Курс: Безопасность в сети

Урок 1

Основы построения компьютерных сетей

СКАЧАНО С WWW.SHAREWOOD.BIZ - ПРИСОЕДИНЯЙСЯ!

Вся рассматриваемая в данном курсе информация, в том числе по инструментам предназначенным для проведения различных видов атак, предназначена исключительно в образовательных целях, чтобы понять как могут применяться приводимые техники хакерами и как от них защититься.

Немного вводной информации

- Длительность урока ~ 2 ч.
- Уровень подготовки: для новичков
- Видеозапись будет
- Разбор вопросов по ходу урока. Требующие развернутого ответа в конце занятия.

Что будем изучать в курсе?

Урок 1. Основы построения компьютерных сетей

Урок 2. Введение в анализ сетевого трафика (Wireshark, TCPDump)

Урок 3. Пассивные сетевые атаки (NMap)

Урок 4. Активные сетевые атаки. Часть 1 (MITM атаки: ARP Spoof, DNS Spoof, DHCP Spoof)

Урок 5. Активные сетевые атаки. Часть 2 (MITM атаки: ARP Spoof, DNS Spoof, DHCP Spoof)

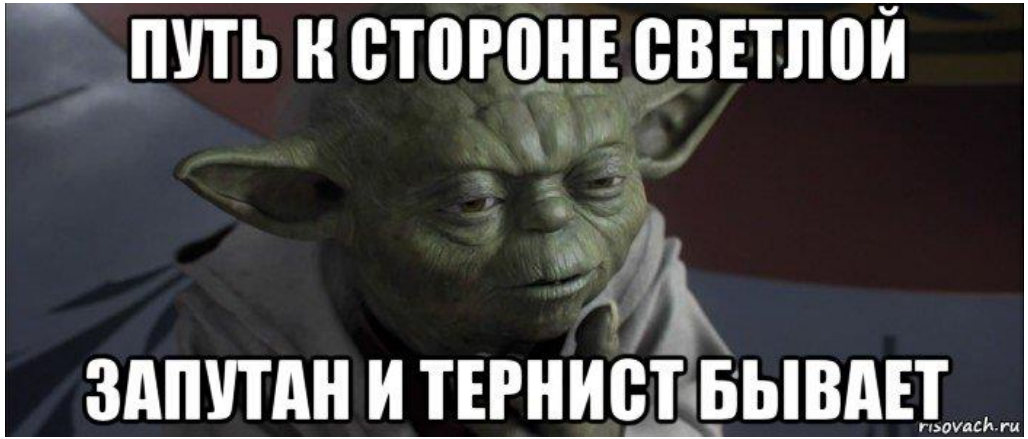
Урок 6. Аудит безопасности беспроводных сетей (WEP/WPA-WPA2 and etc.)

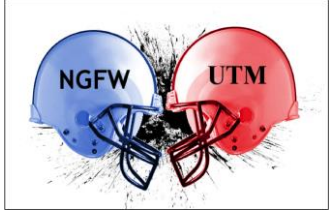
Урок 7. Аудит безопасности типовых сетевых сервисов (Metasploit)

Урок 8. Безопасность Web-приложений (Injection, BeEF, Burp and etc.)

Каких результатов мы добьемся?

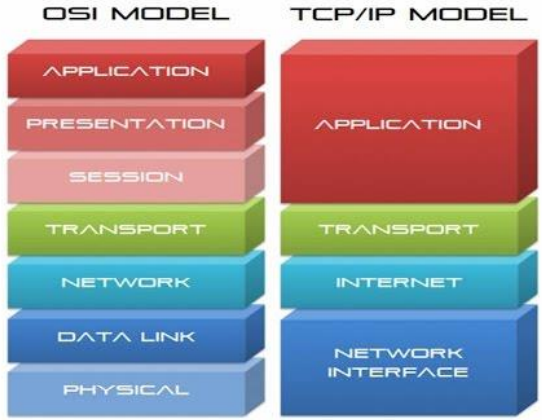
Само собой у каждого действия должна быть конечная цель, то ради чего все начиналось! Наша цель встать на путь изучения ***сетевой безопасности***, как одной из неотъемлемых частей направления ***информационной безопасности***.

