

Nhóm 10:

Chu Đình Huấn - MSSV : N19DCVT013

Nguyễn Giê Nha – MSSV : N19DCVT040

Lớp : D19CQVT01-N

## Bài 1 . Netcarft

Tìm kiếm với trang <https://uis.ptithcm.edu.vn/>

Background			
Site title	Cổng Thông Tin Đào Tạo-Học Viện Công Nghệ Bưu Chính Viễn Thông-CƠ SỞ TẠI TP.HỒ CHÍ MINH-BCVTVMN	Date first seen	October 2013
Site rank	191373	Netcraft Risk Rating	1/10
Description	Not Present	Primary language	Vietnamese
Network			
Site	<a href="https://uis.ptithcm.edu.vn">https://uis.ptithcm.edu.vn</a>	Domain	<a href="https://uis.ptithcm.edu.vn">ptithcm.edu.vn</a>
Netblock Owner	CMC Telecom Infrastructure Company	Nameserver	ns1.vdc2.vn
Hosting company	CMC Corporation	Domain registrar	unknown
Hosting country	VN	Nameserver organisation	unknown
IPv4 address	115.165.166.67 (VirusTotal)	Organisation	unknown
IPv4 autonomous systems	AS45903	DNS admin	support@vdc2.vn

- Thứ hạng :191373
- Ngôn ngữ chính sử dụng : VietNam
- Công ty quản lý hosting : CMC
- Địa chỉ IP : 115.165.166.67
- Domain: ptithcm.edu.vn

Hosting History				
Netblock owner	IP address	OS	Web server	Last seen
▶ CMC Telecom Infrastruc...	115.165.166.67	Windows Server 2016	Microsoft-IIS/10.0	5-Jan-2022
▶ Vietnam Posts and Tele...	123.30.155.178	Windows Server 2012	Microsoft-IIS/8.5	14-Oct-2021
Sender Policy Framework				

- **Lịch sử hosting thay đổi : trước kia thì VietNam Post and Telecommunications HaNoi City quản lý với ip 123.30.255.178 chạy trên nền windows Server 2012 .Sau đó thì do CMC quản lý hosting của trang này với window Server 2016 và update gần nhất là 5-1-2022**

#### Server-Side

Includes all the main technologies that Netcraft detects as running on the server such as PHP.

Technology	Description	Popular sites using this technology
Atlas <a href="#">↗</a>	A set of ASP.NET extensions for implementing Ajax functionality	<a href="http://www.catalog.update.microsoft.com">www.catalog.update.microsoft.com</a> , <a href="http://www.who.int">www.who.int</a> , <a href="http://www.eccexam.com">www.eccexam.com</a>
Using ASP.NET <a href="#">↗</a>	ASP.NET is running on the server	<a href="http://www1.sedecatastro.gob.es">www1.sedecatastro.gob.es</a> , <a href="http://www.microsoft.com">www.microsoft.com</a> , <a href="http://www.cnblogs.com">www.cnblogs.com</a>
SSL <a href="#">↗</a>	A cryptographic protocol providing communication security over the Internet	<a href="http://l.facebook.com">l.facebook.com</a> , <a href="http://mail.google.com">mail.google.com</a> , <a href="http://accounts.google.com">accounts.google.com</a>

#### Client-Side

Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).

Technology	Description	Popular sites using this technology
Asynchronous Javascript	No description	<a href="http://www.linkedin.com">www.linkedin.com</a> , <a href="http://www.speedtest.net">www.speedtest.net</a> , <a href="http://www.startpage.com">www.startpage.com</a>
JavaScript <a href="#">↗</a>	Widely-supported programming language commonly used to power client-side dynamic content on websites	<a href="http://www.google.com">www.google.com</a> , <a href="http://www.instagram.com">www.instagram.com</a> , <a href="http://www.msn.com">www.msn.com</a>

#### Client-Side Scripting Frameworks

Frameworks or libraries allow for easier development of applications by providing an Application Program Interface (API) or a methodology to follow whilst developing.

Technology	Description	Popular sites using this technology
jQuery <a href="#">↗</a>	A JavaScript library used to simplify the client-side scripting of HTML	<a href="http://www.amazon.es">www.amazon.es</a> , <a href="http://www.xnxx.com">www.xnxx.com</a> , <a href="http://www.amazon.it">www.amazon.it</a>
Google Hosted Libraries <a href="#">↗</a>	Google API to retrieve JavaScript libraries	<a href="http://www.roblox.com">www.roblox.com</a> , <a href="http://www.researchgate.net">www.researchgate.net</a> , <a href="http://www.orange.fr">www.orange.fr</a>

#### Doctype

- **Phía server của trang thì được viết bằng ASP.NET còn phía client-side thì được viết bằng JavaScript**

## Bài 2. Quét Nmap và bắt gói tin wireshark

Sơ đồ lab gồm có 2 máy :

1. Máy windows 10 thật có ip : 192.168.217.1
2. Window 10 ảo trên Vmware có ip : 192.168.217.136

### 1. Half-open Scan:

*TCP SYN scan (Half-open scan) : giống như Full-open scan, nhưng sẽ gọi là nửa mở vì thay vì ở bước 3, attacker gửi gói tin ACK, thì attacker gửi ngay gói tin RST để kết thúc ngay kết nối. Còn nếu ở bước 2, mục tiêu gửi gói tin RST thì cũng có nghĩa là cổng đóng.*

Phương pháp này có thể qua mặt được tường lửa hay các cơ chế ghi lại lịch sử (điều này ko phải tuyệt đối). Đây là kỹ thuật quét mặc định của Nmap.

