Л39. Инструменты социальной инженерии (Social Engineering Toolkit, SET) в Kali Linux. Развертывание Eve-ng.

Социальная инженерия означает использование человеческих слабостей для получения ценной информации. Это жизненно важное для испытателя на проникновение искусство обмана, которое применяется при отсутствии или недостатке информации о цели. Люди — наиболее слабое звено в обеспечении безопасности любой организации. Мы существа общественные, поэтому сама природа делает нас уязвимыми для психологических атак. Социальные инженеры используют эти атаки для получения конфиденциальной информации или доступа в ограниченные зоны. Направления атак социального инженера могут быть абсолютно различными. Каждое из этих направлений ограничивается только воображением индивида, основанном на его влиянии и результате, который требуется получить. В этой главе мы обсудим основные принципы и действия, которые применяют профессиональные социальные инженеры для манипулирования людьми, чтобы получить нужную им информацию или выполнить определенные действия.

В этой главе мы рассмотрим следующие темы.

- Основные психологические принципы, формулирующие цели и видение социального инженера.
- Общий процесс психологической атаки и методы социальной инженерии с примерами из реального мира.

С точки зрения безопасности социальная инженерия — это мощное оружие, которое используется для манипулирования людьми, чтобы достичь желаемой цели. Во многих организациях социальная инженерия может быть применена как для обеспечения безопасности сотрудников, так и для получения знаний о человеческих слабостях. Обратите внимание, что методы социальной инженерии очень распространены и применяются многими людьми, например испытателями на проникновение, мошенниками, ворами, деловыми партнерами, вербовщиками, продавцами, информационными брокерами, шпионами, недовольными сотрудниками и даже детьми. Разница лишь в причинах, из-за которых люди идут на обман, а социальные инженеры применяют против цели свои знания.

Технические условия

Для этой главы вам потребуется последняя версия Kali Linux.

Моделирование психологии человека

Психологические возможности человека зависят от того, как он воспринимает реальность. А реальность воспринимается посредством зрения, слуха, обоняния, осязания, а также благодаря влияющим на человека внешним силам. С помощью этих систем органов чувств и внешних сил мы и воспринимаем внешний мир.

С точки зрения социальной инженерии мы можем получить дополнительную информацию об интересующем нас человеке, наблюдая за ним в ходе личного общения или со стороны. Нам нужно наблюдать за его мимикой в неожиданных для него ситуациях, например следить, как он отреагирует на вопросы или утверждения, которых он не ожидал (движение глаз и частота моргания), отмечать его эмоции (удивление, счастье, страх, печаль, гнев или отвращение), анализировать логические нестыковки или словесные расхождения, а также его поведение. Часто для получения конфиденциальной информации или доступа в зоны ограниченного доступа социальному инженеру необходимо напрямую войти в контакт с объектом. Это может быть как личное общение, так и общение средствами электронной коммуникации.

В реальном мире для выполнения данной задачи применяются две общие тактики: собеседование и опрос. Однако на практике на каждую тактику влияют такие факторы, как окружающая среда, знание цели и способность контролировать среду общения. Эти совокупные факторы (коммуникация, окружающая среда, знания и рамки, ограничивающие социального инженера) формируют базовый набор навыков эффективного социального инженера, требуемых для проведения атаки. Вся деятельность в области социальной инженерии основана на доверительных отношениях. Если вы не можете наладить прочные доверительные отношения с целевым объектом, то, скорее всего, потерпите неудачу.

Современная социальная инженерия — это почти наука. Обязательно посетите сайт создателей структуры социальной инженерии (http://www.social-engineer.org/). Материалы опубликовал Кристофер Хаднаги (Christopher Hadnagy), управляющий этим сайтом. С помощью предоставленной им информации мы можем рассказать нашим пользователям и клиентам о методах проведения разных психологических атак.

Процесс атаки

Далее описаны основные шаги, необходимые для начала психологической атаки на вашу цель. Показанный здесь метод далеко не единственный и не самый успешный. Но, узнав о нем, вы получите представление о социальной инженерии.

Сбор разведданных, выявление уязвимых точек, планирование и выполнение атаки — это основные шаги, предпринимаемые социальными инженерами для успешного получения нужной информации или доступа в запретную зону.

- **Сбор разведданных.** Существует множество методов, с помощью которых определяется наиболее привлекательный для испытателя на проникновение объект. Это можно сделать, собрав корпоративные адреса электронной почты (использовав инструмент расширенного поиска). Хорошие результаты можно получить, собрав персональную информацию о людях, работающих в самой целевой организации (в том числе через социальные сети). Дополнительную информацию вам даст выявление сторонних программных пакетов, используемых в целевой организации. Не помешает и участие в корпоративных бизнес-мероприятиях и вечеринках, а также в конференциях. Это позволит выявить наиболее подходящий источник информации.
- **Выявление уязвимых точек.** После того как ключевой источник информации определен, следует двигаться дальше, а именно установить доверительные отношения. Это нужно, чтобы в целевой организации не узнали о ваших попытках получения корпоративной информации. В течение всего процесса очень важно поддерживать высокий уровень скрытности. При поиске информации желательно получить сведения о применяемом устаревшем программном обеспечении, которое может быть использовано для доставки вредоносного контента по электронной почте или через Интернет, что, в свою очередь, позволит заразить компьютер доверенной стороны.
- **Планирование атаки.** Как организовать атаку на интересующий вас объект — выбирать вам. Вы можете пойти на личное общение с целевым объектом, а можете избрать пассивный метод, с применением электронных средств. Основываясь на выявленных уязвимых точках входа, можно легко определить путь и метод атаки. Скажем, найти дружелюбного представителя службы поддержки клиентов, например Боба, который, не сознавая того, что может принести вред организации, без согласования с высшим руководством будет запускать полученные по электронной почте вредоносные файлы.
- **Исполнение.** Для заключительного этапа вам понадобятся решительность и терпение, которые позволят вам контролировать ход атаки и оценить полученные результаты. На этом этапе социальным инженерам потребуются достаточное количество информации и доступ к собственности объекта, что, в свою очередь, даст им возможность в дальнейшем проникнуть в корпоративные активы. При успешном выполнении этой задачи процесс эксплуатации и приобретения будет завершен.

