**ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH  
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN  
Khoa Mạng máy tính và Truyền thông**

**🙢 🕮 🙠**

**Bài Tập Nhóm**

**Môn:**

**AN TOÀN MẠNG MÁY TÍNH**

**Giáo viên hướng dẫn: Tô Nguyễn Nhật Quang**

**Nhóm sinh viên thực hiện :**

***Trần Hữu Tiến 13521072***

***Nguyễn Đặng Thắng***

***Ngô Tuấn Cường***

**Thành phố Hồ Chí Minh - tháng 5/2015**

# Lời cảm ơn

Trên thực tế không có sự thành công nào mà không gắn liền với những sự hỗ trợ, giúp đỡ dù ít hay nhiều, dù trực tiếp hay gián tiếp của người khác. Trong suốt thời gian từ khi bắt đầu học tập ở giảng đường đại học đến nay, em đã nhận được rất nhiều sự quan tâm, giúp đỡ của quý Thầy Cô, gia đình và bạn bè.

Với lòng biết ơn sâu sắc nhất, em xin gửi đến quý Thầy Cô ở Khoa Khoa Mạng Máy Tính và Truyền Thông – Trường Đại Học Công Nghệ Thông Tin đã cùng với tri thức và tâm huyết của mình để truyền đạt vốn kiến thức quý báu cho chúng em trong suốt thời gian học tập tại trường. Và đặc biệt, trong học kỳ này, Khoa đã tổ chức cho chúng em được tiếp cận với môn học mà theo em là rất hữu ích đối với sinh viên ngành Mạng Máy Tính cũng như tất cả các sinh viên thuộc các chuyên ngành Khoa Mạng Máy Tính và Truyền Thông khác. Đó là môn học “An Toàn Mạng Máy Tính”.

Em xin chân thành cảm ơn đã tận tâm Tô Nguyễn Nhật Quang đã hướng dẫn chúng em qua từng buổi học trên lớp cũng như những buổi nói chuyện, thảo luận về lĩnh vực sáng tạo trong nghiên cứu khoa học. Nếu không có những lời hướng dẫn, dạy bảo của thầy thì em nghĩ bài thu hoạchnày của em rất khó có thể hoàn thiện được. Một lần nữa, em xin chân thành cảm ơn thầy.

Bài thu hoạch được thực hiện trong khoảng thời gian gần 8 tuần. Bước đầu đi vào thực tế, tìm hiểu về lĩnh vực sáng tạo trong nghiên cứu khoa học, kiến thức của em còn hạn chế và còn nhiều bỡ ngỡ. Do vậy, không tránh khỏi những thiếu sót là điều chắc chắn, em rất mong nhận được những ý kiến đóng góp quý báu của quý Thầy Cô và các bạn học cùng lớp để kiến thức của em trong lĩnh vực này được hoàn thiện hơn.

MỤC LỤC

[Lời cảm ơn 1](#_Toc436958848)

[1 Hợp Đồng Nhóm 5](#_Toc436958849)

[1.1 Thành viên 5](#_Toc436958850)

[1.2 Mục tiêu đề ra 5](#_Toc436958851)

[1.3 Quy tắc 5](#_Toc436958852)

[1.4 Bảng phân công công việc 6](#_Toc436958853)

[1.5 Đánh giá 7](#_Toc436958854)

[1.6 Cam kết 7](#_Toc436958855)

[Dựa trên hợp đồng nhóm đã đưa ra, chúng tôi cam kết sẽ hoàn thành đúng yêu cầu trên. 7](#_Toc436958856)

[Hồ Chí Minh, Ngày…Tháng…Năm… 7](#_Toc436958857)

[Thành viên 1 Thành viên 2 Thành viên 3 Thành viên 4 7](#_Toc436958858)

[( kí tên ) ( kí tên ) ( kí tên ) ( kí tên ) 7](#_Toc436958859)

[2 Chương 1 8](#_Toc436958860)

[2.1 Firewall 8](#_Toc436958861)