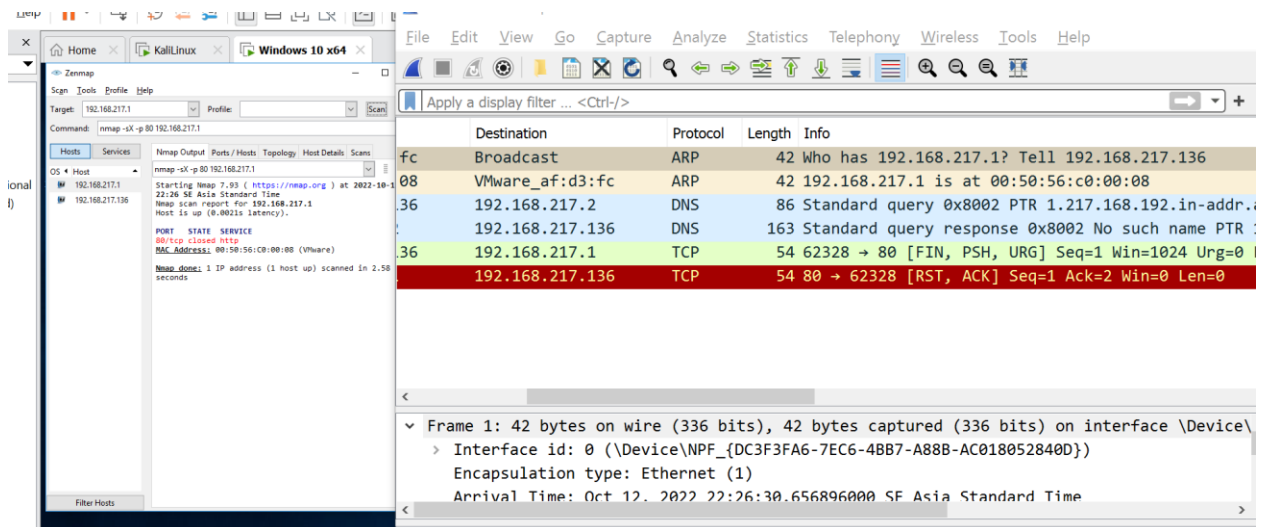
- **nmap -sS -p 135 192.168.247.1**
- -> Quét port 135 (SMB chia sẻ file dùng cho window) cho thấy port chạy giao thức tcp và dùng dịch vụ smrpc (dịch vụ client – server)
- Bên tấn công gửi gói SYN qua mục tiêu, mục tiêu gửi lại SYN + ACK (cổng mở), ngay lập tức bên tấn công gửi tiếp RST (để kết thúc) -> qua mặt được firewall hay các cơ chế ghi lại lịch sử

Destination	Protocol	Length	Info
8.217.136 → 203.77.187.131	TCP	54	1928 → 80 [ACK] Seq=355 Ack=65797 Win=
8.217.136 → 203.77.187.131	TCP	54	1840 → 80 [ACK] Seq=355 Ack=10621 Win=
8.217.136 → 192.168.217.1	TCP	58	57025 → 135 [SYN] Seq=0 Win=1024 Len=
8.217.1 → 192.168.217.136	TCP	58	135 → 57025 [SYN, ACK] Seq=0 Ack=1 Wi
8.217.136 → 192.168.217.1	TCP	54	57025 → 135 [RST] Seq=1 Win=0 Len=0
.187.131 → 192.168.217.136	TCP	1506	80 → 1901 [PSH, ACK] Seq=32401 Ack=35
.187.131 → 192.168.217.136	TCP	1506	80 → 1901 [PSH, ACK] Seq=33853 Ack=35

## 2. Inverse TCP Flag scan **Xmas Scan**

Xmas Scan là kiểu scan trong đó chứa nhiều flag, các gói tin gửi đi song với FIN, PSH và URG -> nếu port đóng thì mục tiêu phản hồi với gói tin RST còn port mở mục tiêu không phản hồi cho kẻ tấn công