Методы атаки

Существует шесть методов, которые вы можете применить к объекту. Они помогут вам в общении и подготовке объекта к заключительной операции. Методы классифицированы и описаны в соответствии с их уникальным представлением в области

социальной инженерии. Мы также включили несколько примеров, чтобы показать вам реальный сценарий применения каждого из выбранных методов. Помните, что основу этих методов атаки составляют психологические факторы. Чтобы методы стали более эффективными, их необходимо регулярно совершенствовать.

Подражание

Чтобы завоевать доверие заинтересовавшего объекта, злоумышленники будут притворяться, подстраиваясь под интересы целевого объекта. Например, чтобы получить конфиденциальные данные, такие как логин и пароль, данные лицевых счетов и банковских карт, используют фишинг (один из видов интернет-мошенничества, когда применяются массовые рассылки от имени популярных компаний или организаций, содержащих ссылки на ложные сайты, внешне неотличимые от настоящих). Чтобы реализовать этот метод, злоумышленник сначала собирает адреса электронной почты целевого объекта, а затем подготавливает мошенническую страницу, которая выглядит и функционирует точно так же, как и настоящий сайт.

После того как злоумышленник подготовит все необходимое, он отправляет официальное электронное письмо (например, касательно данных об учетной записи), которое якобы находится на сайте исходного банка. Для подтверждения этой информации в письме содержится просьба перейти по ссылке, что, в свою очередь, предоставит злоумышленнику актуальную банковскую информацию. Обладая хорошими навыками работы с веб-технологиями и используя передовые инструменты (например, SSLstrip), социальный инженер может легко и эффективно автоматизировать эту задачу. Если вы собираетесь лично встретиться с целевым объектом, можете представиться ему работником банка.

Взаимный обмен

Акт обмена услугами для получения обоюдной выгоды известен как взаимный обмен. Этот метод в социальной инженерии может включать случайные и долгосрочные деловые отношения. На основании доверительных отношений один из партнеров для получения необходимой информации должен предоставить другому что-то взамен. Например, Боб является профессиональным хакером и хочет знать о политике физической безопасности в офисном здании компании ABC. Тщательно изучив вопрос, он решает разработать сайт по продаже антиквариата по сниженным ценам. Боб знает, что этот сайт привлечет к себе внимание двух сотрудников, работающих в этом офисе.

Мы предполагаем, что Боб уже ознакомился с личной информацией этих сотрудников, включая адреса электронной почты, посещаемые ими интернет-форумы и социальные сети и т. д. Алиса, будучи одним из этих сотрудников, начинает регулярно покупать вещи, предлагаемые поддельным сайтом, и становится для Боба главной целью. И настает момент, когда Боб может предложить уникальную антикварную вещь в обмен на необходимую ему информацию. Воспользовавшись человеческой слабостью, а именно увлечением Алисы антикварными вещами, он

пишет ей письмо и просит в обмен на уникальную антикварную вещь разузнать детали политики физической безопасности компании ABC. Поддавшись искушению и позабыв про нормы корпоративной этики, она выдает нужную информацию Бобу. Это доказывает, что в достижении своей цели социальному инженеру может помочь создание искусственной, фальшивой ситуации: когда злоумышленник использует увлечение сотрудника для получения конфиденциальной информации.

Влияние авторитета

Метод атаки, когда человек манипулирует функциональными обязанностями объекта, известен как *атака авторитетом*. Такой вид психологической атаки иногда является частью метода перевоплощения. В большинстве своем, выполняя рутинную работу, люди действуют автоматически. И, когда появляется новая инструкция, отправленная якобы от имени высшего руководства, человек, инстинктивно понимая пагубность своих действий, но находясь под влиянием авторитета, все равно выполняет полученные указания. Это делает нас всех уязвимыми перед определенными угрозами.

Представим себе, что кто-то для получения данных об аутентификации выбрал в качестве объекта сетевого администратора компании XYZ. Чтобы осуществить задуманное, злоумышленник, используя метод взаимного обмена, получает телефонные номера администратора и генерального директора компании. Далее, с помощью сервиса подмены вызовов (например, www.spoofcard.com) злоумышленник звонит сетевому администратору. Сетевой администратор видит, что звонок поступил от генерального директора, и считает его приоритетным. Под влиянием авторитета генерального директора (ведь работник считает, что общается именно с ним) сетевой администратор выдает секретную информацию.

Использование жадности

Один из самых больших человеческих пороков — жадность. Метод использования этой не очень хорошей черты характера описывает способ получения нужной информации. Знаменитая *нигерийская афера 419* (www.419eater.com) является типичным примером того, как можно воспользоваться человеческой жадностью. Рассмотрим такую ситуацию: Боб планирует собирать личную информацию от студентов университета XYZ. Мы предполагаем, что у него уже есть адреса электронной почты всех интересующих его студентов. Далее он разрабатывает сообщение, в котором всем студентам университета XYZ предлагаются ваучеры с радикальными скидками на iPod, и передает его по электронной почте. Но за это студентам нужно сообщить Бобу свою личную информацию (имя, адрес, телефон, дату рождения, номер паспорта и т. д.). Поскольку возможность бесплатно получить последнюю модель iPod для целевых студентов была тщательно просчитана, многие из них могут попасться на эту аферу. В корпоративном мире такой метод атаки может быть расширен для максимизации коммерческой выгоды и достижения бизнес-целей.

Налаживание социальных взаимоотношений

Всем нам необходима определенная форма социальных отношений, чтобы мы смогли поделиться с кем-то своими мыслями, чувствами и идеями. Наиболее уязвимой частью любой социальной связи является сексуальность. Во многих случаях мужчины и женщины привлекают друг друга. Благодаря этому сильному чувству и ложному чувству доверия мы непреднамеренно можем раскрыть секретную информацию. Есть несколько социальных онлайн-порталов, где люди могут пообщаться. К таким ресурсам относятся Facebook, MySpace, Twitter и Orkut.

Допустим, компания XYZ наняла Боба, чтобы тот для достижения устойчивого конкурентного преимущества разузнал о финансовой и маркетинговой стратегии компании ABC. Боб просматривает список сотрудников и находит девушку по имени Алиса, которая отвечает за все деловые операции. Притворяясь обычным выпускником, он пытается наладить с ней отношения (например, через Facebook). Боб намеренно создает ситуации, где он может столкнуться с Алисой. Например, в танцевальном клубе или на музыкальном фестивале. Когда он войдет в доверие, он начнет регулярно встречаться с Алисой. Эта практика позволит ему получать полезные сведения о финансовых и маркетинговых перспективах компании ABC.

