МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕУЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по выполнению практических работ
по дисциплине «ТЕХНОЛОГИИ РАССЛЕДОВАНИЯ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ И ИНЦИДЕНТОВ»
для студентов направления подготовки 02.04.01 «Математика и компьютерные науки»
профиль «Искусственный интеллект в кибербезопасности»

Ставрополь 2026 г.

СОДЕРЖАНИЕ

Практическая работа № 1 Тема. Исследование производства компьютерно-технической экспертизы

Основные теоретические сведения

Понятие судебной экспертизы

Прежде чем перейти к реализации новых подходов, необходимо дать понятие судебной экспертизы.

Согласно ст. 9 Федеральному закону № 73 «О государственной судебно-экспертной деятельности в Российской Федерации» [4]:

«судебная экспертиза - это процессуальное действие, состоящее из проведения исследований и дачи заключения экспертом по вопросам, разрешение которых требует специальных знаний в области науки, техники, искусства или ремесла и которые поставлены перед экспертом судом, судьей, органом дознания, лицом, производящим дознание, следователем, в целях установления обстоятельств, подлежащих доказыванию по конкретному делу;

заключение эксперта - это письменный документ, отражающий ход и результаты исследований, проведенных экспертом».

Таким образом, судебная экспертиза - это особое процессуальное действие, проводимое в случае возникновения в деле вопросов, требующих специальных познаний в области науки, техники, искусства или ремесла. Понятие судебной экспертизы как средства доказывания присутствует во всех процессах [5-7]. Судебная экспертиза - это отдельный и самостоятельный вид доказательства, имеющий перед законом одинаковую доказательную силу наравне с прочими доказательствами [8].

Предметом экспертизы является информация об экспертных задачах, экспертных методиках, методах решения вопросов, а также информация об объектах и их свойствах.

Предметом исследования в рамках экспертизы является предмет познания. Под предметом познания понимаются сведения об объектах, целях и условиях исследования, полученные в опыте и используемые на практике.

Экспертные задачи делятся на общие, типовые, частные и конкретные. Общие задачи - задачи, решаемые во всех классах экспертиз (диагностические, идентификационные и классификационные задачи) [912]. Типовые задачи - задачи, представляющие общую формулировку задач для рода экспертизы. Частные задачи - специфичные задачи для каждой экспертизы. Конкретные задачи - это конкретные вопросы, поставленные перед экспертом.

Понятие компьютерно-технической экспертизы КТЭ является самостоятельным родом судебных экспертиз. (Она относится к классу инженерно-технических экспертиз [13]. КТЭ проводится в «целях определения статуса объекта как компьютерного средства, выявления и изучения его следовой картины в расследуемом преступлении, получения доступа к информации на носителях данных с последующим всесторонним её исследованием» [13].

Основной задачей КТЭ является ответ на вопросы, требующие специальных познаний в области форензики (компьютерной криминалистики) - знаний о методах поиска, закрепления и исследования цифровых доказательств по преступлениям, связанным с компьютерной информацией (киберпреступлениям) [14].

Согласно Приказу Министерства юстиции Российской Федерации (Минюст России) от 27 декабря 2012 г. №237г. «Об утверждении Перечня родов (видов) судебных экспертиз, выполняемых в федеральных бюджетных судебно-экспертных учреждениях Минюста России, и Перечня экспертных специальностей, но которым представляется право самостоятельного производства судебных экспертиз в федеральных бюджетных судебно-экспертных учреждениях Минюста России» в рамках КТЭ происходит исследование информационных компьютерных средств 115]. Такое определение существенно ограничивает круг вопросов, решаемых КТЭ.

В современной научной среде круг вопросов, относящихся к КТЭ, значительно шире. Так, в составе КТЭ выделяют четыре вида экспертиз: аппаратно-компьютерную, программно-компьютерную, информационно-компьютерную (она же экспертиза данных) и компьютерно-сетевую [16]. Выделение такого числа и именно таких видов экспертиз обусловлено свойствами объектов, предоставляемых на экспертизу, и задач, решаемых в рамках каждой конкретной экспертизы.

Аппаратно-компьютерная экспертиза направлена на решение вопросов, связанных с исследованием технической (аппаратной) части компьютерных средств. Как правило, эти вопросы носят диагностический характер.

Программно-компьютерная экспертиза направлена на решение вопросов, связанных с исследованием программного обеспечения. В рамках программно-компьютерной экспертизы исследуются процедуры, алгоритмы, принципы разработки программного обеспечения, а также его использование, текущее состояние, структурные особенности, особенности их эксплуатации.

Выделение компьютерно-сетевой экспертизы связано с бурным развитием науки и техники и появлением широкого круга специфичных задач, сопряженных с сетевыми информационными технологиями. Компьютерно-сетевая экспертиза занимается исследованием обстоятельств и фактов, связанных с применением телекоммуникационных и сетевых технологий.

Ключевым видом КТЭ, позволяющим сформировать целостное построение доказательной базы путем решения большей части диагностических и идентификационных вопросов данного рода экспертизы, является информационно-компьютерная экспертиза. Информационно-компьютерная экспертиза решает задачи, связанные с поиском, обнаружением, оценкой и анализом информации, содержащейся в компьютерной системе.

Методические рекомендации по выполнению Практической работы

Задания

1. Найти и изучить нормативно-правовые акты, регламентирующие производство судебной экспертизы в разных видах отечественного судопроизводства (уголовное, гражданское, арбитражное, административное). Произвести сравнение полноты отражения в данных актах вопросов, связанных с назначением и производством судебной экспертизы (понятие судебной экспертизы, ее виды, обязательность производства, права и обязанности эксперта, заключение эксперта и т.д.) Результаты отразить в отчете (со ссылкой на конкретные статьи (разделы) нормативно-правовых актов).

2. Изучить ведомственные нормативно-правовые акты, регламентирующие судебно-экспертную деятельность в МВД, Министерстве юстиции РФ, ФСБ, МЧС, ФТС РФ. Произвести сравнение данных актов по вопросам организации и производства экспертиз (какие вопросы регламентированы, какие нормы затрат времени (экспертной нагрузки) в них предусмотрены, какие экспертные специальности, а также рода (виды) судебных экспертиз в них предусмотрены и т.д.) - со ссылкой на конкретные разделы). Результаты отразить в отчете.

3. Найти и изучить официальные сайты государственных судебно-экспертных учреждений Российской Федерации. Результаты изучения оформить в виде таблицы с указанием названий головных государственных судебно-экспертных учреждений конкретных министерств (служб) и адресов их официальных сайтов.

Дополнительные задания

1. Изучить ведомственные нормативно-правовые акты, регламентирующие судебно-экспертную деятельность в МВД РФ, Министерстве юстиции РФ, ФСБ РФ. Произвести сравнение названий родов (видов) судебных экспертиз, проводимых в разных министерствах (ведомствах). Результаты сравнения отразить в отчете (со ссылкой на конкретные нормативно-правовые акты).

2. Проанализировать классификацию судебных экспертиз, представленную на сайтах негосударственных экспертных учреждений (организаций) (например, на сайте Центра по проведению судебных экспертиз и исследований АНО «Судебный Эксперт» (https://sudexpa.ru/map/)), оценить ее полноту и корректность, сравнить с перечнем родов (видов) судебных экспертиз, выполняемых в федеральных бюджетных судебно-экспертных учреждениях Минюста России. Результаты отразить в отчете.

3. Найти и изучить сайты негосударственных судебно-экспертных учреждений (организаций) (http://www.sudex.ru/, https://sudexpa.ru/, http://sud-expertiza.ru/ и т.д.). Зафиксировать форму их организации, изучить

учредительные документы (при наличии), рода (виды) проводимых экспертиз, расценки, оценить правовой статус членов данных учреждений и т.д. Результаты отразить в отчете. **Вопросы для контроля**

1. Раскрыть понятия «судебная экспертиза», «судебный эксперт».
2. Сравнить понятия «государственные судебно-экспертные учреждения» и «негосударственные судебно-экспертные учреждения (организации)».
3. Указать по каких критериям (основаниям) возможна классификация судебных экспертиз (привести примеры).
4. Раскрыть понятие «судебно-экспертная деятельность», указать основные направления судебно-экспертной деятельности.

Результаты Практической работы занести в отчет **Содержание отчета по Практической работе**

По результатам выполнения Практической работы студенты оформляют отчет по Практической работе и защищают его в индивидуальном порядке в форме беседы.

Практическая работа № 2 Тема. Анализ методик производства компьютерно-технической экспертизы

Основные теоретические сведения 2.1.Базовые критерии классификации методик КТЭ Содержание экспертных методик КТЭ определяется задачами, целями и объектами рассматриваемого рода судебных экспертиз.

Описание методов и алгоритмов классификации зачастую основывается на представлении исходной информации о классифицируемых объектах в виде графов [54-62]. Далее в работе будет использован подход к классификации и буквенная нотация, предложенные в [54] и использованные в [56].

Для классификации методик КТЭ предлагается использование теории графов, в частности ориентированный граф А(В, С) в котором:

- *B = {bo, bi,i, bi,2, ... bij, be}* — множество вершин графа А;
- *C* - множество ориентированных рёбер графа *A;*
- начало классификации — вершина *bo;*
- конец классификации — вершина *be;*
- *i* — число критериев классификации методик;
- *j* — число признаков конкретного критерия.

В настоящее время число критериев классификации методик производства экспертизы г = 3, а число признаков для КТЭ удовлетворяет требованию $3 < j < 4$ в зависимости от каждого конкретного критерия.

Предлагаемый подход к классификации методик КТЭ с использованием теории графов может быть использован независимо от состава и числа критериев классификации методик и признаков критериев классификации методик. Более того, данный подход может быть использован для классификации методик других родов и видов экспертиз, т. е. этот подход является унифицированным.

Для классификации методик КТЭ используются простые пути на графе. Задача эксперта КТЭ по выбору необходимой методики производства КТЭ сводится к поиску пути на графе, т. е. определение путей между вершинами *bo* и *be* и будет процессом определения методики производства КТЭ.

Множеством простых путей между вершинами и *be* определяется множество методик производства КТЭ (М). Существующие в настоящее время критерии классификации методик КТЭ и признаки критериев представлены в табл. 2.1.

В рамках предложенного подхода, для возможности автоматизации и унификации, авторами предлагается построить граф, где базовые критерии для классификации методик КТЭ формируют множество *B = {bo, bi,i, bi,2, ... bi,j, be}*вершин графа *A* (рис. 2.1).

Согласно рис. 2.1 свойства методик критериев *i* (объекты КТЭ) не имеют зависимостей от значений критериев 2, а критерии 2 не имеют зависимостей от значений критериев 1. -Таблица 2.1

Критерии классификации методик КТЭ [2]

Критерий	Признак критерия
1. Категория задач	1.1. Диагностические — направлены на определение свойств и состояний объекта, определение факта его изменения, определение причины этих изменений и ее связи с рассматриваемым делом (например, причины возникновения ошибок в работе программного обеспечения или неисправности ноутбука) [2] 1.2. Классификационные — направлены на установление характеристик (свойств) неизвестного/известного объекта с целью отнесения его к общепринятому классу (например, отнесение графического редактора к классу векторных или растровых) [2] 1.3. Идентификационные — направлены на установление тождества объекта самому себе, индивидуальноконкретного тождества (например, идентификация программного обеспечения по предоставленному образцу лицензионного программного обеспечения) [2]
2. Цели (вопросы КТЭ)	2.1. Относящиеся к аппаратным средствам [2] 2.2. Относящиеся к программным средствам [2] 2.3. Относящиеся к данным (информации) [2] 2.4. Относящиеся к вычислительной сети и ее элементам [2]
3. Объекты КТЭ	3.1. Аппаратные средства [2] 3.2. Программные средства [2] 3.3. Данные (информация) [2] 3.4. Вычислительная сеть и ее компоненты [2]

То есть методики, относящиеся к любой из трех категорий задач (диагностические, классификационные, идентификационные), могут предназначаться для решения вопросов любой из четырех групп, объектами которых могут являться объекты любой из четырех групп.

Методические рекомендации по выполнению Практической работы

1. Постройте поэтапную методику проведения компьютерно-технической экспертизы в соответствии с кейсом, встречающимся на Вашей работе.

Результаты Практической работы занести в отчет

Содержание отчета по Практической работе

По результатам выполнения Практической работы студенты оформляют отчет по Практической работе и защищают его в индивидуальном порядке в форме беседы.

Практическая работа № 3

Тема. Исследование методов комбинированных атак с использованием фитинга Основные теоретические сведения

В ходе подготовки к целенаправленной атаке осуществляются изучение круга общения персоны, интересов, сфера деятельности атакуемого. Кроме этого, злоумышленникам необходимо понимать, каким программным обеспечением и устройствами пользуется жертва.

В зависимости от используемых методов авторизации, просмотра писем необходимо готовить интерфейс фишинг-движка или тип засылаемой вредоносной программы.

В частности, большое значение имеют операционная система и браузер, а также информация о способах обращения пользователя к аккаунту: посредством веб-интерфейса или почтового клиента.

Важно для злоумышленников знать, в какие периоды времени пользователь осуществляет обработку почты, а также периоды, когда обращение к почтовому адресу не производится. Электронная почта может быть синхронизирована с мобильным телефоном, и оповещения о входящих сообщениях поступают незамедлительно.

Кроме этого, собирается информация об используемых провайдерах и местах, где осуществляет подключение к сети Интернет потенциальная жертва атаки.

Все эти сведения необходимы злоумышленнику для подготовки индивидуального фишинг-движка, подходящего для используемого жертвой компьютерного устройства, а также планирования дальнейших действий. Например, внедрения в переписку, о чем мы поговорим позже.

Рассматривать все тривиальные способы сбора информации о пользователе, которые могут быть доступны злоумышленникам, в данной работе нецелесообразно. Укажем только, что берется в расчет вся общедоступная информация: размещаемые ранее резюме, профили на разнообразных ресурсах, социальные сети, анализ фотографий и документов, сайты объявлений, знакомые и родные.

Необходимо особо указать несколько специфических способов, о существовании которых мало кто догадывается.

Определение браузера и операционной системы атакуемого

Допустим, злоумышленникам известен номер мобильного телефона или электронный адрес выбранной жертвы. Атакующий для подготовки атаки и сбора информации создает на совершенно любом сервере сайт (или одну страницу) с содержимым, так или иначе интересным жертве. Это не фишинг-движок, это нечто другое.

Данный ресурс создается только для сбора информации о посетителе в пассивном формате, то есть без принуждения пользователя к вводу каких-либо данных. Все необходимые данные собираются из переменных, содержащих данные об окружении.

Подобную информацию собирают счетчики посещаемости, устанавливаемые администраторами ресурсов для анализа посетителей сайта, но собираемая информация не имеет привязки к определенному лицу.

Немного теории.

User-Agent - это клиентское приложение, использующее определенный сетевой протокол. При посещении веб-сайта клиентское приложение обычно посылает веб-серверу информацию о себе. Это текстовая строка, являющаяся частью HTTP-запроса.

В рассматриваемом ранее примере фишинг-движка (пример 3) в процессе тестовой авторизации для проверки пароля серверу посылалась информация о клиентском приложении: User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; ru; rv:1.9.2.8) Gecko/20100722 Firefox/3.6.8 (.NET CLR 3.5.30729).

Есть в языке PHP возможность получения информации об окружении посредством переменной $_SERVER, по сути являющейся массивом, содержащим довольно разнообразные данные[1].

Переменная *$_SERVER* - это массив, содержащий такую информацию, как заголовки, пути и местоположения скриптов. Записи в этом массиве создаются веб-сервером.

В качестве примера использования массива можно продемонстрировать получение информации удаленным ресурсом, на стороне которого исполняется скрипт PHP:

```
<?php
echo $_SERVER['HTTP_USER_AGENT'] . "\n\n";
$browser = get_browser(null, true);
print_r($browser);
```

Эту функцию можно добавить к странице совершенно любого

[1] https://php.ru/manual/reserved.variables.server.html.

ресурса и получить информацию об используемой посетителем версии браузера и операционной системы.

Единственное условие работоспособности функции - это наличие на сервере интерпретатора языка PHP, о чем уже упоминалось в предыдущей части.

При исполнении приведенного выше примера кода на сервере, при обращении к ресурсу с использованием браузера Firefox (рис. 2.1) скрипт получает от браузера клиента следующее значение: «Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0».

Рис. 2.1. Браузер Firefox

Как видно из полученных данных, значение Windows NT 6.1 сможет подсказать злоумышленнику, что потенциальная жертва использует операционную систему одной из версий Windows компании Microsoft, а именно Windows 7 или Windows Server 2008 R2.

Значение Win64 указывает на использование семейства 64-битных операционных систем Windows для архитектуры x86-64 (AMD64) и IA-64 (Itanium).

Такие данные критичны для тех, кто собирается начать с заброса бэкдора или использования других вредоносных компьютерных программ или утилит, а также продолжения атаки после получения несанкционированного удаленного доступа к операционной системе. При компиляции[2] вредоноса должны учитываться особенности операционной системы, Win32-nporpaMMa может быть после небольших исправлений перекомпилирована в 64-битном варианте. Хотя для запуска в 64-битной операционной системе Windows 32-битных приложений имеется подсистема WoW64, расположение некоторых стандартных директорий и файлов отличается, что может негативно сказаться на результате работы программы.

Для демонстрации приведенного примера можно также посмотреть, какие данные будут содержаться в переменной $_SERVER

[2] Компиляция - процесс перевода (трансляции) исходного кода компьютерной программы с предметно-ориентированного языка на машинно-ориентированный язык.

['HTTP_USER_AGENT'] при обращении к скрипту с использованиембраузера MS Internet Explorer (рис. 2.2).

Рис. 2.2. Браузер MS Internet Explorer

Скрипт получает значение:

Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Мобильный браузер телефона Samsung при обращении к странице, содержащей приведенный PHP-крипт, расскажет злоумышленникам следующее:

Mozilla/5.0 (Linux; Android 7.0; SAMSUNG SM-J710F Build/ NRD90M) AppleWebKit/537.36 (KHTML, like Gecko) SamsungBrowser/5.4 Chrome/51.0.2704.106 Mobile Safari/537.36

При обращении из-под операционной системы Ubuntu функцией будет получена такая информация:

Mozilla/5/0 (compatible; Konqueror/4.5; Linux) KHTML/4.5.3 Kubuntu Вариант отображения полученных данных при обращении пользователя из MAC OS:

0pera/9.80 (Macintosh; Intel Mac OS X 10.10.3; Edition MAS) Presto/2.12.388 Version/12.15

Таким образом, заманив пользователя на ресурс с размещенным на нем простеньким скриптом, имеется возможность определить используемую потенциальной жертвой версию браузера и операционной системы.

Естественно, для использования этой функции злоумышленники не отображают полученных от браузера значений, а записывают их в текстовый файл на сервере или отправляют на свой электронный адрес. Определение IP-адресов атакуемого

С таким же успехом можно получить информацию об IP-адресе, посредством которого осуществлялось обращение пользователем к странице. Для этого можно использовать переменную 'REMOTE_ USER' того же массива $_SERVER:

$_SERVER['REMOTE_USER'];

Созданный злоумышленниками простенький ресурс может поведать необходимую информацию о пользователе, и все это выглядит совершенно безобидно и законно. Такой ресурс может быть заброшен жертве в социальной сети или любым другим способом, как от имени незнакомого пользователя, так и при использовании одного из аккаунтов «друзей».

Знание операционной системы, браузера и IP-адреса уже позволяет злоумышленнику определиться с типом вредоносной программы, которую можно закинуть жертве, или какие уязвимости использовать в продолжение атаки.

Можно рассмотреть еще один интересный способ получения информации о потенциальной жертве, которая очень важна для злобных кибершпионов.

Анализ служебных заголовков

В основе этого способа получения информации лежит анализ служебных заголовков (свойств) электронного сообщения, которые имеются у любого сообщения и определены в документе RFC-822 (Standard for ARPA Internet Text Message)[3].

Этот метод сводится к навязанной пользователю, в отношении которого осуществляется сбор информации, переписке с использованием принадлежащего ему электронного почтового адреса. Цель - под каким- либо предлогом от пользователя нужно получить электронное письмо.

В самом простом варианте это может выглядеть примерно так. Пользователю на электронный ящик приходит письмо: «Привет, Серега, когда долг вернешь? Да и вообще, давно не виделись, как там дела на работе?» В ответ пользователь, скорее всего, напишет: «Ты кто вообще?»

Навязать переписку можно также с использованием фишинга, то есть используя похожий на известный жертве электронный адрес. В зависимости от личности жертвы злоумышленники могут представиться рекламным агентом, продюсерским центром, режиссером, фондом помощи, представителем СМИ, поставщиком товаров или услуг, клиентом и т. д.

Получив ответное письмо от потенциальной жертвы и проведя его анализ, злоумышленники могут почерпнуть из него весьма ценную для себя информацию. Эта информация никак не связана с тем, что напишет пользователь, даже если это будет пара нецензурных выражений.

Интересующая информация кроется в служебных заголовках электронного письма, которые в обычном режиме просмотра не отображаются ни в почтовом клиенте, ни в интерфейсе почтового сервиса. Но они все-таки есть.

К примеру, служебные заголовки могут содержать информацию о почтовом клиенте, посредством которого пользователь отправил сообщение:

X-Mailer: Apple Mail (2.3273)

В данном случае служебные заголовки содержат информацию об использовании отправителем Apple Mail - почтового клиента от Apple Inc., который входит в стандартную поставку Mac OS X и iOS. Ну совершенно очевидно, что нет никакого смысла подкидывать такому пользователю вредоносную программу - бэкдор или троян, написанную под операционные системы Windows или Android.

---

[3] https://www.w3.org/Protocols/rfc822/.

Если пользователь отправляет письмо непосредственно из браузера, допустим, сервиса mail.ru, то в служебном заголовке будет содержаться следующее значение:

X-Mailer: Mail.Ru Mailer 1.0

При отправке письма посредством почтового клиента Thunderbird:

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:52.0) Gecko/20100101 Thunderbird/52.4.0

При отправке электронного письма через мобильное приложение «Яндекс Почта» служебные заголовки также будут содержать полезную информацию:

X-Mailer: Yamail [http://yandex.ru] 5.0 X-Yandex-Mobile-Caller: mobile

Из информации в служебных заголовках присланного письма также можно установить IP-адрес и наименование устройства, с которого было отправлено электронное письмо.

Полученная из служебных заголовков электронного письма информация поможет злодеям спланировать и провести дальнейшие атаки, спроектировав инструментарий нападения в соответствии с используемым жертвой устройством и программами для просмотра и отправки электронной почты.

Приведенные примеры должны продемонстрировать простоту добывания необходимой информации и лишний раз указать на то, что для проведения атаки и получения чужих паролей не всегда требуются невероятные технические знания, все намного проще, чем кажется.

