УДК 004.056.53
DOI: 10.17586/0021-3454-2018-61-10-881-886

ЗАЩИТА ОТ АТАК НА УЧЕТНУЮ ЗАПИСЬ ПРИВИЛЕГИРОВАННОГО ПОЛЬЗОВАТЕЛЯ

Т. С. Осадчая, А. Ю. Щеглов

Университет ИТМО, 197101, Санкт-Петербург, Россия
E-mail: taniaosadchaya6@gmail.com

Решаются задачи предотвращения возможности хищения учетных данных привилегированных пользователей и уменьшения последствий от такого хищения в доменной сети. Проведено исследование проблем, связанных с данной задачей. Проанализированы способы получения хэша пароля привилегированной учетной записи злоумышленником, рассмотрена опасность такого хищения при использовании доменной сети. Предложено решение, состоящее в построении эшелонированной (многоуровневой) защиты, каждый последующий уровень которой построен исходя из предположения о преодолении злоумышленником предыдущего. Рассмотрен подход, состоящий в усилении парольной защиты и предотвращении возможности администрирования (удаленного и локального) при наличии у злоумышленника данных привилегированной учетной записи. Предложенный подход полностью обеспечивает решение поставленной задачи.

Ключевые слова: *привилегированные пользователи, эшелонированная (многоуровневая) защита, хищение учетных данных, доменная сеть, административные общие ресурсы*

Введение. Согласно статистике, большинство атак на информационные системы в настоящее время связаны с перехватом или подбором паролей пользователей и их использованием. Так, 80 % целевых атак направлены на взлом привилегированной учетной записи [1].

В большинстве компаний для построения корпоративной сети используются технология Active Directory и ОС семейства Windows. Если хотя бы к одному компьютеру домена злоумышленник получил доступ с правами привилегированного пользователя, то можно с большой вероятностью говорить о захвате всего домена, поскольку сеть и система безопасности, на уровне как ОС, так и домена, основаны на определенной доверенной системе [2].

В случае использования доменной структуры пользователя аутентифицирует не локальная подсистема безопасности (Local Security Authority, LSA), а подсистема на контроллере домена, хранящего учетные записи доменных пользователей в Active Directory. Для удаленного взаимодействия этих подсистем (т.е. для аутентификации пользователя или компьютера по сети) используются так называемые аутентификационные пакеты, реализующие различные протоколы: NTLM (библиотека MSV1_0.dll) и Kerberos (библиотека Kerberos.dll). Несмотря на то что все серверные версии Windows начиная с Server 2000, по умолчанию используют протокол Kerberos для удаленной аутентификации пользователя или ресурса, протокол LM/NTLM challenge-response все еще поддерживается и может быть использован, если клиент инициирует такое соединение. Необходимо отметить, что для такой аутентификации не нужно знать пароль, достаточно значения хэша.

Получить хэш пароля возможно:

— из AD-хранилища — Active Directory хранит данные о пользователях в файле NTDS.DIT;

— из локальной SAM-базы, где хранятся LM/NTLM-хэши локальных пользователей;

— из кэша LSA, в который попадают LM/NTLM-хэши доменных пользователей во время активной сессии пользователя (во время активного локального или удаленного сеанса работы, например, когда администратор подключается по RDP для выполнения своих функций) [3];

— из XML-файлов настроек групповой политики безопасности (Group Policy Preference), часто содержащих набор зашифрованных учетных данных в файлах Groups.xml, которые могут быть получены с контроллера домена и расшифрованы;

— в результате атаки на протокол прикладного уровня SMB, реализующего удаленный доступ к разделяемым ресурсам.

Таким образом, получение хотя бы одного хэша учетной записи, обладающей административными правами на каком-либо сервере, может обеспечить удаленный административный доступ к контроллеру домена, а значит, и ко всем серверам и рабочим станциям в домене [3].

При наличии доменной сети администратор на любой рабочей станции может как управлять локальной машиной, так и, благодаря протоколу SMB, удаленно администрировать остальные рабочие станции домена с использованием скрытых административных общих ресурсов (рис. 1). Так, общий ресурс ADMIN$ позволяет получить привилегированный удаленный доступ к каталогу %SYSTEMROOT% другого компьютера, общий ресурс IPC$ используется при организации временных подключений, создаваемых приложениями для обмена данными с помощью именованных каналов. На практике, как правило, этот ресурс применяется для удаленного администрирования серверов в сети.