Помните: чем лучше отношения, тем больше доверие и, следовательно, больше информации поступает от источника. В следующем разделе мы расскажем о некоторых инструментах, например SET, облегчающих эту задачу.

Сила любопытства

Есть старая поговорка: любопытной Варваре на базаре нос оторвали. Это предостережение людям, что иногда наше собственное любопытство берет над нами верх. На работе есть много интересной информации, с которой нам тоже хотелось бы ознакомиться. Например, нам интересно, сколько получает генеральный директор, кто получит повышение, а кого уволят. В результате социальные инженеры могут использовать это естественное любопытство против нас. Нас могут соблазнить ссылкой в электронной почте, якобы ведущей к сайту со сплетнями о знаменитостях. Мы можем «купиться» на документ, в теле которого есть вредоносный код, в свою очередь ставящий под угрозу нашу систему. Испытатели на проникновение могут использовать наше любопытство для организации серии различных атак.

Инструменты социальной инженерии

Инструменты социальной инженерии (Social Engineering Toolkit, SET) — это многофункциональный современный и простой в использовании набор инструментов. SET создан учредителями компании TrustedSec (https://www.trustedsec.com/). Он поможет вам подобрать наиболее эффективный способ использования уязвимостей клиентского приложения и попробовать захватить конфиденциальную информацию цели (например, пароли электронной почты). Наиболее действенный метод атаки — рассылка фишинговых писем с вредоносным вложением.

Очень эффективны Java-апплеты, встроенные в файл, который, в свою очередь, сохраняется на переносном носителе (USB или DVD/CD). Комбинируя методы атаки, вы получите мощную платформу для использования и выбора наиболее убедительной техники.

Для запуска SET выберите в основном меню пункты Applications ▸ Exploitation Tools ▸ Social Engineering Toolkit (Приложения ▸ Инструменты эксплуатации ▸ Инструменты социальной инженерии) или введите в командной строке терминала команду:

```
root@kali:~# setoolkit
```

SET будет запущен, и в терминале появятся его логотип, информация и параметры, которые можно применить при запуске нужных инструментов (рис. 7.1).

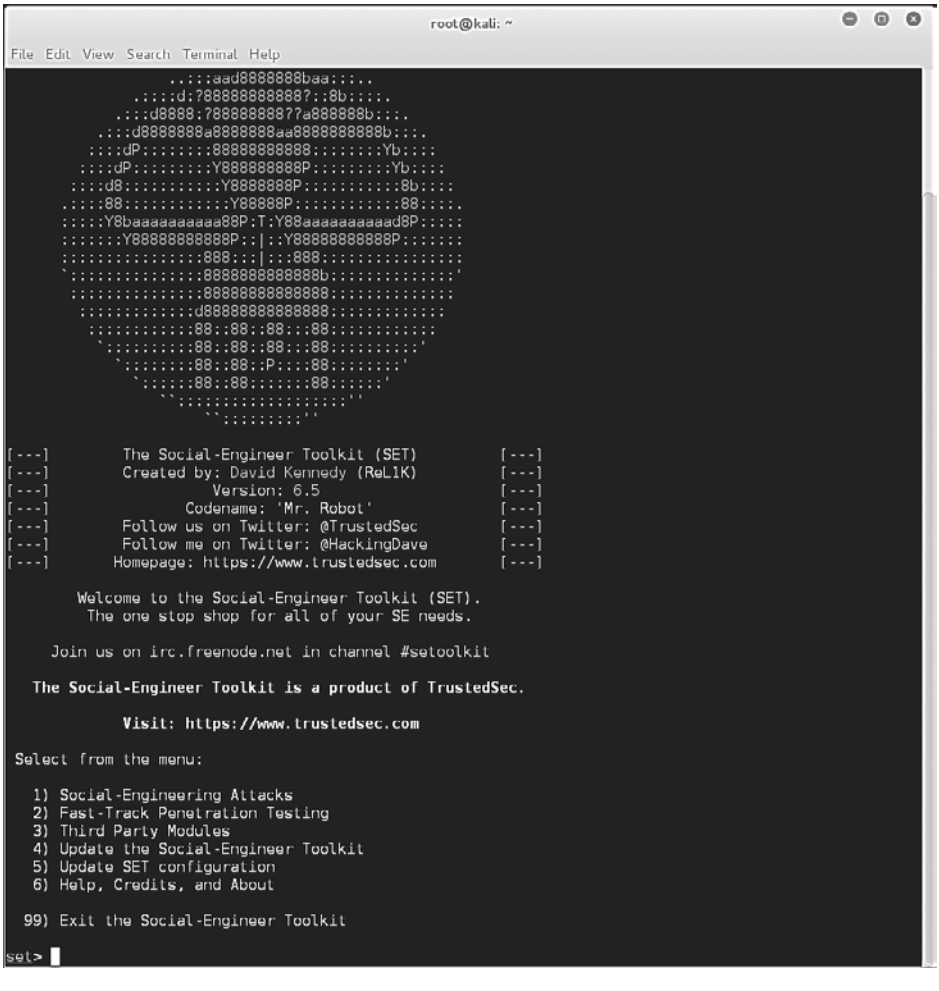

Рис. 7.1. SET запущен

Чтобы совершить обратный вызов из целевой системы, мы в нашем тестовом упражнении воспользуемся любопытством сотрудников целевой организации. Для этого мы с помощью инструментов социальной инженерии создадим исполняемый файл и запишем его на USB-устройство (флешку). Затем мы эту флешку оставим где-то в организации (якобы забудем или потеряем). Скорее всего, кто-то из сотрудников, обнаружив эту флешку, захочет узнать, что на ней, и подключит ее к компьютеру на своем рабочем месте.

Не используйте функции обновления пакетов в Kali Linux. Лучше как можно чаще обновляйте саму Kali, чтобы применить к приложениям все последние поддерживаемые обновления.

Анонимная USB-атака

Для такой атаки мы создадим исполняемый файл, который будет отвечать за обратную связь между целевой машиной и нашим тестовым компьютером. Чтобы доставить этот исполняемый файл на целевую машину, поместим его на USB-устройство и дадим ему название, которое заинтересует пользователя этой машины.

