Nhóm 10:

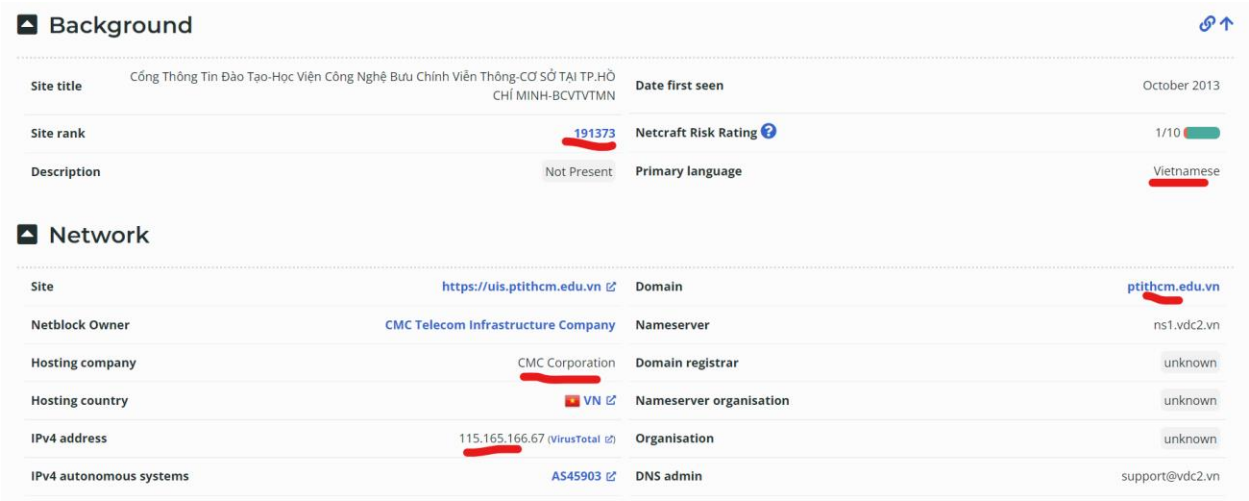
Chu Đình Huấn - MSSV : N19DCVT013

Nguyễn Giê Nha – MSSV : N19DCVT040

Lớp : D19CQVT01-N

Bài 1 . Netcarft

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



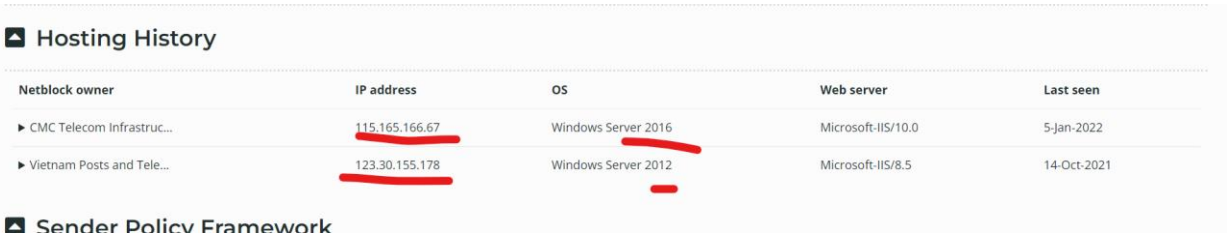
Background

Site title	Cổng Thông Tin Đào Tạo-Học Viện Công Nghệ Bưu Chính Viễn Thông-CƠ SỞ TẠI TP.HỒ CHÍ MINH-BCVTVTMN	Date first seen	October 2013
Site rank	191373	Netcraft Risk Rating	1/10
Description	Not Present	Primary language	Vietnamese

Network

Site	https://uis.ptithcm.edu.vn	Domain	ptithcm.edu.vn
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**