[**2.1.1** **Khái niệm** 8](#_Toc436958862)

[**2.1.2** **Lịch sử** 8](#_Toc436958863)

[**2.1.3** **Lý do sử dụng Firewall** 9](#_Toc436958864)

[**2.1.4** **Các loại Fireware** 9](#_Toc436958865)

[**2.1.5** **Nhiệm vụ.** 10](#_Toc436958866)

[**2.1.6** **Chức năng chính của Firewall** 10](#_Toc436958867)

[**2.1.7** **Firewall bảo vệ và chống lại cái gì?** 10](#_Toc436958868)

[**2.1.8** **Các thành phần cơ bản của Firewall và cơ chế hoạt động** 11](#_Toc436958869)

[**2.1.9** **Thuận lợi và hạn chế của Firewall** 13](#_Toc436958870)

[**2.1.10** **Kết luận** 14](#_Toc436958871)

[2.2 Các thuật toán mã hóa 15](#_Toc436958872)

[**2.2.1** **Phương thức mã hóa RSA** 15](#_Toc436958873)

[Là phương thức mã hóa công khai. Do Ron Rivest, Adi Shamir và Len Adleman tại học viên MIT đề xuất năm 1977. Và hiện nay đang được sử dụng rộng rãi. 15](#_Toc436958874)

[**2.2.2** **Phương thức mã hóa DES** 17](#_Toc436958875)

[**2.2.3** **Thuật toán mã hóa AES** 19](#_Toc436958876)

[2.3 VNP (virtual private network) 21](#_Toc436958877)

[**2.3.1** **Đặt vấn đề** 21](#_Toc436958878)

[**2.3.2** **VPN giới thiệu** 21](#_Toc436958879)

[**2.3.3** **Tính bảo mật của VNP** 23](#_Toc436958880)

[**2.3.4** **Các kĩ thuật sử dụng trong VNP** 24](#_Toc436958881)

[**2.3.5** **Kết luận** 25](#_Toc436958882)

[3 Một số phương pháp tấn công và cách phòng tránh 25](#_Toc436958883)

[3.1 Sniff (Nghe lén) 25](#_Toc436958884)

[**3.1.1** **Khái niệm** 25](#_Toc436958885)

[**3.1.2** **Sơ lược về cách tấn công** 26](#_Toc436958886)

[**3.1.3** **Các loại sniff và cơ chế hoạt động** 26](#_Toc436958887)

[**3.1.4** **Cách phát hiện và phòng chống** 27](#_Toc436958888)

[**3.1.5** **Mức độ ảnh hưởng đến hệ thống** 29](#_Toc436958889)

[3.2 Phishing 29](#_Toc436958890)

[**3.2.1** **Khái niệm** 29](#_Toc436958891)

[**3.2.2** **Thời gian xuất hiện** 29](#_Toc436958892)

[**3.2.3** **Sơ lược cách tấn công** 30](#_Toc436958893)

[**3.2.4** **Cách phòng chống** 30](#_Toc436958894)

[**3.2.5** **Mức độ ảnh hưởng** 31](#_Toc436958895)

[3.3 SQL Injection 32](#_Toc436958896)

[**3.3.1** **Khái niệm** 32](#_Toc436958897)

[**3.3.2** **Thời gian xuất hiện.** 32](#_Toc436958898)

[**3.3.3** **Cách thức tấn công** 32](#_Toc436958899)

[**3.3.4** **Kỹ thuật an ninh dùng để phòng chống SQL Injection** 36](#_Toc436958900)

[**3.3.5** **Mức độ ảnh hưởng** 37](#_Toc436958901)

[3.4 Tấn công từ chối dịch vị (DDoS) 38](#_Toc436958902)

[**3.4.1** **Khái niệm** 38](#_Toc436958903)

[**3.4.2** **Thời gian xuất hiện** 38](#_Toc436958904)

[**3.4.3** **Các cách tấn công** 38](#_Toc436958905)

[**3.4.4** **Cách thức phòng chống:** 41](#_Toc436958906)

