

МВД России

Федеральное государственное казенное учреждение
дополнительного профессионального образования
«Всероссийский институт повышения квалификации сотрудников
Министерства внутренних дел Российской Федерации»

М. Ю. Литвинов, В. И. Алескеров

**ПРОТИВОДЕЙСТВИЕ
СОВРЕМЕННЫМ ВИДАМ ПРЕСТУПЛЕНИЙ,
СОВЕРШАЕМЫХ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ**

Научно-практическое пособие

Часть 3

2-е издание, переработанное и дополненное

Домодедово
ВИПК МВД России
2026

ББК 67.408.135

Л 64

Авторский коллектив:

М. Ю. Литвинов, кандидат технических наук; **В. И. Алескеров**, кандидат юридических наук, доцент.

Рецензенты:

А. А. Курносенко – первый заместитель Министра внутренних дел Российской Федерации генерал-лейтенант полиции;

С. Н. Лебедев – заместитель Министра – начальник СД МВД России генерал-полковник полиции;

В. В. Голованов – начальник ГУУР МВД России генерал-лейтенант полиции;

О. В. Ильиных – начальник ГУПЭ МВД России генерал-лейтенант полиции;

О. А. Баранов – начальник ГУ МВД России по г. Москве генерал-лейтенант полиции;

В. К. Пауков – начальник ГУ МВД по Московской области генерал-лейтенант полиции;

С. А. Синенко – начальник Академии управления МВД России генерал-лейтенант полиции.

Л 64 Противодействие современным видам преступлений, совершаемых в условиях цифровизации : научно-практическое пособие : в 3 частях : 2-е издание, переработанное и дополненное / М. Ю. Литвинов, В. И. Алескеров. – Домодедово : ВИПК МВД России, 2026.

Часть 3. – 2026. – 68 с.

В научно-практическом пособии раскрываются уголовно-правовая и криминалистическая характеристики преступлений, совершаемых в условиях цифровизации. Рассматриваются проблемные вопросы раскрытия преступлений, совершаемых в сфере телекоммуникаций и компьютерной информации, особое внимание уделено раскрытию преступлений в системе дистанционного банковского обслуживания и преступлений террористического характера и экстремистской направленности.

Авторами даны понятия цифровизации, биллинга, идентификации, технического канала связи, телекоммуникационной сети, тайминга и др., с учетом криминалистического и оперативно-розыскного аспектов; впервые рассмотрены некоторые способы маскирования оперативно значимой информации.

Данное пособие предназначено для сотрудников подразделений специальных технических мероприятий, других оперативных подразделений органов внутренних дел и правоохранительной системы Российской Федерации. Будет полезно курсантам, адъюнктам, профессорско-преподавательскому составу высших учебных заведений юридического профиля правоохранительной системы Российской Федерации.

ББК 67.408.135

© ВИПК МВД России, 2026

Приложения

Приложение 1

Памятки в целях профилактики мошенничества

Памятка 1

1. Если поступило SMS-сообщение «Ваша карта заблокирована»:

- ни в коем случае не следовать рекомендациям подозрительных SMS-сообщений;
- при поступлении SMS-сообщений о блокировке карты нужно сразу же позвонить сотрудникам банка по телефону, который указан на банковской карте, официальном сайте банка или в договоре;
- банковские сотрудники никогда не просят назвать пин-код Вашей карты (в том числе ни по телефону, ни в электронном письме). Поэтому, если Вы всё-таки позвонили по указанному в SMS-сообщении номеру, и Вам предлагают прогуляться до ближайшего банкомата, чтобы ввести определённую комбинацию цифр, знайте: это мошенник! Банковские карты нельзя разблокировать через обычный терминал;
- если банкомат принял карту и пин-код – значит она не заблокирована.

2. «Мобильный банк».

Если у Вас украли телефон или Вы потеряли SIM-карту, то нужно сразу же обратиться в банк и отключить по данному номеру услугу «Мобильный банк». Ни в коем случае не выбрасывайте неактивные SIM-карты, чтобы мошенники ими не воспользовались!

3. Ложная информация «проблема у родственника»:

- ни в коем случае не следовать рекомендациям позвонивших;
- в ходе разговора задать уточняющие вопросы (Куда именно попал? В какой отдел? А на каком автомобиле? В каком районе? и т.д.), после чего преступники не захотят разговаривать;
- осуществить звонок родственникам или лицам, с ними проживающим, при невозможности дозвониться родственнику (выключен телефон) не поддаваться панике и сообщить в полицию о поступившем звонке.

4. Покупка, продажа товаров, трудоустройство на работу по объявлениям, размещенным в сети Интернет:

- ни в коем случае не следовать рекомендациям покупателя, продавца, работодателя по передаче им информации по имеющейся банковской карте, а именно, сведений с тыльной стороны карты, а также сведений из SMS-сообщений с одноразовым кодом (денежные средства на банковскую карту можно зачислить, зная только ее номер на лицевой стороне (16 или 18 цифр));

- не перечислять в качестве задатка денежные средства на банковские карты и абонентские номера;

- осуществить проверку принадлежности абонентских номеров продавца, покупателя к региону Российской Федерации (программы в интернете или же программы для телефонов Android, ИОС) и сравнить с объявлением;

- задавать продавцу, покупателю уточняющие вопросы по месту нахождения, расположения, особенностям предмета и т.д.

Памятка 2

Справочная информация для подготовки запросов

Информация, которую можно получить по сайтам:

- по названию сайта можно получить информацию о его полном доменном имени, которое состоит из непосредственного имени домена и далее имён всех доменов, в которые он входит, разделённых точками. Например, полное имя «ru.wikipedia.org» обозначает домен третьего уровня «ru», который входит в домен второго уровня «wikipedia», который входит в домен верхнего уровня «org», который входит в безымянный корневой домен «.» (точка);

- регистратор доменного имени – организация, имеющая полномочия создавать (регистрировать) новые доменные имена и продлевать срок действия уже существующих доменных имён в домене, для которого установлена обязательная регистрация. Таковыми доменами являются: домен нулевого уровня (корневой домен); все домены верхнего уровня (первого уровня);

- компания хостер – организация, оказывающая услуги по предоставлению вычислительных мощностей для размещения информации на сервере, постоянно находящемся в сети Интернет.

В сети Интернет на специальных информационных сайтах (например, 2ip.ru, nic.ru) можно установить регистратора доменного имени и компанию хостера по названию сайта. При свободной политике конфиденциальности

может быть указано лицо, регистрировавшее доменное имя. На ресурсах регистратора доменного имени также при свободной политике конфиденциальности может быть указано лицо, регистрировавшее доменное имя.

При направлении запроса в компанию хостер может быть получена информация об ip-адресах, с которых осуществляется администрирование сайта и реквизиты, используемые клиентом при оплате хостинга (при платной услуге).

Регистратор доменного имени по запросу также может предоставить регистрационные данные, указанные при получении доменного имени клиентом, а также ip-адреса, с которых происходила регистрация.

Электронные почтовые ящики.

Операторы электронной почты сохраняют сведения о регистрации пользователей и сеансах последнего доступа за различный период времени. Также сохраняется содержимое электронной переписки, если пользователь не удалял свою корреспонденцию самостоятельно.

Возможно получить сведения от операторов связи, действующих на территории Российской Федерации (Mail.ru. Rambler.ru. Yandex.ru). Информацию об адресах электронной почты, расположенных за пределами Российской Федерации, необходимо запрашивать через НЦБ Интерпола.

ООО «Мэйл.Ру» сохраняет сведения о регистрации пользователя, а также о последних 10-15 сеансах доступа пользователя к ящику, приблизительно за несколько месяцев. Запрос в ООО «Мэйл.Ру» направляется почтой. Срок исполнения зависит от времени предоставления запроса.

ООО «Рамблер Интернет Холдинг» сохраняет сведения о регистрации пользователя, а также о последних сеансах доступа пользователя к ящику приблизительно 1-2 месяца. Запрос направляется почтой. Срок исполнения составляет около 2-3 недель.

ООО «Яндекс» сохраняет сведения о регистрации пользователя, а также о последних сеансах доступа пользователя к ящику приблизительно 1-2 месяца. Запрос направляется почтой. Срок исполнения составляет около месяца.

Информация по электронным почтовым ящикам, расположенным на собственных почтовых серверах различных сайтов, может быть получена только у администрации ресурса или у компании хостера.

Выемка электронной переписки проводится по постановлению суда в офисах компаний.

Социальные сети.

В сети Интернет действует значительное количество социальных сетей, как правило, в большинстве случаев используются самые распространённые: «ВКонтакте» и «Одноклассники», реже «Мой Мир». При запросе сведений у оператора социальной сети необходимо указывать в запросе идентификатор учетной записи либо ссылку на страницу интересующего пользователя.

Недопустимо указывать в запросах общее описание учетной записи (имя, фамилия, возраст, город и т.п.).

Операторы социальных сетей сохраняют у себя следующую информацию:

- сведения о регистрации учетной записи: указанные пользователем анкетные данные, дату и время регистрации, IP-адрес доступа к сети Интернет при регистрации, как правило, также – абонентский номер сотовой связи, использованный для подтверждения регистрации;
- сведения о доступе пользователя к своей учетной записи в виде зафиксированных моментов даты и времени с соответствующим IP-адресом. Сведения о доступе хранятся, как правило, 2-3 месяца;
- сведения о платежных операциях, проведенных пользователем;
- электронную переписку пользователя, в случае, если она не была удалена владельцем.

ООО «ВКонтакте» располагает сведениями о доступе пользователя к учетной записи около 2 недель с момента получения организацией запроса. Таким образом, установить сведения о более ранних сеансах доступа пользователя не представляется возможным.

Исключением является момент регистрации пользователя, сведения о котором хранятся постоянно.

Запросы в ООО «ВКонтакте» направляются почтой, срок исполнения составляет в среднем около 2-3 недель. В запросе необходимо указывать конкретный идентификатор учетной записи. При необходимости допустимо запрашивать сведения о группах, сообществах, указывая в таком случае идентификатор группы. Допустимо запрашивать сведения о наличии жалоб пользователей социальной сети в адрес интересующего идентификатора. В запросе должны быть указаны основания направления запроса (КУСП, обращение) образец ссылки vk.com/id654654654 или vk.com/sdkjfh.

В случае, когда необходимо получить содержимое электронной переписки пользователя, в адрес ООО «ВКонтакте» приложением к запросу направляется заверенная копия соответствующего постановления.

По удаленным анкетам информация не сохраняется.

ООО «Одноклассники» аналогично постоянно сохраняет сведения о моменте регистрации пользователя в социальной сети, а сведения о доступе пользователя к странице хранит более продолжительное время,

порядка 3-4 месяцев. Сведения об электронной переписке пользователя аналогично предоставляются при наличии постановления суда.

Запрос в ООО «Одноклассники» направляется почтой. В запросе должны быть указаны основания направления запроса (КУСП, обращение) и ссылка на аккаунт или группу ok.ru/klclkjklj. Выемки проводятся на основании постановления в офисах компаний. По удаленным анкетам информация не сохраняется.

Электронные платежные системы.

В сети Интернет действует значительное количество электронных платежных систем, как правило, в большинстве случаев используются самые распространённые: «Яндекс.Деньги», «ВебМани» и т.п. При запросе сведений у оператора платежной системы необходимо указывать в запросе идентификатор учетной записи пользователя.

Операторы платежных систем сохраняют у себя следующую информацию:

- сведения о регистрации учетной записи: указанные пользователем анкетные данные, дату и время регистрации, IP-адрес доступа к сети Интернет при регистрации, как правило, также – абонентский номер сотовой связи, использованный для подтверждения регистрации;
- сведения о доступе пользователя к своей учетной записи в виде зафиксированных моментов даты и времени с соответствующим IP-адресом. Сведения о доступе хранятся, как правило, последние 2-3 месяца;
- сведения о платежных операциях, проведенных пользователем.

Яндекс.Деньги. Сведения о регистрации кошелька сохраняются постоянно, сведения о доступе к кошельку хранятся около 2-3 месяцев, сведения о платежных операциях – продолжительное время.

Запросы в Яндекс.Деньги направляются почтой, время исполнения составляет около 1-2 месяцев.

ВебМани. ООО «ВебМани.Ру» занимается обслуживанием электронных платежных средств ВебМани. При этом следует понимать, что при регистрации пользователь сначала получает общую учетную запись, именуемую WMID, к которой затем самостоятельно закрепляет электронные кошельки. Данные кошельки различаются в зависимости от типа валюты (курс аналогичен обычному банковскому): рублевые, долларовые и т.п. Тип кошелька определяется по первой букве в его наименовании: R – для рублевых, Z – для долларовых, E – для евро, B – для белорусских рублей и т.п.

Запросы по рублевым кошелькам направляются непосредственно в ООО «ВебМани.Ру», запросы по кошелькам иного типа валюты адресуются головной компании WMTransferLtd. и направляются в адрес ООО «ВебМани.Ру» для передачи на исполнение.

Объявления.

Оператором системы электронных объявлений «Авито» является ООО «КЕХ Коммерц». Организация может предоставить сведения по электронному объявлению: дата и время размещения, IP-адреса, контактная информация, наличие жалоб на автора объявления, а также другие объявления, которые размещались данным пользователем. В большинстве случаев необходимо указывать конкретный номер объявления, в порядке исключения (если сведения утрачены) дать как можно более подробное описание объявления: примерную дату публикации (время обнаружения объявления заявителем), реализуемый товар (точно передать описание), контактные данные, которые были указаны в объявлении (телефон, адрес электронной почты и т. п.).

Запрос направляется почтой, время исполнения зависит от скорости доставления запроса в организацию.

IP-адреса.

Для установления окончного оборудования, которому присваивался IP-адрес, необходимо знать точную дату и время присвоения с точностью до секунды. В некоторых случаях необходимо знать ресурс обращения (IP-адрес) и порт соединения.

Для получения информации об IP-адресе необходимо направить запрос провайдеру. Определить провайдера, которому принадлежит IP-адрес, можно из открытых источников 2ip.ru, nls.ru.

Памятка 3

Платежные системы и банки:

- **ПАО «Сбербанк».** Адрес: Россия, 117997 г. Москва, ул. Вавилова, д. 19;
- **ООО «НКО Вестерн Юнион ДП Восток».** Адрес: 125171, г. Москва, Ленинградское шоссе, д. 16 «А», строение 1. Телефоны: 8 (495) 797-21-87, факс 797-21-88;
- **Т-Банк (ранее – АО «Тинькофф Банк»).** Адрес: 127287, г. Москва, ул. 2-я Хуторская, д. 38А, строение 26. Телефоны: 8 (800) 555-22-27, 8 (800) 700-66-66;
- **АО «Связной банк».** Адрес: 123001, г. Москва, пер. Ермолаевский, д. 27, строение 1. Телефон: 8 (800) 100-00-05;
- **ООО «РБК МАНИ».** Адрес: 107023, г. Москва, пл. Семеновская, д. 1а. Телефоны: 8 (495) 648-68-53, 8 (495) 363-11-11;
- **Платежная система RbK.money.** Адрес: Москва, ул. Павловская, д. 7, строение 2, 6 этаж. Телефон: 8(495) 648-68-58;

- **ООО НКО «ЮМАНИ»**. Адрес: 115035, г. Москва, ул. Садовническая, д. 82, строение 2. Телефон: 8 (800) 700-22-99;
- **АО «Национальная сервисная компания» (RURU)**. Адрес: 127473, г. Москва, ул. Краснопролетарская, д. 16, строение 1. Телефоны: 8 (800) 700-48-48, 8 (495) 955-78-36;
- **ООО «ВебМани.Ру»**. Адрес: 107497, г. Москва, Иркутская ул., д. 17, строение 4. Телефоны: 8 967 064-99-83, 8 495 727-20-07;
- **ООО «КИБЕРПЛАТ»**. Адрес: 123610, г. Москва, ЦМТ, Краснопресненская набережная, д. 12, подъезд 7. Телефоны: 8 (495) 967-02-20, 967-02-08;
- **ООО НКО «Деньги. Мэйл.Ру»**. Адрес: 125167, г. Москва, Ленинградский пр-т, д. 39, строение 79. Телефон: 8 (495) 197-86-86;
- **ООО «Платежный»**. Адрес: 129090, г. Москва, Олимпийский пер., д. 14. Телефон: 8 (495) 783-83-93;
- **ООО «Мастеркард»**. Адрес: 127051, г. Москва, Цветной бульвар, д. 2, этаж 4, помещение 1. Телефоны: 8 (495) 937-77-10, 8 (800) 555-02-69;
- **ПАО «МТС Банк»**. Адрес: 115432, г. Москва, проспект Андропова, д. 18. Телефон: 8 800 250-05-20.

Ресурсы сети Интернет

1. **«Одноклассники»**
Адрес: Ленинский проспект, д. 39, стр. 79, БЦ «Skylight» г. Москва, 125167;
2. **«ВКонтакте»**
Адрес: ул. Херсонская, д. 12-14, лит. «А», г. Санкт Петербург, 191024;
3. **«Мэйл.Ру»**
Адрес: Ленинский проспект, д. 39, стр. 79, БЦ «Skylight» г. Москва, 125167;
4. **«Рамблер»**
Адрес: Варшавское шоссе, д. 9, стр. 1, г. Москва, 117105;
5. **«Яндекс»**
Адрес: ул. Льва Толстого, д. 16, г. Москва, 119021;
6. **«Авито»**
Адрес: ул. Лесная, д. 7, ООО «КЕХ еКоммерц», г. Москва, 125196;
7. **«Мамба»**
Адрес: Цветной бульвар, д. 25, строение 3, г. Москва, 127051;

8. «РБК (qip.ru, loveplanet.ru)»

Адрес: Ул. Ленинская Слобода, д.26, строение 2, г. Москва, 115280;

9. «Из рук в руки» (ООО «Пронто-Москва»)

Адрес: 2-й Южнопортовый пр-д, д. 27А, строение 1. г. Москва, 115432.

Регистраторы

АО «РСИЦ» (Региональный Сетевой Информационный Центр)

Адрес: 123308, г. Москва, 3-я Хорошевская ул., д. 2, стр. 1; телефон: (495) 737-06-48, факс: (495) 737-76-73.