Методические рекомендации по выполнению Практической работы

В данной Практической работе мы будем использовать инструмент Gophish для проведения фишинговой рассылки. Для этого мы поднимем свой почтовый сервер и будем экспериментировать на нём. Напоминаю, что проведение подобной атаки без письменного разрешения является преступлением, поэтому мы сами создадим себе пользователей и наши фишиговые письма распространятся только внутри нашей локальной сети.

Чем опасен фишинг? Люди по-прежнему остаются самым уязвимым местом информационной системы, в связи с этим одним из самых простых способов атаки и дальнейшего распространения является атака на сотрудников. Далеко не все сотрудники организаций способны противостоять своим эмоциям и не податься на провокацию злоумышленника.

Для повышения уровня информационной грамотности следует проводить тренировочные рассылки вредоносных писем, чтобы сотрудники научились распознавать подобные атаки и не повелись на удочку реального злоумышленника.

Подобные проверки стоит проводить раз в две недели или один месяц, чтобы держать коллектив в тонусе

Цена данной услуги варьируется от количества хостов и проработанности атаки.

Используемые инструменты

• SMTP-сервер (Почтовый сервер)

• Gophish

Инструкция по установке

Загрузка

git clone https://github.com/Ivanhahanov/InformationSecurityMethodsAndTools.git

После успешного клонирования репозитория на компьютере будет создана директория InformationSecurityMethodsAndTools cd InformationSecurityMethodsAndTools И перейти в директорию Phishing cd Phishing

Развертывание

На данном этапе необязательно выполнять эти команды, так как предстоит создать TLS сертификаты и пользователей почтового сервера, но вы можете выполнить их, чтобы проверить что у вас работает Docker и docker-compose docker-compose up -d

Флаг -d запустит в режиме демона, и вы не будете видеть логи. Сейчас с ресурса DockerHub "спулятся" образы почтового сервера и приложения для фишинга.

DockerHub - это аналог Github для образов docker образов, вы можете туда загружать свои образы, а можете загружать чужие. Все образы имеют рейтинг, вы можете узнать сколько раз образ загружали и сколько ему поставили звёздочек. Это полезная информация, так вы можете понять, насколько тот или иной образ популярен, и решить, стоит ли загружать именно его или поискать другую реализацию. Чтобы посмотреть, что происходит внутри: docker-compose logs -f

Почтовый сервер должен сообщить об ошибках, так как у нас нет пользователей и нет подписанного сертификата. Так что можно выполнить эту команду:

docker-compose down И Mail сервер

плавно завершит работу **Конфигурация**

Создание сертификатов

Нам необходимо создать самоподписанный TLS сертификат. Такие сертификаты используются для шифрования данных, самый распространённый пример - HTTPS.

В нашем случае он нужен для зашифровки писем, чтобы никто не мог их прочитать при перехвате трафика

В контейнере **docker-mailserver** есть утилита для генерации сертификатов.

Запустим контейнер в интерактивном режиме (флаг **-it]).**
Примонтируем раздел, чтобы сертификат создался у нас в директории MailServer/config/ssl локально.

docker run -ti --rm -v "$(pwd)7config/ssl:/tmp/docker-mailserver/ssl - h mail.domain.com -t tvial/docker-mailserver generate-ssl-certificate

Создание сертификата происходит в два этапа

1. создание CA сертификата
2. создание конечного сертификата

Вводимые поля должны быть идентичны, кроме одного поля Common Name (e.g. server FQDN or YOUR name). Здесь в первым случае надо указать **domain.com,** во втором **mail.domain.com** Поля extra оставить пустыми
Пример генерации сертификата:

CA certificate filename (or enter to create) Making CA certificate ...

openssl req -new -keyout ./demoCA/private/cakey.pem -out ./demoCA/careq.pem
Generating a RSA private key
..... +++++
..... +++++
writing new private key to './demoCA/private/cakey.pem' Enter PEM pass phrase: Verifying - Enter PEM pass phrase:

You are about to be asked to enter information that will be incorporated into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank For some fields there will be a default value, If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:RU
State or Province Name (full name) [Some-State]:Moscow
Locality Name (eg, city) []:Moscow
Organization Name (eg, company) [Internet Widgits Pty Ltd]:My-company Organizational Unit Name (eg, section) []:Red Team Common Name (e.g. server FQDN or YOUR name) []:domain.com Email Address []:admin@domain.com

Please enter the following 'extra' attributes to be sent with your certificate request A challenge password []:
An optional company name []:
==> 0

openssl ca -create_serial -out ./demoCA/cacert.pem -days 1095 -batch -keyfile ./demoCA/private/cakey.pem -selfsign -extensions v3_ca -infiles ./demoCA/careq.pem Using configuration from /usr/lib/ssl/openssl.cnf
Enter pass phrase for ./demoCA/private/cakey.pem: Check that the request matches the signature Signature ok
Certificate Details: Serial Number:
5d:ac:b5:3f:cc:b6:26:bf:6a:20:dd:c1:ff:08:a0:be:14:1b:e4:3c Validity
Not Before: Feb 8 13:40:27 2021 GMT Not After : Feb 8 13:40:27 2024 GMT Subject:
countryName = RU
stateOrProvinceName = Moscow organizationName = My-company
organizationalUnitName = Red Team commonName = domain.com
emailAddress = admin@domain.com
X509v3 extensions:
X509v3 Subject Key Identifier:
E9:4F:D1:CC:9D:09:14:A3:9C:23:68:8E:0E:76:9E:35:AE:22:56:61 X509v3 Authority Key Identifier:
keyid:E9:4F:D1:CC:9D:09:14:A3:9C:23:68:8E:0E:76:9E:35:AE:22:56:61

X509v3 Basic Constraints: critical CA:TRUE
Certificate is to be certified until Feb 8 13:40:27 2024 GMT (1095 days)

Write out database with 1 new entries Data Base Updated
==> 0

CA certificate is in ./demoCA/cacert.pem Ignoring -days; not generating a certificate
Generating a RSA private key
.....+++++
.....+++++
writing new private key to '/tmp/docker-mailserver/ssl/mail.domain.com-key.pem'

You are about to be asked to enter information that will be incorporated into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank For some fields there will be a default value, If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:RU
State or Province Name (full name) [Some-State]:Moscow
Locality Name (eg, city) []:Moscow
Organization Name (eg, company) [Internet Widgits Pty Ltd]:My-company Organizational Unit Name (eg, section) []:Red Team Common Name (e.g. server FQDN or YOUR name) []:mail.domain.com Email Address []:admin@domain.com

Please enter the following 'extra' attributes to be sent with your certificate request A challenge password []: An optional company name []: Using configuration from /usr/lib/ssl/openssl.cnf Enter pass phrase for ./demoCA/private/cakey.pem: Check that the request matches the signature Signature ok Certificate Details: Serial Number:
5d:ac:b5:3f:cc:b6:26:bf:6a:20:dd:c1:ff:08:a0:be:14:1b:e4:3d
Validity
Not Before: Feb 8 13:41:55 2021 GMT Not After : Feb 8 13:41:55 2022 GMT Subject:
countryName = RU
stateOrProvinceName = Moscow
organizationName = My-company
organizationalUnitName = Red Team
commonName = mail.domain.com
emailAddress = admin@domain.com
X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE Netscape Comment:
OpenSSL Generated Certificate X509v3 Subject Key Identifier:
2F:6B:63:BE:40:11:03:4E:EC:E7:27:9E:E7:F8:3B:A8:82:9C:84:D9 X509v3
Authority Key Identifier:
keyid:E9:4F:D1:CC:9D:09:14:A3:9C:23:68:8E:0E:76:9E:35:AE:22:56:61

Certificate is to be certified until Feb 8 13:41:55 2022 GMT (365 days) Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y Write out database with 1 new entries

После добавления сертификата надо пересобрать наш mail server, чтобы наш сертификат применился

docker-compose up --build

Флаг --build соберёт контейнеры заново, если появились какие-то изменения в файловой структуре или конфигурациях **Создание пользователей**

Для того чтобы отправлять письма по электронной почте, нам нужны пользователи.

Для создания пользователей у нас есть Bash скрипт **|setup.sh|**

сделать скрипт исполняемым chmod +x setup.sh

создание email аккаунтов user/password
./setup.sh -i tvial/docker-mailserver:latest email add admin@domain.com admin123 ./setup.sh -i tvial/docker-mailserver:latest email add user@domain.com user123

список email аккаунтов

./setup.sh -i tvial/docker-mailserver:latest email list

В результате мы должны увидеть две почты admin@domain.com и us er@ domain .com **Проверка отправки сообщений**

Для проверки работы Почтового сервера рекомендуется использовать утилиту swaks

Установка утилиты sudo apt-get install swaks

Отправка email для user@domain.com

swaks --from admin@domain.com --to user@domain.com --server 127.0.0.1:587 -tlso -au admin@domain.com -ap admin123 --header "Subject: test from admin" --body "testing 123"

Отправка email для admin@domain.com

swaks --from user@domain.com --to admin@domain.com --server 127.0.0.1:587 -tlso -au user@domain.com -ap user123 --header "Subject: test from user" --body "testing 456"

Описание флагов:

- --from - email отправителя
- --to - email получателя
- --server адрес SMTP сервера
- --au почта пользователя для авторизация
- --ap пароль пользователя для авторизация
- --header заголовок письма
- --body тело письма

В результате мы увидим полный список действий, которые произошли при отправке письма

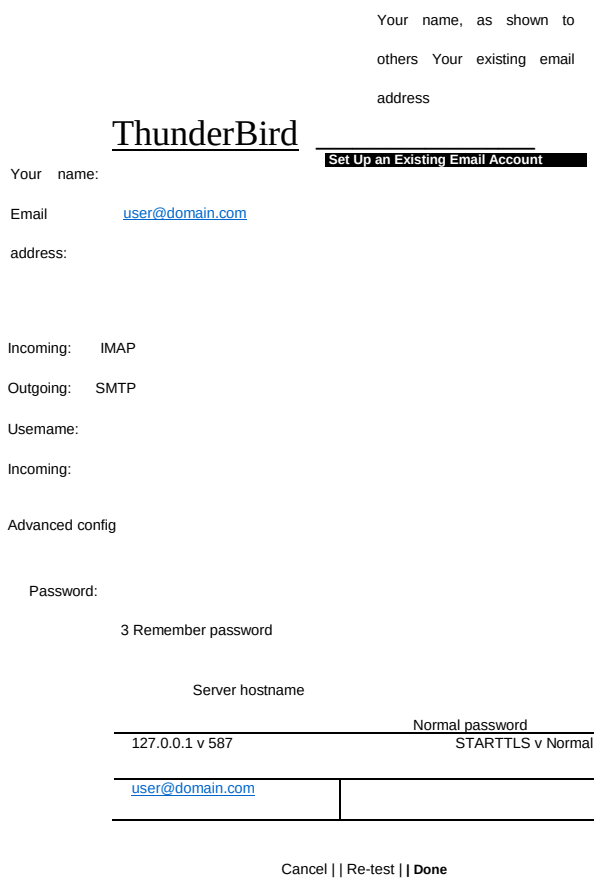
=== Trying 127.0.0.1:587... === Connected to 127.0.0.1. <- 220 mail.domain.com ESMTP -> EHLO ubuntu <- 250-mail.domain.com <- 250-PIPELINING <- 250-SIZE 10240000 <- 250-ETRN <- 250-STARTTLS <- 250-ENHANCEDSTATUSCODES <- 250-8BITMIME <- 250-DSN <- 250 CHUNKING -> STARTTLS
<- 220 2.0.0 Ready to start TLS
=== TLS started with cipher TLSv1.3:TLS_AES_256_GCM_SHA384:256 === TLS no local certificate set
=== TLS peer DN="/C=AU/ST=Some-State/O=Internet Widgits Pty Ltd/CN=mail.domain.com"
~> EHLO ubuntu
<~ 250-mail.domain.com
<~ 250-PIPELINING
<~ 250-SIZE 10240000
<~ 250-ETRN
<~ 250-AUTH PLAIN LOGIN
<~ 250-AUTH=PLAIN LOGIN
<~ 250-ENHANCEDSTATUSCODES
<~ 250-8BITMIME
<~ 250-DSN
<~ 250 CHUNKING
~> AUTH LOGIN
<~ 334 VXNlcm5hbWU6
~> YWRtaW5AZG9tYWluLmNvbQ==
<~ 334 UGFzc3dvcmQ6
~> YWRtaW4xMjM=
<~ 235 2.7.0 Authentication successful
~> MAIL FROM:<admin@domain.com>
<~ 250 2.1.0 Ok
~> RCPT TO:<user@domain.com> <~ 250 2.1.5 Ok ~> DATA
<~ 354 End data with <CR><LF>.<CR><LF> ~> Date: Mon, 08 Feb 2021 17:00:22 +0300 ~> To: user@domain.com ~> From: admin@domain.com ~> Subject: test from admin

~> Message-Id: <20210208170022.076657@ubuntu>
~> X-Mailer: swaks v20190914.0 jetmore.org/john/code/swaks/
~>
~> testing 123

~> .
<~ 250 2.0.0 Ok: queued as 657C948415C ~> QUIT <~ 221 2.0.0 Bye
=== Connection closed with remote host.

Настройка почтового клиента

В качестве почтового клиента возьмём предустановленный



Инструкция по выполнению

1. Открыть в браузере веб приложение Gophish по адресу http s: //localhost: 3333

2. Авторизироваться в системе. Пароль находится в логах, а логин - **admin**

```
uilding with native        build. Learn about native build in Compose here: https://docs.docker.con/go/conpose-native-build/
 tarting gophish ...       done
tarting nail               done
 ttaching to gophish,      nail
ophish j          Runtime configuration:
ophish \          {
ophish |                  "admin_server": {
ophtsh                            'listen url"      : "0.0.0.0:3333",
ophish                            "use tls": true.
ophish j                          "cert_path"       "gophlsh_admin.crt",
ophish                            "key path":       "gophish_admln.key*
ophish |
ophish j                  "phist^server": {
ophish |                          "listen_url"      : "0.0.0.0:80",
ophish                            "use_tls": false.
ophish ]                          "cert_path"       "example.crt",
ophish |                          "key path":       "example.key"
ophish |
ophish                    "db_name": "sqlite3'
ophish                     "db_path": "gophish.db",
ophish                    "mlgratlons_preflx"       "db/db_",
ophish |                  "contact_address": '
ophish j                  "logging": {
ophish 1                          filename":
ophish j                          "level": ""
ophish j                  }
ophish            }
ophish j          time=  "2021-02-08T16:56:32Z"     level=warning msg="No contact address has been configured."
ophish j          time=  "2021-O2-O8T16:56:322"     level=warning msg="Please consider adding a contact_address entry in your config.json"
ophish            goose: no migrations to run.      current version: 20201201000000
ophish            tine=  "2021-02-08T16:56:32Z"     level=Info msg="Please login with the username admin and the password l9af8cd8ea838fa5"
ophish J          time=  "2021-02-0BT16:56:32Z"     level=info msg="Starting adnin server at https://0.0.0.0:3333"
ophish |          time=  "2021-02-08T16:56:32Z"     level=info msg="Starting IHAP nonitor manager"
ophish            time=  "2021-02-08T16:56:32Z"     level=info msg="Starting phishing server at http://0.0.0.0:8O"
ophish j          time=  "2021-02-08T16:56:322"     level=info msg="Starting new 1MAP monitor for user adnin"
ophish            time=  "2021■02■08T16:56:322"     level=info nsg="Background worker Started Successfully - waiting for campaigns"
```

2. Создать новый пароль

3. Теперь приступим к настройке ...

4. Настроить профиль отправителя(**Sending Profile**)

IP хоста взять из докера с помощью команды docker exec mail ip a

```
i: lo: <LOOPBACK,UP,LOWER_UP> ntu 65536 qdisc noqueue state UNKNOWN group default qlen 1000 link/loopback
    00:00:00:00:00:00 brd 00:00:00:00:00:00 inet 127.O.0.1/8 scope host lo
       validlft forever preferredlft forever 58: eth0@if69: «BROADCAST,MULTICAST,UP,LOWER_UP> ntu 1500
qdisc noqueue state UP group default link/ether 02:42:ac:12:00:03 brd ffiff iff iff :ff:ff
link-netnsid O Inet 172.18.0.3/16 brd 172.18.255.255 scope global ethO validlft forever preferredlft
forever
```

New Sending Profile

Name:

admin

Interface Type:

SMTP

From:

Ivan Ivanov <admin@domain.com>

Host:

172.18.0.3:25

Username:

admin@domain.com

Password:

••••••••

Ignore Certificate Errors

Email Headers:

X-Custom-Header {{.URL}}-gophish + Add Custom Header

Show 10 entries Search:

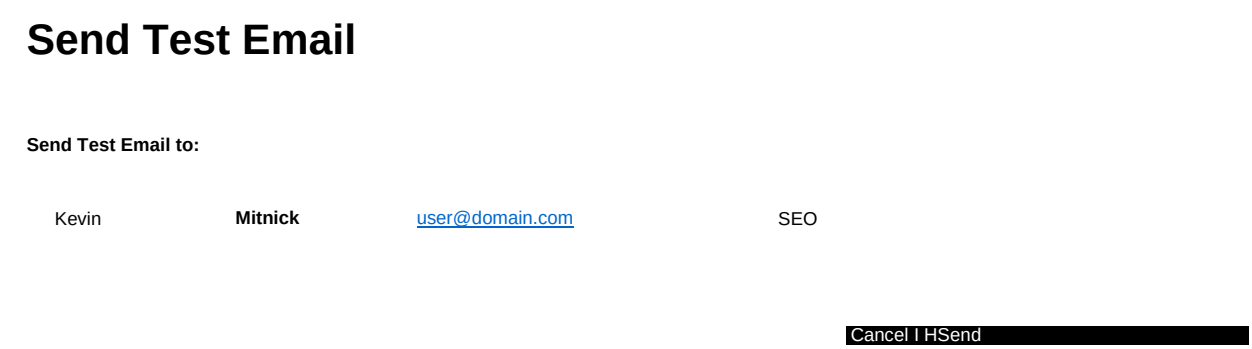
Header	Value
No data available in table	

Showing 0 to 0 of 0 entries Previous Next

Send Test Email

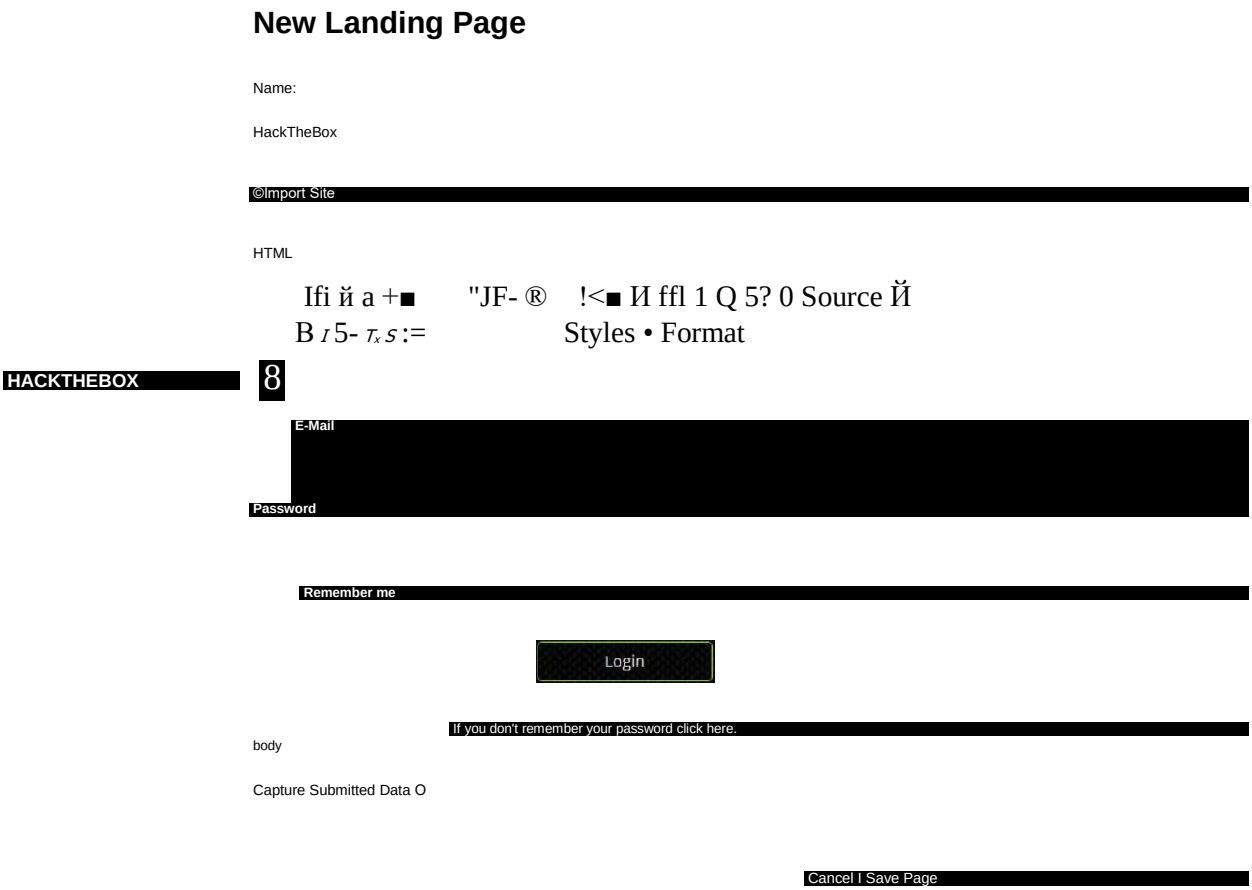
Cancel Save Profile

проверить работоспособность можно с помощью кнопки **Send Test Email**

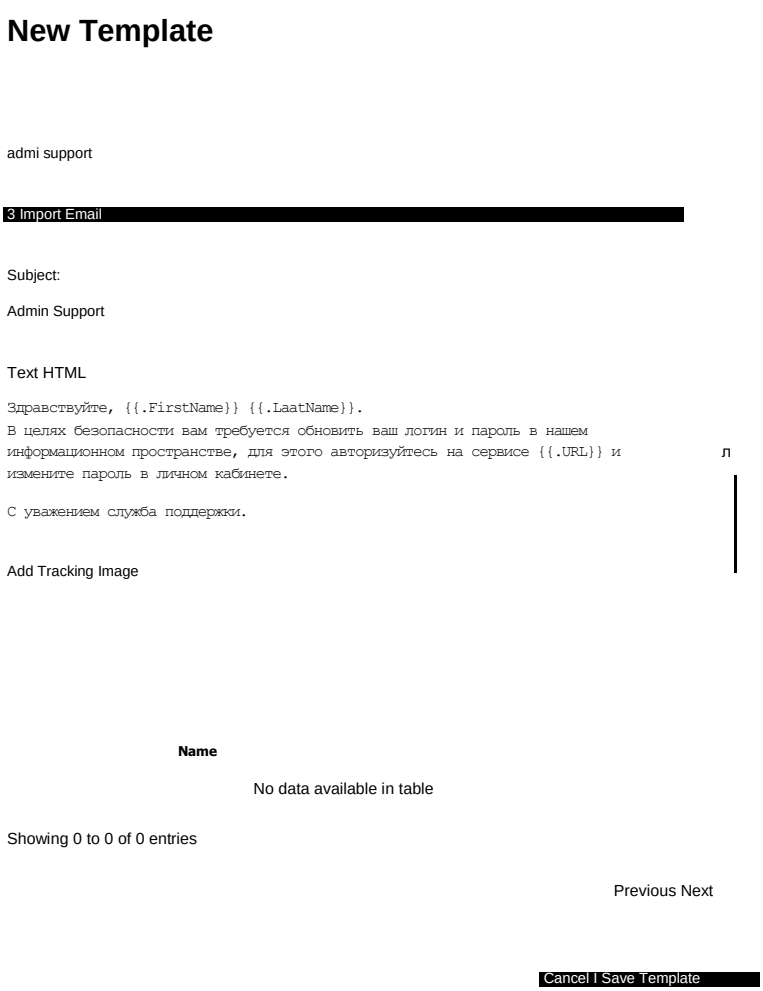


5. Настройка фальшивой страницы**(Ья^1^ Page)**

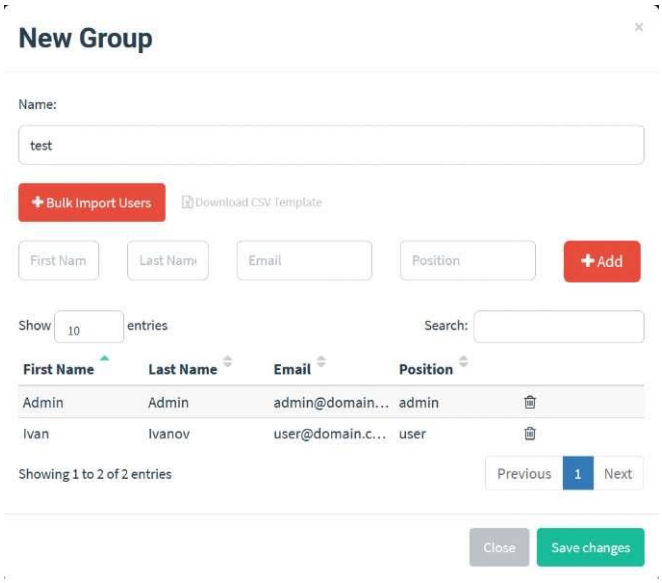
Нажать на кнопку "Import Site" и ввести туда адрес на ваше усмотрение, я выбрал HackTheBox