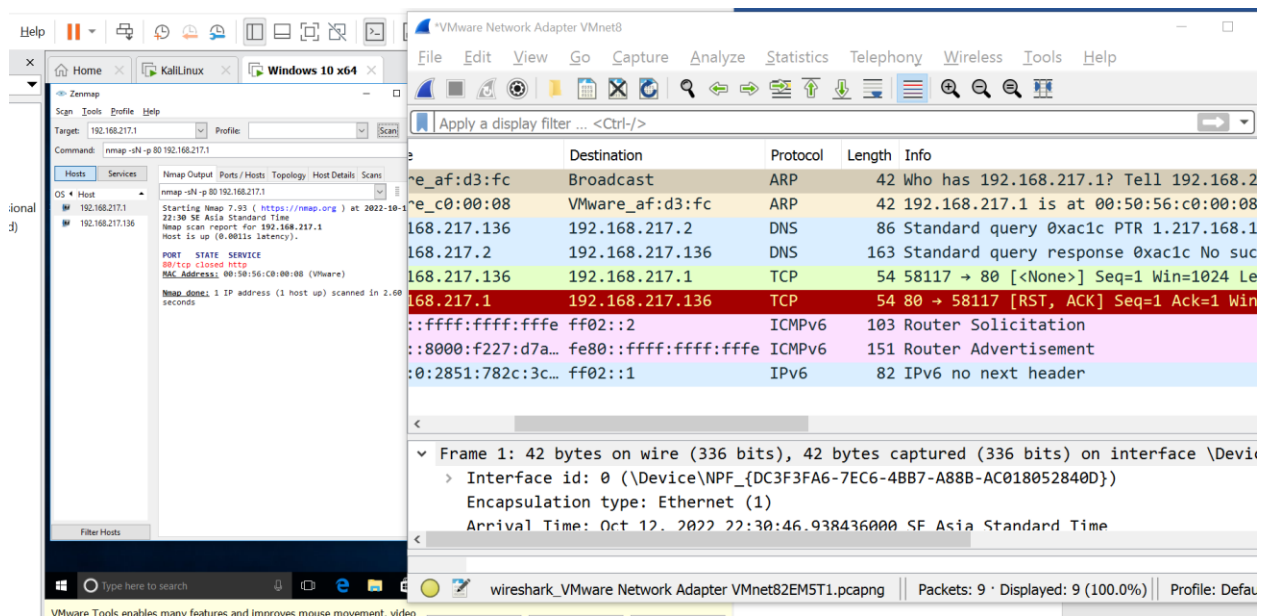
**Nmap -sX -p 80 192.168.217.1**



### 3. Null Scan

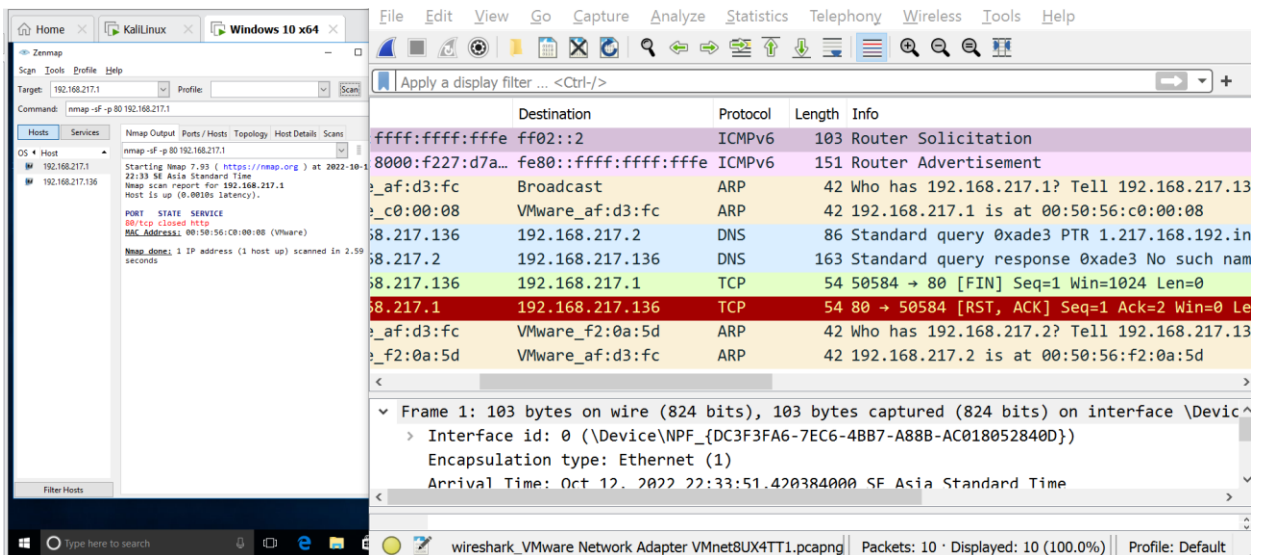
**Null Scan** Là quy trình gửi đi các gói tin không chứa các bộ flag. Các phản hồi đều tương tự với **FIN** và **XMAS Scan**. Nếu gói tin **Null Scan** gửi tới một port mở, sẽ không có phản hồi. Nếu gói tin Null Scan gửi tới port đóng, nó sẽ mang theo gói RST

**nmap -sN -p 80 192.168.247.1**



### 4. FIN SCAN

Kẻ tấn công sẽ gửi một gói tin với cờ **FIN** tới tất cả các cổng của mục tiêu. Với các cổng được mở, mục tiêu sẽ bỏ qua gói tin và không phản hồi về cho kẻ tấn công. Các cổng đóng sẽ gửi về gói tin RST để khởi tạo kết nối.

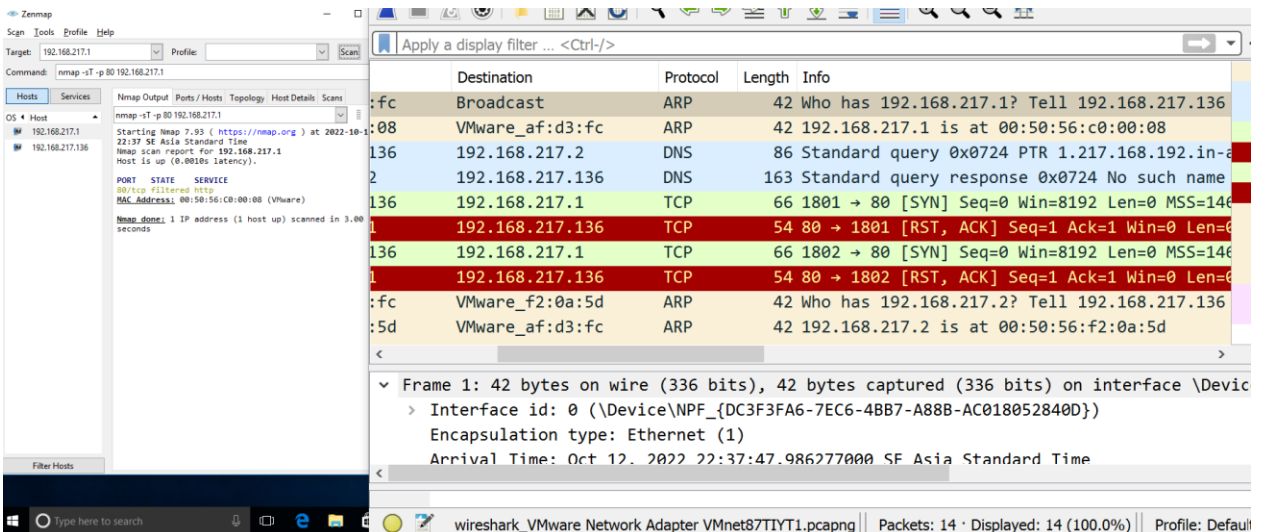


## 5. FULL Open scan

*TCP Connect scan (Full-open scan) : máy attacker sẽ thực hiện kết nối bằng giao thức TCP trên một cổng nhất định với đầy đủ bắt tay 3 bước như mô tả ở trên, tức là attacker gửi đi gói tin SYN. Nếu cổng mở, mục tiêu sẽ trả lời bằng gói tin SYN+ACK. Khi đó attacker gửi tiếp gói tin ACK để duy trì kết nối.*