ООО «Регистратор»

Адрес: 123007, г. Москва, ул. 5-я Магистральная, д. 4, помещение 5; телефон: 8 (495) 363-05-42.

ООО «Регистратор доменных систем РЕГ.РУ»

Адрес: 125315, г. Москва, Ленинградский проспект, д. 72, корпус 3; телефон: 8 (495) 580-11-11.

АО «Региональный Сетевой Информационный Центр»

Адрес: 125315, г. Москва, Ленинградский проспект, д. 72, корпус 3; телефон: 8 (495) 737-06-01, 8 (495) 944-46-01.

Операторы связи

ООО «Кloverтел» (предоставляет услуги IP- телефонии)

Адрес: ул. Ясенева, д. 12, к. 1, кв. 293, г. Москва, 115583, info@clovertel.ru.

ООО «МАТРИКС телеком» (предоставляет услуги IP- телефонии)

Адрес: пер. Милютинский, д. 3, а/я 618, 101000, info@mtx.ru.

АО «Межрегиональный Транзит Телеком» (предоставляет услуги IP- телефонии)

Адрес: ул. Марксистская, д. 22, стр. 1, г. Москва, 109147.

ООО «Системы Связи» (предоставляет услуги IP- телефонии)

Адрес: ул. Флотская, д. 7, помещение 6/3/29, г. Москва, 125581.

Памятка 4

Образец заявления гражданина

Директору Н-ского филиала
ПАО «Ростелеком»

Г.Н. Кузьменко

от гражданина ФИО

зарегистрирован _____

паспорт _____

Заявление

Прошу Вас предоставить информацию о соединениях принадлежащего мне абонентского номера _____ за период с _____ по _____. Прошу информацию предоставить сотрудникам полиции.

Фамилия И.О.

подпись

дата

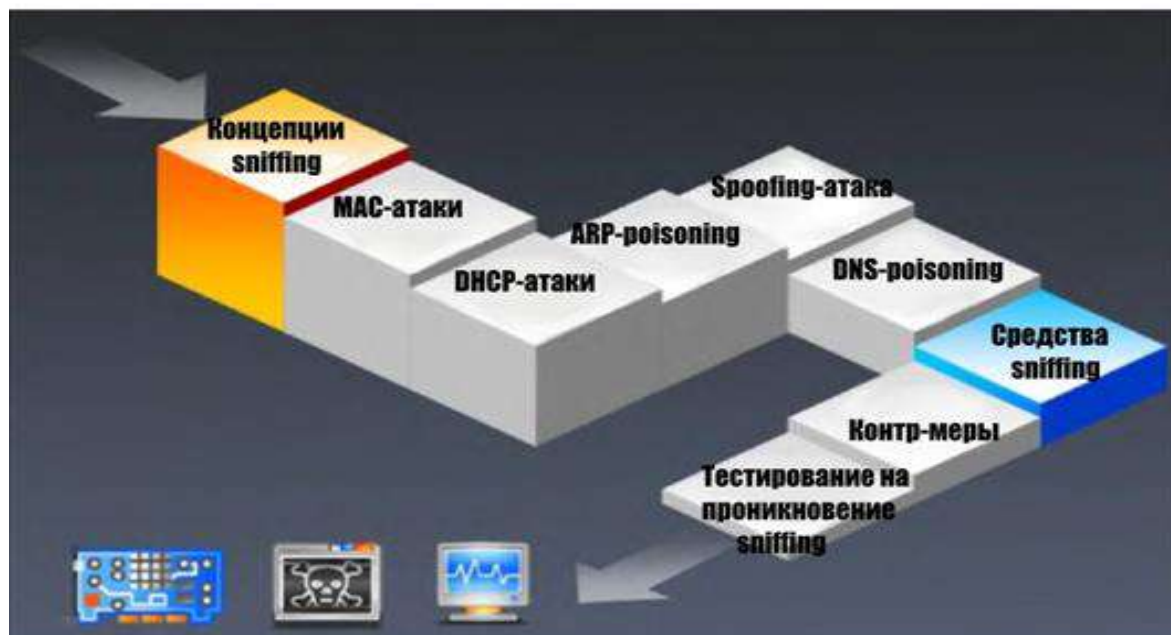
Памятка 5

Сетевые атаки

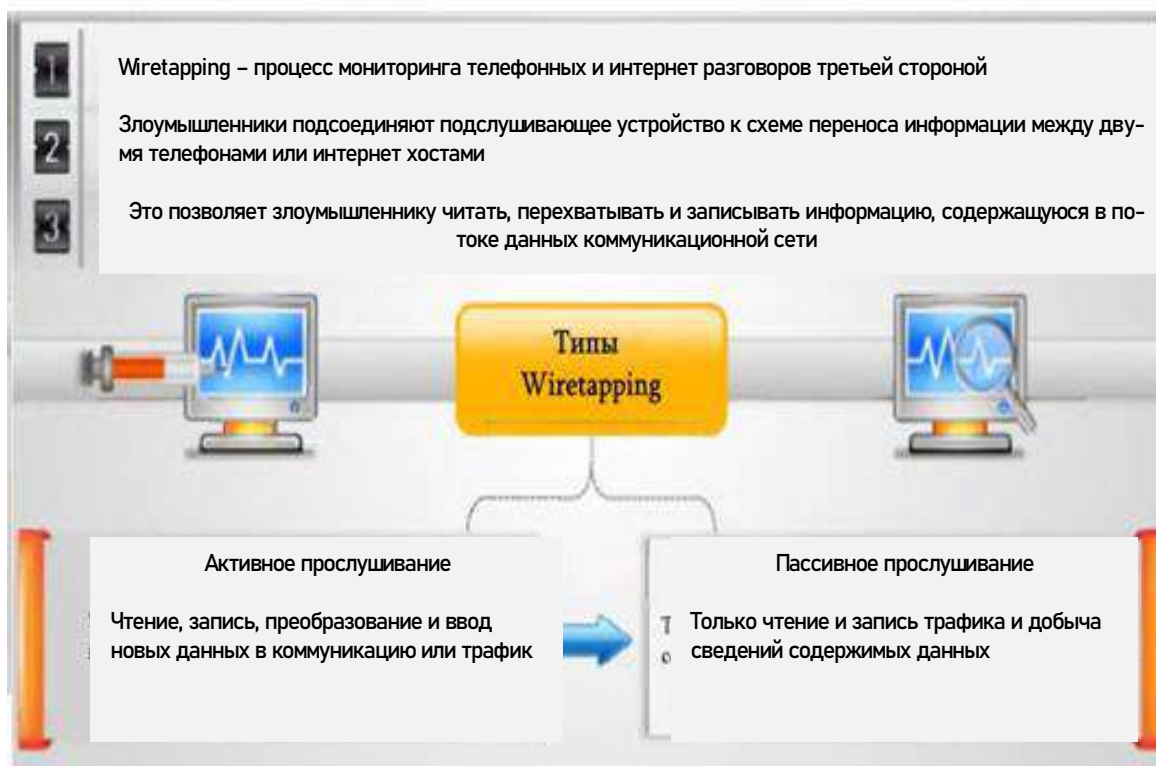
Модуль задач

- Sniffing пакетов - Угрозы sniffing - Типы sniffing-атак - Аппаратные анализаторы протоколов - MAC-flooding - Как работает DHCP - Атака DHCP-сервера - Методы ARP-spoofing - Средства ARP-poisoning	- Как защититься от ARP-poisoning - Угрозы spoofing-атаки - Как защититься от MAC-spoofing - Методы DNS-poisoning - Как защититься от DNS-spoofing - Средства sniffing - Как защититься от sniffing - Как обнаружить sniffing - Тестирование на проникновение sniffing
--	--

Концепции sniffing



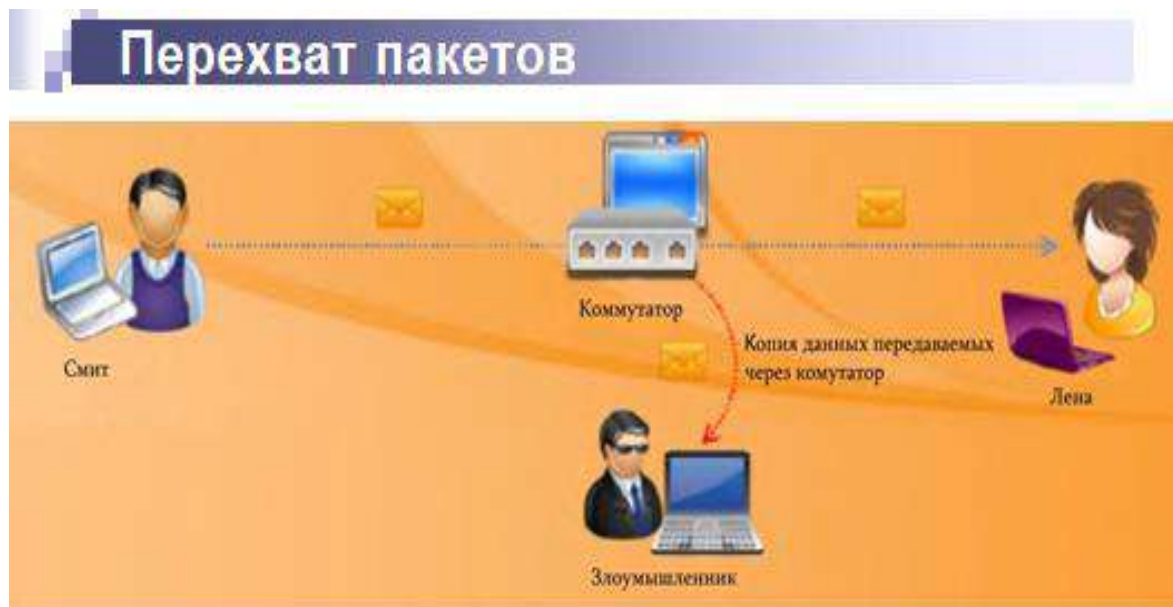
Прослушивание



Законное прослушивание



Устройство доступа собирает трафик, обслуживающего интернет-провайдера сети, сортирует трафик по IP-доменам и подает на системы декода и восстановления перехваченного трафика в оригинальном формате. Это достигается с помощью протоколов, таких как POP3, IMAP, SMTP, P2p и FTP, Telnet и других.



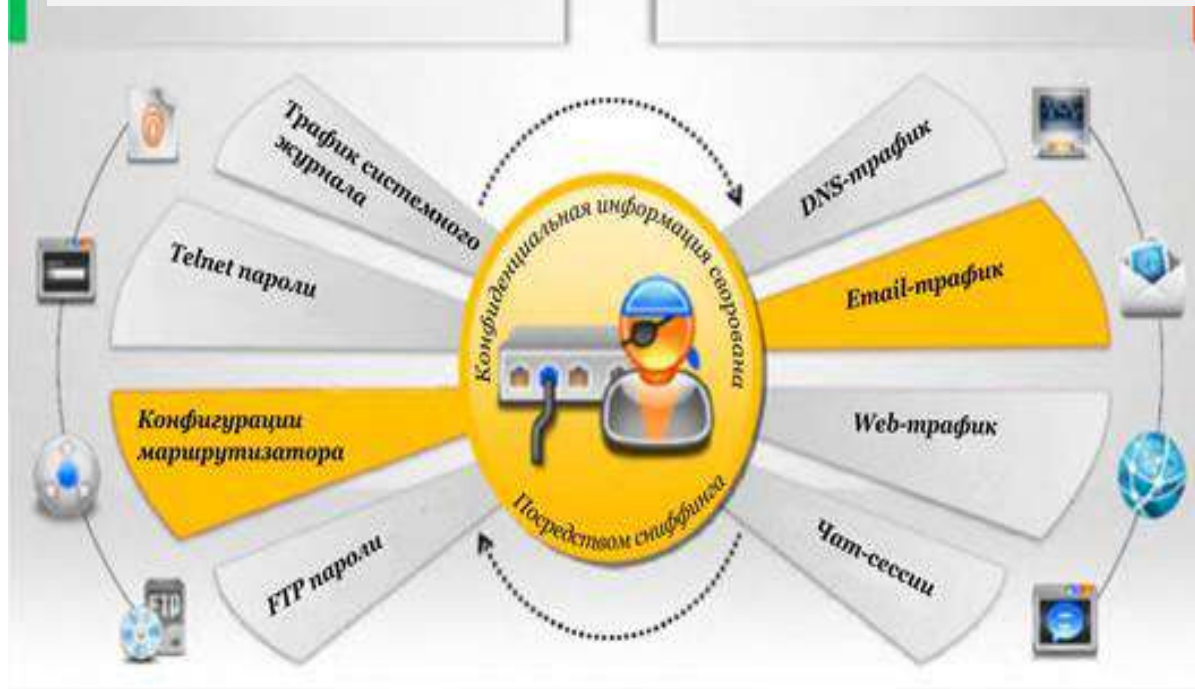
- Перехват пакетов является процессом мониторинга и захвата всех пакетов данных, проходящих через данную сеть с использованием программного обеспечения (приложений) или аппаратного устройства
- Это является одной из форм подслушивания применительно к компьютерным сетям
- Злоумышленники используют анализаторы перехватываемых пакетов данных, содержащих конфиденциальную информацию, такую как пароли, учетную информацию и т.д.
- Злоумышленники получают информацию, читая незашифрованные пакеты данных
- Когда злоумышленник подключается к порту он может контролировать весь транслируемый трафик на этот порт и доступ к конфиденциальной информации, имеющейся в незашифрованном трафике

Хотя большинство сетей сегодня применяют Switch-технологии, sniffing пакетов по-прежнему эффективен, потому что установка удаленных программ на сетевые компоненты с плотными потоками трафика, такие как серверы и маршрутизаторы, становится легкой. Это позволяет проследить и предоставляет доступ ко всему сетевому трафику с одной точки доступа. При использовании sniffing пакетов, возможен перехват пакетов данных, содержащих конфиденциальную информацию, такую как пароли, учетную информацию и т.д. Таким образом, вам будет доступно чтение паролей в незашифрованном виде, действительные электронные почты, номера кредитных карт, финансовые операции, и т.д. А также это позволяет вам узнать SMTP, POP, IMAP трафик, POP, IMAP, HTTP Basic, аутентификацию Telnet, SQL Database, SMB, NFS, FTP-трафик.

Угрозы sniffing

Благодаря размещению сниффера пакетов в сеть в прослушивающий режим злоумышленник может перехватить и проанализировать весь трафик сети в пределах одной подсети

Порты коммутации многих предприятий открытые
Любой находящийся в той же физической локации может подключиться к сети через Ethernet-кабель



Сниффер – программа и /или устройство, которое проверяет данные, передвигаясь по сети. Снифферы могут быть использованы для законной деятельности, например, управление сетью, а также для незаконной деятельности, например, кража информации, найденной в сети. Некоторые из самых простых пакетов используют командную строку интерфейса и сброс захваченных данных на экран, в то время как продвинутые лица используют графический интерфейс и график статистики трафика; они также могут отслеживать множество сеансов и предлагать несколько вариантов конфигурации. Сниффер пакетов способен на захват пакетов информации только в данной подсети. Обычно любой ноутбук можно подключить к сети и получить доступ. Порты коммутаторов многих предприятий являются открытыми. Размещая сниффер пакетов в сеть в прослушивающий режим, возможен захват и анализ всего сетевого трафика.

Как работает sniffer



- Sniffer переводит NIC системы в прослушивающий режим, так что он слушает все данные, передаваемые на своем сегменте
- Sniffer может постоянно следить за всем сетевым трафиком на компьютере через сетевую карту путем декодирования информации, инкапсулированную в пакете данных

Наиболее распространенный способ объединения компьютеров осуществляется через Ethernet. Компьютер, подключенный к локальной сети, имеет два адреса. Одним из них является MAC-адрес, который однозначно идентифицирует каждый узел в сети и хранится на сетевой карты. MAC-адрес используется протоколом Ethernet при построении «фреймов» для передачи данных в систему и из системы. Другой адрес - это IP-адрес. Этот адрес используется приложениями. Канальный уровень использует заголовок Ethernet с MAC-адресом целевой машины, а не IP-адрес. Сетевой уровень отвечает за отображение сетевого IP-адреса в MAC-адрес в соответствии с требованиями протокола передачи данных. Первоначально ищет MAC-адрес целевой машины в таблице, обычно называемую ARP-кэшем. Если запись не найдена для IP-адреса, ARP-трансляция пакетов запроса выводится на всех машинах локальной подсети. Машина с конкретным адресом отвечает исходной машине с ее MAC-адресом. Этот MAC-адрес будет добавлен в ARP-кэш исходной машины. Исходная машина во всех своих контактах с целевой машиной использует этот MAC-адрес. Есть два основных типа сред Ethernet, и снифферы работают немного различным образом в обоих случаях. Этими двумя типами сред Ethernet являются:

Общий Ethernet.

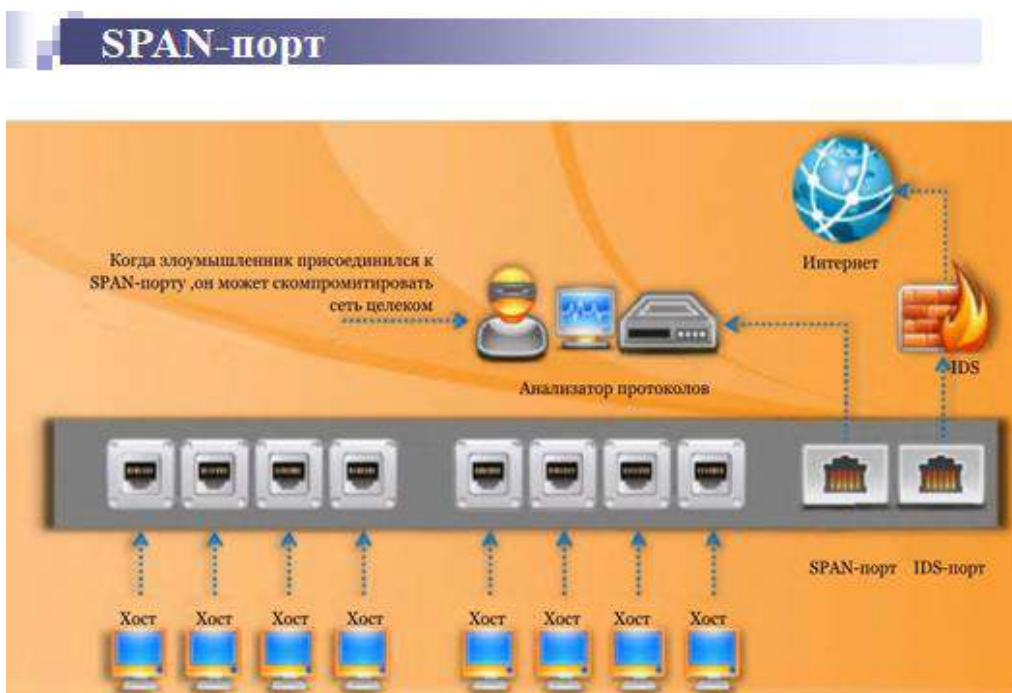
В общей среде Ethernet все узлы соединены с одной и той же шиной и конкурируют между собой за пропускную способность. В этой среде все

остальные машины получают пакеты, предназначенные для одной машины. Таким образом, когда машина 1 хочет поговорить с машиной 2, он отправляет пакет на сети с назначением MAC-адреса машины 2 вместе с собственным исходным MAC-адресом. Другие машины в общей среде Ethernet (машина 3 и машина 4) сравнивают назначенный MAC-адрес фрейма со своим собственным. Если они не совпадают, то кадр отбрасывается. Тем не менее, машинный запуск sniffера игнорирует это правило и принимает все кадры. Сниффинг в общей среде Ethernet полностью пассивный и, следовательно, трудно обнаруживаемый.