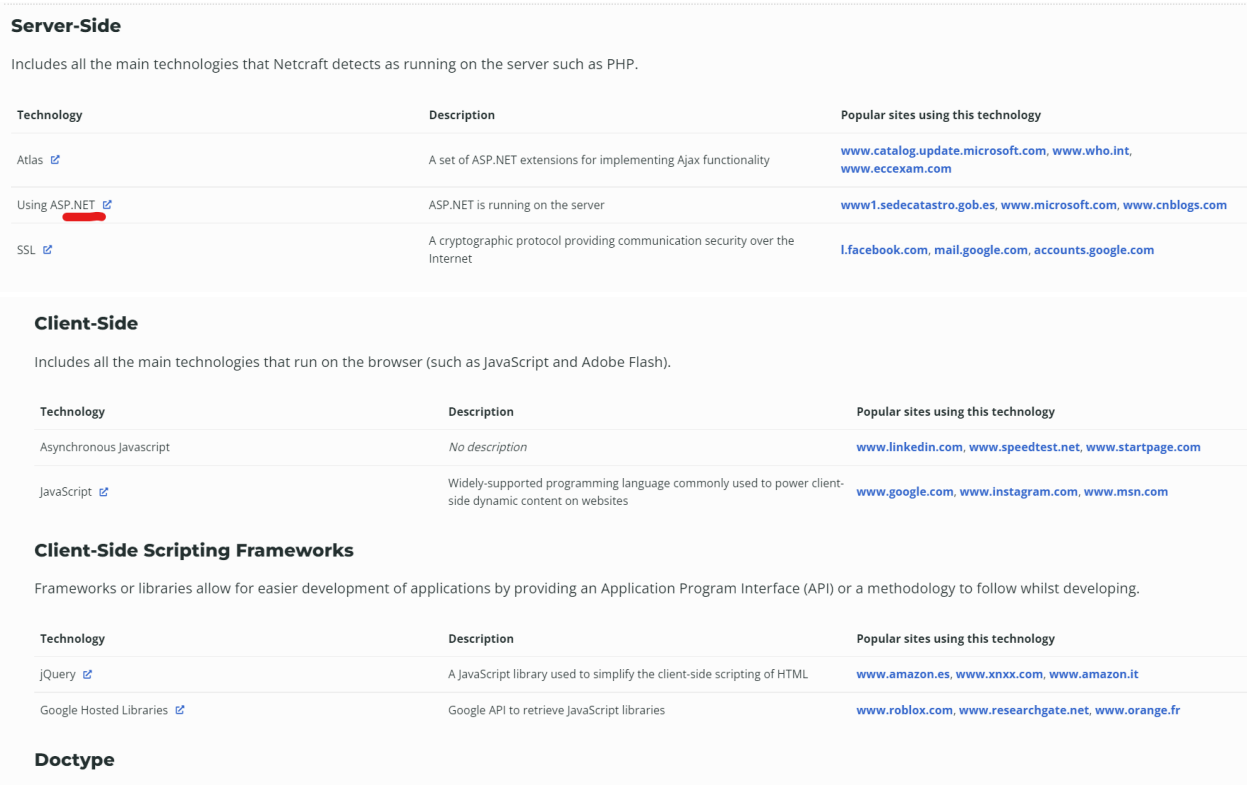


Hosting History

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 quan 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 set of ASP.NET extensions for implementing Ajax functionality	www.catalog.update.microsoft.com, www.who.int, www.eccexam.com
Using ASP.NET	ASP.NET is running on the server	www1.sedecatastro.gob.es, www.microsoft.com, www.cnblogs.com
SSL	A cryptographic protocol providing communication security over the Internet	l.facebook.com, mail.google.com, accounts.google.com

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*	www.linkedin.com, www.speedtest.net, www.startpage.com
JavaScript	Widely-supported programming language commonly used to power client-side dynamic content on websites	www.google.com, www.instagram.com, www.msn.com

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 JavaScript library used to simplify the client-side scripting of HTML	www.amazon.es, www.xnxx.com, www.amazon.it
Google Hosted Libraries	Google API to retrieve JavaScript libraries	www.roblox.com, www.researchgate.net, www.orange.fr

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 widown 10 thật có ip : 192.168.217.1

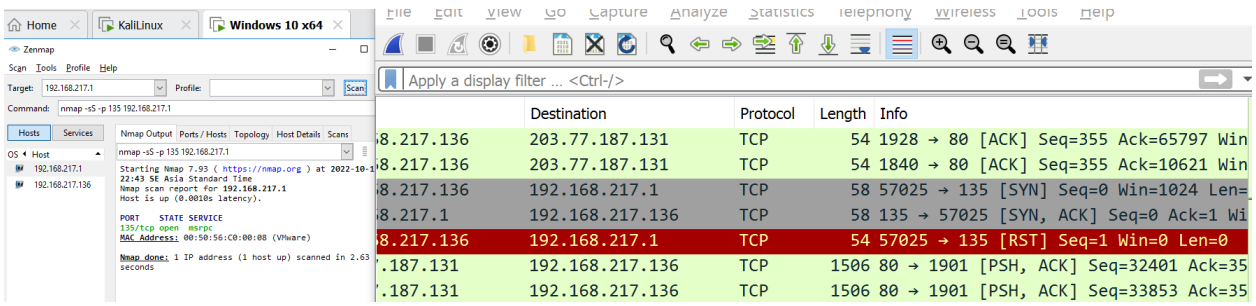
2. Window 10 ảo trên Vmware có ip : 192.168.217.136

1. Halft-open Scan:

TCP SYN scan (Half-open scan) : giống như Full-open scan, nhưng sở dĩ 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.

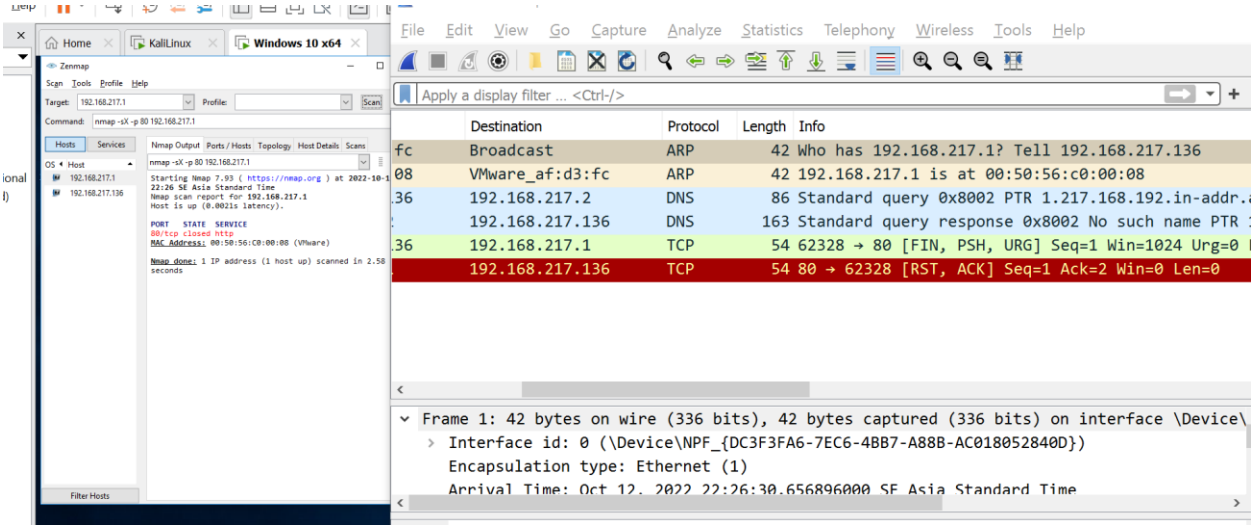
- **nmap -sS -p 135 192.168.247.1**
- *-> Quét port 135 (SMB chia sẻ file dùng cho window) cho thấy port chạy giao thức tcp và dùng dịch vụ smrpc (dịch vụ client – server)*
- ***Bên tấn công gửi gói SYN qua mục tiêu, mục tiêu gửi lại SYN + ACK (cổng mở) , ngay lập tức bên tấn công gửi tiếp RST (để kết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



