Лекция 5. Защита от локального НСД

- Хранение паролей в ОС Unix.
- Хранение паролей в ОС Windows.
- Аутентификация пользователей на основе модели «рукопожатия».

Учетные записи пользователей операционных систем клона Unix

Хранятся в текстовом файле / etc / passwd в виде отдельных строк и имеют следующий формат:

логическое имя пользователя ID : *хеш-значение его пароля* H(P) : *системный идентификатор пользователя* UID : *системный идентификатор первичной группы пользователя* GID : *полное имя и должность пользователя* D : *домашний (рабочий) каталог пользователя* HD : *командный процессор (оболочка), применяемый пользователем,* SH

Привилегии пользователей в ОС Unix

- Определяются полями учетной записи UID, GID, HD и SH.
- При работе в системе пользователь полностью идентифицируется своим системным идентификатором UID, поэтому два пользователя с одинаковым идентификатором, будут обладать совершенно одинаковыми правами в системе.
- В учетных записях псевдопользователей в поле хеш-значения пароля помещается *, что не позволяет применять эти логические имена для входа в систему.

Привилегии пользователей в ОС Unix

- Поскольку привилегии пользователя в КС определяются не его логическим именем, а значением UID, вход в систему пользователя с именем root и с системным идентификатором, отличным от нуля, не обеспечит ему привилегий суперпользователя.
- С другой стороны, вход в систему пользователя с произвольным логическим именем и с UID, равным нулю, даст ему все полномочия суперпользователя.

Алгоритм хеширования паролей

1. На основе времени суток генерируется случайное значение S (12 битов или больше), которое затем преобразуется в строку из двух или более символов и запоминается в файле учетных записей как первые символы поля с хеш-значением пароля.
2. Магическое значение M длиной 64 бита, состоящее из нулей или пробелов, зашифровывается по алгоритму DES, причем в качестве ключа шифрования длиной 56 бит используется пароль пользователя P, а S применяется для модификации алгоритма шифрования.

Алгоритм хеширования паролей

3. Полученное значение длиной 64 бита вновь зашифровывается на том же ключе (общее число повторений равно 25);
4. Полученное окончательное значение преобразуется в 11 символов (каждым 6 битам соответствует один символ из множества {‘.’, ‘/’, ‘0’-‘9’, ‘A’-‘Z’, ‘a’-‘z’});
5. Полученная строка символов записывается в файл учетных записей после случайного значения.

В современных версиях Unix на шагах 2 и 3 вместо функции шифрования DES используется функция хеширования MD5.

Минимальная длина пароля

- Поскольку пароль используется в алгоритме хеширования в качестве ключа DES-шифрования длиной 56 бит, его минимальную длину целесообразно выбирать равной восьми символам (56 бит в кодировке ASCII).

Затенение паролей

- По умолчанию к файлу / etc / passwd разрешен доступ по чтению для всех пользователей КС. Это необходимо, поскольку сведения об идентификаторах пользователя и группы, домашнем каталоге и логическом имени пользователя из этого файла должны быть доступны различным программам.
- Для защиты хеш-значений паролей от чтения непривилегированными пользователями выполняется процедура «затенения» (shadow) паролей.

Затенение паролей

- Хеш-значения паролей перемещаются из файла / etc / passwd в файл / etc / shadow (/ etc / security / passwd.adjunct или / etc / master.passwd в других операционных системах).
- В исходном файле учетных записей при использовании «затенения» паролей в поле хеш-значения пароля помещаются специальные символы (например, x) или случайная строка символов (для усложнения задачи подбора паролей). Доступ к файлу теневых паролей имеет только привилегированный пользователь.

Учетные записи групп

- Информация о группах пользователей в операционных системах семейства Unix помещается в файл / etc / group. Каждая запись в этом файле имеет следующий формат:

имя группы : *пароль группы* : *системный идентификатор группы* GID : *список разделенных запятыми логических имен пользователей-членов группы*

- При использовании паролей групп следует применять «затенение» паролей групп, аналогичное созданию теневых паролей пользователей (в этом случае хеш-значения паролей групп перемещаются в файл / etc / gshadow или аналогичный).

Хранение паролей в ОС Windows

- База данных учетных записей содержится в разделе реестра HKEY_LOCAL_MACHINE \ SAM (в файле Windows \ System32 \ Config \ SAM). К базе данных SAM не может быть получен доступ для чтения или изменения с помощью штатных средств операционной системы даже администратором (она открывается ядром операционной системы во время ее загрузки в монопольном режиме). Для ее редактирования предназначены специальные функции из набора Windows API и специальные системные приложения.

Хранение паролей в ОС Windows

Пароль пользователя в базе данных SAM хранится в виде двух хеш-значений, каждое из которых имеет длину 128 бит. Первое из этих хеш-значений формируется по алгоритму Windows NT:

1. Строка символов пароля P усекается до 14 знаков (при необходимости) и преобразуется в кодировку Unicode, в которой каждый символ представляется двумя байтами.
2. Вычисляется хеш-значение преобразованного пароля H(P) длиной 128 бит (используется функция хеширования MD4).

Алгоритм Windows NT

3. Полученное хеш-значение зашифровывается по алгоритму DES с помощью ключа, равного относительному номеру учетной записи пользователя, $E_{RID}(H(P))$.
4. Полученный результат шифрования записывается в базу данных учетных записей.

Хранение паролей в ОС Windows

Второе хеш-значение пароля пользователя вычисляется по алгоритму LAN Manager:

1. Все буквенные символы (латинского алфавита) строки пароля P преобразуются к верхнему регистру.
2. Строка символов пароля дополняется нулями, если она короче 14 байтов, и делится на две семибайтовые половины P_1 и P_2.
3. Каждое из значений P_1 и P_2 используется в качестве ключа для шифрования по алгоритму DES магической строки M=”KGS!@#$%”, в результате которого получаются два значения из 64 бит каждое – $H_1=E_{P1}(M)$ и $H_2=E_{P2}(M)$.