После того как исполняемый файл будет создан и сохранен на флешке, мы оставим USB-устройство в общественном месте в целевой организации и будем ждать результата.

Для получения дополнительной информации посетите раздел, посвященный SET, расположенный по адресу http://www.social-engineer.org/framework/general-discussion/.

Для осуществления USB-атаки выполните следующие шаги.

1. Выберите из списка основных задач пункт 1) Social Engineering Attacks (Атаки социальной инженерии). Для этого введите в командную строку номер этого пункта, в нашем случае 1, и нажмите клавишу Enter (рис. 7.2).

Рис. 7.2. Начало USB-атаки

2. Для создания исполняемого файла выберите пункт 3) Infectious Media Generator (Генератор инфекционных сред) (рис. 7.3).

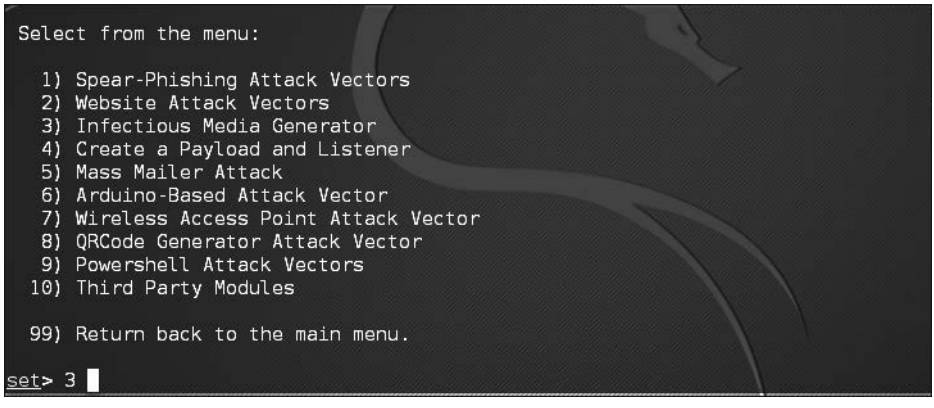

Рис. 7.3. Создаем исполняемый файл

3. Генератор инфекционных носителей предложит тип эксплойта. Для наших целей мы воспользуемся исполняемым файлом Metasploit. Для этого нужно выбрать пункт 2) Standard Metasploit Executable (Стандартный исполняемый файл Metasploit) (рис. 7.4).

Рис. 7.4. Выбираем стандартный исполняемый файл Metasploit

4. Разработано несколько полезных нагрузок, которые мы можем использовать. Например, нагрузка Windows Meterpreter Reverse HTTPS окажется полезна в корпоративной настройке, потому что организации часто разрешают общие подключения HTTPS к Интернету. Для наших целей мы будем использовать простое обратное TCP-соединение. Добавьте полезную нагрузку для обратного соединения TCP, выбрав пункт 2) Windows Reverse_TCP Meterpreter (Windows обратный TCP Meterpreter) (рис. 7.5).

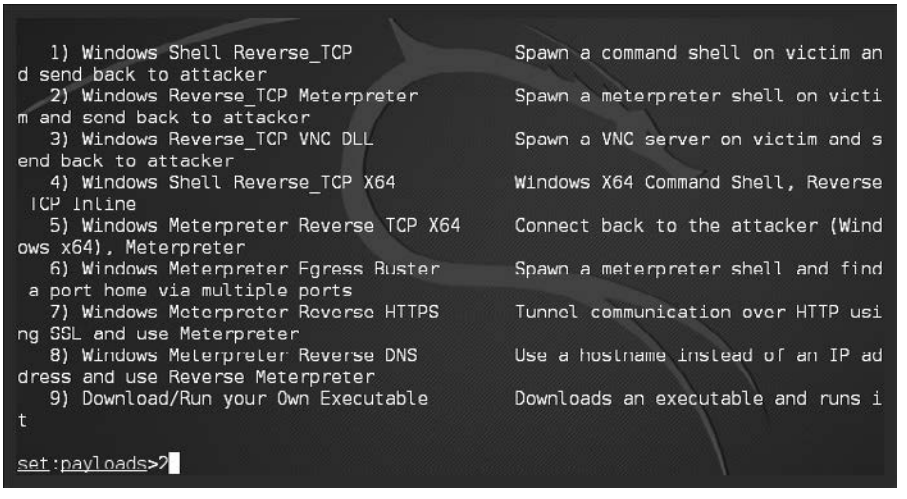

Рис. 7.5. Выбираем полезную нагрузку

5. Нам нужно установить прослушиватель полезной нагрузки. В нашей ситуации им будет IP-адрес тестовой машины (172.16.122.185). В некоторых случаях вы можете использовать центральный сервер с установленной Kali Linux и проводить атаку, задействуя несколько USB-устройств, на которых прослушивателем полезной нагрузки будет IP-адрес тестовой машины. Выберите для обратного порта прослушивателя порт 4444 и нажмите клавишу Enter. Вам будет предложено создать прослушиватель. Для его создания введите `yes`. Будет запущен прослушиватель Meterpreter (рис. 7.6).

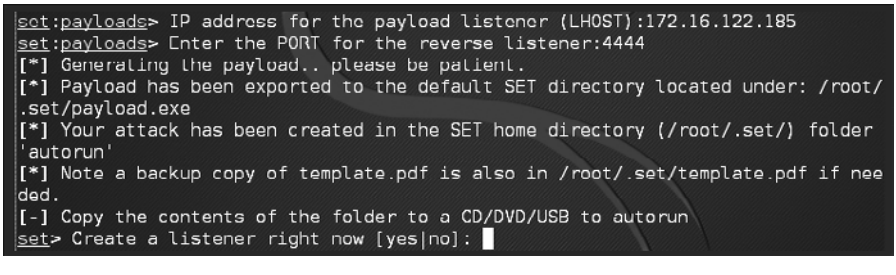

Рис. 7.6. Создание прослушивателя Meterpreter

6. Чтобы увидеть исполняемый файл, перейдите в папку `/root/.set` (рис. 7.7).

