

Bài tập thực hành 1

Task 1: Mở đầu về mạng máy tính

-Kể tên về các thiết bị liên quan đến Mạng mà bạn biết hoặc sử dụng.

+PC,Laptop,Smartphone,Tivi,Ipad,Router,....

-Những vấn đề gì có thể xảy ra nếu không có kết nối Internet trong 5 phút?

+Nếu mất mạng xảy ra trong 5 phút có thể xảy ra những hậu quả nghiêm trọng như chậm trễ các gói tin ảnh hưởng đến các Ngân Hàng xảy ra các vấn đề về chuyển khoản,dữ liệu người dùng,Phi Công không thể nhận các tín hiệu từ Trạm Không Lưu trên mặt đất để vận hành trong suốt quá trình bay, Người dùng thông thường sẽ không thể truy cập các trang Web mà họ mong muốn.

-Mục tiêu về kiến thức sau khi hoàn thành môn học Nhập môn Mạng máy tính của bạn?

+Hiểu được cách vận hành của hệ thống mạng,kiểm soát các hạ tầng mạng để vận hành 1 cách an toàn

+Hack Wifi

Task 2:

No.	Time	Source	Destination	Protocol	Length	Info
132	16.584389	192.168.223.60	192.168.223.255	NBNS	92	Name query NB QYSTGEFC<00>
133	16.585734	192.168.223.60	192.168.223.255	NBNS	92	Name query NB MPYFBGIZA<00>
134	16.642712	192.168.223.60	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
135	16.646461	fe80::d8a5:e865:ba8...ff02::fb		MDNS	102	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
136	16.804819	192.168.223.60	224.0.0.251	MDNS	75	Standard query 0x0000 A nzarvbiim.local, "QM" question
137	16.829296	fe80::d8a5:e865:ba8...ff02::fb		MDNS	95	Standard query 0x0000 A nzarvbiim.local, "QM" question
138	16.884340	192.168.223.60	224.0.0.251	MDNS	75	Standard query 0x0000 A mpyfbgiza.local, "QM" question
139	16.884569	fe80::d8a5:e865:ba8...ff02::fb		MDNS	95	Standard query 0x0000 A mpyfbgiza.local, "QM" question
140	17.202739	192.168.223.77	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
141	17.399465	192.168.223.60	192.168.223.255	NBNS	92	Name query NB MPYFBGIZA<00>
142	17.402767	192.168.223.60	192.168.223.255	NBNS	92	Name query NB QYSTGEFC<00>
143	17.404080	192.168.223.60	192.168.223.255	NBNS	92	Name query NB NZARVBIIM<00>
144	17.829361	192.168.223.60	224.0.0.251	MDNS	70	Standard query 0x0000 A wpad.local, "QM" question
145	17.839056	fe80::d8a5:e865:ba8...ff02::fb		MDNS	90	Standard query 0x0000 A wpad.local, "QM" question
146	17.857945	192.168.223.60	224.0.0.252	LLMNR	64	Standard query 0xb7b8 A wpad
147	17.910360	192.168.223.60	192.168.223.255	NBNS	92	Name query NB WPAD<00>
148	18.203815	192.168.223.56	49.213.114.108	TCP	55	60793 → 443 [ACK] Seq=1 Ack=1 Win=509 Len=1 [TCP segment of a reassembled PDU]
149	18.405917	49.213.114.108	192.168.223.56	TCP	66	443 → 60793 [ACK] Seq=1 Ack=2 Win=201 Len=0 SLE=1 SRE=2

Câu 1:

Tổng thời gian bắt trang Web: <http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html> là 18.405917s,tổng số gói tin bắt được là 149 gói.

Câu 2:

Các giao thức khác:

+TCP(Transmission Control Protocol): tạo cho các ứng dụng trên các máy chủ nối mạng"kết nối" với nhau và trao đổi dữ liệu trực tiếp

+UDP(User Datagram Protocol): Thứ tự truyền nhận không theo một thứ tự có thể gây mất mát gói tin mà mình không biết được nhưng khắc khe về thời gian yêu cầu phải truyền khoảng thời gian nhất định

+SSDP(Simple Service Discovery Protocol): cung cấp các thông tin cần thiết để tạo ra các kết nối giữa các thiết bị có kết nối mạng Internet.