*Nếu cổng đóng, mục tiêu sẽ trả lời bằng gói tin RST. ( ko nên dùng )*

***Nmap-sT -p 80 192.168.217.1***



***Nmap-sT -p 135 192.168.217.1***

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	af:d3:fc	Broadcast	ARP	42	Who has 192.168.217.1? Tell 192.168.217.1
2	0.000000	c0:00:08	VMware_af:d3:fc	ARP	42	192.168.217.1 is at 00:50:56:c0:00:08
3	0.000000	192.168.217.136	192.168.217.2	DNS	86	Standard query 0xc01 PTR 1.217.168.19
4	0.000000	192.168.217.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
5	0.000000	192.168.217.2	192.168.217.136	DNS	163	Standard query response 0xc01 No such
6	0.000000	192.168.217.136	192.168.217.1	TCP	66	1804 → 135 [SYN] Seq=0 Win=8192 Len=0
7	0.000000	192.168.217.1	192.168.217.136	TCP	66	135 → 1804 [SYN, ACK] Seq=0 Ack=1 Win=
8	0.000000	192.168.217.136	192.168.217.1	TCP	54	1804 → 135 [ACK] Seq=1 Ack=1 Win=52556

## 6. ACK flag probe scanning

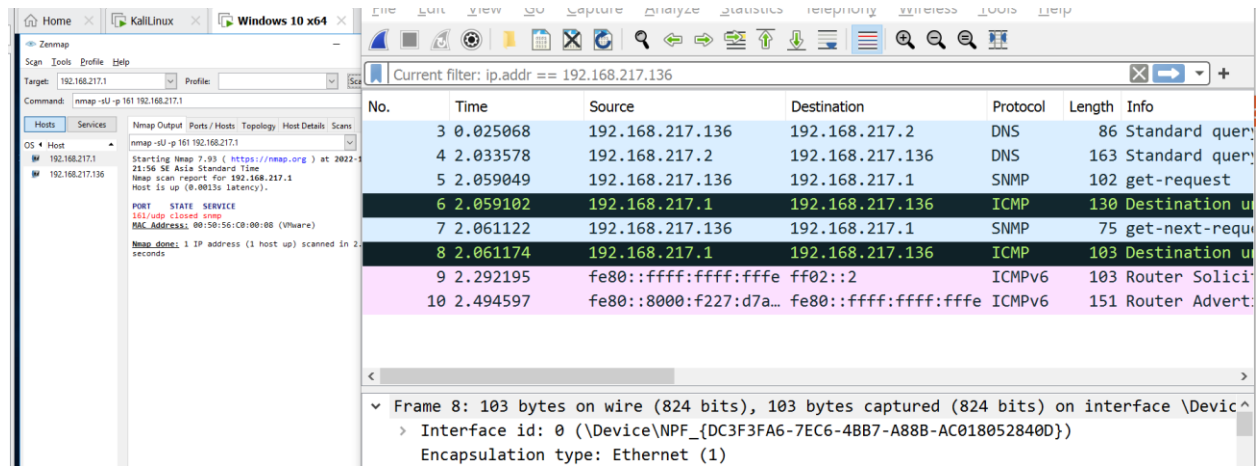
Quét dò cờ ACK : kẻ tấn công gửi gói thăm dò ACK với số thứ tự ngẫu nhiên, không có phản hồi có nghĩa là cổng được lọc (firewall on) còn trả lại phản hồi RST cổng không được lọc (firewall off)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	fe80::ffff:ffff:ffff	ff02::2	ICMPv6	103	Router Solicitation
2	0.000000	fe80::8000:f227:d7a...	fe80::ffff:ffff:ffff	ICMPv6	151	Router Advertisement
3	0.000000	192.168.217.136	192.168.217.2	DNS	86	Standard query 0x19ec PTR 1.217
4	0.000000	192.168.217.2	192.168.217.136	DNS	163	Standard query response 0x19ec
5	0.000000	192.168.217.136	192.168.217.1	TCP	54	62177 → 135 [ACK] Seq=1 Ack=1 W
6	0.000000	192.168.217.1	192.168.217.136	TCP	54	135 → 62177 [RST] Seq=1 Win=0 L
7	0.000000	192.168.217.136	192.168.217.2	NBNS	110	Refresh NB <01><02>_MSBROWSE

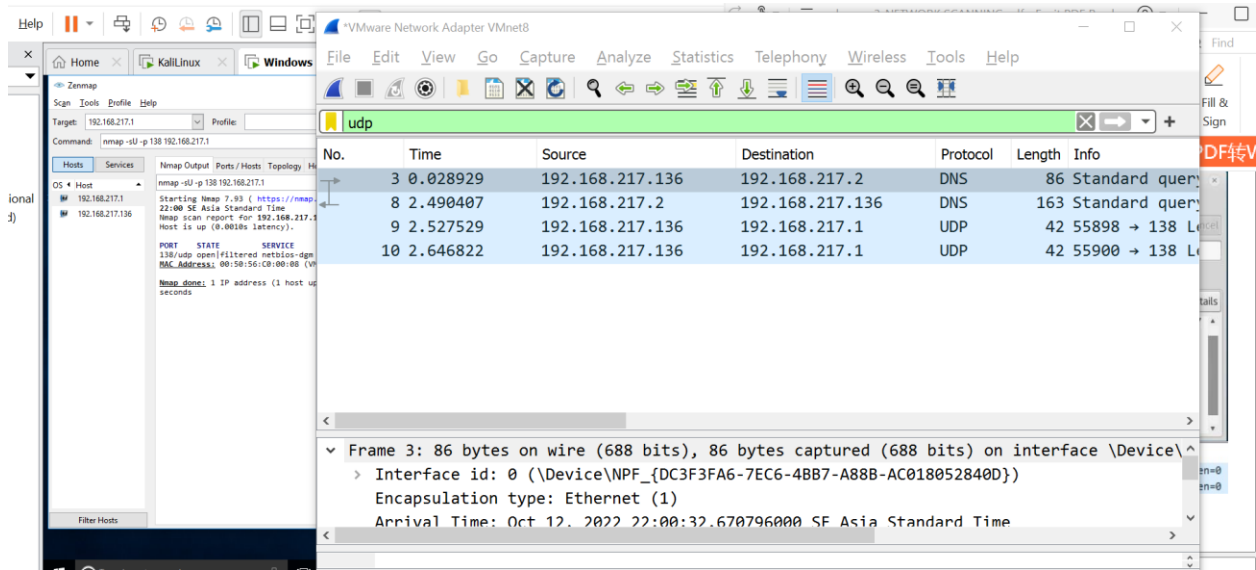
## 7. UDP scanning

- Kỹ thuật thăm dò cổng UDP đang mở. Gói UDP sẽ được gửi đi các cổng của mục tiêu, nếu cổng mở thì mục tiêu sẽ không gửi gì lại, còn cổng đóng thì mục tiêu gửi lại một gói tin ICMP Port Unreachable
- a. Cổng đóng