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

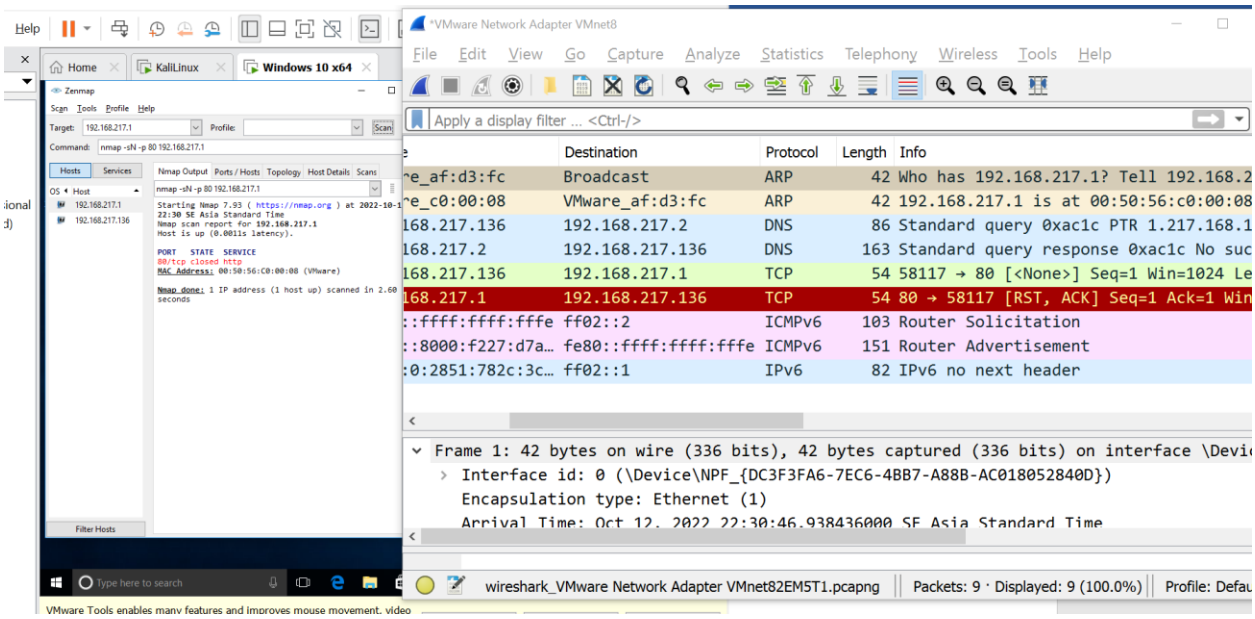
Nmap –sX –p 80 192.168.217.1



3. Null Scan

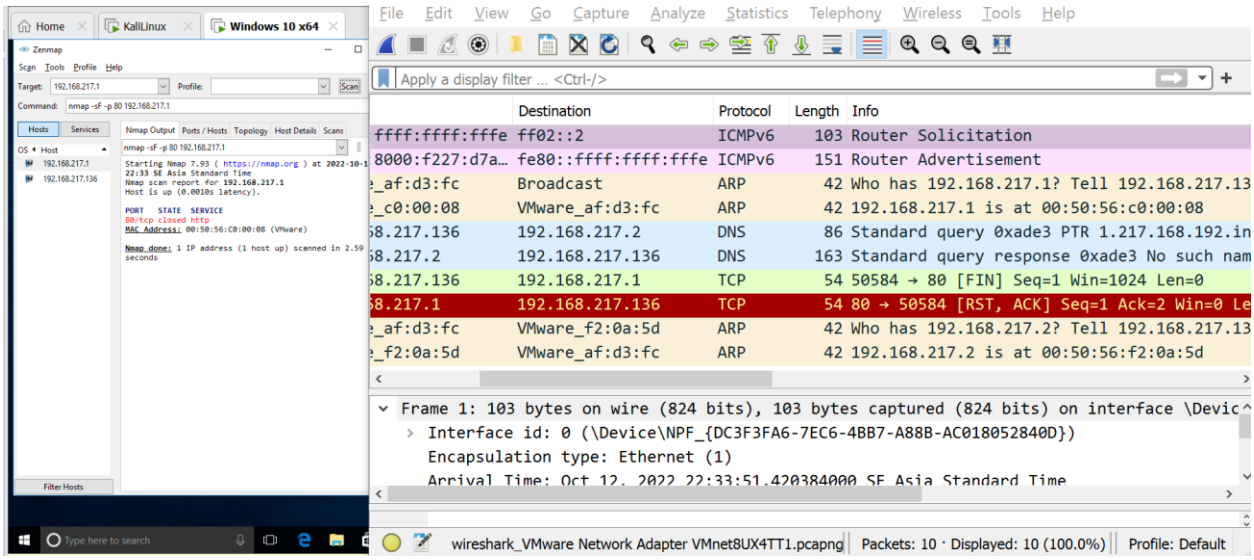
Null Scan *Là quy trình gửi đi các gói tin không chứa các* ***bộ flag****. Các phản hồi đều tương tự với* ***FIN*** *và* ***XMAS Scan****. Nếu gói tin* ***Null Scan*** *gửi tới một port mở, sẽ không có phản hồi. Nếu gói tin Null Scan gửi tới port đóng, nó sẽ mang theo gói RST*