Switched Ethernet.

Среда Ethernet, в которой хосты подключены к коммутатору, а не к концентратору, называется Switch Ethernet. Коммутатор поддерживает таблицы отслеживания MAC-адресов каждого компьютера, и физический порт, с которым связан MAC-адрес, доставляет пакеты, предназначенные для конкретной машины. Коммутатор – устройство, которое посылает пакеты только на предназначенный компьютер и не транслирует его на все остальные компьютеры в сети. Это приводит к лучшей утилизации доступной пропускной способности и повышению безопасности. Таким образом, процесс перехода NIC в прослушивающий режим, чтобы собрать пакеты, не работает. В результате, многие люди думают, что коммутируемые сети являются абсолютно безопасными и невосприимчивыми к sniffingu.

Тем не менее, это не так.



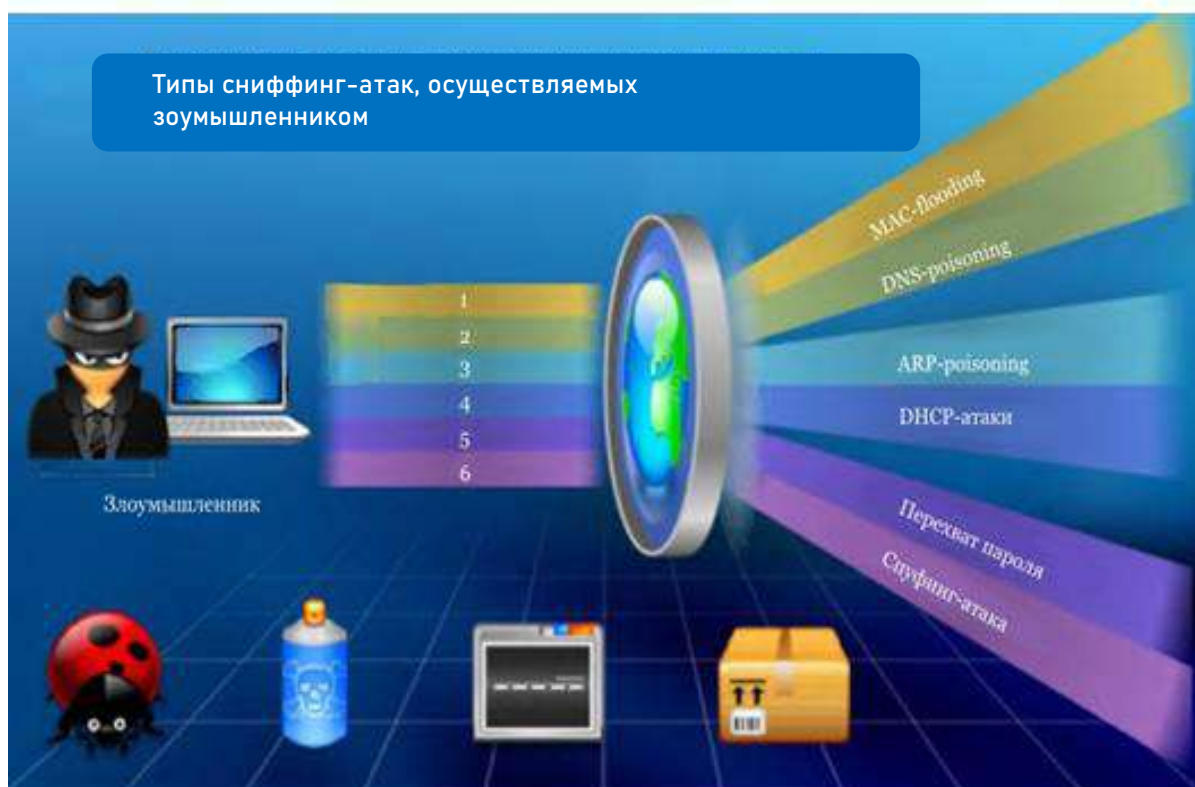
SPAN для анализатора коммутируемых портов Cisco, также известный как зеркалирование портов, является методом, который позволяет контролировать сетевой трафик от одного или нескольких портов коммутатора. Это также помогает анализировать и отлаживать данные, выявлять ошибки и исследовать на несанкционированный сетевой доступ.

Когда включено зеркалирование портов, сетевой коммутатор будет отправлять копию сетевых пакетов из исходного на порт назначения, где сетевые пакеты исследуются с помощью сетевого анализатора. Может быть, один или несколько источников, но должен быть только один порт назначения на коммутаторе. Исходные порты - порты, чьи сетевые пакеты отмониторены и зазеркалены. Вы можете одновременно контролировать трафик из нескольких портов. Например, вы можете контролировать трафик на всех портах конкретной VLAN.



Модель OSI (модель взаимодействия открытых систем) имеет систему коммуникаций, которая делится на более мелкие части. Каждая часть известна как уровень. Каждый уровень занимается предоставлением услуг для его верхнего уровня и приемом услуги из нижнего. OSI имеет сетевой фреймворк для реализации в семи уровнях. Канальным является второй уровень модели OSI. На этом уровне пакеты данных кодируются и декодируются в биты. Снифферы перехватывают пакеты из канального уровня. Снифферы оперируют на канальном уровне модели OSI. Они не придерживаются таким же правилам, как приложения и сервисы, которые находятся выше по стеку. Если один уровень взломан, коммуникации нарушаются без уведомления других уровней о проблеме.

Типы sniffing-атак



MAC-flooding - тип sniffing-атаки, флудящей коммутатор пакетами данных (зачастую MAC-адресами), препятствуя передаче данных между обычными пользователями. Данные вместо передачи от отправителя к получателю разносятся по всем портам. Таким образом, взломщики могут следить за данными в сети.

DNS-poisoning - процесс, при котором пользователь засылается на фиктивный сайт из-за ложных данных предоставленных DNS-сервером. Этот веб-сайт выглядит схоже с истинным, но находится под контролем нарушителя.

ARP-poisoning - атака, при которой нарушитель пытается ассоциировать свой MAC-адрес с IP-адресом жертвы, таким образом трафик, предназначенный для IP-адреса, пересылается нарушителю.

DHCP-атаки - DHCP подвержен двум типам атак. 1) DHCP-starvation: процесс взлома DHCP-сервера посредством отсылки огромного количества запросов на сервер. 2) Атака вредоносного DHCP-сервера: взломщик настраивает вредоносный DHCP-сервер выдавать себя за законный DHCP-сервер в LAN. Вредоносный сервер может начать выдачу лизинга клиента DHCP-сети. Информация, поставленная клиентам, обрывает их доступ к сети по причине DoS.

Сниффинг паролей – метод кражи паролей посредством мониторинга трафика, циркулирующего в сети, вытягивания данных, содержащих пароли. Пароли внутри системы отображаются в незашифрованном тексте, который облегчает нарушителю задачу идентификации и сопряжения с именами пользователей. В случаях, когда пароль зашифрован, нарушители могут воспользоваться алгоритмами дешифрования для его расшифровки. После получения паролей нарушители смогут добиться контроля над сетью и получить доступ к аккаунтам, конфиденциальной информации и т.д.

Spoofing-атаки - ситуация, когда нарушитель успешно притворился кем-то с помощью фальсификации данных, тем самым заполучил доступ к определенным ресурсам или выкрал персональную информацию. Нарушитель в состоянии воспользоваться IP-адресом жертвы для доступа к чужим аккаунтам, отсылки подставных емэйлов и настройки поддельных веб-сайтов для приобретения конфиденциальной информации, такой как пароли, детали аккаунтов и т.д. Нарушители в состоянии даже настроить поддельную беспроводную точку доступа и симулировать законных пользователей для подключения через нелегальное соединение.

Как CAM работает

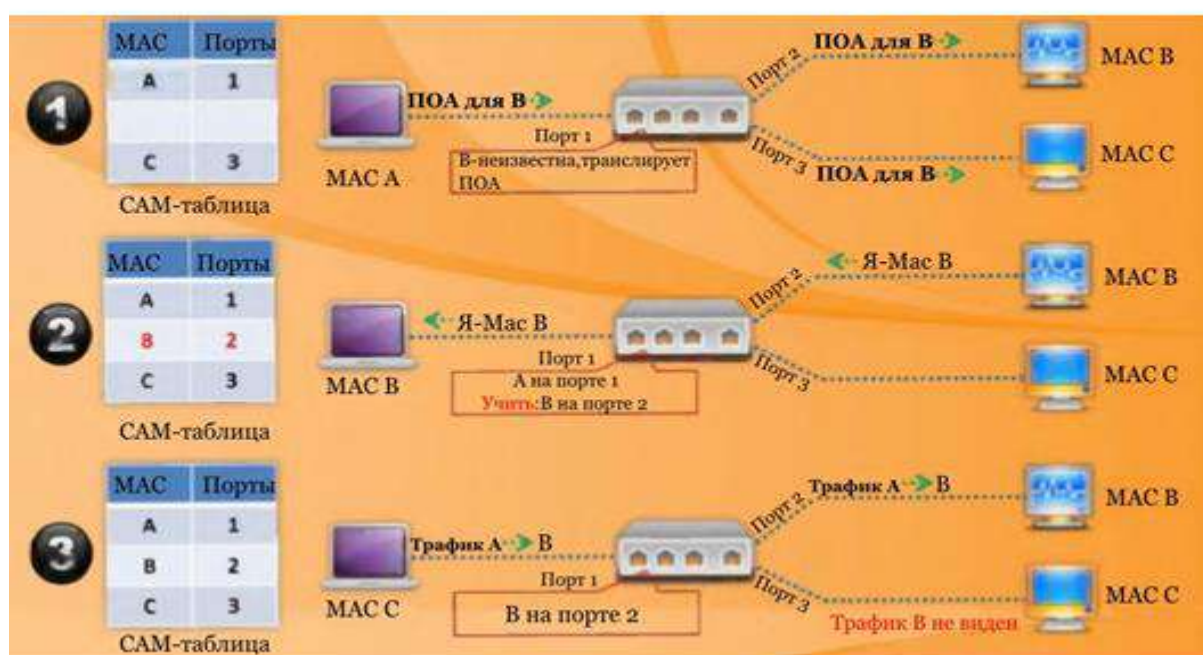
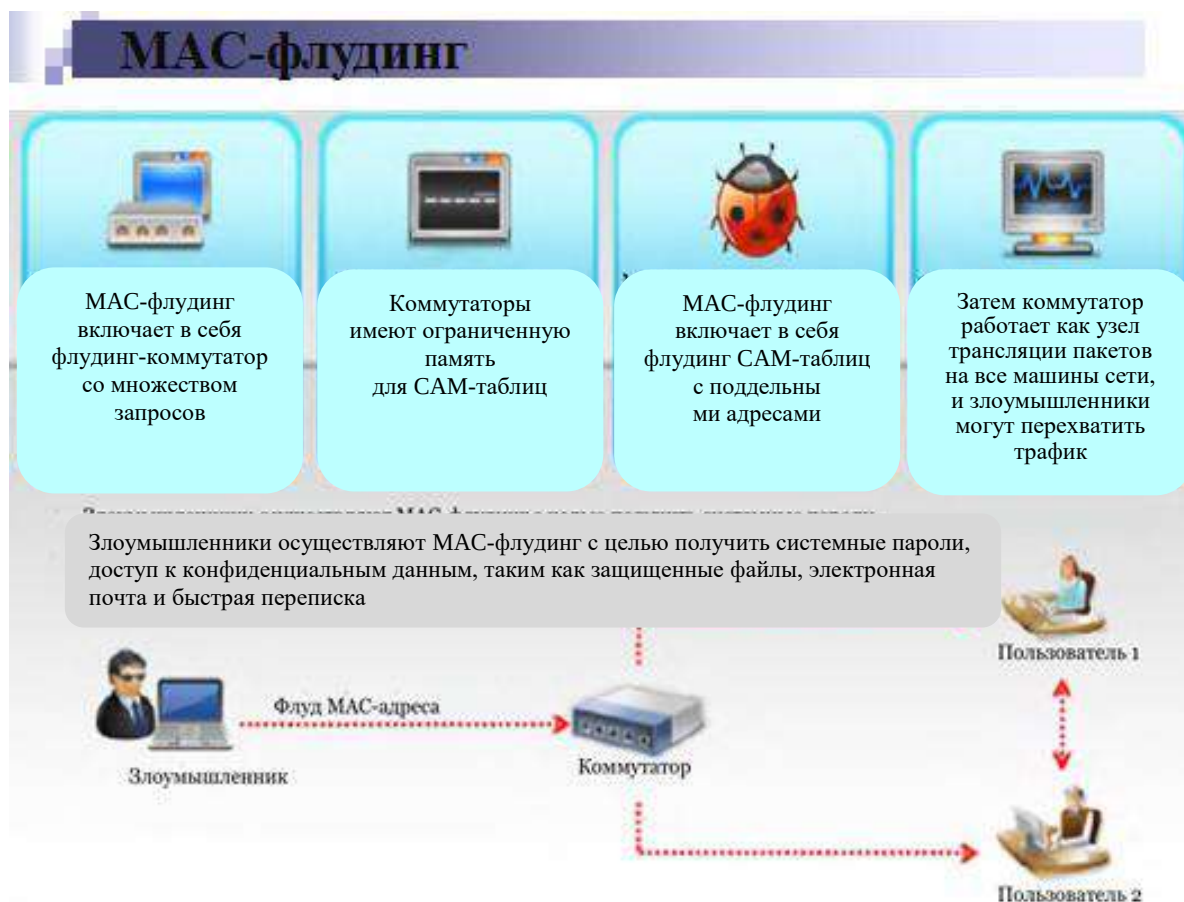


Таблица CAM – контент адресной таблицы памяти, который относится к динамической форме контента и используется с помощью коммутатора Ethernet. Коммутатор Ethernet поддерживает связи между портами. Таблица CAM отслеживает расположение путей MAC-адресов коммутатора

с ограниченным размером. Если таблица CAM флудится с MAC-адресами большего размера, то коммутатор становится концентратором. Таблица CAM работает таким образом, чтобы обеспечить доставку данных назначенному узлу.

Злоумышленники используют эту уязвимость в таблице CAM для sniffing сети передачи данных. Если атакующий имеет возможность подключения к общему коммутатору сегмента Ethernet, то он или она может легко перехватить данные.



Типичный MAC-flooding включает флудинг коммутатора с многочисленными запросами с поддельными исходными MAC-адресами. Проблем не возникает до тех пор, пока таблица MAC-адресов не будет заполнена. После того, как таблица MAC-адресов заполнится, любые дальнейшие запросы могут заставить коммутатор перейти в «failopen-режим».

Коммутатор в «failopen-режиме» действует как концентратор, транслирует данные для всех машин в сети.

Таким образом, злоумышленники могут легко перехватить трафик и могут украсть конфиденциальную информацию.

CAM-таблица заполненная поддельными MAC-адресами



Таблица CAM содержит информацию сети, такую как MAC-адреса, доступные на физических портах коммутатора и связанные с параметрами VLAN. Но эти CAM таблицы ограничены в размерах. С помощью MAC-flooding можно организовать нападение. MAC-flooding осуществляет бомбардировки коммутатора через поддельные исходные MAC-адреса до того, пока CAM таблица не заполнится. После того, как это будет сделано, коммутатор начинает флудить весь входящий трафик на всех портах. Затем коммутатор работает как концентратор, через который можно контролировать фреймы, передаваемые от хоста жертвы на другой хост без записи в CAM таблицы. Эта атака заполняет также CAM таблицы смежных коммутаторов.

DNCP в действии

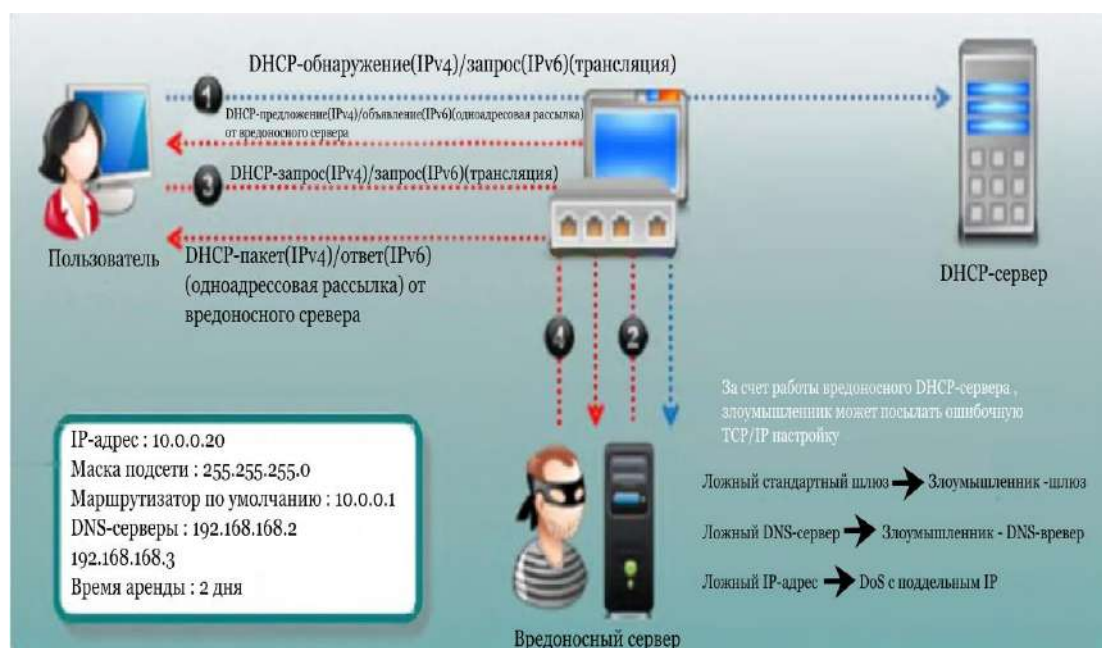


В атаках DHCP Starvation злоумышленник производит flooding DHCP-сервера, посылая большое количество DHCP-запросов и использует все доступные IP-адреса, которые DHCP-сервер может выдать.