## b. Công mở



## 8. Decoy scan

Kĩ thuật giả mạo ip để scan

Mô hình lab: Kali máy tấn công có ip 192.168.217.100, các ip giả mạo 192.168.217.101, 192.168.217.102, 192.168.217.103, 192.168.217.104 .Tấn công vào máy win 10 có ip 192.168.217.136

```
(dinhhuan@kali)-[~]
$ sudo nmap -p 135 -D 192.168.217.101,192.168.217.102,192.168.217.103,192.168.217.104 192.168.217.136
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-27 18:07 +07
Nmap scan report for 192.168.217.136
Host is up (0.00063s latency).

PORT      STATE SERVICE
135/tcp   open  msrpc
MAC Address: 00:0C:29:AF:D3:FC (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.56 seconds

(dinhhuan@kali)-[~]
$
```

5	2.423567	192.168.217.101	192.168.217.136	TCP	60 61142 → 135 [SYN] Seq=0 Win=1024 Len=0 MS
6	2.423630	192.168.217.100	192.168.217.136	TCP	60 61142 → 135 [SYN] Seq=0 Win=1024 Len=0 MS
7	2.423660	192.168.217.102	192.168.217.136	TCP	60 61142 → 135 [SYN] Seq=0 Win=1024 Len=0 MS
8	2.423690	192.168.217.103	192.168.217.136	TCP	60 61142 → 135 [SYN] Seq=0 Win=1024 Len=0 MS
9	2.423718	192.168.217.104	192.168.217.136	TCP	60 61142 → 135 [SYN] Seq=0 Win=1024 Len=0 MS
10	2.424125	192.168.217.136	192.168.217.100	TCP	58 135 → 61142 [SYN, ACK] Seq=0 Ack=1 Win=819

Kiểm tra trên wireshark cách thức là ip của kẻ tấn công và các ip giả mạo đều gửi gói tin SYN tới máy bị tấn công để thăm dò . Lúc này trên máy bị tấn công không biết được ip nào đang scan tới mình để block .

### Bài 3 . IDLE /IPID Scanning

Bước 1: Hacker thực hiện một kết nối SYN/ACK packet đến abc.com và quan sát IPID. Và hiển nhiên máy chủ abc.com sẽ gửi lại RST packet (vì nó là gửi lần đầu thì đang xa lạ nên không chấp nhận ) và ta cũng biết được IPID . Ví dụ IPID cho trường hợp này là 33668.

Bước 2: Sau đó hacker sẽ thực hiện gửi packet đến server.com với địa chỉ IP giả là máy chủ abc.com. Và hiển nhiên máy chủ server.com sẽ gửi lại cho máy chủ abc.com với SYN/ACK được bật và máy chủ abc.com sẽ gửi RST packet trong trường hợp server.com mở cổng mà hacker đang cần kiểm tra. Giả sử trong trường hợp này cổng mở thì khi abc.com gửi RST packet đi thì nó sẽ tăng IPID lên 1. Vậy lúc này IPID có giá trị 33669. Và sẽ không tăng IPID nếu như cổng cần kiểm tra đóng.

Bước 3: Hacker thực hiện gửi SYN/ACK đến abc.com với địa chỉ IP fake và số port thì máy bị tấn công trả lại cho máy fake gói SYN/ACK (port mở - lúc này máy fake gửi gói RST cho hacker vì RST là kết thúc vì tự nhiên nó nhận được SYN/ACK lạ nên cần RST để kết thúc) còn RST(port đóng) và

kiểm tra thử IPID lúc này là bao nhiêu. Nếu như IPID mới bằng IPID cũ + 2 tức là cổng đó mở và ngược lại thì cổng cần kiểm tra đó đóng.



- Để xác định cổng nào đang mở , gửi gói tin SYN đến PORT
- Mục tiêu sẽ phản hồi bằng gói tin SYN + ACK nếu port đang mở , còn PORT đang đóng thì sẽ phản hồi bằng RST
- Gói tin SYN + ACK không yêu cầu có thể , hoặc phớt lờ hoặc phản hồi bằng RST
- Mỗi gói IP đều có một số IPID , số gia OS
  - Cách thực hiện IDLE/IPID
    - + gửi gói tin SYN + ACK đến zombie để lấy IPID , zombie không chờ phản hồi SYN + ACK nên sẽ phản hồi bằng RST -> bị lộ IPID
    - + Gửi gói tin đến mục tiêu , đánh lừa địa chỉ IP của Zombie , Ip port mở mục tiêu phản hồi bằng SYN + ACK cho Zombie và Zombie sẽ phản hồi lại cho mục tiêu gói tin RST , nếu port đóng thì mục tiêu phản hồi lại cho zombie bằng gói RST và Zombie không phản hồi cho mục tiêu gì thêm , IPID zombie không được nhân lên
    - + Gửi syn + ack một lần nữa để lấy được số IPID và so sánh với IPID đã giải nén ở bước 1 , zombie phản hồi bằng RST , lời phản hồi tiết lộ IPID -> giải nén IPID -> port đang mở nếu IPID được nhân lên bằng 2 còn port đóng IPID nhân lên bằng 1

#### Sơ đồ lab :

- máy tấn công là Kali linux có ip : 192.168.217.100
- máy zombie (máy bị giả mạo ip) là máy win 7 có ip : 192.168.217.142
- máy bị tấn công là win 10 có ip : 192.168.217.136
- `sudo nmap -p 135 -sI 192.168.217.142 192.168.217.136`

