.megacorpone.com.
megacorpone.com name server ns3.megacorpone.com.
admin.megacorpone.com has address 3.220.61.179
beta.megacorpone.com has address 3.220.61.179
fs1.megacorpone.com has address 3.220.61.179
intranet.megacorpone.com has address 3.220.61.179
mail.megacorpone.com has address 3.220.61.179
mail2.megacorpone.com has address 3.220.61.179
ns1.megacorpone.com has address 3.220.61.179
ns2.megacorpone.com has address 3.211.51.86
ns3.megacorpone.com has address 3.212.85.86
router.megacorpone.com has address 3.220.61.179
siem.megacorpone.com has address 3.220.61.179
snmp.megacorpone.com has address 3.220.61.179
support.megacorpone.com has address 3.212.85.86
syslog.megacorpone.com has address 3.220.61.179
test.megacorpone.com has address 3.220.61.179
vpn.megacorpone.com has address 3.220.61.179
www.megacorpone.com has address 3.220.87.155
www2.megacorpone.com has address 3.220.61.179
root@kali:~/Desktop#
```

Hình 31 Sử dụng lệnh host để minh họa DNS zone transfer

Nameserver này cho phép zone transfer và cung cấp tập tin zone đầy đủ cho tên miền megacorpone.com, cung cấp danh sách địa chỉ IP và hostname tương ứng.

Task 10: Viết một chương trình Bash script để liệt kê danh sách các nameserver của các đơn vị thành viên thuộc Đại học Quốc Gia TP.HCM (hcmus.edu.vn, hcmussh.edu.vn, uit.edu.vn,

hcmut.edu.vn, hcmiu.edu.vn, uel.edu.vn, hcmier.edu.vn, vnuhcm.edu.vn) và thực hiện zone transfer ứng với các nameserver đã tìm được.

b. Port Scanning

Port Scanning là quá trình kiểm tra các port TCP hoặc UDP trên máy từ xa với mục đích phát hiện những dịch vụ đang chạy trên máy mục tiêu và những khả năng tấn công tiềm ẩn ứng với các dịch vụ đó.

Điều cần thiết là phải hiểu ý nghĩa của việc scan port, cũng như ảnh hưởng khi thực hiện việc scan port. Do số lượng lưu lượng truy cập mà một số quá trình quét có thể tạo ra, cùng với tính chất xâm nhập của chúng, việc scan port một cách “mù quáng” có thể gây ra các tác động xấu đến hệ thống mục tiêu hoặc mạng khách hàng như làm quá tải máy chủ và liên kết mạng hoặc làm kích hoạt IDS. Việc scan sai có thể dẫn đến downtime cho khách hàng.

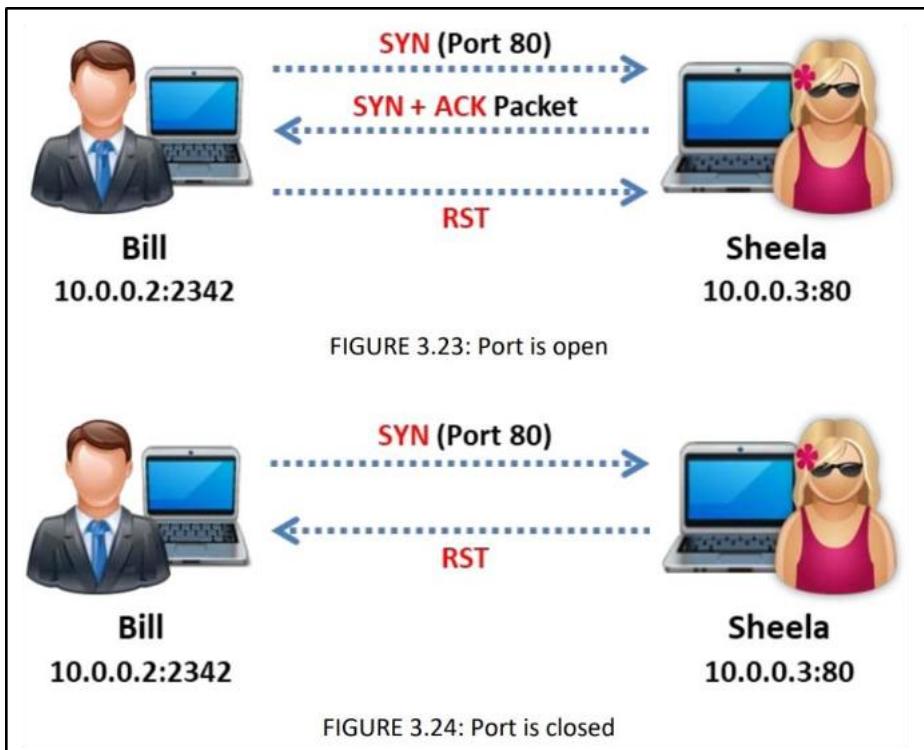
Port Scanning sử dụng Nmap

Nmap (viết bởi Gordon Lyon, hay còn gọi là Fyodor) là một trong những công cụ scan port phổ biến, linh hoạt và mạnh mẽ nhất hiện nay. Nó đã được phát triển tích cực trong hơn một thập kỷ và có nhiều tính năng ngoài chức năng scan port đơn thuần.

Stealth/SYN Scanning

Kỹ thuật quét ưa thích của Nmap là SYN, hay còn gọi là quét "stealth". Có nhiều lợi ích khi sử dụng SYN scan và do đó, nó là kỹ thuật quét mặc định được sử dụng khi không có kỹ thuật quét nào được chỉ định trong lệnh nmap.

SYN scanning là phương thức scan port TCP bằng cách gửi các gói tin SYN đến các port khác nhau trên máy mục tiêu mà không thực hiện quá trình bắt tay ba bước hoàn thiện. Nếu port TCP đó mở, SYN-ACK sẽ được gửi về từ máy mục tiêu, cho ta biết port đang mở. Tại thời điểm đó, Nmap sẽ không quan tâm đến việc gửi gói tin ACK để hoàn tất quá trình bắt tay ba bước.



Hình 32 TCP SYN Scan

```
root@kali:~/Desktop# sudo nmap -sS 192.168.111.150
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-27 12:31 EDT
Nmap scan report for 192.168.111.150
Host is up (0.0051s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp  -- uit.edu.vn ping statistics ---
22/tcp    open  ssh  -- packets transmitted, 0 received, 100% packet loss, time 0ms
23/tcp    open  telnet
25/tcp    open  smtp -- ping uit.edu.vn
53/tcp    open  domain  uit.edu.vn (192.69.123.142) 56(84) bytes of data.
80/tcp    open  http
111/tcp   open  rpcbind uit.edu.vn ping statistics ---
139/tcp   open  netbios-ssn -- transmitted, 0 received, 100% packet loss, time 0ms
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login -- ping uit.edu.vn
514/tcp   open  shell NG uit.edu.vn (192.69.123.142) 56(84) bytes of data.
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock uit.edu.vn ping statistics ---
2049/tcp  open  nfs  -- packets transmitted, 0 received, 100% packet loss, time 0ms
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql -- ping uit.edu.vn
5432/tcp  open  postgresql uit.edu.vn (192.69.123.142) 56(84) bytes of data.
5900/tcp  open  vnc
6000/tcp  open  X11 -- uit.edu.vn ping statistics ---
6667/tcp  open  irc  -- packets transmitted, 0 received, 100% packet loss, time 1013ms
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:FA:DD:2A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
root@kali:~/Desktop#
```

Hình 33 Sử dụng Nmap để thực hiện SYN scan

Bởi vì quá trình bắt tay ba bước chưa hoàn thành, thông tin sẽ không được chuyển đến tầng ứng dụng và kết quả là, sẽ không xuất hiện trong bất kỳ log của ứng dụng nào. SYN Scan cũng nhanh hơn và hiệu quả hơn vì ít gói tin được gửi và nhận hơn.

UDP Scanning

Không có quá trình bắt tay ba bước khi thực hiện quét UDP. Giao thức UDP có thể khó sử dụng hơn so với quét TCP vì khi gửi gói tin đến máy mục tiêu, bạn không thể xác định máy chủ còn sống (alive), chết (dead) hay đã được lọc (filtered). Tuy nhiên, bạn có thể sử dụng một gói tin ICMP để kiểm tra các port mở hoặc đóng. Nếu bạn gửi một gói UDP đến một port mà không có ứng dụng nào sử dụng, IP stack sẽ trả về một gói tin “ICMP port unreachable”. Nếu bất kỳ cổng nào trả về lỗi ICMP, chứng tỏ cổng đó đang đóng, còn nếu không có bất kỳ phản hồi nào, chứng tỏ cổng đó đang mở hoặc đang bị lọc thông qua firewall.

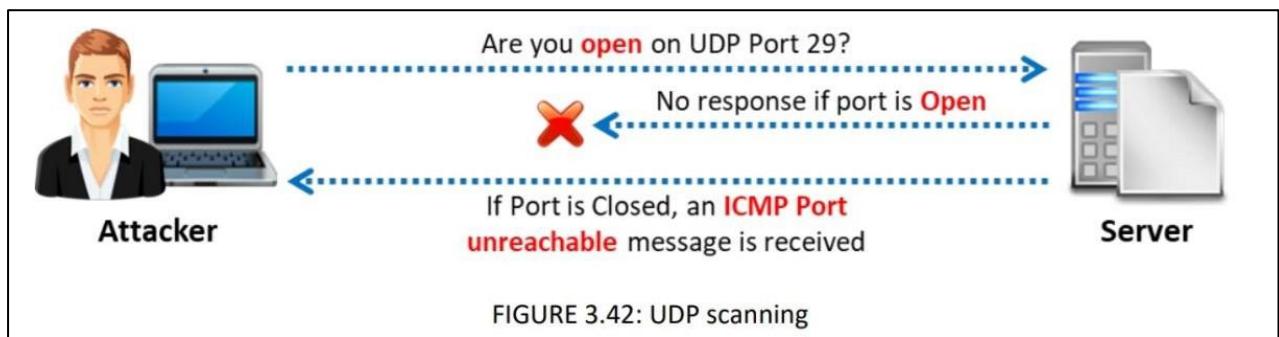


FIGURE 3.42: UDP scanning

Hình 34 UDP Scanning

```
root@kali:~/Desktop# sudo nmap -sU 192.168.111.150
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-27 13:01 EDT
Stats: 0:06:27 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 38.28% done; ETC: 13:18 (0:10:26 remaining)
Nmap scan report for 192.168.111.150
Host is up (0.00066s latency).
Not shown: 994 closed ports
PORT      STATE     SERVICE
53/udp    open      domain
69/udp    open|filtered tftp
111/udp   open      rpcbind
137/udp   open      netbios-ns
138/udp   open|filtered netbios-dgm
2049/udp  open      nfs
MAC Address: 00:0C:29:FA:DD:2A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1070.82 seconds
root@kali:~/Desktop#
```

Hình 35 Sử dụng Nmap để thực hiện UDP Scan

UDP Scan (-sU) có thể được sử dụng cùng với TCP SYN Scan (-sS) để tạo nên một bức tranh hoàn thiện đối với máy mục tiêu.