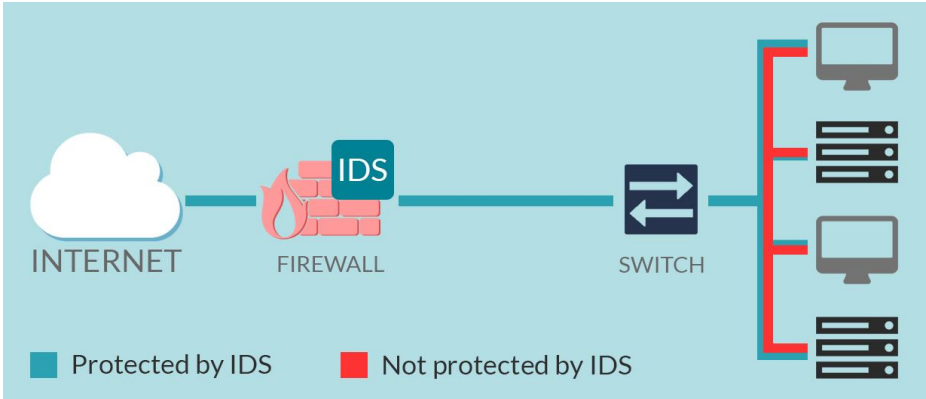




В уроке

- Сетевая Модель ISO/OSI
- Протокол IP
- Протокол TCP
- Протокол UDP
- Чем защитить сеть?





Цель: дать представление о вопросах, связанных с проблемами распределенной обработкой информации и современных методах построения вычислительных сетей.

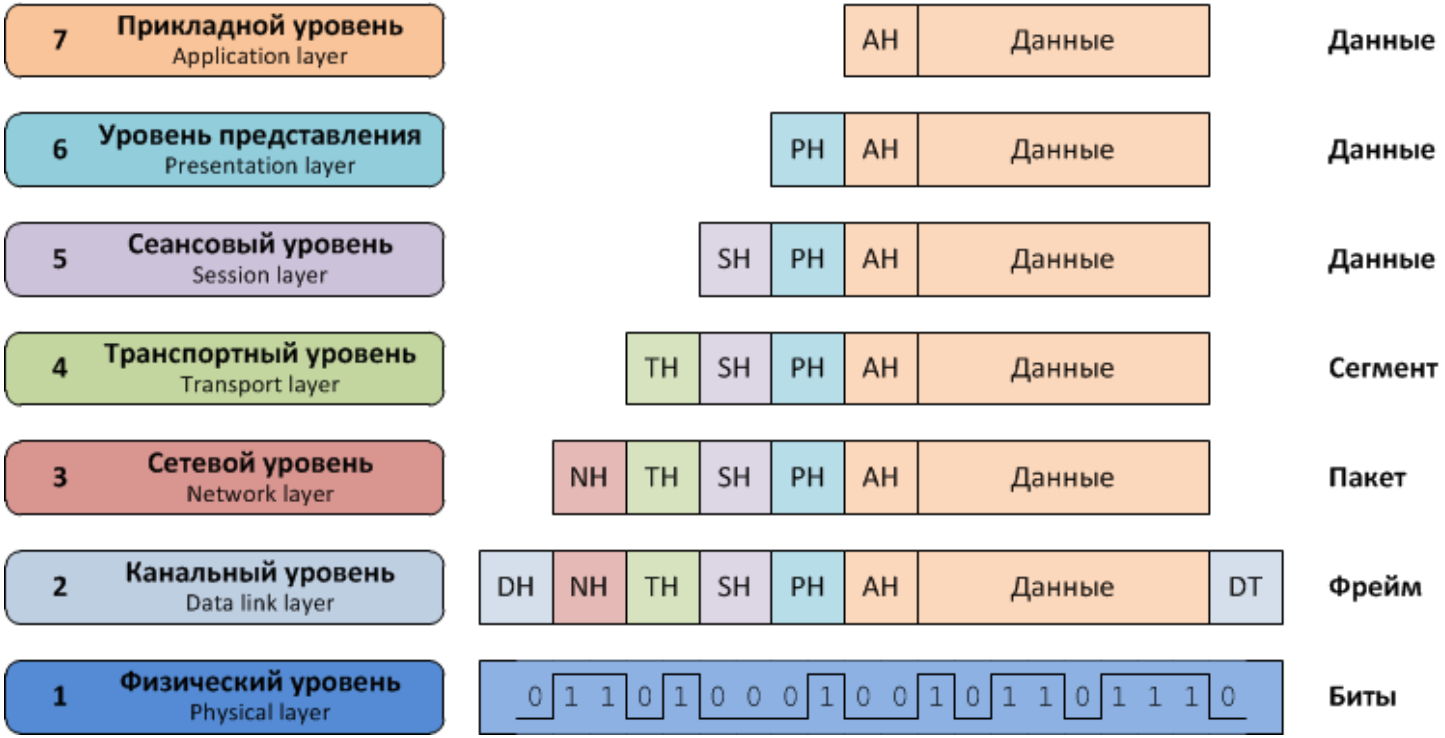
Ключевые слова: распределенная обработка данных, модель *ISO/OSI*, стек протоколов *TCP/IP*, маршрутизация в сетях *TCP/IP*, стандарты и протоколы Интернет.

