Федеральное агентство по образованию
Государственное образовательное учреждение
высшего профессионального образования
Ульяновский Государственный Университет

Кафедра информационной безопасности и теории управления

Г.А. Шепелев

Лабораторный практикум «Информационная безопасность автоматизированных систем»

Ульяновск
2010

Оглавление

Глава 1

Пароли

При выполнении данной лабораторной работы студенты должны усвоить следующие моменты:

- при физическом доступе злоумышленника к машине (иными словами он может снять жёсткий диск или любую другую деталь ЭВМ) или при возможности загрузки ОС со сменного накопителя, нарушитель не ограничен в своих действиях, кроме случаев, когда информация на носителях зашифрована;
- стойкость пароля к полному перебору зависит от используемого алфавита;
- приемлемые с точки зрения безопасности пароли удобно генерировать специальными программами, так называемыми генераторами паролей.

Для выполнения задания потребуется компьютер, на котором установлено по крайней мере две ОС семейства Windows. Например, Windows XP и Windows 2003 Server.

Задание:

1. загрузите любую Windows. Скопируйте файлы %SystemRoot%\system32\config\{system,SAM} на «Рабочий стол»;
2. создайте несколько учётных записей пользователей, 20–30 штук. Длина паролей должна быть в пределах от 7 до 14 символов и удовлетворять следующим требованиям:
   - у первых пользователей задайте пароль, состоящий только из цифр;
   - у второй группы пароли должны создаваться из алфавита, состоящего из цифр и латиницы верхнего или нижнего регистра;
   - у третьей группы пароли составляются из алфавита, состоящего из цифр и латиницы обоих регистров;
   - у четвёртой группы пароли составляются из алфавита, состоящего из цифр, латиницы обоих регистров и специальных символов.

   Для генерации паролей необходимо использовать программу, например, apg. После этого перезагрузите машину;
3. Загрузите другую ОС Windows. Проверьте, подключён ли раздел с предыдущей Windows как логический диск в текущей. Если нет, то примонтируйте его в оснастке «Управление компьютером», назначив ему, например, букву диска «Z:». Далее скопируйте файлы Z:\system32\config\{system,SAM} на «Рабочий стол»;

4. Запустите программу, в которой будет производиться подбор паролей полным перебором, например, Cain&Abel, lcp. Импортируйте файлы SAM и system;

5. Последовательно запустите подбор паролей с выбором соответствующих алфавитов. Запишите время, которое понадобилось программе для отгадывания того или иного пароля, а также длину и алфавит пароля.

Глава 2

Сетевые анализаторы

Цель данной лабораторной работы заключается в следующем:

- осознание того, что все данные в локальных сетях Ethernet, а также и в глобальных IPv4, передаются в открытом виде. Это очевидно влечёт нарушение свойства конфиденциальности информации;
- передача файлов по протоколу SMB;
- передача данных в протоколе SMB осуществляется в открытом виде;
- большинство более высоких протоколов IP не шифруют данные.

Для выполнения данного задания потребуется сетевой концентратор, либо коммутатор с настроенным на прослушивание данных портом, и три машины. На одном компьютере должен быть установлен сетевой анализатор WireShark. ОС на этой машине может быть любой. Компьютер подключается в коммутатор к прослушивающему порту. Два других компьютера должны быть под управлением ОС семейства Windows, они подключаются к портам, данные с которых зеркально передаются на выбранный разъём. В случае с концентратором все три машины просто подключаются к нему.

Задание:

1. на первой ЭВМ запустите WireShark и настройте фильтр на отображение только пакетов ICMP. Со второй машины проверьте командой ping доступность третьей. Убедитесь, что Ваш компьютер перехватывает данные. Теперь настройте фильтр на отображение пакетов SMB;
2. далее, на одной из машин под управлением Windows создайте пользователя и задайте ему пароль;
3. на «Рабочем столе» создайте папку, для удобства назовите её именем пользователя. В свойствах этой папки на вкладке «Безопасность» разрешите доступ хотя на чтение только что созданному пользователю;
4. в свойствах этой папки на вкладке «Доступ» откройте доступ по сети только данному пользователю;
5. в этой папке создайте текстовый файл, напишите в него что-нибудь на английском языке;
6. переходим к третьей машине. Подключите папку с предыдущей машины как сетевой диск с использованием имени Вашего пользователя и пароля. Скопируйте файл на локальную машину;
7. теперь просмотрите в списке пойманных WireShark все пакеты и найдите тело файла.