В результате, сервер не может выдать больше никаких IP-адресов, что приводит к отказу в обслуживании (DoS атаке). Из-за этой проблемы действительные пользователи не могут получить или продлить их IP-адреса, и поэтому не имеют доступ к сети.

Злоумышленник передает DHCP запросы с поддельными MAC-адресами с помощью таких инструментов, как Gobbler.

DHCP-истощающая атака



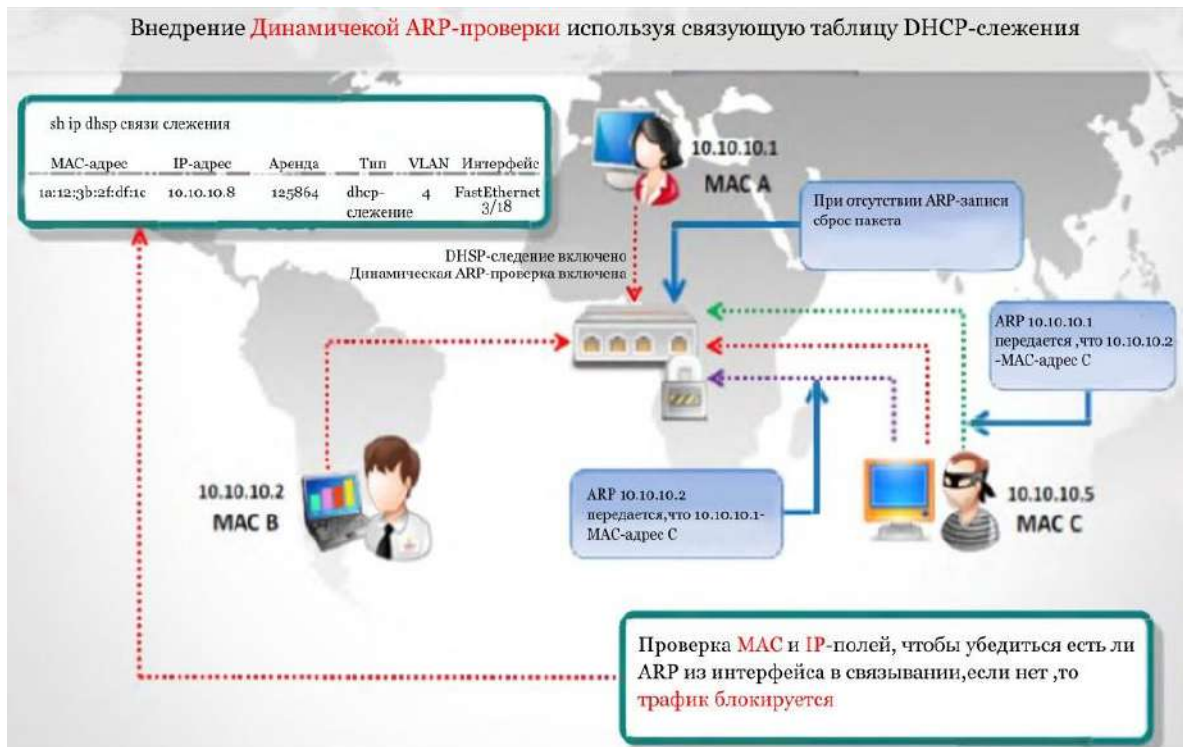
В атаках вредоносного DHCP-сервера, злоумышленник будет вводить вредоносный сервер в сеть. Этот сервер имеет способность реагировать на открытые DHCP-запросы клиентов. Хотя оба сервера отвечают на запрос, т.е. вредоносный сервер и реальный DHCP-сервер, сервер, который отвечает первым, выбирается клиентом. В случае, когда мошенник сервер дает ответ раньше, чем реальный сервер DHCP, клиент принимает ответ вредоносного сервера. Информация, предоставляемая клиентам этим вредоносным сервером, может нарушить их доступ к сети, в результате чего - DOS. Ответ DHCP от DHCP-сервера атакующего может присвоить IP-адрес злоумышленника в качестве шлюза клиента по умолчанию. В результате весь трафик от клиента будет отправлен на IP-адрес злоумышленника. Затем злоумышленник захватывает весь трафик и направляет этот трафик в соответствующий шлюз по умолчанию. С точки зрения клиента, вроде бы все работает правильно. Этот тип атаки не может быть обнаружен клиентом в течение длительного времени. Иногда клиент вместо стандартного DHCP-сервера использует вредоносный DHCP-сервер. Вредоносный сервер направляет клиента посетить поддельные веб-сайты с целью получения его данных.

Для смягчения атаки вредоносного DHCP-сервера установите интерфейс, к которому вредоносный сервер подключен как ненадежный. Это действие будет блокировать проникновению в DHCP-сервер сообщений от этого интерфейса.

Как защититься от DHCP-Starvation (мор) атаки и атаки вредоносного сервера



Как защититься от ARP-poisoning



ARP-poisoning-атаки могут быть предотвращены путем внедрения динамической проверки ARP (DAI). DAI - функция безопасности, которая позволяет проверить Address Resolution Protocol (ARP) пакетов в сети. Когда DAI включен в сеть VLAN, все порты на VLAN считаются ненадежными по умолчанию. DAI проверяет пакеты ARP, используя DHCP Snooping таблицы привязок. Следовательно, необходимо включить DHCP Snooping до включения DAI. Если вы включили DHCP Snooping после включения DAI, то никакой связи между VLAN у устройств не будет установлено на основе ARP. Следовательно, это может привести к добровольному отказу в обслуживании на любом устройстве в этом VLAN.

Для того чтобы проверить пакет ARP, DAI осуществляет обязательный осмотр привязки IP- и MAC-адреса, хранящейся в базе данных отслеживания DHCP перед передачей пакета в его пункт назначения. Если любая неправильная привязка IP- и MAC-адреса встречается, то DAI удаляет соответствующий ARP-пакет. Таким образом, исключается риск man-in-the-middle атак. DAI гарантирует, что только нормальные запросы и отклики ARP передадутся.

MAC-spoofing/дублирование



MAC дублирующая атака запускается перехватом MAC-адресов клиентов, которые активно связаны с портом коммутатора и повторно используют один из этих адресов.

Перехватывая трафик в сети, злоумышленник может перехватить и использовать MAC-адрес законного пользователя, чтобы получить весь трафик, предназначенный для пользователя.

Эта атака позволяет атакующему получить доступ к сети и присвоить себе чью-то личность уже в сети.

MAC дублирующая атака запускается перехватом MAC-адресов клиентов, которые активно связаны с портом коммутатора и повторно используют один из этих адресов.

Перехватывая трафик в сети, злоумышленник может перехватить и использовать MAC-адрес законного пользователя, чтобы получить весь трафик, предназначенный для пользователя.

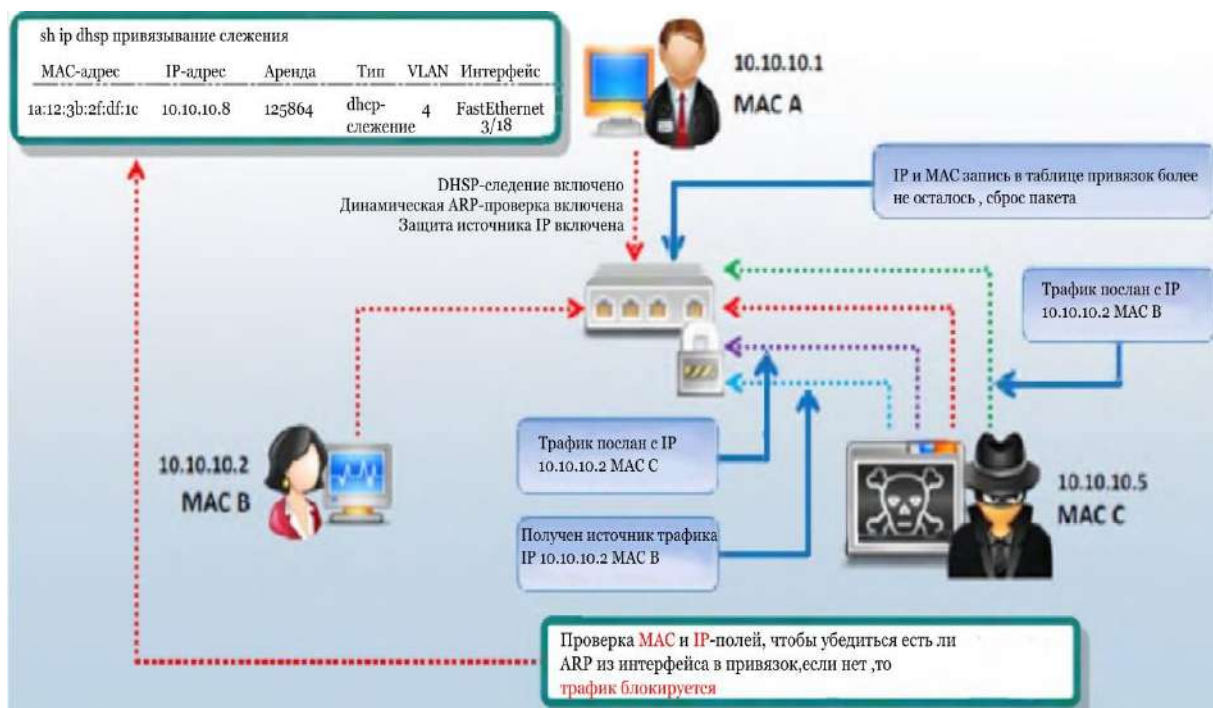
Эта атака позволяет атакующему получить доступ к сети и присвоить себе чью-то личность уже в сети.

Как защититься от spoofing-атаки

Выполнение оценки безопасности является основной целью хакера. «Этичные» хакеры выполняют различные нападения на сети или организации с целью поиска лазеек в архитектуре безопасности. Но на этом их работа не заканчивается. Поиск лазеек безопасности организации – второстепенная задача. Основной и важнейшей задачей этичного взлома является применение соответствующих контрмер к найденным лазейкам, чтобы их исправить.

После того как проверена сеть на MAC-spoofing атаки и обнаружены лазейки в безопасности, необходимо применить контрмеры для защиты сети против MAC-spoofing. Есть много контрмер для MAC-spoofing, которые

пригодны в различных ситуациях. В зависимости от архитектуры безопасности сети и найденных лазеек, возможно применить соответствующие контрмеры к сети. Лучший способ защиты от подделки MAC-адресов является размещение серверов позади маршрутизатора, т.к. маршрутизаторы зависят только от IP-адресов, в то время как переключатели зависят от MAC-адресов для коммуникации в сети. Настройка интерфейса безопасности портов – другой способ смягчить MAC-spoofing. После того, как команда безопасности порта включена, она позволяет указать MAC-адрес системы, подключенной к определенному порту. Она также позволяет задать действия, которые следует предпринять, если возникает нарушение безопасности порта.



Возможные методы для защиты от атак с подделкой адресов MAC:

- DHCP Snooping Binding Таблица: DHCP Snooping фильтрует ненадежные DHCP-сообщения и помогает строить и связывать DHCP-таблицы привязок. Эта таблица содержит MAC-адрес, IP-адрес, занимаемое время, типы связывания, номер VLAN и информационный интерфейс для соответствия с ненадежными интерфейсами переключателя. Он действует как брандмауэр между ненадежными узлами и DHCP-серверами. Это также помогает в дифференциации между надежными и ненадежными интерфейсами;
- функцию Dynamic ARP Inspection (проверка динамического ARP): она проверяет связи IP-адресов к MAC-адресам для каждого ARP-пакета в сети. Если какие-либо недействительные привязки найдены, то они будут отброшены на проверку динамического ARP;

- функция IP Source Guard: функция IP Source Guard является функцией безопасности, которая поможет вам ограничить трафик IP на ненадежном слое 2 портов путем фильтрации трафика на основе DHCP Snooping базу данных привязок. Это поможет вам избежать spoofing-атаку, когда атакующий пытается подменить или использовать IP-адрес другого хоста;
- кодировка: коммуникация должна быть зашифрована между точкой доступа и компьютером, чтобы избежать MAC-spoofing;
- извлечение MAC-адреса: вы всегда должны получать MAC-адреса непосредственно из сетевого адаптера вместо получения его из операционной системы.

DNS-poisoning



DNS (Domain Name Service) является протоколом, который переводит доменное имя (например, www.google.com) в IP-адрес (например, 8.8.8.8). Для поддержания DNS используются таблицы DNS, которые содержат имя домена и его эквивалент IP адрес, сохраненный в распределенной большой базе данных. DNS-poisoning, которая также называется DNS-spoofing, является атака, в которой злоумышленник пытается перенаправить жертву на вредоносный сервер вместо настоящего. Злоумышленник может совершить этот тип атаки, манипулируя записями таблицы DNS

в системе DNS. Предположим, жертва хочет получить доступ к веб-сайту ABC.com, злоумышленник манипулирует записями в таблице DNS таким образом, что жертва перенаправляется на сервер злоумышленника. Это может быть сделано путем изменения IP-адреса ABC.com на IP-адрес сервера злоумышленника. Таким образом, жертва подключается к серверу злоумышленника без ведома. После того, как жертва подключается к серверу злоумышленника, злоумышленник может скомпрометировать систему жертвы и украсть данные.

Аналогичным образом может быть поставлена под угрозу система путем проведения DNS-poisoning атак.

Интернет-DNS-spoofing



Для запуска DNS-poisoning атаки обычно выполняются следующие действия:

- 1) Устанавливается фальшивый веб-сайт на вашем компьютере.
- 2) Устанавливается treewalk, измените файл, упомянутый в readme.txt к вашему IP-адресу. Treewalk сделает вас DNS-сервером.
- 3) Изменяется файл DNS-spoofing.bat, замените IP-адрес на вашем компьютере.

4) Троянизируется файл DNS-spoofing.bat, отправьте его к Ребекке (например: chess.exe).

5) Когда хост нажмет файл с трояном, он заменит DNS-запись Ребекки в ее свойствах TCP / IP на соответствующую вашей машине.

6) DNS-сервер для Ребекки и ее DNS-запросы будут проходить через злоумышленника.

7) Когда Ребекка вводит XSECURITY, сайт, на который она перейдет - это поддельный сайт XSECURITY. Затем перехватывается пароль и отправляется на реальный сайт.

Есть четыре типа атак DNS-poisoning, с помощью которых вы можете поставить под угрозу систему:

- IntranetDNSspoofing (локальной сети);
- InternetDNSspoofing (удаленной сети);
- DNSpoisoningProxy-сервера;
- DNScachepoisoning.

Как видно из диаграммы, сначала атакующий отравляет маршрутизатор, запустив ARPSpoof / dnsspoof для того, чтобы перенаправлять DNS-запросы клиентов на машину злоумышленника. Когда клиент (Ребекка) посылает DNS-запрос к маршрутизатору, отравленный маршрутизатор посылает пакет DNS-запроса к машине злоумышленника. После получения DNS-запроса, злоумышленник посылает поддельные DNS-ответы, которые перенаправляют клиента на фальшивый сайт, созданный злоумышленником. Так как веб-сайт принадлежит атакующему, злоумышленник может увидеть всю информацию, представленную клиентом для этого сайта. Таким образом, злоумышленник может перехватить конфиденциальные данные, такие как пароли и т.д., представленные поддельному веб-сайту. После того, как злоумышленник получает необходимую информацию, он или она перенаправляет клиента на реальный сайт.

Лабораторные работы

Лабораторная работа № 1

Анализ защищенности протокола modbus TCP

1. Цель лабораторной работы

Целью лабораторной работы является изучение открытого коммуникационного протокола Modbus и проведение сетевой атаки на протокол.

В ходе выполнения лабораторной работы обучающиеся получают следующие основные навыки:

- выявление уязвимостей сетевых промышленных протоколов на примере протокола Modbus;
- подготовка полезной нагрузки для возможности списания определенного объема топлива;
- подготовка скрипта для проведения replay-атаки с использованием сформированной ранее полезной нагрузки.

Время выполнения работы – два академических часа.

2. Краткие теоретические сведения

Modbus – открытый коммуникационный протокол, основанный на архитектуре ведущий-ведомый (master-slave). Широко применяется в промышленности для организации связи между электронными устройствами. Может использоваться для передачи данных через последовательные линии связи RS-485, RS-422, RS-232, и сети TCP/IP (Modbus TCP, рис. 1).

ARP	00 WHO has 10.10.2.253? Tell 10.10.2.21
Modbus...	78 Query: Trans: 53524; Unit: 1, Func: 4: Read Input Registers
Modbus...	325 Response: Trans: 53524; Unit: 1, Func: 4: Read Input Registers
TCP	66 39995 → 502 [ACK] Seq=3349 Ack=72262 Win=1324 Len=0 TSval=128032355
ARP	60 Who has 10.10.2.253? Tell 10.10.2.21

Рис. 1. Пример Modbus TCP трафика

Обычно в сети есть только одно ведущее, так называемое, «главное» устройство, и несколько ведомых – «подчинённых» устройств. Главное устройство инициирует транзакции (передаёт запросы). Мастер может

адресовать запрос индивидуально любому подчиненному или инициировать передачу широковещательного сообщения для всех подчиненных устройств. Подчинённое устройство, опознав свой адрес, отвечает на запрос, адресованный именно ему. При получении широковещательного запроса ответ подчинёнными устройствами не формируется.