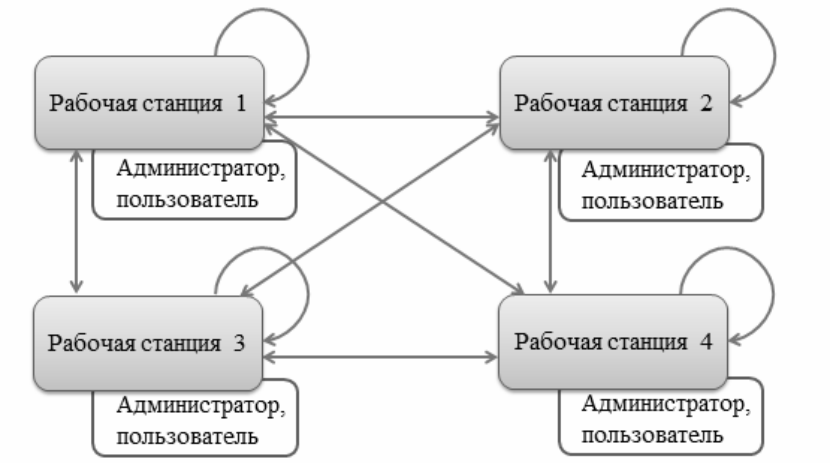

Рис. 1

Целью исследования является повышение уровня безопасности защищаемой системы, предотвращение хищения учетных данных привилегированных пользователей и уменьшение последствий от такого хищения в доменной сети. Для этого необходимо затруднить возможность хищения пароля и хэша пароля; снизить риски в случае хищения: предотвратить возможность администрирования злоумышленником при наличии у него данных привилегированной учетной записи.

Решение указанных задач в комплексе обеспечивает построение *эшелонированной (многоуровневой) защиты*, каждый последующий уровень которой построен согласно предположению, что злоумышленник преодолел предыдущий уровень.

Так, **первый уровень защиты** должен обеспечивать усиление парольной защиты для усложнения возможности кражи паролей учетных записей. *Первым способом* решения данной задачи является использование смарт-карт и электронных USB-ключей (токенов) для аутентификации пользователей. Эти устройства могут использоваться для аутентификации пользователя в домене Windows с целью интерактивного или удаленного входа в систему, а также для аутентификации клиента — взаимной идентификации пользователя и домена [4].

Использование смарт-карт и электронных USB-ключей позволяет существенно повысить безопасность сети за счет совершенствования методов аутентификации, при этом исчезает проблема, связанная с использованием „слабых“ словарных паролей.

Вторым способом решения задачи является реализация средством защиты дополнительного механизма идентификации и аутентификации пользователей. Такой способ предполагает другие способы хранения, обработки и передачи паролей. Задачей защиты является предотвращение возможности несанкционированного входа в систему при компрометировании пароля, создаваемого в ОС. Обеспечивается это тем, что средство защиты реализует защищенное хранение в своей базе учетных записей пользователей, которым разрешен вход в систему, и их паролей, которые не связаны с паролями ОС. При этом также возможно использование смарт-карт и электронных USB-ключей. Кроме того, пароль для входа в систему, созданный в средстве защиты, при удаленной аутентификации пользователей по каналу не передается — передается пароль ОС, но его хищение не позволит использовать скрытые административные общие ресурсы для удаленного администрирования.

Данный способ используется при:

— локальном входе в систему;

— запуске приложений с правами другого пользователя;

— удаленном доступе к разделенным сетевым ресурсам локальной сети;

— удаленном доступе по RDP;

— доступе к терминальной сессии;

— запуске исполняемых файлов с запросом учетных данных администратора (UAC);

— разблокировке системы посредством снятия заставки.

Таким образом, поскольку ни пароль, созданный средством защиты, ни хэш этого пароля, не находятся в указанных местах хранения паролей Windows, а также не передаются по сети, кража пароля Windows при условии, что на всех рабочих станциях установлено средство защиты и используется усиленная аутентификация, не позволит злоумышленнику похитить учетные данные пользователей.