+IGMPv2(Internet Group Mangement Protocol):Giao thức truyền thông được sử dụng bởi máy chủ và bộ định tuyến lân cận trên mạng IPv4,nó là một phần không thể thiếu của IP multicast

+DNS (Domain Name System):Hệ thống phân giải tên miền, biên dịch tên miền thành địa chỉ IP để có thể tự động đăng nhập

http						
Manage saved bookmarks	Source	Destination	Protocol	Length	Info	
100 15.222725	192.168.223.56	128.119.245.12	HTTP	519	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1	
106 15.502033	128.119.245.12	192.168.223.56	HTTP	492	HTTP/1.1 200 OK (text/html)	

Câu 3:

http						
No.	Time	Source	Destination	Protocol	Length	Info
100	15.222725	192.168.223.56	128.119.245.12	HTTP	519	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
106	15.502033	128.119.245.12	192.168.223.56	HTTP	492	HTTP/1.1 200 OK (text/html)

Arrival Time: Sep 30, 2020 14:26:27.745297000 SE Asia Standard Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1601450787.745297000 seconds
[Time delta from previous captured frame: 0.000153000 seconds]
[Time delta from previous displayed frame: 0.279308000 seconds]
[Time since reference or first frame: 15.502033000 seconds]
Frame Number: 106
Frame Length: 492 bytes (3936 bits)
Capture Length: 492 bytes (3936 bits)

[Time delta from previous displayed frame: 0.279308000 seconds]

[Time delta from previous displayed frame: 0.279308000 seconds]từ khi gói tin HTTP GET đầu tiên được gửi cho đến khi HTTP 200 OK đầu tiên được nhận với Website đã thử nghiệm :

<http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html>

Câu 4

Nội dung hiển thị trên trang web <http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html> bắt được gói "Congratulations!You've downloadled the first Wireshark lab file!" vì đó là object trả về sau khi ta đã request lên trên Server và giá trị Respond trả về là có chứa file HTML cả trên lúc đi và cả lúc về.

1	<html>					
2	Congratulations! You've downloaded the first Wireshark lab file!					
3	</html>					
4						
+	100 15.222725	192.168.223.56	128.119.245.12	HTTP	519 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1	
-	106 15.502033	128.119.245.12	192.168.223.56	HTTP	492 HTTP/1.1 200 OK (text/html)	

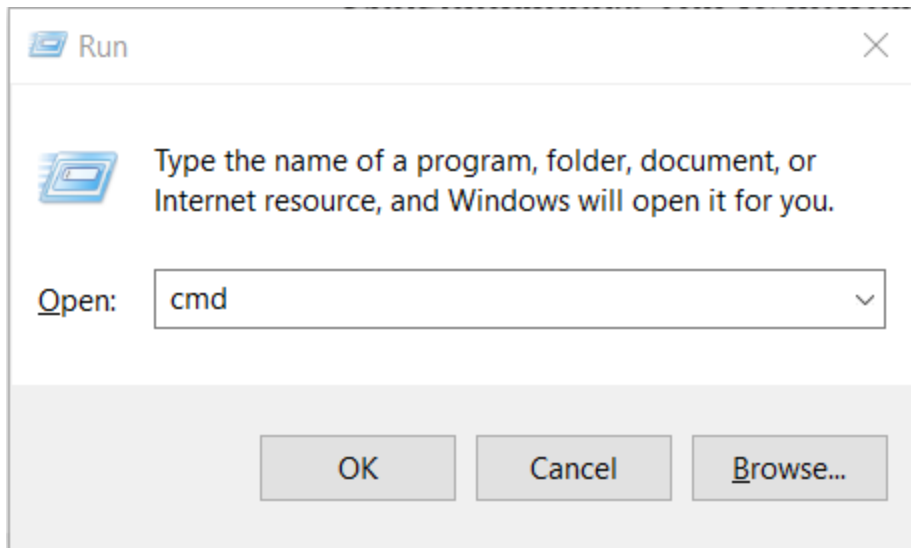
>	Ethernet II, Src: Dell_83:2f:3d (8c:ec:4b:83:2f:3d), Dst: WistronN_f3:c0:9c (00:1b:b1:f3:c0:9c)
>	Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.223.56
>	Transmission Control Protocol, Src Port: 80, Dst Port: 61136, Seq: 1, Ack: 466, Len: 438
>	Hypertext Transfer Protocol
√	Line-based text data: text/html (3 lines)
	<html>\n
	Congratulations! You've downloaded the first Wireshark lab file!\n
	</html>\n

Câu 5

Ta có thể xác định địa chỉ IP của bản thân bằng cách:

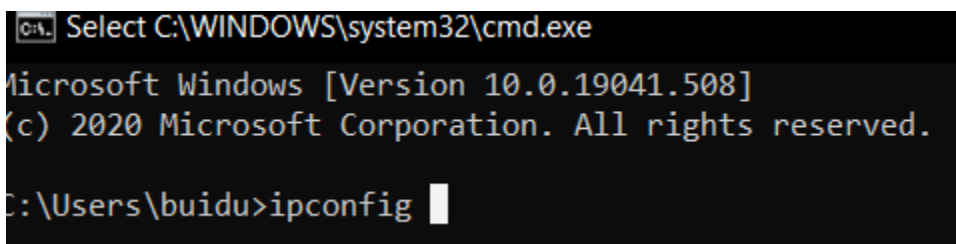
B1:chọn Window +R

B2:Gõ vào cmd trình cửa sổ Run



B3:Nhấn OK

B4:Gõ vào lệnh ipconfig rồi nhấn Enter



B5:Kéo xuống phần Wireless LAN adapter Wi-Fi nhìn vào phần IPv4 Address đó chính là IP địa chỉ của bạn cần tìm tùy theo lớp Wi-Fi mà bạn kết nối tại đâu và tại thời điểm nào nên địa chỉ IPv4 Address sẽ thay đổi.

Địa chỉ các IP khi thực hành trên WireShark :

444	11.237556	192.168.223.56	99.83.201.180	HTTP	577	GET /LCHS/Contents/ticketing/movie-schedule.aspx HTTP/1.1
524	11.684631	192.168.223.56	99.83.201.180	HTTP	673	GET /LCHS/CSS/reset.css?t=20180508001 HTTP/1.1
552	11.695235	192.168.223.56	99.83.201.180	HTTP	674	GET /LCHS/CSS/common.css?t=20181122001 HTTP/1.1
555	11.695367	192.168.223.56	99.83.201.180	HTTP	676	GET /LCHS/CSS/banner.css?t=2017007050001 HTTP/1.1
556	11.695575	192.168.223.56	99.83.201.180	HTTP	680	GET /LCHS/CSS/swiper.min.css?t=2017007050001 HTTP/1.1
566	11.698809	99.83.201.180	192.168.223.56	HTTP	284	HTTP/1.1 200 OK (text/html)

Trên đây là địa chỉ IP của mình khi nhận diện trên Wireshark là: 192.168.223.56

Và địa chỉ Ip của Web Lotte Cinema sau khi đã hoàn thành đến HTTP 200 OK là 99.83.201.180

http						
	Source	Destination	Protocol	Length	Info	
100	15.222725	192.168.223.56	HTTP	519	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1	
106	15.502033	128.119.245.12	HTTP	492	HTTP/1.1 200 OK (text/html)	

Trên đây là địa chỉ của trang Web <http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html> sau khi đã dẫn tới địa chỉ HTTP 200 OK là 128.119.245.12

Câu 6:

Khi bắt đầu đăng nhập vào một đường dẫn nào đến một trang Web thì các địa chỉ chạy từ protocol TCP sang các protocol khác để có thể xác định địa chỉ đó cần gửi request từ client nào đến Server nào mà nó muốn đến sau đó sẽ tiếp tục chạy tiếp Acknowledge rồi tiếp theo đến tầng ACK+HTTP Request cuối cùng thì sẽ trả về HTTP respond trong đó mang theo object để có thể tải nội dung mà trong đó trang Web đó có.

Mở Rộng:

Nguồn: <https://thuthuat.taimienphi.vn/cach-xem-ip-cua-web-bat-ky>

Có thể xem địa chỉ IP của máy tính và của một Website khác bằng nhiều cách:

-Xem IP của máy tính từ thanh taskbar, bằng Command Prompt

Nguồn : <https://quantrimang.com/huong-dan-cach-xac-dinh-dia-chi-ip-tren-may-tinh-88276>

-Xem IP của trang Web bằng 2 cách Command Prompt hoặc Xem IP của Bất Kỳ qua trang Web khác:

+Bước 1: vào trình duyệt Web và truy cập vào link : <https://www.hcidata.info/host2ip.cgi>

+Bước 2: nhập tên trang web cần xem IP vào mục **Host Name** rồi nhấn **Find IP Address**

Convert Host Name to IP Address or Vice Versa

Host Name	<input type="text" value="taimienphi.vn"/>	IP Address	<input type="text" value="127.0.0.1"/>
	<input type="button" value="Find IP Address"/>		<input type="button" value="Find Host Name"/>

The process of finding the IP address is achieved by searching the DNS (Domain Name Servers) also known as DNS lookup, NSLOOKUP or (erroneously) IP lookup

The process of finding the host name (or domain name) from an IP address involves sending a n at that IP address to return its name. Usually this will be the same as the domain name. However be one of the domain names hosted or it could be something totally different.

There are some special IP addresses. 127.0.0.1 is always the IP address of every computer. No address of 127.0.0.1 and a name of 'localhost'. In addition, a computer can have more than one have an IP address that is known to other computers.

+Bước 3: Nhấn **Find IP Address** để xem thông tin địa chỉ IP