МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра космического приборостроения и систем связи

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«___» _____ 2017 г.

АНАЛИЗ ТРАФИКА КОМПЬЮТЕРНОЙ СЕТИ С ПОМОЩЬЮ СНИФФЕРОВ

Методические указания по выполнению практической работы №3 для студентов, обучающихся по направлению подготовки 11.03.02 «Инфокоммуникационные технологии и системы связи» по дисциплине: «Основы построения инфокоммуникационных систем и сетей» ч.2

Курск 2017

УДК 621.391

Составители: А.В. Хмелевская, А.Н. Шевцов

Рецензент
Доктор технических наук, старший научный сотрудник,
профессор кафедры *В.Г. Андронов*

Анализ трафика компьютерной сети с помощью снифферов: методические указания по выполнению практической работы №3 по дисциплине: «Основы построения инфокоммуникационных систме и сетей», ч.2 / Юго-Зап. гос. ун-т; сост.: А.В. Хмелевская, А.Н. Шевцов. – Курск, 2017. – 8 с.: табл. 1. – Библиогр.: с. 8.

Методические указания по выполнению практической работы содержат краткие теоретические сведения о анализе трафика компьютерной сети с помощью снифферов.

Методические указания полностью соответствуют требованиям типовой программы, утвержденной УМО по направлению подготовки 11.03.02 «Инфокоммуникационные технологии и системы связи», а также рабочей программе дисциплины: «Сети и системы передачи информации».

Предназначены для студентов, обучающихся по направлению подготовки 11.03.02, очной и заочной форм обучения.

Текст печатается в авторской редакции

Подписано в печать 15.12.17 . Формат 60x841/16.
Усл. печ. л. 0,465 .Уч.-изд. л. 0,42 .Тираж 100 экз. Заказ. 3238 Бесплатно
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94

1 Цель работы

- приобретение практических знаний и навыков в перехвате и анализе трафика сегмента компьютерной сети.

2 Теоретические сведения

Снифферы (дословный перевод - ‘вынюхиватели’) являются специализированным ПО, предназначенным для анализа потока сообщений (трафика) компьютерной сети передачи информации [4]. Известными системами подобного рода (но глобального уровня) являются ЭШЕЛОН (североамериканский проект, назначением которого является анализ содержимого линий связи Европы) и СОРМ (тотальное протоколирование трафика русскоязычной Сети). Большинство программ и сервисов (ICQ, TelNet, FTP, HTTP, POP3 и т.д.) пересылают пароль и логин пользователя открытым текстом (без всякой кодировки и шифровки), и работающий сниффер без труда позволит перехватывать такие сессии.

К простым ПО подобного класса относится, например комплект SpyNet (simik.lgg.ru/spynet312.exe); в штатную поставку Windows’NT Server и др. входит утилита Network Monitor (устанавливается добавлением сервиса Network Monitor Tools & Agent).

Обычно сетевая карта, работающая в сегменте некоммутируемой Ethernet в принципе ‘прослушивает’ весь трафик своего сегмента; однако в нормальном (без PROMISCUOUS MODE) режиме анализируются лишь первые 48 бит заголовка пакета и, если не найден собственный MAC-адрес, карта перестает читать ‘чужой’ пакет. Функциональность сниффера достигается переводом сетевой карты в режим PROMISCUOUS MODE, обеспечивающий перехват всех сообщений, циркулирующих в данном сегменте сети безотносительно MAC-адресов (достигается программной установкой соответствующего бита управляющего регистра карты). В случае коммутируемого Ethernet перевод карты в PROMISCUOUS MODE не позволяет прослушивать ‘чужие’ сообщения, в этом случае используется технология ‘ARP-спуфинга’ (путем соответствующей подделки ARP-сообщений

данная сетевая карта ‘притворяется’ маршрутизатором с MAC-адресом, однако, данной карты), при этом трафик всех составляющих сегмента сети насильственно направится в сторону карты- обманщика.

3. Задание на практическую работу

4. Содержание отчета

Практическая работа рассчитана на 2 часа для очной формы обучения направления подготовки 11.03.02 и выполняется в 3й контрольной точке.

По результатам выполненной работы представляется отчет, в котором должны содержаться следующие пункты:

1. Цель работы;
2. Индивидуальное задание;
3. Краткие теоретические сведения
4. Ход выполнения работы;
5. Основные результаты, полученные в работе, схемы, таблицы, графики;
6. Выводы о проделанной работе с анализом полученных результатов;
7. Ответы на контрольные вопросы.

Минимальный балл за практическую работу составляет 0.5 балла (выполнил работу, но не защитил). Максимальный балл – 3 (выполнил работу и защитил без замечаний).

Примерные критерии оценки качества отчётов по лабораторной работе:

– оформление отчёта не соответствует предъявляемым требованиям – минус 0,5 балла;

– полученные экспериментальные материалы не обработаны (осциллограммы, спектрограммы и т. п.) – минус 0,5 балла;

– выводы не соответствуют результатам работы – минус 0,5 балла;

– работа защищена не вовремя (после окончания 3й контрольной точки) – минус 0,5 балла.

5 Контрольные вопросы

1. Что представляет из себя ПО класса снифферов и с какой целью применяется?
2. Каковы ограничения методов перехвата информации снифферами?
3. Каким образом сетевая плата конкретной ПЭВМ в локальной сети распознает назначение пакетов по принципу ‘свой-чужой’?
4. Какие методы применяют с целью исключения возможности перехвата сообщений снифферами?

6 Библиографический список

1. Основы построения телекоммуникационных систем и сетей [Текст] : учебник / под ред.: В. Н. Гордиенко, В. И. Крухмалева. - 2-е изд., испр. - М. : Горячая линия - Телеком, 2008. - 424 с.

2. Проектирование и техническая эксплуатация цифровых телекоммуникационных систем и сетей [Текст] : учебное пособие / Е. Б. Алексеев [и др.] ; под ред. В. Н. Гордиенко и М. С. Тверецкого. - Москва : Горячая линия-Телеком, 2014. - 391 с.

3. Крук, Б. И. Телекоммуникационные системы и сети [Текст] : учебное пособие / Б. И. Крук, В. Н. Попантонопуло, В. П. Шувалов ; под ред. В. П. Шувалова. - 4-е изд., испр. и доп. - Москва : Горячая линия - Телеком. Т. 1 : Современные технологии. - 2013. - 620 с.

4. Гольдштейн Б. С., Соколов Н. А., Яновский Г. Г. Сети связи. [Текст]/ Б. С. Гольдштейн, Н. А. Соколов, Г. Г. Яновский – СПб.: БХВ – Петербург, 2010. – 302 с.