

**Open SysConf '19**

зачем нужен отдельный лог-сервер  
или история одного инцидента ИБ

Yevgeniy Goncharov, 2019

# Агенда

Немного теории:

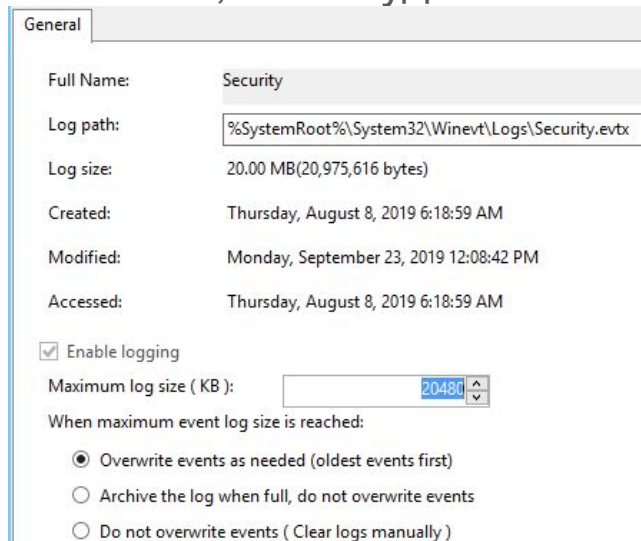
- про логи
- политики аудита
- как можно чистить / собирать логи
- инцидент
- как могут помочь логи со сборщика

---

- Среда - Windows, Active Directory домен
- Ситуация - зашифрованные файловые шар

# Зачем нужны логи / Ротация / Аудит

- Содержат информацию о работе служб, приложений, пользователей иных сущностей системы (протоколирование операций, событий)
- В том числе помогают траблшутить / решать проблемы
- Великое множество - логи приложений, системные логи, логи аудита и т. п. и т.д
- Важно знать и понимать:
  - Сколько и как хранить
  - Как и где настраивать
- Аудит системных событий
  - Где настраиваются
  - Какие типы аудита существуют



# Кратко о виндовом аудите

Есть возможность настройки:

- Аудита событий входа в систему (интересна выдача билетов, проверка подлинности)
- Аудита управления учетными записями (изменение атрибутов)
- Аудит событий входа (интересен (не) успех)
- Аудита доступа к объектам (интересен доступ к объектам ФС)
- Аудита изменения политики (интересно кто менял)
- Аудита использования привилегий (интересны попытки привилигированного запуска)
- Аудита отслеживания процессов (события управления процессами - старт, стоп и т.п. интересны события касающиеся планировщика Windows)
- Аудита системных событий (интересно кто очистил логи, изменял системное время)

# Настройки GPO

пример настроек ->

- несколько вариаций настроек
- как может пригодиться (не) успех
- object access + фс аудит

The screenshot displays the Windows Group Policy Editor interface. On the left, the tree view shows the hierarchy: Local Computer Policy > Security Settings > Local Policies > Audit Policy. The 'Audit Policy' folder is expanded, showing sub-policies like User Rights Assignment, Security Options, and Advanced Audit Policy Configuration. The 'Advanced Audit Policy Configuration' folder is also expanded, showing a list of audit categories: Account Logon, Account Management, Detailed Tracking, DS Access, Logon/Logoff, Object Access, Policy Change, and Privilege Use. On the right, a table lists the security settings for these categories. The 'Audit privilege use' setting is highlighted in grey.

Policy	Security Setting
Audit account logon events	Success
Audit account management	Success
Audit directory service access	Success, Failure
Audit logon events	Success
Audit object access	Success, Failure
Audit policy change	Success
Audit privilege use	Success
Audit process tracking	Success
Audit system events	No auditing

# Чистка логов

- Ок, но кто-то может почистить логи
- логи могут перетереться (системой или специально)
- диск может быть переполнен / поврежден
- могут быть удалены отдельные события
- логи можно подменить

# Сбор логов - Решения из коробки / Велосипеды / Open Source решения

- Windows Event Collector (быстро настраивается, но медленный поиск / фильтрация)
- Слать логи в БД (быстрый поиск, но нужно костылить отправку, требует БД)
- Слать логи в специализированные системы сбора / агрегации логов (SysLog, GrayLog, ELK, Splunk, etc. Обычно требует Linux, прямые руки и немного сноровки)
- Бэкап никто не отменял