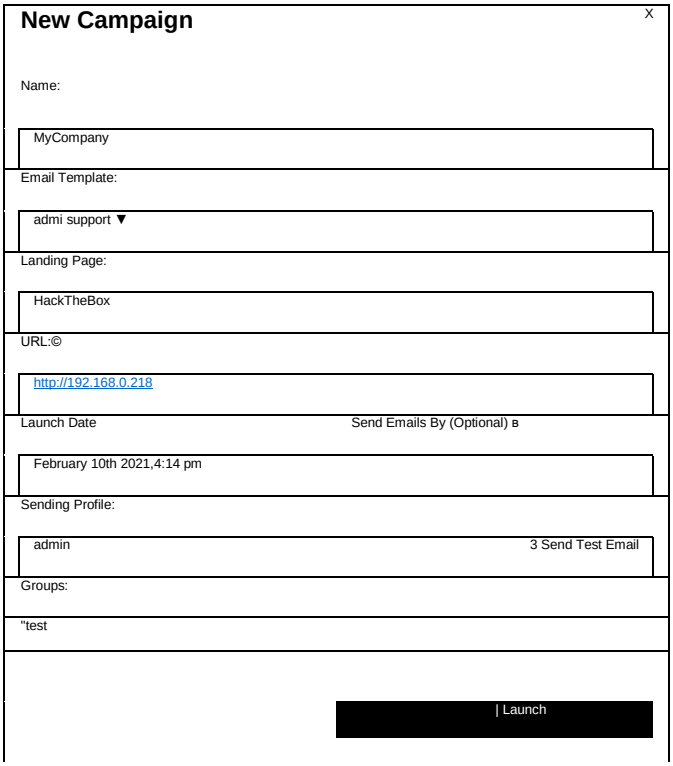
6. Настройка шаблона письма**(Email Template)**



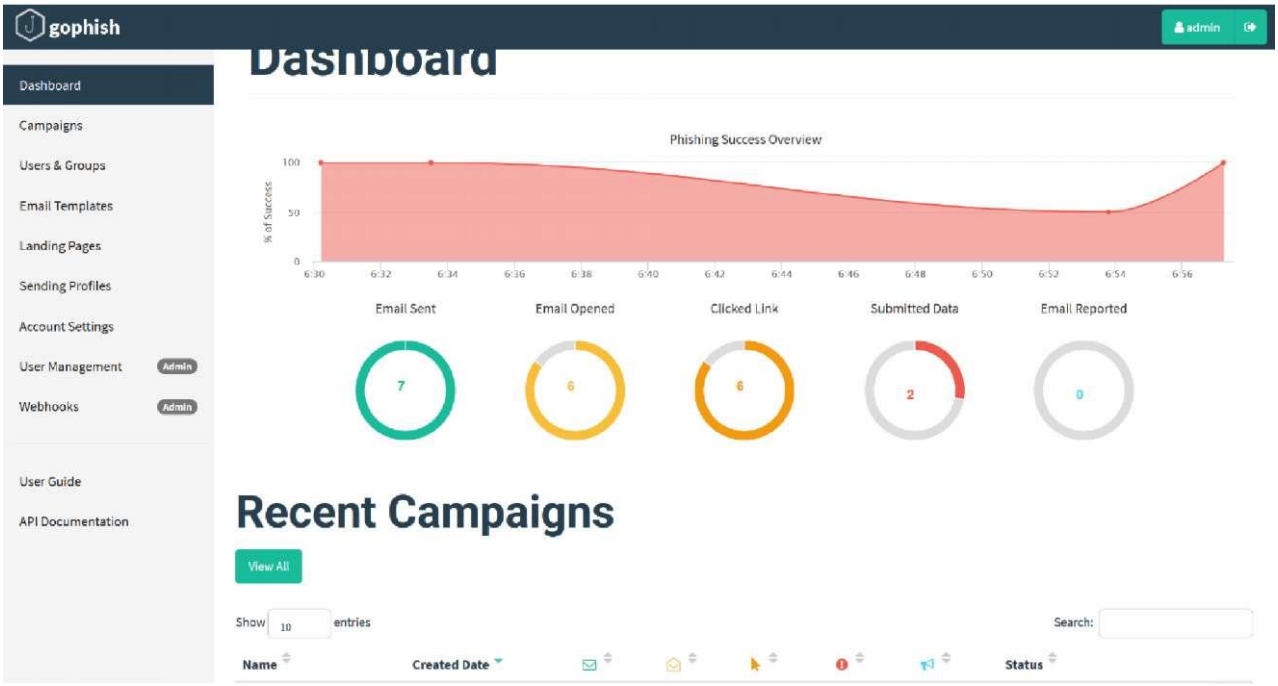
7. Настройка получателей(User & Groups)



8. Настройка рассылки компании(Compaigns)



9. Результат вы можете увидеть у себя во вкладке **Dashboard.** При переходе по ссылке в письме, это будет фиксироваться в круговой диаграмме и на графике, если за основу взять шаблон с логином и паролем, то система автоматически бьдет фиксировать ввод пароля



Содержание отчета по Практической работе

Варианты сдачи, на усмотрение преподавателя

Сформировать отчёт в формате .pdf приложить туда скрины поддельных страниц и писем которые пришли созданным вами пользователями. В отчёте предоставить информацию о проведенном

тестировании, сколько человек перешло по ссылкам, какой процент сотрудников вашей вымышленной компании подверглись атаке и описать советы по предотвращении подобных атак. Проявите фантазию, чтобы преподавателю тоже было интересно читать отчёты.

Предоставить всё вышеперечисленное преподавателю и ответить на вопросы.

По результатам выполнения Практической работы студенты оформляют отчет по Практической работе и защищают его в индивидуальном порядке в форме беседы.

Практическая работа № 4

Тема. Анализ средств противодействия и защиты от различных типов киберпреступлений

Основные теоретические сведения

Пока правоохранительная система и законодательная база совершенствуются в погоне за технологическим прогрессом и легкими на подъем преступниками, рынок систем информационной безопасности может предложить частным и корпоративным потребителям разнообразные комплексные решения, в том числе отечественного производителя.

Для защиты системы, к которой физически имеет доступ только один человек (личный мобильный телефон или ноутбук), вполне достаточно установленного сносного антивируса со встроенным сетевым экраном, несложного приложения для шифрования значимой информации и, конечно, базовых знаний о последних тенденциях в сфере вредоносных программ и возможных вариантах проведения кибератак.

Когда речь идет о локальной сети даже небольшого предприятия, ситуация уже иная, число факторов риска резко возрастает до небес. При возникновении какого-либо происшествия довольно трудно моментально разобраться в причинах инцидента информационной безопасности и тем более найти крайних.

Самыми распространенными способами защиты являются межсетевые экраны, обеспечивающие разделение сетей и направленные на предотвращение нарушений пользователями установленных правил безопасности. Современные межсетевые экраны отличаются удобными панелями управления и довольно большим функционалом (организации VPN, интеграции с антивирусами и другими возможностями). Наблюдаются тенденции к реализации межсетевых экранов аппаратными средствами, что объясняется желанием снизить затраты и повысить степень защищенности.

Одновременно работа производителей антивирусного программного обеспечения направлена на обеспечение нескольких слоев независимых модулей защиты корпоративных сетей. Разрабатываемые системы призваны защищать рабочие станции, контролировать почтовые шлюзы, прокси-серверы и другие возможные пути проникновения вредоносных программ.

Один и тот же вредоносный файл может определяться или не определяться той или иной антивирусной системой, поэтому эффективным решением для более надежной защиты является параллельное использование двух и более антивирусов.

Другим веянием эпохи являются системы обнаружения атак, которые становятся частью комплексов обеспечения безопасности, контроля доступа и средств защиты информации внутри корпоративной сети. Внедряются автоматизированные системы управления информационной безопасностью, обладающие общей консолью управления и возможностями разграничения доступа между сотрудниками согласно их функционалу.

Производители предлагают разнообразные и все более универсальные многозадачные продукты, управление которыми требует от специалистов службы безопасности определенных навыков и курсов обучения.

Однако любое универсальное программное обеспечение состоит из нескольких модулей-приложений, направленных на «закрытие» специфических проблем информационной безопасности. Одни решают вопросы борьбы со спамом и фишингом, другие ориентированы на мониторинг инфраструктуры и поиск сетевых уязвимостей, третьи контролируют корпоративную почту и утечку информации через внешние накопители.

Большинство представленных на рынке продуктов обладает необходимым набором основных функций:

О контроль электронной почты, включая письма и вложения, отсылаемые в том числе через браузер;

О анализ и обмен сообщениями в социальных сетях и других ресурсах; анализ мессенджеров;

О просмотр всех популярных протоколов передачи данных;

О фиксация действий пользователей по записи и их передача на носители информации.

В качестве модного средства для борьбы с инцидентами информационной безопасности в корпоративных сетях внедряются программы для контроля всех действий сотрудников за рабочим компьютером, включающие в себя фиксацию, анализ, блокирование и оповещение об опасной или непродуктивной деятельности.

Действительно, при большой численности персонала и распределенных офисных помещениях без автоматических комплексных решений трудно что-либо контролировать.

Для обеспечения информационной безопасности на предприятиях применяется управление событиями информационной безопасности, включающее в себя сбор, анализ и представление информации от сетевых устройств и приложений. Внедрение управлений событиями призвано унифицировать обработку большинства операций по информационной безопасности.

Из практики можно заключить, что сотрудники финансовых компаний и операторов связи, которые имеют доступ к информации абонентов и клиентов, очень часто становятся не просто источником утечки информации, а участниками преступных групп, занимающихся мошенничеством.

К введению «тотальных» систем безопасности некоторые компании до сих пор относятся с осторожностью, и небезосновательно.

Когда речь идет о контроле корпоративной электронной почты, мониторинге файлов и директорий, запущенных процессов и приложений, логировании системных событий, с законодательной точки зрения все вроде бы понятно. Но когда разговор заходит о таких функциях слежения за сотрудниками, как контроль социальных сетей, отслеживание поисковых запросов и вводимых с клавиатуры значений, снятие скриншотов и просмотр рабочего стола, съемки с

веб-камеры и запись окружения посредством встроенного в ноутбук или компьютер микрофона...

Можно предполагать, как себя чувствуют сотрудники, но автору не по себе даже от перечисления всех этих функций.

Однако, как показывает судебная практика, работодатель вправе контролировать исполнение работником трудовой функции любыми законными способами, включая осуществление контроля за использованием служебной техники и корпоративной почты.

Если в результате такого контроля системы безопасности будет раскрыта личная информация сотрудника компании, то, по мнению суда, виноват будет сам сотрудник, поскольку он использует предоставленные работодателем средства связи в личных целях.

В системах безопасности также применяются программные средства, основанные на анализе интернет-трафика, использовании приложений, аппаратных ресурсов, но весьма сомнительно использование средств перехвата по типу кейлогеров, хотя некоторые специалисты считают это приемлемым.

Различие между представленными на рынке продуктами, по мнению автора, состоит в некоторых пользовательских аспектах, таких как настройка фильтров, оповещений, встроенные аналитические функции.

Автор не тестировал возможности обхода устанавливаемых такими системами ограничений и чуткость организуемого контроля, но, основываясь на опыте, не склонен оценивать высоко степень создаваемой ими защищенности.

При внедрении и использовании таких систем информационной безопасности начинает дремать бдительность сотрудников безопасности, которые реагируют только на сообщения системы.

Комплексные системы призваны сводить к минимуму риски информационной безопасности и, по большей части, направлены на предотвращение утечки конфиденциальной информации.

Положительной чертой таких систем безопасности являются сбор и архивирование данных о событиях в сети, действиях пользователей, соединениях. Эти данные действительно являются ценными и могут оказать неоценимую помощь при расследовании инцидента информационной безопасности.

Методические рекомендации по выполнению Практической работы

1. Выбрать любую утилиту, которая не занята (1 студент - 1 утилита или инструмент) для проведения Компьютерной Криминалистики из списка.

2. Написать отчет-инструкцию максимально подробную:

- Что за инструмент
- Для чего применяется данный инструмент
- Как пользоваться (защита очна, каждый студент рассказывает и показывает функционал утилиты или инструмента).

6. Ответить на теоретические вопросы о работе утилит, инструментов.

^исок инструментов:

- Autopsy

- Encrypted Disk Detector
- Wireshark
- Magnet RAM Capture
- Network Miner
- NMAP
- RAM Capturer
- Forensic Investigator
- FAW
- HashMyFiles
- USB Write Blocker
- Crowd Response
- NFI Defraser
- ExifTool
- Toolsley
- SIFT
- Dumpzilla
- Browser History
- ForensicUserInfo
- Back Track
- Paladin
- Sleuth Kit
- CAINE
- FTK Imager
- dc3dd
- Guymager
- Paragon или Acronis
- Belkasoft RAM Capturer
- Imagemounter
- Libewf
- Xmount
- DumpIt
- Encase Forensic Imager
- Forensics Acquisition of Websites
- Crowd Inspect
- dCode
- Encryption Analyzer

Содержание отчета по Практической работе

По результатам выполнения Практической работы студенты оформляют отчет по Практической работе и защищают его в индивидуальном порядке в форме беседы.

Практическая работа № 5

Тема. Оценка средств, реализуемых в рамках «Чёрного рынка» информационных услуг в РФ

Основные теоретические сведения

OSINT (англ. Open source intelligence) или разведка на основе открытых источников включает в себя поиск, сбор и анализ информации, полученной из общедоступных источников. Ключевой целью является поиск информации, которая представляет ценность для злоумышленника либо конкурента. Сбор информации во многом является ключевым элементом проведения пентеста. От того, насколько качественно он был осуществлён, может зависеть, как эффективность пентеста в целом, так и эффективность отработки отдельных векторов атаки (социальная инженерия, брутфорс, атака на Web-приложения и пр.). В разрезе кибербезопасности/пентеста OSINT чаще всего применяется для сбора публичных данных о компании, и это касается не только информации о email-адресах ее сотрудников. Не менее интересной будет информация о:

- DNS-именах и IP-адресах;
- доменах и субдоменах, зарегистрированных за компанией;
- фактах компрометации почтовых адресов;
- открытых портах и сервисах на них;
- публичных эксплойтах для найденных сервисов;
- конфиденциальных документах;
- имеющихся механизмах безопасности и т.д.

Сегодня посмотрим с помощью каких инструментов и какую информацию можно найти в открытых источниках на примере нашей компании.

Статья носит информационный характер. Не нарушайте законодательство.

Консольные инструменты

TheHarvester

TheHarvester - это целый фреймворк для сбора e-mail адресов, имён субдоменов, виртуальных хостов, открытых портов/банеров и имён сотрудников компании из различных открытых источников. Позволяет производить как пассивный поиск по нескольким поисковым системам: google, yahoo, bing, shodan.io, googleplus, linkedin и т.д., так и активный — например, перебор имен субдоменов по словарю.

Используя различные поисковые источники можно получить различный результат. Например, при использовании поисковой системы Yahoo:

```
# theHarvester -d pentestit.ru -b yahoo
```

```
[*] Target: peritestit.ru

[»] Searching Yahoo.

[*] No IPs found.

[*] Emails found: 4
      .^pentestit. ru
      (apentestit. ru
          (apentestit.ru _
           (apentestit. ru

[*] Hosts found: 18

corplab.pentestit.ru:37.187.73.112
edu.pentestit.ru:37.187.73.112 httpsedu.
pentestit.ru: httpslab.pentestit.ru:
```

```
httpswaf.pentestit.ru:
httpswebinar.pentestit.ru:
httpswww.accessify.compcorplab.pentestit.ru:
httpswww.pentestit.ru:
httpswww.reddit.comdomainlab.pentestit.ru:
lab.pentestit.ru:37.187.73.112
mail.pentestit.ru:10.1.4.12
sites.vulns.pentestit.ru:192.168.68.28
vpn.pentestit.ru:91.121.71.57
waf .pentestit.ru:37.187.73.112
webinar. pentestit.ru:37.187.73.112
www.pentestit.ru:37.187.73.112
root@kali: |
```

А при использовании Google: # theHarvester -d pentestit.ru -b google

```
[*] Target: pentestit.ru

[*] Searching Google.
        Searching 0 results.
        Searching 100 results.
        Searching 200 results.
        Searching 300 results.
        Searching 400 results.
        Searching 500 results.

1*1 No IPs found.

[*] Emails found: 3

    Jlpentestit. ru
    ■@pentestit. ru
    @pentestit.ru

1*1 Hosts found: 11

2017.pentestit.ru:37.187.73.112 ip.pentestit.ru:37.187.73.112
lab.pentestit.ru:37.187.73.112 nw.pentestit.ru:37.187.73.112
samag.pentestit.ru: vpn-t.pentestit.ru:95.107.11.32
vpn.pentestit.ru:91.121.71.57 vulns.pentestit.ru:37.187.73.112
waf.pentestit.ru:37.187.73.112 www.pentestit.ru:37.187.73.112
root@kali:~# |
```

Dmitry

Dmitry - еще один консольный инструмент для поиска информации об интересующих хостах. Базовый функционал может собирать возможные субдомены, адреса электронной почты, информацию о времени безотказной работы, сканирование TCP-портов, поиск whois и многое другое. Функционал довольно обширный, но по возможностям и скорости обнаружения открытых портов все же уступает предыдущему инструменту, но это не мешает использовать их совместно. Все-таки, подобные вопросы требуют использования информации из разных источников для большей достоверности.

dmitry -winsepfb pentestit.ru

```
Gathered Inic-whois information for pentestit.ru


domain:         PENTESTIT.RU
nserver:        nsl.pentestit.ru. 37,107.79,86
nserver:        ns2,pentestit.ru. 95.1Q7.11.32
state:          REGISTERED, DELEGATED, UNVERIFIED
```

```
person:          Private Person
registrar:       REGRURU
admin-contact: http://www.reg.ru/vrfhois/admin contact
created:         2013-04-2BT17:54:53Z
paid-till:       2021-04-28T18:54:532
free-date:       2021-05-29
source:          TCI
```

Чтобы получить максимальное количество информации о домене указываем все ключи. В числе прочего, инструмент будет сканировать порты, но в ограниченном диапазоне, поэтому лучше для этих целей использовать Nmap Nmap

Nmap («Network Mapper») — это утилита с открытым исходным кодом для исследования сети и проверки безопасности. Она была разработана для быстрого сканирования больших сетей, хотя прекрасно справляется и с единичными целями. Это нестареющая классика и первый инструмент, который используют при проведении пентеста. Его функционал довольно обширен, но в нашем случае от него потребуется только определение открытых портов, названия запущенных сервисов и их версии.

nmap -v pentestit.ru -sV -Pn

```
Not shown: 997 filtered ports PORT STATE SERVICE VERSION 80/tcp open http
nginx 443/tcp open ssl/http nginx 8443/tcp closed https-alt
```

Узнав открытые порты запустим тот же Nmap, но уже будем использовать различные группы скриптов, которые помогут обнаружить возможные ошибки конфигурации:

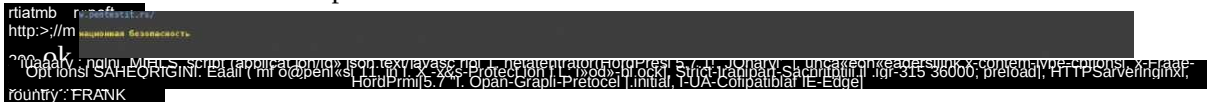
nmap -sV pentestit.ru --script "version, discovery, vuln, auth" -p22,80,443 -Pn

При выполнении этой команды Nmap выполнит все скрипты, собранные в этих группах для получения информации из каждой группы: получение расширенного вывода версии сервисов, поиск расширенной информации о сервере, поиск публичных уязвимостей и т.д. Эта информация так же поможет определить возможные точки входа в сетевой периметр организации.

WhatWeb

Многие компании имеют свой сайт, который также можно проанализировать. WhatWeb как раз идентифицирует веб-сайты. Главная задача инструмента - ответить на вопрос какие технологии использует веб-приложение. WhatWeb распознает веб- технологии, в том числе систему управления контентом (CMS), пакеты статистики/аналитики, библиотеки JavaScript, и многое другое. Имеет более 1700 плагинов, каждый из которых предназначен для распознавания чего-то одного. Также идентифицирует номера версий, email адреса, ID аккаунтов, модули веб-платформ, SQL ошибки и прочее.

whatweb -v pentestit.ru



TiDos

TiDos - универсальная платформа, охватывающая всё от сбора начальных данных до анализа на уязвимости. В своем арсенале имеет 5 модулей, которые позволяют

выполнять как поиск информации о цели в открытых источниках, так и искать некоторые уязвимости (но все же не является полноценным сканером уязвимостей). Так как нас интересует только сбор информации, то и рассматривать будем только один раздел, содержащий порядка 50 модулей. Этот раздел позволяет проводить как пассивный сбор данных:

• поиск email-адресов и прочую контактную информацию в Интернете;

• информацию о домене (whois-информация);

• информацию о конфигурации DNS;

• список субдоменов;

• список подсетей и т.д.