Спецификация Modbus описывает структуру запросов и ответов. Их основа – элементарный пакет протокола, так называемый PDU (Protocol Data Unit). Структура PDU не зависит от типа линии связи и включает в себя код функции и поле данных. Код функции кодируется однобайтовым полем и может принимать значения в диапазоне 1...127. Диапазон значений 128...255 зарезервирован для кодов ошибок. Поле данных может быть переменной длины (табл. 1). Размер пакета PDU ограничен 253 байтами.

Для передачи пакета по физическим линиям связи PDU помещается в другой пакет, содержащий дополнительные поля. Этот пакет носит название ADU (Application Data Unit). Формат ADU зависит от типа линии связи.

Следует обратить внимание, что поле контроля ошибок в Modbus TCP отсутствует, так как целостность данных обеспечивает TCP/IP-стек.

Таблица 1. Параметры таблиц данных модулей

Номер регистра	Адрес регистра	Тип	Название	Тип
1-9999	0000 до 270E	Чтение-запись	Discrete Output Coils	DO
10001-19999	0000 до 270E	Чтение	Discrete Input Contacts	DI
30001-39999	0000 до 270E	Чтение	Analog Input Registers	AI
40001-49999	0000 до 270E	Чтение-запись	Analog Output Holding Registers	AO

Рассмотрим пакет инициализации соединения (табл. 2).

Таблица 2. Инициализация Modbus TCP соединения

00 01	IDтранзакции (обычно – нули)
00 00	IDпротокола
00 06	Длина
01	Идентификатор юнита
04	Функция 4 – чтение входных регистров (см. Таблица 3)
10 00 00 7d	Данные

Таблица 3. Функции Modbus TCP соединения

Код функции	Что делает функция		Тип значения	Тип доступа
01 (0x01)	Чтение DO	Read Coil Status	Дискретное	Чтение
02 (0x02)	Чтение DI	Read Input Status	Дискретное	Чтение
03 (0x03)	Чтение АО	Read Holding Registers	16 битное	Чтение
04 (0x04)	Чтение АИ	Read Input Registers	16 битное	Чтение
05 (0x05)	Запись одного DO	Force Single Coil	Дискретное	Запись
06 (0x06)	Запись одного АО	Preset Single Register	16 битное	Запись
15 (0x0F)	Запись нескольких DO	Force Multiple Coils	Дискретное	Запись
16 (0x10)	Запись нескольких АО	Preset Multiple Registers	16 битное	Запись

Рассмотрим ответный пакет на создание соединения (рис. 2).

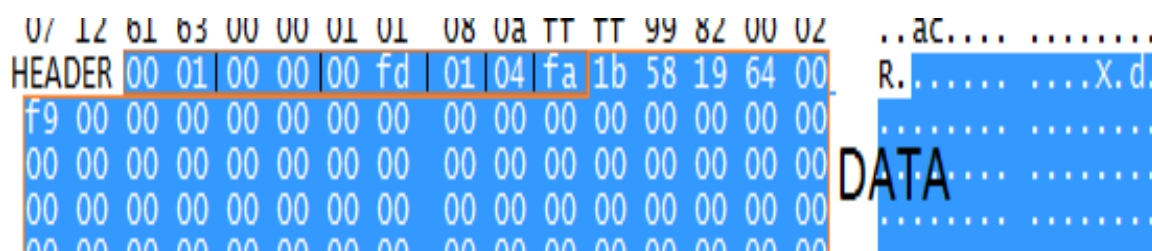


Рис. 2. Ответный Modbus TCP пакет

В пакете явно выделяются заголовок и блок данных (табл. 4)

Таблица 4. Ответный пакет Modbus TCP соединения

Заголовок	
«00 01»	Номер пакета в сессии
«00 00»	Функциональный код Function Code
«00 fd» = 253 байт	Длина
«01»	Идентификатор юнита
«04»	Функция 4 – чтение входных регистров
«fa» = 250 байт	Количество считанных байт
Блок данных	
«1b 58» = 7000	Значение 1
«19 64» = 6500	Значение 2
«00 f9» = 249	Значение 3

Описание стенда

Управление состоянием стенда осуществляется посредством переключения кнопки «Питание» в правом верхнем углу приложения (рис. 3).



Рис. 3. Стенд выключен (слева), стенд включен (справа)

Управление состоянием топливного склада осуществляется путем отправки запросов на заправку из топливного склада в левом нижнем углу приложения (рис. 4) нажатием на кнопку, соответствующую требуемому объему жидкости.



Рис. 4. Кнопки управления объемом топлива

3. Описание инструментария

Для выполнения работы потребуется анализатор сетевого трафика.

3.1. Утилита tcpdump является инструментом, позволяющим перехватывать и анализировать сетевой трафик, проходящий через компьютер, на котором запущена данная программа

Типичный вызов tcpdump выглядит следующим образом:

```
$ tcpdump -i $eth dst $ip and port $port
```

где:

- \$eth – это название интерфейса, от которого должна осуществиться отправка пакета;
- \$ip – это имя или IP-адрес сервера имен для запроса;
- \$port – это номер порта для подключения к серверу.

Параметры запроса:

- i интерфейс: Задаёт интерфейс, с которого необходимо анализировать трафик (без указания интерфейса – анализ «первого попавшегося»);
- n: Отключает преобразование IP в доменные имена. Если указано -nn, то запрещается преобразование номеров портов в название протокола;
- e: Включает вывод данных канального уровня (например, MAC-адреса);
- v: Вывод дополнительной информации (TTL, опции IP);
- s размер: Указание размера захватываемых пакетов (по умолчанию – пакеты больше 68 байт);
- w имя_файла: Задать имя файла, в который необходимо сохранять собранную информацию;
- r имя_файла: Чтение дампа из заданного файла;
- p: Захватывать только трафик, предназначенный данному узлу (по умолчанию – захват всех пакетов, например, в том числе широковещательных);
- q: Переводит tcpdump в «бесшумный режим», в котором пакет анализируется на транспортном уровне (протоколы TCP, UDP, ICMP), а не на сетевом (протокол IP);
- t: Отключает вывод меток времени.

Фильтрующие параметры tcpdump:

- dst хост: Проверяет, совпадает ли адрес получателя IP-пакета с указанным значением. Возможно, задавать как IP, подсеть в формате 10.0.0.1/24, так и имя хоста;
- src хост: Проверяет, совпадает ли адрес отправителя IP-пакета с указанным значением. Возможно, задавать как IP, подсеть в формате 10.0.0.1/24, так и имя хоста;
- host хост: Проверяет, совпадает ли адрес отправителя или получателя с заданным значением. Возможно, задавать как IP, подсеть в формате 10.0.0.1/24, так и имя хоста;
- net имя_сети: Проверяется, находится ли адрес отправителя/получателя в заданной сети. Возможно, указание сети в формате CIDR (например, 10.0.0.1/22) либо указание имени сети, заданной в файле /etc/networks;
- ip | arp | rarp | tcp | udp | icmp [хост]: Проверяет, принадлежит ли пакет одному из указанных протоколов, и при указании адреса хоста проверяет, совпадает ли адрес отправителя\получателя с заданным. Возможно, задавать как IP, подсеть в формате 10.0.0.1/24, так и имя хоста;
- [tcp | udp] dst port номер_порта: Проверяется, принадлежит ли пакет протоколу TCP/UDP и равен ли порт назначения заданному. Можно указать номер порта либо имя, заданное в файле /etc/services;

- [tcp | udp] src port номер_порта: Проверяется, принадлежит ли пакет протоколу TCP/UDP и равен ли порт источника заданному. Можно указать номер порта либо имя, заданное в файле /etc/services;
- [tcp | udp] port номер_порта: Проверяется, принадлежит ли пакет протоколу TCP/UDP и равен ли порт назначения или источника заданному. Можно указать номер порта либо имя, заданное в файле /etc/services;
- ip broadcast: Проверяется, является ли IP-пакет широковещательным;
- ether { src | dst | host } MAC_адрес: Проверяется, принадлежит ли сетевой пакет источнику, назначению, источнику или назначению, имеющему заданный MAC-адрес;
- ether broadcast: Проверяется, является ли ARP-пакет широковещательным.

Пример использования:

1) Вывод сетевой статистики с интерфейса ppp0 без преобразования IP в DNS тех фреймов, у которых MAC-адрес источника равен 11:20:b3:d8:d8:2c:

```
$ tcpdump -n -I ppp0 ether src 11:20:b3:d8:d8:2c.
```

2) Вывод широковещательного трафика с интерфейса vlan0:

```
$ tcpdump -n -e -I vlan0 ether broadcast.
```

3) Фильтровать сетевые пакеты, где IP-адрес указан как источник или как получатель пакета:

```
$ tcpdump -n -I eth0 host 192.168.66.1.
```

4) Фильтровать сетевые пакеты, где IP-адрес указан как источник пакета:

```
$ tcpdump -n -I eth0 src 192.168.66.1.
```

5) Сохранение сетевых пакетов с интерфейса «eth0» в файл «capture.pcap» по пути «/var/tmp»:

```
$ tcpdump -ni eth0 -s0 -w /var/tmp/capture.pcap.
```

3.2. Утилита Wireshark

Wireshark является программой-анализатором трафика для компьютерных сетей Ethernet и некоторых других. Имеет графический пользовательский интерфейс.

Функциональность, которую предоставляет Wireshark, очень схожа с возможностями программы tcpdump, однако Wireshark имеет графический пользовательский интерфейс и гораздо больше возможностей по сортировке и фильтрации информации. Программа позволяет пользователю просматривать весь проходящий по сети трафик в режиме реального времени, переводя сетевую карту в неразборчивый режим (promiscuous mode).

3.3. Утилита python

Для выполнения лабораторной работы достаточно воспользоваться предварительно созданным скриптом на языке Python, в который необходимо будет внести изменения на основе данных, полученных в течение работы. Поля «ip» и «port» должны быть заполнены данными удаленной машины, к которой будет осуществлено подключение. Поле «payload» должно быть заполнено данными, необходимыми для проведения атаки на протокол.

```
import socket
ip = "127.0.0.1"
port = 65535
payload = '\x00\x00\x00\x00'

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect((ip, port))
s.send(payload)
```

4. Используемое методическое и лабораторное обеспечение

1) Виртуальная машина «KP_ASU_SCADA_SRV» с установленной ОС Ubuntu Linux 3.19.0, содержащая в себе ПО клиентской части станда АСУ ТП (интерфейс SCADA) с использованием протокола Modbus.

2) Виртуальная машина «KP_ASU_PLC_1» с установленной ОС Linux Debian 3.2.68, содержащая в себе ПО серверной части станда АСУ ТП (эмуляция ПЛК) с использованием протокола Modbus.

3) Виртуальная машина обучаемого с установленной ОС Kali Linux, содержащая в себе следующее программное обеспечение: tcpdump, wireshark, python 2.7.

5. Порядок выполнения работы

Лабораторная работа состоит из нескольких заданий. Задача лабораторной работы – собрать ключевую информацию (указана в задании) из сетевого трафика, проанализировать его, найти возможность выполнения вектора атаки на проприетарный сетевой протокол и сформировать отчет по проведенной атаке.

5.1. Ход работы

- 1) Подключиться к клиентской виртуальной машине обучающегося. Логин – root, пароль – qwe123!@#.
- 2) В утилите Wireshark, используя синтаксис утилиты tcpdump, для записанного между клиентом и сервером образца трафика, определить функции, используемые в течение сетевого взаимодействия компонентов сети.
- 3) На основе полученной информации необходимо сформировать собственный пакет, который позволит установить значение воды в баке равным необходимому в задании. Значение можно отслеживать, подключившись к удаленной машине «zero-rel» в левой верхней части приложения (рис. 5).



Рис. 5. Уровень топлива в интерфейсе

5.2. Завершение работы

Выключить виртуальные машины «KP_ASU_SCADA_SRV», «KP_ASU_PLC_1».

6. Содержание отчёта о выполненной работе

В отчёте о выполненной лабораторной работе необходимо указать в виде таблицы найденную ключевую информацию.

6.1. Пример задания

- 1) Подключиться к клиентской виртуальной машине обучающегося.
- 2) В утилите Wireshark, используя синтаксис утилиты tcpdump, для записанного между клиентом и сервером образца трафика, определить функции, используемые в течение сетевого взаимодействия компонентов сети.
- 3) На основе полученной информации необходимо сформировать собственный пакет, который позволит установить значение воды в баке равным необходимому в задании.

6.2. Пример отчета

Отчет может выполняться как на компьютере, так и на бумажном носителе в зависимости от требований преподавателя.

№	Задание	Значение
1	Получение номера и названия функции записи протокола Modbus	
2	Написание полезной нагрузки	
3	Написание и эксплуатация Python-скрипта с полезной нагрузкой, получение нового значения объема топлива	

7. Контрольные вопросы

- 1) Объясните основную концепцию протокола Modbus.
- 2) Назовите причину возможности проведения атаки на протокол.
- 3) Предложите решения, позволяющие устранить возможность атаки на протокол.

8. Бланк отчета

8.1. Задание

- 1) Подключиться к клиентской виртуальной машине обучающегося.
- 2) В утилите Wireshark, используя синтаксис утилиты tcpdump, для записанного между клиентом и сервером образца трафика, определить функции, используемые в течение сетевого взаимодействия компонентов сети.
- 3) На основе полученной информации необходимо сформировать собственный пакет, который позволит установить значение воды в баке равным необходимому в задании.

8.2. Ответы

№	Задание	Значение
1	Получить номер и название функции записи протокола Modbus	
2	Написать полезную нагрузку	
3	Написать и выполнить Python-скрипт с полезной нагрузкой для получения нового значения объема топлива	

Лабораторная работа № 2

Анализ защищенности программируемого логического контроллера (ПЛК)

1. Цель лабораторной работы

Целью лабораторной работы является изучение методов анализа сети и атака перебором с использованием словаря.

В ходе выполнения лабораторной работы обучающиеся получают следующие основные навыки:

- навыки подключения к АСУ ТП различными способами;
- работа с языком Python для решения задачи перебора пароля с использованием словаря.

Время выполнения работы – два академических часа.

2. Краткие теоретические сведения

Атака полным перебором (bruteforce) – метод атаки, использующий перебор всех возможных в пределах данного набора символов последовательностей для решения задачи. Как правило, используется для неправомерной аутентификации.

Атака является самым простым и универсальным способом получения неправомерного доступа, однако, в зависимости от мощности алфавита перебираемого сообщения и длины сообщения, перебор может занимать огромное количество времени.

Например, при алфавите мощностью равной 36, длине сообщения в 10 символов и скорости перебора равной 100000 сообщений в секунду, перебор займет 1162 года.

По причине того, что атака может не принести результата в необходимые сроки, она используется в нескольких случаях:

1) Вместе со словарем – набором популярных пользовательских паролей, которые перебираются вместо генерируемого набора случайных символов. Этот способ использования атаки полным перебором будет использоваться в данной работе.

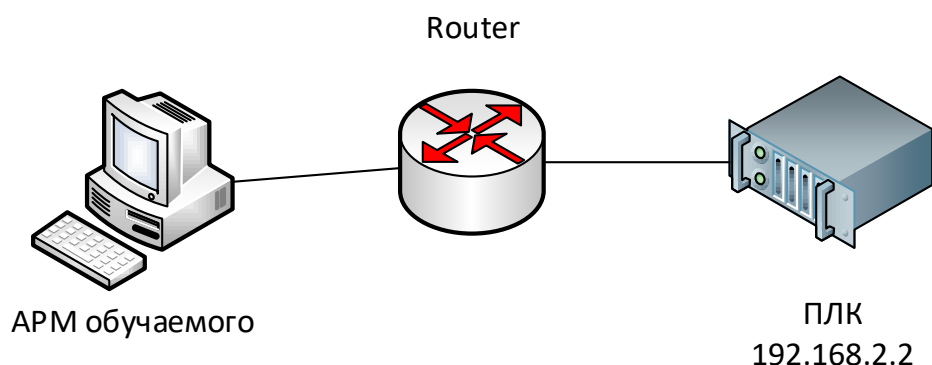
2) Если заведомо известно, что перебор сообщений займет приемлемое для атакующего время.

Python – высокоуровневый язык программирования общего назначения, ориентированный на повышение производительности разработчика и читаемости кода. Синтаксис ядра Python минималистичен. В то же время стандартная библиотека включает большой объем полезных функций.

Python по причине невысокой сложности в освоении и приемлемой скорости работы имеет популярность, как язык написания скриптов вредоносной направленности. Скрип, написанный на Python, будет использоваться в данной работе.

Предполагается, что обучаемый самостоятельно нашел скрипт и адаптировал его для своих нужд, что является близким к жизни сценарием.

2.1. Схема стенда



3. Инструментарий

Terminal – это приложение, внутри которого выполняется командный интерпретатор. Его еще часто называют интерфейсом командной строки. Он интерпретирует команды специального языка скриптов.