Второй уровень защиты необходим, если учетные данные привилегированного пользователя все же похищены. Поскольку при использовании доменной структуры, зная пароль привилегированного пользователя, можно осуществлять удаленное администрирование всех рабочих станций, входящих в домен, с любой рабочей станции, необходимо предотвратить эту возможность. Для этого необходимо организовать выделенное рабочее место системного администратора, с которого будет разрешено администрирование остальных рабочих станций (рис. 2).

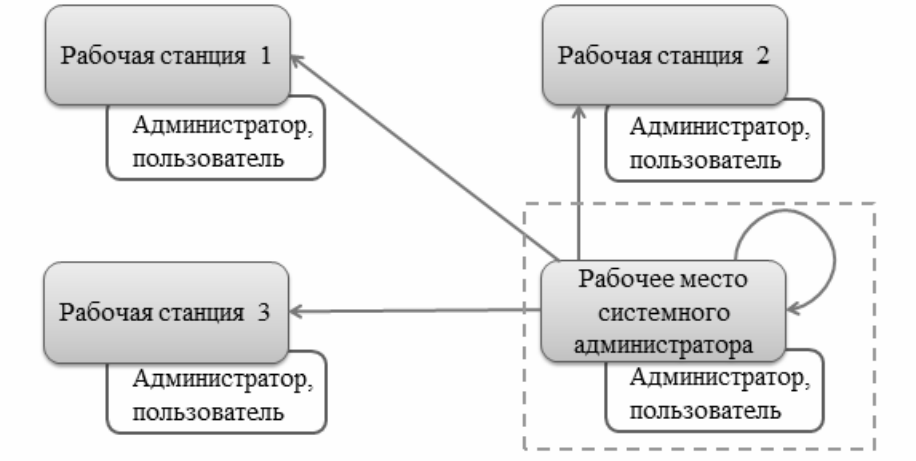

Рис. 2

Для локализации рабочего места системного администратора необходимо в средстве защиты на всех компьютерах, кроме выбранного в качестве рабочего места администратора,

установить разграничительную политику для доступа к скрытому административному общему ресурсу ADMIN$ (рис. 3).

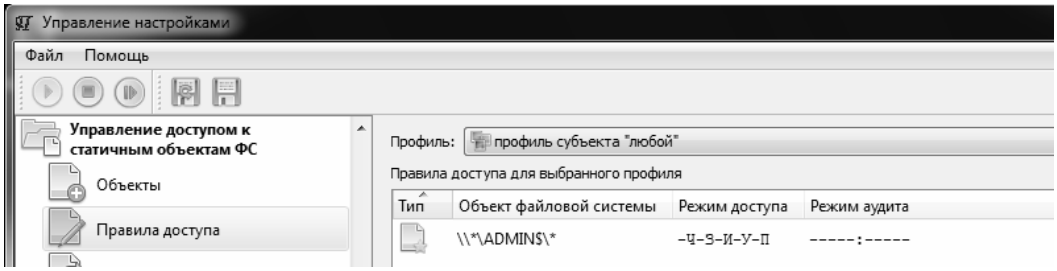

Рис. 3

В этом случае к общему ресурсу, предоставляющему администраторам доступ по сети к корневому каталогу удаленной операционной системы (%SYSTEMROOT%), даже зная пароль привилегированного пользователя, подключиться нельзя. Аналогичная разграничительная политика может быть задана и для других административных общих ресурсов, в том числе ресурса IPC$, используемого для удаленного администрирования серверов в сети.

Необходимо также отметить, что при удаленном доступе к административному общему ресурсу ADMIN$ в журнале аудита на целевой машине появляется информация о доступе к каталогу %SYSTEMROOT%, выполненном учетной записью „Администратор“, причем первичным пользователем (т.е. учетной записью, от лица которой запущен процесс, запрашивающий доступ к ресурсу) является система.

Следовательно, после организации рабочего места системного администратора необходимо предотвратить возможность внесения злоумышленником изменений в корневой каталог на локальной машине, если им были похищены учетные данные привилегированного пользователя. Для этого необходимо на всех остальных рабочих станциях создать следующее правило для субъекта „Администратор“ (пользователь — администратор домена) (рис. 4).