так и активный:

• сбор баннеров;

• проверка файлов robots.txt и sitemap.xml;

• определение CMS;

• определение альтернативных версий сайта путем обращения с различным параметром User-Agent;

SpiderFoot

SpiderFoot - это инструмент автоматизации проведения OSINT. Он интегрируется со многими доступными источниками данных и использует ряд методов анализа данных, что упрощает навигацию по этим данным. SpiderFoot не совсем консольный инструмент т.к. имеет встроенный веб-сервер с интуитивно понятным веб- интерфейсом. Позволяет собирать информацию о:

• IP-адресах;

• Домены/Субдомены;

• Имена пользователей;

• Телефонные адреса;

• Проверка некоторых данных на предмет утечки и т.д.
Примеры результатов

pentestit_scan renins

Φ Summary | Browse | * Graph | Φ Scan Settings | ■ Log

Browse IP Address

Data Element	Source Data Element	Source Module	Identified
10.1.4.12	mail.pentestit.ru	sfp_dnsresolve	2021-04-28 05:37:16
188.165.231.27 192.168.222.1	hn4.pentestit.ru	sfp_dnsresolve	2021-04-28 05:38:33
	hnl.pentestit.ru	sfp_dnsresolve	2021-04-28 05:38:02
37.187.73.112	lab.pentestit.ru	sfp_dnsresolve	2021-04-28 05:34:08
37.187.73.112	www.pentestit.ru	sfp_dnsresolve	2021-04-28 05:33:17
37.187.73.112	audit.pentestit.ru	sfp dnsresolve	2021-04-28 05:36:12
	ip.pentestit.ru	sfp_dnsresolve	2021-04-28 05:36:54
37.187.73.112 37.187.73.112	wl.pentestit.ru	sfp_dnsresolve	2021-04-28 05:37:16
37.187.73.112 □	repository.pentestit.ru	sfp_dnsresolve	2021-94-28 05:37:39
37.187.73.112	webinar.pentestit.ru	sfp_dnsresolve	2021-04-28 05:37:39

pentestitscan ^^

Φ Summary -E Browse # Graph Φ Scan Settings fll Log

Browse Account on External Site

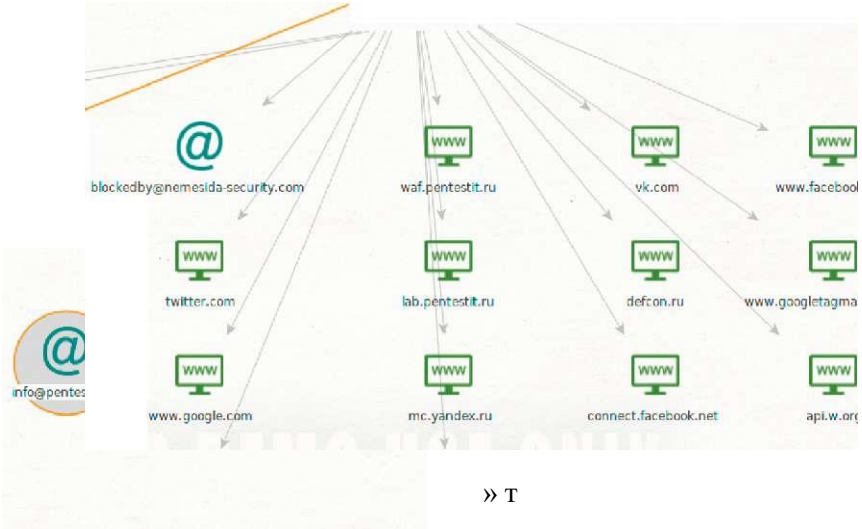
Data Element Module	Data Element	Source Source Identified		
	Career.habr (Category: business) https://career.habr.com/pentestit	pentestit	sfp_accounts	2021-04-28 05:27:26
	DockerHub (Category: coding) https://hub.docker.com/v2/users/pentestit/	pentestit	sfp_accounts	2021-04-28 05:27:24
	GitHub (Category: coding) https://github.com/pentestit	pentestit	sfp^ accounts	2021- 04-28 Q :27 :24 5: :
	Internet Archive User Search (Category: misc) https://archive.org/search.php?query=pentestit	pentestit	sf .accounts p_	2021- 04-28 05 :27 :27 : :
	Medium (Category: news) https://medium.com/@pentestit	pentestit	sf .accounts p_	2021- 04-28 65 : : 25 : 27:
	Pinterest (Category: social) https://www.pinterest.com/pentestit/	pentestit	sf ^accounts p_	2021- 04-28 Q : : 25 5: 27:
	Repl.it (Category: coding) https://replit.com/@pentestit	pentestit	sf .accounts p_	2021 04-28 05 :27 :25 : :
	Telegram (Category: social) https://t.me/pentestit	pentestit	sfp_accounts	2021-04-28 05:27:25

Maltego

Maltego - довольно популярный инструмент для проведения OSINT мероприятий и построения взаимосвязей в виде графов. Бесплатной версии может быть вполне достаточно для поиска информации, однако нужно помнить, что для многих модулей, например поисковой системы Shodan, требуется получить API ключи задействованных сервисов.

Пример результатов

pentestit.ru



» T

hostmaster@ripe.net

a
Proxy

A
Abuse velocity: low

37.187.73.112

abuse@ripe.net @ abuse@ovh.net

A

По окончании можно можно софрмировать отчет в формате PDF для удобного просмотра найденной информации. Пример отчета

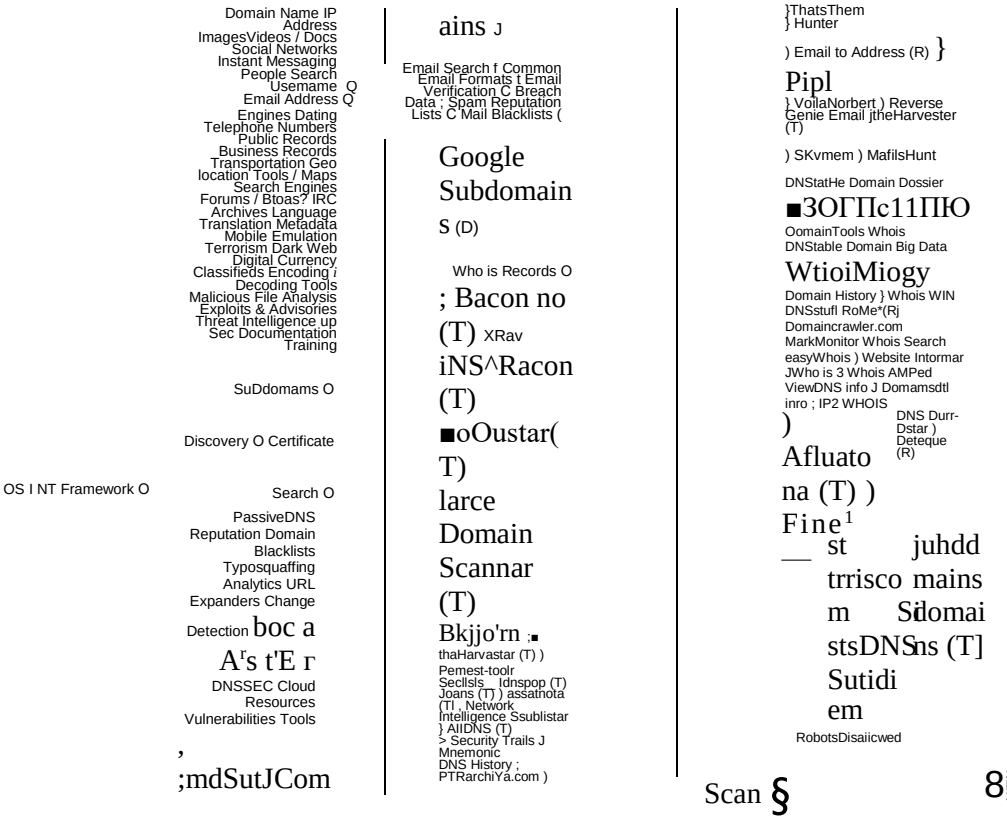
1. Top 10 Entities

Использование онлайн-сервисов также один из возможных путей при проведении сбора данных о цели. Обобщенная база таких сервисов - это osintframework. Здесь собраны и отсортированы по разделам различные инструменты. К слову говоря, здесь также предоставлены ссылки на полезные инструменты и фреймворки, относящиеся к конкретному разделу, как например, TheHarvester или Recon-ng. osintframework.com

Website Titles (1)

Pentestit | Информационная безопасность

3. Entity Details



Поиск email

hunter - на сайте вводим название комании или ее домен, и получаем список адресов, которые удалось найти вместе с ресурсами, где эти данные фигурировали.

♦- hunter Login

All the email

pentestit.ru

addresses found for pentestit,ru 6

Most common pattern:

{fHlastHPpentestit.ru i o@>pentestit.ru •

m harkovPpentestit.ru •

5 email addresses

htt p:// ro 5 sbiz, ru /h o m e/1696 63 Dec 23, 2018

20+ sources 1

h p@ipentestit.ru • n f@pentestit.ru •

1 source

d o@pentestit.ru •

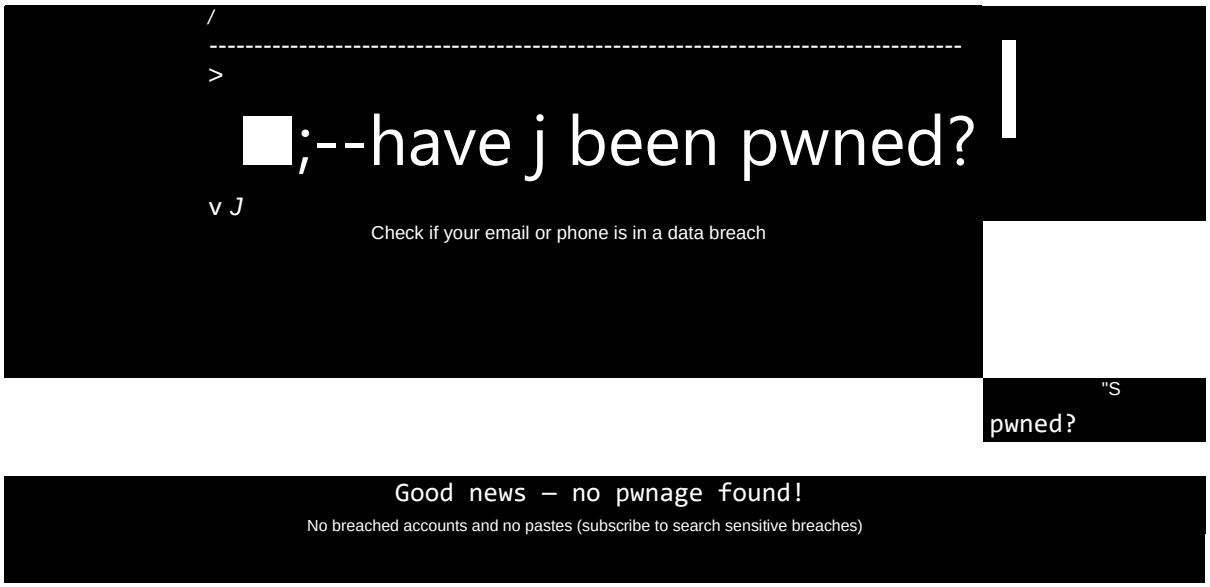
3 sources 1

9 sources ■

4 sources 1

Как приятный бонус доступно расширение для браузера, которое при посещении веб-сайта будет автоматически искать связанные с ним email-адреса. mailshunt - по аналогии с предыдущим сервисом указываем домен компании и получаем список найденных учетных записей.

Найденные email-адреса можно проверить на предмет утечки на известном сервисе haveibeenpwned.com. Скомпрометированные пароли отображаться не будут, но так хотя бы можно будет разделить список адресов на "чистые" и потенциально скомпрометированные. _____



Whois

who.is - вводим домен компании и в ответе получаем whois-информацию, DNS- записи и т.д.

pentestit.ru

DNS information Whois Diagnostics

DNS Records for pentestit.ru

cache expires in 4 minutes and 51 seconds

Hostname	Type	TTL	Priority	Content
pentestit.rj	SOA	59		hydrogen.ns.hetzner.com dns@hetzner.com 2021040700 86400 10800 3600000 3600
pentestit. ш	NS	59		helium.ns.hetzner.de
pentestit. ш	NS	59		hydrogen.ns.hetzner.com
pentestit. ш	NS	59		oxygen.ns.hetzner.com
pentestit. ru	MX	59	10	mail.p@ntBstit.ru
WMW.pentestit.ru	A	59		37.187.73.112

2whois — помимо получения whois-информации сервис предоставляет онлайн- сервисы nslookup, dig, анализ DNS и многое другое. Результат

Домен или IP

pentestit.ru

@ Проверить

® Домен pentestit.ru занят!

О Информация о домене *pentestit.ru* по данным whois.ripn.net:

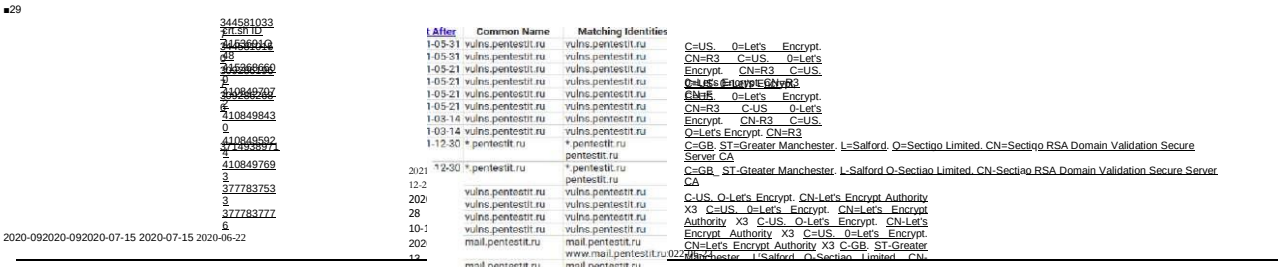
dome ir_:	PENTESTIT. SI"
nse rver:	heliun.ns.hetzner.de.
r.se rver:	hydrogen.ns.hetzner.com.
: ,'L'i:	oxygen . ns . hetzner . corn.
stale:	REGISTERED, DELEGATED, UNVERIFIED
pe r son:	Privets Person
reg istra r:	REGRU-RU
aamin-сслtac:	: http://www.reg.ru/whois/adjriin oonzact
created:	2Г113-04-2ВГ17 : :53z
paid-tlll:	2D22-04-2BT18:54:53Z
free-da:	2022-05-29
£ource:	TCI
La si updated	on 2021-D4-25T10:36:3QZ

О Записи с DNS серверов для домена *pentesdt.ru :*

ХОСТ	КЛАСС	ТИП	СОДЕРЖАНИЕ ЗАПИСИ	TTL
pentestit.ru	IN	NS	**target** = helium, ns.hetzrer.de	59 сек,
pentestit.ru	IN	NS	**target** = hydrogen.ns hetznercom	59 сек.
pentestit.ru	IN	NS	**target** = oxygen ns.hetzner.com	59 сек,
pentestit.ru	IN	SOA	**mname** = hydrogen.nshetzner.com **rname** = dns.hetznercom **serial** = 2021040700 **refresh** = 86400 **retry** = 10800 **expire** = 3600000 **rninimum-ttl** = 3600	59 сек.
pentestit.ru	IN	MX	**pri =** 10 **target** = mail.pentestit**.ru**	59 сек.
pentestit.ru	IN	TXT	**txt** = v=spf1 +mx-all **entries =**	59 сек,

crt.sh - еще один полезный и довольно простой в использовании сервис поиска субдоменов.

Type: Identity Match: ILIKE Search:'pentestit.ru



Также можно воспользоваться сервисом securitytrails.com для все того же поиска субдоменов.

Domain	Rank	Hosting Provider
lab.pentestit.ru	193,001	OVH SAS
pentestit.ru	5,211,625	
zsa.pentes-tit.ru		OVH SAS
aud it.pentestit.ru		OVH SAS
hn4.pentestit.'u		OVH SAS
corplab.pentestit.ru		OVH SAS
ns2.pentesth.ru		
hn2.pentesti:.ru		
mail.pentestit.ru		OVH SAS
www.pentestit.ru		OVH SAS
remote.pentestit.ru		PJSC Rostelecom
vpn.pentestit.ru		OVH SAS
rl.pentestit ru		PJSC Rostelecom
edu.pentestr.ru		OVH SAS
vulns.pentestit.ru		OVH SAS

hackertarget - инструмент схож с предыдущими, т.к. использует в своем арсенале инструменты с открытым исходным кодом, но в этом случае набор инструментов значительно расширен, что позволяет дополнительно использовать, например, OpenVas, Nmap, Nikto, WhatWeb и т.д. Результат

rl.pentestit.ru,95.167.11.32 hn4.pentestit. ru,
188.165.231.27 hn6.pentestit.ru,91.121.71.57
zsa.pentestit,ru,37.137.73.112
lab.pentestit.ru,37.187.73.112
corplab.pentestit.ru,37.187.73.112 waf.
pentestit. ru, 37.137.. 73.112
mail.pentestit.ru,37.137.79.36
lp.pentestit.ru,37.187.73.112
webinar.pentestit.ru,37,187.73.112
watcher.pentestit.ru,147.78.67. 77 vulns .
pentestit. ru,37.187.73.1.12 audit.
pentestit.ru,37.187.73.112
riw.pentestit.ru,,37,187.73.112
www.pentestit,ru,37.187,73.112
repository.pentestit.rUj 37.187.73.112

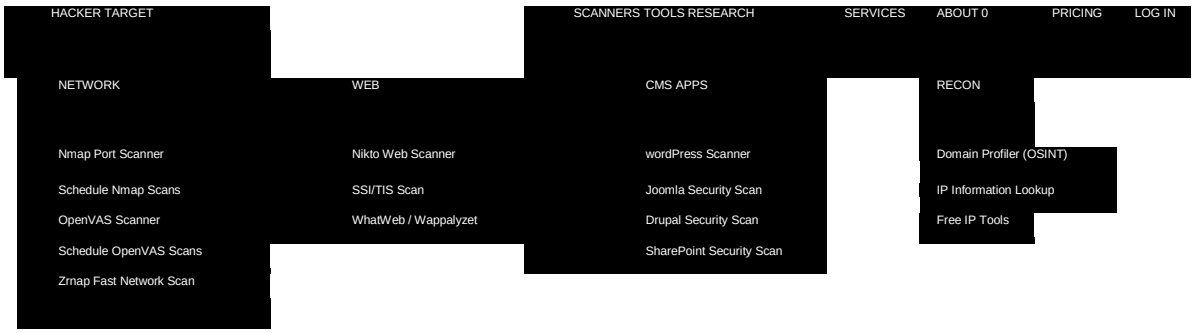
Online Test of a zone transfer that will attempt to get all DNS records for a target domain. The zone transfer will be tested against all name servers (NS) for a domain. pentestit.ru

CHECK EXTERNAL ZONE TRANSFER

; <o> DiG 9.11.3-lubuntul. 14-Ubuntu <o> axfr @helium.ns, hetzner.de pentestit.ru ; (2 servers found) ;; global options: +cmd ; Transfer failed.

; <o> DiG 9.11.3-lubuntul.14-Ubuntu <o> axfr @oxygen.ns, hetzner.com pentestit.ru ; (2 servers found) ;; global options: +cmd ; Transfer failed.

; «» DiG 9,11.3-lubuntul.14-Ubuntu <o> axfr {ahydrogen . ns. hetzner. coin pentestit.ru ; (2 servers found) ;; global options: +cmd ; Transfer failed.

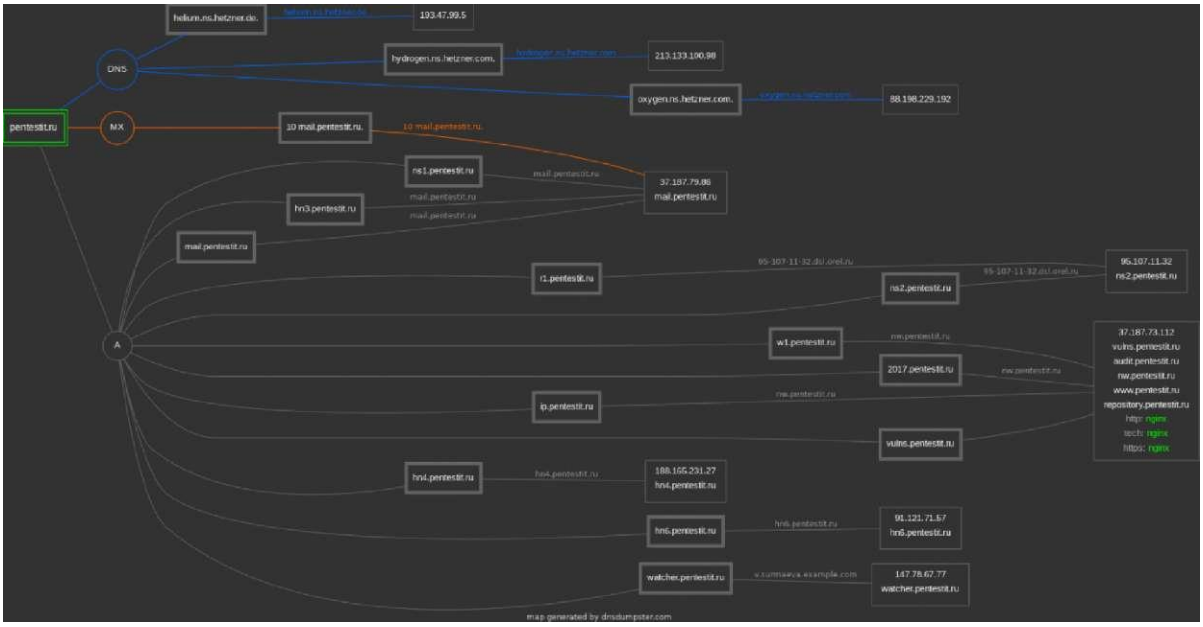


dnsdumpster.com — умеет рисовать графы взаимосвязей и выгружать результаты в Excel, но имеет ограничение на выдачу только 100 субдоменов.

Google Dorks

Google Dork Queries (GDQ) - это набор запросов для выявления индексируемых поисковой системой страниц. Одним словом - всего, что должным образом не спрятано от поисковых роботов. Вот небольшой список команд, которые чаще всего используются:

- **site** - искать по конкретному сайту;
- **inurl** - указать на то, что искомые слова должны быть частью адреса страницы/сайта;
- **intitle** - оператор поиска в заголовке самой страницы;



• **ext** или **filetype** - поиск файлов конкретного типа по расширению.