По умолчанию используется командный интерпретатор Bash. Это улучшенный вариант интерпретатора Bourne Shell, который обычно называют просто «Shell». В настоящее время Bash – фактически стандарт де-факто в большинстве Unix-подобных систем.

```
root@kali-template:~# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.4.89 netmask 255.255.240.0 broadcast 10.10.15.255
    inet6 fe80::250:56ff:fe9f:61f4 prefixlen 64 scopeid 0x20<link>
    ether 00:50:56:9f:61:f4 txqueuelen 1000 (Ethernet)
    RX packets 332 bytes 32533 (31.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 35 bytes 3223 (3.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Рис. 6. Скриншот работы Terminal

Работа с приложением реализована с помощью ввода команд в окно терминала.

Командная строка начинается с пользователя (root), после «@» следует его имя (kali-template), затем следует название текущего каталога –

по умолчанию открывается домашний каталог пользователя, который в Unix-системах обозначается знаком «~» (тильда). Далее следует знак «#», который называется приглашением – приглашением вводить команды интерпретатору.

Формат команд:

[команда] [аргументы ...]

Примеры основных команд:

- Определение текущей директории

pwd;

- Смена директории

cd [путь];

В частности:

cd .. – сменит директорию на вышестоящую над текущей,

cd / – сменит директорию на корневую,

cd ~ – переместит в домашнюю папку,

- Отображение всех файлов и директорий в текущей директории

ls [опции] [файл];

- Поиск файла или директории по имени. Команда поддерживает регулярные выражения

find [директория начала поиска] [опции];

Пример:

find. -type d -name *cookie* – поиск, начиная с текущей директории, исключительно папок, в названии которых содержится «cookie»;

- Поиск файла по его содержимому

grep [опции] [путь];

- Удаление файла

rm [опции] [путь];

- Чтение файла, объединение файлов, создание файла

cat [опции] [путь];

- Вывод списка работающих процессов

ps [опции];

- Задание приоритета процессу

nice [опции] [ID процесса].

Также, работая с терминалом, необходимо знать о функциях некоторых клавиш:

- Дозаполнение названия файла или директории. При введении нескольких букв нажмите Tab, чтобы набор был завершен автоматически;

- Остановка текущего процесса

Ctrl+C;

- Перемещение по истории введенных команд

↑ и ↓.

Nmap (NetworkMapper) – свободная утилита, предназначенная для разнообразного настраиваемого сканирования IP-сетей с любым коли-

чеством объектов, определения состояния объектов сканируемой сети (портов и соответствующих им служб).

Часто используется для анализа сетей с целью обнаружения уязвимых мест – открытых портов и др.

Формат команд:

`nmap [тип сканирования] [опции] [цель сканирования]`.

Пример команды:

– Сканирование первых 1024 портов первой половины из всех доступных подсетей адресного пространства 10.10.

`nmap -p 1-1024 10.10.0-255.0-127.`

4. Используемое методическое и лабораторное обеспечение

1) Виртуальная машина «KP_ASU_PLC_1» с установленной ОС Linux Debian 3.2.68, содержащей в себе ПО серверной части станда АСУ ТП (эмуляция ПЛК) с использованием протокола Modbus.

2) Виртуальная машина обучаемого с установленной ОС Kali Linux, содержащей в себе следующее программное обеспечение: tcpdump, wireshark, python 2.7.

5. Порядок выполнения работы

Лабораторная работа состоит из нескольких заданий. Задача лабораторной работы – собрать необходимые сведения (указана в задании) с помощью различных инструментов, проанализировать их, использовать собранную информацию для эксплуатации уязвимостей и сформировать отчет, содержащий полученные сведения.

5.1. Ход работы

- 1) Обучающиеся должны просканировать порты ПЛК.
- 2) Обучающимся надо проверить реакцию порта на попытку подключения.
- 3) Обучающиеся должны написать на Python скрипт для атаки перебором.

5.2. Завершение работы

Выключить виртуальную машину «KP_ASU_PLC_1».

6. Содержание отчёта о выполненной работе

В отчёте о выполненной лабораторной работе необходимо указать данные в виде таблиц с заполненными значениями.

6.1. Пример задания

- | |
|---|
| 1) Обнаружить открытый порт ПЛК.
2) Подключиться к 9108 порту.
3) Подобрать пароль с помощью скрипта и словаря. |
|---|

6.2. Пример отчета

Отчет может выполняться как на компьютере, так и на бумажном носителе в зависимости от требований преподавателя.

№	Задание	Значение
1	Обнаружить открытый порт ПЛК	
2	Подключиться к 9108 порту	
3	Подобрать пароль с помощью скрипта и словаря.	

7. Контрольные вопросы

- 1) Укажите ключевую слабость атаки полным перебором.
- 2) Назовите популярные словари, используемые для проведения атаки полным перебором.
- 3) На каком уровне модели OSI работает используемый скрипт? Почему? (Ответить на примере исходного кода.)
- 4) Для чего в скрипте используется проверка на пустую строку? Можно ли избежать этой проверки?

8. Бланк отчета

8.1. Задание

- | |
|---|
| 1) Обнаружить открытый порт ПЛК.
2) Подключиться к 9108 порту.
3) Подобрать пароль с помощью скрипта и словаря. |
|---|

8.2. Ответы

№	Задание	Значение
1	Обнаружить открытый порт ПЛК	
2	Подключиться к 9108 порту	
3	Подобрать пароль с помощью скрипта и словаря.	

Лабораторная работа № 3

Анализ защищенности scada-сервера

1. Цель лабораторной работы

Целью лабораторной работы является изучение способов поиска возможности удаленного подключения к серверу, а также анализ режимов шифрования для дальнейшего нелегитимного получения пароля.

В ходе выполнения лабораторной работы обучающиеся получают следующие основные навыки:

- навыки подключения к АСУ ТП различными способами;
- навыки выявления слабых режимов шифрования;
- работа со специальным программным обеспечением для выполнения анонимных подключений типа reverse_tcp.

Время выполнения работы – два академических часа.

2. Краткие теоретические сведения

ECB (Electronic Code Book) – это режим шифрования, при котором исходное сообщение делится на блоки длины k , и каждый блок последовательно и независимо шифруется с использованием одного и того же ключа.

Шифрование:

Пусть дано сообщение P (открытый текст, последовательность бит, данные).

Во время шифрования выполняются следующие действия:

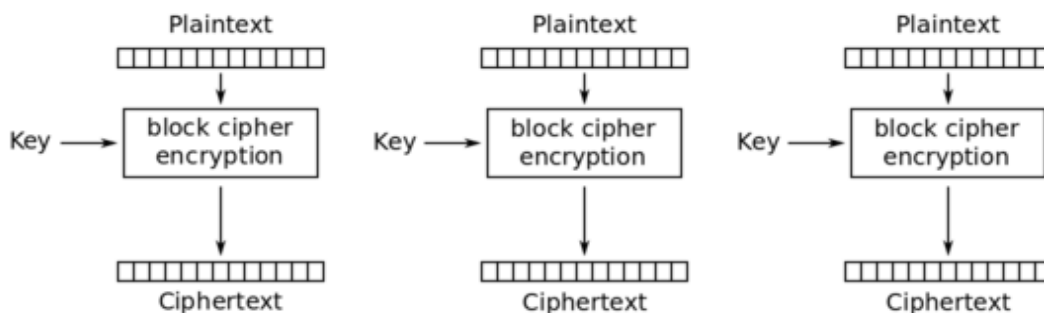


Рис. 7. Режим шифрования «ECB»

Сообщение делится на блоки одинакового размера. Размер (длина) блока равен n и измеряется в битах. В результате получается последовательность блоков $P_1, P_2, P_3... P_q$. Последний блок при необходимости дополняется до длины n .

Каждый блок P_i шифруется алгоритмом шифрования E_k с использованием ключа k :

$$C_i = E_k(P_i, k),$$

где:

i – номер блока;

k – ключ;

P_i – блок сообщения (открытый текст);

C_i – зашифрованный блок (шифротекст);

E_k – функция, выполняющая блочное шифрование.

В результате получают зашифрованные блоки $C_1, C_2, C_3 \dots C_q$.

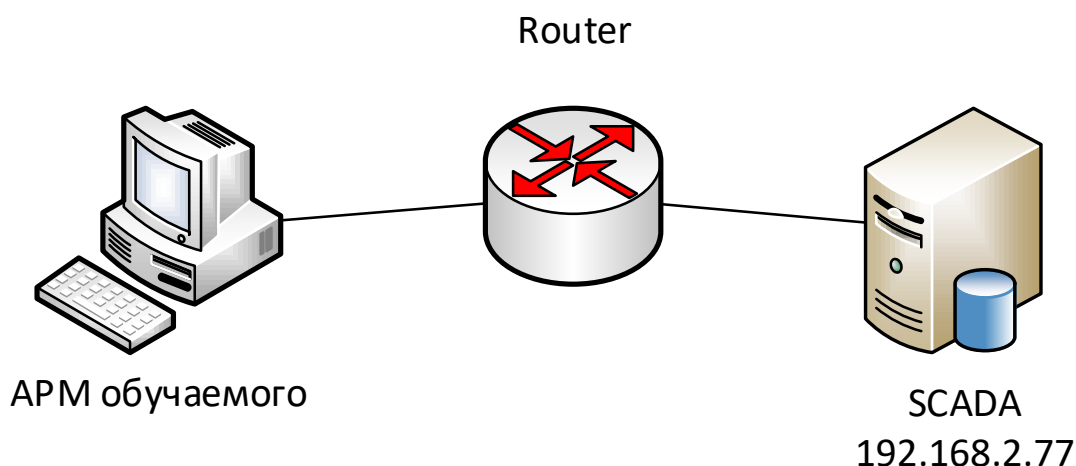
Расшифровка:

выполняется функцией D_k с использованием того же ключа k :

$$C_i = E_k(P_i, k).$$

Недостатком ЕСВ является сохранение статистических особенностей открытого текста.

2.1. Схема стенда



2.2. Инструментарий

Terminal – это приложение, внутри которого выполняется командный интерпретатор. Его еще часто называют интерфейсом командной строки. Он интерпретирует команды специального языка скриптов.

По умолчанию используется командный интерпретатор Bash. Это улучшенный вариант интерпретатора Bourne Shell, который обычно называют просто «Shell». В настоящее время Bash – фактически стандарт де-факто в большинстве Unix-подобных систем.

```
root@kali-template:~# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.4.89 netmask 255.255.240.0 broadcast 10.10.15.255
    inet6 fe80::250:56ff:fe9f:61f4 prefixlen 64 scopeid 0x20<link>
    ether 00:50:56:9f:61:f4 txqueuelen 1000 (Ethernet)
    RX packets 332 bytes 32533 (31.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 35 bytes 3223 (3.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Рис. 8. Скриншот работы Terminal

Работа с приложением реализована с помощью ввода команд в окно терминала.

Командная строка начинается с пользователя (root), после «@» следует его имя (kali-template), затем следует название текущего каталога – по умолчанию открывается домашний каталог пользователя, который в Unix-системах обозначается знаком «~» (тильда). Далее следует знак «#», который называется приглашением – приглашением вводить команды интерпретатору.

Формат команд:

[команда] [аргументы ...]

Примеры основных команд:

- Определение текущей директории

pwd;

- Смена директории

cd [путь];

В частности:

cd .. – сменит директорию на вышестоящую над текущей,

cd / – сменит директорию на корневую,

cd ~ – переместит в домашнюю папку;

- Отображение всех файлов и директорий в текущей директории

ls [опции] [файл];

- Поиск файла или директории по имени. Команда поддерживает регулярные выражения

find [директория начала поиска] [опции];

Пример:

find. -type d -name *cookie* – поиск, начиная с текущей директории, исключительно папок, в названии которых содержится «cookie»;

- Поиск файла по его содержимому

grep [опции] [путь];

- Удаление файла
rm [опции] [путь];
- Чтение файла, объединение файлов, создание файла
cat [опции] [путь];
- Вывод списка работающих процессов
ps [опции];
- Задание приоритета процессу
nice [опции] [ID процесса].

Также, работая с терминалом, необходимо знать о функциях некоторых клавиш:

Дозаполнение названия файла или директории. При введении нескольких букв нажмите Tab, чтобы набор был завершен автоматически;

- Остановка текущего процесса
Ctrl+C;
- Перемещение по истории введенных команд
↑ и ↓.

Nmap (NetworkMapper) – свободная утилита, предназначенная для разнообразного настраиваемого сканирования IP-сетей с любым количеством объектов, определения состояния объектов сканируемой сети (портов и соответствующих им служб).

Часто используется для анализа сетей с целью обнаружения уязвимых мест – открытых портов и др.

Формат команд:

nmap [тип сканирования] [опции] [цель сканирования].

Пример команды:

- Сканирование первых 1024 портов первой половины из всех доступных подсетей адресного пространства 10.10.

nmap -p 1-1024 10.10.0-255.0-127.

Wireshark – программа-анализатор трафика для компьютерных сетей Ethernet и некоторых других. Имеет графический пользовательский интерфейс. Программа позволяет пользователю просматривать весь проходящий по сети трафик в режиме реального времени, переводя сетевую карту в неразборчивый режим (promiscuous mode).

Функционал Wireshark включает в себя «прослушивание» сети, возможность экспорта медиа-информации и др.

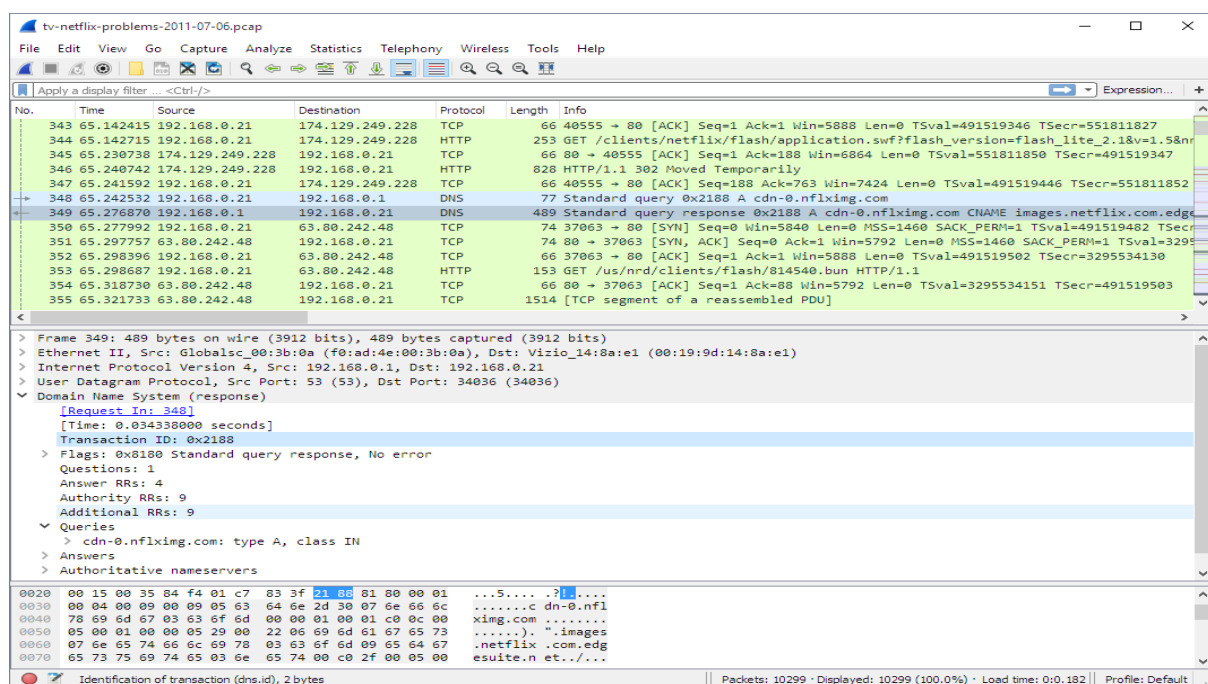


Рис. 9. Скриншот работы Wireshark

netcat – утилита Unix, позволяющая устанавливать соединения TCP и UDP, принимать оттуда данные и передавать их. Несмотря на свою полезность и простоту, данная утилита не входит ни в какой стандарт (например, POSIX).

Формат команд:

nc [опции] [IP хоста] [порт].

Ключи:

- h – Справка; ничего не делается;
- v – Дополнительная диагностика (verbose);
- o – выходной файл. Выводить дампы данных;
- i – Задержка между отправляемыми данными (в секундах);
- t – Совместимость с Telnet;
- z – Не посылать данные (сканирование портов);
- u – Подключаться по UDP (вместо TCP);
- l – Пассивный режим (прослушивание порта);
- p – Локальный номер порта (для -l);
- s – Использовать заданный локальный («свой») IP-адрес;
- n – Отключить DNS и поиск номеров портов по /etc/services;
- w – Задать тайм-аут (в секундах);
- q – Задать время ожидания после EOF на входе (в секундах);
- e – Запустить указанную программу для обмена данных с сетью (вместо стандартных ввода и вывода);
- c – То же, в виде команды для /bin/sh.

3. Используемое методическое и лабораторное обеспечение

1) Виртуальная машина «KP_ASU_SCADA_SRV» с установленной ОС Ubuntu Linux 3.19.0, содержащая в себе ПО клиентской части стенда АСУ ТП (интерфейс SCADA) с использованием протокола Modbus.

2) Виртуальная машина обучаемого с установленной ОС Kali Linux, содержащая в себе следующее программное обеспечение: tcpdump, wireshark, python 2.7.

4. Порядок выполнения работы

Лабораторная работа состоит из нескольких заданий. Задача лабораторной работы – собрать необходимые сведения (указана в задании) с помощью различных инструментов, проанализировать их, использовать собранную информацию для эксплуатации уязвимостей и сформировать отчет, содержащий полученные сведения.

4.1. Ход работы

- 1) Подключиться к виртуальной машине «KP_ASU_SCADA_SRV».
- 2) Найти открытый порт удаленного сервера.
- 3) Подключиться к открытому порту, совершить попытку аутентификации.
- 4) Определить ключ генерации пароля нового пользователя.
- 5) Определить пароль администратора сервера.
- 6) Получить IP-адрес SCADA-сервера с помощью netcat.

4.2. Завершение работы

Выключить виртуальную машину «KP_ASU_SCADA_SRV».

5. Содержание отчёта о выполненной работе

В отчёте о выполненной лабораторной работе необходимо указать данные в виде таблиц с заполненными значениями.

5.1. Пример задания

- | |
|---|
| <ol style="list-style-type: none">1) Подключиться к виртуальной машине «KP_ASU_SCADA_SRV».2) Найти открытый порт удаленного сервера.3) Подключиться к открытому порту, совершить попытку аутентификации.4) Определить ключ генерации пароля нового пользователя.5) Определить пароль администратора сервера.6) Получить IP-адрес SCADA-сервера с помощью netcat. |
|---|

5.2. Пример отчета

Отчет может выполняться как на компьютере, так и на бумажном носителе в зависимости от требований преподавателя.

№	Задание	Значение
1	Найти открытый порт удаленного сервера	
2	Подключиться к порту, совершить попытку авторизации и регистрации.	
3	Определить длину ключа шифра	
4	Определить пароль администратора	
5	Получить IP необходимый для завершения аутентификации	
6	Запустить generator	

6. Контрольные вопросы

- 1) Назовите достоинства режима ЕСВ.
- 2) Назовите недостатки ЕСВ.