Глава 3

Перехват парольных хешей Windows

На машине под управлением ОС Windows создайте пользователей (20-25 штук) с различными типами паролей: 1) у первой группы (4-5 пользователей) пароли должны создаваться над алфавитом, содержащем только цифры; 2) во второй группе пароли задаются над алфавитом, состоящем из цифр и букв латинского алфавита верхнего или нижнего регистров; 3) для третьей группы алфавит должен содержать цифры и латиницу обоих регистров; 4) у четвёртой группы пароли генерируются над алфавитом, состоящем из цифр, латиницы обоих регистров и специальных символов. Длины паролей во всех группах должны лежать в диапазоне от 6 до 10 символов. Затем на этом же компьютере открыть доступ по протоколу SMB для всех созданных пользователей. Изменяя значение параметра LmCompatibilityLevel, последовательно задать процесс подтверждения с помощью свёртки LM, NTLM и NTLMv2. Для всех трёх случаев выполнить удалённую проверку подлинности каждого пользователя и перехватить передаваемое по сети значение функции-свёртки. Для перехваченных свёрток полным перебором продемонстрировать отличие функций, а также стойкость паролей к атаке данного типа (временную оценку).

Глава 4

Локальные сетевые соединения

На компьютерах под управлением различных ОС вывести список всех открытых сетевых соединений, тип протокола, номер порта, имя программы и т.п. Запустить любую программу, открывающую соединение. Снова вывести список всех открытых соединений и показать характеристики созданного программой сетевого соединения.

Глава 5

Протокол ARP

5.1 Глушение коммутаторов

Выполнить атаку данного типа в коммутируемой сети, состоящей минимум из трёх машин. Продемонстрировать возможность перехвата данных при развитии событий по двум возможным сценариям. Во время атаки выводить таблицу коммутации и количество записей в ней. Настроить функцию port-security для порта, к которому подключён компьютер, выполняющий перехват данных. Снова выполнить глушение коммутатора. Продемонстрировать невозможность перехвата данных, а также таблицу коммутации.

5.2 Отравление кеша ARP

С помощью ettercap, Cain&Abel, dsniff или arp-sk провести атаку данного типа в коммутируемой сети. Вывести arp-таблицы на машинах-жертвах до и после атаки.

С помощью метода статической записи в arp-таблице защитить одну из машин от атаки данного типа. Повторно отравить кэш на машинах-жертвах. Вывести arp-таблицы на атакуемых ЭВМ до и после проведения атаки.

Используя сетевой анализатор показывать на атакующем компьютере результат проведения атаки.

Глава 6

Виртуальные частные сети

6.1 PPTP

6.2 IPSec

6.3 OpenVPN

Установить и настроить сетевые соединения по технологии OpenVPN двух типов:

1. соединение «точка-точка». Необходимо сгенерировать симметричный ключ шифрования, распределить его между двумя ЭВМ и настроить OpenVPN. ОС на компьютерах должны быть различными, например, Windows и GNU/Linux, FreeBSD и GNU/Linux;

2. соединение «клиент-сервер», состоящее минимум из одного сервера и двух клиентов. Необходимо создать корневой самоподписанный сертификат X.509, и на его основе построить инфраструктуру открытых ключей для всех участников соединения. Распределить соответствующие ключи/сертификаты между участниками и настроить OpenVPN. Хотя бы на две ЭВМ должны быть установлены различные ОС.

Проверку работоспособности соединения ВЧС провести при помощи сетевого анализатора (WireShark, NetworkManager), передавая пакеты как по ВЧС, так и по физической сети Ethernet.

Глава 7

Криптографические средства

7.1 Защита электронной почты средствами GnuPG

Настроить почтовый сервер (для данной цели подойдёт простая программа, например, esms), и учётные записи электронной почты. Обменяться электронными почтовыми сообщениями, перехватить и показать их. Установить GnuPG (для используемого почтового клиента, если имеется, установить соответствующий модуль), сгенерировать ключевую пару и обменяться с другими участниками открытыми ключами. Снова обменяться почтовыми сообщениями, зашифрованными (возможно, с электронной подписью) на открытом ключе адресата (или группы адресатов). Перехватить письма и продемонстрировать их содержимое.

Литература

[1] Википедия — свободная энциклопедия. Разделы на английском, немецком и русском языках. http://wikipedia.org.

[2] *Владимиров, А.А.* Wi-фу: «боевые» приёмы взлома и защиты беспроводных сетей / А.А. Владимиров, К.В. Гавриленко, А.А. Михайловский. «Защита и администрирование». — М.: НТ Пресс, 2005. — 463 с.

[3] *Галатенко, В. А.* Основы информационной безопасности / В. А. Галатенко; Под ред. члена-корреспондента РАН В.Б. Бетелина. — М.: ИНТУИТ.РУ «Интернет-Университет Информационных технологий», 2003. — 280 с.

[4] Журнал «Information security». http://itsec.ru.

[5] *Оглтри, Т.* Firewalls. Практическое применение межсетевых экранов: Пер. с англ. / Т. Оглтри. «Защита и администрирование». — М.: ДМК Пресс, 2001. — 400 с.

[6] *Сердюк, В. А.* Информационная безопасность автоматизированных систем предприятий / В. А. Сердюк // *Бухгалтер и компьютер.* — 2007. — № 1. — С. 39–43.

[7] Учебные материалы по курсу «Безопасность сетей Windows для профессионалов». http://askit.ru.

[8] *Цирлов, В. Л.* Основы информационной безопасности автоматизированных систем / В. Л. Цирлов. — Феникс, 2008. — 87 с.