Протокол - набор правил и соглашений для передачи и приема сообщений между уровнями.

Работу сети обеспечивает множество различных протоколов: например, протоколы управления физической связью, установления связи по сети, доступа к различным ресурсам и т.д.

Модель ISO/OSI

В модели OSI взаимодействие делится на 7 уровней или слоев



	OSI Layer	TCP/IP	Datagrams are called
Software	**Layer 7** Application	HTTP, SMTP, IMAP, SNMP, POP3, FTP	**Upper Layer Data**
	Layer 6 Presentation	ASCII Characters, MPEG, SSL, TSL, Compression (Encryption & Decryption)	
	Layer 5 Session	NetBIOS, SAP, Handshaking connection	
	Layer 4 Transport	TCP, UDP	**Segment**
	Layer 3 Network	IPv4, IPv6, ICMP, IPSec, MPLS, ARP	**Packet**
Hardware	**Layer 2** Data Link	Ethernet, 802.1x, PPP, ATM, Fiber Channel, MPLS, FDDI, MAC Addresses	**Frame**
	Layer 1 Physical	Cables, Connectors, Hubs (DLS, RS232, 10BaseT, 100BaseTX, ISDN, T1)	**Bits**

Инкапсуляция и обработка пакетов

- При продвижении пакета данных по уровням сверху вниз каждый новый уровень добавляет к пакету свою служебную информацию в виде заголовка и, возможно, трейлера (информации, помещаемой в конец сообщения). Эта операция называется *инкапсуляцией* данных верхнего уровня в пакете нижнего уровня. Служебная
- информация предназначается для объекта того же уровня на удаленном компьютере, ее формат и интерпретация определяются протоколом данного уровня.

Инкапсуляция и обработка пакетов

- Как правило, единицу обмена данными между уровнями называют *сообщением* (*message*). Однако, кроме термина
- «*сообщение*» существуют и другие названия. Встандартах
- *ISO* для протоколов любого уровня используетсятакой
- термин как «*блок данных протокола*» - *Protocol Data Unit* (*PDU*). Кроме этого, часто используются названия *кадр* (*frame*), *пакет* (*packet*), *дейтаграмма* (*datagram*).

Функции уровней модели ISO/OSI (Физический)

- Включает все физические аспекты передачи двоичной информации по линии связи, например, по такой как коаксиальный кабель, витая пара или оптоволоконный кабель.
- Обеспечивает аппаратный способ посылки и получения данных

Функции уровней модели ISO/OSI (Канальный)

- Реализация механизмов обнаружения и коррекции ошибок
- *MAC* (*Medium Access Control*) - Управление доступом к среде
- *LLC* (*Logical Link Control*) –Управление логической связью (каналом)

Функции уровней модели ISO/OSI (Сетевой)

- Служит для образования единой транспортной системы, объединяющей несколько сетей с *различными* принципами передачи информации между конечными узлами
- Осуществляет доставку данных между сетями

Примеры

- *IP стека TCP/IP*
- *IPX стека Novell*

Функции уровней модели ISO/OSI (Транспортный)

- Регламентирует пересылку *пакетов* сообщений между процессами, выполняемыми на компьютерах сети
- Завершает организацию передачи данных: контролирует на сквозной основе поток данных, проходящий по маршруту, определенному третьим уровнем: правильность передачи блоков данных, правильность доставки в нужный пункт назначения, их комплектность, сохранность, порядок следования