[**3.4.5** **Mức độ ảnh hưởng:** 41](#_Toc436958907)

**LỜI NÓI ĐẦU**

Sự phát triển của mạng máy tính trong thập niên vừa qua rất nhanh chóng, từ những nhóm người dùng chung một mạng để chia sẽ tập tin, trao đổi thông tin một cách dễ dàng hơn cho đến những hệ thống mạng của một doanh nghiệp hay một tập đoàn lớn nhằm tăng hiệu quả về thời gian và kinh tế, tất cả đều nhờ đến mạng máy tính. Chính vì sự phổ biến và quan trọng đó đã có không ít kẻ xấu nhằm lợi dụng lỗ hổng bảo mật của các hệ thống mạng máy tính đó để nhằm xâm nhập hệ thống với quyền quản trị để lấy đi những thông tin quan trọng nhằm mục đích xấu. Đã có nhiều cách tấn công vào mạng, hệ thống khác nhau, được ra đời ở nhiều nơi trên thế giới, những cuộc tấn công như vậy thường gây thiệt hại về mặt kinh tế rất lớn, và tất nhiên những chuyên gia về mạng hệ thống củng đã tìm được những cách khắc phục để hạn chế tối đa tổn thất đó. Trên thực tế đó, hôm nay, nhóm chúng tôi xin trình bày những bài tập của giáo viên bộ môn đưa ra và dần dần áp dụng vào thực tế. Trong đề tài mà chúng tôi thự hiện vẫn còn một số thiếu sót mong mọi người bỏ qua cho. Xin cảm ơn!

# Hợp Đồng Nhóm

## Thành viên

|  |  |
| --- | --- |
| **Họ và Tên** | **MSSV** |
| Trần Hữu Tiến | 13521072 |
| Nguyễn Đặng Thắng |  |
| Ngô Tuấn Cường |  |

## Mục tiêu đề ra

* Hoàn thành tốt những bài tập được thầy giao.
* Giúp đỡ nhau trong công việc.
* Rèn luyện khả năng làm việc nhóm.
* Hoàn thành học phần một cách xuất sắc nhất.
* Chia sẻ những kinh nghiệm quý giá trong quá trình tìm hiểu của mình cho các bạn trong nhóm.

## Quy tắc

* Làm việc trên cơ sở đồng thuận về ý kiến quan điểm chung.
* Tôn trọng ý kiến cá nhân của các thành viên nếu nó vẫn đảm bảo yêu cầu của công việc.
* Hoàn thành công việc đúng thời hạn.
* Giúp đỡ lẫn nhau khi có khó khăn.
* Ai không hoàn thành thì sẽ phải chịu trách nhiệm về công việc của mình.

## Bảng phân công công việc

|  |  |  |  |
| --- | --- | --- | --- |
| **Mã số sinh viên** | **Thành viên** | **Vai trò** | **Công việc** |
| 13521072 | Trần Hữu Tiến | Member | * Giới thiệu một số phương pháp tấn công và cách phòng tránh. * Thiết kế đồ án. * Đăng kí và nộp đồ án. |
|  | Nguyễn Đặng Thắng | Member |  |
|  | Ngô Tuấn Cường | Member |  |

## Đánh giá

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **MSSV** | **Họ Tên** | **Tỷ lệ công việc được giao (%)** | **Tỷ lệ công việc hoàn thành (%)** | **Nhận xét**  **Trọng số điểm** |
| 13521072 | Trần Hữu Tiến | 33% | 95% | Tích cực trong công việc, hoành thành đúng thời hạn. 4.5 điểm |
|  | Nguyễn Đặng Thắng | 33% |  |  |
|  | Ngô Tuấn Cường | 33% |  |  |

Bài 1: TỔng quan về an ninh mạng

## Câu 1

### Mô tả cấu trúc của một gói tin TCP và giải thích các chức năng của TCP header.

**Một gói tin TCP gồm 2 phần:**

* Header.
* Dữ liệu.

