ĐỒ ÁN THỰC HÀNH 1 – PHÂN TÍCH GÓI TIN

MÔN MẠNG MÁY TÍNH

Quy định:

- Bài tập nhóm
- Sinh viên dùng chương trình Wireshark và VMWare để làm bài
- Bài nộp có tên là dạng **MSSV1-MSSV2-MSSV3.**rar/zip. Gồm:
  a. File báo cáo ***MSSV1-MSSV2-MSSV3.pdf*** trả lời các câu hỏi và bắt buộc có hình chụp chứng minh (chú thích, đóng khung các thông tin quan trọng của hình chụp) ứng với từng câu trả lời. Khi chip hình phải chụp đầy đủ và có 1 phần Desktop Bacground
  b. File ***bai2.pcap***, ***bai3.pcap*** chứa thông tin gói tin bắt được tương ứng với từng bài
- Lưu ý: Sinh viên chỉ trình bày phần phân tích gói tin, không trình bày phần cấu hình các dịch vụ trong báo cáo
- Bài làm giống nhau hoặc nộp bài không đúng quy định: 0 điểm bài tập này

Đề bài:

Bài 1: Gói tin truy cập web

```
> Frame 38: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits) on interface 0
> Ethernet II, Src: IntelCor_8c:5e:ba (00:1c:c0:8c:5e:ba), Dst: Dell_e7:b3:9f (20:47:47:e7:b3:9f)
v Internet Protocol Version 4, Src: 216.58.199.99, Dst: 172.29.51.16
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 114
    Identification: 0x02cc (716)
  > Flags: 0x00
    Fragment offset: 0
    Time to live: 54
    Protocol: TCP (6)
    Header checksum: 0x02ef [validation disabled]
    [Header checksum status: Unverified]
    Source: 216.58.199.99
    Destination: 172.29.51.16
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
v Transmission Control Protocol, Src Port: 443, Dst Port: 54102, Seq: 47, Ack: 414, Len: 74
    Source Port: 443
    Destination Port: 54102
    [Stream index: 0]
    [TCP Segment Len: 74]
    Sequence number: 47    (relative sequence number)
    [Next sequence number: 121    (relative sequence number)]
    Acknowledgment number: 414    (relative ack number)
    Header Length: 20 bytes
  > Flags: 0x018 (PSH, ACK)
    Window size value: 398
    [Calculated window size: 398]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0x3e38 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > [SEQ/ACK analysis]
v Secure Sockets Layer
  > TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
```

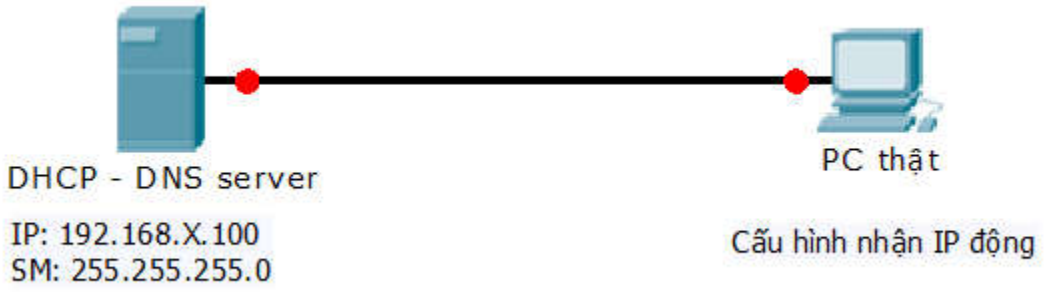
1. Cho biết địa chỉ IP nguồn, IP đích, MAC nguồn, MAC đích của gói tin trên?

2. Cho biết thông tin port nguồn, port đích của gói tin trên?
3. Gói tin trên sử dụng giao thức gì ở tầng Application?
4. Hãy cho biết giao thức sử dụng ở tầng transportation trong gói tin?

Bài 2: DHCP

Chuẩn bị:

- Thiết lập card mạng ảo là Host Only
- Thực hiện cài đặt dịch vụ DHCP theo mô hình:



  - Khoảng địa chỉ IP sẽ cấp (Address Pool): 192.168.X.10 – 192.168.X.90
  - Subnet Mask: 255.255.255.0
  - Khoảng địa chỉ IP để dành: 192.168.X.10 – 192.168.X.20
  - Gateway: 192.168.X.1
  - DNS Server: 192.168.X.100
- Cấu hình PC thật nhận IP động từ DHCP Server vừa cấu hình
- Thực hiện bắt gói tin trên card mạng VMNet 1 của máy thật
- Thực hiện xin cấp IP mới tại máy thật

Yêu cầu:

Phân tích các gói tin bắt được và trả lời câu hỏi

1. Liệt kê tên các gói tin DHCP bắt được trong quá trình xin cấp mới địa chỉ IP
2. Dịch vụ DHCP sử dụng port ở server và client là bao nhiêu?
3. Địa chỉ IP mà DHCP server đề nghị cấp cho client được gửi từ gói tin nào?
4. Hãy cho biết sự khác biệt giữa 2 trường thông tin: Your IP address và Client IP Address trong gói tin DHCP ACK.

Bài 3: DNS

Chuẩn bị:

- Dùng lại mô hình vừa thực hiện ở câu 2
- Cài đặt và cấu hình dịch vụ DNS như sau:
- Quản lý forward zone congtymmt.vn và reverse zone tương ứng
- Cấu hình record với các pointer (PTR) tương ứng:
  DNS Serever: dns.congtymmt.vn với địa chỉ IP 192.168.X.10
  Web Server: www.congtymmt.vnvới địa chỉ IP 192.168.X.11
- Thực hiên lệnh truy vấn DNS tại máy thật (nslookup) địa chỉ www.congtymmt.vn

Yêu cầu:

Phân tích các gói tin bắt được và trả lời câu hỏi

1. Có bao nhiêu gói tin được truyền và nhận trong quá trình truy vấn?
2. DNS sử dụng port ở server và client là bao nhiêu?
3. Giao thức sử dụng ở tầng transportation của gói tin DNS responses
4. Cho biết thông tin Name Server quản lý zone congtymmt.vn

Biết X là 2 chữ số cuối của Mã số sinh viên một bạn bất kì trong nhóm

——HẾT——