Практический опыт

Информационная безопасность «на коленках»

Yevgeniy Goncharov, 2016

Кратко

- Наши подходы и задачи
- Насущные вопросы
- Разбор полетов
- Итог
- Вопросы / Контакты

Подходы и Задачи

- Автоматизация все и вся
- Тюнинг систем
- Утилизация ресурсов – «грузим железо» по полной
- Проактивные действия
- Мгновенная реакция
- Экономия денег бизнесу

Былые боли

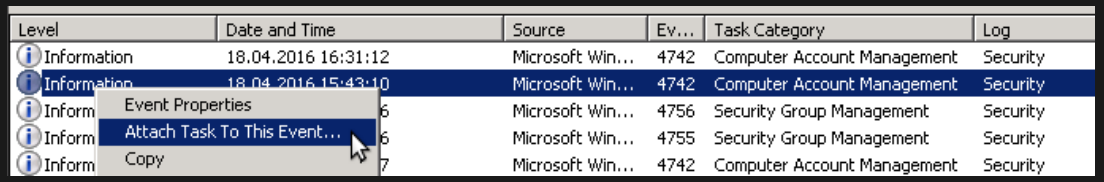
- Много администраторов с неограниченным доступом
- Трудно отследить кто, что делал
- Кто меняет пароли и блокирует учетные записи?!
- Мониторинг ресурсов – следим за доступностью, производительностью, ресурсами
- Обновление стороннего ПО – автоматический багфиксинг. Важно!
- Как заблокировать / контролировать «левое» ПО?
- Война с «топами». Новая культура
- Хаос в общих ресурсах (папки, принтеры, разрешения)

Мониторинг событий

- Все события регистрируются в едином журнале событий
- Каждое событие имеет свой ID
- На каждое определенное событие можно создать триггер
- Триггер может вызывать определенное автоматизированное действие
- Решается встроенными средствами Windows – встроенный планировщик задач + скрипт + реакция на событие

Автоматизация

- Создаем задачу на определенное событие

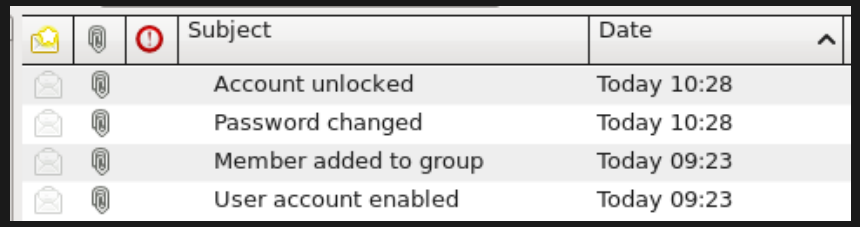


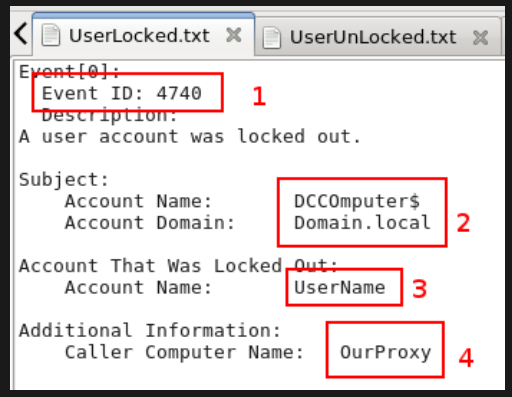
- Пишем скрипт, который отрабатывает по событию, прикрепляем к задаче

```
wevtutil qe ForwardedEvents /q:*[System[(EventID=4740)]] /f:text /rd:true /c:1 > %systemroot%\logs\UserLocked.txt
```

- Указываем в задаче отправку письма с вложением UserLocked.txt (или отправляем из PowerShell скрипта в Windows Server 2012)