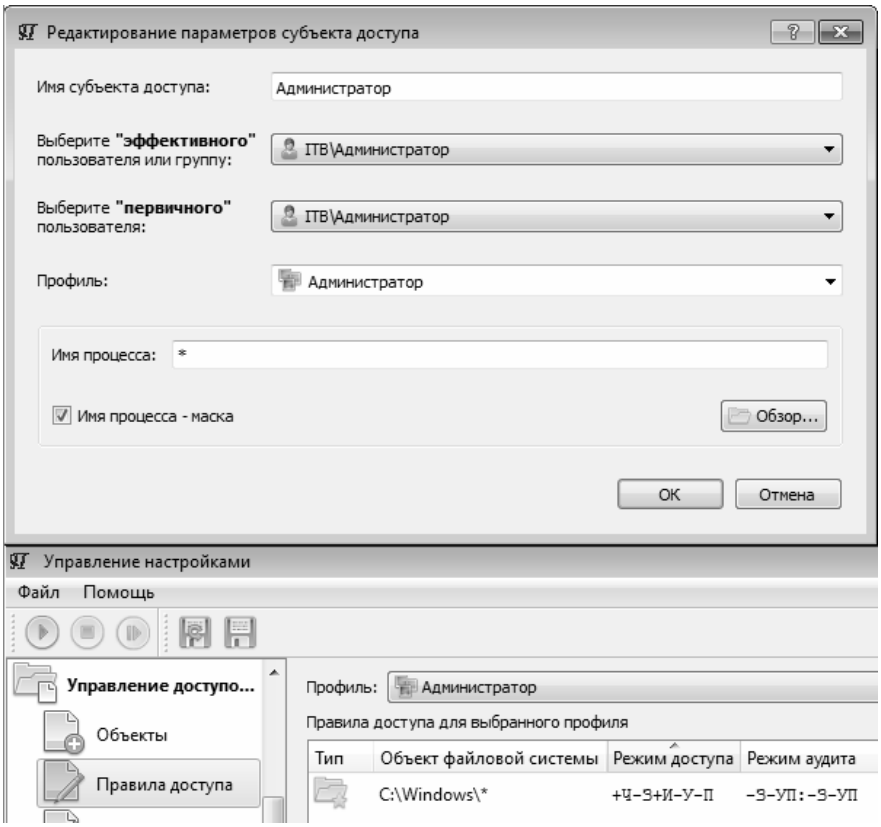

Рис. 4

В результате доменному пользователю „Администратор“ модифицировать корневой каталог с этой рабочей станции будет нельзя (рис. 5).

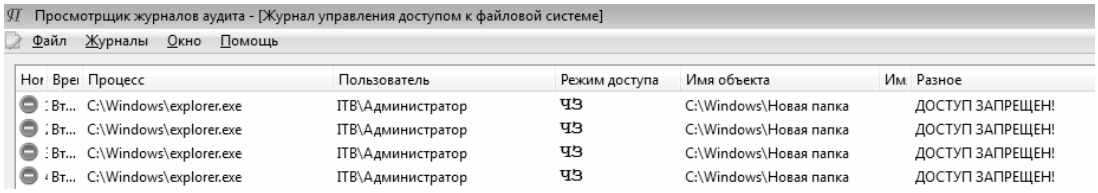

Рис. 5

После применения такой разграничительной политики и дополнительной защиты рабочего места системного администратора организационными мерами будет предотвращена возможность как локального администрирования от имени привилегированной учетной записи системного администратора, так и удаленного администрирования с остальных компьютеров в домене.

Необходимо отметить, что такой подход базируется на реализации механизма самозащиты, не позволяющего привилегированным пользователям каким-либо способом влиять на функционирование средства защиты информации. Данный механизм не позволит привилегированному пользователю, не являющемуся администратором безопасности, повлиять на запущенную службу и драйверы средства защиты, модифицировать его настройки. При этом механизм самозащиты должен быть реализован на уровне ядра операционной системы системными драйверами из состава средства защиты, которые нельзя выгрузить системным процессом или службой. Это будет препятствовать любому воздействию привилегированных пользователей на систему защиты (удаление, остановка служб и т.д.).