7. Бланк отчета

7.1. Задание

1) Подключиться к виртуальной машине «KP_ASU_SCADA_SRV».
2) Найти открытый порт удаленного сервера.
3) Подключиться к открытому порту, совершить попытку аутентификации.
4) Определить ключ генерации пароля нового пользователя.
5) Определить пароль администратора сервера.
6) Получить IP-адрес SCADA-сервера с помощью netcat.

7.2. Ответы

№	Задание	Значение
1	Найти открытый порт удаленного сервера	
2	Подключиться к порту, совершить попытку авторизации и регистрации.	
3	Определить длину ключа шифра	
4	Определить пароль администратора	
5	Получить IP необходимый для завершения аутентификации	
6	Запустить generator	

Лабораторная работа № 4

Анализ защищенности log-серверов

1. Цель лабораторной работы

Целью лабораторной работы является изучение методов анализа сети и атака перебором с использованием словаря.

В ходе выполнения лабораторной работы, обучающиеся получают следующие основные навыки:

- навыки проведения атаки типа «Path Traversal»;
- навыки работы со специальным программным обеспечением для проведения сетевых атак;
- навыки осуществления анонимного сетевого подключения типа «reverse_tcp».

Время выполнения работы – два академических часа.

2. Краткие теоретические сведения

Path Traversal – атака, направленная на несанкционированное получение доступа к директории, к которой атакующий не имеет доступа, из директории, к которой он имеет доступ.

Это осуществляется, например, манипуляциями с содержимым адресной строки (в веб-интерфейсе), или с содержимым команды перехода в unix-оболочках.

Один из вариантов PathTraversal – введение в адресную строку адреса директории, к которой у атакующего есть доступ, затем использование специальных символов для перехода в директорию более высокого уровня (необходимого для получения доступа к требуемой директории), и далее написание адреса искомой директории.

При этом сервер может быть сконфигурирован таким образом, чтобы предотвращать Path Traversal путем фильтрации адресной строки.

Пусть атакующий имеет доступ к директории /home, а ему нужно попасть в директорию /etc, сервер находится по адресу: 192.168.2.222.

Варианты манипуляций с адресной строкой:

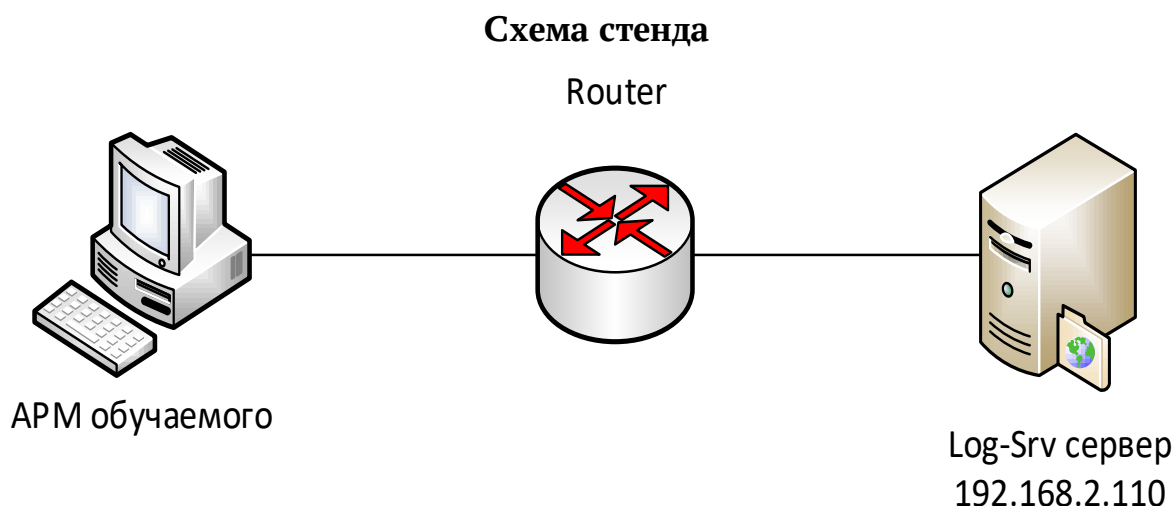
1) 192.168.2.222/home/./etc

2) 192.168.2.222/home/%2e%2e/etc

%2e: «2e» – номер символа «.» в таблице ASCII

3) 192.168.2.222/home/%252e%252e/etc

%252e: «25» – номер символа «%» в таблице ASCII



3. Инструментарий

Terminal – это приложение, внутри которого выполняется командный интерпретатор. Его еще часто называют интерфейсом командной строки. Он интерпретирует команды специального языка скриптов.