•Собирает информацию из блоков в ее прежний вид

Примеры

- *TCP* и *UDP* стека *TCP/IP*
- протокол *SPX* стека *Novell*

Функции уровней модели ISO/OSI (Сеансовый)

- Обеспечивает управление диалогом для того, чтобы фиксировать, какая из сторон является активной в настоящий момент
- Предоставляет средства синхронизации, восстанавливает аварийно оконченные *сеансы*
- Управляет сеансами связи между процессами прикладного уровня
- На практике немногие приложения используют сеансовый уровень, и он редко реализуется

Примеры

- *L2TP, NetBIOS, PPTP, RPC*

Функции уровней модели ISO/OSI (Уровень представления)

- обеспечивает гарантию того, что информация, передаваемая прикладным уровнем, будет понятна прикладному уровню в другой системе
- При необходимости уровень представления выполняет преобразование форматов данных в некоторый общий формат представления, а на приеме, соответственно, выполняет обратное преобразование
- На этом уровне может выполняться компрессия/декомпрессия, шифрование и дешифрование данных, благодаря которому секретность обмена данными обеспечивается сразу для всех прикладных сервисов

Пример

- *Secure Socket Layer (SSL)*

Функции уровней модели ISO/OSI (Прикладной уровень)

- Вдействительности просто набор разнообразных протоколов, с помощью которых пользователи сети получают доступ к разделяемым ресурсам, таким как файлы, принтеры или гипертекстовые Web-страницы, а также организуют свою совместную работу, например, с помощью протокола электронной почты

Примеры

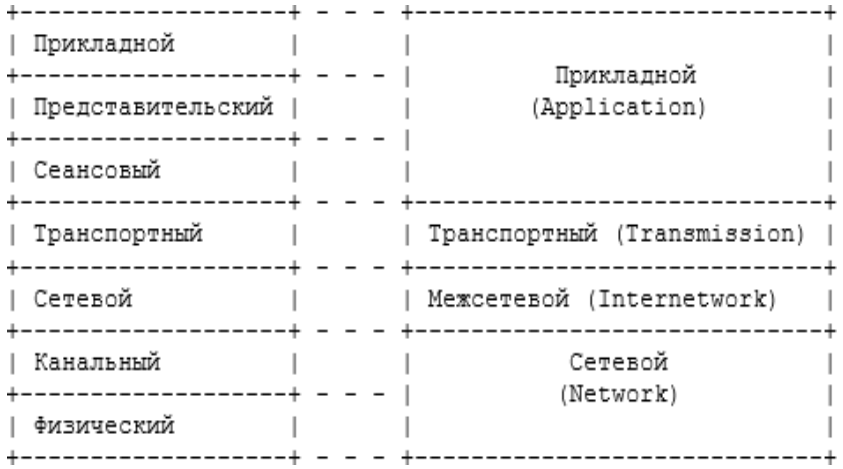
- SMB, FTP, TFTP, SMTP, HTTP и т.д.

Стек протоколов TCP/IP

- Стек протоколов *TCP/IP* – это промышленный стандартный набор протоколов, которые обеспечивают совместимость между компьютерами разных типов.
- Совместимость – одно из основных преимуществ *TCP/IP*, поэтому большинство *ЛВС* его поддерживает. Кроме того, TCP/IP предоставляет доступ к ресурсам Интернета, а также маршрутизируемый протокол для сетей масштаба предприятия. Поскольку *TCP/IP* поддерживает маршрутизацию, обычно он используется в качестве межсетевого протокола.
- Благодаря своей популярности *TCP/IP* стал стандартом де-факто для межсетевого взаимодействия.

Архитектура протоколов TCP/IP

- Ур. 4 (физический, нижний): не регламентируется (*Ethernet*, *Token Ring*, *FDDI*, *Fast Ethernet*, *100VG-AnyLAN*, *SLIP* и *PPP*, *X.25*, *frame relay*, *ATM*, *IEEE 802.11*).
- Ур. 3 (межсетевой): *IP*, *ARP* (*Address Resolution Protocol*), *RIP* (*Routing Internet Protocol*) и *OSPF* (*Open Shortest Path First*), *ICMP* (*Internet Control Message Protocol*).
- Ур. 2 (транспортный): протокол управления передачей *TCP* (*Transmission Control Protocol*) и протокол дейтаграмм пользователя *UDP* (*User Datagram Protocol*).
- Ур. 1 (прикладной): *FTP* (*File Transfer Protocol*) реализует удаленный доступ к файлу, аутентификация пользователей, распечатка содержимого каталогов и т.д., *TFTP* (*Trivial File Transfer Protocol*) - только передача файлов поверх *UDP* (без установления соединения), *SNMP* (*Simple Network Management Protocol*) - для организации сетевого управления