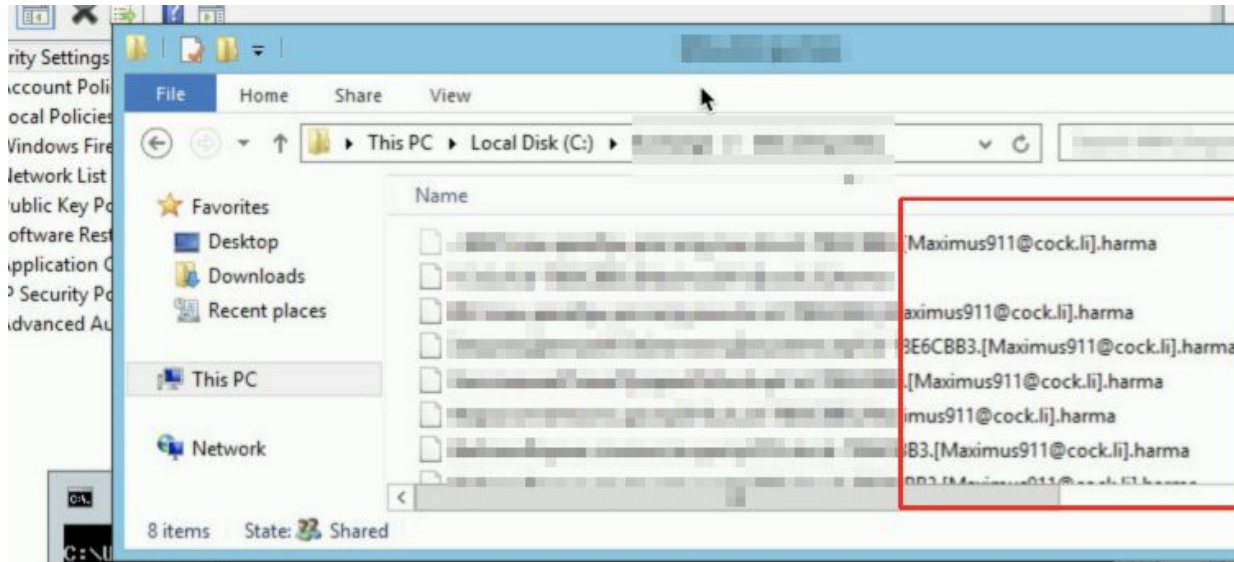
<https://docs.microsoft.com/en-us/windows/win32/wec/windows-event-collector>

# Кратко об инциденте

- В одной Компании были обнаружены зашифрованные файлы
- Обнаружение произошло спустя неделю или больше после фактического шифрования файлов
- Файлы зашифровались только в общих каталогах
- Непонятно кто или что является источником
- Задача - найти, не понять, не простить
- Локализовать проблему