Комбинируя различным образом команды для поиска можно найти практически все, вплоть до логина/пароля администратора.

site:pentestit.ru filetype:pdf X H | Q,

Q Все О Картинки Щ) Новости <J> Покупки ф Карты і Ещё Настройки Инструменты

Результатов: 3 (0,24 сек.)

https://wafpertestit.**ru** > wp-content > uploads > N... ▼ PDF

Презентация - Nemesida WAF - Pentes1i1

Управление и мониторинг работы Memesida. WAF производится через веб-интерфейс, а обновление компонентов— через **Linux-** репозиторий.

https://waf.pertestit.**ru** > uploads > policy_nwc **т** PDF

Регламент использования Nemesida WAF Cloud

ПРАВОМЕРНОЕ ИСПОЛЬЗОВАНИЕ 2.1. Клиент обязуется использовать Сервис исключительно в законных целях в соответствии с настоящим ...

https://waf.pentestit.**ru** > uploads > nws_eula ~ PDF

Лицензионное соглашение с конечным пользователем

21 сент. 2020 г. — ПО «Nemesida WAF» - программное обеспечение «Nemesida WAF», принадлежащее Лицензиару, экземпляр которого правомерно ...

Можно ли где-то найти готовые запросы для поиска информации? - Можно. На

Методические рекомендации по выполнению Практической работы

1. В соответствии с вариантами Практической работы провести поиск информации из открытых источников

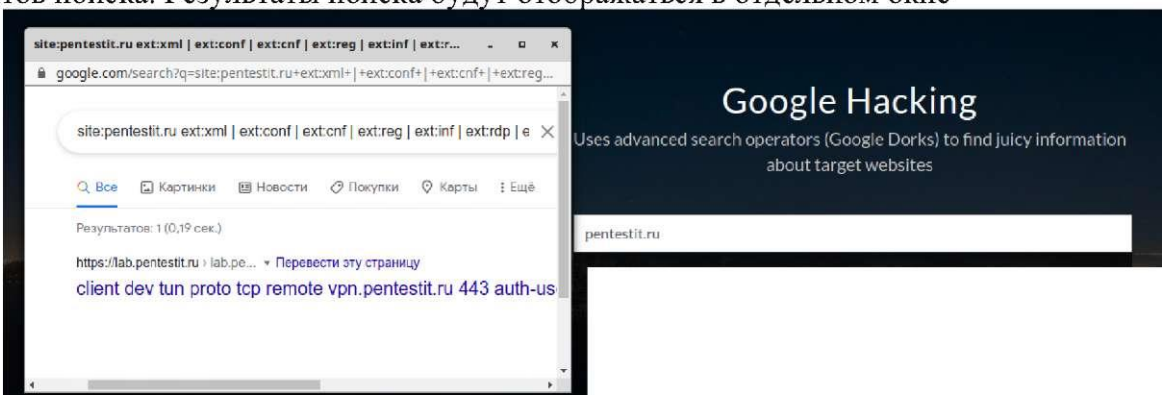
Результаты Практической работы занести в отчет **Содержание отчета по Практической работе**

Q Publicly exposed documents Q Directory listing vulnerabilities Q Configuration files exposed Q, Database files exposed Q. Logfiles exposed Q. Backup and old files Q Login pages

Q. SQL errors Q PHP errors/warnings Q phpinfoO Q. Search Pastebin.com/pastingsites Q. Search Github.com and Gitiab.com Q. Search Stackoverflow.com Q Signup pages

exploit-db в разделе google hacking database.

pentest-tools - полезный ресурс для сбора инормации, но в бесплатном варианте имеет множество ограничений, например, 2 сканироания в сутки. Но при этом бесплатно доступен Google Hacking, где достаточно указать домен и выбирать из предложенных вариантов поиска. Результаты поиска будут отображаться в отдельном окне



По результатам выполнения Практической работы студенты оформляют отчет по Практической работе и защищают его в индивидуальном порядке в форме беседы.

Практическая работа № 6 Тема. Исследование принципов социальной инженерии в киберпреступлениях

Основные теоретические сведения

Хакеры используют методы *социальной инженерии,* чтобы обманом заставить жертв предоставить им доступ к своим системам. Социальная инженерия предполагает использование технологий в целях оказания на человека психологического воздействия. Эти методы применяются для кражи паролей, дестабилизации работы правительств и фальсификации результатов выборов.

Вероятно, вы уже знакомы с методами социальной инженерии, с помощью которых злоумышленники пытаются заставить пользователей совершить то или иное действие. Такие методы называются *фишинговыми* атаками. Опытные пользователи обычно довольно легко распознают поддельные электронные письма, а спам-фильтры вполне эффективно выявляют их по характерному содержимому и орфографическим ошибкам, а это означает, что от плохо спланированных атак защититься совсем не сложно.

Тем не менее при использовании подходящей наживки фишинговая атака может оказаться весьма успешной. В этой работе мы рассмотрим три метода социальной инженерии, которые позволяют хакерам создавать поддельные электронные письма, сайты и видео, а затем применим их для осуществления единой скоординированной атаки.

Изощренная атака с применением социальной инженерии

Вот пример атаки, которую можно было бы осуществить, используя методы, описанные в этой работе. На первом этапе хакер отправляет поддельное электронное письмо от имени Facebook, в котором сообщается, что жертва была отмечена на некой фотографии. Щелкнув на ссылке в данном письме, жертва попадает на поддельный экран входа в систему Facebook. После попытки аутентификации жертва перенаправляется на реальную страницу входа в Facebook, а ее имя пользователя и пароль отправляются хакеру. На этот раз жертва успешно проходит аутентификацию в системе, вероятно полагая, что в первый раз она просто ввела неправильный пароль.

Подобные атаки с использованием электронной почты также можно комбинировать с методами социальной инженерии, предполагающими использование мультимедийного контента. Например, в дополнение ко всему прочему хакер может создать голосовое или видеосообщение от супруга жертвы, рекомендующего ей ожидать получения определенного письма или текстового сообщения. Или сгенерировать дипфейк-видео, на котором

генеральный директор предупреждает своих сотрудников о том, что в скором времени им поступит некое электронное сообщение. *Подделка электронных писем*

Чтобы понять, как злоумышленники могут отправлять поддельные электронные письма, сначала необходимо разобраться с принципами работы электронной почты. На рис. 7.1 схематически показан процесс передачи электронного письма.

В основе работы электронной почты лежит совокупность *почтовых серверов,* и каждый почтовый домен (например, @virginia.edu) связан с одним или несколькими почтовыми серверами, которые сортируют входящие сообщения по соответствующим почтовым ящикам и отправляют исходящие сообщения на другие почтовые серверы. Когда Алиса (alice@companyX.com) решает отправить сообщение Джону на адрес john@companyY.com, она загружает свое электронное письмо на почтовый сервер своей компании, который помещает его в свою очередь исходящих сообщений. Как только электронное письмо достигает начала этой очереди, сервер выполняет поиск в DNS, чтобы выяснить IP-адрес почтового сервера Джона.

Затем почтовый сервер Алисы устанавливает TCP-соединение с почтовым сервером Джона и использует *простой протокол передачи почты* (simple mail transfer protocol, SMTP) для передачи электронного письма на почтовый сервер Джона. SMTP — это текстовый протокол, позволяющий почтовым серверам обмениваться информацией. Безопасная версия этого протокола, SMTPS, предполагает использование TLS-соединения для обмена сообщениями.

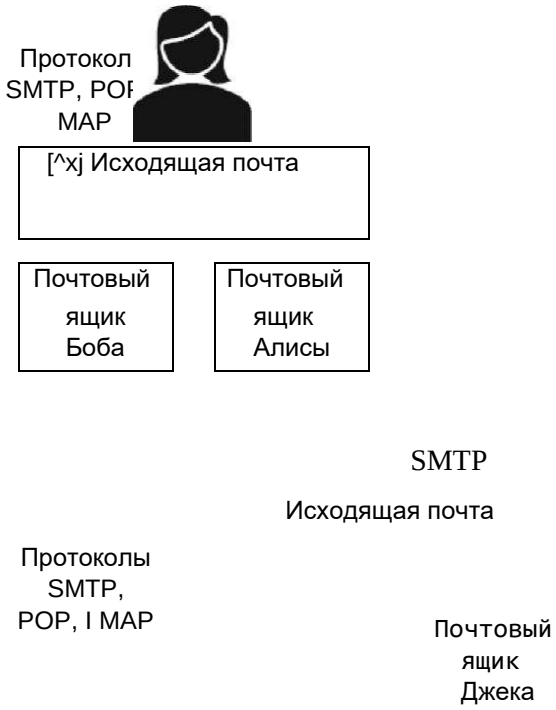


Рис. 7.1. Процесс передачи электронного письма

Когда почтовый сервер Джона получает письмо Алисы, он помещает его в почтовый ящик Джона. Затем Джон получает доступ к этому письму, подключившись к почтовому серверу своей компании.

Поиск данных почтового сервера в DNS

Вы можете найти данные почтового сервера в DNS с помощью команды dig. Например, выясним IP-адрес и URL почтового сервера gmail.com. Для этого мы используем флаг mx, чтобы отобразить запись MX (mail exchanger), содержащую информацию о почтовом сервере:
kali@kali:~$ **dig mx gmail.com** ;; ANSWER SECTION: gmail.com. 3435
IN MX 5 gmail-smtp-in.l.google.com. ' gmail.com. 3435 IN MX 10
alt1.gmail-smtp-in.Lgoogle.com. gmail.com. 3435 IN MX 40 alt4.gmail-
smtp-in.l.google.com.

Мы видим несколько почтовых серверов, каждому из которых назначен приоритет. Почтовый сервер с наименьшим номером ' имеет наивысший приоритет. Именно к нему вам следует подключиться в первую очередь. Итак, gmail-smtp-in.l.goog- le.com — это SMTP-сервер, который принимает соединение на порте 25.

Обмен данными по протоколу SMTP Обмен данными по протоколу SMTP напоминает обычный разговор, но, разумеется, предполагает использование специальных кодов. Рассмотрим эти сообщения, чтобы лучше разобраться в том, как работает данный протокол.

Взламывать чужие компьютеры незаконно и неэтично (а нам рано или поздно потребуется взломать SMTP-сервер), поэтому воспользуемся SMTP-сервером, работающим на порте 25 нашей виртуальной машины Metasploitable. Убедитесь в том, что Kali Linux и pfSense работают. Затем запустите виртуальную машину Metasploitable и войдите в систему, используя имя пользователя msfadmin и пароль msfadmin. Выполните следующую команду, чтобы получить IP-адрес сервера: msfadmin@metasploitable:~$ **ifconfig eth0**

eth0 Link encap:Ethernet HWaddr 00:17:9A:0A:F6:44 inet addr: 192.168.1.101 Bcast:192.168.1.255 Mask:255.255.255.0 ' Значение после inet addr: " — и есть IP-адрес. Помните о том, что в вашей лаборатории этот адрес может быть другим.

Используйте инструмент netcat на виртуальной машине Kali Linux для подключения к порту 25 на этом IP-адресе, выполнив следующую команду: kali@kali:~$ **nc 192.168.1.101 25**
Server: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)

Установив соединение, сервер посылает в ответ код 220, который свидетельствует об успешном подключении. В данном случае мы также видим, что машина Metasploitable использует почтовый сервер Postfix с открытым исходным кодом, который поддерживает *расширенный простой протокол передачи почты* (extended simple mail transfer protocol, ESMTP).

Получив сообщение с кодом 220, ответьте сообщением HELO (HELO — это не опечатка). Для большей ясности я отметил клиентский запрос тегом Client:, а ответ сервера — тегом Server:. Эти теги не входят в состав сообщений.

Именно здесь начинается обман. С помощью своего сообщения HELO вы можете выдать себя за кого угодно. В данном случае мы выдаем свой компьютер за сервер secret.gov:
Client: HELO secret.gov
Server: 250 metasploitable.localdomain

Получив наше сообщение, сервер должен подтвердить этот факт, ответив сообщением с кодом 250. Некоторые почтовые серверы используют забавные сообщения наподобие «Сервер Gmail к вашим услугам». Итак, мы проверили идентичность сервера, на который отправляем почту.

Теперь мы можем пойти еще дальше и притвориться, что отправляем почту с адреса head@secret.gov:
Client: MAIL FROM: <head@secretgov> Server:
250 2.1.0 Ok

Сервер отвечает сообщением 250 Ok. Отлично. Он нам поверил. После этого мы отправляем сообщение RCPT TO: с указанием получателя нашего электронного письма. В данном случае в качестве получателя мы указываем учетную запись sys: Client: RCPT TO:<sys> Server: 250 2.1.5 Ok

Если бы машина Metasploitable предусматривала связанный домен, например, virginia.edu, то мы бы указали в качестве получателя <sys@virgina.edu>.

Если этот адрес электронной почты зарегистрирован на сервере, то ответит сообщением 250 Ok, как показано здесь. В противном случае он пришлет сообщение с кодом ошибки.

Возможно, вы уже думаете о том, как хакер мог бы с помощью такого поведения получить с сервера список электронных адресов, однако я советую на время отложить эти размышления. Пришло время отправить основной текст электронного письма. Команда DATA сообщает серверу о нашей готовности загрузить электронное письмо. Client: DATA
Server: 354 End data with <CR><LF>.<CR><LF>

Сервер отвечает сообщением с кодом 354, которое свидетельствует о том, что он готов к приему электронной почты. Оно также содержит инструкции, касающиеся завершения электронного письма. В данном случае мы должны закончить свое электронное письмо символами *возврата каретки* (<CR>) и *перевода строки* (<LF>): <CR><LF>.<CR><LF>. Эти символы остались с тех времен, когда компьютерные клавиатуры напоминали пишущие машинки. (Протокол SMTP был разработан в 1982 году и, несмотря на свой почтенный возраст, до сих пор используется такими современными почтовыми серверами, как Gmail.)

Вот так выглядит письмо, которое мы отправляем: Client:

From: "The Boss Lady" <head@secret.gov> Subject: Hello SYS

Click This link link text Your Enemy, someone . Server: 250 2.0.0 Ok: queued as B16A9CBFC Client: QUIT Server: 221 2.0.0 Bye.

Чтобы убедиться в получении поддельного электронного письма, выполните следующую команду на своей виртуальной машине Metasploitable в целях чтения содержимого почтового ящика sys:
msfadmin@metasploitable:~$ **sudo cat /var/spool/mail/sys**

Вы должны увидеть сообщение от head@secret.gov с введенным вами текстом:

From: "The Boss lady" <head@secret.gov> Subject:
Hello SYS
Message-Id: <20200718011936.45737CBFC@metasploitable.localdomain> Date: Sat, 17
Jul 2022 21:19:14 -0400 (EDT)
To: undisclosed-recipients:;
Click This link <a href-'url">Hnk text
Your Enemy, someone

Поздравляю! Вы отправили свое первое поддельное письмо.

Написание спуфера электронной почты

Выполнять вышеописанные действия вручную довольно утомительно, поэтому напишем небольшую программу на языке Python для отправки поддельных электронных писем. На рабочем столе виртуальной машины Kali Linux создайте новую папку с именем spoofer. В ней создайте файл Python с именем espoofer.py, откройте его в среде разработки или любом текстовом редакторе, а затем скопируйте в него следующий код, который передает сообщения по протоколу SMTP через TCP-соединение. import sys, socket size = 1024
def sendMessage(smtpServer, port, fromAddress, toAddress,message): IP =

smtpServer PORT = int(port)

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM) s.connect((IP, PORT)) # Открытие сокета на порте print(s.recv(size).decode()) # отображение ответа s.send(b'HELO '+ fromAddress.split('@')[1].encode() +b'\n') "" print(s.recv(size).decode())

отправка адреса отправителя: s.send(b'MAIL FROM:<' + fromAddress.encode() + b'>\n')
print(s.recv(size).decode()) # отправка адреса получателя:
s.send(b'RCPT TO:<' + toAddress.encode() + b'>\n') print(s.recv(size).decode()) s.send(b"DATA\n") #
отправка данных print(s.recv(size).decode()) s.send(message.encode() + b'\n') s.send(b'\r\n.\r\n')
print(s.recv(size).decode()) # отображение ответа s.send(b'QUIT\n') # завершение сообщения
print(s.recv(size).decode()) # отображение ответа s.close()

def main(args): smtpServer = args[1] port
= args[2] fromAddress = args[3]
toAddress = args[4] message = args[5] sendMessage(smtpServer, port, fromAddress, toAddress, message)
if__ name__ == " __main _ ": main(sys.argv)

Мы отправляем свое первое сообщение на сервер, выдавая свой компьютер за почтовый сервер, связанный с адресом отправителя "". Затем выводим на экран ответ, полученный от сервера . Далее отправляем данные, после чего завершаем сообщение отправкой символов <CR><LF>.<CR><LF>, которые в языке Python представляются с помощью символов \r и \n. Наконец, мы считываем параметры командной строки, определяющие наш целевой почтовый сервер и заголовки нашего электронного письма .

Теперь запустим этот скрипт Python. Откройте терминал и перейдите в папку, содержащую файл espoofer.py: kali@kali:~$ **cd ~/Desktop/spoofer**

Запустите программу espoofer.py, используя следующие аргументы:
kali@kali:~$ **python3 espoofer.py *<1P-адрес Metasploitable>* 25 ^**
hacking@virginia.edu sys "Hello from the other side! "

В результате выполнения этой программы с адреса hacking@virginia.edu на адрес электронной почты для учетной записи sys будет отправлено сообщение Hello from the other side!.

Подобная атака не всегда оказывается успешной. Некоторые SMTP-серверы могут использовать такие защитные механизмы, как *идентификация сообщений, создание отчетов и определение соответствия по доменному имени* (domain based message authentication, reporting, and conformance, DMARC), которые позволяют принимающему SMTP-серверу удостовериться в том, что SMTP-сообщения получены с авторизованного IP-адреса. Тем не менее существуют и другие хитрости. Например, вы можете зарегистрировать доменное имя, напоминающее атакуемое. Такие инструменты, как URLCrazy, позволяют быстро находить похожие домены. Чтобы сократить количество спама, некоторые интернет-провайдеры блокируют входящие пакеты на порте 25. Поэтому если вы хотите провести аудит системы за пределами своей виртуальной среды, то вам придется направить свой трафик через *виртуальную частную сеть* (virtual private network, VPN).

Методические рекомендации по выполнению Практической работы

Чтобы лучше разобраться в теме фишинга и дипфейков, выполните следующие упражнения. В первом из них вы познакомитесь с методом клонирования голоса с помощью компьютера. Во втором освоите инструмент King Phisher, позволяющий проводить масштабные фишинговые атаки.

Клонирование голоса

В текущей работе мы создали дипфейк-видео. Однако при этом лишь оживили картинку, которая не сопровождается никакими звуками. Методы клонирования голоса используют машинное обучение для имитации голоса человека. Группа исследователей из Google создала продвинутый синтезатор речи под названием Tacotron 2. Вы можете прослушать аудиообразцы, созданные с его помощью, перейдя по ссылке: https://google.github.io/tacotron/publications/tacotron2/index.html. На этой веб-странице содержатся образцы как человеческого, так и сгенерированного машиной голоса. Попробуйте их различить.

Для того чтобы сымитировать чей-то голос, синтезатору Tacotron 2 требуется всего лишь пятисекундный образец звука. Хотя Google еще не выпустил свою реализацию Tacotron 2, другие разработчики уже создали систему, описанную в статье Google, в которой была представлена его

концепция. Вы можете найти ссылку на одну из этих реализаций на странице https://github.com/Rayhane-mamah/Tacotron-2.

Если настройка этой системы покажется вам слишком сложной задачей, то можете попробовать другие, более доступные реализации более ранних систем клонирования голоса, например https://github.com/CorentinJ/Real-Time-Voice-Cloning.

Попробуйте клонировать голос известного человека. Если вам не захочется писать код самостоятельно, то можете воспользоваться такими коммерческими инструментами, как Descript (https://www.descript.com/), которые позволяют клонировать собственный голос с помощью нескольких щелчков кнопкой мыши. ***Масштабный фишинг***

King Phisher — это инструмент для массовой рассылки фишинговых писем, который поставляется с Kali Linux. Данное упражнение позволит вам ознакомиться с этим инструментом и его возможностями. Запустите необходимые фоновые сервисы, выполнив следующие команды: kali@kali:~$ **sudo service postgresql start** kali@kali:~$ **sudo service king-phisher start**

Затем запустите приложение King Phisher, найдя соответствующий пункт в меню Kali Applications (Приложения) (рис. 7.7). Запуск данного приложения занимает пару секунд.

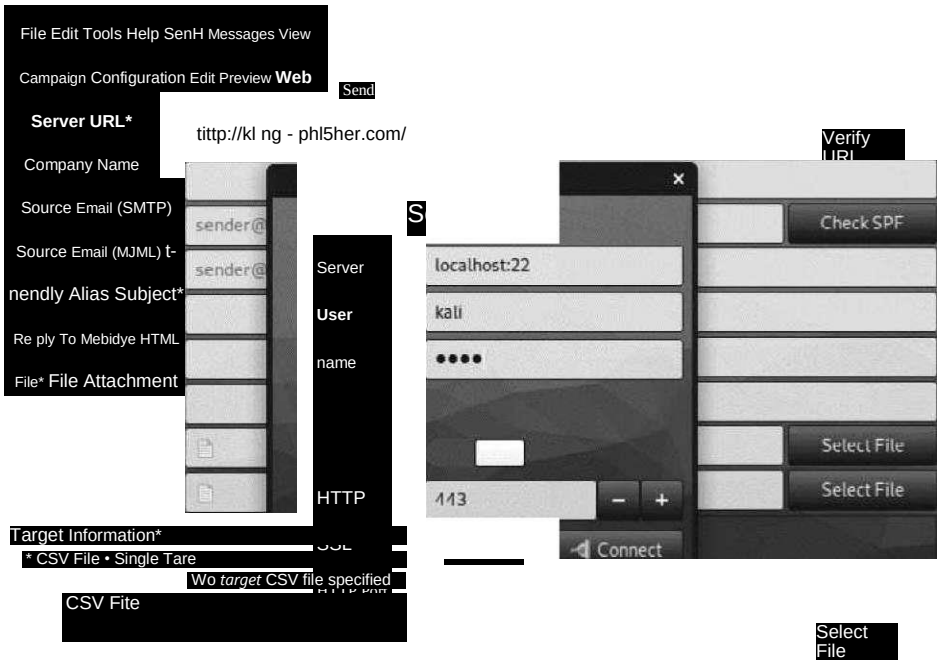


Рис. 7.7. Интерфейс King Phisher

Запустив King Phisher, вы можете войти в систему, используя имя пользователя и пароль своей машины Kali Linux, поскольку сервер размещен локально. Теперь вы можете приступить к реализации своей фишинговой кампании. При этом старайтесь действовать этично! ***Аудит SMTP***

Еще один отличный инструмент для тестирования безопасности SMTP-сервера — swaks, который предустановлен в Kali Linux. С его помощью вы можете отправить тестовое письмо, выполнив лишь одну команду:

kali@kali:~$ **swaks --to sys --server <*1P-адрес Metasploitable*>**

Вот фрагмент результата выполнения этой команды: ===
Trying 192.168.1.101:25... === Connected to 192.168.1.101.
<- 220 metasploitable.localdomain ESMTP Postfix (Ubuntu) -> EHLO
kali
<- 250-metasploitable.localdomain <- 250 2.1.5 Ok -> DATA
- - 354 End data with <CR><LF>.<CR><LF>

- > Date: Fri, 13 May 2022 15:46:17 -0500

- > To: sys

- > From: kali@kali

- > Subject: test Fri, 13 May 2022 15:46:17 -0500

- > Message-Id: <20201113154617.001295@kali>
- > X-Mailer: swaks v20190914.0 jetmore.org/john/code/swaks/ ->
  > This is a test mailing

- > .