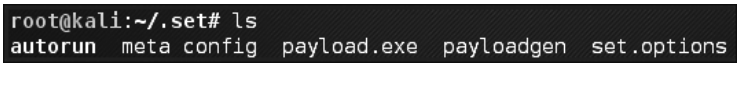

Рис. 7.7. Исполняемый файл в списке файлов папки /root/.set

7. Просто скопируйте файл `payload.exe` на Рабочий стол. После этого вы можете загрузить его на USB-устройство. Но нам нужно провернуть еще один трюк: дать этому файлу такое имя, которое заинтересует целевой объект, например `Executive Bonus` (Исполнительный бонус). Такое переименование полезно, если на целевой машине на USB-портах отключена функция автозапуска. Когда USB-устройство подготовлено, «потеряйте» его в общественном месте целевого предприятия или на автостоянке.
8. Ничего не подозревающий целевой объект находит «потерянное» USB-устройство и подключает его к своему компьютеру. На этом этапе исполняемый файл запускается и мы видим открытую на тестовой машине оболочку Meterpreter (рис. 7.8).

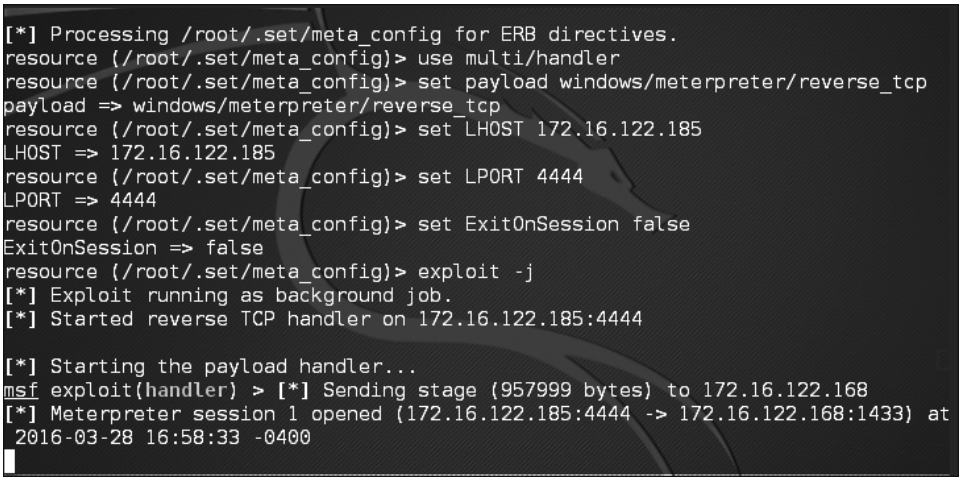

Рис. 7.8. Оболочка Meterpreter открыта на тестовой машине

Используйте эту атаку, если она предусмотрена договором между вами и клиентом и ваш клиент понимает, что вы будете делать. Такая атака также требует доступа к физическому расположению целевой организации или машины. Есть варианты, когда можно отправить файл полезной нагрузки по электронной почте или с помощью другого сервиса обмена сообщениями.

Набор инструментов постоянно обновляется его создателями и в любой момент может быть радикально изменен. Мы только слегка раскрыли возможности SET. Если вы желаете продолжить изучение этого грозного набора инструментов, посетите сайт, расположенный по адресу https://www.trustedsec.com/downloads/social-engineer-toolkit/. Начните с просмотра представленных на этом сайте видеоматериалов.

Сбор учетных данных

В этой атаке мы создадим поддельную копию известного сайта. Наша копия, однако, позволит нам захватить учетные данные пользователя. Чтобы человек мог посетить наш сайт, потребуется отправить ссылку на него по электронной почте с заголовком или темой, которая заинтересует пользователя. Ему будет предложено войти в систему, и все — учетные данные будут захвачены.

1. Введите команду `setoolkit`, а затем, находясь в главном меню, введите `1`, чтобы перейти к меню социальной инженерии.
2. Чтобы выбрать 2) Website Attack Vectors (Векторы атаки на сайт), введите в командной строке `2` (рис. 7.9).

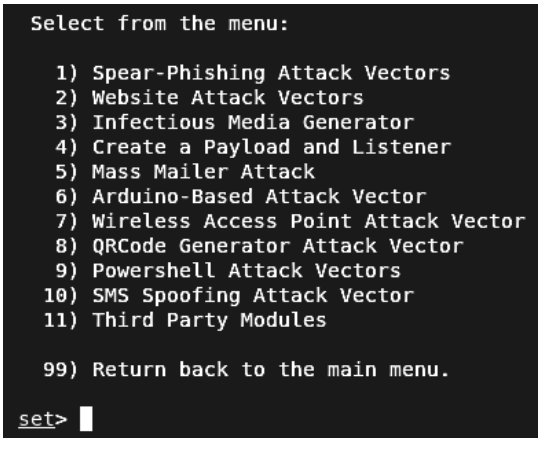

Рис. 7.9. Выбираем направление атаки на сайт

3. Для сбора учетных данных введите в командную строку `3` (рис. 7.10).

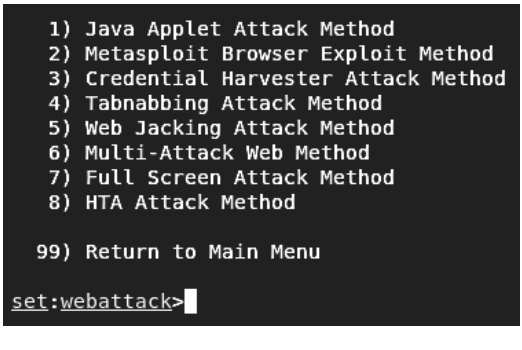

Рис. 7.10. Выбираем Metasploit Browser Exploit Method

На данный момент мы успешно загрузили модуль Credential Harvester. В нем у нас есть три варианта действий: использование веб-шаблонов, клонирование сайта или пользовательский импорт. Для нашего сценария мы выберем вариант 2) Site Cloner (Клонирование сайта) (рис. 7.11).