**\*Đối với trường hợp port mở :**

```

dinhhuan@kali: ~
File Actions Edit View Help
(dinhhuan@kali)~$ sudo nmap -p 135 -sI 192.168.217.142 192.168.217.136
WARNING: Many people use -Pn w/Idlescan to prevent pings from their true IP.
On the other hand, timing info Nmap gains from pings can allow for faster, more reliable scans.
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-27 18:19 +07
Idle scan using zombie 192.168.217.142 (192.168.217.142:443); Class: Incremental
Nmap scan report for 192.168.217.136
Host is up (0.0070s latency).

PORT      STATE SERVICE
135/tcp   open  msrpc
MAC Address: 00:0C:29:AF:D3:FC (VMware)

Nmap done: 1 IP address (1 host up) scanned in 5.06 seconds

(dinhhuan@kali)~$

```

34	8.246883	192.168.217.136	192.168.217.142	TCP	58 [TCP Port numbers reused] 135 → 443 [SYN, ACK] Seq=1 Win=0 Len=0
35	8.247155	192.168.217.142	192.168.217.136	TCP	54 443 → 135 [RST] Seq=1 Win=0 Len=0
36	8.296744	192.168.217.100	192.168.217.142	TCP	60 56779 → 443 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
37	8.297659	192.168.217.142	192.168.217.100	TCP	54 443 → 56779 [RST] Seq=1 Win=0 Len=0
38	8.351342	192.168.217.100	192.168.217.142	TCP	60 56656 → 443 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
39	8.357378	192.168.217.142	192.168.217.100	TCP	54 443 → 56656 [RST] Seq=1 Win=0 Len=0
40	8.357680	192.168.217.142	192.168.217.136	TCP	60 [TCP Retransmission] [TCP Port numbers reused] 443 → 135 [RST] Seq=1 Win=0 Len=0
41	8.358345	192.168.217.136	192.168.217.142	TCP	58 [TCP Previous segment not captured] [TCP Port numbers reused] 135 → 443 [SYN, ACK] Seq=1 Win=0 Len=0
42	8.358569	192.168.217.142	192.168.217.136	TCP	54 443 → 135 [RST] Seq=1 Win=0 Len=0
43	8.411176	192.168.217.100	192.168.217.142	TCP	60 56778 → 443 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
44	8.411589	192.168.217.142	192.168.217.100	TCP	54 443 → 56778 [RST] Seq=1 Win=0 Len=0
45	8.465481	192.168.217.100	192.168.217.142	TCP	60 56633 → 443 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
46	8.465834	192.168.217.142	192.168.217.100	TCP	54 443 → 56633 [RST] Seq=1 Win=0 Len=0
47	10.506986	192.168.217.136	20.198.118.190	TLSv1.2	125 Application Data
48	10.507000	20.198.118.190	192.168.217.136	TCP	54 443 → 135 [ACK] Seq=1 Ack=73 Win=64340 Len=0

Packet 35 - VMware Network Adapter VMnet8

```

0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes
Differentiated Services Field: 0x00
  0000 00.. = Differentiated Services Codepoint: Default (0)
  .... ..00 = Explicit Congestion Notification: Not ECN-Capable
Total Length: 40
Identification: 0x02ee (750)

```

Packet 42 - VMware Network Adapter VMnet8

```

0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  0000 00.. = Differentiated Services Codepoint: Default (0)
  .... ..00 = Explicit Congestion Notification: Not ECN-Capable
Total Length: 40
Identification: 0x02f1 (753)
Flags: 0x40, Don't fragment

```

-Bắt gói tin 35 trên wireshak thấy IPID 750 , và bắt gói 42 mở gói xem IPID thấy 752 -> IPID tăng lên 2 tức là port mở

**\*Đối với trường hợp port đóng**

```
(dinhhuan@kali)-[~]
$ sudo nmap -p 80 -sI 192.168.217.142 192.168.217.136
WARNING: Many people use -Pn w/Idlescan to prevent pings from their true IP.
On the other hand, timing info Nmap gains from pings can allow for faster, more reliable scans.
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-27 18:30 +07
Idle scan using zombie 192.168.217.142 (192.168.217.142:443); Class: Incremental
Nmap scan report for 192.168.217.136
Host is up (0.0015s latency).

PORT      STATE      SERVICE
80/tcp    closed|filtered http
MAC Address: 00:0C:29:AF:D3:FC (VMware)

Nmap done: 1 IP address (1 host up) scanned in 5.64 seconds

(dinhhuan@kali)-[~]
$
```

32	4.103522	192.168.217.142	192.168.217.100	TCP	54 443 → 63454 [RST] Seq=1 Win=0 Len=0
33	4.103767	192.168.217.142	192.168.217.136	TCP	60 443 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
34	4.104088	192.168.217.136	192.168.217.142	TCP	54 80 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
35	4.155318	192.168.217.100	192.168.217.142	TCP	60 63531 → 443 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
36	4.157393	192.168.217.142	192.168.217.100	TCP	54 443 → 63531 [RST] Seq=1 Win=0 Len=0
37	4.179373	192.168.217.100	192.168.217.142	TCP	60 63396 → 443 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
38	4.179843	192.168.217.142	192.168.217.100	TCP	54 443 → 63396 [RST] Seq=1 Win=0 Len=0
39	4.234013	192.168.217.100	192.168.217.142	TCP	60 63436 → 443 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
40	4.234375	192.168.217.142	192.168.217.100	TCP	54 443 → 63436 [RST] Seq=1 Win=0 Len=0
41	4.234665	192.168.217.142	192.168.217.136	TCP	60 [TCP Retransmission] [TCP Port numbers reused] 44
42	4.235447	192.168.217.136	192.168.217.142	TCP	54 80 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
43	4.286351	192.168.217.100	192.168.217.142	TCP	60 63500 → 443 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
44	4.286749	192.168.217.142	192.168.217.100	TCP	54 443 → 63500 [RST] Seq=1 Win=0 Len=0
45	4.313350	192.168.217.100	192.168.217.142	TCP	60 63539 → 443 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0
46	4.313704	192.168.217.142	192.168.217.100	TCP	54 443 → 63539 [RST] Seq=1 Win=0 Len=0