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.*

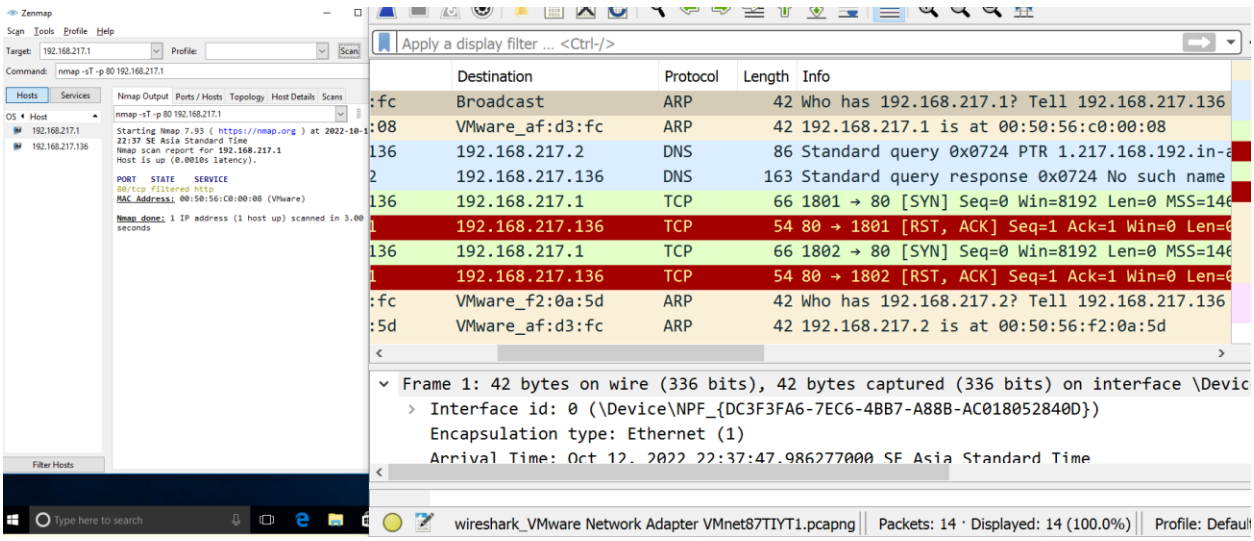


5. FULL Open scan

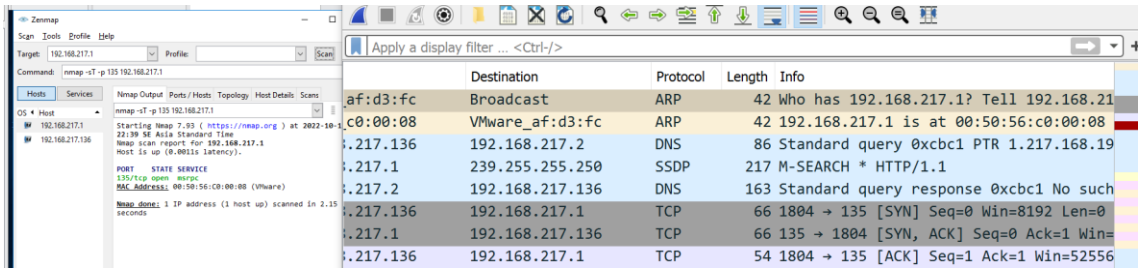
TCP Connect scan (Full-open scan) : máy attacker sẽ thực hiện kết nối bằng giao thức TCP trên một cổng nhất định với đầy đủ bắt tay 3 bước như mô tả ở trên, tức là attacker gửi đi gói tin SYN. Nếu cổng mở, mục tiêu sẽ trả lời bằng gói tin SYN+ACK. Khi đó attacker gửi tiếp gói tin ACK để duy trì kết nối.

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

Nmap-sT –p 80 192.168.217.1

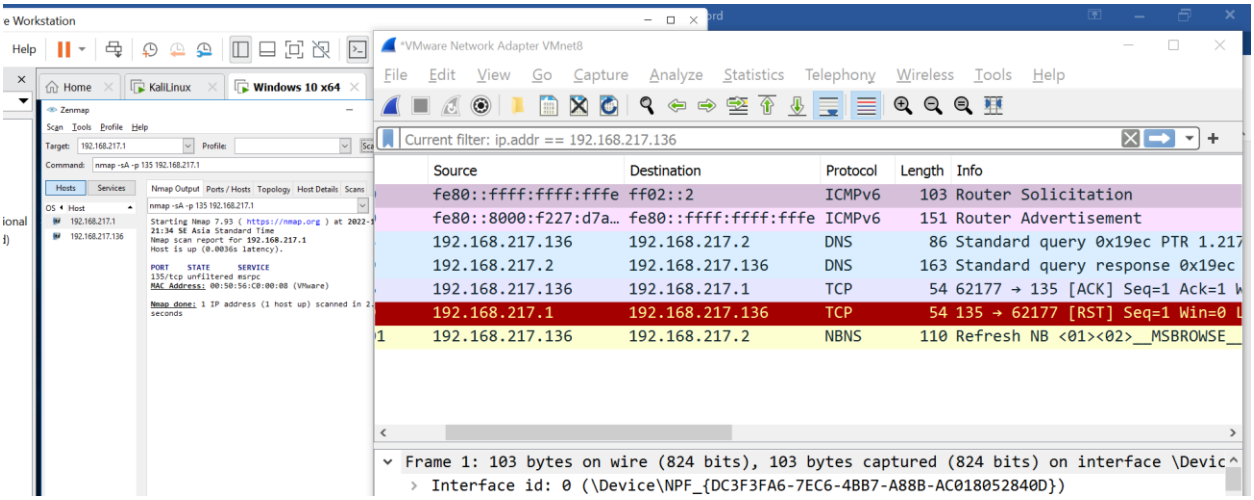


Nmap-sT –p 135 192.168.217.1



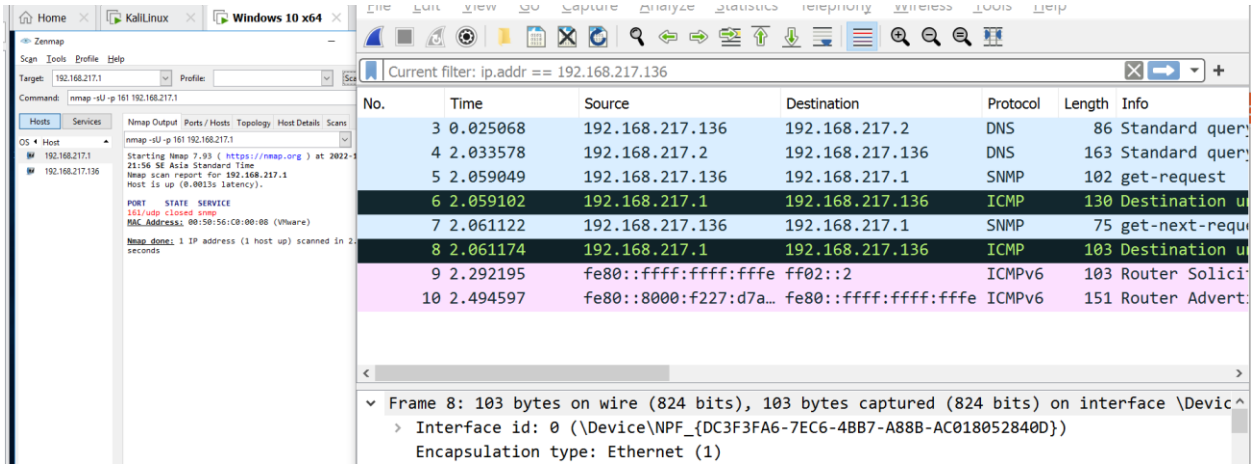
6. ACK flag probe scanning

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)