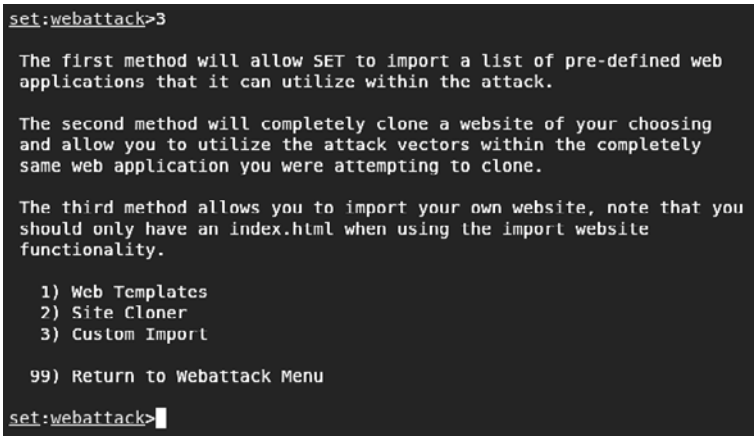

Рис. 7.11. Выбираем вариант клонирования сайта

В первую очередь нам нужно ввести IP-адрес, по которому будет размещен сайт, то есть адрес хоста, где вы сейчас находитесь. Вы можете подтвердить свой IP, введя в другом терминале `ifconfig`, и этот адрес автоматически должен появиться в командной строке (рис. 7.12).

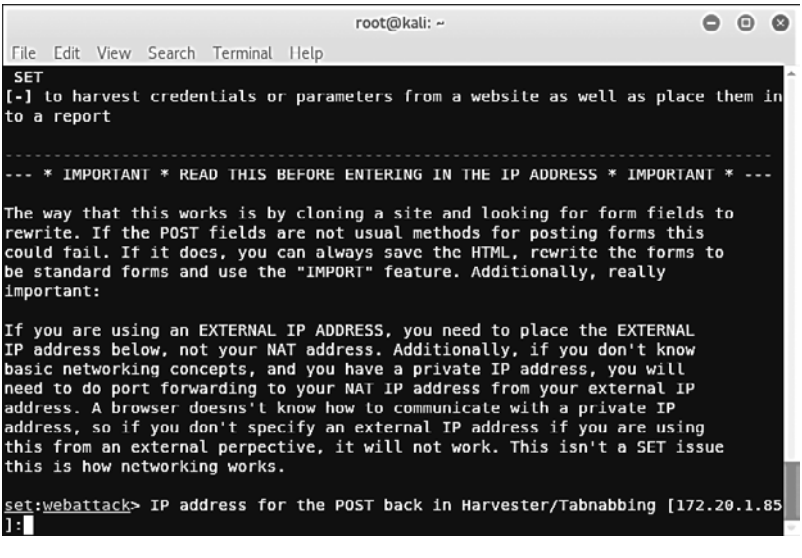

Рис. 7.12. IP-адрес тестовой машины в командной строке

IP-адрес нашей тестовой машины — 172.20.1.85. IP-адрес вашей тестовой машины будет другим. После того как IP будет введен, необходимо указать адрес сайта, который вы хотите клонировать. Мы выбрали https://www.facebook.com (рис. 7.13).

```
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://www.facebook.com

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] You may need to copy /var/www/* into /var/www/html depending on where your d
irectory structure is.
Press {return} if you understand what we're saying here.
```

Рис. 7.13. Адрес клонируемого сайта

Клонирование сайта займет некоторое время. Когда этот процесс завершится, вы увидите сообщение с просьбой изучить структуру каталогов веб-сервера. В Kali Linux структура по умолчанию — `/var/www/`. Чтобы запустить веб-сервер, нажмите клавишу Enter.

Чтобы подтвердить работу клонированного сайта, мы выполнили тест в браузере в KALI, перешли по адресу 127.0.0.1 и своему сетевому IP 172.20.1.85 и подтвердили, что сайт загружен (рис. 7.14).

Как видно из скриншота, SET сообщил о двух тестах, которые мы провели, чтобы подтвердить доступность сайта.

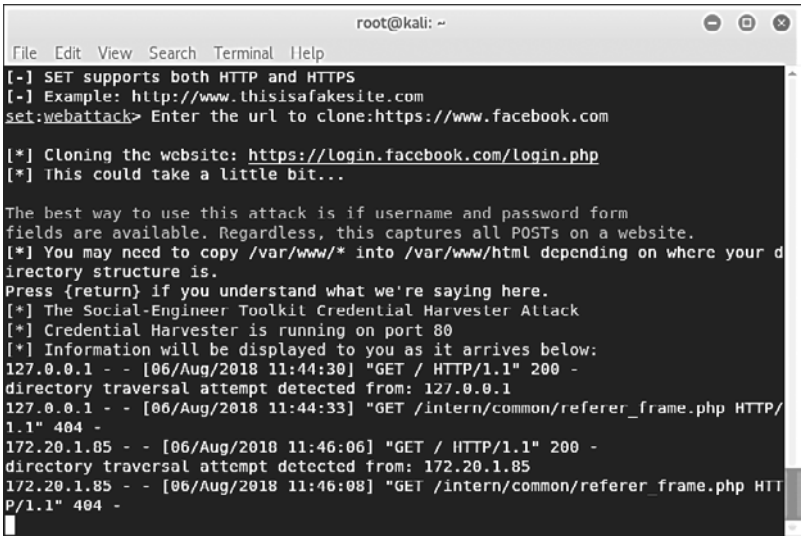

Рис. 7.14. Подтверждение загрузки сайта

На данный момент мы успешно настроили нашу платформу взаимодействия, с которой создадим поддельное электронное письмо со ссылкой на нашу систему и отправим эту ссылку на почтовый ящик нашей жертвы. Вашим основным источником будут результаты проведенной ранее разведки. Письмо должно выглядеть так, как будто его отправил человек, хорошо знакомый с целевым объектом. Кроме того, чтобы целевой объект ничего не заподозрил, нужно сохранить стилистику и подписи этого корреспондента.

Многие люди отвечают на электронные письма с мобильных телефонов, и обычно подписи в письмах, отправленных с мобильного, значительно отличаются от таких же подписей в письмах с ноутбука. Например, когда письмо отправлено с ноутбука, в подписи сотрудника компании на ноутбуке указано его полное имя, скажем Джон Уинтер, а при ответе с мобильного телефона написано --J. Вы должны это учитывать.

Вместо того чтобы ориентироваться на нескольких пользователей, у которых есть адрес вашей электронной почты, можно ориентироваться на всех пользователей сети, частью которой вы являетесь. Для этого потребуется выполнить еще несколько шагов и воспользоваться дополнительными инструментами. К этому вопросу мы вернемся в главе 11, при тестировании беспроводного проникновения.