```
root@kali:~/Desktop# sudo nmap -sS -sU 192.168.111.150
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-27 13:20 EDT
Nmap scan report for 192.168.111.150
Host is up (0.00072s latency).

Not shown: 1925 closed ports, 48 open|filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
53/udp    open  domain
111/udp   open  rpcbind
137/udp   open  netbios-ns
2049/udp  open  nfs
MAC Address: 00:0C:29:FA:DD:2A (VMware)
```

Hình 36 Sử dụng Nmap thực hiện quét kết hợp UDP và SYN scan

Task 11: Thực hiện bắt Wireshark để mô tả cách gói tin được gửi và nhận khi thực hiện SYN Scan, TCP Connect Scan, UDP Scan sử dụng Nmap. So sánh với sử dụng phương thức các phương thức này với nhau (số lượng gói tin được gửi, số lượng gói tin được nhận, thời gian quét, kết quả hiển thị...)

Network Sweeping

Để xử lý số lượng lớn máy chủ hoặc để cố gắng duy trì lưu lượng mạng, chúng ta có thể cố gắng thăm dò mục tiêu bằng kỹ thuật Network Sweeping, trong đó chúng ta bắt đầu bằng cách scan rộng và sử dụng các lần scan cụ thể hơn đối với các máy chủ cần quan tâm. Khi thực hiện Network Sweeping với Nmap bằng cách sử dụng tùy chọn `-sn`, quá trình khám phá máy chủ không chỉ bao gồm việc gửi một gói tin ICMP echo request. Một số đầu dò khác được sử dụng cùng với ICMP request. Nmap cũng gửi một gói TCP SYN đến port 443, một gói TCP ACK đến port 80 và một ICMP timestamp request để xác minh xem máy chủ có sẵn hay không.

```
root@kali:~# nmap -sn 192.168.111.1-254
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-27 13:14 EDT
Nmap scan report for 192.168.111.1
Host is up (0.00055s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.111.2
Host is up (0.00017s latency).
MAC Address: 00:50:56:E5:A6:14 (VMware)
Nmap scan report for 192.168.111.150
Host is up (0.00027s latency).
MAC Address: 00:0C:29:FA:DD:2A (VMware)
Nmap scan report for 192.168.111.254
Host is up (0.00014s latency).
MAC Address: 00:50:56:E4:1A:EA (VMware)
Nmap scan report for 192.168.111.131
Host is up.
Nmap done: 254 IP addresses (5 hosts up) scanned in 1.77 seconds
root@kali:~#
```

Hình 37 Sử dụng nmap để thực hiện Network Sweep

Sử dụng tham số **-oG** để lưu kết quả ra định dạng có thể dễ dàng quản lý, tìm kiếm.

```
root@kali:~# nmap -v -sn 192.168.111.1-254 -oG ping-sweep.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-27 13:17 EDT
Initiating ARP Ping Scan at 13:17
Scanning 253 hosts [1 port/host]
Completed ARP Ping Scan at 13:17, 1.97s elapsed (253 total hosts)
Initiating Parallel DNS resolution of 253 hosts. at 13:17
Completed Parallel DNS resolution of 253 hosts. at 13:17, 0.00s elapsed
Nmap scan report for 192.168.111.1
Host is up (0.0017s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.111.2
Host is up (0.00016s latency).
MAC Address: 00:50:56:E5:A6:14 (VMware)
Nmap scan report for 192.168.111.3 [host down]
Nmap scan report for 192.168.111.4 [host down]
Nmap scan report for 192.168.111.5 [host down]
Nmap scan report for 192.168.111.6 [host down]
Nmap scan report for 192.168.111.7 [host down]
Nmap scan report for 192.168.111.8 [host down]
Nmap scan report for 192.168.111.9 [host down]
Nmap scan report for 192.168.111.10 [host down]
Nmap scan report for 192.168.111.11 [host down]
Nmap scan report for 192.168.111.12 [host down]
Nmap scan report for 192.168.111.13 [host down]
```

Hình 38 Sử dụng nmap để thực hiện Network Sweep và lưu kết quả vào tập tin

Sau đó, sử dụng lệnh **grep** để lấy ra danh sách các host đang hoạt động.

```
root@kali:~# grep Up ping-sweep.txt | cut -d " " -f 2
192.168.111.1
192.168.111.2
192.168.111.150
192.168.111.254
192.168.111.131
root@kali:~#
```

Hình 39 Sử dụng lệnh grep để tìm kiếm các host đang hoạt động

Chúng ta cũng có thể quét các cổng TCP hoặc UDP cụ thể trên toàn mạng, thăm dò các dịch vụ và port phổ biến. trong nỗ lực xác định vị trí các hệ thống có thể hữu ích hoặc có các lỗ hổng đã biết. Thực hiện scan này có xu hướng chính xác hơn ping sweep.

```
root@kali:~# nmap -p 80 192.168.111.1-254 -oG web-sweep.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-27 13:29 EDT
Nmap scan report for 192.168.111.1
Host is up (0.0014s latency).

PORT      STATE SERVICE
80/tcp    closed http
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.111.2
Host is up (0.00018s latency).

PORT      STATE SERVICE
80/tcp    closed http
MAC Address: 00:50:56:E5:A6:14 (VMware)

Nmap scan report for 192.168.111.150
Host is up (0.00022s latency).

PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 00:0C:29:FA:DD:2A (VMware)

Nmap scan report for 192.168.111.254
Host is up (0.00038s latency).

PORT      STATE SERVICE
80/tcp    filtered http
MAC Address: 00:50:56:E4:1A:EA (VMware)
```

Hình 40 Chỉ quét port 80 trên toàn mạng

Sau đó, sử dụng lệnh grep để lấy ra danh sách các host đang hoạt động và đang mở port 80.

```
root@kali:~# grep open web-sweep.txt | cut -d " " -f 2
192.168.111.150
192.168.111.131
root@kali:~#
```

Hình 41 Chỉ hiển thị các host đang mở port 80 trong toàn mạng

Task 12:

- Thực hiện kiểm tra các host đang hoạt động trong mạng bằng các ngôn ngữ lập trình khác (Bash script, Python, C/C++, Perl, ...).
- Sử dụng Wireshark để phân tích gói tin khi sử dụng Nmap với tùy chọn **-sn**

OS Fingerprinting

Nmap được tích hợp sẵn một tính năng gọi là OS Fingerprinting (tham số **-O**). Tính năng này cố gắng đoán hệ điều hành cơ bản, bằng cách kiểm tra các gói nhận được từ mục tiêu. Các hệ điều hành khác nhau thường có TCP/IP stack hơi khác nhau, chẳng hạn như giá trị TTL mặc định và TCP window size. Những khác biệt nhỏ này tạo ra một dấu vân tay thường có thể được nhận dạng bởi Nmap. Nmap sẽ kiểm tra lưu lượng mạng gửi và nhận từ máy mục tiêu, đồng thời cố gắng nhận dạng hệ điều hành với một danh sách đã biết.

```

root@kali:~/Desktop# sudo nmap -O 192.168.111.150
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-27 13:46 EDT
Nmap scan report for 192.168.111.150
Host is up (0.0011s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:FA:DD:2A (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.70 seconds
root@kali:~/Desktop# 

```

Hình 42 Sử dụng Nmap để xác định hệ điều hành của máy mục tiêu

Banner Grabbing/Service Enumeration

Chúng ta có thể xác định các dịch vụ đang chạy trên các port được chỉ định bằng cách kiểm tra các banner của dịch vụ (-sV) và chạy các script khám phá hệ điều hành và dịch vụ (-A). Tuy nhiên, lưu ý rằng banner có thể được chỉnh sửa bởi quản trị viên. Do đó, chúng có thể được cố ý đặt tên thành dịch vụ giả mạo để đánh lừa kẻ tấn công.

```

root@kali:~# nmap -sV -sT -A 192.168.111.150
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-28 10:30 EDT
Nmap scan report for 192.168.111.150
Host is up (0.12s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to 192.168.111.131
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   vsFTPD 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)

```

Hình 43 Sử dụng nmap để khám phá các dịch vụ, thu thập thông tin banner

Nmap Scripting Engine (NSE)

Chúng ta có thể sử dụng Nmap Scripting Engine (NSE) để khởi chạy các đoạn script do người dùng tạo ra nhằm tự động hóa các tác vụ quét khác nhau. Các script này thực hiện một loạt chức năng bao gồm DNS enumeration, các loại tấn công brute force, và thậm chí là xác định lỗ hổng bảo mật. Các tập lệnh NSE nằm trong thư mục `/usr/share/nmap/scripts`.

Ví dụ, sử dụng `smb-os-discovery` để thử kết nối tới dịch vụ SMB trên máy mục tiêu nhằm xác định hệ điều hành của nó.

```

root@kali:~# nmap 192.168.111.150 --script=smb-os-discovery
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-28 10:42 EDT
Nmap scan report for 192.168.111.150
Host is up (0.0025s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:FA:DD:2A (VMware)

Host script results:
| smb-os-discovery:
| OS: Unix (Samba 3.0.20-Debian)
| Computer name: metasploitable
| NetBIOS computer name:
| Domain name: localdomain
| FQDN: metasploitable.localdomain
|_ System time: 2020-09-28T10:42:26-04:00

Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
root@kali:~#

```

Hình 44 Sử dụng nmap NSE để xác định hệ điều hành

Task 13:

- Liệt kê các banner, dịch vụ đang chạy trên máy Metasploitable 2 (chỉ liệt kê các dịch vụ TCP).
- Sử dụng thêm 2 NSE script (tự chọn) để quét máy mục tiêu (Metasploitable 2)

3. Quét lỗ hổng sử dụng công cụ Nessus

Nessus là một công cụ quét lỗ hổng phổ biến, hỗ trợ hơn 130000 plugin. Ban đầu, Nessus được phát triển như một ứng dụng mã nguồn mở, tuy nhiên, năm 2005, mã nguồn đã được đóng. Sự thay đổi đối với mô hình nguồn đóng dẫn đến các nhánh của dự án mã nguồn mở được phát triển, và một trong số đó là OpenVAS.

a. Cài đặt và cấu hình Nessus

Trước khi cài đặt, đảm bảo máy Kali Linux luôn ở phiên bản mới nhất:

```
root@kali:~# sudo apt update && sudo apt upgrade
Get:1 http://kali.cs.nctu.edu.tw/kali kali-rolling InRelease [30.5 kB]
Get:2 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 Packages [16.6 MB]
Get:3 http://kali.cs.nctu.edu.tw/kali kali-rolling/contrib amd64 Packages [99.7 kB]
Fetched 16.7 MB in 26s (638 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
144 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
  libmozjs-68-0 libsnmp35
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  libhandy-1-0 libmozjs-78-0 libnetsnmptrapd40 libsnmp40 libyara4
The following packages have been kept back:
  python-cffi-backend
The following packages will be upgraded:
  apache-users cpp debianutils dvisvgm exim4-base exim4-config
  exim4-daemon-light exploitdb fierce fonts-cantarell fonts-noto-color-emoji
```

Hình 45 Update và Upgrade Linux

Mặc dù Nessus không có trong repository của Kali, chúng ta có thể tải về tập tin 64-bit .deb tại trang chủ của Tenable: <https://www.tenable.com/downloads/nessus>

Sau khi đảm bảo tính toàn vẹn được bảo toàn trong quá trình tải tập tin về máy, thực hiện cài đặt bằng lệnh apt:

```
root@kali:~# sudo apt install ./Nessus-8.12.0-debian6_amd64.deb
Reading package lists... Done
Building dependency tree
Reading state information... Done
Note, selecting 'nessus' instead of './Nessus-8.12.0-debian6_amd64.deb'
The following packages were automatically installed and are no longer required:
  libmozjs-68-0 libsnmp35
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  nessus
0 upgraded, 1 newly installed, 0 to remove and 1 not upgraded.
Need to get 0 B/42.3 MB of archives.
After this operation, 0 B of additional disk space will be used.
Get:1 /root/Nessus-8.12.0-debian6_amd64.deb nessus amd64 8.12.0 [42.3 MB]
Selecting previously unselected package nessus.
(Reading database ... 424411 files and directories currently installed.)
Preparing to unpack .../Nessus-8.12.0-debian6_amd64.deb ...
Unpacking nessus (8.12.0) ...
Setting up nessus (8.12.0) ...
Unpacking Nessus Scanner Core Components...

- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
- Then go to https://kali:8834/ to configure your scanner
```

Hình 46 Cài đặt Nessus

Sau khi cài đặt thành công, thực hiện khởi động dịch vụ *nessusd*

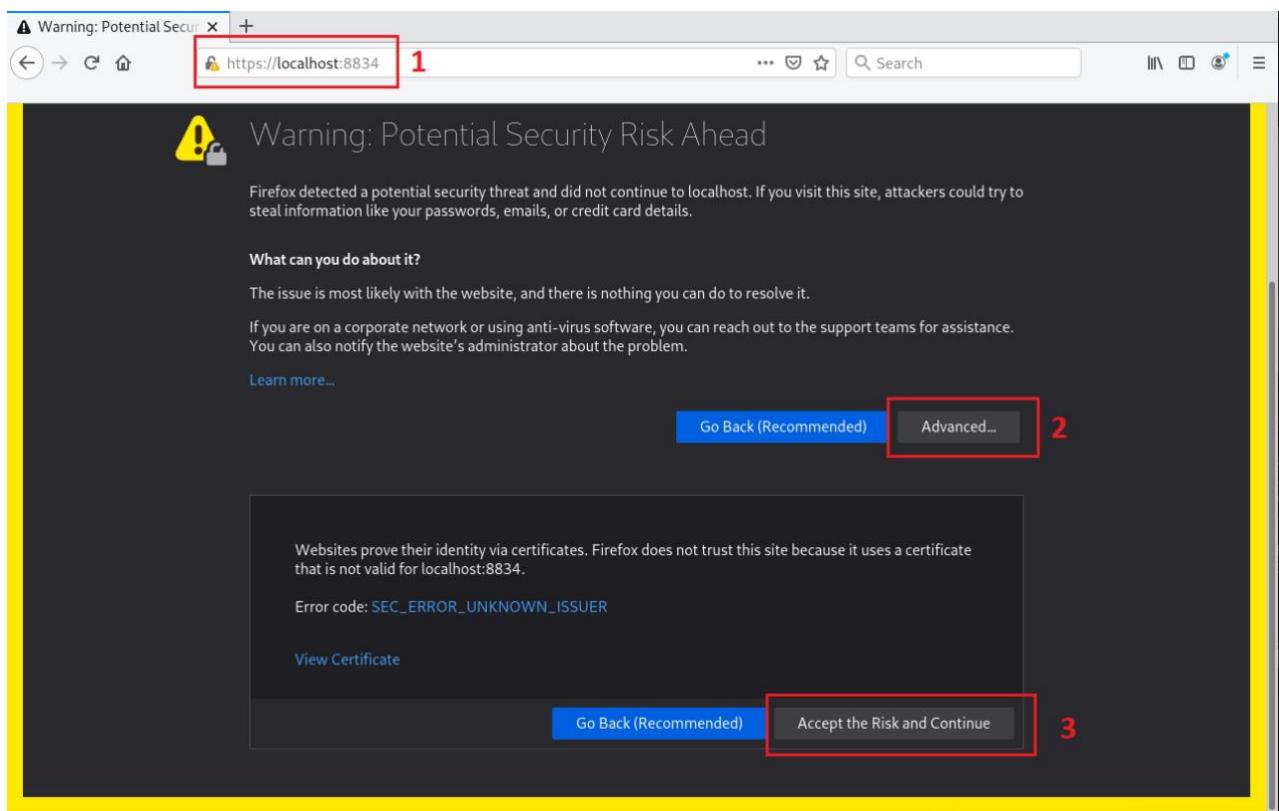
```
root@kali:~# /bin/systemctl start nessusd.service
root@kali:~# systemctl status nessusd
● nessusd.service - The Nessus Vulnerability Scanner
  Loaded: loaded (/lib/systemd/system/nessusd.service; disabled; vendor preset: >
  Active: active (running) since Sun 2020-10-11 08:25:20 EDT; 18s ago
    Main PID: 18102 (nessus-service)
      Tasks: 12 (limit: 4602)
     Memory: 133.7M
       CGroup: /system.slice/nessusd.service
               └─18102 /opt/nessus/sbin/nessus-service -q
                 ├─18103 nessusd -q

