АНАЛИЗ ИНЦИДЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.С. Плешков, Д.Д. Рудер
Алтайский государственный университет, г. Барнаул

В настоящее время возникновение инцидентов информационной безопасности является серьезной проблемой, с которой сталкивается любая организация в процессе обеспечения непрерывности своей деятельности. Эти инциденты затрагивают не только объекты критической информационной инфраструктуры предприятия, но и конфиденциальность всей обрабатываемой в корпоративной сети информации.

Термин «инцидент информационной безопасности» имеет множество вариантов определения, смысл которых почти одинаков. Так согласно «ГОСТ Р ИСО/МЭК ТО 18044-2007» [1], инцидент информационной безопасности – событие, являющееся следствием одного или нескольких нежелательных или неожиданных событий информационной безопасности, имеющих значительную вероятность компрометации бизнес-операции и создания угрозы информационной безопасности.

С понятием «инцидент информационной безопасности» тесно связаны методы «тестирования на проникновение». Под термином «тестирование на проникновение» [2, 3] подразумевается имитация действий реального злоумышленника по реализации несанкционированного проникновения в информационную систему.

Целью работы является изучение и анализ инцидентов информационной безопасности создаваемых методом тестирования на проникновение в компьютерных системах под управлением операционной системы Windows 10 для оценки степени защищенности этих систем от сетевых атак на стороне клиента.

Создание инцидента информационной безопасности происходит в несколько этапов, каждый из которых характеризуется определенной степенью компрометации целевой системы злоумышленником.

На первом этапе необходимо получить несанкционированный доступ к системе-жертве. Для получения несанкционированного доступа осуществляется атака на стороне клиента, которая состоит из следующих этапов:

– Атакующий в программном обеспечении Empire Framework [4] запускает «слушателя» (listener), в котором устанавливает свой внешний ip-адрес и порт, который будет

прослушиваться «слушателем» на предмет входящих соединений. В данной работе используется слушатель типа http.

– После этого атакующий выбирает в качестве полезной нагрузки (stager) генерацию специализированного макроса для документа программного обеспечения Microsoft Word.

– Далее атакующий встраивает макрос в документ формата docm (документ с поддержкой макросов) и заполняет его ценной для потенциальной жертвы информацией.

– После этого атакующий отправляет вредоносный документ пользователю-жертве.

– Используя различные техники социальной инженерии, атакующий заставляет пользователя-жертву запустить вредоносный документ и согласиться на включение макросов для этого документа (по умолчанию запуск макросов отключен).

В итоге после успешного выполнения всех этапов, описанных выше, атакующий получит несанкционированный доступ к системе-жертве с правами скомпрометированного пользователя (рис. 1).

Рис. 1. Получение несанкционированного доступа

Взглянув на рис. 1 можно увидеть, что у атакующего открылась активная сессия на целевой системе с ip-адресом 192.168.77.2. Теперь атакующий может открыть интерактивную сессию для непосредственного взаимодействия с системой, продолжив проникновение и достижение поставленной цели.

Атакующий получил стабильную активную сессию на целевой системе, т.е. если пользователь закроет вредоносный документ, то атакующий не потеряет доступа, т.к. его сессия расположена на стабильном легитимном процессе powershell.exe.

Второй этап включает в себя локальное повышение прав до максимально возможных. После получения несанкционированного

доступа к целевой системе, атакующему необходимо узнать версию операционной системы-жертвы и права доступа, которые он получил в результате осуществления описанной выше атаки.

В статье описана атака на учетную запись пользователя, входящего в локальную группу Администраторы. Для получения административных прав доступа, необходимо обойти службу User Account Control (UAC), которая ограничивает привилегии административной учетной записи до прав учетной записи обычного пользователя, если повышенные привилегии не требуются для работы в системе. Для обхода службы UAC можно воспользоваться скриптом bypassuac_fodhelper. Концепция уязвимости, которую эксплуатирует указанный скрипт, заключается в том, что при выполнении исполняемого файла fodhelper.exe Windows 10 обращается к двум ключам реестра – «HKCU:\Software\Classes\ms-settings\shell\open\command\(default)» и «HKCU:\Software\Classes\ms-settings\shell\open\command\DelegateExecute», которых, по-умолчанию, в реестре системы не существует. Присвоив ключу реестра «HKCU:\Software\Classes\ms-settings\shell\open\command\(default)», в качестве значения определенные пользовательские команды, можно добиться выполнения данных команд в контексте «авто-возвышения» (autoElevate), для которого предупреждения службы UAC не возникают. Контекст «авто-возвышения» пользовательских команд возникает из-за процесса fodhelper.exe, который расположен в надежном месте «C:\Windows\System32», подписан сертификатом компании Microsoft, и как следствие, является доверенным для системы, в результате чего выполнение данного процесса и процессов, порожденных им, происходит в контексте «авто-возвышения» [5]. Результат обхода службы UAC представлен ниже (рис. 2).