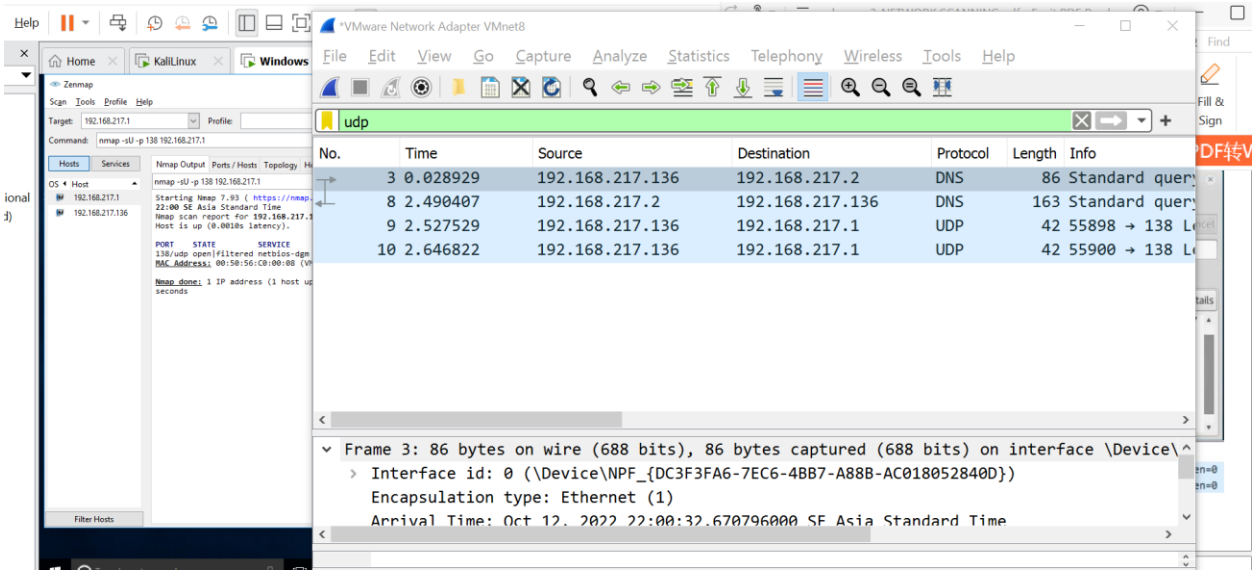


7. UDP scanning

- 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 Ủneachable
  a. Cổng đóng



b. Cổng 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 MSS
6	2.423630	192.168.217.100	192.168.217.136	TCP	60 61142 → 135 [SYN] Seq=0 Win=1024 Len=0 MSS
7	2.423660	192.168.217.102	192.168.217.136	TCP	60 61142 → 135 [SYN] Seq=0 Win=1024 Len=0 MSS
8	2.423690	192.168.217.103	192.168.217.136	TCP	60 61142 → 135 [SYN] Seq=0 Win=1024 Len=0 MSS
9	2.423718	192.168.217.104	192.168.217.136	TCP	60 61142 → 135 [SYN] Seq=0 Win=1024 Len=0 MSS
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 wireshak 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 chi 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

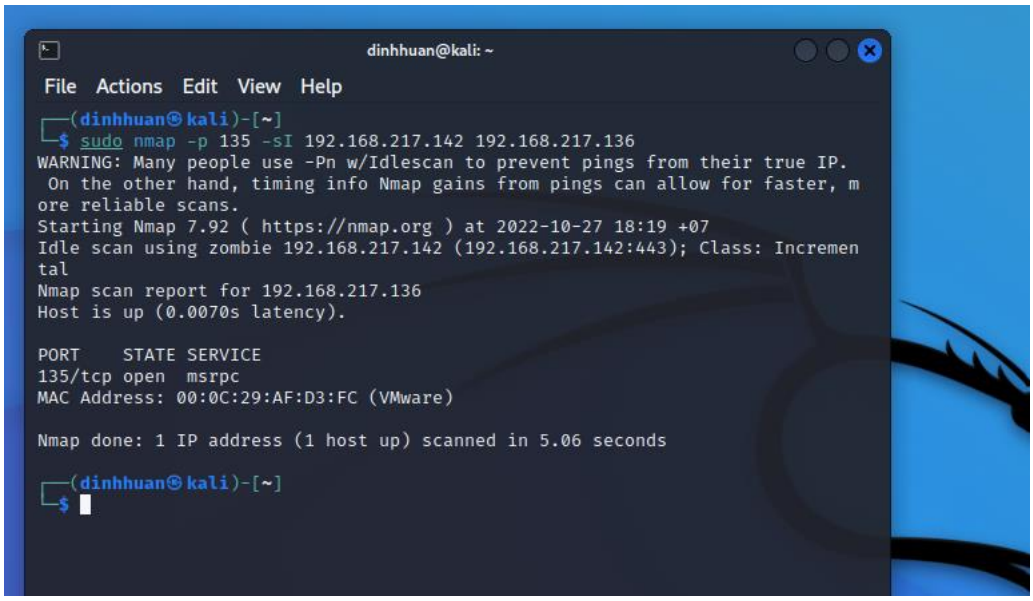
kiểm tra thử IPID lúc này là bao nhiêu. Nếu như IPID mới bằng IPID cũ + 2 tức là cổng đó mở và ngược
lại thì cổng cần kiểm tra đó đóng.

