МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

УНИВЕРСИТЕТ ИТМО

А.Н. Бегаев, С.Н. Бегаев, В.А. Федотов

ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ

РЕКОМЕНДОВАНО К ИСПОЛЬЗОВАНИЮ В УНИВЕРСИТЕТЕ ИТМО
по направлению подготовки (специальности) 10.03.01 «Информационная безопасность»
в качестве учебного пособия для реализации основных профессиональных
образовательных программ высшего образования бакалавриата

УНИВЕРСИТЕТ ИТМО

Санкт-Петербург

2018

Бегаев А.Н., Бегаев С.Н., Федотов В.А. Тестирование на проникновение. – СПб: Университет ИТМО, 2018. – 45 с.

Рецензент: Кременчуцкий Александр Лазаревич, профессор, к.т.н.

Учебно-методическое пособие содержит теоретический материал, посвященный основам тестирования на проникновение. В пособии системно излагаются и описываются основные этапы проведения тестирования на проникновение исследователями безопасности, а в частности, процесс сбора информации, процесс получения информации от сетевых сервисов (сканирования сети), процедура поиска и эксплуатации уязвимостей, а также эксплуатации уязвимостей веб-приложений. Учебно-методическое пособие содержит задания обучающего характера, выполненные в форме лабораторных работ, которые служат для закрепления и усвоения полученных навыков.

Учебно-методическое пособие предназначено для студентов, обучающихся по направлению подготовки 10.03.01 «Информационная безопасность» по дисциплине «Технология сертификации средств защиты информации».

Рекомендовано к печати Советом мегафакультета КТиУ (протокол №2 от 14 февраля 2018 года).

УНИВЕРСИТЕТ ИТМО

Университет ИТМО – ведущий вуз России в области информационных и фотонных технологий, один из немногих российских вузов, получивших в 2009 году статус национального исследовательского университета. С 2013 года Университет ИТМО является участником программы повышения конкурентоспособности российских университетов среди ведущих мировых научно-образовательных центров, известной как проект «5 в 100». Цель Университета ИТМО заключается в становлении исследовательского университета мирового уровня, предпринимательского по типу, ориентированного на интернационализацию всех направлений деятельности.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Данное учебно-методическое пособие содержит материалы, которые позволят студентам освоить теоретические основы тестирования на проникновение и попрактиковаться в выполнении лабораторных работ, посвященных Интернет-разведке и эксплуатации уязвимостей в ходе изучения дисциплины «Технология сертификации средств защиты информации».

Понимание основ эксплуатации уязвимостей позволяет студентам осознать важность и необходимость сертификации, позволяющей снизить риск наличия недекларированных возможностей.

Структурно пособие состоит из шести теоретических разделов, в которых описаны различные этапы тестирования на проникновение, и двух лабораторных работ.

Дополнительно приведен список рекомендуемых источников, который включает литературу и другие источники, рекомендуемые авторами для более глубокого освоения и понимания данной тематики.

1 ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ

Лучший способ остановить преступника - думать, как преступник. Установки охранных сигнализаций и ограждений недостаточно для обеспечения безопасности от взлома. Чтобы эффективно остановить грабителя, вы должны предсказать его каждое движение. Точно так же для предотвращения компрометации инфраструктуры организации – лучший способ - это думать, как злоумышленник.

Один из популярных способов оценки компаниями своей защищённости от атак - это привлечение внешних фирм и исследователей безопасности, которые специализируются на тестировании безопасности компьютерных систем.

Исследователь безопасности является «этичным хакером», который нанимается организацией для того, чтобы попытаться скомпрометировать сеть компании с целью оценки ее безопасности. Перед любым тестированием между заказчиком и исследователем безопасности заключается договор, в котором прописываются ограничения. Ограничения обычно определяют то, что может и не может быть сделано в ходе тестирования на проникновение. Например, исследователю безопасности, как правило, не разрешается выполнять атаки на отказ в обслуживании на целевую сеть или внедрять вирусы. Тем не менее, объем тестирования, выполняемого исследователем безопасности, варьируется в зависимости от потребностей организации.

Существует несколько методов тестирования на проникновение:

1. Метод «черного ящика». В ходе такого тестирования исследователю неизвестно ничего о сети компании. Например, если это внешнее тестирование методом «черного ящика», исследователю может быть предоставлен только адрес веб-сайта и его задачей является осуществить взлом так, как если бы он был реальным злоумышленником.

2. Метод «белого ящика». В ходе тестирования по методу «белого ящика» исследователь имеет полное представление о внутренней организации сети. Перед проведением тестов исследователю могут быть предоставлены схемы сети или список используемых операционных систем и приложений. Хотя в реальной жизни такая ситуация маловероятна, метод является наиболее эффективным и точным, так как он представляет собой наихудший сценарий, при котором злоумышленник имеет полное представление о сети.

3. Метод «серого ящика». В ходе тестирования по методу «серого ящика» исследователь имитирует действия сотрудника организации, то есть он получает учетную запись для доступа к внутренней сети и стандартные права на доступ. Этот метод позволяет оценить внутренние угрозы, исходящие со стороны сотрудников компании.

Исследователи безопасности ищут уязвимости и угрозы безопасности.

Уязвимость — это слабость, недостаток, используя который можно намеренно нарушить её целостность и вызвать неправильную работу.

Угроза представляет собой потенциальное нарушение безопасности, которое может нанести ущерб, такой как раскрытие конфиденциальных данных, изменение данных, уничтожение данных или отказ в обслуживании.

Для защиты активов от угроз в любой инфраструктуре необходимо обеспечивать их безопасность. Угрозы могут быть связаны с конфиденциальностью, целостностью или доступностью.

1. Угроза нарушения конфиденциальности заключается в том, что существует риск раскрытия информации тем, кто не располагает полномочиями доступа к ней. Она имеет место, когда получен доступ к некоторой информации ограниченного доступа, хранящейся в вычислительной системе или передаваемой от одной системы к другой.
2. Угроза целостности (неправомерного изменения данных). - это риск изменения данных неавторизованными пользователями.
3. Угроза доступности представляет собой создание таких условий, при которых доступ к услуге или информации будет либо заблокирован, либо возможен за время, которое не обеспечит выполнение тех или иных бизнес-целей.

Предполагается, что исследуемая инфраструктура защищена, когда возможность утечки, кражи или изменения обрабатываемой информации сохраняется на приемлемом уровне. Приемлемый уровень определяется путем проведения анализа затрат-рисков, при котором стоимость защиты данных сопоставляется с риском потери или компрометации данных. Цель тестирования на проникновение заключается не в снижении риска до нуля, а в снижении риска до приемлемого уровня, установленного руководством. В конечном счете, остается некоторый остаточный риск, который может быть принят.

Основная цель тестирования на проникновение – это отчет по результатам тестирования, который призван привлечь внимание руководства к существующей в организации политике безопасности. Политика безопасности — это документ, в котором излагаются лучшие методы обеспечения безопасности внутри организации, установленные лицами, ответственными за защиту активов организации. Уязвимости системы безопасности существуют не из-за внедренной технологии или конфигурации, а потому, что политика безопасности не устраняет проблему или потому что, пользователи не следуют этой политике.

При тестировании на проникновение важно различать понятия существующей уязвимости и уязвимости нулевого дня. Уязвимость нулевого дня — это недокументированная новая уязвимость, против

которой ещё не разработаны защитные механизмы. Уязвимости нулевого дня представляют собой серьёзную опасность, так как предотвратить их воспроизведение зачастую является трудной задачей. Лучшей практикой защиты от атак с использованием уязвимостей нулевого дня является внедрение эвристического анализа или обнаружения на основе сигнатур.

Типовые факторы возникновения угроз безопасности и необходимости в поведении тестирования на проникновение:

1. Беспроводные локальные сети. Беспроводные сети пользуются популярностью во многих организациях благодаря простоте использования и гибкости. Однако беспроводные сети восприимчивы к подслушиванию.

2. Сложная топология сети. Раньше было достаточно одной операционной системы для управления сетью. Сегодня администраторы помимо основных задач по администрированию большого числа средств защиты и сетевого оборудования поддерживают работу нескольких операционных систем. А тем временем технологии усложняются с каждым годом. Статического веб-сайта, размещенного на веб-сервере, недостаточно. Теперь компаниям требуется несколько межсетевых экранов, шифровальных средств, кластеры с балансировкой нагрузки, серверные базы данных и динамические интерфейсные веб-сайты. Такое повышение сложности технологий и топологий сетей затрудняет администраторам обеспечивать должную защиту от угроз безопасности и своевременную установку соответствующих патчей.

3. Частота обновлений программного обеспечения. Наряду с повышением сложности происходит увеличение количества исправлений (патчей) программного обеспечения, которые необходимо устанавливать. Администраторам трудно оставаться в курсе всех необходимых исправлений, чтобы установить их своевременно и обезопасить свои системы. В результате системы остаются необновлёнными и, следовательно, уязвимыми для атаки.

4. Маркетинговые требования. Финансовые учреждения, интернет-магазины и центры обработки данных - это небольшой перечень типов компаний, которые продают свою безопасную сеть потенциальным клиентам. Тестирование на проникновение необходимо для проверки безопасности инфраструктур таких компаний. Иногда результаты тестов также предоставляются потенциальным клиентам.

5. Доступность инструментов взлома. Существует множество программных средств для осуществления атак на сети, большинство из которых бесплатны и находятся в открытом доступе. Что еще хуже, для работы многие из этих инструментов не требуют детального понимания принципов работы сетей и компьютера, что облегчает проведение атак для всех, кто имеет базовые навыки владения компьютером.

6. Открытое программное обеспечение. Несмотря на то, что доступность исходных кодов является преимуществом для многих, оно

также упрощает процесс обнаружения уязвимостей. Поскольку хакеры также могут читать исходный код, они могут быстро обнаруживать уязвимости, например, уязвимости, связанные с переполнением буфера, позволяющие нарушить работу программы или приводящие к выполнению произвольного кода.

7. Неконтролируемые удаленные пользователи. Все больше и больше компаний позволяют сотрудникам работать удаленно. К сожалению, администраторы безопасности не могут контролировать эти удаленные системы. Злоумышленники, которые знают об этих удаленных соединениях, могут использовать их в своих интересах. Компании могут нанимать исследователей безопасности для того, чтобы выполнять тестирование по методу «серого ящика», при котором производится имитация действий удаленных пользователей и производится попытка получения доступа и повышения своих привилегий во внутренних системах.

Этапы тестирования на проникновение:

Первый этап – *разведка.* На этапе разведки исследователь производит попытки собрать как можно больше информации о выбранной цели. Разведка может быть активной и пассивной. При активной разведке исследователь безопасности использует такие инструменты, как nslookup, dig или SamSpade, чтобы исследовать целевую сеть, например, с целью определения диапазона IP-адресов. При пассивной разведывательной атаке исследователь безопасности использует общедоступную информацию для того, чтобы узнать о технологиях, используемых в организациях.

Второй этап - *сканирование*. Здесь исследователь безопасности изучает топологию сети путем сканирования открытых портов с помощью таких инструментов, как NMap. Цель - определить службы, запущенные на целевых хостах. Также на этом этапе исследователь безопасности выполняет определение типа операционной системы. Этап сканирования также включает проверку на наличие уязвимостей. Тестирование на наличие уязвимостей предшествует обнаружению методов для получения доступа к целевому узлу.

Получение доступа - после проверки целевой сети на наличие уязвимостей, исследователь безопасности пытается эксплуатировать эти уязвимости и, в случае успеха, предпринимает шаги для поддержания доступа к целевому хосту.

Поддержание доступа осуществляется путем установки бэкдоров, которые позволяют исследователю безопасности повторно подключаться к системе.

Последний этап тестирования - *удаление доказательств (следов проникновения)*. Исследователи проверяют, могут ли быть стёрты файлы журналов, хранящие следы их активности в сети.