Межсетевой протокол IPv4

Межсетевой протокол *IP* специфицирован в *RFC 791*. Его основные характеристики перечислены ниже:

- реализует обмен информации пакетами, которые будем называть *IP*-сегментами (максимальный размер *IP*-сегмента - 65535 байт);
- является протоколом взаимодействия без установления логического соединения;
- для адресации узлов сети используется адрес длиной 4 байта;
- обеспечивает в случае необходимости фрагментацию IP-дейтаграммы;
- *IP*- дейтаграммы имеют конечное время жизни в сети;
- не гарантирует надежность доставки *IP*-дейтаграммы адресату;
- не имеет средств управления интенсивностью передачи *IP*-дейтаграммы посылающей стороной (*flow control*);
- не гарантирует правильную последовательность *IP*-дейтаграммы на принимающей стороне


СТРУКТУРА IP-ПАКЕТА
ВЕРСИЯ IP 4 БИТА
ДЛИНА ЗАГОЛОВКА 4 БИТА
ТИП ОБСЛУЖИВАНИЯ 8 БИТ
ДЛИНА ПАКЕТА 16 БИТ
ИДЕНТИФИКАТОР ФРАГМЕНТА 16 БИТ
R
DF
MF
СМЕЩЕНИЕ ФРАГМЕНТА 13 БИТ
TTL (ВРЕМЯ ЖИЗНИ) 8 БИТ
ПРОТОКОЛ 8 БИТ
КОНТРОЛЬНАЯ СУММА ЗАГОЛОВКА 16 БИТ
IP-АДРЕС ОТПРАВИТЕЛЯ 32 БИТА
IP-АДРЕС ПОЛУЧАТЕЛЯ 32 БИТА
ПАРАМЕТРЫ (ПОЛЕ ПЕРЕМЕННОЙ ДЛИНЫ И ЗАПОЛНЕНИЯ НУЛЯМИ ДО 4-Х БАЙТ)
ДАННЫЕ

Протокол управления передачей TCP

Протокол управления передачей *TCP* (*Transmission Control Protocol*) является протоколом транспортного уровня и базируется на возможностях, предоставляемых межсетевым протоколом *IP*. Основная задача *TCP* - обеспечение надежной передачи данных в сети. Описание протокола *TCP* дано в *RFC 793*.

- реализует взаимодействие в режиме с установлением логического (виртуального) соединения;
- обеспечивает двунаправленную дуплексную связь;
- организует потоковый (с точки зрения пользователя) тип передачи данных;
- дает возможность пересылки части данных, как "экстренных";
- для идентификации партнеров по взаимодействию на транспортном уровне использует 16-битовые "номера портов";
- реализует принцип "скользящего окна" (*sliding window*) для повышения скорости передачи;
- поддерживает ряд механизмов для обеспечения надежной передачи данных.


СТРУКТУРА TCP-ПАКЕТА
ПОРТ ОТПРАВИТЕЛЯ 32 БИТ
ПОРТ ПОЛУЧАТЕЛЯ 32 БИТ
ПОРЯДКОВЫЙ НОМЕР 32 БИТ
НОМЕР ПОДТВЕРЖДЕНИЯ 32 БИТ
СМЕЩЕНИЕ 4 БИТА
ЗАРЕЗЕРВИРОВАННО 6 БИТ
U
A
P
R
S
F
РАЗМЕР ОКНА 16 БИТ
КОНТРОЛЬНАЯ СУММА 16 БИТ
УКАЗАТЕЛЬ СРОЧНОСТИ 16 БИТ
ПАРАМЕТРЫ (ПОЛЕ ПЕРЕМЕННОЙ ДЛИНЫ И ЗАПОЛНЕНИЯ НУЛЯМИ ДО 4-Х БАЙТ)
ДАННЫЕ