# Когда User Name пришел на работу

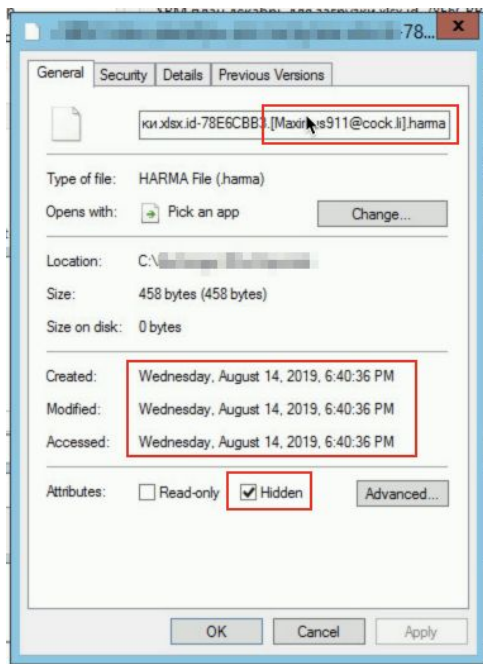




КОГДА ОСОЗНАЛ И ПОНЯЛ, ЧТО ЗДЕСЬ ЧТО-ТО НЕ ТАК

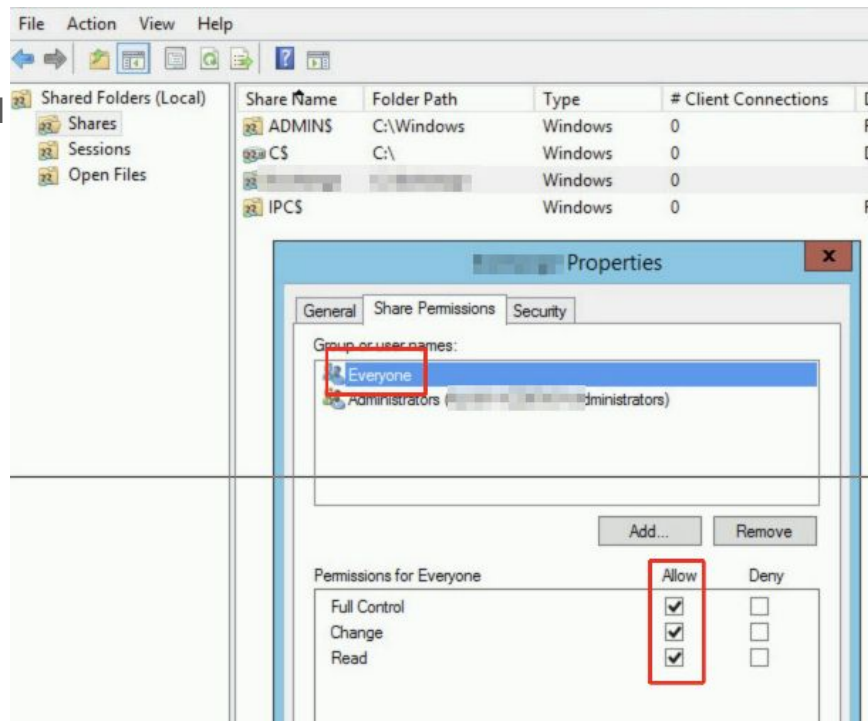
# И начал копать

Дата, время шифровки - 14 августа, 2019, 6:40PM, файлам присвоен hidden атрибут, изменено расширение на hama, файлы зашифрованы



# Посмотрел, что за папка и какие у нее разрешения

- + пострадала только сетевая шара
- + в Security разрешения аналогичны
- + похоже пришло откуда-то извне



# Логов аудита нет, но есть SID

Инцидент обнаружен спустя некоторое время, **локальный файлы логов аудита (Security) были перезаписаны системой**, но у файла остался владелец, тот из-под кого было произведено шифрование, это оказался Гость, но точно **не** локальный



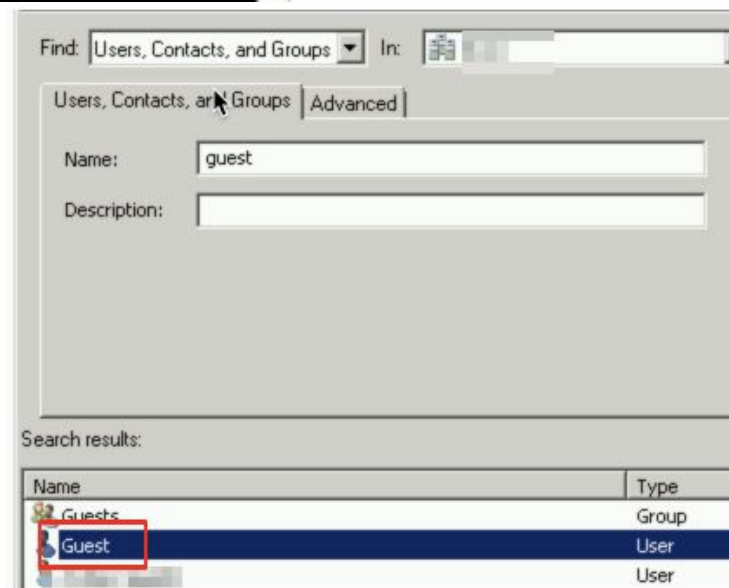
# Убеждаемся, что Гость доменный

```
C:\Windows\system32>wmic useraccount where sid='S-1-5-21-1008537768-501' get name  
Name  
Guest
```

Включенный Гость, Аллилуя, Карл!)

