Оглавление

Задание № 2.2. Компрометация

Формулировка задания

В настоящем задании необходимо:

2.2.1. Скомпрометировать ключи пользователя *Помощник глав админа Иванов*.

О компрометации

Компрометация может происходить с удалением или без удаления сетевого узла, пользователя.

Как правило, ключи считаются скомпрометированными в следующих случаях:

- посторонним лицам мог стать доступным файл дистрибутива ключей пользователя;
- посторонним лицам могло стать доступным съемное устройство с ключами пользователя;
- посторонние лица могли получить неконтролируемый физический доступ к ключам пользователя, хранящимся на компьютере;
- уволился пользователь, имевший доступ к паролям и ключам;
- съемное устройство с ключами вышло из строя, и не опровергнут тот факт, что это произошло в результате несанкционированных действий злоумышленника.

2.2.1. Компрометация ключей пользователя

Для компрометации ключей пользователя *Помощник глав админа Иванов* выполните следующие действия:

1. В окне ViPNet Удостоверяющий и ключевой центр перейдите в раздел *Пользователи*,
2. Выделите пользователя *Помощник глав админа Иванов* и в контекстном меню выберите пункт *Считать скомпрометированными.*
3. В появившемся окне *Компрометация ключей пользователей* нажмите кнопку *Да* (после этого пользователь *Помощник глав админа Иванов* будет помечен красным цветом). Если вместе с

ключами пользователя были скомпрометированы его ключи электронной подписи, установите флажок *Аннулировать сертификаты выбранных пользователей (Рисунок 108)*.

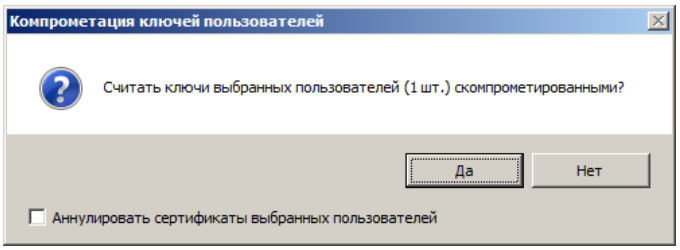

Рисунок 1 – Окно *Компрометация ключей пользователя*

4. Повторно вызовите нажатием правой кнопки мыши на пользователя *Помощник глав админа Иванов* контекстное меню и выберите пункт *Ключи пользователя> Создать и передать ключи в ЦУС*.
5. В окне *ViPNet Удостоверяющий и ключевой центр* перейдите в раздел *Сетевые узлы*.
6. После этого создайте и передайте в ЦУС ключи для узла *Помощник глав админа.*
7. Затем выделите правой кнопкой мыши (или сочетанием клавиш Ctrl+W) остальные узлы, для которых нужно создать ключи и в контекстном меню выберите пункт *Создать и передать ключи в ЦУС* (или сочетанием клавиш Ctrl+F).

	Примечание. Если у скомпрометированного пользователя есть в наличии ключи электронной подписи и сертификат, которые хранятся на его узле, то создайте для него новые ключи и сертификат. Это связано с тем, что на узле ключи электронной подписи защищены персональным ключом пользователя. Поэтому после смены персонального ключа пользователь не сможет получить доступ к своим текущим ключам электронной подписи и сертификату.

8. В окне *ViPNet Центр управления сетью* нажмите кнопку *Справочники и ключи> Отправить справочники и ключи…*
9. В открывшемся окне выберите узел *Помощник глав админа* и нажмите кнопку *Отправить (Рисунок 109)*.
10. Проконтролируйте доставку обновления на узел *Помощник глав админа*.
11. Проконтролируйте применение обновления на скомпрометированном узле *Помощник глав админа*.
12. После перезапуска ПО ViPNet Client, появиться диалоговое окно, в котором необходимо будет указать путь до РНПК и ввести пароль пользователя.
13. После успешного обновления на узле *Помощник глав админа*, появиться диалоговое окно с информацией о том, что текущий пароль истек и его следует сменить. Для смены пароля необходимо

выбрать пункт *Открыть настройки пароля и установить новый пароль* – 11111111 *(Рисунок 110).*

14. Отправьте обновления на остальные узлы.

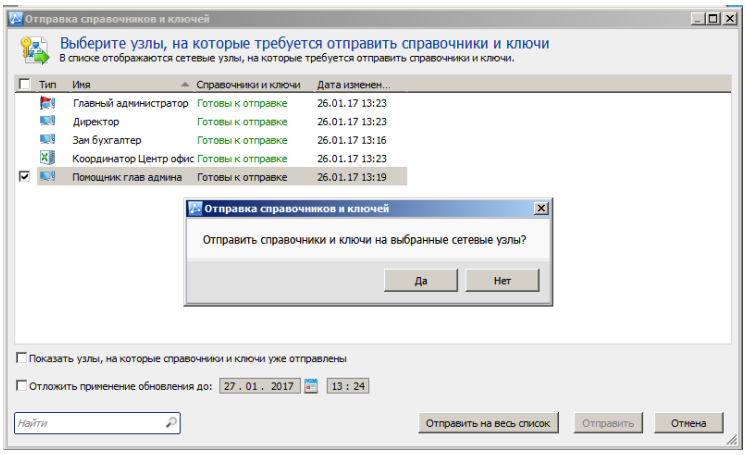

Рисунок 2 – Отправка ключей на узел *Помощник глав админа*

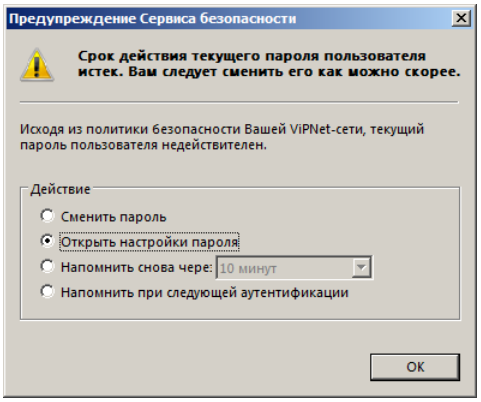

Рисунок 3 – Смена пароля на узле *Помощник глав админа*

В результате правильного выполнения задания на сетевом узле *Помощник глав админа* должен быть доступен *Главный администратор* (в программе *ViPNet Client Монитор* в разделе *Защищенная сеть* выберите *Главный администратор* и нажмите клавишу *F5).*