2 СБОР ИНФОРМАЦИИ

Первый этап взлома любой информационной системы начинается со сбора максимального количества информации о цели. Практически никогда не удается собрать всю информацию из одного-единственного источника. Данные приходится собирать из множества различных мест, с тем чтобы впоследствии получить полную картину информационной системы организации.

На данном этапе выявляются слабые места сети, через которые в будущем и будет осуществляться проникновение в систему. При правильном подходе можно не только выявить потенциально уязвимые места, но и наметить возможные векторы атаки на обозначенную цель.

Для проведения успешной атаки найдет применение любая доступная информация о предприятии.

Обычно, имея только название организации, начинают сбор следующих данных:

- домены;
- сетевые адреса или сетевые блоки;
- местонахождение;
- контактная информация;
- новости о слиянии или приобретении;
- вакансии;
- ссылки на связанные с организацией веб-сервисы;
- различные документы;
- структура организации.

Это только примерный список, и продолжать его можно достаточно долго. Например, просмотрев вакансии предприятия, можно узнать, какие информационные системы используются внутри организации. А проанализировав HTML-код домашней странички, можно найти ссылки на внутренние ресурсы. От того, как будет проведен сбор информации, зависит направление, а также тип и успешность атаки. Большая часть процесса сбора информации не требует специальных знаний, достаточно умения пользоваться поисковыми системами. Зачастую они индексируют даже ту информацию, которую пытались скрыть от внешнего мира.

2.1 Использование Google для сбора информации

Хакер или аудитор может использовать для сбора информации не только Google, но также Yahoo или любой другой поисковый сервис. Для ускорения и облегчения процесса поиска и сбора информации можно использовать операторы поиска. Без них отыскать нужную информацию будет не просто сложно, но практически невозможно.

Например, по запросу royalmail Google выдает около 61 800 000 результатов. По запросу site:royalmail.com — 261 000, а после уточнения site:royalmail.com filetype:doc — всего 5.

Таким образом, мы из полумиллиарда результатов поиска отфильтровали только то, что нам было интересно.

Операторы:

- оператор *site* ограничит вывод результатов запроса информацией с одного сайта (пример использования - site:nic.ru);
- оператор *filetype* используется для поиска файлов определенного типа (пример использования - filetype:doc);
- оператор *inurl* ищет заданный текст только в url сайта;
- оператор *intitle* ищет информацию, исходя из заголовка документа.

2.2 Поиск информации о людях

Если вы нашли список сотрудников компании, то будет полезным собрать о них как можно больше информации. Довольно часто бывает, что взлом ресурса, который, казалось бы, не имеет никакого отношения к организации, которую мы пытаемся взломать, приводит к ее компрометации. Такое возможно, если сотрудники используют одни и те же пароли для доступа к различным системам.

Лучшим местом поиска информации, равно как и для западных коллег, остаются социальные сети. Благодаря тому, что ими пользуется огромное количество людей, они становятся бездонным источником информации. По ним можно отследить все — карьеру, образ жизни, интересы и многое другое. Пользуясь данными о геометках фотографий можно посмотреть, что происходит за закрытыми дверями организации.

2.3 Поиск по архивным данным

Чтобы найти информацию, которую организация прежде публиковала в Интернете, а затем удалила (по причине допуска ошибки или потери актуальности данной информации) можно воспользоваться сервисом archive.org. Это так называемый архив Интернета, который собирает копии веб-страниц, графические материалы, видео- и аудиозаписи и программное обеспечение. Архив обеспечивает долгосрочное архивирование собранного материала и бесплатный доступ к своим базам данных для широкой публики.

2.4 Демонстрация сбора информации

Проведем сбор информации из открытых источников о компании АО «НПО «Эшелон». С помощью Google найдем сайт организации (рисунок 1).

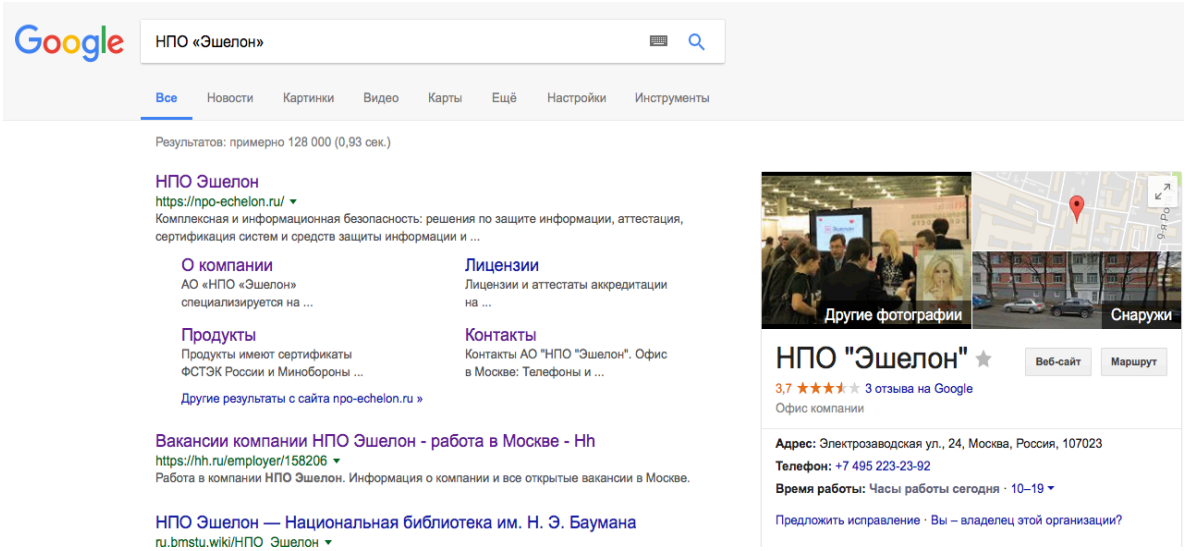


Рисунок 1 - Поиск информации о компании НПО «Эшелон»

Для определения почтовых учетных записей сотрудников организации, нужно проанализировать информацию на сайте. Проанализировав раздел «Контакты» определяем общий почтовый домен организации «@npo-echelon.ru» (рисунок 2).

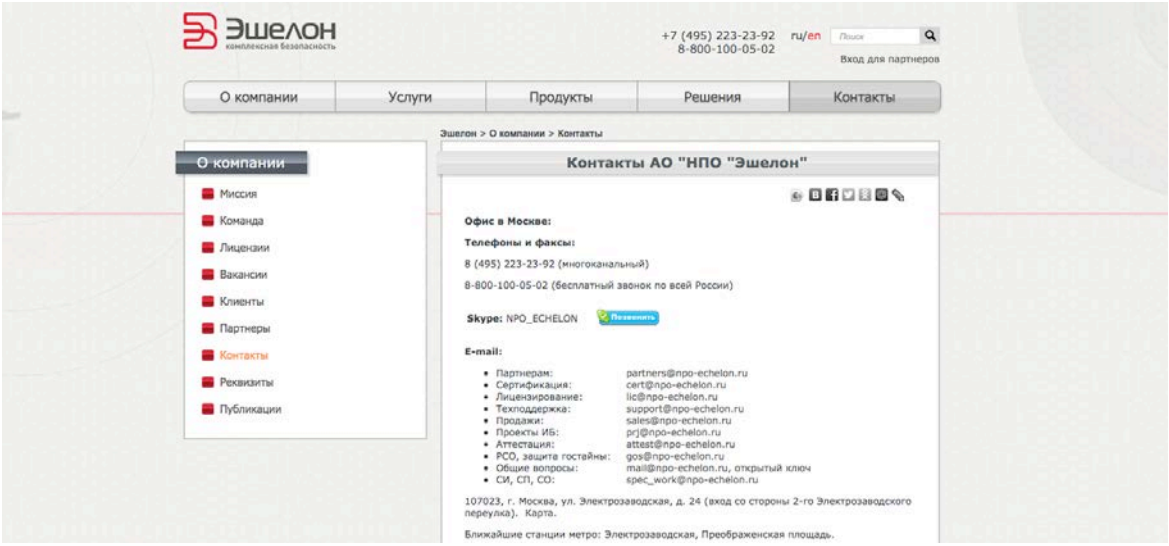
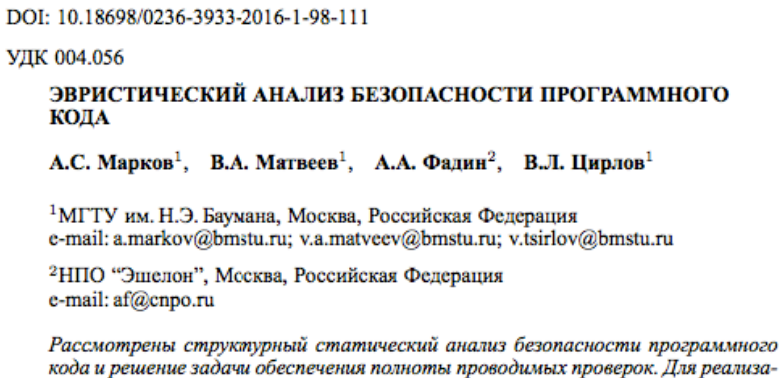


Рисунок 2 – Поиск информации о сотрудниках компании

Анализируя контент сайта, обнаруживаем пример персональной электронной почты «a.markov@bmstu.ru» в разделе «Публикации» (рисунок 3).



DOI: 10.18698/0236-3933-2016-1-98-111

УДК 004.056

ЭВРИСТИЧЕСКИЙ АНАЛИЗ БЕЗОПАСНОСТИ ПРОГРАММНОГО КОДА

А.С. Марков[1], В.А. Матвеев[1], А.А. Фадин[2], В.Л. Цирлов[1]

[1]МГТУ им. Н.Э. Баумана, Москва, Российская Федерация
e-mail: a.markov@bmstu.ru; v.a.matveev@bmstu.ru; v.tsirlov@bmstu.ru

[2]НПО "Эшелон", Москва, Российская Федерация
e-mail: af@cnpo.ru

Рассмотрены структурный статический анализ безопасности программного кода и решение задачи обеспечения полноты проводимых проверок. Для реализа-

Рисунок 3 – Детекция адресов электронной почты сотрудников

Предполагаем, что почтовый адрес на домене «@npo-echelon.ru» формируется аналогично. Для проверки предположения формируем запрос в поисковике (рисунок 4).

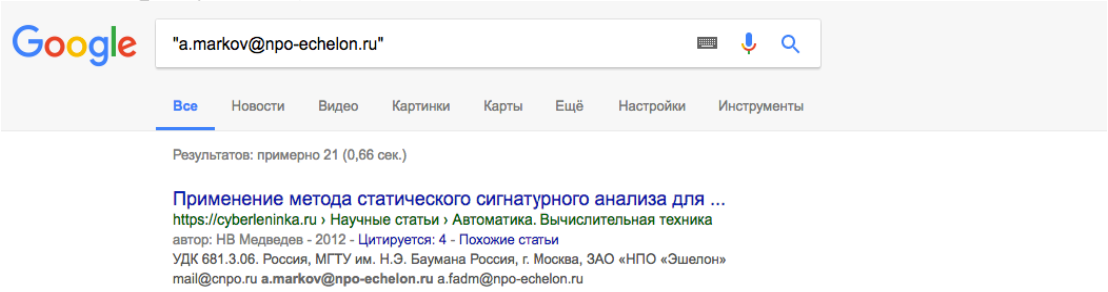


Рисунок 4 – Проверка рабочего почтового адреса

Для поиска по файлов на домене организации, содержащих заголовок «АК-ВС» и имеющих расширение PDF нужно сформировать запрос «site:“npo-echelon” filetype:pdf intitle:АК-ВС» (рисунок 5).

