Основи безпеки інформації в комп'ютерних мережах

Виконав: студент групи СН-41
Сікач Б.Я.

Комп'ютерна, або обчислювальна, мережа – це сукупність комп'ютерів, пов'язаних між собою лініями зв'язку, які утворюються за допомогою кабелів і комунікаційних пристроїв.

Характеристики:

- **Топологія (фізична, логічна)**
- **Принцип з’єднання абонентів**
  - **Комутація каналів**
  - **Комутація пакетів**

Система з відкритою архітектурою (відкрита система) – це система, що здатна взаємодіяти з іншою системою за допомогою реалізації міжнародних стандартних протоколів. За сприяння Міжнародної організації зі стандартів в 1978р. було розроблено модель взаємодії відкритих систем OSI (Open Systems Interconnection).

Рівень OSI-моделі	Функції	Рівень протоколу	Реалізація
7. Прикладний	Доступ до мережних служб	Протокол верхнього рівня	Програмна
6. Представлення	Представлення і кодування даних		
5. Сеансовий	Керування сеансом зв'язку	Протокол середнього рівня	
4. Транспортний	Безпечне та надійне з'єднання між кінцевими пунктами		
3. Мережевий	Визначення маршруту та логічна адресація		
2. Канальний	Фізична адресація	Протокол нижнього рівня	Апаратна
1. Фізичний	Робота з середовищем передачі, сигналами та двійковими даними		

Сукупність протоколів, які забезпечують взаємодію двох систем і передачу повідомлень між ними, утворює *стек протоколів.*

Стеки мережних протоколів, які використовують найчастіше, їх порівняння із рівнями еталонної моделі OSI.

Рівні моделі OSI	IBM/ Microsoft	TCP/IP		Novell	Стек OSI
Прикладний	SMB	Telnet,FTP, SMTP, NNTP, HTTP, SNMP			X.400, X.500, VTP, FTAM
Представницький				NCP, SAP	Протокол подання OSI
Сеансовий	NetBIOS	TCP			Сеансовий протокол OSI
Транспортний			UDP	SPX	Транспортний протокол OSI
Мережний	—	IP, ICMP, RIP, OSPF		IPX, RIP, NLSP	IS-IS
Канальний	Ethernet (802.3), Token Ring (802.5), FDDI, SLIP, PPP, X.25, ATM, LAP-B, LAP-D				
Фізичний					

Віддалена атака – атака на розподілену обчислювальну систему, що здійснюють програмні засоби каналами зв'язку. Така атака може бути здійснена на протоколи і мережні служби, а також на операційні системи та прикладні програми вузлів мережі.

Типові віддалені атаки:

- угадування паролів, або атаки за словником;
- реєстрація та маніпуляції з мережним трафіком;
- імпорт фальшивих пакетів даних;
- підміна довіреного об'єкта в розподіленій системі;
- упровадження в розподілену систему фальшивого об'єкта через нав'язування фальшивого маршруту;
- відмова в обслуговуванні.

Базовими документами у сфері захисту розподілених систем є технічно узгоджені документи ISO/IEC 7498-2 і Рекомендації CCITT (The International Telegraph and Telephone Consultative Committee) X.800 «Архітектура безпеки взаємодії відкритих систем для застосувань CCITT».

У рекомендаціях X.800 увагу закцентовано на таких функціях (сервісах) безпеки:

- **автентифікація;**
- **керування доступом;**
- **конфіденційність даних;**
- **цілісність даних;**
- **унеможливлення відмови від авторства.**

Реалізувати сервіси безпеки можна, впровадивши на певному рівні моделі OSI такі механізми:

- ***шифрування;***
- ***цифровий підпис;***
- ***керування доступом;***
- ***контроль цілісності даних;***
- ***автентифікаційний обмін;***
- ***заповнення трафіку;***
- ***керування маршрутом;***
- ***нотаризація***

Рекомендації X.800 визначають також універсальні (Pervasive) механізми безпеки. До них належать:

- ***довірена функціональність;***
- ***мітки безпеки;***
- ***детектування подій;***
- ***аудит безпеки;***
- ***відновлення безпеки***

Керування безпекою взаємодії відкритих систем здійснюють шляхом:

- **адміністрування системи у цілому;**
- **адміністрування сервісів безпеки;**
- **адміністрування механізмів безпеки.**

Адміністрування системи в цілому здійснюється шляхом:

- загального керування політикою безпеки, зокрема через підтримку її актуальності;
- взаємодії з іншими функціями керування безпекою взаємодії відкритих систем;
- взаємодії з функціями адміністрування сервісів безпеки та функціями адміністрування механізмів безпеки;
- керування реагуванням на події;
- керування аудитом безпеки;
- керування відновленням безпеки.

ІСТОРІЯ ЗЛОМУ МЕРЕЖ ПЕНТАГОНУ

2002 р. - британський хакер Гаррі Маккіннон зламав комп'ютерні мережі Пентагону та НАСА (збитки 800 млн. доларів).

2002 р. - мережі Пентагону зламав 17-річний австрійський хакер Маркус Хірш.

2006 р. - румунський хакер Едуарда Лусіан Мандру зламав мережі Пентагону, використовуючи для організації атак японські сервера (вартість отриманих секретних документів $35 000).

2008 р. - найбільший кібернапад на військові комп'ютери США. Почався з того, що в ноутбук на одній з близькосхідних баз була вставлена флешка з шкідливим програмним забезпеченням.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Андрончик А.Н. Защита информации в компьютерных сетях. - Екатеринбург: УГТУ-УПИ, 2008. – 248с.
2. Гайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009. – 608с.
3. http://ru.wikipedia.org/wiki/OSI_model Сетевая модель OSI.
4. http://www.lenta.ru/articles/2005/06/09/hacker/ Самый масштабный взлом Пентагона, или Сетевые кошки-мышки.