Вредоносный Java-апплет

Здесь мы используем похожую функцию атаки сбора учетных данных, встроив на этот раз пользовательский апплет Java в страницу, запрашивающую у пользователя права на выполнение. После того как пользователь примет приглашение, полезная нагрузка выполнится и целевая машина подключится к нашему компьютеру, обеспечивая тем самым удаленный доступ.

1. Еще раз запустите инструменты социального инженера. Чтобы выбрать соответствующее меню, в командной строке введите 1. Далее, чтобы выбрать Website Attack Vectors, введите 2.
2. Чтобы выбрать вектор атаки 1) Java Applet Attack (Атака Java-апплета), введите в командную строку 1 (рис. 7.15).
3. После загрузки мы остановимся на варианте 2) Site Cloner (Клонирование сайта), как делали это в предыдущем примере.
4. Вас спросят, используете ли вы переадресацию портов или NAT-enabled. Мы в этом примере введем no, поскольку эти функции настраиваются во внутренней среде.
5. Настройте IP-адрес прослушивателя. SET по умолчанию обнаружит ваш IP и автоматически добавит его в соответствующее поле ввода. От вас требуется просто нажать клавишу Enter.

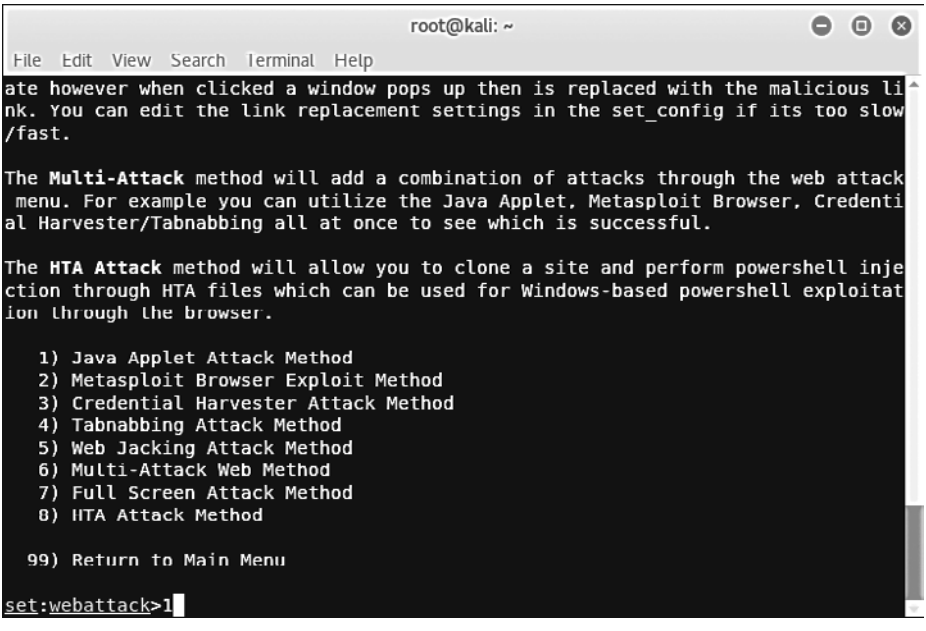

Рис. 7.15. Выбор вектора атаки Java Applet Attack

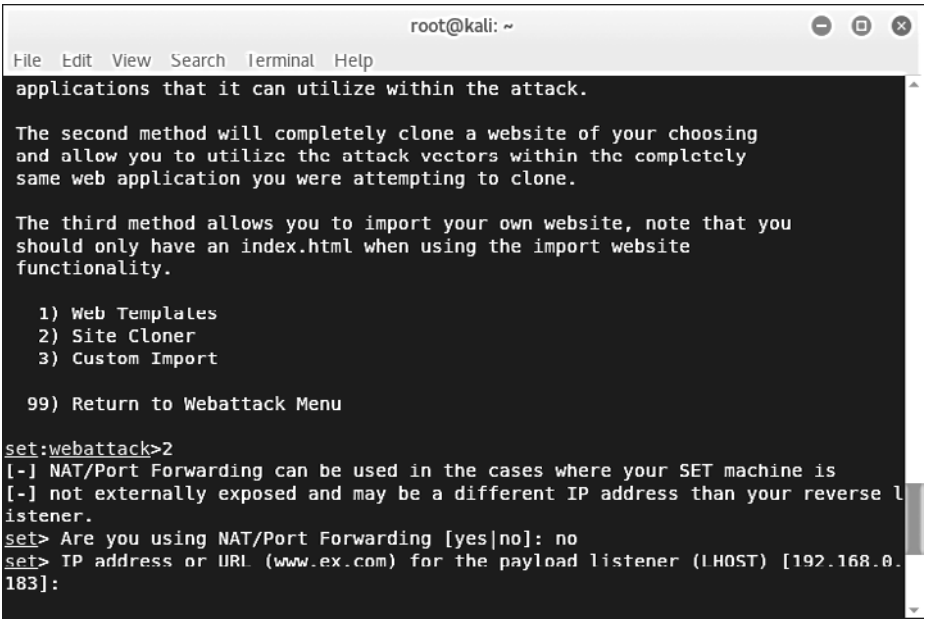

Рис. 7.16. Выбираем вариант 2) Site Cloner (Клонирование сайта)

6. Далее вам будет предложено настроить сам апплет Java, используя один из трех вариантов. Мы выберем встроенную функцию (2), которая поставляется с SET. Если вы знаете, как кодировать на Java, введите 3.