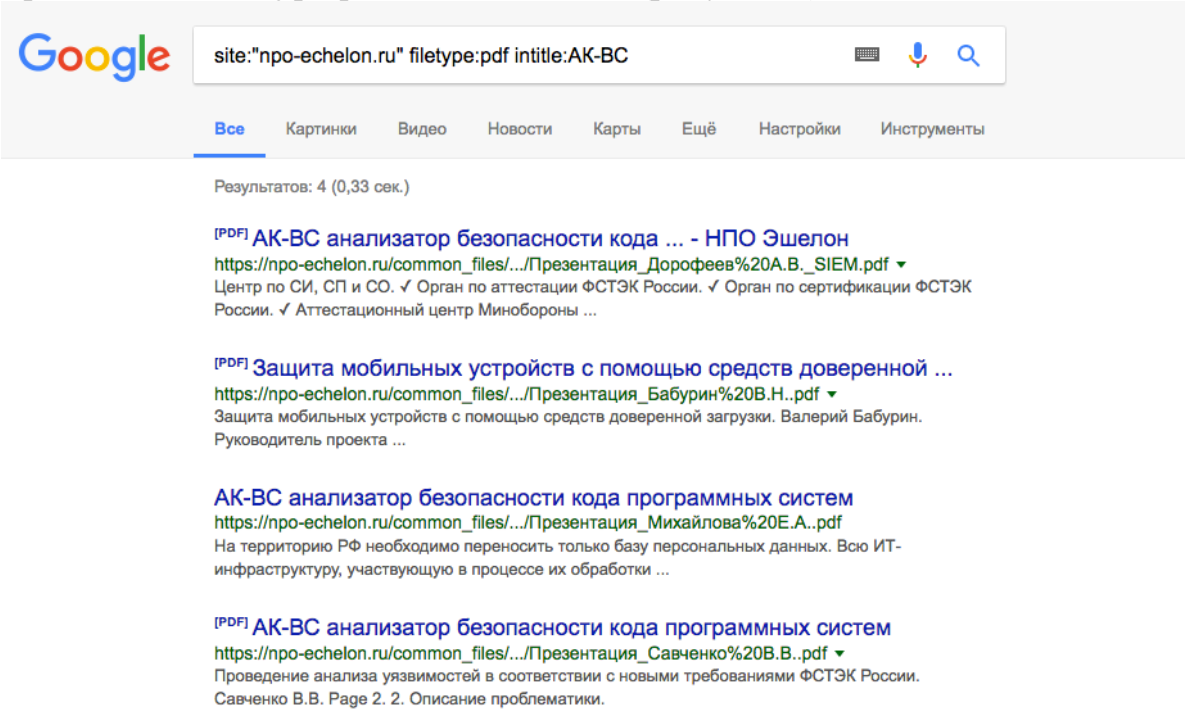


Рисунок 5 – Поиск по файлам на домене организации

Для получения списка закрытых для индексации поисковиками директорий, необходимо открыть файл «robots.txt» Для его получения в адресной строке нужно ввести https://npo-echelon.ru/robots.txt (рисунок 6).

```
User-agent: MJ12bot
Disallow: /

User-agent: *
Disallow: /bitrix/
Disallow: /admin/
Disallow: /upload/
Disallow: /img/
Disallow: /rss/forum.kz/
Crawl-delay: 8 # задает таймаут в 8 секунд
```

Рисунок 6 – Список закрытых для индексации поисковиками директорий

Для анализа сайта на предмет предыдущих версий необходимо воспользоваться сервисом «waybackmachine.org» (рисунок 7).

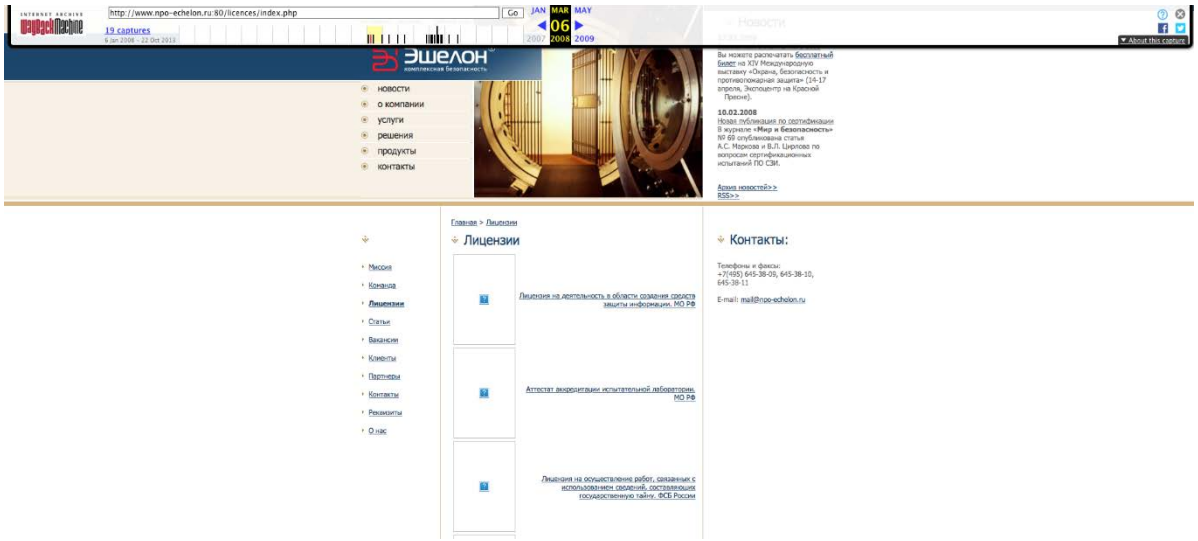


Рисунок 7 – Анализ на предмет предыдущих версий сайта

Для получения информации о домене необходимо в консоли unix-системы запустить утилиту «whois» с IP-адресом и доменным именем сайта. IP-адрес определяется путем запуска команды «ping» (рисунок 8-9).

```
MacBook-Pro:~ vladimir$ ping npo-echelon.ru
PING npo-echelon.ru (92.53.126.205): 56 data bytes
64 bytes from 92.53.126.205: icmp_seq=0 ttl=54 time=7.869 ms
^C
--- npo-echelon.ru ping statistics ---
2 packets transmitted, 1 packets received, 50.0% packet loss
round-trip min/avg/max/stddev = 7.869/7.869/7.869/0.000 ms
MacBook-Pro:~ vladimir$ whois 92.53.126.205
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

refer:        whois.ripe.net

inetnum:      92.0.0.0 - 92.255.255.255
organisation: RIPE NCC
status:       ALLOCATED

whois:        whois.ripe.net

changed:      2007-03
source:       IANA

% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '92.53.126.0 - 92.53.127.255'

% Abuse contact for '92.53.126.0 - 92.53.127.255' is 'abuse@timeweb.ru'

inetnum:        92.53.126.0 - 92.53.127.255
netname:        TimeWeb-12
descr:          TimeWeb shared hosting
country:        RU
admin-c:        TMWB-RIPE
tech-c:         TMWB-RIPE
status:         ASSIGNED PA
mnt-by:         TIMEWEB-MNT
created:        2014-04-15T06:48:00Z
last-modified:  2014-04-15T06:48:00Z
source:         RIPE

role:           TimeWeb Co. Ltd. Role Account
address:        22A,Zastavskaya str.
address:        196084, Saint-Petersburg
address:        Russia
phone:          +7 812 2441081
phone:          +7 495 6041081
phone:          +8 800 3331081
abuse-mailbox:  abuse@timeweb.ru
admin-c:        AAB215-RIPE
tech-c:         AAB215-RIPE
tech-c:         NARR-RIPE
tech-c:         IM3126-RIPE
tech-c:         SVV280-RIPE
nic-hdl:        TMWB-RIPE
mnt-by:         TIMEWEB-MNT
created:        2008-03-18T10:36:42Z
last-modified:  2018-02-20T11:50:26Z
source:         RIPE # Filtered
```

Рисунок 8 – Запуск утилиты «whois» с IP-адресом

```
MacBook-Pro:~ vladimir$ whois npo-echelon.ru
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

refer:        whois.tcinet.ru

domain:       RU

organisation: Coordination Center for TLD RU
address:      8 Marta street 1, bld 12
address:      Moscow  127083
address:      Russian Federation

contact:      administrative
name:         .RU domain Administrative group
organisation: Coordination Center for TLD RU
address:      8 Marta street 1, bld 12
address:      Moscow  127083
address:      Russian Federation
phone:        +7 495 730 29 71
fax-no:       +7 495 730 29 68
e-mail:       ru-adm@cctld.ru

contact:      technical
name:         Technical Center of Internet
organisation: Technical Center of Internet
address:      8 Marta street 1, bld 12
address:      Moscow  127083
address:      Russian Federation
phone:        +7 495 730 29 69
fax-no:       +7 495 730 29 68
e-mail:       ru-tech@tcinet.ru

nserver:      A.DNS.RIPN.NET 193.232.128.6 2001:678:17:0:193:232:128:6
nserver:      B.DNS.RIPN.NET 194.85.252.62 2001:678:16:0:194:85:252:62
nserver:      D.DNS.RIPN.NET 194.190.124.17 2001:678:18:0:194:190:124:17
nserver:      E.DNS.RIPN.NET 193.232.142.17 2001:678:15:0:193:232:142:17
nserver:      F.DNS.RIPN.NET 193.232.156.17 2001:678:14:0:193:232:156:17
ds-rdata:     33094 8 2 7228B0DCE8E4DEDA575C7DB69CBF55C43FCCC4BB60FBCC717DDABED1D17338E1

whois:        whois.tcinet.ru

status:       ACTIVE
remarks:      Registration information: http://www.cctld.ru/en

created:      1994-04-07
changed:      2017-10-03
source:       IANA

% By submitting a query to RIPN's Whois Service
% you agree to abide by the following terms of use:
% http://www.ripn.net/about/servpol.html#3.2 (in Russian)
% http://www.ripn.net/about/en/servpol.html#3.2 (in English).

domain:         NPO-ECHELON.RU
nserver:        dns1.yandex.ru.
nserver:        dns2.yandex.ru.
state:          REGISTERED, DELEGATED, VERIFIED
org:            JSC NPO Echelon
registrar:      R01-RU
admin-contact: https://partner.r01.ru/contact_admin.khtml
created:        2007-02-08T21:00:00Z
paid-till:      2019-02-08T21:00:00Z
free-date:      2019-03-12
source:         TCI

Last updated on 2018-03-19T09:06:34Z
```

Рисунок 9 - Запуск утилиты «whois» с доменным именем сайта

Для автоматизированного поиска субдоменов организации устанавливаем утилиту Sublist3r согласно инструкции (https://github.com/aboul3la/Sublist3r) и запускаем ее с указанием домена (рисунок 10).

Рисунок 10 – Запуск утилиты Sublist3r

Таким образом, используя информацию только открытых источников, удалось установить имя почтового домена компании, имена субдоменов компании, способ формирования адресов рабочей почты сотрудников.

3 СКАНИРОВАНИЕ

Собрав на предыдущем этапе информацию о целевой организации из открытых источников, исследователь безопасности переходит ко второму этапу – непосредственному получению информации от внутренних сетевых сервисов целевой организации. Если на предыдущем этапе действия исследователя безопасности было практически невозможно обнаружить ни одним из известных инструментов, используемых в целях предотвращения атак, то на этапе сканирования, когда идет обращение к сервисам напрямую, активность достаточно легко заметить. Если поставленной задачей является проведение аудита информационной системы таким образом, чтобы об этом не узнал персонал одела ИТ, то встает вопрос сокрытия используемого IP-адреса с помощью использования различных прокси-серверов или специализированного программного обеспечения.

3.1 Сканирование портов

Сканирование портов является самым первым этапом активной разведки и, пожалуй, одним из основных. Данный метод позволяет выявить активные машины, работающие в сети целевой организации, а также установленное на них программное обеспечение, запущенные сетевые сервисы и, в некоторых случаях, версию операционной системы. Сканирование TCP-портов основано на «трехстороннем рукопожатии» (three-way handshake). Сканер посылает пакет SYN на сканируемый порт и в случае, когда порт открыт, получает в ответ пакет ACK, а если порт закрыт — пакет RST. Сканирование UDP-портов имеет свою особенность, так как протокол UDP, в отличие от TCP, не гарантирует надежной доставки информации и не использует «рукопожатий». Если при сканировании обнаруживается, что порт закрыт, сканер получает назад сообщение «порт недоступен». В свою очередь, отсутствие такого сообщения позволяет сканеру принять решение о том, что порт открыт. Но тут есть одна проблема: если перед сервером стоит брандмауэр, который блокирует идущие от сканера запросы, то сканер не будет получать сообщение о неудачном подключении и примет неверное решение о том, что порт открыт.