<- 250 2.0.0 Ok: queued as BADADCBFC -> QUIT <- 221 2.0.0 Bye
=== Connection closed with remote host.

Чтобы ознакомиться со всеми возможностями инструмента swaks, выполните команду: kali@kali:~$ **swaks -help**

Познакомьтесь с другими инструментами OSINT, выполнив следующие упражнения, которые упорядочены по уровню сложности. В первом из них вы используете инструмент nmap для сбора информации о сервере путем выполнения различных вариантов сканирования. Во втором с помощью инструмента Discover запустите несколько инструментов OSINT и объедините результаты в один отчет. В третьем и последнем упражнении вы создадите собственный инструмент OSINT, который будет извлекать адрес электронной почты администратора из базы данных whois и искать соответствующий пароль в просочившихся в сеть списках. ***Сканирование с помощью nmap***

В следующем коде я перечислил несколько вариантов сканирования, которые можно произвести с помощью инструмента nmap. В первом варианте используется скрипт http- enum для перечисления файлов и папок на сайте. Это отличный способ обнаружить скрытые файлы или каталоги:

kali@kali:~$ **sudo nmap -sV -p 80 --script http-enum *<1P-адрес машины жертвы>***

Второй вариант сканирования nmap используется для того, чтобы идентифицировать операционную систему сервера и работающие серверы, оставшись при этом незамеченными:

kali@kali:~$ **sudo nmap -A -sV -D *<фактивный-IP-1, фиктивный-IP-2, Мой-IP, ^***
фиктивный-1P-3...> <1P-адрес машины жертвы>

Параметр -A активирует функцию определения операционной системы и версии, а также поддержку скриптов сканирования и инструмент traceroute. Флаг -D позволяет использовать фиктивные хосты для того, чтобы избежать обнаружения межсетевым экраном путем отправки фиктивных пакетов с поддельным IP-адресом источника наряду с реальным IP-адресом сканирующей машины. В третьем примере инструмент nmap используется в качестве сканера уязвимостей.

kali@kali:~$ **sudo nmap -sV --script vulners *<1P-адрес машины жертвы>***

Здесь мы предоставляем скрипт vulners, который сканирует машину и составляет список всех обнаруженных CVE-уязвимостей. Вы можете найти список всех скриптов nmap, установленных на виртуальной машине Kali Linux, перечислив содержимое каталога script с помощью команды:

kali@kali:~$ **ls /usr/share/nmap/scripts/**

Наконец, попробуйте просканировать все часто используемые порты (-p-), применяя скрипты по умолчанию (-sC), и выведите результаты в нормальном формате (-oN) в файл с именем scanResults.nmap:

kali@kali:~$ **nmap -sV -sC -p- -oN scanResults.nmap *<1P-адрес машины жертвы>***

Discover

Discover — это инструмент с открытым исходным кодом, который содержит различные скрипты для автоматизации разведки по открытым источникам и сканирования уязвимостей. После завершения сканирования Discover сгенерирует отчет, включающий
всю обнаруженную им информацию (рис. 8.16).

Программа Discover предусматривает два режима OSINT-сканирования: пассивный и активный, которые различаются степенью вероятности обнаружения. Записи запросов, произведенных в рамках пассивного сканирования, хранятся у третьих лиц, поэтому жертвы вряд ли узнают о том, что они подверглись сканированию. Активное сканирование предполагает исследование инфраструктуры жертвы и с большей вероятностью привлечет ее внимание.

Начните с изучения следующих инструментов пассивного сканирования Discover: **ARIN** и **Whois** определяют IP-адреса (Американский регистратор интернетномеров (American Registry for Internet Numbers, ARIN) — это организация,которая отвечает за регистрацию и распределение IP-адресов и поддерживает базу данных whois);

dnsrecon собирает OSINT-данные с DNS-серверов (также поддерживает активное сканирование);

goofile ищет в домене файлы определенных типов;

theHarvester ищет в общедоступных источниках, наподобие Google и LinkedIn, адреса электронной почты, связанные с исследуемым доменом; **сканер Metasploit** выполняет сканирование с помощью инструмента Metasploit Framework;

URLCrazy проверяет варианты URL, которые могут быть использованы для сквоттинга, например facebeok.com;

Recon-ng содержит множество инструментов, специально предназначенных для разведки по открытым интернет-источникам (также поддерживает активное сканирование).

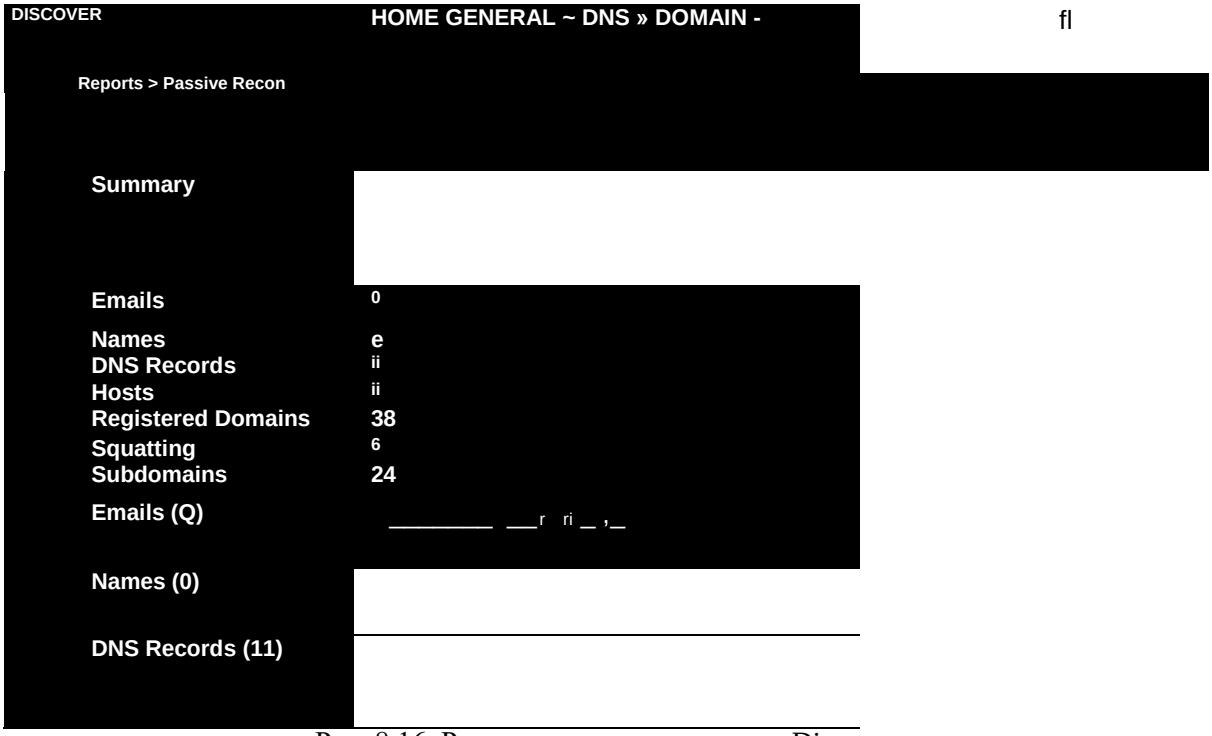


Рис. 8.16. Результаты сканирования в Discover

К инструментам активного сканирования относятся:

traceroute — отправляет ICMP-пакеты для обнаружения маршрутизаторов на пути к серверу;

Whatweb — зондирует сайт для выяснения того, какие технологии использовались при его создании.

Вам не обязательно запускать эти инструменты по отдельности. Инструмент Discover может сделать это за вас и сгенерировать исчерпывающий отчет.

Выполните следующую команду, чтобы клонировать репозиторий Discover и поместить его в каталог opt на виртуальной машине Kali Linux, содержащий все установленные программы Linux: kali@kali:~$ **sudo git clone https://github.com/leebaird/discover /opt/discover/**

Перейдите в каталог с репозиторием и запустите скрипт update.sh, чтобы установить программу Discover и все ее зависимости: kali@kali:~$ **cd /opt/discover/** kali@kali:~/opt/discover$ **sudo ./update.sh**

В процессе установки вам будет предложено ввести информацию для создания сертификата. Помните: вам не обязательно предоставлять личную информацию. Просто придумайте что-нибудь, как вы это делали при создании предыдущих сертификатов.

Пока идет процесс установки, создайте папку Results на рабочем столе Kali Linux, в которую вы будете сохранять свои отчеты. По завершении установки запустите инструмент Discover, выполнив команду: kali@kali:~/opt/discover$ **sudo ./discover.sh**

Чтобы попрактиковаться, выберите вариант Domain в меню Recon и выполните пассивное и активное сканирование собственного домена или домена, на сканирование которого вы получили разрешение. Процесс сканирования может занять более часа.

Его результаты должны быть сохранены в папке /root/data/. Переместите их в папку Results для облегчения дальнейшего доступа, выполнив команду: kali@kali:~$ **mv /root/data/ ~/Desktop/Results**

Какую информацию вам удалось обнаружить?

Создание OSINT-инструмента

Какую часть интернета вы можете одолеть своими силами? Создайте сканер, который выполняет поиск в базе whois по любому из четырех миллиардов IPv4- адресов. Вы вполне можете проверить все IP-адреса при условии, что не пытаетесь подключиться к ним, а просто ищете информацию об администраторе в общедоступной базе данных.

Другими словами, вы должны запустить команду:

kali@kali:~$ **whois 8.8.8.8**

и извлечь все найденные адреса электронной почты. Затем используйте API haveibeenpwned, доступный на https://haveibeenpwned.com/API/v2, чтобы выяснить, не соответствует ли адрес электронной почты администратора какому-либо из утекших паролей.

При тестировании возможностей инструмента вы можете ограничить сканирование парой адресов, а затем масштабировать его по мере необходимости.

Бонус

Проверьте скачанную ранее утекшую базу данных, содержащую 1,4 миллиарда адресов электронной почты и паролей, на предмет наличия пароля, соответствующего адресу электронной почты, найденному при сканировании базы whois. Выполните циклическую обработку коллекции IP-адресов и выведите результат в CSV-файл, в каждой строке которого содержатся IP-адрес, адрес электронной почты и пароль

Результаты Практической работы занести в отчет **Содержание отчета по Практической работе**

По результатам выполнения Практической работы студенты оформляют отчет по Практической работе и защищают его в индивидуальном порядке в форме беседы.

Практическая работа № 7 Тема. Исследование методов захвата контроля над сетью принципы и методы противодействия

Основные теоретические сведения

Проброс трафика с помощью устройства с двойной привязкой

Сети, открытые для пользования всем людям, обычно называются общедоступными. Пример такой сети — интернет. С другой стороны, сети, закрытые для широкой публики, такие как внутренняя сеть организации, называются частными. Тем не менее пользователям частной сети нередко требуется доступ к ресурсам, содержащимся в такой общедоступной сети, как интернет. Например, сотрудникам корпораций необходим доступ к поисковой системе Google. Для защиты внутренней сети компании часто используют межсетевые экраны, устанавливаемые между общедоступной сетью (интернет) и частной корпоративной сетью. Поскольку межсетевой экран подключен как к общедоступной, так и к частной сети, машина, на которой он запущен, называется *устройством с двойной привязкой* (dual homed device).

Устройства с двойной привязкой чрезвычайно важны для злоумышленников, находящихся в общедоступной сети, поскольку для получения доступа к частной сети организации они должны обойти межсетевой экран. Маршрутизация трафика через машину с двойной привязкой для получения доступа к сети называется *пробросом* (pivoting). Настроим тестовую сеть, чтобы продемонстрировать применение этой техники. Мы скомпрометируем виртуальную машину Metasploitable, которую сначала превратим в устройство с двойной привязкой, и используем ее в качестве прокси-сервера, чтобы получить доступ к частной сети для совершения атаки на виртуальную машину Ubuntu.

Настройка устройства с двойной привязкой

Машина pfSense в нашей виртуальной среде — пример устройства с двойной привязкой, поскольку выступает в качестве моста между нашей частной сетью и интернетом. Однако мы не будем компрометировать маршрутизатор pfSense, чтобы продемонстрировать технику проброса трафика, поскольку он защищает наши устройства от атак реальных хакеров. Вместо этого мы превратим в устройство с двойной привязкой виртуальную машину Metasploitable и подключим ее к другой частной сети, содержащей виртуальную машину Ubuntu. Схема сети, которую мы будем атаковать, представлена на рис. 14.1.

Первичный интерфейс сервера Metasploitable обозначен цифрой Этот интерфейс мы используем для подключения сервера к нашей смоделированной общедоступной сети, содержащей виртуальную машину Kali Linux. Второй интерфейс будет подключен к частной сети. Наша цель будет заключаться в том, чтобы взломать сервер Metasploitable и использовать его для маршрутизации трафика с первичного интерфейса в частную сеть через вторичный интерфейс. Однако для начала необходимо настроить виртуальную среду.

Мы начнем с включения второго интерфейса на виртуальной машине Metasploitable и его подключения к частной сети. Для этого перейдите к настройкам машины Metasploitable в VirtualBox (рис. 14.2).

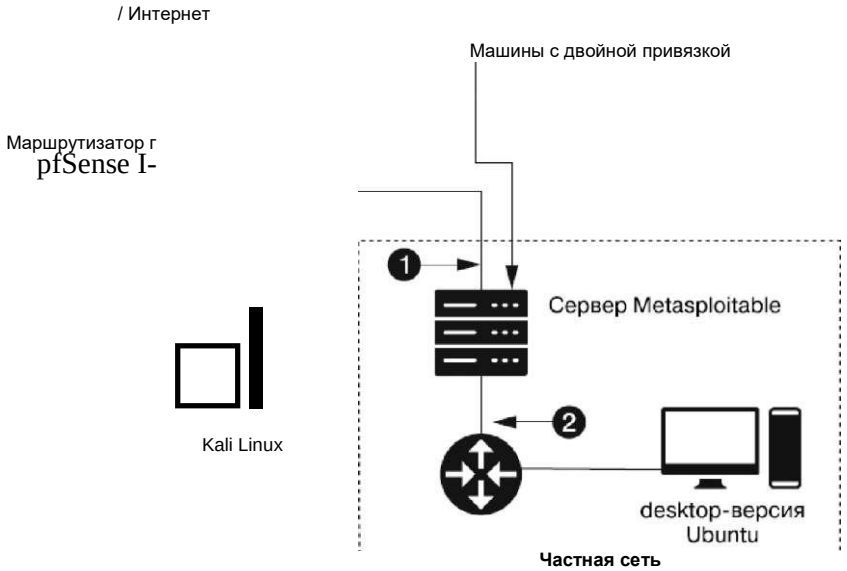


Рис. 14.1. Схема сети

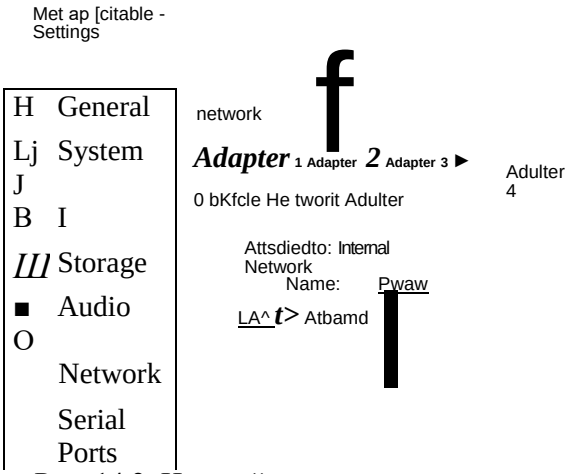


Рис. 14.2. Настройка второго сетевого интерфейса

Перейдите на вкладку Network (Сеть) В разделе Adapter 2 (Адаптер 2) установите флажок Enable Network Adapter (Включить сетевой адаптер) . В качестве имени частной сети задайте Private LAN .

Теперь мы должны назначить IP-адрес только что включенному интерфейсу. Мы сделаем это, отредактировав файл interface сервера Metasploitable. Выполните следующую команду, чтобы открыть этот файл в текстовом редакторе vim, который предустановлен в Metasploitable:

msadmin@metasploitable:~# **sudo vim /etc/network/interface**

Этот файл описывает сетевые интерфейсы, доступные в вашей системе, и способы

их активации. Для получения дополнительной информации см. interfaces(5).

интерфейс Loopback auto lo

iface lo inet loopback

Первичный сетевой интерфейс auto eth0

iface eth0 inet dhcp '
Вторичный сетевой интерфейс auto eth1
iface eth1 inet
static address
10.0.0.1 netmask
255.255.255.0

Открыв файл, вы должны увидеть определение первичного интерфейса Как правило, этот интерфейс подключен к общедоступной сети. Значение iface eth0 соответствует интерфейсу Ethernet (eth0). Параметр inet обозначает адресацию IPv4, а dhcp — что мы разрешаем DHCP-серверу назначить этому интерфейсу IP-адрес. *DHCP* (dynamic host configuration protocol, протокол динамической настройки узла) — протокол, который обычно используют маршрутизаторы для назначения IP-адресов машинам, подключающимся к сети. Например, ваш домашний маршрутизатор Wi-Fi имеет встроенный DHCP-сервер, а это означает, что ваш ноутбук использует протокол DHCP для получения IP-адреса при подключении к сети. Это гарантирует то, что ваш ноутбук не будет использовать тот же IP-адрес, что и компьютер, подключившийся к вашей сети до него. При использовании значения static IP-адреса назначаются вручную.

При настройке второго интерфейса мы установим для него статический IPv4- адрес 10.0.0.1 и маску подсети 255.255.255.0 . Сохраните файл, а затем запустите интерфейс eth1, выполнив следующую команду:

msadmin@metasploitable:~# **sudo ip link set dev ethl up**

Наконец, перезапустите сетевой интерфейс:

msadmin@metasploitable:~# **sudo /etc/init.d/networking**

restart ***Подключение машины к частной сети***

После настройки устройства с двойной привязкой мы можем переместить виртуальную машину Ubuntu в нашу новую частную сеть. Однако после перемещения у нее уже не будет доступа к интернету. Поэтому, прежде чем делать это, настроим ее.

Для входа в систему Ubuntu мы будем использовать OpenSSH — реализацию SSH-сервера с открытым исходным кодом, которая позволяет пользователям подключаться к машине с помощью протокола SSH. Авторизуйтесь в системе своей виртуальной машины Ubuntu и установите сервер OpenSSH:

victim@ubuntu:~$ **sudo apt-get install openssh-server** victim@ubuntu:~$ **sudo systemctl enable ssh**

Когда установка завершится, переместите виртуальную машину Ubuntu в частную сеть, изменив настройки интерфейса в VirtualBox для подключения к сети Private LAN.

Теперь вам нужно назначить IP-адрес интерфейсу на виртуальной машине Ubuntu. Это связано с тем, что в нашей частной сети нет DHCP-сервера. Назначьте статический IP-адрес своей виртуальной машине Ubuntu, перейдя в раздел Settings (Настройки) (рис. 14.3).

В разделе Network (Сеть) щелкните на значке Settings (Настройки) в виде шестеренки и перейдите на вкладку IPv4. Выберите способ настройки Manual (Вручную) и задайте IP-адрес 10.0.0.15, маску сети 255.255.255.0 и шлюз по умолчанию 10.0.0.1.

Убедитесь в том, что вы можете получить доступ к серверу Metasploitable с виртуальной машины Ubuntu, отправив ему ping-запросы. Если связь с сервером Metasploitable налажена, то вы должны получить следующее, не потеряв ни единого пакета: victim@ubuntu:~$ **ping 10.0.0.1**

AC

PING 10.0.0.1 (10.0.0.1): 56 data bytes

64 bytes from 10.0.0.1	icmp	seq =	0 ttl=	115	time =	=15.04 9	ms	
64 bytes from 10.0.0.1	icmp	seq =	1 ttl=	115	time =	=14.38 5	ms	
64 bytes from 10.0.0.1	icmp	seq =	2 ttl=	115	time =	15.036	ms	
64 bytes from 10.0.0.1	icmp	seq =	3 ttl=	115	time =	22.304	ms	
64 bytes from 10.0.0.1	icmp	seq =	4 ttl=	115	time =	=23.75 2	ms	
64 bytes from 10.0.0.1	icmp	seq =	5 ttl=	115	time =	14.254	ms	
64 bytes from 10.0.0.1	icmp	seq =	6 ttl=	115	time =	14.321	ms	

--- 10.0.0.1 ping statistics --

7 packets transmitted, 7 packets received, 0.0% packet loss round-trip min/avg/max/stddev = 14.254/17.014/23.752/3.835 ms

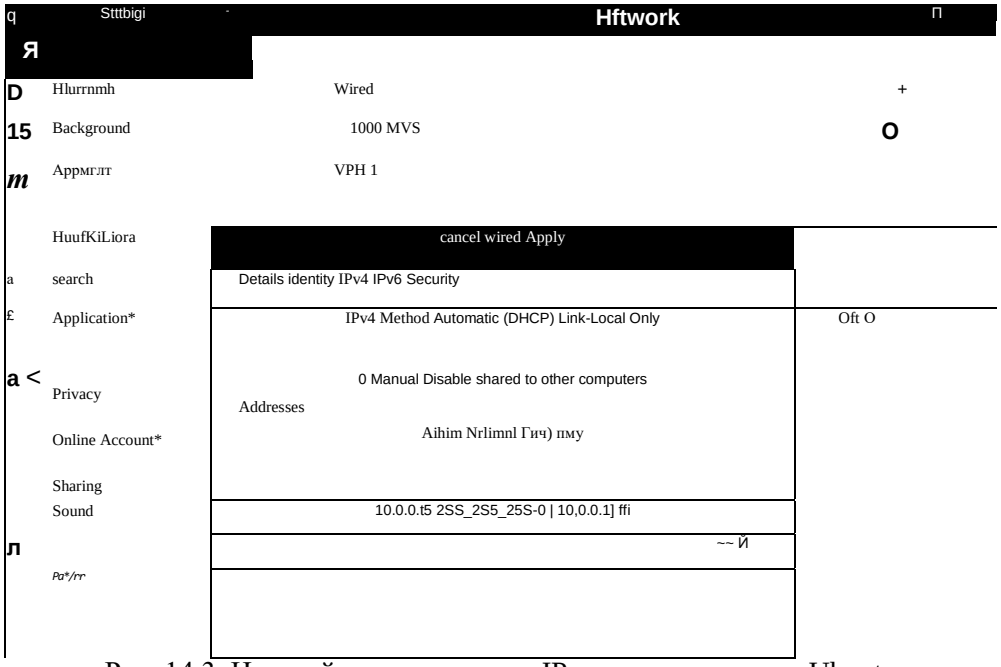


Рис. 14.3. Настройка статического IP-адреса на машине Ubuntu

Методические рекомендации по выполнению Практической работы

Следующие упражнения помогут вам лучше освоить техники повышения привилегий и проброса трафика. В первом упражнении вы расширите возможности своей машины Metasploitable так, чтобы она могла направить трафик из частной сети, то есть превратите ее в полноценный маршрутизатор. Во втором упражнении будут перечислены рекомендуемые материалы по повышению привилегий при работе с устройствами под управлением ОС Windows.