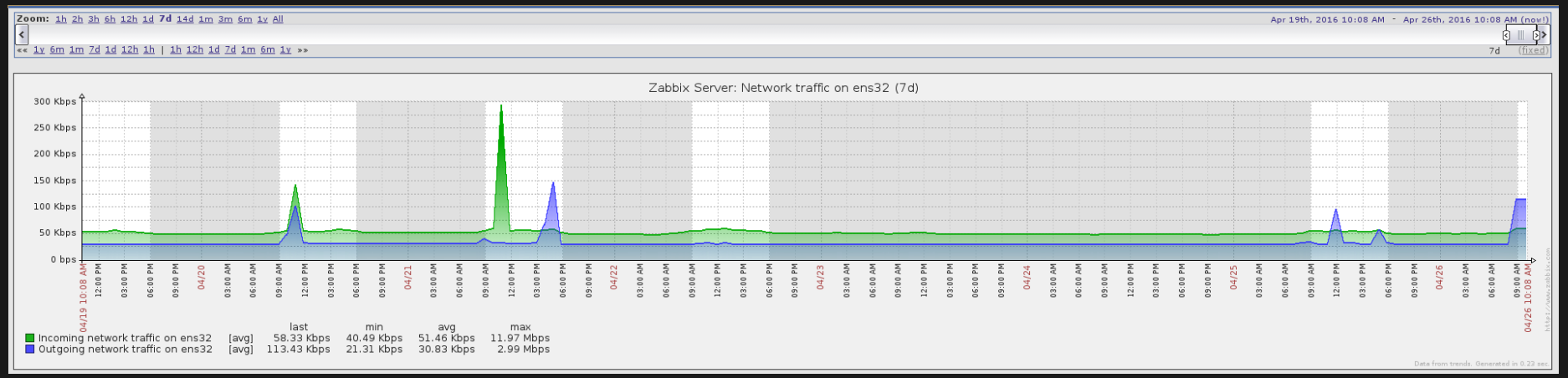
- Наблюдаем результат в почте





Мониторинг систем

- Доступность сервера
- Нагрузка на каналы связи
- Загрузка сервера (память, процессор)
- Место на жестком диске. Важно!
- Мониторинг событий безопасности Windows / Linux / Сетевых устройствах (SNMP)
- Решается Open Source – Zabbix



Пример визуализации Zabbix в Grafana

Обновление ПО

- Обновления стороннего софта. Недооценено
- Проблемные точки – бухгалтерия, маркетинг, топ менеджеры
- Множественные уязвимости Java / Adobe Flash / Adobe Reader / Codecs / Другие
- Необходимо всегда держать актуальные версии софта
- Автоматически обновлять. Без участия конечного пользователя
- Решается свободно распространяемым инструментом SCUP (либо аналогичным ему) + WSUS – частично позволяет отслеживать уязвимости, применять патчи, устанавливать свой софт (exe, msi), использовать скрипты, манипулировать папками / файлами

Блокировка ПО

- Блокируем все, разрешаем только нужное
- Разрешения на уровнях ролей (маркетинг, бухгалтерия и т.п.)
- Разрешения в зависимости от выполняемых задач (сторонние люди)
- Частичное блокирование съемных устройств (флешки, внешние диски и т.п.)
- Блокировка заведомо «вредного» ПО, скриптов
- Решается инструментами GPO – Software Restriction Policies, начиная с Windows Server 2008 + Application Control Policies – относительно гибкое создание правил с использованием групп безопасности, версионности ПО его издателя, хеша, создание привил запуска скриптов, установщиков ПО

Контроль стороннего ПО

- Контроль элементов интерфейса
- Контроль настроек
- Централизация настроек
- Использование GPO – Административные шаблоны (написанные самостоятельно, предоставляемые производителями ПО – Firefox, Google Chrome)

Виртуализация

- Уже не роскошь, а необходимость (утилизация аппаратных ресурсов)
- Используем – Hyper-V, VMware, KVM
- Миграция сервисов в виртуальную среду
- Частично мигрировали на KVM
- Экономия места в ЦОДе, снижение затрат на электроэнергию

The End

Вопросы и ответы ;)

Много примеров в блоге – http://sys-admin.kz / форуме http://forum.sys-admin.kz