3.2 Определение активных хостов

Определение активных хостов помогает сократить время, которое требуется для проведения аудита. Определив активные хосты и сконцентрировавшись только на них, исследователь безопасности может

сэкономить большое количество времени и уменьшить объем работы. Для определения активных хостов можно использовать команду ping.

Ping — стандартная утилита, которая входит в состав любой ОС. Однако у данного метода есть один недостаток — очень часто ICMP, на основе которого и работает ping, заблокирован на уровне брандмауэра. И в этом случае хост, на который отправляются запросы, не будет на них отвечать.

Поскольку ping обладает достаточно ограниченной функциональностью, вдобавок используется утилита hping3, которая работает не только с ICMP, но и с TCP-протоколом, следовательно, она может отправлять запросы на любой порт, получать ответы и обрабатывать их.

3.3 Получение информации от DNS-сервера

Благодаря информации, которую можно получить от DNS-сервера, можно составить список публичных внешних, а порой и внутренних серверов, используемых целевой организацией. Взаимодействовать с DNS-сервером можно несколькими различными способами, например, через кроссплатформенную утилиту nslookup.

Типы записей, используемых DNS-сервисом:

- A (Address) — связывает доменное имя и IP-адрес;
- SOA (Start of Authority) — показывает, какие DNS отвечают за эталонную информацию о данной зоне;
- CNAME (Canonical Name) — дополнительное имя для данного домена;
- MX (Mail Exchange) — определяет, какие почтовые серверы обслуживают данную зону;
- SRV (Service) — показывает, какие сервисы обслуживают данную зону (например, серверы активной директории);
- PTR (Pointer) — привязывает IP-адрес к доменному имени;
- NS (Name Server) — показывает, какие DNS-серверы обслуживают данную зону.

Используя информацию из этих записей, можно получить много полезной информации.

4 ПОИСК И ЭКСПЛУАТАЦИИ УЯЗВИМОСТЕЙ

Итак, найден сервер, к которому можно получить доступ. Обычно для несанкционированного подключения используют уязвимости в установленном программном обеспечении. Поиск уязвимостей можно осуществлять вручную, используя полученную информацию и базы данных уязвимостей. Однако это очень долгий и трудоемкий процесс. А можно воспользоваться сканерами уязвимостей. Самые популярные из них — Nessus, OpenVAS, Retina и Nexpose. Они позволяют не только находить открытые уязвимости в установленном программном обеспечении и операционных системах, но и определять устаревшие протоколы шифрования, зараженные компьютеры и многое другое. OpenVAS входит в состав Kali Linux.

Kali Linux является передовым Linux-дистрибутивом для проведения тестирования на проникновение и аудита безопасности. Kali включает более 600 инструментов, ориентированных на различные задачи информационной безопасности, такие как тестирование на проникновение, сбор информации, форензика и обратная инженерия. Kali Linux разрабатывается, финансируется и поддерживается Offensive Security, лидирующей компанией в сфере обучения информационной безопасности. В качестве основы для создания Kali Linux был выбран распространенный дистрибутив – Debian, что делает его использование простым для широкого круга пользователей Ubuntu, Knoppix и других дистрибутивов, основанных на Debian.

Все действия, проводимые на данном этапе в ходе проведения тестирования на проникновение, могут быть замечены администраторами целевой системы. Если это случится, то они наверняка попробуют помешать проведению дальнейших действий.

Для разработки, тестирования и применения эксплойтов была создана программная платформа Metasploit Framework.

Эксплойт — это специальная программа, использующая известные уязвимости в программном обеспечении для проведения атаки с целью получения контроля над системой или вывода ее из строя (отказа в обслуживании). Эксплойты бывают удаленными, работающими через компьютерную сеть, и локальными, запускающимися непосредственно в самой системе. В Metasploit эксплоиты делятся на активные и пассивные. Активные начинают эксплуатировать определенную уязвимость в программном обеспечении сразу же после запуска и закачивают свою работу в случае удачи или провала. Пассивные ждут подключения удаленного хоста и только после этого начинают свою работу. Например, можно запустить эксплойт, отправив жертве клиентскую часть по электронной почте. После того, как получатель откроет приложение к письму, клиентская часть соединится с запущенным ранее эксплойтом, и тот

начнет атаку. Просмотреть все доступные эксплойты можно, используя команду show exploits, однако, учитывая их огромное количество, это не всегда удобно.

Metasploit является универсальным инструментом для проведения аудита безопасности. Данный фреймворк постоянно поддерживается и обновляется. Основная работа с бесплатной версией происходит через командный интерфейс с использованием msfconsole. Однако, существует и графический интерфейс Armitage.

Metasploit состоит из ядра, которое обеспечивает совместную работу следующих подключаемых компонентов:

1. интерфейсы: консольный и графические;

2. модули:

– эксплойты (обеспечивают возможность эксплуатации найденной уязвимости);

– полезная нагрузка (программа, которая запускается после успешной работы эксплойта и выполняет переделенную функцию, например, создание пользователя, открытие порта и т. д.);

– вспомогательные модули (сканер портов, перебор паролей, анализ трафика и т. д.);

– энкодеры (позволяют скрыть вредоносный код от систем защиты путем его многократного преобразования) и т. д.

3. расширения — позволяют значительно расширить функционал Metasploit.

5 ПАРОЛЬНЫЕ АТАКИ НА РАЗЛИЧНЫЕ СЕРВИСЫ

По умолчанию пара логин и пароль используется для аутентификации во всех системах. Будь то веб-приложение, операционная система или база данных.

Существует два основных метода атак на пароли. На самом деле существует множество способов взлома пароля, но все они — это в основном модификации либо прямого перебора, либо перебора по словарю.

1. Перебор паролей. Название метода говорит само за себя: в данном случае атакующий просто подбирает пароль. Вначале, например, перебираются все цифры от 0 до 9, затем от 10 до 99, от 100 до 999 и т. д. Вручную подобрать пароль таким способом не представляется возможным, для этого используют специальное программное обеспечение, которое мы рассмотрим чуть позже.

2. Атаки по словарю. Суть метода заключается в том, что атакующий подбирает пароль не случайным образом, а берет слова из заранее подготовленного файла с паролями. Разумеется, перебор, как и в предыдущем случае, не ведется вручную.

Файл с паролями можно найти в Интернете. Но поскольку очень часто пользователи используют для создания паролей название своей профессии, дату рождения или название организации, то в некоторых случаях самостоятельно созданный список паролей будет намного лучше найденных в Интернете.

Разумеется, создать вручную список хотя бы из 1000 паролей — задача довольно сложная. Существуют способы автоматизации этого процесса. Например, утилита Crunch, входящая в состав Kali Linux. Она может генерировать списки слов, основываясь на заданных пользователем правилах.

Например, зная политику безопасности компании хотя бы в отношении паролей, можно создать список из строк, содержащих, например, девять символов, одну заглавную букву и одну цифру.

Второй способ создания собственного, персонализированного списка паролей — это использование слов и фраз с сайта организации. Для данной цели можно использовать инструмент под названием cewl, который также входит в состав Kali Linux.

Пароли редко хранятся в открытом виде, в подавляющем большинстве они записаны в виде хешей. Хеш — результат работы функции, преобразующей входные данные в строку определенной длины. Хеши паролей хранятся в файлах и базах данных. Из хеша нельзя получить пароль, только перебором можно подобрать пароль с таким же хешем. Для разных паролей не может существовать одинаковых хешей (в современных алгоритмах). Для перебора необходимо вначале установить тип алгоритма, с помощью которого получен данный хеш. Все это делается с

использованием специального ПО, например, John the Ripper. Также для этих целей можно использовать радужные таблицы.

Радужные таблицы – это заранее рассчитанный набор данных, который содержит хеш-функции из множества комбинации букв и цифр. Если значение хеш-функции известно, то в таблице очень быстро можно найти соответствующий пароль.

Предпосылками создания радужных таблиц является построение цепочек возможных паролей. В начале каждой отдельной цепочки есть случайный пароль, далее цепочка подвергается действию хеш-функции и функции репродукции. Эта функция преобразует результат хеш-функции в некоторый возможный пароль. Промежуточные пароли в цепочку не сохраняются, а в таблицу заносятся только первый и последний элементы цепочек.

Таблицы предоставляют доступ только к той хеш-функции, для которой они создавались.

6 СРЕДСТВО ДЛЯ ТЕСТИРОВАНИЯ ЭКСПЛОЙТОВ METASPLOITABLE 2

Главная цель существования Metasploitable 2 - помочь специалистам по информационной безопасности оценить свои навыки, легально проверить различные инструменты; помочь разработчикам лучше понять механизм написания безопасного кода; а также дать возможность студентам и преподавателям узнать больше о безопасности контролируемой среды. Metasploitable 2 предоставляет возможность попрактиковаться в эксплуатации наиболее популярных уязвимостей.

Виртуальная машина Metasploitable является умышленно уязвимой версией виртуальной машины Ubuntu Linux, в предустановленной в ней операционной системе заранее открыты все порты и присутствуют наиболее известные уязвимости, некоторые из которых встречаются в реальной жизни на действующих системах.

7 ДЕМОНСТРАЦИЯ ЭКСПЛУАТАЦИИ УЯЗВИМОСТЕЙ

Далее рассмотрены способы эксплуатации уязвимостей на примере двух сервисов. Эксплуатация допускается в ручном и автоматизированном режимах.

Для атаки на сервис *ftp* версии *vsftpd 2.3.4* необходимо с помощью утилиты *searchsploit* и ключевого слова осуществить поиск существующих эксплойтов (рисунок 11). Для поиска также допускается использование онлайн-баз, таких как *exploit-db*.

Результатом поиска является ссылка на готовый эксплойт при его наличии. Для автоматизированной эксплуатации необходимо запустить «Metasploit», набрав *msfconsole* в терминале «Kali Linux», затем определить местоположение эксплойта с помощью команды search и выбрать его командой *use* (рисунок 12).

```
root@bad:~#
root@bad:~# searchsploit vsftpd 2.3.4
---------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                                |  Path
                                                                                              | (/usr/share/exploitdb/platforms/)
---------------------------------------------------------------------------------------------- ---------------------------------
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)                                        | unix/remote/17491.rb
---------------------------------------------------------------------------------------------- ---------------------------------
root@bad:~#
```

Рисунок 11 – Поиск эксплойтов утилитой searchsploit

```
Terminal
File  Edit  View  Search  Terminal  Help
A database appears to be already configured, skipping initialization

# cowsay++
 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *


       =[ metasploit v4.16.7-dev                  ]
+ -- --=[ 1682 exploits - 964 auxiliary - 299 post       ]
+ -- --=[ 498 payloads - 40 encoders - 10 nops           ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > search vsftpd 2.3.4

Matching Modules
================

   Name                                  Disclosure Date  Rank       Description
   ----                                  ---------------  ----       -----------
   auxiliary/gather/teamtalk_creds                        normal     TeamTalk Gather Credentials
   exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  VSFTPD v2.3.4 Backdoor Command Execution
   exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  VSFTPD v2.3.4 Backdoor Command Execution


msf >
```

Рисунок 12 – Результаты поиска эксплойтов

После выбора эксплойта необходимо командой *options* проверить доступные опции для настройки, затем настроить обязательные командой *set*. После окончания настроек эксплойт запускается командой *run* (рисунок 13).