Oct 11 08:25:20 kali systemd[1]: Started The Nessus Vulnerability Scanner.
lines 1-11/11 (END)
```

Hình 47 Khởi động Nessus

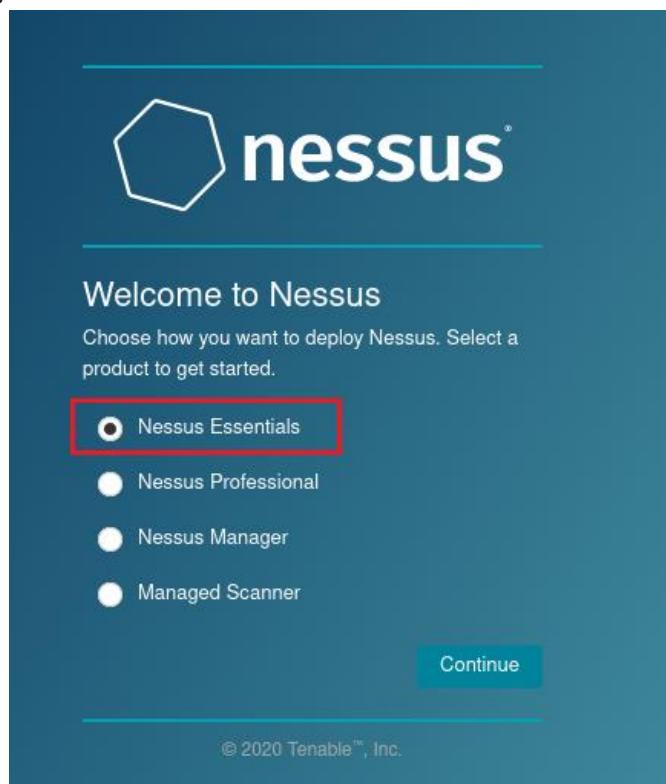
Sau khi khởi động Nessus, mở trình duyệt và truy cập vào đường dẫn <https://localhost:8834/>.

Chúng ta sẽ được thông báo lỗi certificate, chọn *Advanced... -> Accept the Risk and Continue*



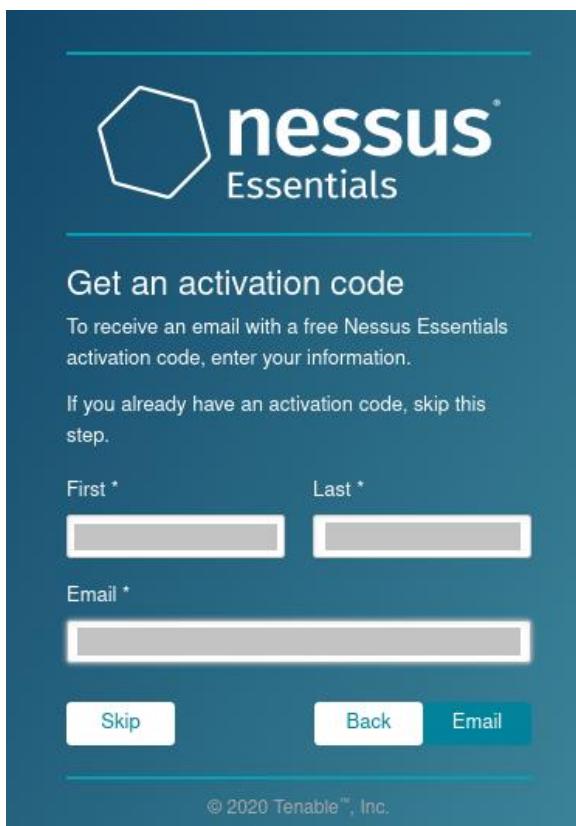
Hình 48 Bỏ qua các cảnh báo

Sau khi trang được tải lên, chúng ta được thông báo chọn phiên bản Nessus muốn sử dụng. Trong trường hợp này, chọn *Nessus Essentials*, sau đó chọn *Continue*



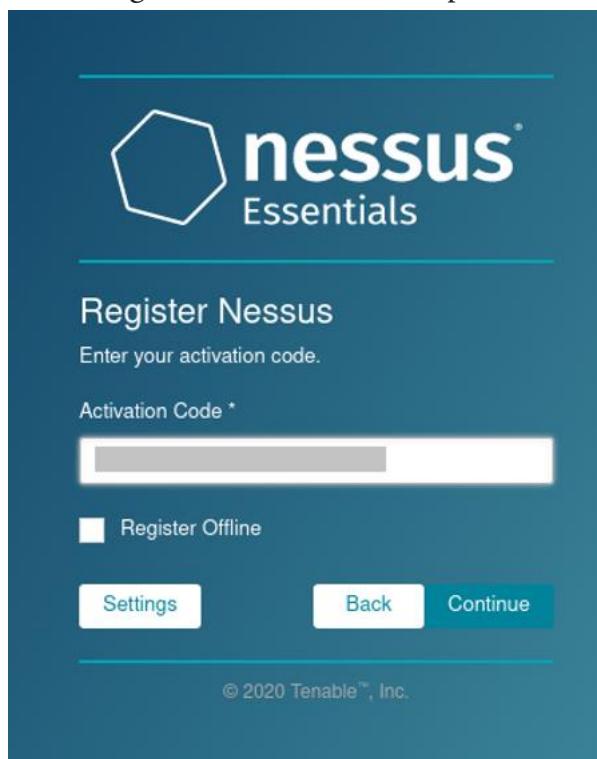
Hình 49 Chọn Nessus Essential

Tiếp theo, nhập các thông tin theo yêu cầu. Lưu ý, nhập đúng địa chỉ email để Nessus có thể gửi Activation code về hộp thư điện tử, sau đó nhấn *Email*



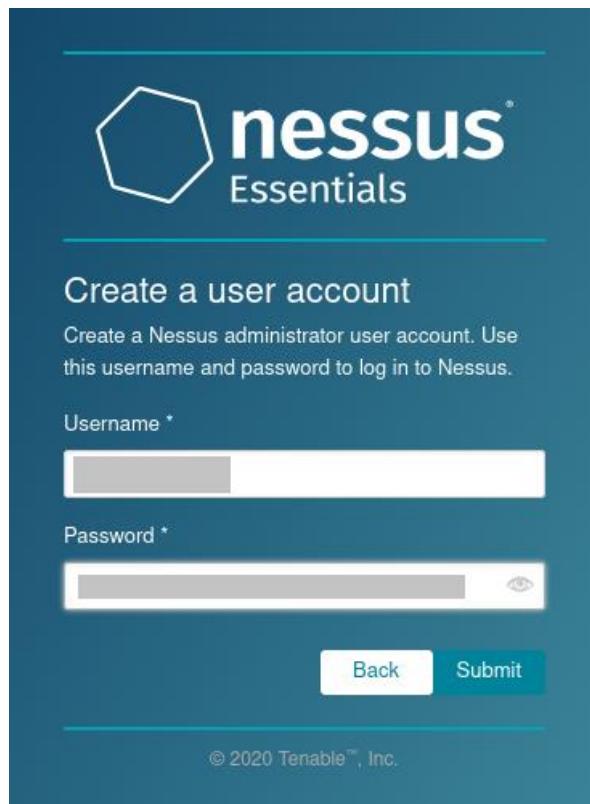
Hình 50 Đăng ký tài khoản

Sau khi nhận activation code trong hộp thư điện tử, nhập vào và nhấn *Continue*



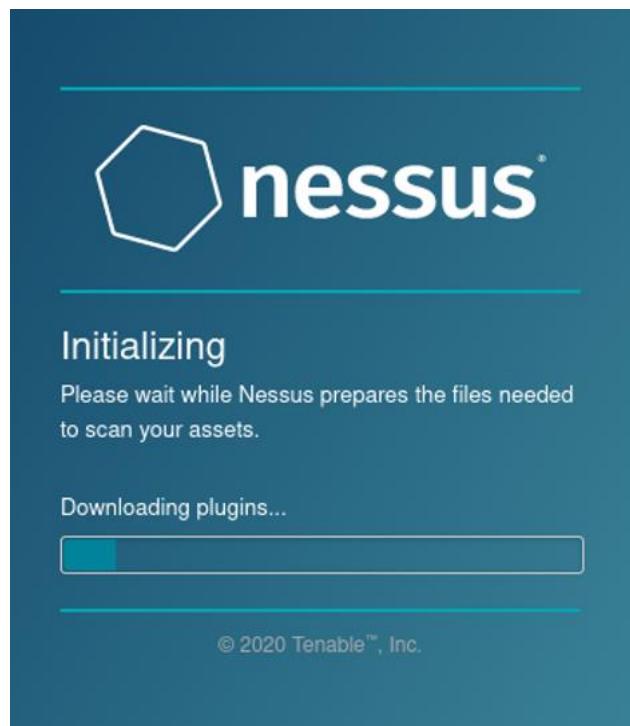
Hình 51 Nhập activation code

Bây giờ, Nessus đã được kích hoạt, công việc tiếp theo sẽ là tạo tài khoản quản trị Nessus. Nhập tên username, password và sau đó nhấn *Submit*



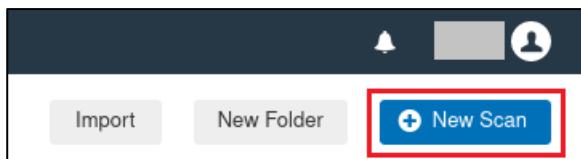
Hình 52 Tạo tài khoản quản trị

Cuối cùng, chờ quá trình cập nhật và cài đặt các plugin hoàn tất. Quá trình này sẽ mất khá nhiều thời gian.



Hình 53 Quá trình khởi tạo và cập nhật Nessus

Sau khi Nessus được cài đặt thành công, thực hiện scan lần đầu tiên. Để bắt đầu, chúng ta bấm nút *New Scan*



Hình 54 Tạo một scan mới

Nessus hỗ trợ nhiều loại quét lỗ hổng khác nhau. Tuy nhiên, trong nội dung bài thực hành này, chúng ta sẽ tập trung vào **Basic Network Scan**

Scan Templates

[Back to Scans](#)

Scanner

DISCOVERY

- Host Discovery**: A simple scan to discover live hosts and open ports.

VULNERABILITIES

- Basic Network Scan** (highlighted with a red box): A full system scan suitable for any host.
- Advanced Scan**: Configure a scan without using any recommendations.
- Advanced Dynamic Scan**: Configure a dynamic plugin scan without recommendations.
- Malware Scan**: Scan for malware on Windows and Unix systems.
- Mobile Device Scan**: Assess mobile devices via Microsoft Exchange or an MDM. (UPGRADE)
- DROWN Detection**: Remote checks for CVE-2016-0800.
- Intel AMT Security Bypass**: Remote and local checks for CVE-2017-5689.
- Shadow Brokers Scan**: Scan for vulnerabilities disclosed in the Shadow Brokers leaks.
- Spectre and Meltdown**: Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754.
- WannaCry Ransomware**: Remote and local checks for MS17-010.

COMPLIANCE

- Audit Cloud Infrastructure**: Audit the configuration of third-party cloud services. (UPGRADE)
- Internal PCI Network Scan**: Perform an internal PCI DSS (11.2.1) vulnerability scan. (UPGRADE)
- MDM Config Audit**: Audit the configuration of mobile device managers. (UPGRADE)
- Offline Config Audit**: Audit the configuration of network devices. (UPGRADE)
- PCI Quarterly External Scan**: Approved for quarterly external scanning as required by PCI. (UPGRADE)

Hình 55 Chọn Basic Network Scan

Nessus sẽ hiển thị màn hình cài đặt cấu hình scan với 2 tham số được yêu cầu khai báo: tên và danh sách các mục tiêu cần scan. Nessus hỗ trợ khai báo mục tiêu sử dụng địa chỉ IP, dãy địa chỉ IP; danh sách FQDN hoặc IP được cách nhau bằng dấu “,”.

Ví dụ, trong bài thực hành này, chúng ta sẽ thực hiện quét máy Metasploitable2, có địa chỉ IP là 192.168.111.150. Chúng ta sẽ nhập “Metasploitable2 – Basic” trong trường *Name* và địa chỉ IP trong trường *Targets*:

New Scan / Basic Network Scan

[Back to Scan Templates](#)

Settings Credentials Plugins

BASIC

- General
- Schedule
- Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name: Metasploitable2 – Basic

Description:

Folder: My Scans

Targets: 192.168.111.150

Upload Targets Add File

Hình 56 Nhập địa chỉ IP cần scan vào mục targets

Trong mục tiêu bài thực hành này, chúng ta đã chọn template Basic Network Scan, các thuộc tính sẽ được thiết lập mặc định. Tuy nhiên, trong thực tế, chúng ta cần xem xét đến các yếu tố khác như môi trường quét, thời gian, mục tiêu sẽ được quét, ... Một số điều cần xem xét khi sử dụng template Basic Network Scan bao gồm:

- Mục tiêu quét nằm trong mạng nội bộ hay có thể truy cập từ bên ngoài Internet?
- Chúng ta có được phép tấn công brute force thông tin đăng nhập không?
- Scan tất cả TCP và UDP port hay chỉ một số port thông dụng?
- Các kiểm tra nào mà scanner có thể chạy, và kiểm tra nào không thể chạy?
- Scanner chạy quét có thông tin đăng nhập hay không có thông tin đăng nhập?

Mặc định, template Basic Network Scan chỉ thực hiện quét các port thông dụng. Tuy nhiên, bây giờ chúng ta cần thực hiện quét *tất cả* các port. Để thay đổi, click vào *Discovery* phía bên trái của thẻ *Settings*

New Scan / Basic Network Scan

[Back to Scan Templates](#)

Settings **Credentials** **Plugins**

BASIC

- General
- Schedule
- Notifications
- DISCOVERY**
- ASSESSMENT
- REPORT
- ADVANCED