Алгоритм LAN Manager

4. Выполняется шифрование по алгоритму DES на ключе, равном относительному номеру учетной записи, результата сцепления H_1 и H_2 – $E_{RID}(H_1 || H_2)$.
5. Полученный результат шифрования помещается в базу данных SAM.

Алгоритм LAN Manager является мене стойким (искусственно уменьшается мощность алфавита, из которого выбираются символы пароля, а разделение пароля на две половинки облегчает его подбор в том случае, если длина пароля не превышает семи знаков, так как результат шифрования магической строки на нулевом ключе заранее известен нарушителю).

Сложность паролей в ОС Windows

Требования к паролям при включении специального параметра безопасности:

- длина не менее 6 символов;
- включение символов хотя бы из трех подмножеств (строчные буквы, прописные буквы, цифры, специальные знаки);
- Несовпадение с именем ученой записи или его частью.

Хранение паролей в ОС Windows

- Несмотря на то, что доступ к базе данных SAM с помощью штатных средств Windows для нарушителя практически невозможен, он, тем не менее, может ее скопировать, загрузив на атакуемом компьютере другую ОС (помешать этому можно только с помощью организационных мер). Затем нарушитель сможет получить доступ к базе данных учетных записей как к обычному файлу (с помощью специальных программных средств).

Программа syskey

- Обеспечит шифрование хеш-значений паролей с помощью первичного ключа длиной 128 бит, хранящегося в реестре также в зашифрованном виде.
- После запуска программы syskey администратор должен выбрать способ хранения системного ключа длиной 128 бит, который будет использован для шифрования первичного ключа.

Способы хранения системного ключа

- в системном реестре (преимущество этого варианта в отсутствии необходимости присутствия привилегированного пользователя при перезагрузке операционной системы, а недостаток – в наименьшей защищенности хранения системного ключа);
- в файле startup.key (длиной 16 байт) в корневом каталоге специальной дискеты (в этом случае придется отдельно позаботиться о защищенном хранении этой дискеты и ее резервной копии);
- без физического сохранения системного ключа, который будет генерироваться из специальной парольной фразы длиной не менее 12 символов.

Альтернатива использованию программы syskey

- Включение параметра безопасности «Сетевая безопасность: не хранить хеш-значений Lan Manager при следующей смене пароля».

База данных SAM

- Содержит учетные записи пользователей и групп.
- Права учетной записи в системе определяются ее уникальным идентификатором безопасности SID (security identifier).
- Идентификатор безопасности представляет собой структуру переменной длины, которая однозначно определяет пользователя или группу.

Аутентификация пользователей на основе модели «рукопожатия»

Пользователь U и система S согласовывают при регистрации пользователя в КС функцию f, известную только им. Протокол аутентификации пользователя в этом случае выглядит так:

1. S: генерация случайного значения x (запроса); вычисление y=f(x); вывод x.
2. U: вычисление отклика y′=f′(x); ввод y′.
3. S: если y и y′ совпадают, то пользователь авторизуется в системе, иначе попытка входа в систему отклоняется.

Аутентификация пользователей на основе модели «рукопожатия»

К функции f предъявляется требование, чтобы по известным x и f(x) нельзя было «угадать» f. Преимущества аутентификации на основе модели «рукопожатия» перед парольной аутентификацией:

- между пользователем и системой не передается никакой конфиденциальной информации;
- каждый следующий сеанс входа пользователя в систему отличен от предыдущего, поэтому даже длительное наблюдение за этими сеансами ничего не даст нарушителю.

Аутентификация пользователей на основе модели «рукопожатия»

К недостаткам аутентификации на основе модели «рукопожатия» относится большая длительность этой процедуры по сравнению с парольной аутентификацией.

Взаимная аутентификация

Парольная аутентификация совершенно неприменима в случае взаимного подтверждения подлинности пользователей компьютерной сети. Действительно, пусть *А* и *Б* обозначают двух пользователей сети, имеющих соответственно пароли $Р_А$ и $Р_Б$. Тогда протокол взаимной аутентификации *А* и *Б* мог бы выглядеть так:

1. *А*->*Б*: А, запрос $Р_Б$.
2. *Б*->*А*: Б, запрос $Р_А$.
3. *А*->*Б*: А, $Р_А$.
4. *Б*->*А*: Б, $Р_Б$.

Взаимная аутентификация

- Но в момент отправки своего пароля (неважно, в открытой или защищенной форме) *А* не может быть уверении в подлинности *Б*, который может воспользоваться паролем *А*, чтобы выдать себя за *А* при взаимодействии с еще одним пользователем компьютерной сети *В*.
- Модель «рукопожатия» вполне приемлема для взаимной аутентификации:

Взаимная аутентификация по модели «рукопожатия»

1. *А*: выбор значения x; вычисление y=f(x).
2. *А*->*Б*: А, x.
3. *Б*: вычисление y′=f(x).
4. *Б*->*А*: Б, y′.
5. *А*: если y и y′ совпадают, то *А* может доверять *Б*.

Затем процедура аутентификации повторяется с переменой «ролей» (теперь *Б* начинает процесс и выбирает значение x′), чтобы *Б* мог также быть уверен в подлинности *А*.

Аутентификация пользователей на основе модели «рукопожатия»

- При локальном доступе пользователя к системе функция f может быть задана таблицей своих значений (для возможности ее запоминания и вычисления отклика) или вычисляться с помощью специального устройства, имеющегося у пользователя.
- Но в основном модель «рукопожатия» применяется при удаленной аутентификации.