Откуда ты Гость?

```
C:\>net user Guest | findstr active  
Account active Yes  
  
C:\>
```



# Раскопки при помощи локальных / доменных логов

печаль, но они перезатерлись

Когда случился эксепшн, а логов нет





# Лог-сервер - наш друг / Корреляция событий

2019-08-14 18:40:16.000 [REDACTED]  
An account was successfully logged on.

---

**Subject:**  
Security ID

✉ **ab5ba9b4-be90-11e9-91a4-5254006aa0f1**

**Received by**  
WinLogs-gelf on P 016c025c / ala01-mon03.rb.kz

**Stored in index**  
graylog\_2012

**Routed into streams**

- All messages

**ActivityID**  
{4F32ADC8-0240-0004-08F6-2E00CA7}

**AuthenticationPackageName**  
Kerberos

**Category**  
Logon

**Channel**  
Security

**EventID**  
4624

**EventReceivedTime**  
2019-08-14 18:40:17

**EventType**  
AUDIT\_SUCCESS

1

version  
0

**full\_message**

Logon Type: 3

New Logon:

Security ID: S-1-5-21-[REDACTED] 501

Account Name: Guest

Account Domain: [REDACTED]

Logon ID: 0x58b9bd76

Logon GUID: {078BE7FB-F7CF-4BCD-8E22-0C84B784D1EB}

Process Information:

Process ID: 0x0

Process Name: -

Network Information:

Workstation Name: [REDACTED]

Source Network Address: 172.17.0.1

Source Port: 65075

Detailed Authentication Information:

Logon Process: Kerberos

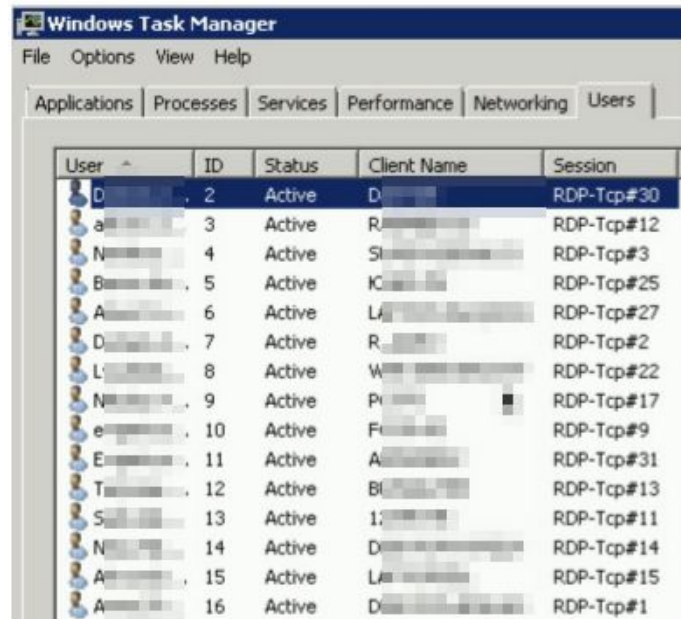
Authentication Package: Kerberos

Transited Services: -

2

# Злой комп

- Есть файлы зашифрованные Гостем
- Зашифрованы файлы, к которым предоставлен доступ всем
- Похоже, что источник не привилегирован в системе
- Действует на автомате
- Смотрим кто ходит на сервер
  - много кто, включая внешних пользователей



The screenshot shows the Windows Task Manager interface with the 'Users' tab selected. It displays a list of active users and their sessions. The table below represents the data shown in the screenshot.

User	ID	Status	Client Name	Session
D...	2	Active	D...	RDP-Tcp#30
a...	3	Active	R...	RDP-Tcp#12
N...	4	Active	S...	RDP-Tcp#3
B...	5	Active	K...	RDP-Tcp#25
A...	6	Active	L...	RDP-Tcp#27
D...	7	Active	R...	RDP-Tcp#2
L...	8	Active	W...	RDP-Tcp#22
N...	9	Active	P...	RDP-Tcp#17
e...	10	Active	F...	RDP-Tcp#9
E...	11	Active	A...	RDP-Tcp#31
T...	12	Active	B...	RDP-Tcp#13
S...	13	Active	I...	RDP-Tcp#11
N...	14	Active	D...	RDP-Tcp#14
A...	15	Active	L...	RDP-Tcp#15
A...	16	Active	D...	RDP-Tcp#1