Name: Metasploitable2 – Basic

Description:

Folder: My Scans

Targets: 192.168.111.150

Upload Targets [Add File](#)

Hình 57 Truy cập thiết lập Discovery

Trong mục Scan Type, thay đổi giá trị từ Port scan (common ports) thành Custom

Settings **Credentials** **Plugins**

BASIC

- DISCOVERY**
- ASSESSMENT
- REPORT
- ADVANCED

Scan Type

Port scan (common ports)

Port scan (common ports)

Port scan (all ports)

Custom

Use fast network discovery

Port Scanner Settings:

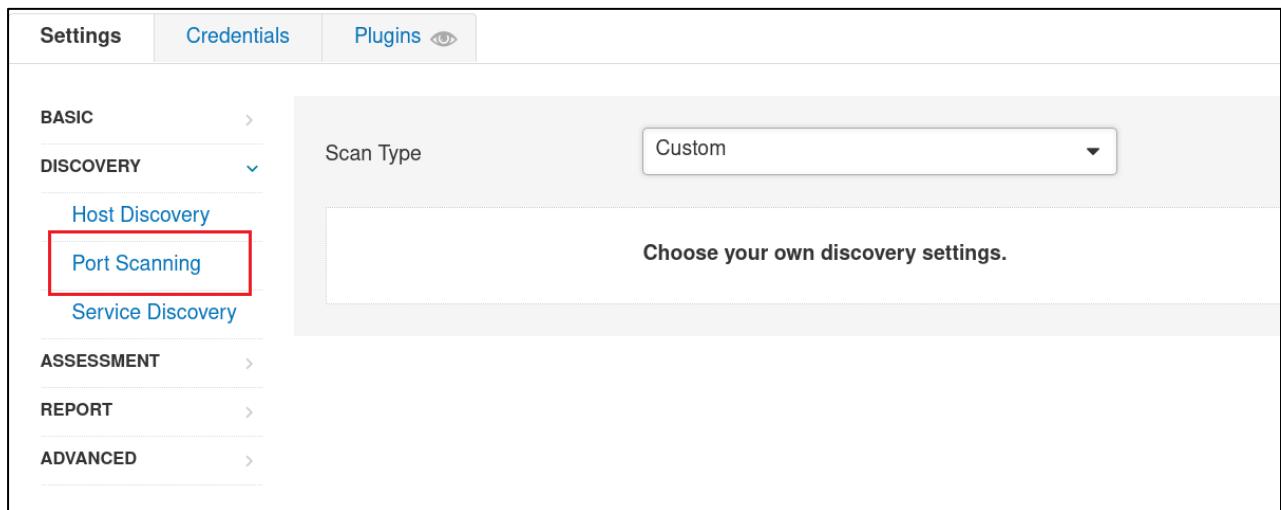
- Scan common ports
- Use netstat if credentials are provided
- Use SYN scanner if necessary

Ping hosts using:

- TCP
- ARP
- ICMP (2 retries)

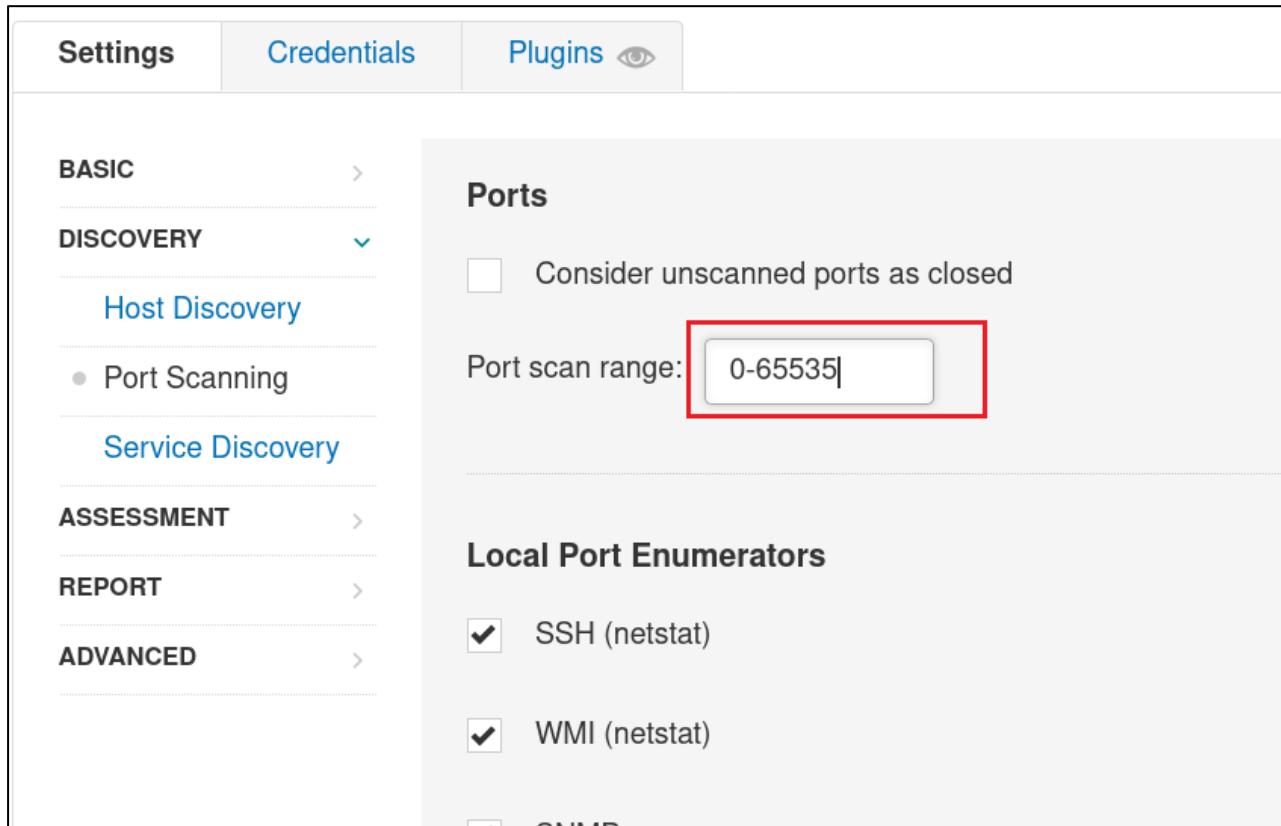
Hình 58 Cấu hình Scanner sử dụng loại Custom Port

Bên trái, chọn Port Scanning ở trong mục con của Discovery để cấu hình dãy port muốn scan.



Hình 59 Chọn tùy chọn Port Scanning

Trong mục *Port Scanning*, chúng ta sẽ thiết lập dãy port muốn scan ở trong phần *Port scan range*. Nhập giá trị “0-65535” để thực hiện quét tất cả các port.



Hình 60 Cấu hình Scanner để quét tất cả các port

Trong kịch bản này, chúng ta đã chọn định nghĩa scan chỉ quét các port TCP, không quét UDP. Điều này sẽ tăng tốc độ quét, nhưng sẽ bỏ qua các dịch vụ UDP quan trọng trên máy mục tiêu. Trong quá trình quét, chúng ta phải cân nhắc tính ổn định của mạng mục tiêu, phạm vi mục tiêu, thời lượng tương tác và nhiều yếu tố khác khi định cấu hình tùy chọn quét cổng.

Ngoài ra, chúng ta đã không cấu hình bất kỳ thông tin đăng nhập nào, điều đó đồng nghĩa với việc quét mà không cần tài khoản đăng nhập. Thêm vào đó, chúng ta chấp nhận mặc định trong Basic Network Scan, có nghĩa là brute force tài khoản đăng nhập sẽ không được kích hoạt.

Bây giờ, chúng ta đã xem xét hoàn tất tất cả các tùy chọn cấu hình và hiểu (ít nhất là ở cấp độ cao) scanner sẽ làm gì, chúng ta có thể tiến hành chạy quét lần đầu tiên.

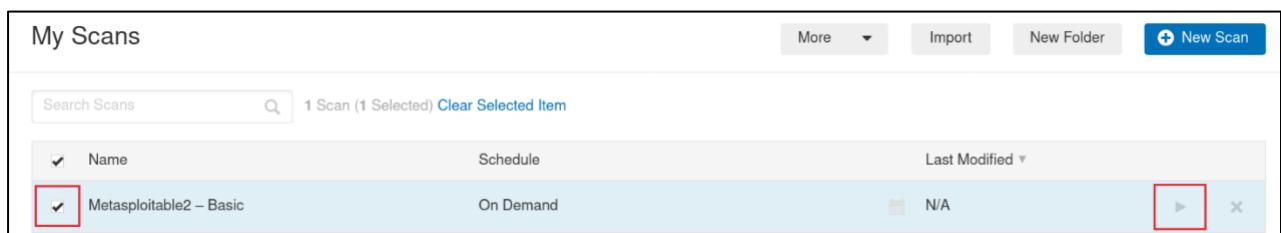
b. Quét lỗ hổng không sử dụng tài khoản chứng thực

Sau khi thiết lập mọi tham số, kéo xuống dưới và chọn Save



Hình 61 Chọn save để lưu lại các cài đặt

Sau khi save, quay về mục *My Scans*, chọn vào template “Metasploitable2 – Basic”, sau đó chọn *Launch*



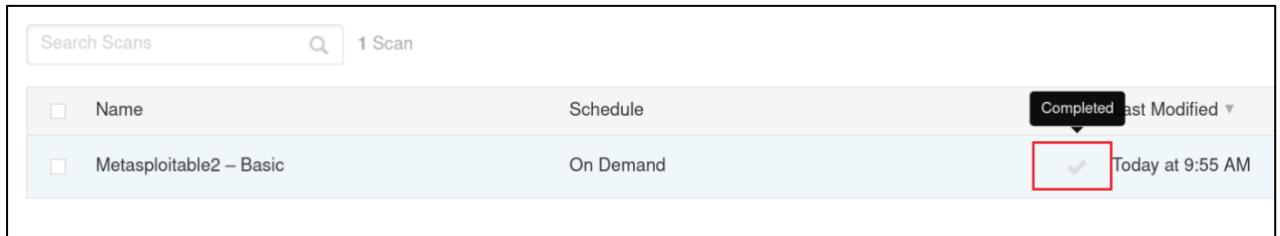
Hình 62 Tiến hành chạy quét lần đầu tiên

Trạng thái hiện tại được cập nhật thành *Running*



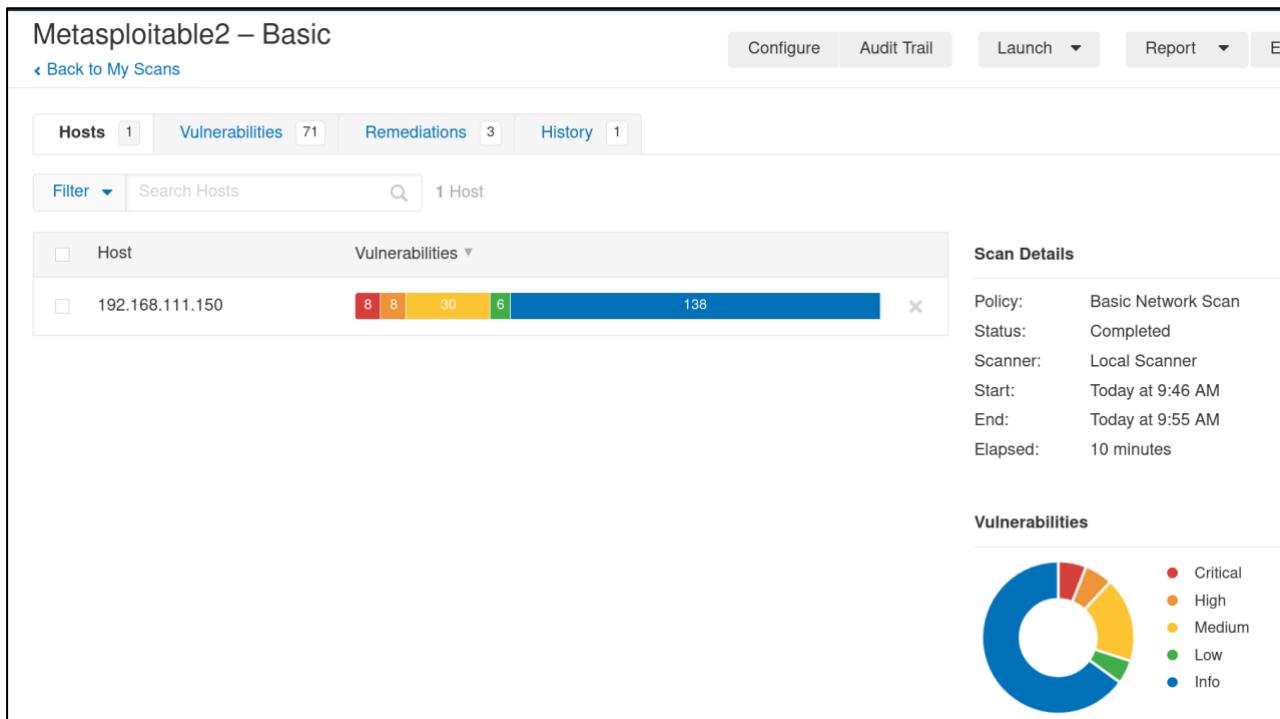
Hình 63 Chờ quá trình scan hoàn tất

Sau khi quét hoàn tất, trạng thái sẽ chuyển sang *Completed*



Hình 64 Quá trình scan hoàn tất

Sau khi scan hoàn tất, click vào tên scan, “Metasploitable2 – Basic” để hiển thị danh sách các host được khám phá trong quá trình scan và tóm tắt các lỗ hổng tồn tại.



Hình 65 Giao diện tổng quan

Cho dù chúng ta quét một hay nhiều máy chủ, chúng ta có thể nhấp vào địa chỉ IP hoặc tên máy chủ để hiển thị các lỗ hổng được phát hiện đối với mục tiêu đó, như thể hiện trong Hình 65

Metasploitable2 – Basic / 192.168.111.150

Configure Audit Trail Launch Report Export

Vulnerabilities 71

Filter Search Vulnerabilities 71 Vulnerabilities

Sev	Name	Family	Count	
CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3	
CRITICAL	Bind Shell Backdoor Det...	Backdoors	1	
CRITICAL	NFS Exported Share Inf...	RPC	1	
CRITICAL	rexecd Service Detection	Service detection	1	
CRITICAL	Unix Operating System ...	General	1	
CRITICAL	VNC Server 'password' ...	Gain a shell remotely	1	
MIXED	DNS (Multiple Issues)	DNS	6	
MIXED	ISC Bind (Multiple I...	DNS	5	

Host Details

- IP: 192.168.111.150
- MAC: 00:0C:29:FA:DD:2A
- OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- Start: Today at 9:46 AM
- End: Today at 9:55 AM
- Elapsed: 10 minutes
- KB: Download

Vulnerabilities

Severity	Count
Critical	10
High	10
Medium	10
Low	10
Info	40

Hình 66 Xem các lỗ hổng đã được phát hiện

Chúng ta có thể thực hiện lọc các lỗ hổng theo mức độ ảnh hưởng, CVE, khả năng khai thác, và nhiều hơn thế nữa. Để hiển thị các lỗ hổng có thể dẫn đến kiểm soát máy chủ mục tiêu, chúng ta có thể click *Filter* và thay đổi giá trị lọc thành “Exploit Available”, giữ nguyên các giá trị mặc định của “is equal to” và “true”. Sau khi cấu hình xong, click vào *Apply*

Filter Search Vulnerabilities 71 Vulnerabilities

Filters

Match All of the following:

Exploit Available is equal to true

Apply Cancel Clear Filters

Hình 67 Lọc các lỗ hổng với các lỗi khai thác

Kết quả lọc sẽ chỉ hiển thị các lỗ hổng theo nhóm được định nghĩa bởi Nessus

Sev	Name	Family	Count	
CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3	
CRITICAL	NFS Exported Share Informatio...	RPC	1	
HIGH	Apache Tomcat AJP Connector ...	Web Servers	1	
HIGH	ISC BIND Denial of Service	DNS	1	
HIGH	Multiple Vendor DNS Query ID ...	DNS	1	
HIGH	rlogin Service Detection	Service detection	1	
HIGH	rsh Service Detection	Service detection	1	
MEDIUM	SMTP Service STARTTLS Plain...	SMTP problems	1	

Hình 68 Danh sách lỗ hổng được phân loại theo nhóm

Trong khi việc gom nhóm có thể hữu ích, chúng ta sẽ click vào biểu tượng hình bánh răng bên góc phải của bảng và chọn *Disable Groups*.