Известные номера портов для некоторых служб

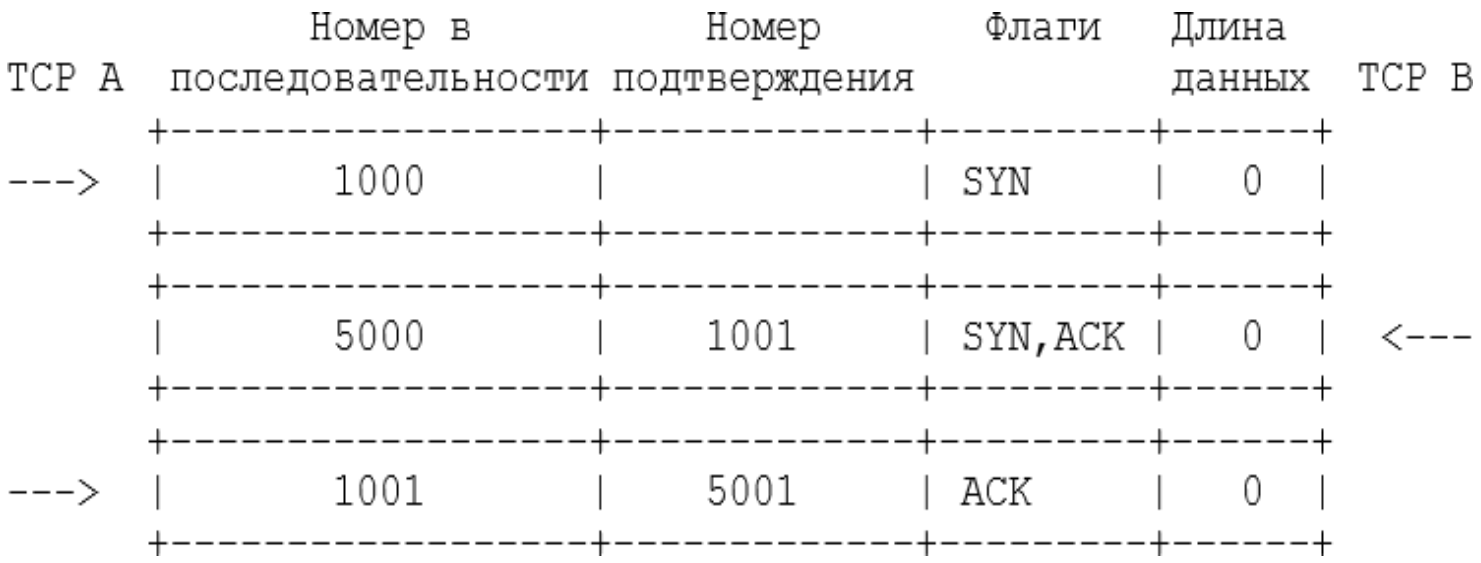
Port Number	Protocol	Application
20	TCP	FTP Data
21	TCP	FTP Control
22	TCP	SSH
23	TCP	Telnet
25	TCP	SMTP
53	UDP,TCP	DNS
67,68	UDP	DHCP
69	UDP	TFTP
80	TCP	HTTP
110	TCP	POP3
161	UDP	SNMP
443	TCP	SSL
16,384-32,767	UDP	RTP-based Voice and Video