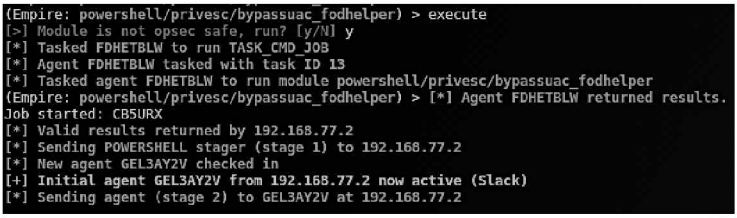

Рис. 2. Получение прав учетной записи администратора

Взглянув на рис. 2 можно увидеть, что в результате выполнения скрипта произошло открытие новой активной сессии, для которой служба UAC отключена. Это можно проверить командой whoami /priv.

Полученные привилегии не являются максимальными в системе. Для дальнейшей эскалации прав необходимо воспользоваться скриптом getsystem с техникой «Token», позволяющей получить привилегии пользователя «Система», за счет кражи токена безопасности системного процесса. В результате выполнения данного скрипта атакующий получает максимальные привилегии в системе (рис. 3).

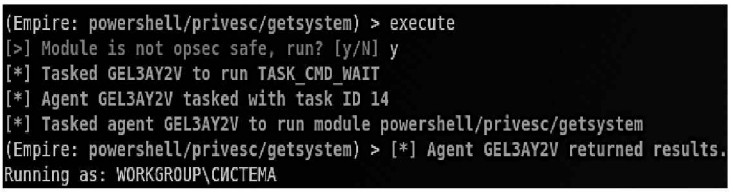

Рис. 3. Максимальные привилегии атакующего

Третий этап включает в себя получение хешей паролей всех локальных учетных записей пользователей целевой системы. После получения максимальных привилегий, атакующий может извлечь имена и хеши паролей всех пользователей из базы данных SAM. В статье рассмотрен скрипт sam из набора mimikatz, отображающий имена и NTLM хеши локальных учетных записей пользователей (рис. 4).

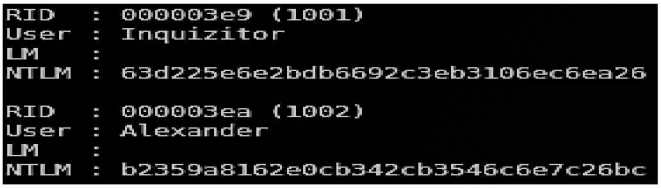

Рис. 4. Получение хешей паролей пользователей

Взглянув на рис. 4 можно увидеть, что скрипт получил хеши паролей пользователей: «Alexander и «Inquizitor». В дальнейшем эти

хеши паролей могут быть расшифрованы или использованы для атаки «Pass the Hash».

По результатам выполненной работы установлено:

– исследование компьютерных систем методом тестирования на проникновение позволяет получить объективную оценку защищенности этих систем от несанкционированного доступа, и понять какие последствия при этом могут наступить;

– командная оболочка PowerShell является мощным и эффективным механизмом осуществления сетевых атак, позволяя злоумышленнику получить стабильную интерактивную сессию на целевой системе;

– сетевые атаки на стороне клиента используют различные техники социальной инженерии, эксплуатирующие в качестве главной уязвимости человека, поэтому пользователи компьютерных систем обязаны знать основы их осуществления и уметь противостоять им.

Библиографический список

1. ГОСТ Р ИСО/МЭК ТО 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. – Введ. 2008.07.01. – М.: Стандартинформ, 2007. – 68 с.

2. Kennedy D., O'Gorman J., Kearns D., Aharoni M. Metasploit. The Penetration Tester's Guide. San Francisco: No Starch Press, 2011. – 332 p.

3. Малинин П.В., Поляков В.В. Иерархический подход в задаче идентификации личности по голосу с помощью проекционных методов классификации многомерных данных // Доклады Томского государственного университета систем управления и радиоэлектроники. 2010. № 1-1 (21). С. 128-130.

4. Empire [электронный ресурс]. – Режим доступа: https://www.powershellempire.com/. Заглавие с экрана.

5. Christian, B. First entry: Welcome and fileless UAC bypass [электронный ресурс]. – Режим доступа: https://winscripting.blog/2017/05/12/first-entry-welcome-and-uac-bypass/. Заглавие с экрана.