Wireshark · Packet 42 · VMware Network Adapter VMnet8

```
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (
v Differentiated Services Field: 0x00 (
0000 00.. = Differentiated Service:
.... ..00 = Explicit Congestion Not
Total Length: 40
Identification: 0x5a14 (23060)
> Flags: 0x40, Don't fragment
```

Wireshark · Packet 34 · VMware Network Adapter VMnet8

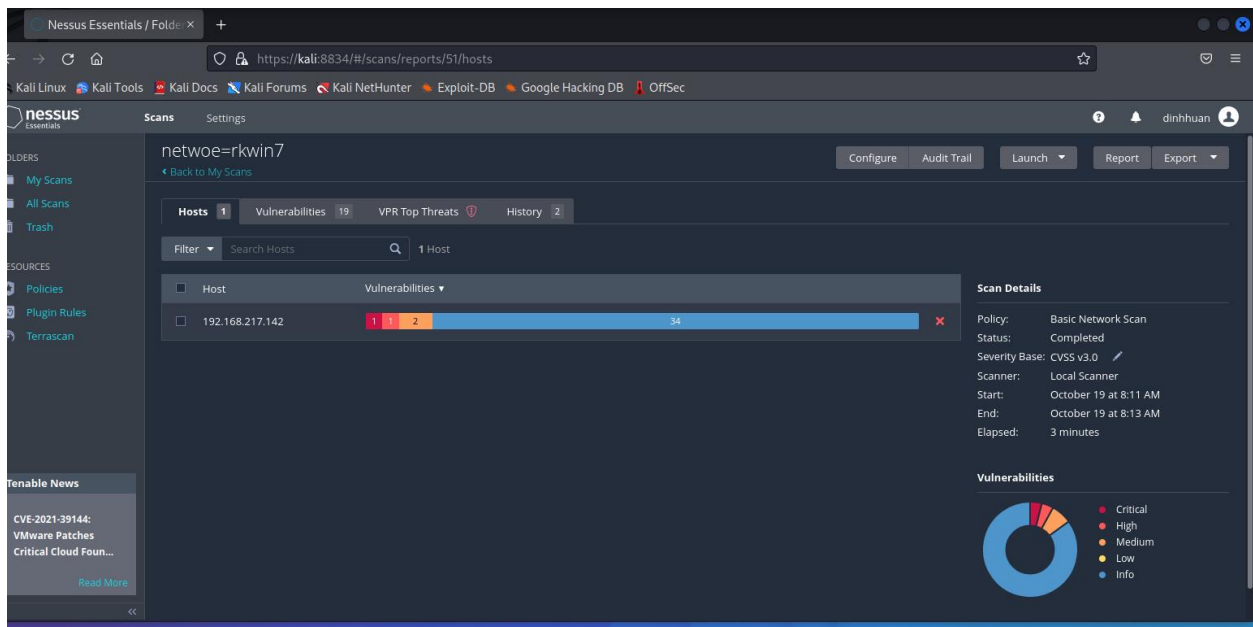
```
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (!
v Differentiated Services Field: 0x00 (l
0000 00.. = Differentiated Services:
.... ..00 = Explicit Congestion Not
Total Length: 40
Identification: 0x5a13 (23059)
> Flags: 0x40, Don't fragment
```

Bắt gói tin 34 trên wireshak thấy IPID 23059 , và bắt gói 42 mở gói xem IPID thấy 23060 -> IPID tăng lên 1 tức là port đóng .

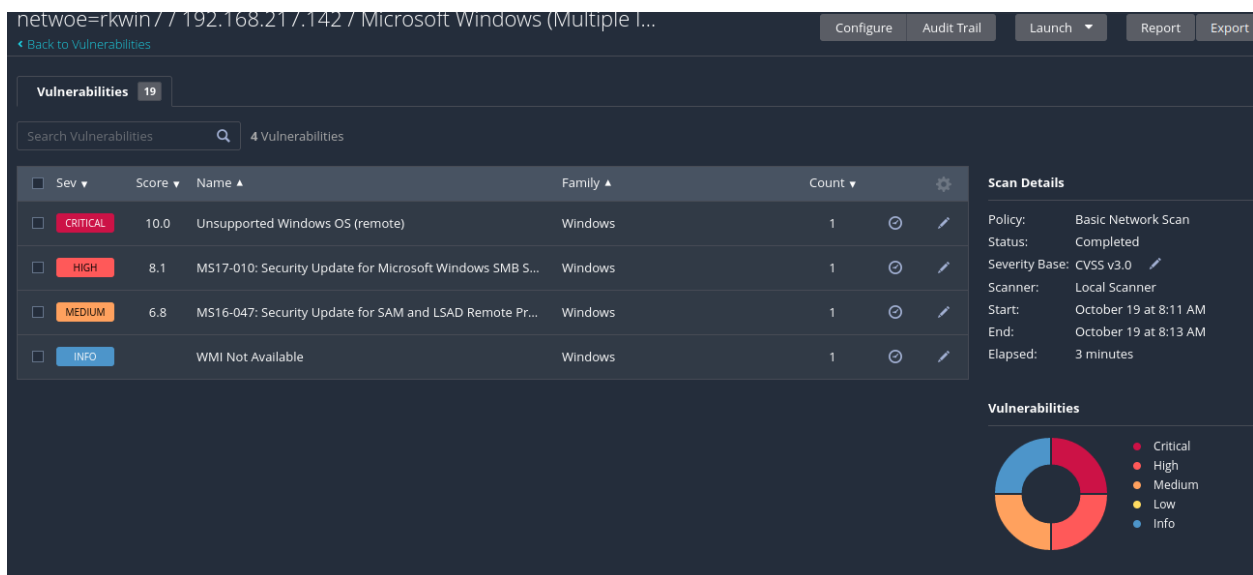
## Bài 4 : Quét thông tin với nessus

Thực hiện quét thông tin window 7 với ip 192.168.217.142

-Kết quả quét được có 34 lỗi thường, 2 lỗi medium , 1 lỗi high và 1 lỗi nguy hiểm



## Chi tiết các lỗi



### Nguyên nhân và cách khắc phục lỗi Critical :

network=rkwin7 / Plugin #108797

[Back to Vulnerability Group](#)

Vulnerabilities19

CRITICAL

Unsupported Windows OS (remote)

>

Description

The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.