По умолчанию используется командный интерпретатор Bash. Это улучшенный вариант интерпретатора Bourne Shell, который обычно называют просто «Shell». В настоящее время Bash – фактически стандарт де-факто в большинстве Unix-подобных систем.

```
root@kali-template:~# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.4.89 netmask 255.255.240.0 broadcast 10.10.15.255
    inet6 fe80::250:56ff:fe9f:61f4 prefixlen 64 scopeid 0x20<link>
    ether 00:50:56:9f:61:f4 txqueuelen 1000 (Ethernet)
    RX packets 332 bytes 32533 (31.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 35 bytes 3223 (3.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Рис. 10. Скриншот работы Terminal

Работа с приложением реализована с помощью ввода команд в окно терминала.

Командная строка начинается с пользователя (root), после «@» следует его имя (kali-template), затем следует название текущего каталога – по умолчанию открывается домашний каталог пользователя, который в Unix-системах обозначается знаком «~» (тильда). Далее следует знак «#», который называется приглашением – приглашением вводить команды интерпретатору.

Формат команд:

[команда] [аргументы ...]

Примеры основных команд:

– Определение текущей директории

pwd;

– Смена директории

cd [путь];

В частности:

cd .. – сменит директорию на вышестоящую над текущей,

cd / – сменит директорию на корневую,

cd ~ – переместит в домашнюю папку;

– Отображение всех файлов и директорий в текущей директории

ls [опции] [файл];

– Поиск файла или директории по имени. Команда поддерживает регулярные выражения

find [директория начала поиска] [опции];

Пример:

find. -type d -name *cookie* – поиск, начиная с текущей директории, исключительно папок, в названии которых содержится «cookie»;

– Поиск файла по его содержимому

grep [опции] [путь];

– Удаление файла

rm [опции] [путь];

– Чтение файла, объединение файлов, создание файла

cat [опции] [путь];

– Вывод списка работающих процессов

ps [опции];

– Задание приоритета процессу

nice [опции] [ID процесса].

Также, работая с терминалом, необходимо знать о функциях некоторых клавиш:

Дозаполнение названия файла или директории. При введении нескольких букв нажмите Tab, чтобы набор был завершен автоматически;

– Остановка текущего процесса

Ctrl+C;

– Перемещение по истории введенных команд

↑ и ↓.

netcat – утилита Unix, позволяющая устанавливать соединения TCP и UDP, принимать оттуда данные и передавать их. Несмотря на свою полезность и простоту, данная утилита не входит ни в какой стандарт (например, POSIX).

Формат команд:

nc [опции] [IP хоста] [порт].

Ключи:

– h – Справка; ничего не делается;

- v – Дополнительная диагностика (verbose);
- o – Выходной файл. Выводить дампы данных;
- i – Задержка между отправляемыми данными (в секундах);
- t – Совместимость с Telnet;
- z – Не посылать данные (сканирование портов);
- u – Подключаться по UDP (вместо TCP);
- l – Пассивный режим (прослушивание порта);
- p – Локальный номер порта (для -l);
- s – Использовать заданный локальный («свой») IP-адрес;
- n – Отключить DNS и поиск номеров портов по /etc/services;
- w – Задать тайм-аут (в секундах);
- q – Задать время ожидания после EOF на входе (в секундах);
- e – Запустить указанную программу для обмена данных с сетью (вместо стандартных ввода и вывода);
- c – То же, в виде команды для /bin/sh.

Burpsuite – это платформа для проведения аудита безопасности веб-приложений. Содержит инструменты для составления карты веб-приложения, поиска файлов и папок, модификации запросов, фаззинга, подбора паролей и многого другого.

После включения и настройки Burpsuite и браузера программа выступает в роли прокси для трафика, получаемого браузером и исходящим от него. При этом пользователь контролирует передачу пакетов с возможностью их модификации.

Настройка Burpsuite:

- 1) Подготовить браузер к использованию утилиты Burpsuite.

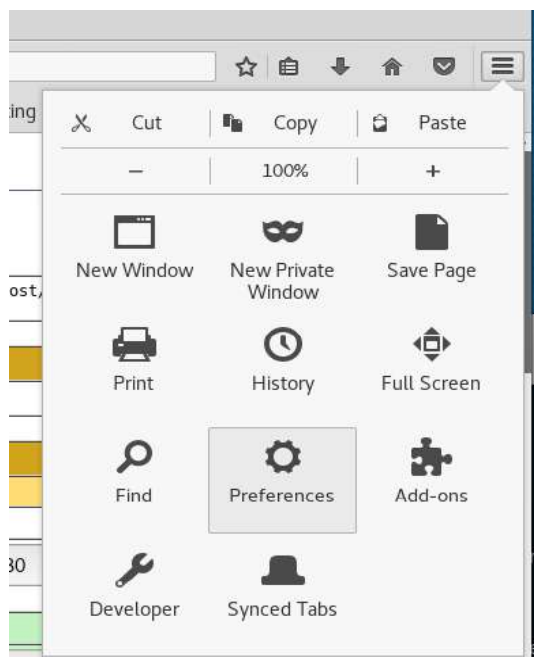


Рис. 11. Меню настройки браузера FireFox

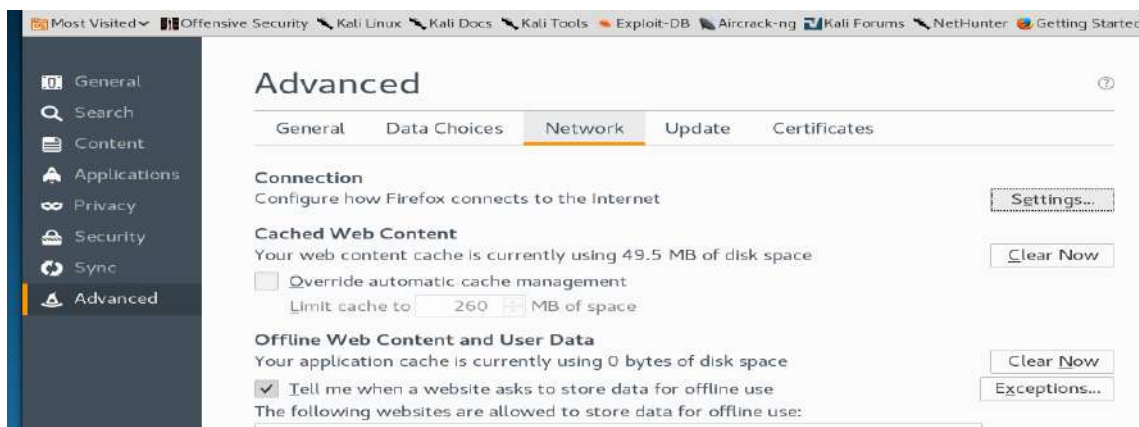


Рис. 12. Вкладка «Advanced»

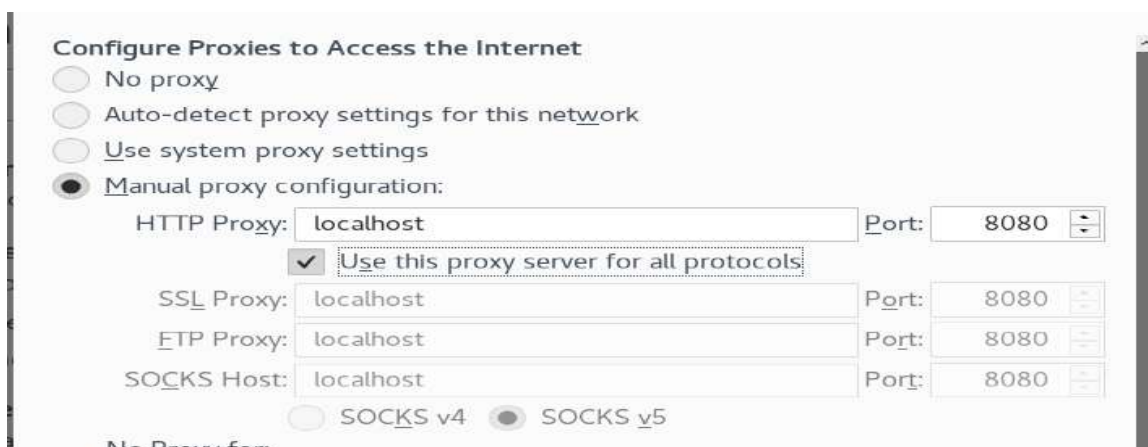


Рис. 13. Настройка прокси-сервера браузера

2) Запустить BurpSuit.



Рис. 14. Локация приложения «burpsuite»

3) Выбрать «I Accept».

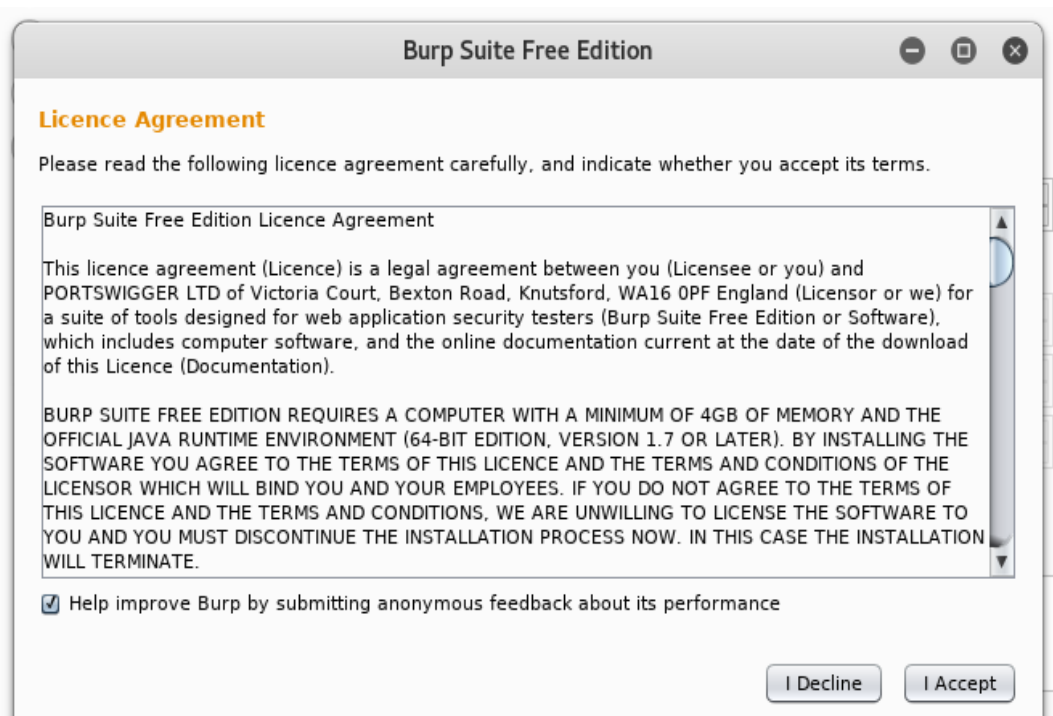


Рис. 15. Окно пользовательского соглашения

Далее, «Next»

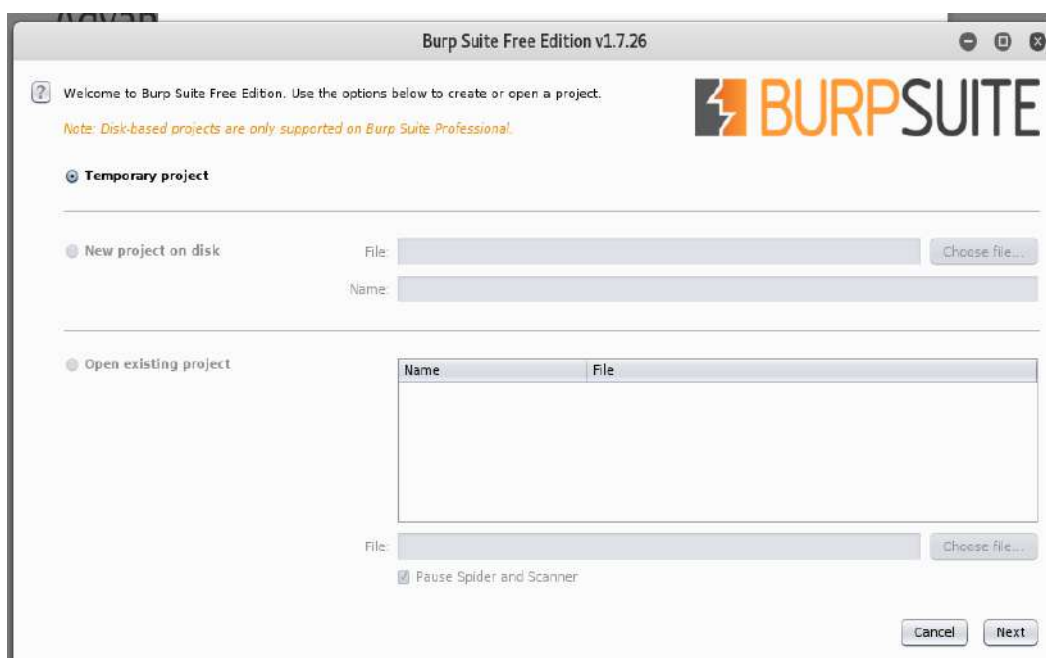


Рис. 16. Окно выбора проекта по умолчанию

Далее, «Startburp»



Рис. 17. Окно запуска burpsuite

4) Настройка Proxy в Burpsuite.

Перейти во вкладку Proxy, а затем во вкладку Options и установить перехват с порта 8080.

Для этого в настройках Proxy Listeners выделить listener и нажать на кнопку Edit. В появившемся окне перейти во вкладку Binding и установить номер перехватываемого порта – 8080, перехватываемый адрес – Loopback.

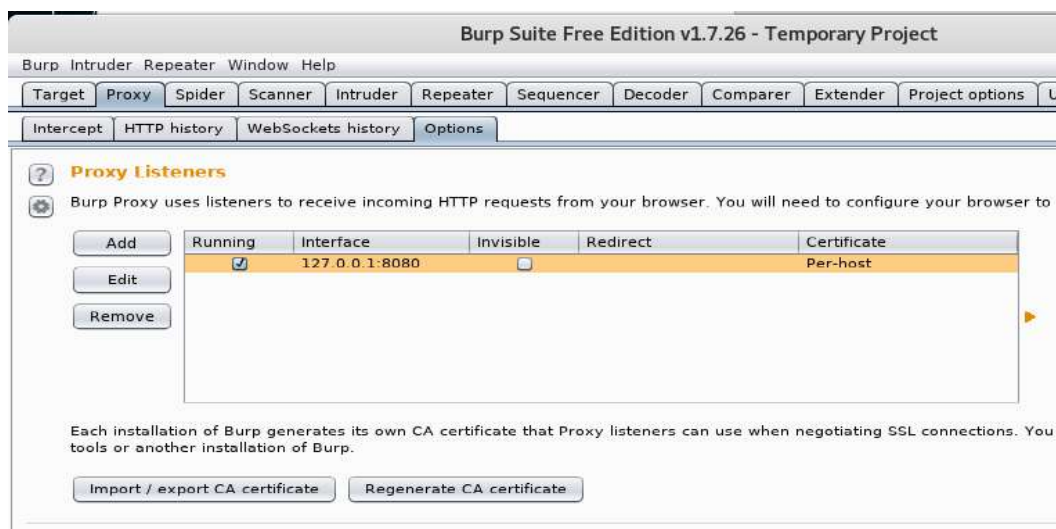


Рис. 18. Настройки proxy-сервера burpsuite

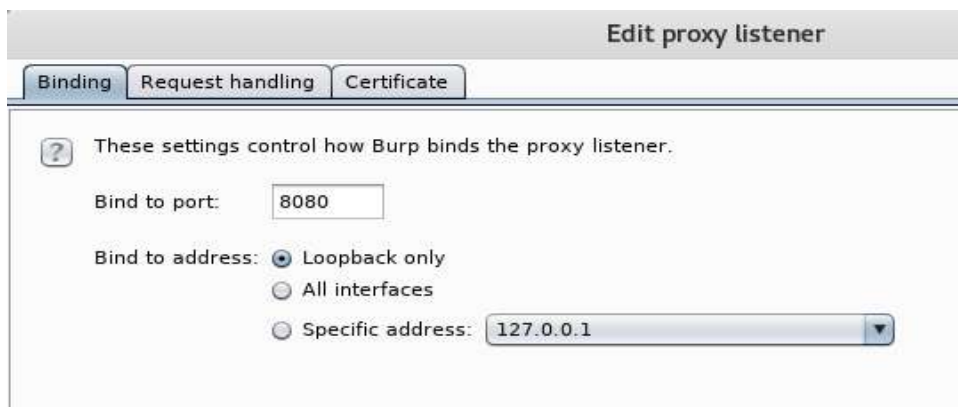


Рис. 19. Настройки Listener в Burpsuite

5) Запустить перехватчик трафика Proxy Listener. Для этого поставить галочку в колонке «Running».



Рис. 20. Настройки burpsuite

Для просмотра перехвата и редактирования перейти во вкладку Intercept.



Рис. 21. Включение перехвата трафика

6) Далее необходимо удалить существующую cookie.

Важно знать, что адреса ресурсов сервера, к которым обращается пользователь посредством браузера, сохраняются в cookie этого браузера. Чтобы Virpsuite работал корректно, необходимо периодически удалять cookie из браузера.

Сделать это можно следующим образом: в MozillaFirefox (браузер по умолчанию в KaliLinux) открыть «Preferences»:

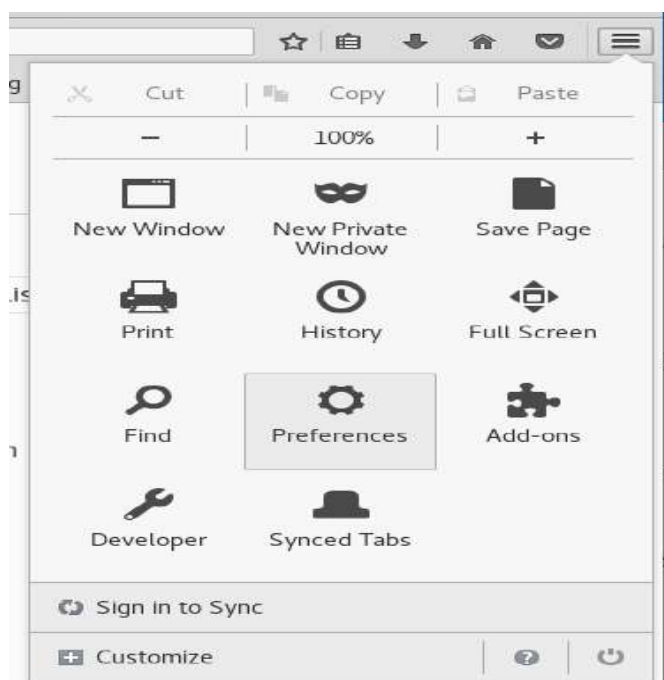


Рис. 22. Меню настройки браузера FireFox

7) Выбрать вкладку «Privacy» и нажать «remove individual cookies»:

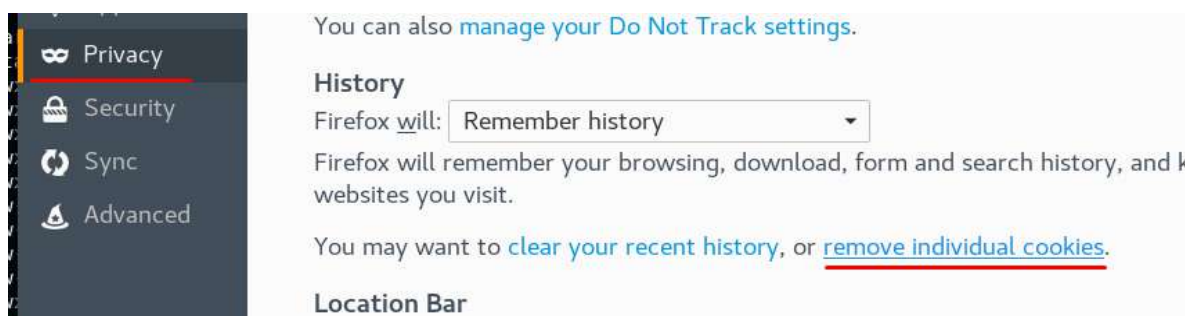


Рис. 23. Вкладка «Privacy»

8) Выбрать cookie адреса 192.168.2.110 (адрес Log-сервера) и нажать «remove selected».

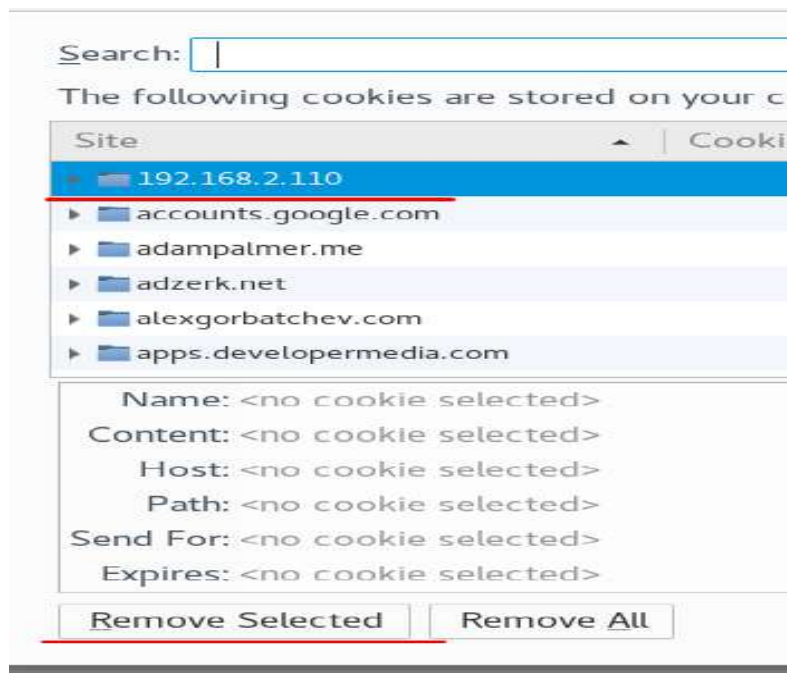


Рис. 24. Удаление существующих cookie

Использование Burpsuite:

Для включения или выключения Intercept-режима в Burpsuite необходимо нажать «InterceptOn/Off».

9) Перехват ответа на выбранный пакет.

Нажать кнопку «Action» интерфейса Burpsuite, далее «Do Intercept» и «Response to this request». После этого отправить пакет адресату кнопкой «Forward».

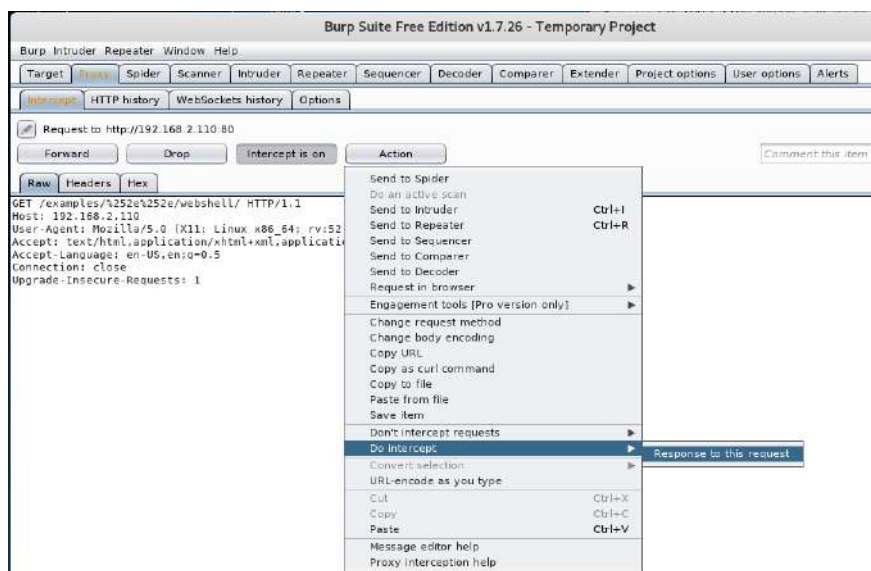


Рис. 25. Включение режима перехвата ответов на запрос

10) Модификация пакета.

Содержимое пакетов отображается во вкладке Raw (подвкладка Proxy, затем Intercept). Перед отправкой пакета можно менять его содержимое в поле, в котором оно отображается. Например, поменять значение параметра «Path»:



Рис. 26. Содержимое входящего пакета

Далее нажать «Forward» для передачи пакета адресату

4. Используемое методическое и лабораторное обеспечение

1) Виртуальная машина «KP_ASU_SCADA_LOG» с установленной ОС Kali Linux, содержащая в себе ПО клиентской части стенда АСУ ТП (Log-сервер) с использованием сервисов apache2 и tomcat6.

2) Виртуальная машина обучаемого с установленной ОС Kali Linux, содержащая в себе следующее программное обеспечение: tcpdump, wireshark, python 2.7.

5. Порядок выполнения работы

Лабораторная работа состоит из нескольких заданий. Задача лабораторной работы – собрать необходимые сведения (указана в задании) с помощью различных инструментов, проанализировать их, использовать собранную информацию для эксплуатации уязвимостей и сформировать отчет, содержащий полученные сведения.

5.1. Ход работы

- 1) Подключиться к виртуальной машине обучающегося.
- 2) Осуществить атаку типа Path Traversal и получить доступ к управляющей консоли.
- 3) Залить shell на сервер «KP_ASU_SCADA_LOG».
- 4) Получить доступ к webshell.
- 5) Осуществить reverse shell.

5.2. Завершение работы

Выключить виртуальную машину «KP_ASU_SCADA_LOG».

6. Содержание отчёта о выполненной работе

В отчёте о выполненной лабораторной работе необходимо указать данные в виде таблиц с заполненными значениями.

6.1. Пример задания

- 1) Осуществить атаку типа Path Traversal и получить доступ к управляющей консоли;
- 2) Залить webshell на сервер «KP_ASU_SCADA_LOG»;
- 3) Получить доступ к webshell;
- 4) Осуществить reverse shell.

6.2. Пример отчета

Отчет может выполняться как на компьютере, так и на бумажном носителе в зависимости от требований преподавателя.

№	Задание	Значение
1	Осуществить атаку типа Path Traversal и получить доступ к управляющей консоли	
2	Установить webshell на сервер	
3	Перейти в webshell	
4	Осуществить reverse shell	

7. Контрольные вопросы

- 1) На что направлены атаки типа «PathTraversal»?
- 2) Почему необходимо изменять значение /path в cookie во время атаки «PathTraversal»?

8. Бланк отчета

8.1. Задание

- | |
|---|
| 1) Осуществить атаку типа Path Traversal и получить доступ к управляющей консоли; |
| 2) Установить webshell на сервер «KP_ASU_SCADA_LOG»; |
| 3) Получить доступ к webshell; |
| 4) Осуществить reverse shell. |

8.2. Ответы

№	Задание	Значение
1	Осуществить атаку типа Path Traversal и получить доступ к управляющей консоли	
2	Установить webshell на сервер	
3	Перейти в webshell	
4	Осуществить reverse shell	

Оглавление

	Стр.
Приложения	3
Приложение 1	3
Памятки в целях профилактики мошенничества	3
Приложение 2	31
Лабораторные работы	31
Лабораторная работа № 1	31
Анализ защищенности протокола MODBUS TCP	31
1. Цель лабораторной работы	31
2. Краткие теоретические сведения	31
3. Описание инструментария	34
3.1. Утилита tcpdumptcpdump является инструментом, позволяющим перехватывать и анализировать сетевой трафик, проходящий через компьютер, на котором запущена данная программа	34
3.2. Утилита Wireshark	36
3.3. Утилита python	37
4. Используемое методическое и лабораторное обеспечение	37
5. Порядок выполнения работы	37
5.1. Ход работы	38
5.2. Завершение работы	38
6. Содержание отчёта о выполненной работе	38
6.1. Пример задания	38
6.2. Пример отчета	39
7. Контрольные вопросы	39
8. Бланк отчета	39
8.1. Задание	39
8.2. Ответы	39

ЛАБОРАТОРНАЯ РАБОТА № 2	40
АНАЛИЗ ЗАЩИЩЕННОСТИ ПРОГРАММИРУЕМОГО ЛОГИЧЕСКОГО КОНТРОЛЛЕРА (ПЛК)	40
1. Цель лабораторной работы.....	40
2. Краткие теоретические сведения.....	40
2.1. Схема стенда.....	41
3. Инструментарий	41
4. Используемое методическое и лабораторное обеспечение	43
5. Порядок выполнения работы	43
5.1. Ход работы.....	43
5.2. Завершение работы	43
6. Содержание отчёта о выполненной работе	43
6.1. Пример задания	44
6.2. Пример отчета	44
7. Контрольные вопросы	44
8. Бланк отчета.....	44
8.1. Задание	44
8.2. Ответы	44
ЛАБОРАТОРНАЯ РАБОТА № 3.....	45
АНАЛИЗ ЗАЩИЩЕННОСТИ SCADA-СЕРВЕРА.....	45
1. Цель лабораторной работы	45
2. Краткие теоретические сведения.....	45
2.1. Схема стенда.....	46
2.2. Инструментарий	46
3. ИСПОЛЬЗУЕМОЕ МЕТОДИЧЕСКОЕ И ЛАБОРАТОРНОЕ ОБЕСПЕЧЕНИЕ.....	50
4. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ.....	50
4.1. Ход работы.....	50
4.2. Завершение работы	50

5. СОДЕРЖАНИЕ ОТЧЁТА О ВЫПОЛНЕННОЙ РАБОТЕ	50
5.1. Пример задания	50
5.2. Пример отчета	51
6. КОНТРОЛЬНЫЕ ВОПРОСЫ.....	51
7. БЛАНК ОТЧЕТА.....	51
7.1. ЗАДАНИЕ	51
ЛАБОРАТОРНАЯ РАБОТА № 4.....	52
АНАЛИЗ ЗАЩИЩЕННОСТИ LOG-СЕРВЕРОВ.....	52
1. Цель лабораторной работы	52
2. Краткие теоретические сведения.....	52
3. Инструментарий	53
4. ИСПОЛЬЗУЕМОЕ МЕТОДИЧЕСКОЕ И ЛАБОРАТОРНОЕ ОБЕСПЕЧЕНИЕ.....	62
5. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ.....	62
5.1. Ход работы.....	63
5.2. Завершение работы	63
6. СОДЕРЖАНИЕ ОТЧЁТА О ВЫПОЛНЕННОЙ РАБОТЕ	63
6.1. Пример задания	63
6.2. ПРИМЕР ОТЧЕТА	63
7. Контрольные вопросы	63
8. БЛАНК ОТЧЕТА.....	64
8.1. Задание	64
8.2. Ответы	64

Научное издание

Литвинов Михаил Юрьевич,
кандидат технических наук
Алескеров Вагиф Исмаилович,
кандидат юридических наук, доцент

**ПРОТИВОДЕЙСТВИЕ
СОВРЕМЕННЫМ ВИДАМ ПРЕСТУПЛЕНИЙ,
СОВЕРШАЕМЫХ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ**

Часть 3

Редактирование О.Н. Колокольчикова
Техническое редактирование Е.В. Бухарина

Подписано в печать 30.06.2026.
Формат 60х84 1/16. Объем 4,5 усл.-изд. л.
Тираж 100 экз. Заказ 09/26. Цена договорная.

Федеральное государственное казенное учреждение
дополнительного профессионального образования
«Всероссийский институт повышения квалификации сотрудников
Министерства внутренних дел Российской Федерации».

142007, Московская обл., г. Домодедово, микрорайон Авиационный,
ул. Пихтовая, д. 3.