Заключение. В результате применения такого подхода будет обеспечена дополнительная защита при аутентификации, а также обеспечена возможность администрирования компьютеров в сети исключительно с рабочей станции системного администратора.

Рассматриваемый подход был реализован на практике и апробирован при построении комплексной системы защиты информации (КСЗИ) „Панцирь+“ для ОС Microsoft Windows. Данный материал является частью общей технологии защиты от целевых атак, разработанной и внедренной КСЗИ „Панцирь+“ для ОС Microsoft Windows [5].

СПИСОК ЛИТЕРАТУРЫ

1. *Brook Ch.* 88 % сетей уязвимы к взлому привилегированных аккаунтов [Электронный ресурс]: <https://threatpost.ru/88-percent-of-networks-susceptible-to-privileged-account-hacks/13219/>.
2. Атаки на домен: завладеваем корпоративной сетью // Хакер [Электронный ресурс]: <https://xakep.ru/2011/03/31/55263>.
3. *Карпов А.* NTLM не умер, он просто так пахнет [Электронный ресурс]: <https://www.securitylab.ru/analytics/362448.php>.
4. *Подлесный М.* Регистрация без пароля // Windows IT Pro/RE. 2002. № 8.
5. *Щеглов А. Ю.* КСЗИ „Панцирь+“. Эффективное решение защиты корпоративных информационных систем от целевых атак [Электронный ресурс]:<http://npp-itb.ru/images/docs/alldocs/slides.pdf>.

Сведения об авторах

Татьяна Сергеевна Осадчая — магистрант; Университет ИТМО; кафедра вычислительной техники; E-mail: taniaosadchaya6@gmail.com

Андрей Юрьевич Щеглов — д-р техн. наук, профессор; Университет ИТМО; кафедра вычислительной техники; E-mail: info@npp-itb.spb.ru

Поступила в редакцию
15.02.18 г.

Ссылка для цитирования: *Осадчая Т. С., Щеглов А. Ю.* Защита от атак на учетную запись привилегированного пользователя // Изв. вузов. Приборостроение. 2018. Т. 61, № 10. С. 881—886.

PROTECTION AGAINST ATTACKS ON PRIVILEGED USER ACCOUNT

T. S. Osadchaya, A. Yu. Shcheglov

ITMO University, 197101, St. Petersburg, Russia
E-mail: taniaosadchaya6@gmail.com

The tasks of preventing the possibility of theft of credentials of privileged users and reducing the consequences of such theft in the domain network are considered. The problems associated with this task are studied. Ways to get the password hash of a privileged account by an attacker are analyzed, the risk of such theft when using a domain network is assessed. A solution is proposed that consists in building a layered (multi-level) protection, each subsequent level of which is built on the assumption that the attacker has overcome the previous protection level. An approach is proposed which consists in strengthening password protection and preventing the possibility of administration (remote and local) if an attacker has a privileged account data. The proposed approach is stated to provide a complete solution to the problem.

Keywords: privileged users, echelon (multi-level) protection, identity theft, domain network, administrative shares

REFERENCES

1. https://threatpost.ru/88-percent-of-networks-susceptible-to-privileged-account-hacks/13219/. (in Russ.)
2. https://xakep.ru/2011/03/31/55263/. (in Russ.)
3. https://www.securitylab.ru/analytics/362448.php. (in Russ.)
4. Podlesnyy M. Windows IT Pro/RE, 2002, no. 8. (in Russ.)
5. http://npp-itb.ru/images/docs/alldocs/slides.pdf. (in Russ.)

Data on authors

Tatiana S. Osadchaya — Student; ITMO University; Department of Computer Science Engineering; E-mail: taniaosadchaya6@gmail.com

Andrey Yu. Shcheglov — Dr. Sci., Professor; ITMO University; Department of Computer Science Engineering; E-mail: info@npp-itb.spb.ru

For citation: Osadchaya T. S., Shcheglov A. Yu. Protection against attacks on privileged user account. *Journal of Instrument Engineering*. 2018. Vol. 61, N 10. P. 881—886 (in Russian).

DOI: 10.17586/0021-3454-2018-61-10-881-886