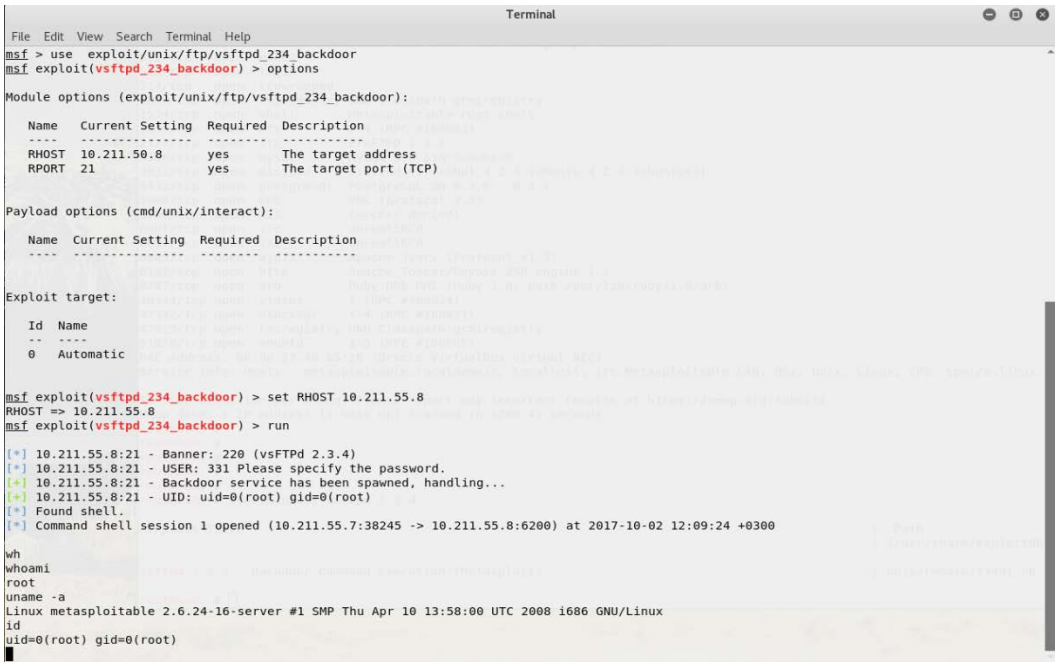


Рисунок 13 – Процесс проверки, настройки и запуска эксплойта

Для проверки корректности полученной сессии необходимо ввести команду *uname* с параметром *-a*.

Эксплуатация неверно сконфигурированных сервисов может осуществляться в ручном режиме. Для эксплуатации неверно сконфигурированного набора *r* сервисов, находящихся на портах 512, 513,514 необходимо воспользоваться штатными средствами, набрав в консоли «Kali Linux» команду *rlogin* и адрес «атакуемой» машины.

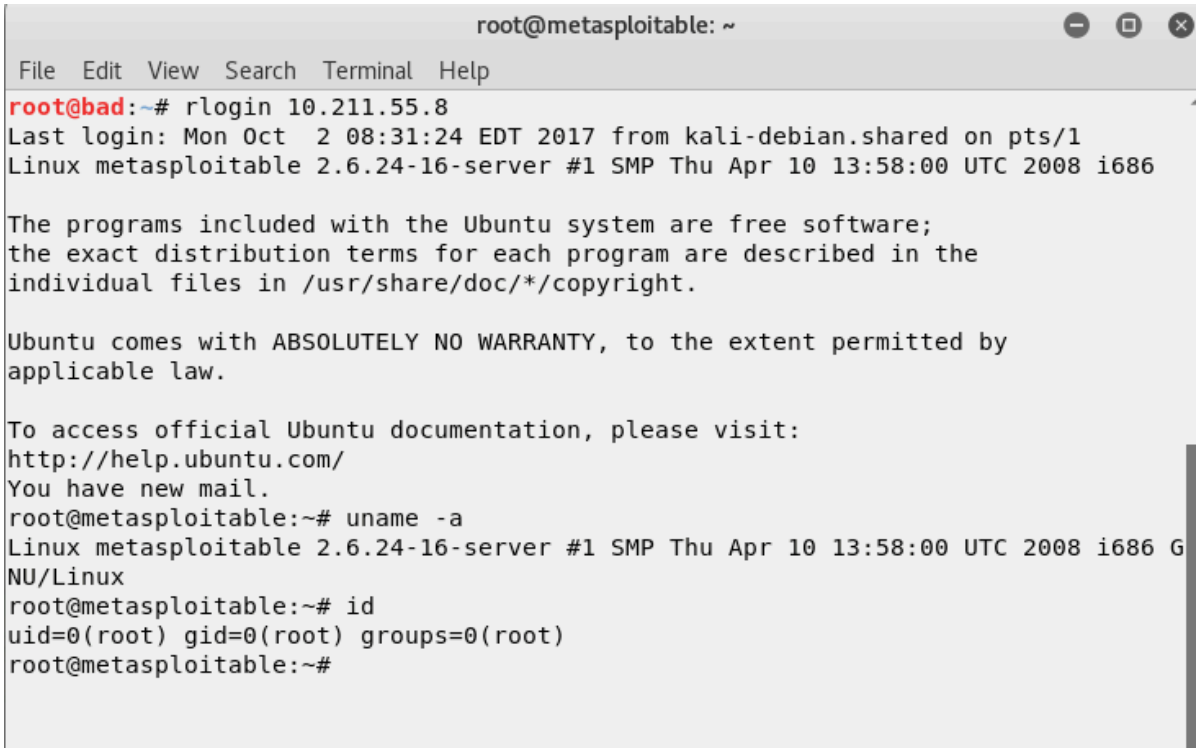


Рисунок 14 - Проверка корректности полученной сессии

Для проверки корректности полученной сессии необходимо ввести команду *uname* с параметром *-a*.

Автоматизированная эксплуатация уязвимости так же возможна с применением эксплойтов, не включенных в состав «Metasploit». Для атаки на уязвимую версию модуля «OpenSSL», используемого сервисом *ssh*, необходимо скачать архив с ключами *rsa* по ссылке https://github.com/offensive-security/exploit-database-bin-sploits/raw/master/bin-sploits/5622.tar.bz2 и распаковать его. Затем необходимо скачать утилиту по ссылке https://www.exploit-db.com/exploits/5720/ и запустить ее. В качестве параметров указываются путь до директории с *rsa* ключами, адрес уязвимой машины, пользователь и порт, на котором находится сервис *ssh* (рисунок 15).

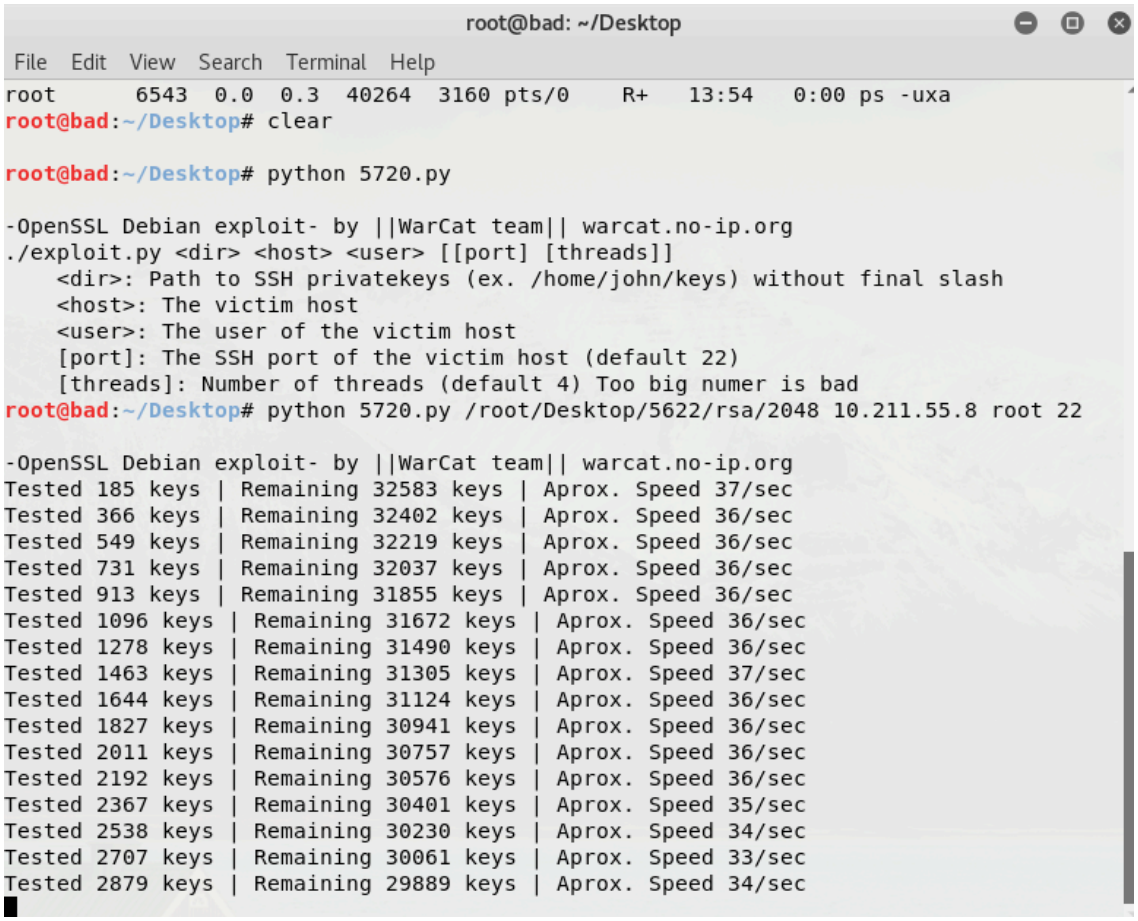


Рисунок 15 – Побор rsa ключа путем эксплуатации уязвимости библиотеки OpenSSL

Результатом выполнения программы является подходящий ключ rsa. Для получения доступа к уязвимой машине необходимо выполнить следующую команду «ssh -l[пользователь] – p[порт] -i [путь до rsa ключа] [ip адрес]» (рисунок 16).

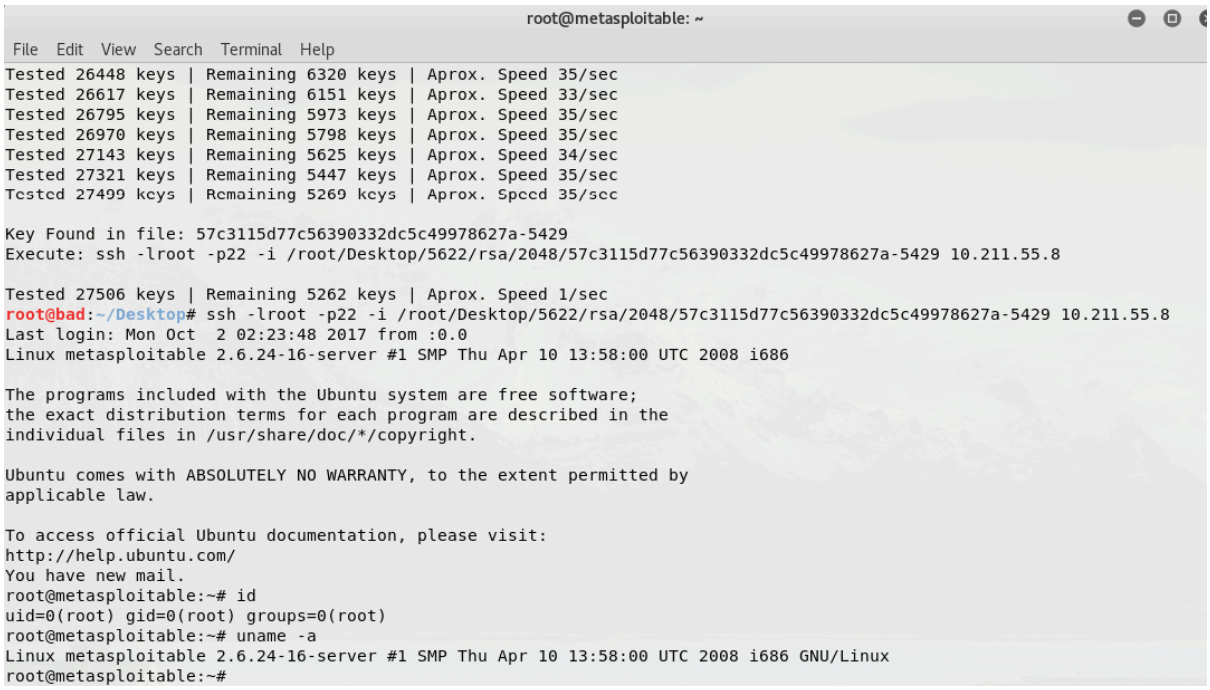


Рисунок 16 – Подключение к удаленной рабочей машине с использованием обнаруженного ключа

Для проверки корректности полученной сессии необходимо ввести команду «uname» с параметром «-a».