Sev	Name	Family	Count	
CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3	
CRITICAL	NFS Exported Share Informatio...	RPC	1	

Hình 69 Vô hiệu hóa tính năng gom nhóm

Kết quả sẽ hiển thị danh sách tất cả lỗ hổng trên 1 trang, được sắp xếp theo mức độ ảnh hưởng.

Vulnerabilities 9			
1 Filter ▾	Search Vulnerabilities	9 Vulnerabilities	
Sev ▾	Name ▾	Family ▾	Count ▾
<input type="checkbox"/>	CRITICAL Debian OpenSSH/OpenSSL Pa...	Gain a shell remotely	2
<input type="checkbox"/>	CRITICAL Debian OpenSSH/OpenSSL Pa...	Gain a shell remotely	1
<input type="checkbox"/>	CRITICAL NFS Exported Share Informatio...	RPC	1
<input type="checkbox"/>	HIGH Apache Tomcat AJP Connector ...	Web Servers	1
<input type="checkbox"/>	HIGH ISC BIND Denial of Service	DNS	1
<input type="checkbox"/>	HIGH Multiple Vendor DNS Query ID ...	DNS	1
<input type="checkbox"/>	HIGH rlogin Service Detection	Service detection	1
<input type="checkbox"/>	HIGH rsh Service Detection	Service detection	1
<input type="checkbox"/>	MEDIUM SMTP Service STARTTLS Plain...	SMTP problems	1

Hình 70 Hiển thị kết quả không sử dụng chế độ gom nhóm

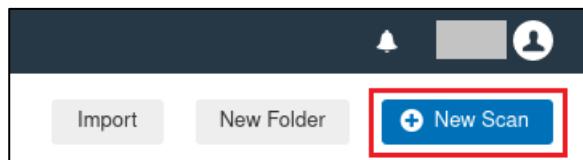
Task 14:

- Thực hiện lại các bước trên để quét máy Metasploitable 2 không sử dụng tài khoản chứng thực.
- Bật Wireshark sau đó tiến hành quét và xác định các bước mà Nessus đã thực hiện để hoàn tất quá trình quét.
- Quét lại nhưng quét thêm port UDP.

c. Quét lỗ hổng sử dụng tài khoản chứng thực

Chúng ta có thể có được nhiều thông tin chi tiết hơn và giảm thiểu các false positive bằng cách thực hiện scan sử dụng tài khoản chứng thực của máy mục tiêu. Tuy nhiên, lưu ý rằng với tư cách là những pentester, chúng ta sẽ không thực hiện scan có tài khoản chứng thực trong hầu hết các trường hợp nếu không có sự cho phép rõ ràng của quản trị viên của mạng mục tiêu do có nguy cơ làm gián đoạn (không chủ ý) tới hệ thống của mục tiêu.

Để bắt đầu, chúng ta sẽ chọn nút *New Scan*



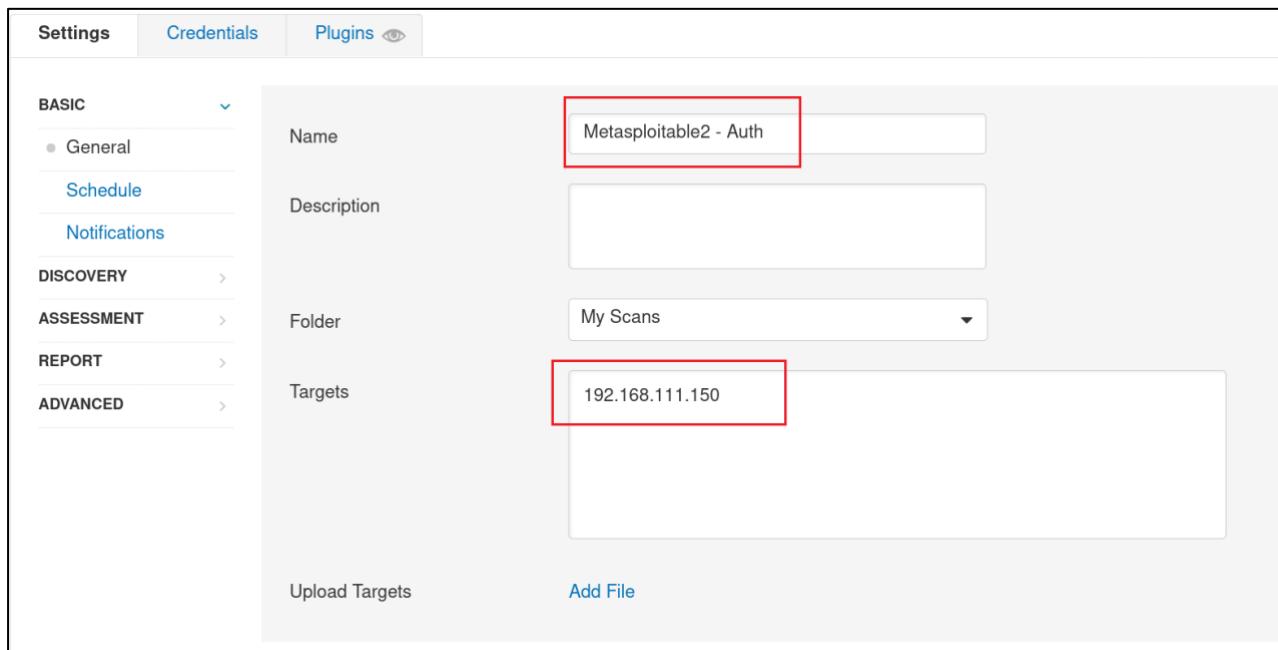
Hình 71 Khởi tạo 1 lần scan mới

Mặc dù tất cả template của Nessus đều chấp nhận thông tin đăng nhập của người dùng, chúng ta sẽ sử dụng template *Credentialed Patch Audit*, được cấu hình sẵn để thực hiện kiểm tra bảo mật cục bộ đối với máy mục tiêu. Template này không chỉ quét các bản vá lỗi còn thiếu ở mức độ hệ điều hành mà còn quét các ứng dụng lỗi thời có thể dễ bị tấn công như leo thang đặc quyền.

VULNERABILITIES			
Basic Network Scan A full system scan suitable for any host.	Advanced Scan Configure a scan without using any recommendations.	Advanced Dynamic Scan Configure a dynamic plugin scan without recommendations.	Malware Scan Scan for malware on Windows and Unix systems.
Mobile Device Scan Assess mobile devices via Microsoft Exchange or an MDM. <i>UPGRADE</i>	Web Application Tests Scan for published and unknown web vulnerabilities.	Credentialated Patch Audit Authenticate to hosts and enumerate missing updates. <i>(highlighted)</i>	Badlock Detection Remote and local checks for CVE-2016-2118 and CVE-2016-0128.
Bash Shellshock Detection Remote and local checks for CVE-2014-6271 and CVE-2014-7169.	DROWN Detection Remote checks for CVE-2016-0800.	Intel AMT Security Bypass Remote and local checks for CVE-2017-5689.	Shadow Brokers Scan Scan for vulnerabilities disclosed in the Shadow Brokers leaks.
Spectre and Meltdown Remote and local checks for CVE-2017-5752, CVE-2017-5755	WannaCry Ransomware Remote and local checks for CVE-2017-0120	Ripple20 Remote Scan A remote scan to fingerprint hosts	Zerologon Remote Scan A remote scan to detect Microsoft Network Logon (MS17-010) and NTLMv2 (MS17-012) vulnerabilities

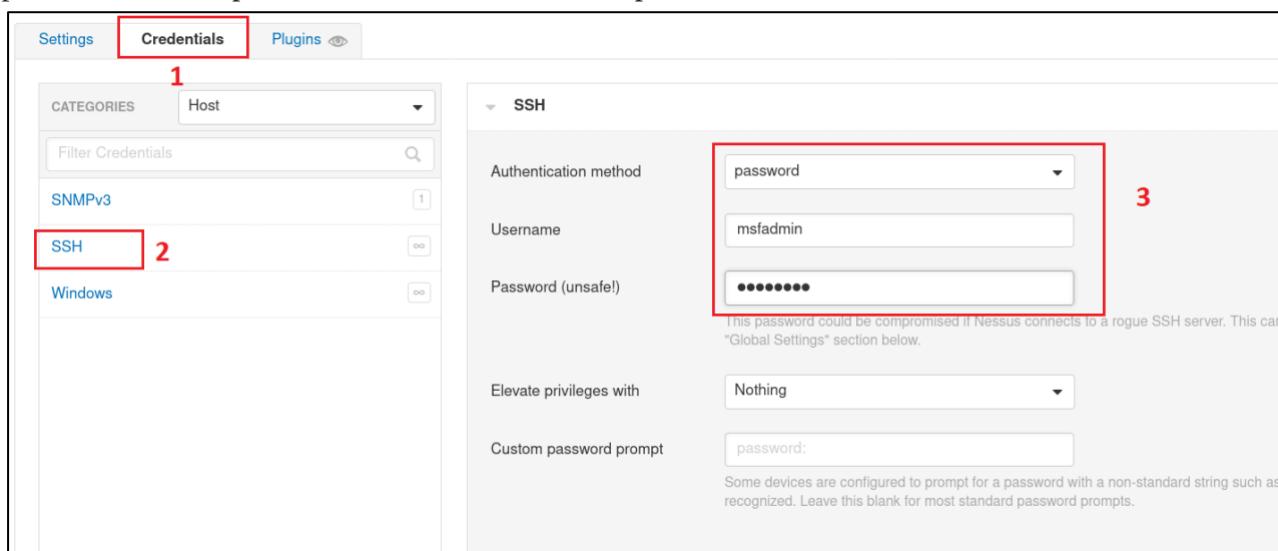
Hình 72 Chọn template “Credentialated Patch Audit”

Tương tự như Basic Network Scan, chúng ta cần cung cấp tên và mục tiêu cần quét.



Hình 73 Cấu hình cơ bản của Authenticated Scan

Tiếp theo, chọn thẻ *Credentials* và chọn loại *SSH*. Trong mục *Authentication method*, chọn *password*, thiết lập username là “msfadmin” và password là “msfadmin”.



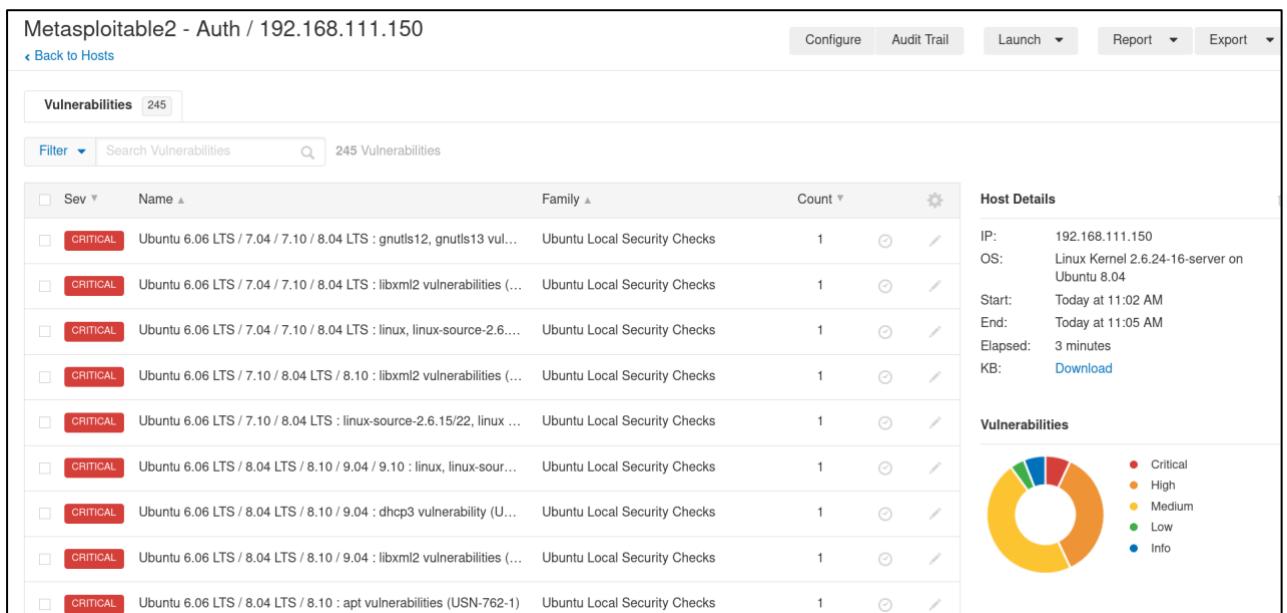
Hình 74 Nhập thông tin tài khoản SSH

Cuối cùng, thực hiện quét máy mục tiêu bằng cách chọn *Launch*



Hình 75 Thực hiện scan mục tiêu có sử dụng tài khoản chứng thực

Sau khi scan chuyển sang trạng thái “Completed”, chúng ta có thể click vào tên scan và mở danh sách các host và click vào địa chỉ IP của máy metasploitable 2, kết quả sẽ hiển thị danh sách các lỗ hổng được khám phá có thể được khai thác trên máy chủ.



Hình 76 Danh sách các lỗ hổng khi quét có tài khoản chứng thực

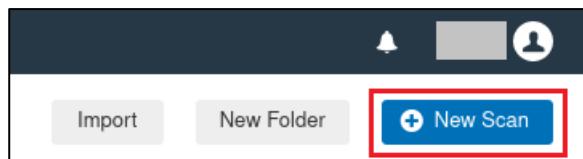
Task 15:

Thực hiện lại các bước trên để quét máy Metasploitable 2 có sử dụng tài khoản chứng thực. Kiểm tra kết quả quét và so sánh với việc quét không sử dụng tài khoản chứng thực. Hãy liệt kê các ưu, nhược điểm khi quét có tài khoản chứng thực và không có tài khoản chứng thực.

d. Quét với plugin được chỉ định

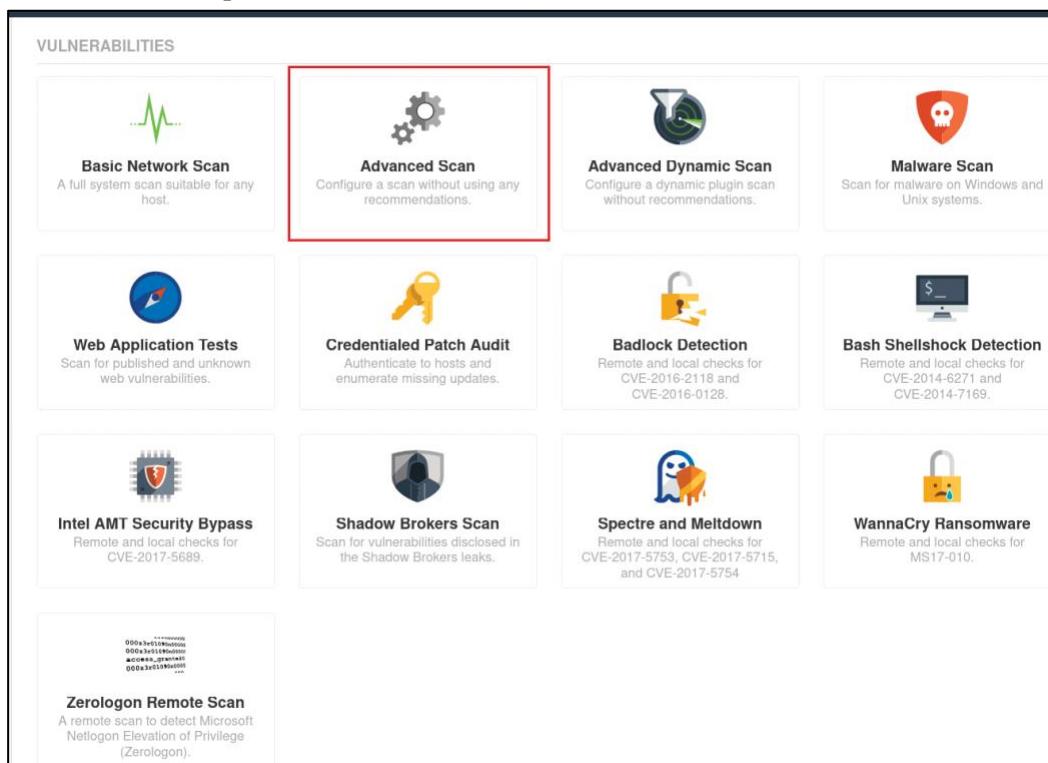