# Кто пытается ходить

- Брутят в несколько потоков
- Рандомными именами
- Казахстан, Болгария, Малайзия, etc

Security Number of events: 8 330 685 (!) New events available

Filtered: Log: Security; Source: ; Event ID: 4625. Number of events: 17 361

Keywords	Date and Time	Source	Event ID	Task Category
Audit Failure	28.08.2019 9:49:33	Microsoft Wi...	4625	Logon
Audit Failure	28.08.2019 9:49:22	Microsoft Wi...	4625	Logon
Audit Failure	28.08.2019 9:49:22	Microsoft Wi...	4625	Logon
Audit Failure	28.08.2019 9:49:22	Microsoft Wi...	4625	Logon
Audit Failure	28.08.2019 9:49:22	Microsoft Wi...	4625	Logon
Audit Failure	28.08.2019 9:49:21	Microsoft Wi...	4625	Logon
Audit Failure	28.08.2019 9:49:20	Microsoft Wi...	4625	Logon
Audit Failure	28.08.2019 9:49:14	Microsoft Wi...	4625	Logon
Audit Failure	28.08.2019 9:49:14	Microsoft Wi...	4625	Logon
Audit Failure	28.08.2019 9:49:06	Microsoft Wi...	4625	Logon
Audit Failure	28.08.2019 9:49:06	Microsoft Wi...	4625	Logon
Audit Failure	28.08.2019 9:49:02	Microsoft Wi...	4625	Logon
Audit Failure	28.08.2019 9:49:02	Microsoft Wi...	4625	Logon
Audit Failure	28.08.2019 9:48:58	Microsoft Wi...	4625	Logon

Event 4625, Microsoft Windows security auditing.

General Details

An account failed to log on.

Subject:

- Security ID: NULL SID
- Account Name: -
- Account Domain: -
- Logon ID: 0x0

Logon Type: 3

Account For Which Logon Failed:

- Security ID: NULL SID
- Account Name: АДМИНИСТРАТОР
- Account Domain: -

Failure Information:

- Failure Reason: Unknown user name or bad password.
- Status: 0xc000006d

Log Name: Security

# Смотрим дальше

- Не работает служба обновлений
- Отсутствует антивирус

The screenshot displays the Windows Update control panel window. The title bar reads "Windows Update" and the breadcrumb path is "Control Panel > System and Security > Windows Update". On the left, there are links for "Control Panel Home", "Check for updates", "Change update settings", "View update history", and "Turn on hidden updates". The main content area features a red shield icon with a white 'X' and the text: "Turn on automatic updating. Updates are not being installed automatically. Turn on automatic updating to help improve the security and performance of your computer to install updates on this computer." Below this is a button labeled "Turn on automatic updates" and a link "Let me choose my settings".

Below the Windows Update window, a large orange warning icon is visible with the text "Scan not complete. Restart required." Below this, a table shows scan statistics:

Scan time:	14m : 43s
Items scanned:	4,393,110
Threats detected:	41
Threats quarantined:	41

A Malwarebytes notification window is overlaid on the bottom of the scan results. The title bar says "Malwarebytes". The message reads: "All selected items have been removed successfully. A log file has been saved to the logs folder. Your computer needs to be restarted to complete the removal process. Would you like to restart now?" There are "Yes" and "No" buttons at the bottom.

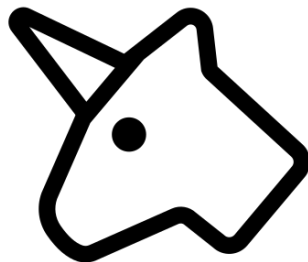
Нужно закрыть трубу



# Итог

- Следим за безопасностью при помощи лог-сервера
- Следим за обновлениями и антивирусным ПО
- Следим за политиками аудита и политиками безопасности
- Следим за учетными записями и событиями в локальной сети
- Занимаемся резервным копированием
- Прорабатываем план на случай заражения / исключительной ситуации
- Повышаем уровень грамотности себя и окружающих (человеческий фактор никто не отменял)
- Делимся знаниями
- Помогаем друг-другу решать проблемы

The End



**Open SysConf '19**

Yevgeniy Goncharov

@sysadminkz, <https://sys-adm.in/>, [https://t.me/sysadm\\_in\\_channel](https://t.me/sysadm_in_channel)