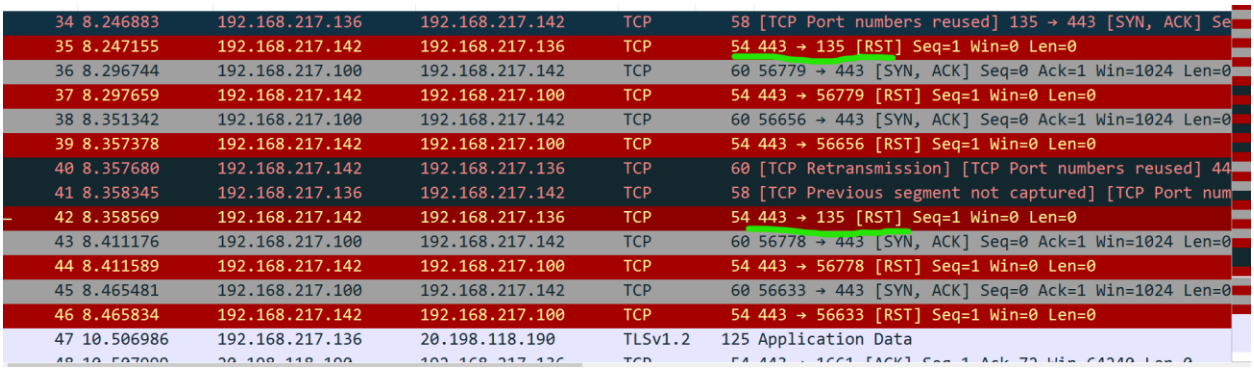
- Để xác định cổng nào đang mở , gửi gói tin SYN đến PORT
- Mục tiêu sẽ phản hồi bằng gói tin SYN + ACK nếu port đang mở , còn PORT đang đóng thì thì sẽ phản hồi bằng RST
- Gói tin SYN + ACK không yêu cầu có thể ,hoặc phớt lờ hoặc phản hồi băng RST
- Mỗi gói IP đều có một số IPID , số gia OS
  - Cách thực hiện IDLE/IPID
    + gửi gói tín SYN + ACK đến zombie để lấy IPID , zombiekhông chờ phản hồi SYN + ACK nên sẽ phản hồi bằng RST -> bị lộ IPID

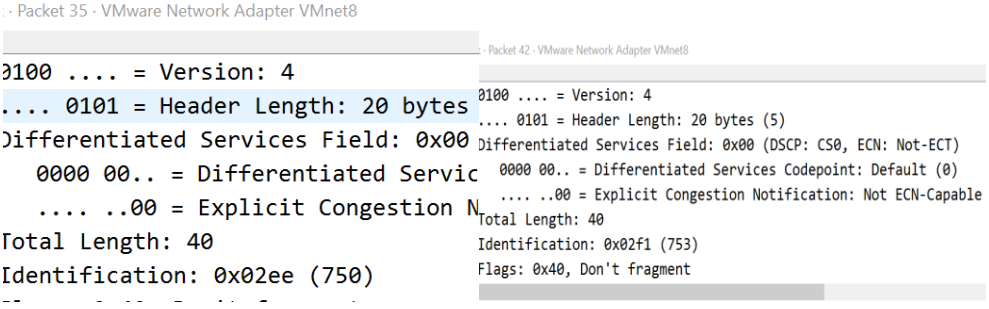
    + Gửi gói tin đến mục tiêu , đánh lừa địa chỉ IP của Zombie , Ip port mở mục tiêu ohanr hồi bằng SYN + ACK cho Zombie và Zombie sẽ phản hồi lại cho mục tiêu gói tin RST , nếu port đóng thì mục tiêu phản hồi lại cho zombie bằng gói RST và Zombie không phản hồi cho mục tiêu gì thêm , IPID zombie không 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 băng 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 :**