Mặc định, Nessus sẽ kích hoạt số lượng các plugin khi chạy các template mặc định. Mặc dù điều này có thể có ích trong nhiều trường hợp, nhưng chúng ta có thể tinh chỉnh các tùy chọn của mình, ví dụ, chạy một plugin nào đó nhanh chóng. Chúng ta có thể sử dụng tính năng này để kiểm chứng các phát hiện trước đó hoặc nhanh chóng phát hiện ra tất cả các mục tiêu dễ bị khai thác bởi một lỗ hổng trong cùng một môi trường.

Trong trường hợp này, chúng ta sẽ chạy plugin *NFS Exported Share Information Disclosure*. Để chạy scan cho một plugin, chúng ta lại bắt đầu bằng *New Scan*



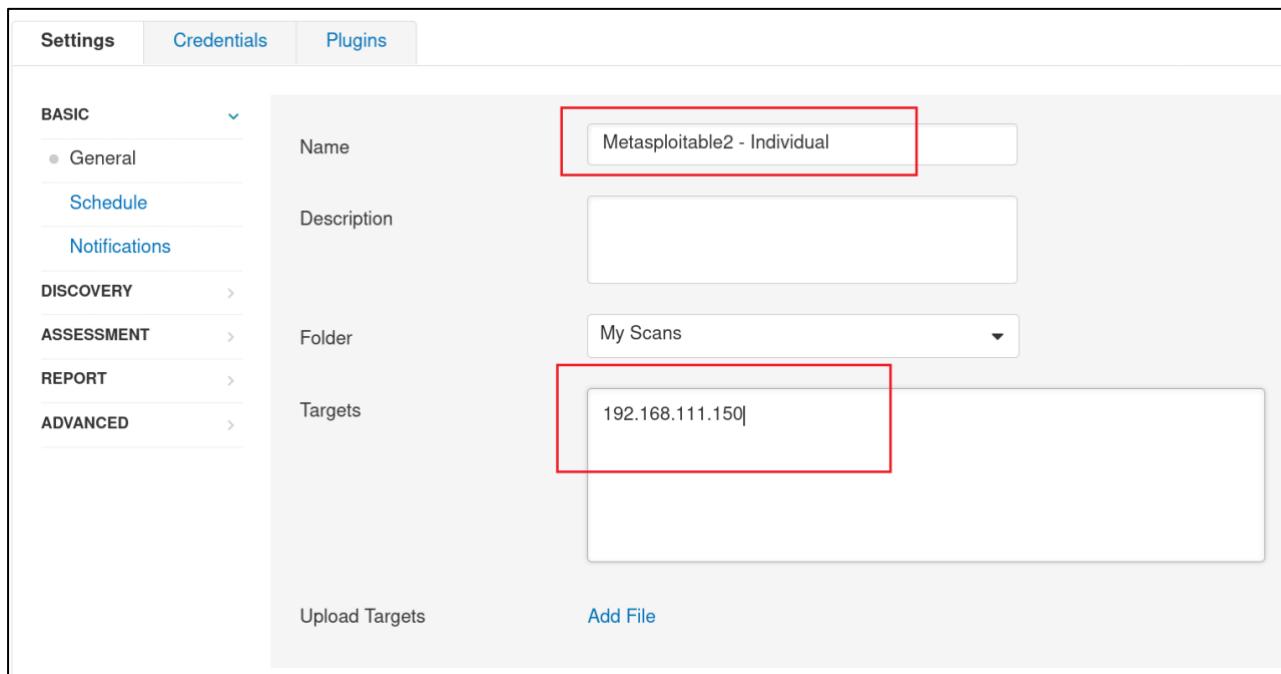
Hình 77 Khởi tạo scan mới

Lần này, chúng ta sẽ sử dụng template *Advanced Scan*. Không giống với các template Basic Network Scan và Credentialled Patch Audit đã được sử dụng trước đó, template Advanced Scan không sử dụng các đề xuất cho các cấu hình quét. Tuy nhiên, template này cung cấp một bộ các giá trị mặc định “Nâng cao” thường bị ẩn hoặc không khả dụng đối với các template khác. Lưu ý rằng Advanced Scan cho phép chúng ta chọn các plugin riêng lẻ, một tùy chọn không có sẵn cho hầu hết các template khác.



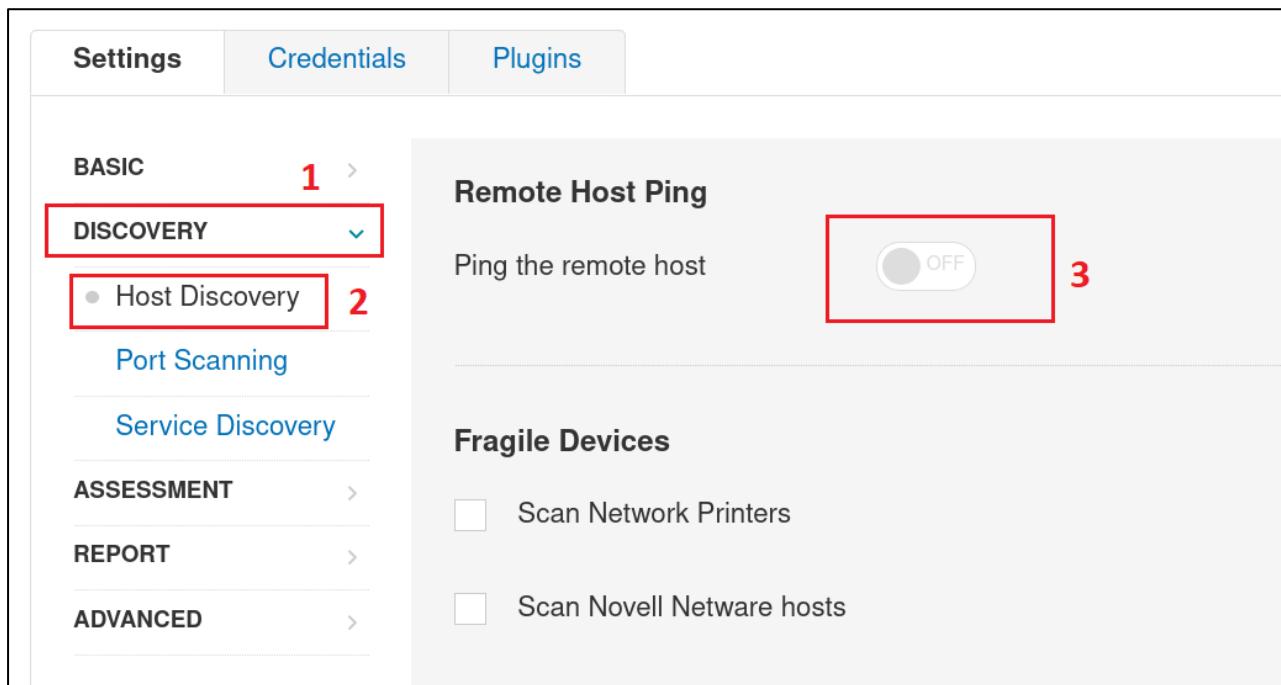
Hình 78 Chọn template “Advanced Scan”

Tương tự, cũng đặt tên và đổi tượng cần scan.



Hình 79 Thiết lập tên và đổi tương cần quét

Để tiết kiệm thời gian và ít để lại dấu vết, chúng ta sẽ tắt *Host discovery*, vì chúng ta biết được host vẫn còn hoạt động.



Hình 80 Tắt tính năng Host Discovery

Vì chúng ta chỉ scan dịch vụ RPC và biết rằng RPC chạy trên TCP port 111, nên chúng ta chỉ scan duy nhất port này.

The screenshot shows the ZAP Settings interface. On the left, there's a sidebar with categories: BASIC, DISCOVERY (selected), ASSESSMENT, REPORT, and ADVANCED. Under DISCOVERY, 'Host Discovery' is expanded, showing 'Port Scanning' (marked with a red box and number 1) and 'Service Discovery'. In the main panel, under 'Ports', there's a checkbox for 'Consider unscanned ports as closed' and a field for 'Port scan range' containing '111' (marked with a red box and number 2). Below this, under 'Local Port Enumerators', there are checkboxes for SSH (netstat), WMI (netstat), and SNMP. There are also two additional checkboxes: 'Only run network port scanners if local port enumeration failed' and 'Verify open TCP ports found by local port enumerators'. A vertical red box on the left side of the main panel is labeled with a red number 3.

Hình 81 Tắt hết các port không cần thiết

Sau khi giảm thiểu tối đa các tùy chọn scan, bây giờ tiến hành chọn plugin. Chọn thẻ *Plugins* và click vào *Disable All* ở góc phải

The screenshot shows the 'New Scan / Advanced Scan' interface. At the top, there's a back button and tabs for 'Settings' (selected), 'Credentials', and 'Plugins' (marked with a red box and number 1). To the right are buttons for 'Disable All' (marked with a red box and number 2) and 'Enable All'. Below these are links for 'Show Enabled' and 'Show All'. The main area displays a table of plugins, all of which are currently disabled (indicated by the 'DISABLED' status column). The columns are: STATUS, PLUGIN FAMILY, TOTAL, STATUS, PLUGIN NAME, and PLUGIN ID. The table lists various security checks and attacks, such as AIX Local Security Checks, Amazon Linux Local Security Checks, Backdoors, Brute force attacks, CentOS Local Security Checks, CGI abuses, CGI abuses : XSS, CISCO, Databases, and Debian Local Security Checks. The total count for disabled plugins is 11377.

Hình 82 Tắt hết tất cả các plugin

Để tiến hành quét NFS shares, chúng ta sẽ di chuyển đến “RPC” bên cột bên trái và thiết lập “NFS Exported Share Information Disclosure” ở cột bên phải thành *Enabled*

Category	Plugin Name	Status	Count
DISABLED	Policy Compliance	DISABLED	13
DISABLED	Red Hat Local Security Checks	DISABLED	6977
MIXED	RPC	ENABLED	38
DISABLED	SCADA	DISABLED	3
DISABLED	Scientific Linux Local Security Checks	DISABLED	3016
DISABLED	Service detection	DISABLED	496
DISABLED	Settings	DISABLED	103
DISABLED	Slackware Local Security Checks	DISABLED	1219
DISABLED	SMTP problems	DISABLED	148
DISABLED	SNMP	DISABLED	33
DISABLED	Solaris Local Security Checks	DISABLED	3726
	NFS Exported Share Information Disclosure	ENABLED	11356
	NFS portmapper localhost Mount Request Restricted...	DISABLED	11358
	NFS Predictable Filehandles Filesystem Access	DISABLED	11353
	NFS Server Superfluous	DISABLED	42255
	NFS Share Export List	DISABLED	10437
	NFS Share User Mountable	DISABLED	15984
	NFS Shares World Readable	DISABLED	42256
	NIS passwdbyname Map Disclosure	DISABLED	12238

Hình 83 Bật plugin NFS

Bây giờ ta đã cấu hình xong, tiến hành quét. Click vào *Launch*.



Hình 84 Tiến hành quét NFS

Sau khi trạng thái quét chuyển sang “Completed”, chúng ta có thể click vào tên scan, sau đó địa chỉ IP máy mục tiêu. Di chuyển đến lỗ hổng Critical duy nhất và click vào để hiển thị chi tiết thông tin lỗ hổng.

CRITICAL NFS Exported Share Information Disclosure

Description

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

Solution

Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

Output