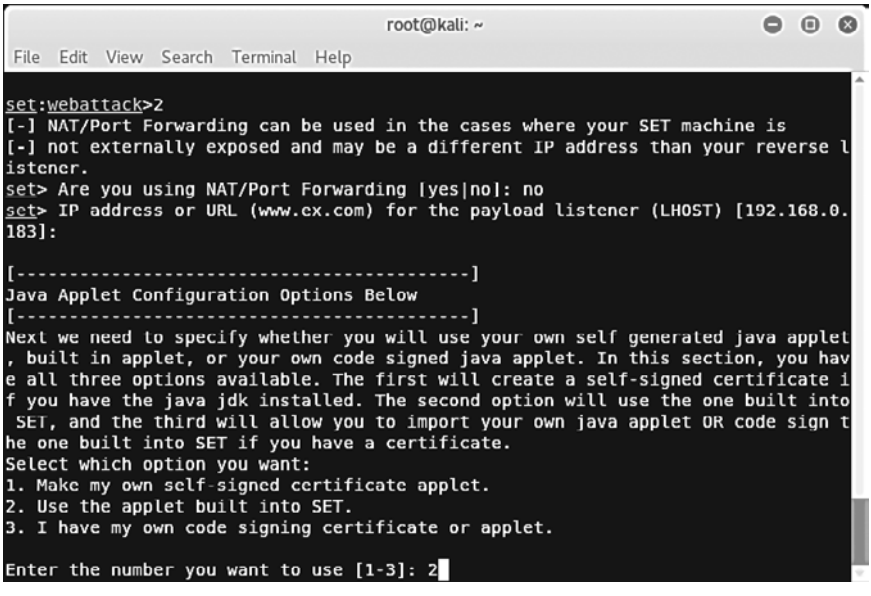

Рис. 7.17. Выбираем нужный вариант настройки апплета

7. После этого SET приступит к созданию апплета. Вам будет предложено ввести IP-адрес целевого сайта для клонирования. Вы наверняка захотите выбрать сайт, которому жертва доверяет и на котором точно примет запрос на запуск Java-апплета. Мы для этого выбрали сайт https://www.chase.com. После клонирования SET автоматически добавит апплет Java (рис. 7.18).

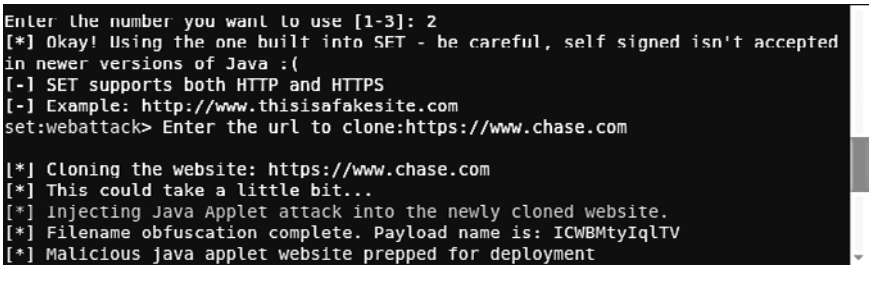

Рис. 7.18. Клонирование сайта с автоматическим добавлением апплета

8. Добавьте в апплет полезную нагрузку. В этом примере мы будем использовать вариант 3 (рис. 7.19).

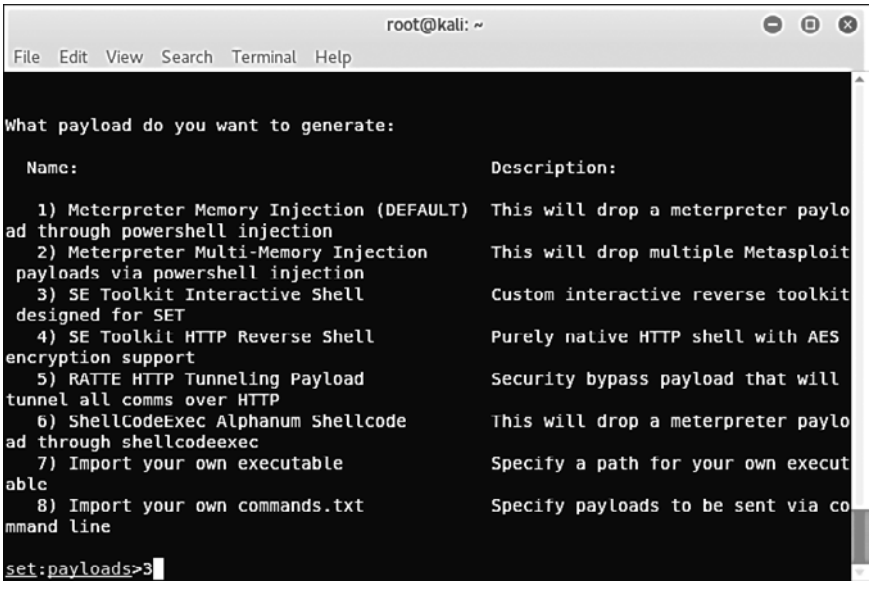

Рис. 7.19. Выбираем полезную нагрузку апплета

9. Теперь осталось выбрать порт прослушивания. Мы оставили порт, предлагаемый по умолчанию, — 443 (рис. 7.20).

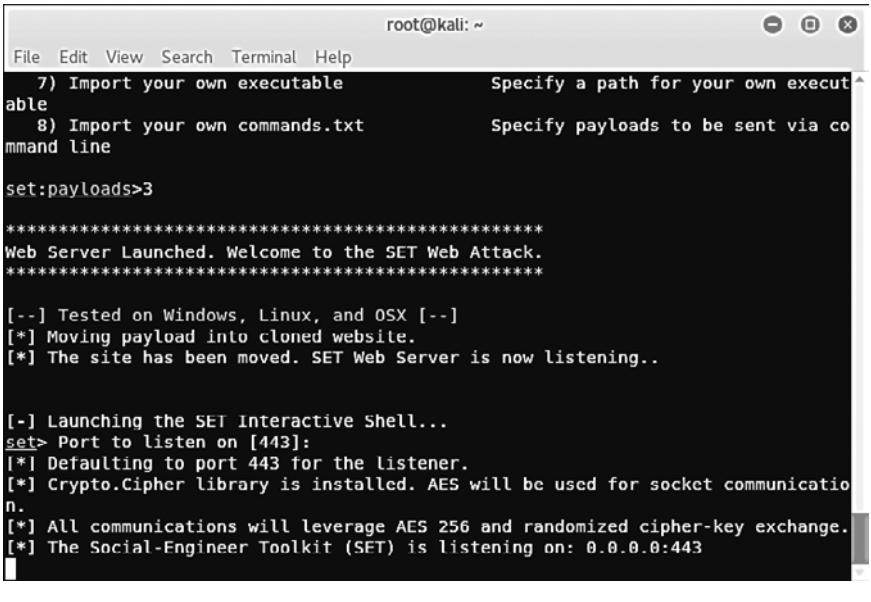

Рис. 7.20. Выбираем порт для прослушивания

Настройка завершена. Подобно credential-harvester, мы можем переслать нашей жертве ссылку по электронной почте. Перед этим следует убедиться, что письмо, в которое встроена ссылка, не вызовет подозрений и жертва щелкнет кнопкой мыши на этой ссылке.