8 ЭКСПЛУАТАЦИЯ УЯЗВИМОСТЕЙ В WEB-ПРИЛОЖЕНИЯХ

Предположим, что в ходе сбора информации о целевой организации было обнаружено веб-приложение. Веб-приложением можно назвать все что угодно, главный принцип — приложение запускается на стороне сервера, а для доступа к нему используется клиент. Это может быть домашняя страничка организации, веб-интерфейс для просмотра корпоративной почты, онлайн-система мониторинга или браузерный чат, все это - веб-приложения.

Взлом веб-приложения становится возможным по двум причинам:

1) это программный комплекс, который, как и любой другой, может быть взломан;

2) чем больше программного кода, тем выше вероятность наличия ошибки в нем.

Объемы информации, с которыми работают веб-приложения, весьма велики. На веб-сервере могут храниться персональные данные пользователей (клиентов, сотрудников) и информация, в том или ином виде составляющая коммерческую или профессиональную тайну (например, финансовая информация или служебная переписка).

8.1 Межсайтовый скриптинг (XSS)

XSS — тип атаки на пользователя, который осуществляется благодаря включению в ответы веб-приложения кода злоумышленника. Чаще всего такому типу атак подвержены приложения, в которых отсутствует проверка введенных пользователем данных. Скажем, при регистрации пользователь может ввести в поле «имя» не только буквы, но и специальные символы, такие как «№» или «*», хотя в имени не может быть специальных символов.

Чаще всего злоумышленники используют JavaScript или Flash, но учитывая разнообразие поддерживаемых браузером технологий, это может быть что угодно. Самыми частыми целями такого типа атак являются:

- кража cookie-файла пользователя, взаимодействие с передаваемой во время сессии информацией, а также перенаправление пользователя на другой сайт. При помощи XSS можно украсть cookie-файл. Для этого понадобятся: уязвимая форма и утилита netcat, позволяющая взаимодействовать в интерактивном режиме с любым сетевым сервисом (может выступать как в роли сервера, так и в роли клиента);
- перенаправление браузера - таким образом можно заставить пользователя скачать файл. Когда пользователь зайдет на скомпрометированную страницу, браузер автоматически предложит ему скачать указанный файл.

8.2 Включение локальных или удаленных файлов

RFI (Remote File Inclusion) - это выполнение удаленных файлов на серверной стороне, иными словами это сервер, возвращающий с каким-то запросом код программы, который будет открыт и запущен на сервере-жертве. Зачастую из-за плохо написанного кода и некорректно сконфигурированного веб-сервера появляется возможность включать данные из локального или находящегося на удаленном сервере файла в исполняемый код.

8.3 SQL-инъекции

SQL-инъекции представляют собой один из самых интересных, сложных и мощных видов атак. Для их реализации требуются хорошие знания баз данных, самого SQL и веб-программирования. Если данные перед отправкой на сервер не проходят должной проверки, то существует возможность проведения атаки данного типа. SQL-инъекции — это атаки на веб-приложения, использующие для своей работы базы данных. Атаки, по сути, представляют собой внедрение кода в существующий запрос с целью получения доступа к данным или манипулирования ими. Благодаря повсеместной распространенности SQL атаки этого типа работают практически на всех платформах.

8.4 Command Injection

Командная инъекция - это атака, где целью является выполнение произвольных команд в операционной системе сервера через уязвимое приложение. Атаки с помощью командной инъекции возможны, когда веб-приложение принимает небезопасные пользовательские данные (формы, cookie, заголовки HTTP и т. д.) в системную оболочку. В этой атаке команды операционной системы предоставляемые атакующим обычно выполняются с привилегиями уязвимого приложения. Атаки командного внедрения возможны во многом из-за недостаточной проверки входных данных.

8.5 CSRF

CSRF (англ. Cross Site Request Forgery — «межсайтовая подделка запроса», также известна как XSRF) — вид атак на посетителей веб-сайтов, использующий недостатки протокола HTTP. Если жертва заходит на сайт, созданный злоумышленником, от её лица тайно отправляется запрос на другой сервер (например, на сервер платёжной системы), осуществляющий некую вредоносную операцию (например, перевод денег на счёт

злоумышленника). Для осуществления данной атаки жертва должна быть аутентифицирована на том сервере, на который отправляется запрос, и этот запрос не должен требовать какого-либо подтверждения со стороны пользователя, которое не может быть проигнорировано или подделано атакующим скриптом.

ЛАБОРАТОРНАЯ РАБОТА №1

Цель лабораторной работы: получение практических навыков тестирования на проникновение в части Интернет-разведки в рамках изучения дисциплины «Технология сертификации средств защиты информации».

Задание на лабораторную работу:

1. Выбрать организацию, о которой будет собираться информация;
2. Определить правила формирования почтовых учетных записей в организации;
3. Используя специальные операторы поисковиков найти документы с расширением PDF на домене организации;
4. Найти неиндексируемые URLs в файле robots.txt на домене организации;
5. Используя сервис (waybackmachine.org) посмотреть кэшированные копии сайта организации;
6. Определить диапазон сети, в который входит IP-адрес сайта и информацию о домене с помощью утилиты whois;
7. Найти субдомены основного домена организации и ознакомится с их содержимым.

ЛАБОРАТОРНАЯ РАБОТА №2

Цель лабораторной работы: получение практических навыков тестирования на проникновение в части эксплуатации уязвимостей в рамках изучения дисциплины «Технология сертификации средств защиты информации».

Для выполнения лобарной работы необходимы:

1. Средство виртуализации – VirtualBox;
2. Образ виртуальной машины для исследования – Metasploitable2;
3. Образ виртуальной машины атакующего – Kali Linux.

Подготовка к выполнению лабораторной работы:

1) Для выполнения лабораторной работы необходимо развернуть инфраструктуру. Для этого нужно скачать и установить среду виртуализации. Классическим решением является Oracle VM VirtualBox (https://www.virtualbox.org/), однако допускается использование аналогов.

2) Устанавливаем виртуальную машины «жертвы». В данной лабораторной работе это Metasploitable2 (Linux), содержащий набор уязвимых приложений. Для установки необходимо скачать файл https://sourceforge.net/projects/metasploitable/. Внутри zip-архива содержится файл с расширением «vmdk» (Virtual Machine Disk), содержащий образ Metasploitable2.

3) Далее в среде виртуализации необходимо создать новую виртуальную машину, выбрав тип «Linux», версию «Linux 2.6/3.x/4.x(64-bit)», указав в качестве жесткого диска скаченный ранее vmdk файл.

4) Для установки виртуальной машины «атакующего» необходимо по ссылке https://www.kali.org/downloads/ скачать iso файл с финальной версией дистрибутива Kali Linux.

5) Далее создаем новую виртуальную машину, выбрав тип «Linux», версию «Linux 2.6/3.x/4.x(64-bit)». После того как виртуальная машина будет создана, необходимо выбрать ее в списке сбоку и открыть меню настроек.

6) Во вкладке «Носители» необходимо выбрать «Контролер: IDE» и добавить новый экземпляр, указав в качестве источника скаченный iso образ (рисунок 17).

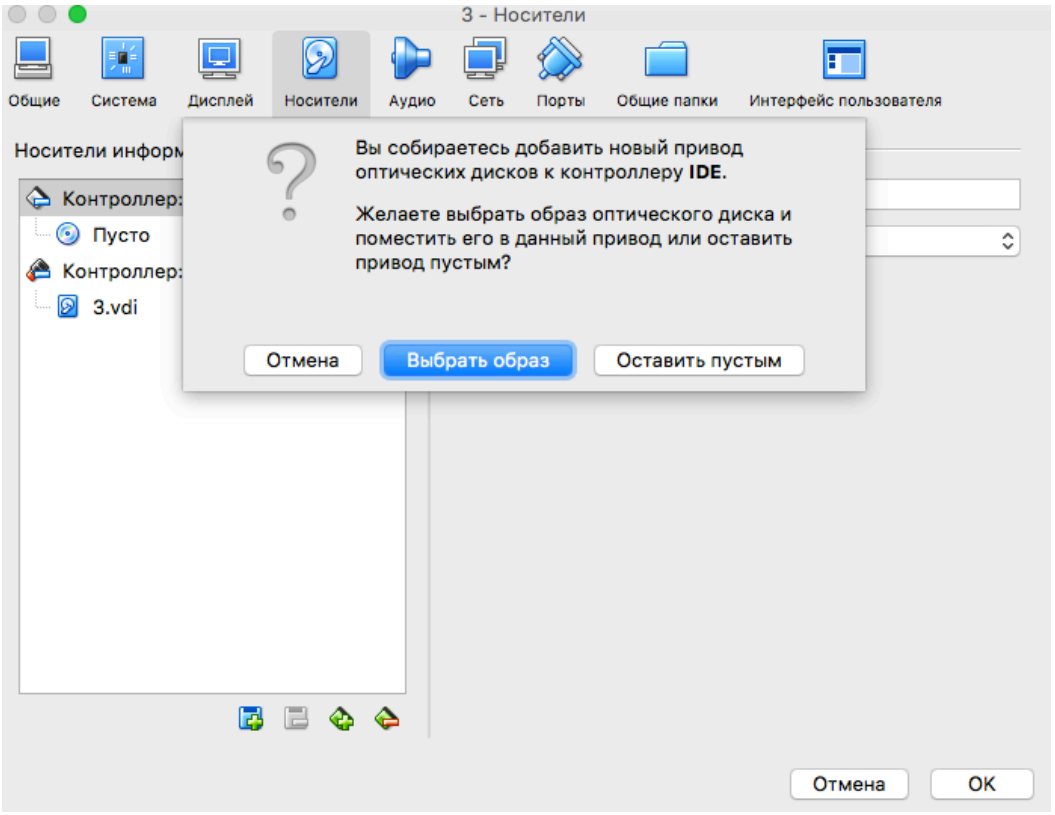


Рисунок 17 – Настройка виртуальной машины

7) Для завершения настройки инфраструктуры необходимо сконфигурировать сеть таким образом, чтобы виртуальные машины видели друг друга. Для этого во вкладке «Сеть» настроек (см. предыдущий этап) для каждой виртуальной машины необходимо выбрать тип подключения «NAT» (Network Adress Translation — механизм в сетях, построенных с использованием TCP/IP протокола, преобразующий IP-адреса транзитных пакетов). (рисунок 18).