Chức năng của TCP header:

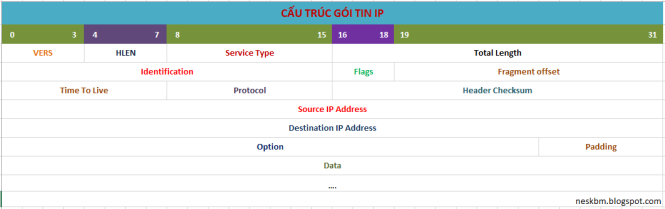
* **Cấu trúc:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **+** | **Bít 0 – 3** | **4 – 9** | **10 - 15** | **16 - 31** |
| **0** | Source Port | | | Destination Port |
| **32** | Sequence Number | | | |
| **64** | Acknowledgement Number | | | |
| **96** | Data Offset | Reserved | Flags | Window |
| **128** | Checksum | | | Urgent Pointer |
| **160** | Options (optional) | | | |
| **160/192+** | Data | | | |

* **Giải thích:**
  + **Source port:** Số hiệu của cổng tại máy tính gửi.
  + **Destination port:** Số hiệu của cổng tại máy tính nhận.
  + **Sequence number:** Trường này có 2 nhiệm vụ. Nếu cờ SYN bật thì nó là số thứ tự gói ban đầu và byte đầu tiên được gửi có số thứ tự này cộng thêm 1. Nếu không có cờ SYN thì đây là số thứ tự của byte đầu tiên.
  + **Acknowledgement number:** Nếu cờ ACK bật thì giá trị của trường chính là số thứ tự gói tin tiếp theo mà bên nhận cần.
  + **Data offset:** Trường có độ dài 4 bít quy định độ dài của phần header (tính theo đơn vị từ 32 bít). Phần header có độ dài tối thiểu là 5 từ (160 bit) và tối đa là 15 từ (480 bít).
  + **Reserved:** Dành cho tương lai và có giá trị là 0.
  + **Flags (hay Control bits):** Bao gồm 6 cờ:
    - **URG:** Cờ cho trường Urgent pointer.
    - **ACK:** Cờ cho trường Acknowledgement.
    - **PSH:** Hàm Push.
    - **RST:** Thiết lập lại đường truyền.
    - **SYN:** Đồng bộ lại số thứ tự.
    - **FIN:** Không gửi thêm số liệu.
* **Window:** Số byte có thể nhận bắt đầu từ giá trị của trường báo nhận (ACK).
* **Checksum:** 16 bít kiểm tra cho cả phần header và dữ liệu. Phương pháp sử dụng được mô tả trong [RFC 793](http://tools.ietf.org/html/793).
* **Urgent pointer:** Nếu cờ URG bật thì giá trị trường này chính là số từ 16 bít mà số thứ tự gói tin (*sequence number*) cần dịch trái.

### Mô tả cấu trúc của một gói tin IP và giải thích chức năng của IP header

Cấu trúc:



Giải thích:

**VERS**(4 bit): chỉ ra phiên bản hiện hành của IP đang được dùng, có 4 bit. Nếu trường này khác với phiên bản IP của thiết bị nhận, thiết bị nhận sẽ từ chối và loại bỏ các gói tin này.

**HLEN**(**4** bit):  chỉ độ dài phần tiêu đề (Internet Header Length) của datagram, tính theo đơn vị word (**32**bits). Nếu không có trường này thì độ dài mặc định của phần tiêu đề là 5 từ.

**Service Type** (**8**bits): cho biết các thông tin về loại dịch vụ và mức ưu tiên của gói IP, có dạng cụ thể như sau:

[https://kysudien.files.wordpress.com/2014/12/6c50f-untitled.png?w=400&h=32](https://kysudien.files.wordpress.com/2014/12/6c50f-untitled.png)

**Precedence**(**3**bits): chỉ thị về quyền ưu tiên gửi datagram, cụ thể là:

* 111 Network Control (cao nhất).
* 011- flash.
* 110 Internetwork Control.
* 010 Immediate
* 101 CRITIC/ECP.
* 001 Priority.
* 100 Flas Override.
* 000 Routine (thấp nhất).