Этапы TCP-взаимодействия

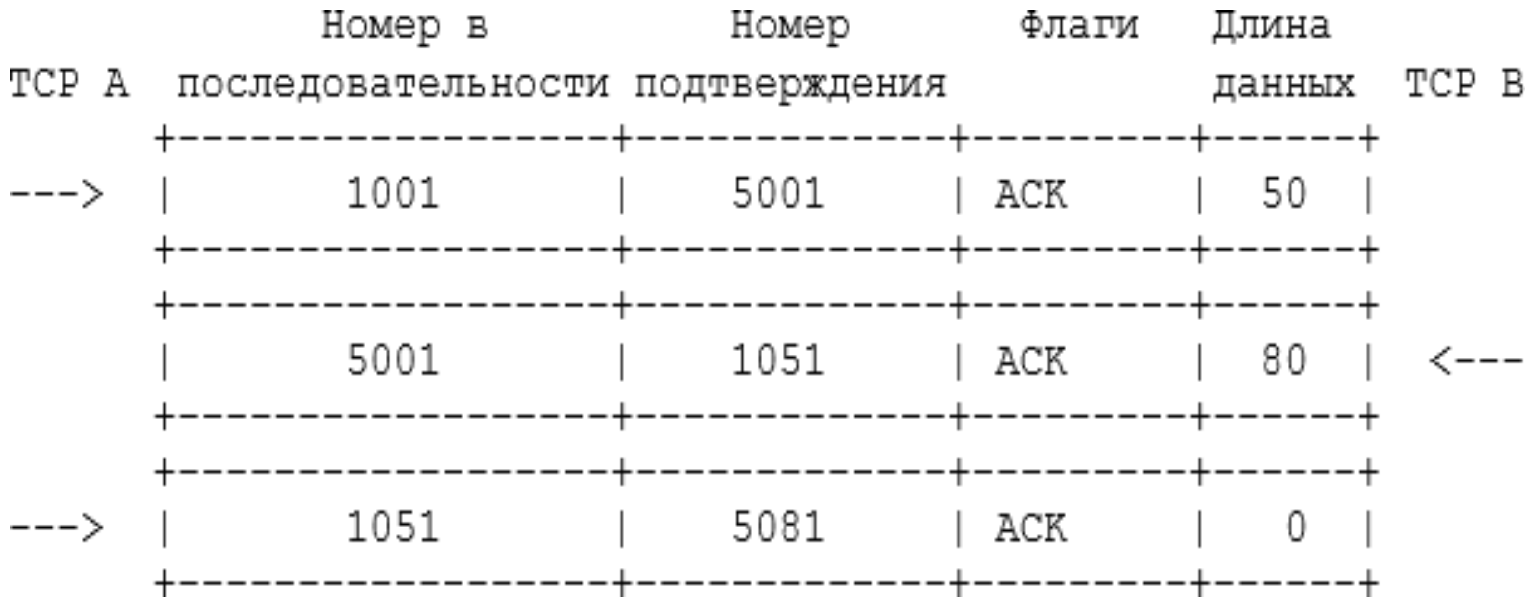
Взаимодействие партнеров с использованием протокола *TCP* строится в три этапа:

- установление логического соединения;
- обмен данными;
- закрытие соединения.

Установление TCP соединения



Передача данных



Закрытие соединения

TCP A	Номер в последовательности	Номер подтверждения	Флаги	Длина данных	TCP B
--->	1051	5081	ACK,FIN	0	
	5081	1052	ACK	0	<---
	5081	1052	ACK	40	<---
--->	1052	5121	ACK	0	
	5121	1052	ACK,FIN	0	<---
--->	1052	5122	ACK	0	

Протокол дэйтаграмм пользователя UDP

- Протокол дэйтаграмм
- пользователя *UDP* (*User Datagram Protocol*) является протоколом транспортного уровня и базируется на возможностях,
- предоставляемых
- межсетевым протоколом *IP*. Основная задача *UDP* - обеспечение "быстрой"
- передачи данных в сети. Его
- транспортный адрес в
- заголовке *IP*-сегмента равен
- 17. Описание протокола *UDP*
- дано в *RFC 768*.

- реализует взаимодействие в режиме без установлением логического (виртуального) соединения;
- организует поблочный (дэйтаграммный, пакетный) тип передачи данных;
- для идентификации партнеров по взаимодействию на транспортном уровне использует 16-битовые "номера портов";
- не гарантирует надежной передачи данных (возможна как потеря *UDP*-пакетов, так и их дублирование);
- не имеет средств уведомления источника *UDP*-пакета о правильности/ошибочности в его приеме адресатом;
- не обеспечивает правильный порядок доставки *UDP*-пакетов от источника к приемнику;
- может гарантировать целостность данных в *UDP*- пакете за счет использования контрольной суммы;
- очень прост (особенно, по сравнению с протоколом *TCP*).

Формат заголовка UDP-пакета

Чем защитить сеть ?

Полезные ссылки и ресурсы !!!

Сайты:

Kali Linux - https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-hyperv-image-download/

DVL - https://en.wikipedia.org/wiki/Damn_Vulnerable_Linux

VirtualBox - https://www.virtualbox.org/wiki/Downloads или **VMWare**

Ссылка на **RFC** на русском языке (https://rfc2.ru/)

Книги:

1. Обнаружение нарушений безопасности в сетях, Норткат С., Новак Д.
2. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 100-101. Одом Уэндел
3. Искусство эксплойта, Эриксон

Спасибо за внимание!
Вопросы...

Контакты:
victr35@yandex.ru
victrchaplygim