```
The following NFS shares could be mounted :
+ /
+ Contents of / :
- .
- ..
- bin
- boot
- cdrom
- dev
.

more...
```

Port ▲	Hosts
2049 / udp / rpc-nfs	192.168.111.150

Hình 85 Xem kết quả scan với chỉ 1 plugin duy nhất

Task 16:

- Thực hiện lại các bước ở trên để quét máy Metasploitable 2 sử dụng plugin NFS Exported Share Information Disclosure.
- Chạy Wireshark hoặc tcpdump trong suốt quá trình scan sử dụng 1 plugin duy nhất. Liệt kê các port khác mà Nessus thực hiện scan, mà không phải port 111? Tại sao Nessus lại scan các port khác, trong khi chúng ta đã chỉ định chỉ scan duy nhất 1 port là 111?
- Mô tả cách làm để ngăn chặn việc Nessus scan port khác không phải là port được chỉ định
- Thực hiện quét lại sử dụng 2 plugin khác.

D. YÊU CẦU & ĐÁNH GIÁ

- Sinh viên tìm hiểu và thực hành theo hướng dẫn, thực hiện theo nhóm đã đăng ký.
- Nộp báo cáo kết quả gồm chi tiết những việc (Report) mà nhóm đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Báo cáo:
 - File .PDF. Tập trung vào nội dung, không mô tả lý thuyết.

- Đặt tên theo định dạng: [Mã lớp]-LabX_MSSV1_MSSV2.
- Ví dụ: [NT140.P12.ANTT.1]-Lab1_2252xxxx_2252yyyy.
- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Bài sao chép, trẽ, ... sẽ được xử lý tùy mức độ vi phạm.

HẾT

Chúc các bạn hoàn thành tốt!