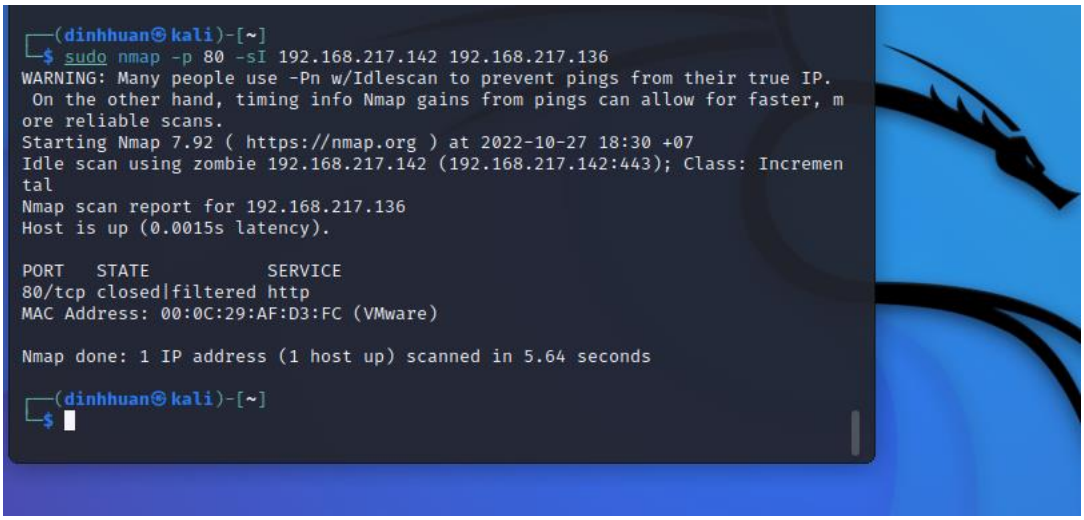


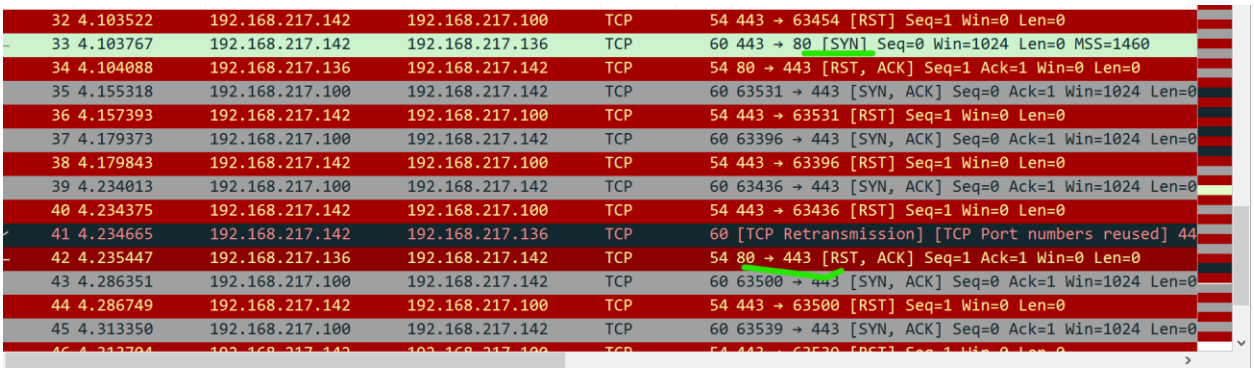


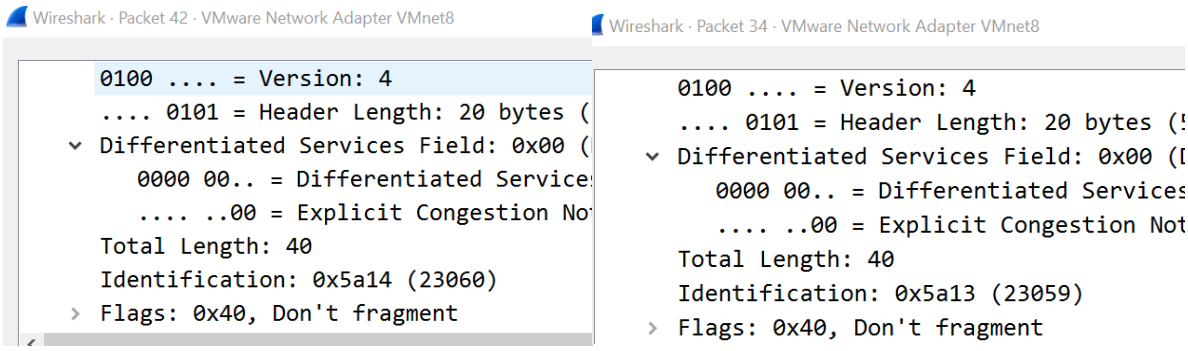


-Bắt gói tin 35 trên wireshak thấy IPID 750 , và bắt gói 42 mở gói xem IPID thấy 752 -> IPID tăng lên 2 tức là port mở

*Đối với trường hợp port đóng





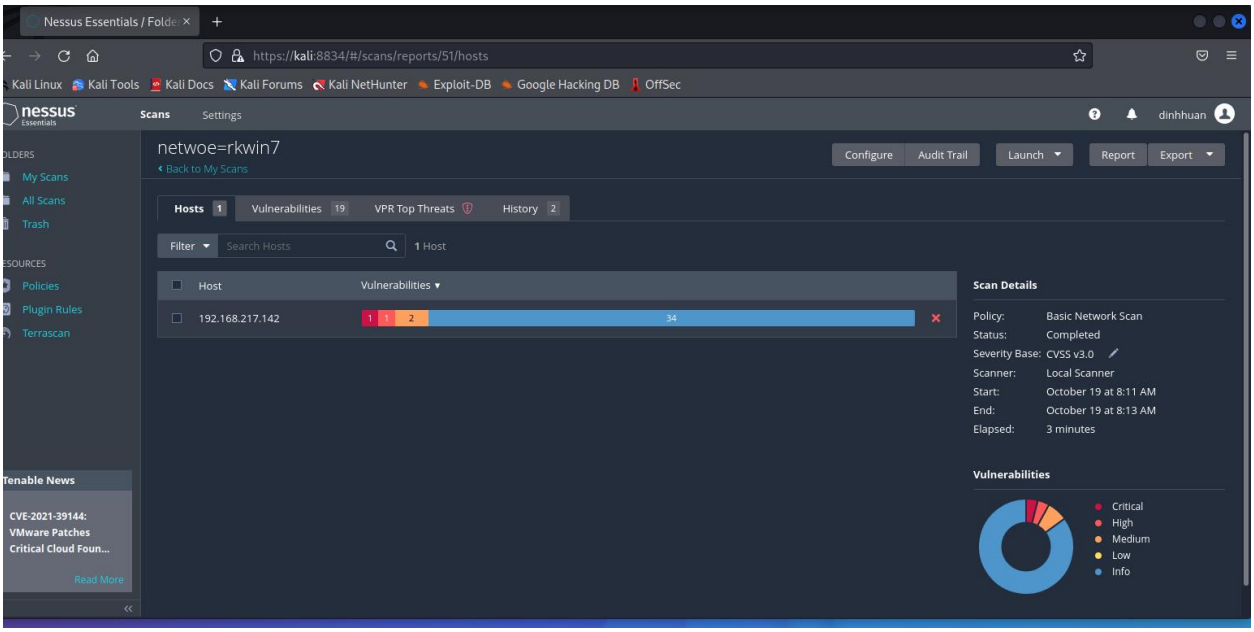


Bắt gói tin 34 trên wireshak thấy IPID 23059 , và bắt gói 42 mở gói xem IPID thấy 23060 -> IPID tăng lên 1 tức là port đóng .