Solution

Upgrade to a supported service pack or operating system

See Also

<https://support.microsoft.com/en-us/lifecycle>

Output

The following Windows version is installed and not supported:

Microsoft Windows 7 Home

Port▲

Hosts

Plugin Details

Severity:Critical

ID:108797

Version:1.14

Type:remote

Family:Windows

Published:April 3, 2017

Modified:July 5, 2017

Risk Information

Risk Factor:Critical

CVSS v3.0 Base Score:10.0

CVSS v3.0 Vector:CVSS:3.0/!U:/N:/S:/C:/H:/I:/H/A:/H

CVSS v2.0 Base Score:10.0

CVSS v2.0 Vector:CVSS2#:/!:/C/A:/C

Nguyên nhân và cách khắc phục lỗi mức high :

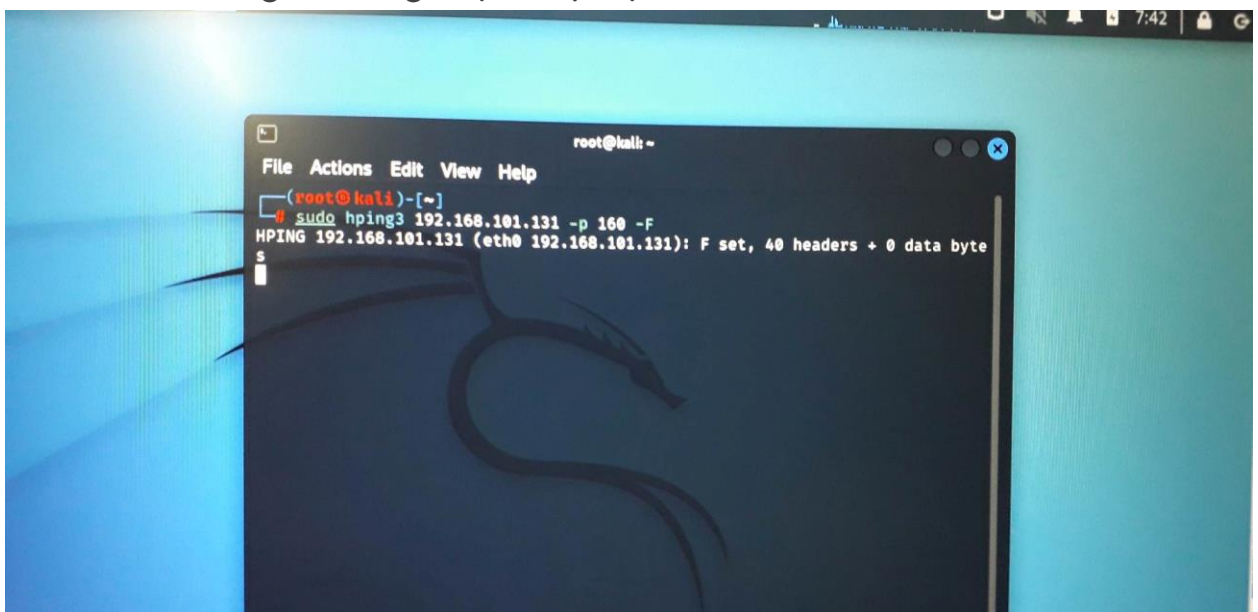
HIGH	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ET...
<b>Description</b> <p>The remote Windows host is affected by the following vulnerabilities :</p> <ul style="list-style-type: none"><li>- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)</li><li>- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)</li></ul> <p>ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.</p> <b>Solution</b> <p>Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.</p> <p>For unsupported Windows operating systems, e.g. Windows XP, Microsoft recommends that users discontinue the use of SMBv1. SMBv1 lacks security features that were included in later SMB versions. SMBv1 can be disabled by following the vendor instructions provided in Microsoft KB2696547. Additionally, US-CERT recommends that users block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.</p>	

### Hping3

a. kali > hping3 -S 192.168.1.116 -p 80

```
root@kali:~# hping3 -S 192.168.1.116 -p 80
HPING 192.168.1.116 (eth0 192.168.1.116): S set, 40 headers + 0 data bytes
len=46 ip=192.168.1.116 ttl=128 DF id=17420 sport=80 flags=RA seq=0 win=0 rtt=1.
3 ms
len=46 ip=192.168.1.116 ttl=128 DF id=17422 sport=80 flags=RA seq=1 win=0 rtt=1.
0 ms
len=46 ip=192.168.1.116 ttl=128 DF id=17423 sport=80 flags=RA seq=2 win=0 rtt=0.
9 ms
len=46 ip=192.168.1.116 ttl=128 DF id=17425 sport=80 flags=RA seq=3 win=0 rtt=7.
5 ms
len=46 ip=192.168.1.116 ttl=128 DF id=17426 sport=80 flags=RA seq=4 win=0 rtt=0.
9 ms
len=46 ip=192.168.1.116 ttl=128 DF id=17428 sport=80 flags=RA seq=5 win=0 rtt=0.
5 ms
```

Kết quả của bài kiểm tra này sẽ trả về **SA** cờ, có nghĩa là nó tương ứng với **SYN/ACK** , nghĩa là, giao tiếp đã được chấp nhận, hoặc tương tự, **cảng đang mở** . Ngược lại, nếu giá trị là **RA** nó tương ứng với **RST / ACK** hoặc điều gì giống nhau, giao tiếp không được thực hiện một cách chính xác vì **cảng đã đóng** hoặc được lọc



### Fin scan port hping3

Sudo hping3 192.12.12.x -p 160 -F

Attacker gửi đi các gói tin tới mục tiêu .Nếu mục tiêu không phản hồi thì là port mở còn mục tiêu gửi về gói tin RST thì là port đóng . Hacker gửi gói tin FIN thăm dò bằng giao thức TCP lúc này win10 gửi lại gói tin [RST/ACK] thì là port đó đang đóng . còn không phản hồi là port đó đang mở .