**D**(delay)  (1 bit) : chỉ độ trễ yêu cầu

* D = 0 độ trễ bình thường.
* D = 1 độ trễ thấp.

**T**(Throughput) (1 bit) : chỉ số thông lượng yêu cầu

* T = 1 thông l ượng bình thường.
* T = 1 thông l ượng cao.

**R**(Reliability) (1 bit): chỉ độ tin cậy yêu cầu

* R = 0 độ tin cậy bình thường.
* R = 1 độ tin cậy cao.

**Total Length** (**16**bits): chỉ độ dài toàn bộ datagram, kể cả phần header (tính theo đơn vị bytes), vùng dữ liệu của datagram có thể dài tới 65535 bytes. Để biết chiều dài của dữ liệu chỉ cần lấy tổng chiều dài này trừ đi HLEN.

**Identification**(**16**bit):  cùng với các tham số khác như (Source Address và Destination Address) tham số này dùng để định danh duy nhất cho một datagram trong khoảng thời gian nó vẫn còn trên liên mạng. Đây là 1 số nguyên.

**Flags**(**3**bits): Liên quan đến sự phân đoạn (Fragment) của datagram. cụ thể:

**0        DF         MF**

**Bit 0**: reserved chưa sử dụng luôn lấy giá trị 0

**Bit 1**:

DF = 1: Gói tin bị phân đoạn, có nhiều hơn 1 đoạn

DF = 0: Gói tin ko bị phân đoạn.

**Bit 2**:

MF = 0: Đây là đoạn cuối cùng

MF = 1: Đây chưa phải là đoạn cuối cùng, còn đoạn khác phía sau nữa

**Fragment Offset**(**13**bits):  chỉ vị trí của đoạn (fragment) ở trong datagram, tính theo đơn vị 64 bits, có nghĩa là mỗi đoạn (trừ đoạn cuối cùng) phải chứa một vùng dữ liệu có độ dài là bội của 64 bits. Nó được dùng để ghép các mảnh Datagram lai với nhau

**Time To Live** (**TTL**– **8**bit): giá trị này được đặt lúc bắt đầu gửi gói tin. Và nó sẽ giảm dần khi đi qua 1 router. gói tin sẽ bị hủy nếu giá trị này = 0 khi chưa đến đích. Việc làm này nhằm giải quyết vấn đề gói tin bị lặp vô hạn trên mạng.

**Protocol** (**8**bits): Chỉ ra giao thức lớp trên, chẳng hạn như TCP hay UDP

**Header Checksum**:  mã kiểm soát lỗi sử dụng phương pháp CRC (Cyclic Redundancy Check) dùng để đảm bảo thông tin về gói dữ liệu được truyền đi một cách chính xác (mặc dù dữ liệu có thể bị lỗi). Nếu như việc kiểm tra này thất bại, gói dữ liệu sẽ bị huỷ bỏ tại nơi xác định được lỗi. Cần chú ý là IP không cung cấp một phương tiện truyền tin cậy bởi nó không cung cấp cho ta một cơ chế để xác nhận dữ liệu truyền tại điểm nhận hoặc tại những điểm trung gian. Giao thức IP không có cơ chế Error Control cho dữ liệu truyền đi, không có cơ chế  kiểm soát luồng dữ liệu (flow control).

**Source Address** (**32**bits): địa chỉ của trạm nguồn.

**Destination Address** (**32**bits): địa chỉ của trạm đích.

**Option**(**có độ dài thay đổi**) sử dụng trong một số trường hợp, nhưng thực tế chúng rất ít dùng. Option bao gồm bảo mật, chức năng định tuyến đặc biệt

**Padding**(**độ dài thay đổi**): Các số 0 được bổ sung vào field này để đảm bảo IP Header luôn la bội số của 32 bit.

**Data**(**độ dài thay đổi**): vùng dữ liệu có độ dài là bội của 8 bits, tối đa là 65535 bytes.