Настройка NAT на устройстве с двойной привязкой

Разрешите своему устройству с двойной привязкой маршрутизировать пакеты из частной сети, как это сделал бы настоящий маршрутизатор, путем включения NAT. Для этого сначала включите пересылку IP-пакетов:

msfadmin@metasploitable:~$ echo 1 > **/proc/sys/net/ipv4/ip_forward** Как и в случае атаки типа «ARP-спуфинг», нам нужно включить функцию ip_forward, чтобы позволить машине принимать и пересылать пакеты, не соответствующие ее IP-адресу. Затем используйте утилиту iptables, чтобы разрешить виртуальной машине Metasploitable маршрутизировать пакеты из нашей частной сети во внутреннюю сеть нашей виртуальной среды:

msfadmin@metasploitable:~$ **iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -**

o ^ eth1 -j MASQUERADE

Проверьте, можете ли вы получить доступ к внешнему миру, направив ping-запрос межсетевому экрану pfSense с виртуальной машины Ubuntu, находящейся в частной локальной сети:

victim@ubuntu:~$ **ping 192.168.1.1**

Материалы по теме повышения привилегий в ОС Windows

Прочтите статью Ханно Хайнрихса Exploiting GlobalProtect for Privilege Escalation, Part One: Windows, доступную по адресу https://www.crowdstrike.com/blog/exploiting-escalation-of-privileges-via-globalprotect-part-1/. Блог Crowdstrike — отличное место для поиска информации о новых уязвимостях.

Еще одна ошибка, позволяющая злоумышленникам совершать атаки на повышение привилегий, — уязвимость переполнения буфера в Sudo (CVE-2021-3156); вы можете прочитать о ней подробнее на странице https://github.com/stong/CVE-2021-3156.

Результаты Практической работы занести в отчет

Содержание отчета по Практической работе

По результатам выполнения Практической работы студенты оформляют отчет по Практической работе и защищают его в индивидуальном порядке в форме беседы.

Практическая работа № 8 Тема. Исследование методик тестирования сетей на проникновение Основные теоретические сведения

Сегодня мы все так или иначе обитаем в цифровом виде в сетевых облаках. Ваши налоговые декларации, фотографии ваших детей, которые вы делаете на мобильный телефон, местоположения, даты и время всех мест, куда вы направлялись с помощью GPS, - все они хранятся там и готовы для похищения любым злоумышленником, которому хватит опыта и упорства.

Обычное предприятие среднего размера имеет в 10 раз (как минимум) больше подключенных устройств, работающих в его сети, чем сотрудников, которые используют эти устройства для выполнения повседневных бизнес-операций. Возможно, сначала данный факт не вызовет у вас тревогу, учитывая, насколько глубоко интегрированы компьютерные системы в наше общество, наше существование и как от них зависит наше выживание.

Если предположить, что вы живете на планете Земля - а у нас есть достоверные сведения, что это так, - с вероятностью выше среднего вы имеете: © учетную запись электронной почты (или четыре); © аккаунт в социальной сети (или семь);

© как минимум два десятка комбинаций имени пользователя и пароля, которые вам приходится бережно хранить, чтобы иметь возможность входить на различные веб-сайты, мобильные приложения и облачные сервисы, необходимые для вашей ежедневной продуктивной работы.

Независимо от того, оплачиваете ли вы счета, покупаете продукты, бронируете номер в отеле или ищете что-нибудь в интернете, вам необходимо создать профиль учетной записи, содержащий как минимум имя пользователя, юридическое имя и адрес электронной почты. Часто вас просят предоставить дополнительную личную информацию, например такую:

© почтовый адрес; © номер телефона; © девичья фамилия матери; © номер банковского счета; © данные кредитной карты.

Мы все устали от этой рутины. Мы даже не утруждаем себя чтением всплывающих юридических соглашений, в которых говорится, что компании планируют делать с информацией, которую мы им предоставляем. Мы просто нажимаем «Я согласен» и поскорее переходим на страницу, которая нас заинтересовала, - чтобы посмотреть вирусное видео про кошек или заказать очаровательную кофейную кружку с саркастической шуткой о том, как вы устали.

Ни у кого нет времени читать всю эту юридическую чушь, особенно когда срок действия бесплатной доставки истекает всего через 10 минут. (Постойте, что это? Они предлагают программу вознаграждений! Мне нужно срочно создать новую учетную запись!) Возможно, даже более тревожным, чем частота, с которой мы раскрываем случайным интернет-компаниям нашу личную информацию, является тот факт, что большинство из нас наивно полагают, будто корпорации, с которыми мы взаимодействуем, принимают надлежащие меры предосторожности для безопасного и надежного хранения нашей конфиденциальной информации. Вы не представляете, насколько это далеко от реальности.

Утечки корпоративных данных

Если вы не жили в горной пещере последние двадцать лет, то, полагаю, вы много слышали об утечках корпоративных данных. Только в первой половине 2018 года было

выявлено 943 нарушения согласно отчету корпорации Gemalto, которая специализируется на средствах контроля доступа и защиты данных (http://mng.bz/YxRz). С точки зрения публикаций в СМИ, большинство нарушений, как правило, выглядят примерно так: «Транснациональная корпорация XYZ только что сообщила, что неизвестное количество конфиденциальных учетных записей клиентов было украдено неизвестной группой злоумышленников, которым удалось проникнуть в сеть компании, используя неизвестную уязвимость или способ атаки». Полный масштаб взлома, включая все, что похитили хакеры, - как вы уже догадались - неизвестен. Затем мы наблюдаем падение стоимости акций, поток гневных твитов, громкие заголовки в газетах и заявление об отставке генерального директора, а также нескольких членов наблюдательного совета. Генеральный директор уверяет нас, что отставка не имеет ничего общего с утечкой персональных данных; он уже давно собирался уйти на заслуженный отдых. Конечно, кто-то должен взять на себя официальную вину, но мы ведь понимаем, что главный директор по информационной безопасности (CISO), который много лет безупречно служил компании, не может уйти в отставку; вместо этого увольняют и публично забивают камнями в социальных сетях подвернувшихся под руку менеджеров, гарантируя, что, как принято говорить в Голливуде, они больше никогда не войдут в этот город.

Как работают хакеры

Почему взломы происходят так часто? Неужели компании настолько плохо умеют действовать по правилам, когда дело касается информационной безопасности и защиты наших данных? И да, и нет.

Неудобная правда заключается в том, что колода карт в этой игре оказывается подтасованной в пользу киберзлоумышленников. Помните мое предыдущее замечание о количестве сетевых устройств, которые предприятия постоянно подключают к своей инфраструктуре? Это значительно увеличивает возможность атаки, или *ландшафт угроз* компании.

Что делает защитник

Позвольте мне пояснить. Предположим, ваша работа - защищать организацию от киберугроз. Вам необходимо уделить внимание каждому ноутбуку, настольному компьютеру, смартфону, физическому серверу, виртуальному серверу, маршрутизатору, коммутатору и модной кофеварке, подключенной к вашей сети.

Затем вы должны убедиться, что каждое приложение, работающее на этих устройствах, правильно защищено с по мощью надежных паролей (предпочтительно с двухфакторной аутентификацией) и настроено в соответствии с текущими стандартами и передовыми методами для каждого соответствующего устройства. Кроме того, вы должны своевременно применять все исправления безопасности и обновления, выпущенные отдельными поставщиками программного обеспечения, как только они становятся доступными. Однако, прежде чем сделать хоть малейшее движение в этом направлении, вы должны трижды проверить, не мешают ли обновления повседневной деятельности вашего бизнеса, иначе люди будут злиться на вас за попытку защитить компанию от хакеров.

Все перечисленное нужно делать постоянно для каждого устройства, имеющего IP-адрес в вашей сети. Так просто, правда?

Что делает злоумышленник

А теперь перейдем на темную сторону. Предположим, ваша задача - проникнуть в компанию, т. е. каким-то образом взломать сеть и получить несанкционированный доступ к системам или информации с ограниченным доступом. Вам достаточно найти только одну систему, которая осталась без внимания защитника; только одно устройство, которое пропустило исправление или содержит пароль по умолчанию или легко- угадываемый пароль; единственное неправильно настроенное приложение, развернутое в спешке, чтобы

уложиться в невыполнимые сроки для бизнеса, обусловленные целевыми показателями прибыли, поэтому небезопасная настройка конфигурации (которая по умолчанию задана поставщиком) осталась без внимания. Это все, что нужно для проникновения, даже если цель проделала безупречную работу по контролю за каждым узлом в сети. В компаниях постоянно работают команды, которым нужно срочно внести какие-то изменения.

Если вы сейчас подумали, что это несправедливо или что это слишком сложно для защитников и слишком легко для атакующих, значит, вы поняли истинное положение дел. Итак, что должны делать организации, чтобы избежать взлома? Вот тут-то и пригодится *тестирование на проникновение,* или *пентестинг* (сокращение от penetration testing).

Моделирование состязательной атаки: тестирование на проникновение

Один из наиболее эффективных способов выявления слабых мест в системе безопасности до того, как они приведут к взлому, - это нанять профессионального «злоумышленника», или *пентестера,* чтобы смоделировать атаку на инфраструктуру компании. Пентестер должен предпринять все доступные действия, чтобы имитировать настоящего злоумышленника, в некоторых случаях действуя в обстановке полной секретности, незаметно для ИТ-отдела и службы внутренней безопасности организации, пока не придет время опубликовать свой окончательный отчет. В этой работе будем называть данный тип наступательных действий по обеспечению безопасности просто *тестом на проникновение.*

Конкретный объем и способы выполнения теста могут отличаться в зависимости от потребностей организации, заказывающей оценку (клиента), а также от возможностей и предложений услуг консалтинговой фирмы, проводящей тест. Воздействие пентестера может быть сосредоточено на веб-приложениях и мобильных приложениях, сетевой инфраструктуре, беспроводных устройствах, физических офисах и всем остальном, что вы можете придумать для атаки. Упор можно сделать на скрытность, пытаясь остаться незамеченным, или на сбор информации об уязвимостях как можно большего количества хостов за короткое время. Пентестеры могут использовать человеческий фактор (социальная инженерия), специально разработанный код эксплойта или даже копаться в мусорных баках клиента в поисках паролей для доступа. Все зависит от масштаба планируемого вторжения. Однако наиболее распространенный тип вторжения - тот, который я выполнял для сотен компаний за последнее десятилетие. Я называю его *тестом на проникновение во внутреннюю сеть* (internal network penetration test, INPT). Этот тип проникновения имитирует наиболее опасный тип злоумышленника для любой организации: злонамеренного или иным образом скомпрометированного инсайдера - человека, имеющего доступ к внутренней сети организации.

ОПРЕДЕЛЕНИЕ *Злоумышленник* - это обобщенное название лица, осуществляющего ту или иную атаку. Это определение относится к любому, кто пытается нанести вред информационной инфраструктуре организации.

Планируя INPT, вы предполагаете, что злоумышленник смог успешно получить физический доступ в корпоративный офис или, возможно, получил удаленный доступ к рабочей станции сотрудника с по мощью фишинга. Также возможно, что злоумышленник посетил офис в нерабочее время, представившись охранником, или в течение дня, представившись торговцем либо доставщиком цветов. Возможно, злоумышленник - действующий сотрудник компании, который прошел со своим пропуском через парадную дверь.

Существует бесчисленное множество способов получить физический доступ в офис, которые не вызовут особых затруднений. Во многих случаях злоумышленнику просто нужно пройти через главный вход и бродить по коридорам, вежливо улыбаясь любому, кто проходит мимо, и делая вид, что он разговаривает по мобильному телефону, пока он не

обнаружит укромный уголок, где можно подключиться к розетке локальной сети. Профессиональные компании, предлагающие услуги высококлассного тестирования на проникновение (пентест), обычно выставляют счета от 150 до 500 долларов в час. В результате для клиента, заказавшего тест на проникновение, зачастую дешевле пропустить эту творческую часть вторжения и с самого начала предоставить злоумышленнику физический доступ к внутренней подсети.

Так или иначе, злоумыш лен ни ку удалось получить доступ к корпоративной сети. Что он может сделать? Что он видит? Обычный сценарий вторжения предполагает, что злоумышленник ничего не знает о внутренней сети и не имеет специального доступа или учетных данных. Все, что у него есть, - это доступ к сети, и обычно этого ему достаточно.

Типичные этапы вторжения

Типичное тестовое вторжение состоит из четырех этапов, выполняемых по порядку, как показано на рис. 1.1. Отдельные названия каждого этапа - это не догма, их можно выбирать. Одна компания-пентестер может использовать термин «разведка» вместо сбора информации. Другая компания может использовать термин «доклад» вместо документации. Независимо от того, как называется каждый этап, большинство экспертов в нашей отрасли соглашаются с перечнем задач пентестера на каждом этапе.

Рис. 1.1 Четыре этапа теста на проникновение в сеть

© *Этап 1* - сбор информации:

a) составьте карту сети;

b) определите возможные цели;

c) перечислите слабые места в службах, работающих на этих

целях. © *Этап 2* - целенаправленное проникновение:

а) взломайте уязвимые сервисы (получите к ним несанкционированный доступ). © *Этап 3* - постэксплуатация и повышение привилегий:

a) определите информацию о скомпрометированных системах, которая может быть использована для дальнейшего доступа (закрепления в системе);

b) поднимите привилегии до самого высокого уровня доступа в сети, фактически став системным администратором компании;

© *Этап 4* - документирование:

а) соберите доказательства проникновения;

составьте окончательный отчет.

b) После того как тестовая часть вторжения завершена, пентестер мысленно покидает позиции злоумышленника и превращается в консультанта. Остальную часть вторжения он посвящает составлению максимально подробного отчета. Этот отчет содержит детальное описаниевсех способов, которыми удалось взломать сеть и обойти меры безопасности, а также предложение мер, которые компания может предпринять, чтобы закрыть эти выявленные бреши и гарантировать, что они больше не будут использованы кем-либо еще. В 9 из 10 случаев этот процесс занимает в среднем около 40 часов, но необходимое время может меняться в зависимости от размера организации.

1.4 Когда тест на проникновение наименее эффективен

Наверняка вы слышали известную поговорку: «Если у вас в руках молоток, все вокруг кажется гвоздями». Оказывается, это высказывание можно применить практически к любой профессии. Хирург хочет разрезать пациента, фармацевт хочет выписать ему таблетки, а пентестер хочет взломать вашу сеть. Но действительно ли всем организациям нужен тест на проникновение?

На самом деле ответ на этот вопрос зависит от уровня информационной безопасности компании. Я не могу сказать вам точно, сколько раз мне удавалось перехватить управление внутренней сетью компании в первый же день теста на проникновение, но количество таких компаний исчисляется сотнями. Конечно, мне хотелось бы сказать, что это получилось благодаря моим суперхакерским навыкам или потому, что я такой крутой, но это было бы грубым преувеличением.

Мои успехи гораздо больше связаны с чрезвычайно распространенной ситуацией: незрелая организация, которая не озаботилась даже базовыми требованиями безопасности, заказывает продвинутый тест на проникновение, хотя ей следовало бы начать с простой оценки уязвимости или моделирования угроз высокого уровня и анализа инфраструктуры. Нет смысла проводить тщательный тест на проникновение через защитные барьеры, если в безопасности вашей инфраструктуры зияют дыры, которые может обнаружить даже новичок.

Доступные мишени

Злоумышленники часто ищут путь наименьшего сопротивления и пытаются найти легкие пути в сеть, прежде чем выкатить на позицию большие пушки и взломать проприетарное программное обеспечение или разработать собственный код эксплойта нулевого дня. По правде говоря, средний пентестер обычно не умеет делать подобные вещи, потому что у него никогда не возникало потребности в этих навыках. Нет необходимости усложнять простые задачи, когда в большинстве корпораций можно найти гораздо более легкие пути. Мы называем эти простые способы *низко висящими фруктами* (low-hanging fruit, LHF), или *доступными мишенями.* В качестве примеров подобных мишеней можно назвать следующие уязвимости:

© пароли/конфигурации по умолчанию;

© одинаковые учетные данные в нескольких системах;

© наличие прав локального администратора у всех пользователей;

© отсутствующие патчи общедоступных эксплойтов.

Доступных мишеней гораздо больше, но эти четыре чрезвычайно распространены и чрезвычайно опасны. Однако следует отметить, что большинство векторов LHF-атак легко устранимы своими силами. Вы должны научиться соблюдать базовые принципы безопасности, прежде чем нанимать профессионального хакера для атаки на вашу сетевую инфраструктуру.

Организации со значительным количеством LHF-систем в своей сети не должны расходовать средства на оплату комплексного теста на проникновение. Было бы лучше

потратить это время и деньги на то, чтобы сосредоточиться на базовых концепциях безопасности, таких как надежные учетные данные во всех подсистемах, регулярное обновление программного обеспечения, укрепление и развертывание системы, а также

каталогизация активов.

Когда компании действительно нужен тест на проникновение?

Если компания задается вопросом, следует ли проводить тест на проникновение, я советую честно ответить на следующие вопросы. Начните с простых ответов «да/нет». Затем каждый ответ «да» компания должна подкрепить утверждением «Да, это обеспечено за счет процесса/проце- дуры/приложения XYZ, за которое отвечает сотрудник ABC». Итак, попробуйте ответить на следующие вопросы:

1 Ведем ли мы актуальные записи о каждом IP-адресе и DNS-имени в сети?

2 Есть ли у нас регламент установки исправлений для всех операционных систем и сторонних приложений, работающих в сети?

3 Используем ли мы коммерческие инструменты поиска уязвимостей для выполнения планового сканирования сети?

4 Удалили ли мы права локального администратора на всех ноутбуках сотрудников?

5 Требуем ли мы и обеспечиваем ли использование надежных паролей для всех учетных записей во всех системах?

6 Используем ли мы везде многофакторную аутентификацию?

Если ваша компания не может однозначно ответить «да» на все эти вопросы, то у квалифицированного пентестера, вероятно, не возникнет проблем со взломом раковины и извлечением жемчужины вашей организации. Я не говорю, что в таком случае вам совершенно незачем покупать тест на проникновение, просто вы должны ожидать болезненных результатов.

Ваш заказ может показаться пентестерам забавным; они могут даже хвастаться своим друзьям или коллегам тем, как легко они проникли вашу сеть. Но настоящая проблема в том, что такое тестирование будет бесполезным для вашей организации. Это подобно тому, как если бы человек никогда не занимался спортом или не придерживался здоровой диеты, а затем нанял тренера по фитнесу, чтобы тот посмотрел на его тело оценивающим взглядом и сказал: «Вы в плохой физической форме. С вас 10 000 долларов».

Проведение теста на проникновение в сеть

Итак, вы ответили на все вопросы и определили, что вашей организации действительно нужны услуги пентестера. Хорошо! Что дальше? До сих пор я обсуждал тестирование на проникновение как услугу, за которую вы обычно платите стороннему консультанту. Однако все больше и больше организаций создают собственные «красные коман ды» для регулярного проведения таких тестовых вторжений.

ОПРЕДЕЛЕНИЕ *Красная коман да* - специализированное подразделение отдела собственной безопасности организации, полностью сосредоточенное на учениях по обеспечению безопасности и имитации состязательных атак. Кроме того, термин «красная коман да» часто используется для описания конкретного типа вторжения, которое считается максимально реалистичным, имитирует продвинутых злоумышленников и использует целенаправленный подход, а не методы, основанные на широте охвата.

Я могу предположить, что вы получили или надеетесь получить должность, которая потребует от вас проведения теста на проникновение для компании, в которой вы работаете. Возможно, вы уже провели несколько тестов, но чувствуете, что вам не помешают дополнительные знания и опыт.

Методические рекомендации по выполнению Практической работы

1. Провести тестирование на проникновение в тестовой сети виртуальной организации.

Результаты Практической работы занести в отчет

Содержание отчета по Практической работе

По результатам выполнения Практической работы студенты оформляют отчет по Практической работе и защищают его в индивидуальном порядке в форме беседы.

Практическая работа № 9 Тема. Разработка отчёта о тестировании на проникновение и построение плана противодействия

Основные теоретические сведения

Документирование

Ваше проникновение приближается к финишу, но вы еще не закончили. После завершения технической части тестирования вы должны изложить свои выводы, наблюдения и рекомендации в кратком и полезном отчете для вашего клиента или заинтересованных сторон.

В этой части лекции основное внимание уделяется двум основным действиям, которые вы выполняете в конце теста на проникновение. Во-первых, это работы по очистке, которые не касаются стирания ваших следов. Помните, что в этой лекции основное внимание уделяется типичному тесту на проникновение во внутреннюю сеть, который обычно не является скрытым по своей природе. Скорее, очистка означает, что вы должны проявить профессионализм и удалить ненужные артефакты, такие как оставшиеся файлы, бэкдоры и изменения конфигурации на этапах атаки. Л

Удаление активных соединений оболочки

В ходе пентеста Capsulecorp вы открыли соединение оболочки Meter- preter с двумя скомпрометированными системами. Первое упомянуто в разделе 7.3, когда вы эксплуатировали непропатченную систему Windows. О втором говорится в разделе 10.2, когда вы обращались к системе второго уровня, имеющей авторизованного пользователя с правами администратора домена. Чтобы прервать все активные сеансы Meterpreter, вы должны использовать команду sessions -K - обратите внимание на заглавную букву K - из вашей консоли msfconsole. Затем, чтобы убедиться, что сеансы были прерваны, выполните коман ду sessions -l. Результирующий вывод представляет собой ответ msfconsole без активных соединений с оболочкой, как показано ниже:

Active sessions

No active sessions. Нет активных сессий.

msf5 >

Если по какой-либо причине sessions -K не может прервать ни одну из ваших сессий, жестко выйдите из msfconsole с по мощью коман ды exit -y. Если вы настроили на машине-жертве постоянную оболочку Meterpreter, которая обращается к вашей атакующей машине, не волнуйтесь; мы расскажем, как с этим справиться, в разделе 11.5.3. На данный момент вы можете просто отключить все активные слушатели, которые у вас есть, с по мощью коман ды jobs -k в msfconsole.