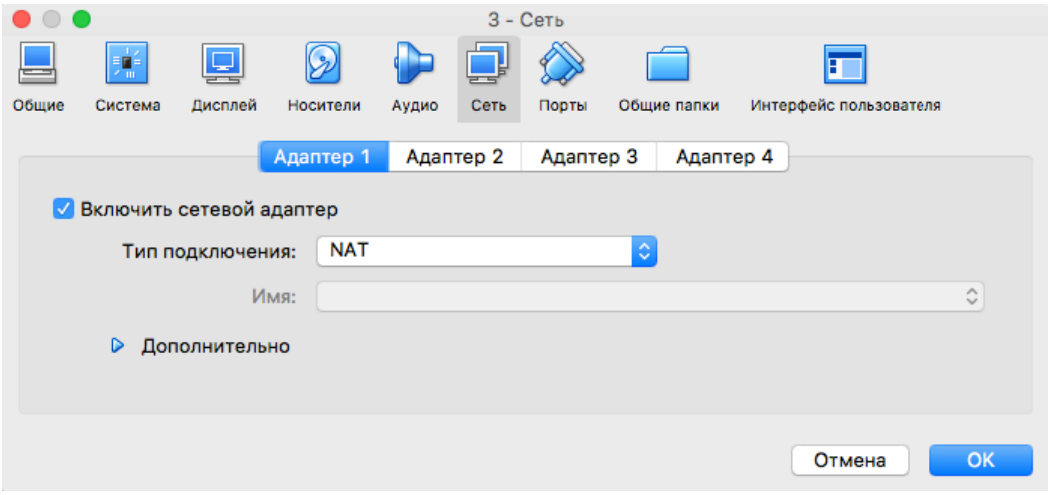


Рисунок 18 – Настройка виртуальной сети между виртуальными машинами

8) Далее необходимо проверить корректность настроек. С помощью команды «ifconfig» узнайте IP-адреса, полученные виртуальными машинами, а затем с помощью команды «ping» проверьте соединение (рисунок 19-21).

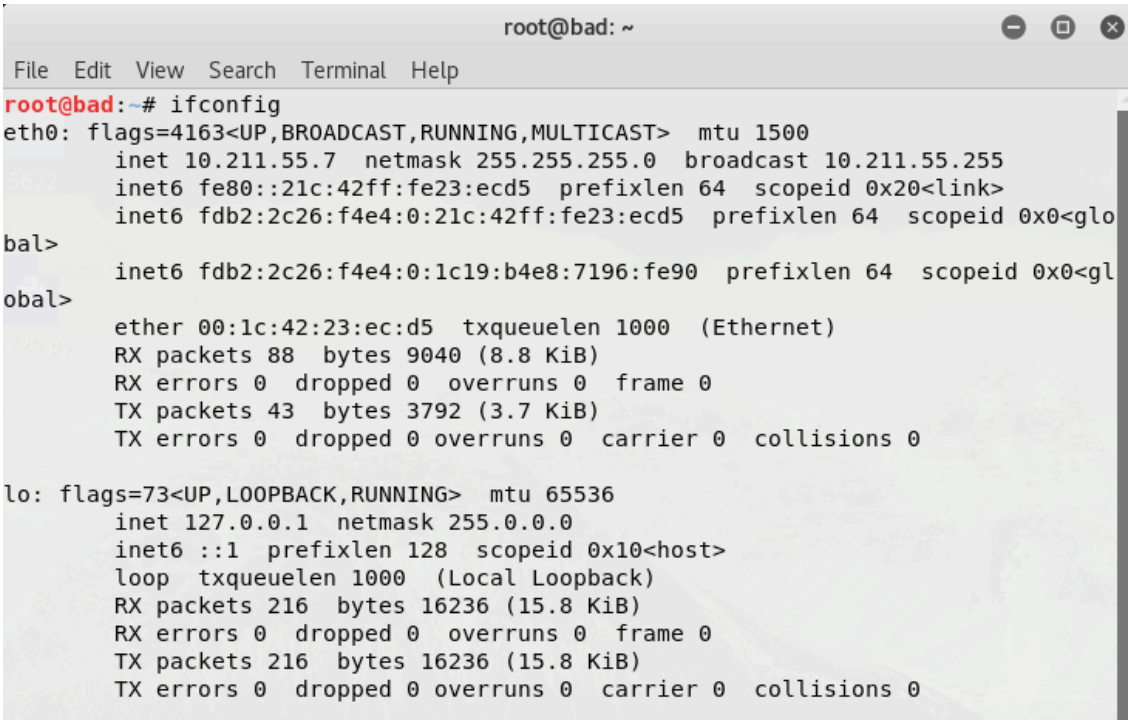


Рисунок 19 – Проверка сетевых настроек машины атакующего

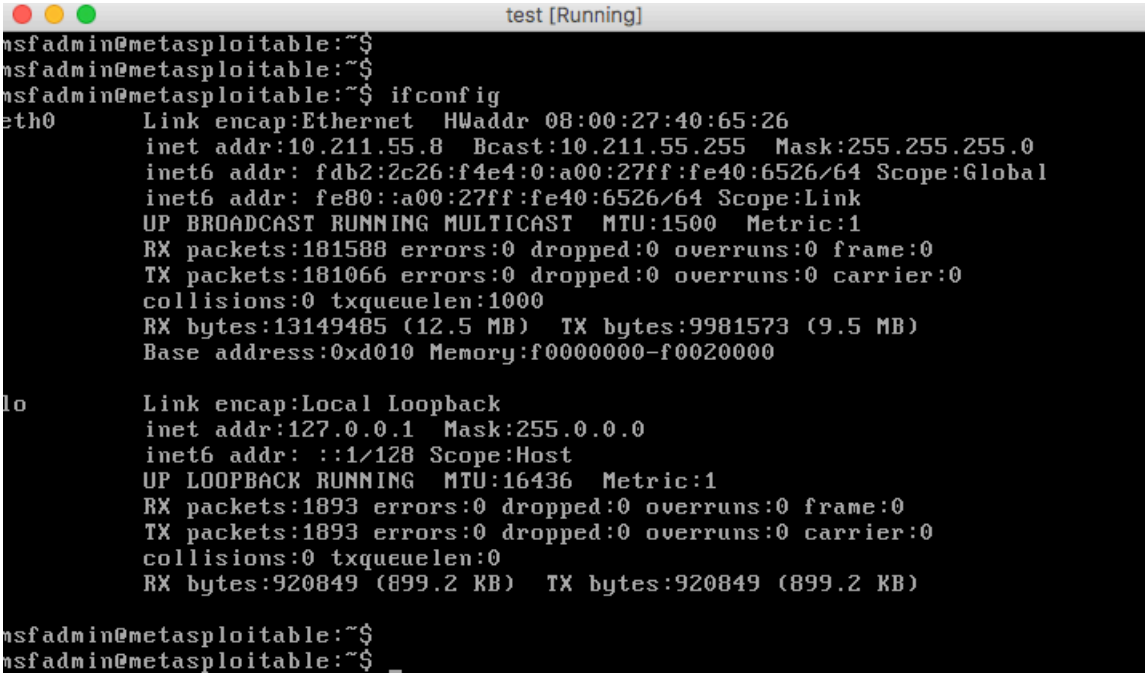


Рисунок 20 - Проверка сетевых настроек исследуемой машины

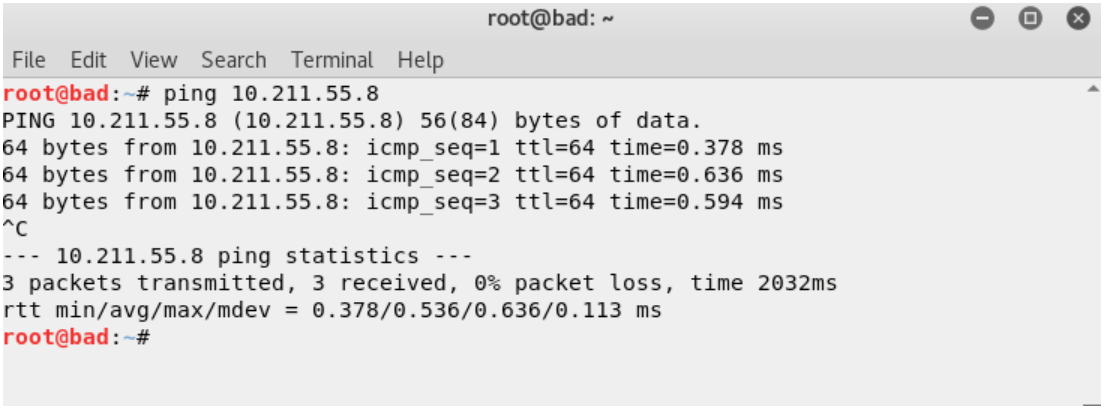


Рисунок 21 – Проверка соединения между виртуальными машинами

9) Для определения запущенных на исследуемой машине сетевых сервисов с машины «атакующего» необходимо произвести сканирование при помощи утилиты nmap (рисунок 22).

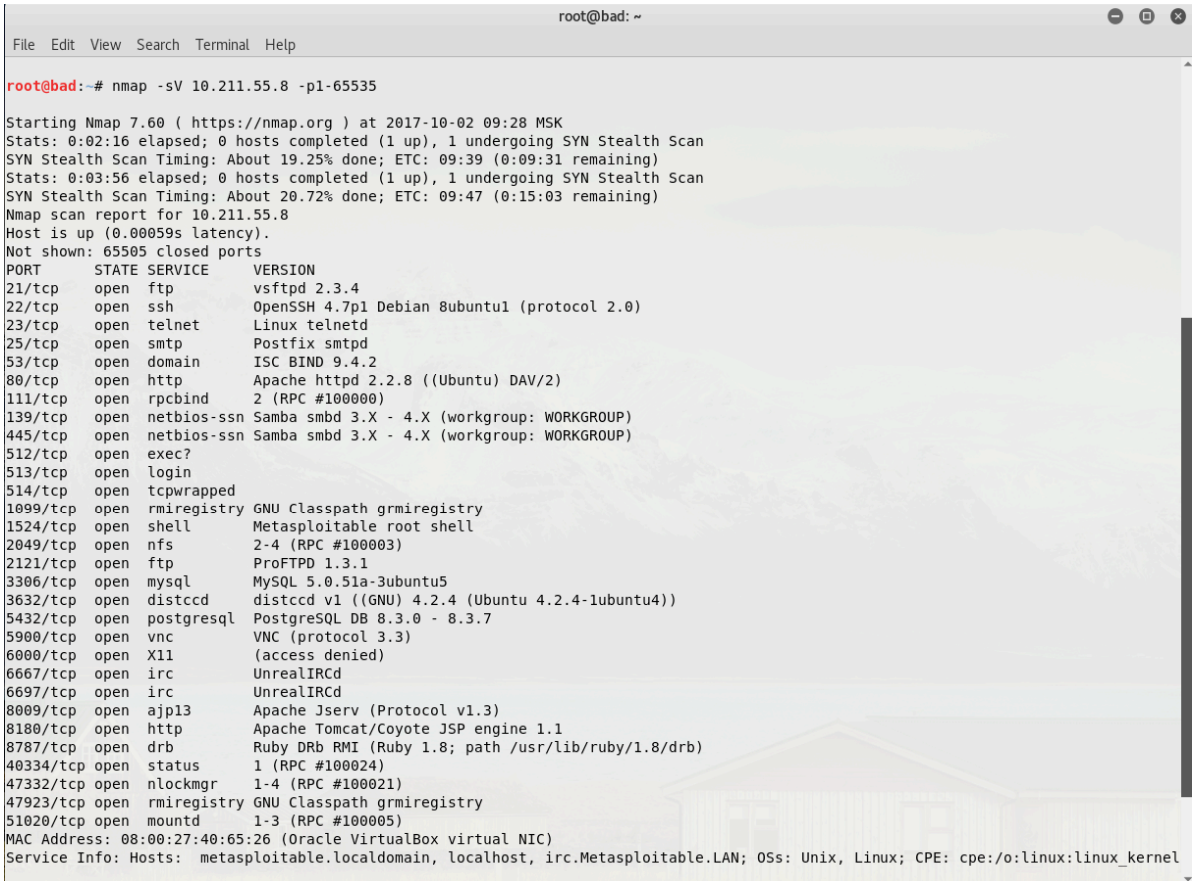


Рисунок 22 – Результат сканирования исследуемой машины

Полученный список сервисов используется для дальнейшей эксплуатации.

Задание на лабораторную работу:

1. Настроить инфраструктуру для выполнения лабораторной работы.
2. Определить доступные сервисы на исследуемой машине.

3. Получить удаленный доступ, путем эксплуатации уязвимостей четырех различных сервисов.

4. Оформить отчет по лабораторной работе.