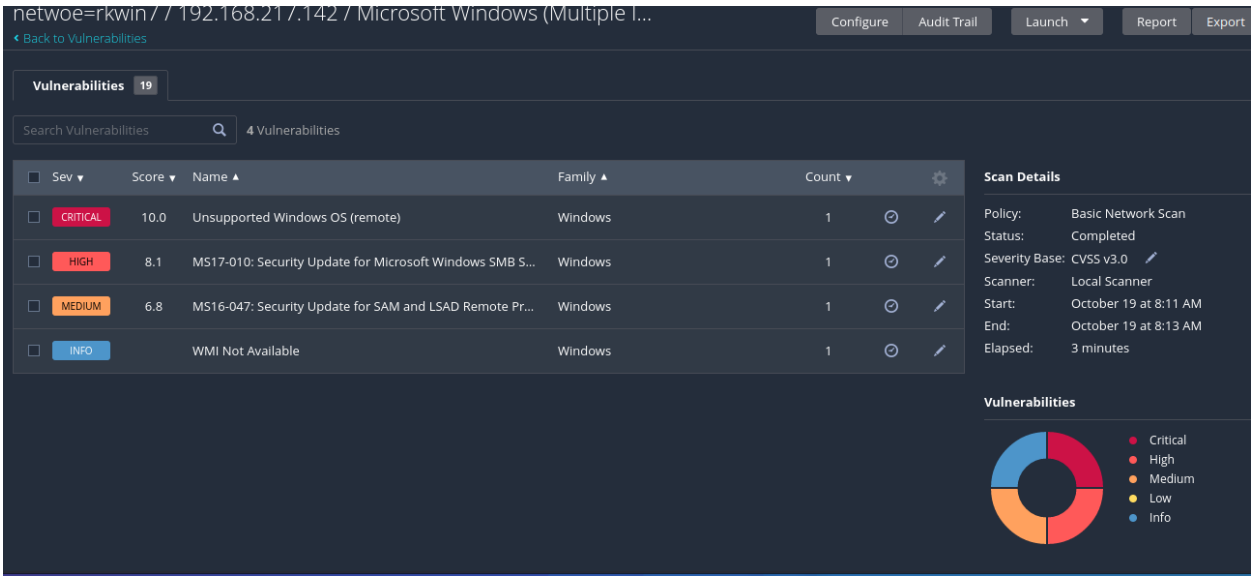
Bài 4 : Quét thông tin với nessus

Thực hiện quét thông tin window 7 với ip 192.168.217.142

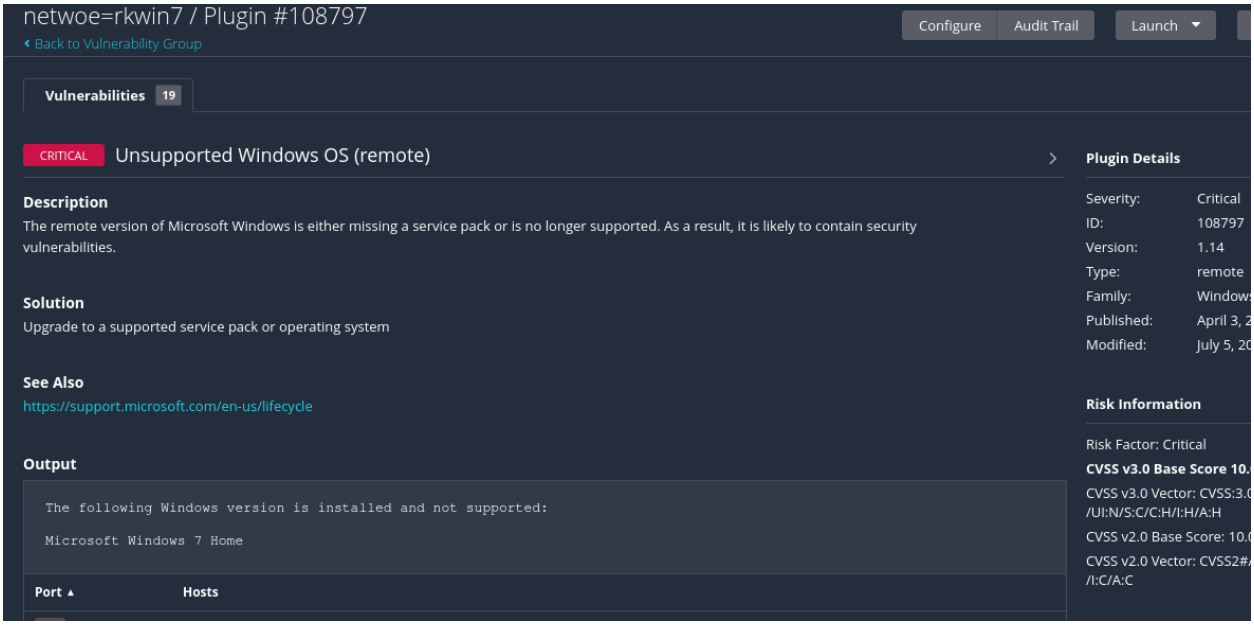
-Kết quả quét được có 34 lỗi thường, 2 lỗi medium , 1 lỗi high và 1 lỗi nguy hiểm



Chi tiết các lỗi



Nguyên nhân và cách khắc phục lỗi Critical :



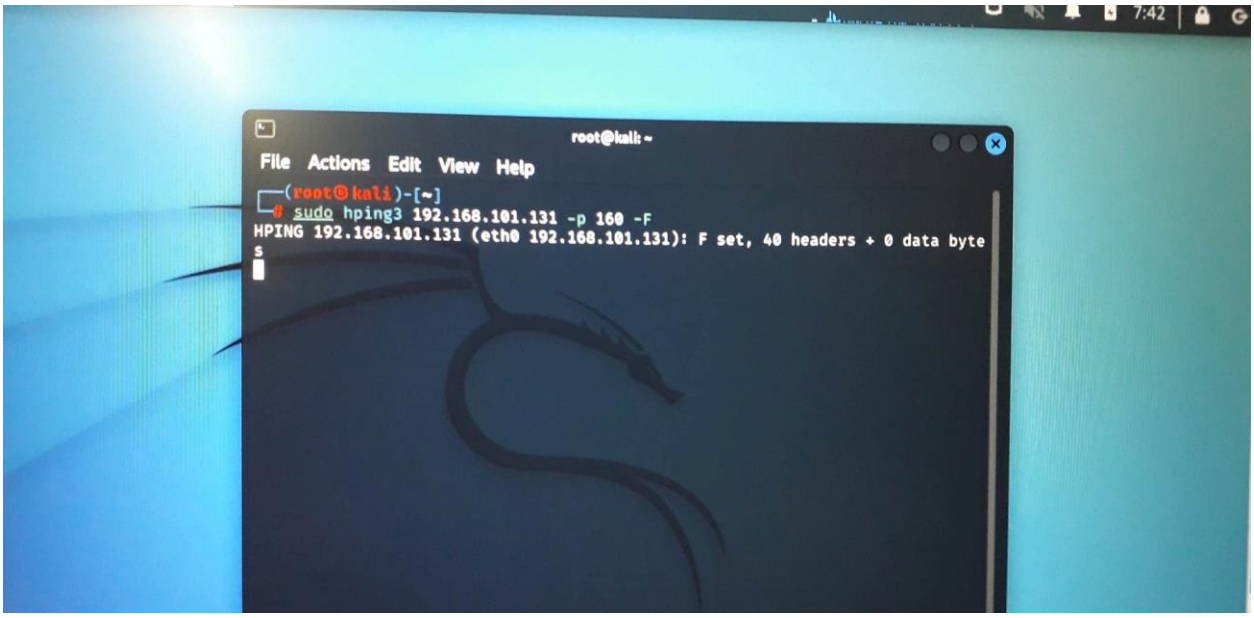
Nguyên nhân và cách khắc phục lỗi mức high :

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 .