Деактивация локальных учетных записей пользователей

При проведении пентеста вы можете создать локальную учетную запись пользователя для дальнейшей компрометации цели. Эти учетные записи могут подвергнуть вашего клиента ненужному риску, если оставить их включенными. Все учетные записи пользователей, которые вы создаете во время проникновения, необходимо удалить до завершения тестирования.

В случае пентеста Capsulecorp вы технически не создавали никаких учетных записей пользователей, но вы перезаписали файл /etc/passwd сервера Linux другим файлом, содержащим учетную запись пользователя root, которую вы могли контролировать. Я полагаю, вы могли бы привести аргумент, что это скорее бэкдор, чем новая учетная запись пользователя, но я говорю об этом здесь в качестве напоминания о том, что если вы создали учетную запись пользователя, вы должны удалить ее. Необходимо очистить запись в /etc/passwd.

Удаление записей из /etc/passwd

Чтобы удалить записи из /etc/passwd, подключитесь по SSH к скомпрометированному серверу Linux как пользователь с привилегиями root. Если вы не знаете пароль root, используйте те учетные данные, которые вы использовали для получения доступа к системе изначально, а затем используйте запись пентеста, которую вы добавили в файл /etc/passwd, для повышения до root. Если бы вы прямо сейчас просмотрели содержимое файла /etc/passwd, он бы выглядел примерно так, как в листинге 11.1, с записью pentest внизу файла.

Листинг 11.1 Файл /etc/passwd с записью бэкдора

```
lxd:x:105:65534::/var/lib/lxd/:/bin/false uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
nail:x:1000:1000:Nail:/home/nail:/bin/bash
pentest:$1$pentest$NPv8jf8/11WqNhXAriGwa.:0:0:root:/root:/bin/bash
```

Запись pentest, которая является бэкдором учетной записи с правами root.

Как и в разделе 9.3.2, откройте файл /etc/passwd в текстовом редакторе, например vim. Прокрутите вниз до последней строки, содержащей учетную запись pentest/root, и удалите ее. Сохраните файл, и все готово. Дабы убедиться, что запись пользователя была правильно удалена, запустите коман ду su pentest из командной строки SSH, чтобы попытаться переключиться на учетную запись пользователя pentest. Вы увидите сообщение об ошибке: «No passwd entry for user 'pentest.'» (отсутствует запись пароля для пользователя pentest). Если вы не видите это сообщение, значит, вам не удалось удалить запись из файла /etc/passwd. Вернитесь и внимательно повторите действия, описанные в этом разделе. **Удаление оставшихся файлов из файловой системы**

На протяжении всего проникновения вы, несомненно, оставили следы тестирования в скомпрометированных системах. Эти следы представляют собой оставшиеся файлы, помещенные на диск. Очевидные риски заключаются в двоичных исполняемых файлах, которые могут быть использованы для прямого взлома одной из систем вашего клиента. Су-щест вуют также менее очевидные файлы, и будет считаться, как минимум, непрофессиональным оставлять их без дела.

Очистка после проникновения эффективна, только если вы тщательно вели записи **Не будет лишним подчеркнуть это еще раз, хотя, возможно, вам уже надоели мои постоянные напоминания. Очень важно вести подробные записи о ваших действиях во время любого пентеста. Безусловно, это поможет с правильной очисткой поля боя; но это также просто полезная привычка, потому что в какой-то момент вашей карьеры что-то пойдет не так. Рано или поздно вы что-нибудь сломаете. Это не конец света, но вашему клиенту нужно будет повторить ваши шаги, чтобы выяснить, как решить возникшую проблему.**

Столь же неизбежными и, вероятно, более частыми будут случаи, когда вы ничего не сломали, но что-то сломалось, пока вы выполняли проникновение, и на вас указали пальцем. В этом случае точные записи ваших действий помогут вам оправдаться и, что более важно, помогут вашему клиенту понять, что ему нужно искать в другом месте, чтобы разобраться в любой проблеме с сетью, с которой он столкнулся.

В этом разделе мы рассмотрим четыре экземпляра оставшихся файлов, которые использовались в ходе выполнения пентеста Capsulecorp. Во всех случаях шаги одинаковы: удаление файлов из файловой системы. Если вы отметили каждый созданный вами файл в

каждой системе, в которой вы создавали файлы, у вас не должно возникнуть проблем с тем,чтобы зайти и навести за собой порядок.

Не всегда виноват пентестер

Мой любимый пример неправомерного обвинения в неисправности во время проникновения произошел в кредитном союзе среднего размера (менее 1 миллиарда долларов годового дохода). Еще один консультант и я прибыли на место в понедельник утром, чтобы начать тестирование. Нас поместили в конференц-зал, что является довольно стандартной практикой, и мы расстегивали молнии в рюкзаках и вынимали наше снаряжение. Я даже не подключил кабель Ethernet к сети, когда в комнату ворвался мужчина и с порога закричал: «Что вы натворили? Сервер Exchange не работает, и никто не может получить электронную почту!» Мы оба посмотрели на мужчину, потом на наши ноутбуки, которые даже не были включены и не были подключены к сети, а затем снова на него. Прежде чем мы успели что-то сказать, он понял, что это не могли быть мы, извинился и закрыл дверь.

Мы не удержались от смеха - не потому, что у нашего клиента были проблемы с электронной почтой, а из-за того, как быстро они нашли крайних. Я был очень рад, что мы смогли без труда доказать, что это не наша вина; в конце концов, я даже не включил свой ноутбук.

Я бывал в других ситуациях, когда клиент был «уверен», что я что-то сломал, и убедить его в обратном было нелегко. В этом случае позже в тот же день этот сотрудник пришел и рассказал нам, что привело к отказу сервера Exchange; он был очень профессионален и извинился даже больше раз, чем необходимо, за предположение, что проблема была вызвана нами. ***Удаление копий куста реестра Windows***

В разделе 6.2.1 вы создали копию двух кустов реестра Windows. Копии кустов SYSTEM и SAM были помещены в каталог c:\windows\temp. Используя любые удобные для вас средства удаленного администрирования, выполните следующие две коман ды (измените коман ду соответствующим образом, если вы назвали свои копии как-нибудь иначе, кроме sys и sam): del c:\windows\temp\sam del c:\windows\temp\sys

Убедитесь, что файлы были удалены, просмотрев содержимое каталога с по мощью коман ды dir c:\windows\temp. Из вывода видно, что файлы sam и sys больше не присутствуют на машине-жертве (листинг 11.2).

Листинг 11.2 Список файлов каталога temp без копий куста реестра

```
          Volume in drive C has no
label.
          Volume          Serial
Number is 04A6-B95A
          CME 0 10.0.10.201:445
gjOHAN 957

  . . .fecso                    AsPNETSetup 00000.lo
0 07:07CME          DTR g
          0 e                           959
ш.ашеюы45 GOHAN ASPNETSetup 00001.lo
          0 0 g
          0 0 g
                                  FB8686B0
                               -2861- 4187-AF85
                                 58,398
                                MpCmd
                                 Run.log
```

59,704
MpSigS
tub.log
rad9230D.t
mp 102
silconfig.lo
g 69
05/13/2020 08:16 AM 286,450 SqlSetup.log 05/18/2020 08:27 AM 0 yBCnqc
7 File(s) 406,570 bytes 4 Dir(s) 2,399,526,912 bytes free ***Удаление пар ключей SSH***

В разделе 9.1.2 вы загрузили ключ SSH в скомпрометированную систему Linux, чтобы использовать его для автоматического подключения к атакующей машине. Сам по себе ключ SSH не представляет значительного риска для вашего клиента, поскольку его можно использовать только для подключения к вашему компьютеру. Но его все равно следует удалить из соображений вежливости и профессионализма.

Чтобы удалить пару ключей, подключитесь по SSH к скомпрометированной машине Linux и выполните коман ду rm /root/.ssh/pentestkey*. Эта коман да удалит файлы открытого и закрытого ключей. Вы можете убедиться, что ключи отсутствуют, выполнив коман ду ls -lah /root/.ssh. Как видно из выходных данных, на сервере Linux, который я скомпрометировал во время пентеста Capsulecorp, ключей больше нет (лис тинг 11.3).

Листинг 11.3 Список каталогов без пар ключей SSH

total 8.0K

drwx -----2 rootroot4.0KApr242019.

drwx -----3 rootroot4.0KApr242019..

-rw -------1 rootroot 0Apr242019authorized_keys ***Нет пар ключейSSH.***

Поскольку вы занялись очисткой скомпрометированной цели Linux, вам также следует позаботиться о сценарии bash, который был создан для использования ключей SSH. Сценарий bash, созданный вами в разделе 9.1.4, был помещен в каталог /tmp под именем callback.sh. Удалите его, набрав коман ду rm /tmp/callback.sh. Затем убедитесь, что он был удален, введя коман ду ls -lah /tmp.

Методические рекомендации по выполнению Практической работы

1. В соответствии с Практической работой №8 - произвести удаление всех следов тестирования на проникновение в исследуемую сеть.

Результаты Практической работы занести в отчет

Содержание отчета по Практической работе

По результатам выполнения Практической работы студенты оформляют отчет по Практической работе и защищают его в индивидуальном порядке в форме беседы.

Рекомендуемая литература

Основная литература:

1. Масалков А.С. Особенности киберпреступлений: инструменты нападения и защиты информации / А.С. Масалков. - М.: ДМК Пресс, 2018. - 226 с. - ISBN 978-5-97060-651-3. - Текст: электронный // Лань: электронно-библиотечная система. - URL: https://e.lanbook.com/book/105842 (дата обращения: 23.10.2022). - Режим доступа: для авториз. пользователей.

2. Шелупанов А.А. Форензика. Теория и практика расследования киберпреступлений: монография / А.А. Шелупанов, А.Р. Смолина. - М.: Горячая линия - Телеком, 2018. - 104 с. - ISBN 978-5-9912-0769-0.

3. Грэм Дэниел Г. Этичный хакинг. Практическое руководство по взлому.СПб.: Питер, 2022. - 384 с.: ил. - (Серия «Библиотека программиста»). ISBN 978-5-4461-1952-3

4. Дэвис Р. Искусство тестирования на проникновение в сеть / пер. с анг. В. С. Яценкова. - М.: ДМК Пресс, 2021. - 310 с.: ил. ISBN 978-5-97060-529-5

Дополнительная литература:

1. Уголовный кодекс РФ. URL: http://www.consultant.ru/document/cons_doc_LAW_10699/.

2. Уголовно-процессуальный кодекс РФ. URL: http://www.consultant.ru/document/cons_doc_LAW_34481/.

3. Федеральный закон от 31.05.2001 № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации». URL: http://www.consultant.ru/document/cons_doc_LAW_31871/.

4. Black Hat Python: программирование для хакеров и пентестеров. 2-е изд. - СПб.: Питер, 2022. - 256 с.: ил. - (Серия «Библиотека программиста»). ISBN 978-5-4461-3935-4

5. GHIDRA. Полное руководство / пер. с анг. А. А. Слинкина. - М.: ДМК Пресс, 2022. - 750 с.: ил.

Интернет - ресурсы:

1. Официальный сайт Федеральной службы по техническому и экспортному контролю https://fstec.ru/
2. Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) https://rkn.gov.ru/
3. Официальный сайт Федеральной службы безопасности Российской Федерации http://www.fsb.ru/
4. Консультант Плюс - законодательство РФ кодексы и законы в последней редакции http://www.consultant.ru/
5. Интернет портал Защита-информации^и http://www.iso27000.ru/
6. Научная электронная библиотека eLIBRARY.RU http://elibrary.ru

7. Консорциум сетевых электронных библиотек ЭБС «Лань» https://e.lanbook.com/
8. ЭБС «Университетская библиотека ОНЛАЙН» https://www.biblioclub.ru/ -
9. ЭБС IPR SMART https://www.iprbookshop.ru/
10. ЭБС Znanium https://znanium.com/
11. ЭБС «Юрайт» http://www.biblio-online.ru
12. Поисковые интернет-системы Яндекс, Rambler, Google и др.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания

для обучающихся по организации и проведению самостоятельной работы

по дисциплине «ТЕХНОЛОГИИ РАССЛЕДОВАНИЯ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ И ИНЦИДЕНТОВ»

Ставрополь
2026

1. Общие положения

Самостоятельная работа – планируемая учебная, учебно-исследовательская, научно-исследовательская работа студентов, выполняемая во внеаудиторное (аудиторное) время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия (при частичном непосредственном участии преподавателя, оставляющем ведущую роль за работой студентов).
Самостоятельная работа студентов (СРС) в ВУЗе является важным видом учебной и научной деятельности студента. Самостоятельная работа студентов играет значительную роль в рейтинговой технологии обучения.
К основным видам самостоятельной работы студентов относятся:
− формирование и усвоение содержания конспекта лекций на базе рекомендованной лектором учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);
− написание докладов;
− подготовка к семинарам, практическим и лабораторным работам, их оформление;
− составление аннотированного списка статей из соответствующих журналов по отраслям знаний (педагогических, психологических, методических и др.);
− выполнение учебно-исследовательских работ, проектная деятельность;
− подготовка практических разработок и рекомендаций по решению проблемной ситуации;
− выполнение домашних заданий в виде решения отдельных задач, проведения типовых расчетов, расчетно-компьютерных и индивидуальных работ по отдельным разделам содержания дисциплин и т.д.;
− компьютерный текущий самоконтроль и контроль успеваемости на базе электронных обучающих и аттестующих тестов;
− выполнение курсовых работ (проектов) в рамках дисциплин;
− выполнение выпускной квалификационной работы и др.
Методика организации самостоятельной работы студентов зависит от структуры, характера и особенностей изучаемой дисциплины, объема часов на ее изучение, вида заданий для самостоятельной работы студентов, индивидуальных качеств студентов и условий учебной деятельности.
Процесс организации самостоятельной работы студентов включает в себя следующие этапы:

- подготовительный (определение целей, составление программы, подготовка методического обеспечения, подготовка оборудования);
- основной (реализация программы, использование приемов поиска информации, усвоения, переработки, применения, передачи знаний, фиксирование результатов, самоорганизация процесса работы);
- заключительный (оценка значимости и анализ результатов, их систематизация, оценка эффективности программы и приемов работы, выводы о направлениях оптимизации труда).

Самостоятельная работа по дисциплине «Информационные технологии командной работы и проектной деятельности» направлена на формирование следующих **компетенций**:

Код	Формулировка

ПК-1	Способен обеспечивать защиту от несанкционированного дост сооружений и средств связи сетей электросвязи (за исключением се связи специального назначения) в процессе их эксплуатации

2. Цель и задачи самостоятельной работы

Ведущая цель организации и осуществления СРС совпадает с целью обучения студента – формирование набора общенаучных, профессиональных и универсальных компетенций будущего бакалавра.

При организации СРС важным и необходимым условием становятся формирование умения самостоятельной работы для приобретения знаний, навыков и возможности организации учебной и научной деятельности. Целью самостоятельной работы студентов является овладение фундаментальными знаниями, профессиональными умениями и навыками деятельности по профилю, опытом творческой, исследовательской деятельности. Самостоятельная работа студентов способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня.

Задачами СРС являются:

- систематизация и закрепление полученных теоретических знаний и практических умений студентов;
- углубление и расширение теоретических знаний;
- формирование умений использовать нормативную, правовую, справочную документацию и специальную литературу;
- развитие познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;
- формирование самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;
- развитие исследовательских умений;
- использование материала, собранного и полученного в ходе самостоятельной работы и лабораторных занятий.

3. Технологическая карта самостоятельной работы студента

Коды реализуемых компетенций	Вид деятельности студентов	Итоговый продукт самостоя-тельной работы	Средства и технологии оценки	Объем часов, в том числе (астр.)		
				СРС	Контактная работа с преподавателем	Всего
1 семестр						
ПК-1	Самостоятельное изучение литературы	Дискуссия	Собеседование	12,0	12,0	24,0
ПК-1	Подготовка к лекциям	Конспект лекций	Собеседование	12,0	12,0	24,0

ПК-1	Подготовка к практическим занятиям	Отчет в электронном виде	Собеседование	12,0	12,0	24,0
Итого за 1 семестр				36,0	36,0	72
Итого				36,0	36,0	72

4. Контрольные точки и виды отчетности по ним

Контроль качества и сроков самостоятельной работы выполняется в соответствии с учебным графиком и оформляется в соответствии с заданием. Предусмотрена следующая рейтинговая оценка знаний

Описание шкалы оценивания

В рамках рейтинговой системы успеваемость студентов по каждой дисциплине оценивается в ходе текущего контроля и промежуточной аттестации.

Текущий контроль

5. Порядок выполнения самостоятельной работы студентом

5.1. Методические рекомендации по работе с учебной литературой

При работе с книгой необходимо подобрать литературу, научиться правильно ее читать, вести записи. Для подбора литературы в библиотеке используются алфавитный и систематический каталоги.

Важно помнить, что рациональные навыки работы с книгой - это всегда большая экономия времени и сил.

Правильный подбор учебников рекомендуется преподавателем, читающим лекционный курс. Необходимая литература может быть также указана в методических разработках по данному курсу.

Изучая материал по учебнику, следует переходить к следующему вопросу только после правильного уяснения предыдущего, описывая на бумаге все выкладки и вычисления (в том числе те, которые в учебнике опущены или на лекции даны для самостоятельного вывода).

При изучении любой дисциплины большую и важную роль играет самостоятельная индивидуальная работа.

Особое внимание следует обратить на определение основных понятий курса. Студент должен подробно разбирать примеры, которые поясняют такие определения, и уметь строить аналогичные примеры самостоятельно. Нужно добиваться точного представления о том, что изучаешь. Полезно составлять опорные конспекты. При изучении материала по учебнику полезно в тетради (на специально отведенных полях) дополнять конспект лекций. Там же следует отмечать вопросы, выделенные студентом для консультации с преподавателем.

Выводы, полученные в результате изучения, рекомендуется в конспекте выделять, чтобы они при перечитывании записей лучше запоминались.

Опыт показывает, что многим студентам помогает составление листа опорных сигналов, содержащего важнейшие и наиболее часто употребляемые формулы и понятия. Такой лист помогает запомнить формулы, основные положения лекции, а также может служить постоянным справочником для студента.

Чтение научного текста является частью познавательной деятельности. Ее цель – извлечение из текста необходимой информации. От того на сколько осознанна читающим собственная внутренняя установка при обращении к печатному слову (найти нужные сведения, усвоить информацию полностью или частично, критически проанализировать материал и т.п.) во многом зависит эффективность осуществляемого действия.

Выделяют ***четыре основные установки в чтении научного текста***:

информационно-поисковый (задача – найти, выделить искомую информацию)

усваивающая (усилия читателя направлены на то, чтобы как можно полнее осознать и запомнить как сами сведения, излагаемые автором, так и всю логику его рассуждений)

аналитико-критическая (читатель стремится критически осмыслить материал, проанализировав его, определив свое отношение к нему)

творческая (создает у читателя готовность в том или ином виде – как отправной пункт для своих рассуждений, как образ для действия по аналогии и т.п. – использовать суждения автора, ход его мыслей, результат наблюдения, разработанную методику, дополнить их, подвергнуть новой проверке).

Основные виды систематизированной записи прочитанного:

Аннотирование – предельно краткое связное описание просмотренной или прочитанной книги (статьи), ее содержания, источников, характера и назначения;

Планирование – краткая логическая организация текста, раскрывающая содержание и структуру изучаемого материала;

Тезирование – лаконичное воспроизведение основных утверждений автора без привлечения фактического материала;

Цитирование – дословное выписывание из текста выдержек, извлечений, наиболее существенно отражающих ту или иную мысль автора;

Конспектирование – краткое и последовательное изложение содержания прочитанного.

Конспект – сложный способ изложения содержания книги или статьи в логической последовательности. Конспект аккумулирует в себе предыдущие виды записи, позволяет всесторонне охватить содержание книги, статьи. Поэтому умение составлять план, тезисы, делать выписки и другие записи определяет и технологию составления конспекта.

5.2. Методические рекомендации по составлению конспекта лекций:

1.

нимательно прочитайте текст. Уточните в справочной литературе непонятные слова. При записи не забудьте вынести справочные данные на поля конспекта.

2.

ыделите главное, составьте план.

3.

ратко сформулируйте основные положения текста, отметьте аргументацию автора.

4.

аконспектируйте материал, четко следуя пунктам плана. При конспектировании старайтесь выразить мысль своими словами. Записи следует вести четко, ясно.

5.

рамотно записывайте цитаты. Цитируя, учитывайте лаконичность, значимость

мысли.

В тексте конспекта желательно приводить не только тезисные положения, но и их доказательства. При оформлении конспекта необходимо стремиться к емкости каждого предложения. Мысли автора книги следует излагать кратко, заботясь о стиле и выразительности написанного. Число дополнительных элементов конспекта должно быть логически обоснованным, записи должны распределяться в определенной последовательности, отвечающей логической структуре произведения. Для уточнения и дополнения необходимо оставлять поля.

Овладение навыками конспектирования требует от студента целеустремленности, повседневной самостоятельной работы.

5.3. Методические рекомендации по подготовке к практическим занятиям

Успех практического занятия зависит от качества подготовки к нему как со стороны преподавателя, так со стороны магистрантов. Хорошую подготовку магистранта к практике продемонстрирует начало выступления с *плана доклада*, который подготовлен им самостоятельно или под руководством преподавателя. Практика свидетельствует о том, что нередки случаи, когда магистрант, содержательно выступая по вопросу в целом, не может сформулировать мысли, которые он только что высказал пространно. Иначе говоря, он недостаточно ясно представляет себе структуру собственного выступления, что говорит о его поверхностной подготовке, о механическом переписывании материала в свой конспект.

Тщательное предварительное продумывание магистрантом плана доклада, реферата, выступления по основному вопросу облегчит ему понимание внутренней логики проблемы, поможет лучше ориентироваться при изучении рекомендованной литературы. Этот подход позволит усвоить ведущие положения, сформировать четкие суждения, продемонстрировать умение соразмерно компоновать материал в соответствии с его важностью в данном контексте, содействовать выработке навыков подготовки к докладам, лекциям.

В определенной ситуации магистранту рекомендуется остановиться лишь на одном или двух пунктах его плана, что способствует развитию гибкости мышления, умению ориентироваться в изложении подготовленного материала. Руководителю же занятия это позволяет предотвратить повторения, выделить главное, сэкономить время. Следует иметь в виду, что отдельные магистранты, готовясь к практике, сначала пишут текст выступлений, а затем, помня требования преподавателя, приступают к составлению его плана. От такой практики магистрантам надо отказаться с первых же занятий.