ЗАКЛЮЧЕНИЕ

Данное учебно-методическое пособие призвано помочь студентам, изучающим в рамках своей образовательной программы дисциплину «Технология сертификации средств защиты информации», эффективнее освоить изучаемый материал – понять основы эксплуатации уязвимостей и осознать важность и необходимость сертификации.

Лабораторные работы, включенные в состав данного учебно-методического пособия, призваны помочь понять, как на практике происходит процесс сбора информации, процесс получения информации от сетевых сервисов (сканирования сети), процедура поиска и эксплуатации уязвимостей в рамках проведения тестирования на проникновение.

СПИСОК ЛИТЕРАТУРЫ

1. Скабцов Н.В. Аудит безопасности информационных систем. – СПб.: Питер, 2018, – 272 с.
2. Стародубцев Ю.И. Управление качеством информационных услуг / Ю.И. Стародубцев, А.Н. Бегаев, М.А. Дятлова; под общ. ред. Ю.И. Стародубцева. – СПб: Изд-во Политехн. Ун-та, 2017, – 454 с.
3. Weidman G. Penetration Testing: A Hands-On Introduction to Hacking. – NY.: Press.Inc, 2014, – 478 с.
4. Барабанов А.В., Дорофеев А.В., Марков А.С., Цирлов В.Л. Семь безопасных информационных технологий/Под. ред. А.С.Маркова. М.: ДМК Пресс, 2017. 224 с.
5. Бегаев А.Н., Тарасюк М.В. Контроль безопасности программного кода в составе объекта информатизации // Защита информации. Инсайд. 2013. № 5 (53). С. 63-67.
6. Дорофеев А. Тестирование на проникновение: демонстрация одной уязвимости или объективная оценка защищенности? // Защита информации. Инсайд. 2010. № 6 (36). С. 72-73.
7. Дорофеев А.В. Подготовка к CISSP: телекоммуникации и сетевая безопасность // Вопросы кибербезопасности. 2014. № 4 (7). С. 69-74.
8. Стародубцев Ю.И., Бегаев А.Н., Давлятова М.А. Управление качеством информационных услуг. СПб.: Изд-во Политехн. ун-та, 2017. 454 с.
9. Dorofeev A.V., Rautkin Y.V. Applied Aspects of Security Testing. In CEUR Workshop Proceedings, 2017, Vol-2081 (Selected Papers of the VIII All-Russian Scientific and Technical Conference on Secure Information Technologies, BIT 2017), pp. 49-53.
10. Дорофеев А.В., Марков А.С. Структурированный мониторинг открытых персональных данных в сети Интернет // Мониторинг правоприменения. 2016. № 1 (18). С. 41-53.
11. Doroveev A.V., Markov A.S., Tsirlov V.L. Social media in identifying threats to ensure safe life in a modern city // Communications in Computer and Information Science. 2016. V. 674. P. 441-449.
12. Барабанов А. Инструментальные средства проведения испытаний систем по требованиям безопасности информации // Защита информации. Инсайд. 2011. № 1 (37). С. 49-51.
13. Мамаев М.А., Петренко С.А. Обзор современных компьютерных атак на TCP/IP-сети // Защита информации. Инсайд. 2008. № 3 (21). С. 50-67.
14. Марков А.С., Миронов С.В., Цирлов В.Л. Опыт тестирования сетевых сканеров уязвимостей // Информационное противодействие угрозам терроризма. 2005. № 5. С. 109-122.

15. Мукминов В.А., Войнов Ю.В. Методика оценки реального уровня защищенности АСУ в условиях компьюторных атак // Известия Института инженерной физики. 2013. Т. 1. № 27. С. 80-85.
16. Рауткин В.Ю. Обзор способов достоверной идентификации сетевых устройств // Вопросы кибербезопасности. 2013. № 3. С. 54-60.
17. Барабанов А.В., Марков А.С., Фадин А.А., Цирлов В.Л. Статистика выявления уязвимостей программного обеспечения при проведении сертификационных испытаний // Вопросы кибербезопасности. 2017. № 2 (20). С. 2-8.
18. Барабанов А.В., Марков А.С., Цирлов В.Л. Испытания межсетевых экранов по требованиям безопасности информации: Учебное издание. М.: НЦПИ при Минюсте России, 2017. 44 с.
19. Александров Я.А., Чернов А.В., Марченко Е.А., Тахавиев Р.В., Сафин Л.К. Автоматическая оценка надежности процедуры аутентификации // Защита информации. Инсайд. 2016. № 5 (71). С. 20-25.
20. Марков Г.А., Шарунов В.А. К вопросу о парольной защите почтовых сервисов // Вопросы кибербезопасности. 2015. № 5 (13). С. 55-59.
21. Барабанов А.В., Лавров А.И., Марков А.С., Полотнянщиков И.А. Исследование атак типа "Межсайтовая подделка запросов" // Вопросы кибербезопасности. 2016. № 5 (18). С. 43-50.
22. Барабанов А.В., Федичев А.В. Разработка типовой методики анализа уязвимостей в веб-приложениях при проведении сертификационных испытаний по требованиям безопасности информации // Вопросы кибербезопасности. 2016. № 2 (15). С. 2-8.
23. Веряев А.С., Фадин А.А. Формализация требований безопасности информации к средствам анализа защищенности // Вопросы кибербезопасности. 2015. № 4 (12). С. 23-27.
24. Егоров М. Выявление и эксплуатация SQL-инъекций в приложениях // Защита информации. Инсайд. 2011. № 2 (38). С. 76-82.
25. Кубарев А.В. Подход к формализации уязвимостей информационных систем на основе их классификационных признаков // Вопросы кибербезопасности. 2013. № 2. С. 29-33.
26. Петухов А.А. Использование XSS для организации ботнетов нового поколения // Защита информации. Инсайд. 2010. № 4 (34). С. 50-53.
27. Barabanov A.V., Lavrov A.I., Markov A.S., Polotnyanschikov I.A., Tsirlov V.L. The study into cross-site request forgery attacks within the framework of analysis of software vulnerabilities. Trudy ISP RAN/Proc. ISP RAS, vol. 29, issue 5, 2017, pp. 7-18 DOI: 10.15514/ISPRAS-2017-29(5)-1.
28. Уточка Р.А., Фадин А.А., Шахалов И.Ю. Проблемные вопросы гарантированного уничтожения информации на носителях с полупроводниковой энергонезависимой перезаписываемой памятью. // Вестник Московского государственного технического университета им. Н.Э. Баумана. Серия: Приборостроение. 2011. № SPEC. С. 7-19.

29. Хлопов Б.В., Митягин А.Ю., Фесенко М.В. Исследование возможности применения косвенного метода контроля для оценки качества экстренного уничтожения информации с полупроводниковых носителей на основе микросхем с энергозависимой памятью (флеш-памятью) // Известия Института инженерной физики. 2014. Т. 2. № 32. С. 11-18.

Миссия университета – генерация передовых знаний, внедрение инновационных разработок и подготовка элитных кадров, способных действовать в условиях быстро меняющегося мира и обеспечивать опережающее развитие науки, технологий и других областей для содействия решению актуальных задач.

НАПРАВЛЕНИЕ ПОДГОТОВКИ (СПЕЦИАЛЬНОСТИ) 10.03.01 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Направление подготовки (специальности) 10.03.01 «Информационная безопасность» реализуется как профессиональная образовательная программа высшего образования бакалавриата в Университете ИТМО. Кафедра проектирования и безопасности компьютерных систем осуществляла подготовку бакалавров в области информационной безопасности компьютерных систем по данному направлению подготовки.

ИСТОРИЯ РЕАЛИЗАЦИИ НАПРАВЛЕНИЯ

1945-1966 РЛПУ (кафедра радиолокационных приборов и устройств). Решением Советского правительства в августе 1945 г. в ЛИТМО был открыт факультет электроприборостроения. Приказом по институту от 17 сентября 1945 г. на этом факультете была организована кафедра радиолокационных приборов и устройств, которая стала готовить инженеров, специализирующихся в новых направлениях радиоэлектронной техники, таких как радиолокация, радиоуправление, теленаведение и др. Организатором и первым заведующим кафедрой был д.т.н., профессор С.И. Зилитинкевич (до 1951 г.). Выпускникам кафедры присваивалась квалификация инженер-радиомеханик, а с 1956 г. – радиоинженер (специальность 0705).

В разные годы кафедрой заведовали доцент Б.С. Мишин, доцент И.П. Захаров, доцент А.Н. Иванов.

1966–1970 КиПРЭА (кафедра конструирования и производства радиоэлектронной аппаратуры). Каждый учебный план специальности 0705 коренным образом отличался от предыдущих планов радиотехнической специальности своей четко выраженной конструкторско-технологической

направленностью. Оканчивающим институт по этой специальности присваивалась квалификация инженер-конструктор-технолог РЭА.

Заведовал кафедрой доцент А.Н. Иванов.

1970–1988 КиПЭВА (кафедра конструирования и производства электронной вычислительной аппаратуры). Бурное развитие электронной вычислительной техники и внедрение ее во все отрасли народного хозяйства потребовали от отечественной радиоэлектронной промышленности решения новых ответственных задач. Кафедра стала готовить инженеров по специальности 0648. Подготовка проводилась по двум направлениям – автоматизация конструирования ЭВА и технология микроэлектронных устройств ЭВА.

Заведовали кафедрой: д.т.н., проф. В.В. Новиков (до 1976 г.), затем проф. Г.А. Петухов.

1988–1997 МАП (кафедра микроэлектроники и автоматизации проектирования). Кафедра выпускала инженеров-конструкторов-технологов по микроэлектронике и автоматизации проектирования вычислительных средств (специальность 2205). Выпускники этой кафедры имеют хорошую технологическую подготовку и успешно работают как в производстве полупроводниковых интегральных микросхем, так и при их проектировании, используя современные методы автоматизации проектирования. Инженеры специальности 2205 требуются микроэлектронной промышленности и предприятиям-разработчикам вычислительных систем.

Кафедрой с 1988 г. по 1992 г. руководил проф. С.А. Арустамов, затем снова проф. Г.А. Петухов.

С 1996 г. кафедрой заведует д.т.н., профессор Ю.А. Гатчин.

1997–2011 ПКС (кафедра проектирования компьютерных систем). Кафедра выпускала инженеров по специальности 210202 «Проектирование и технология электронно-вычислительных средств». Область профессиональной деятельности выпускников включала в себя проектирование, конструирование и технологию электронных средств, отвечающих целям их функционирования, требованиям надежности, дизайна и условиям эксплуатации. Кроме того, кафедра готовила специалистов по защите информации, специальность 090104 «Комплексная защита объектов информатизации». Объектами профессиональной деятельности специалиста по защите информации являются методы, средства и системы обеспечения защиты информации на объектах информатизации.

В 2009 и 2010 годах кафедра заняла второе, а в 2011 году – почетное первое место в конкурсе среди кафедр университета.

С **2011 года ПБКС** (кафедра проектирования и безопасности компьютерных систем). Кафедра осуществляет подготовку бакалавров и магистров по направлениям 090900 «Информационная безопасность» (с 2013 г. коды направления: для бакалавров 10.03.01, для магистров 10.04.01) и 211000 «Конструирование и технология электронных средств» (с 2013 г. коды направления: для бакалавров 11.03.03, для магистров 11.04.03), а также продолжает подготовку инженеров по специальностям 090104 и 210202.

С 2017 года кафедрой заведовал к.т.н., доцент Д.А. Заколдаев.

За время своего существования кафедра выпустила более 4750 инженеров, специалистов, бакалавров и магистров. На кафедре защищено 100 кандидатских и 16 докторских диссертаций.

В связи с реорганизацией структуры мегафакультета компьютерных технологий и управления, факультета безопасности информационных технологий, одним из подразделений которых являлась кафедра ПБКС, осуществление руководства направлением подготовки (специальности) 10.03.01 «Информационная безопасность» возложено на отдел «дирекция образовательных программ факультета безопасности информационных технологий».