Дослідження організації антивірусного захисту навчально-методичних сервісів на платформі Docker

Виконав студент

IV курсу групи ДА-61 Калюжний Є. Ю.

Дипломний керівник: доцент,

к.т.н. Гіоргізова-Гай В. Ш.

Опис роботи

- **Мета роботи:** організація захисту від вірусів та шкідливого ПЗ системи навчально-методичних матеріалів на платформі Docker та забезпечення безпечного користування сервісами користувачів системи.
- **Об’єкт дослідження:** організація антивірусного захисту навчально-методичних сервісів на платформі Docker.
- **Предмет дослідження:** комплексний підхід до антивірусного захисту додатка NextCloud на платформі Docker та демонстрація його роботи.

Постановка задачі

- Виконати аналіз існуючих вразливостей Docker-контейнерів та методи їх захисту.
- Порівняти методи антивірусного захисту Docker-контейнерів.
- Вибрати антивірусне ПЗ для навчально-методичного сервісу NextCloud.
- Створити та налаштувати інфраструктуру залежних сервісів NextCloud на основі Docker Compose.
- Провести тестування системи.

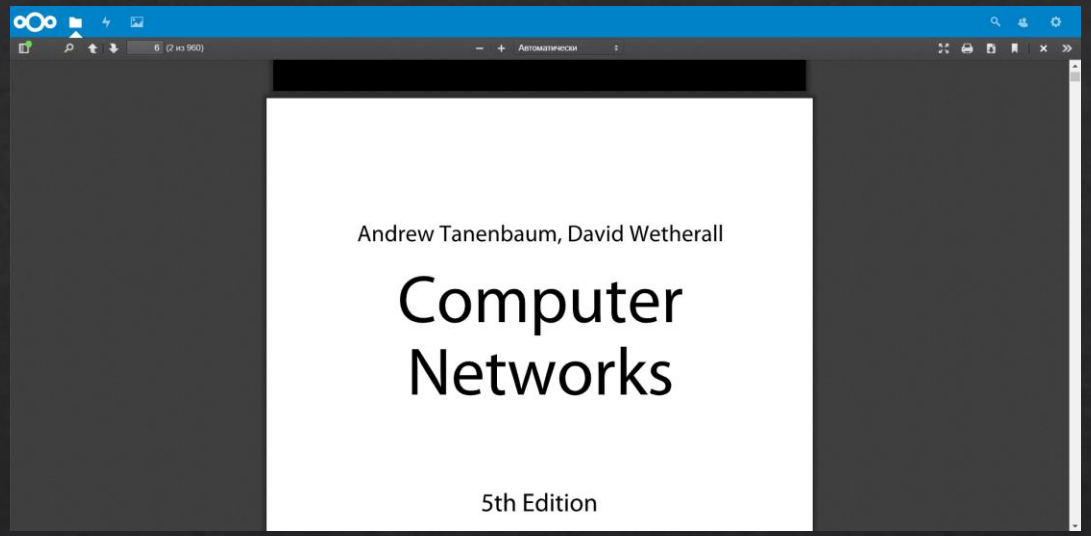
Вразливості контейнерів

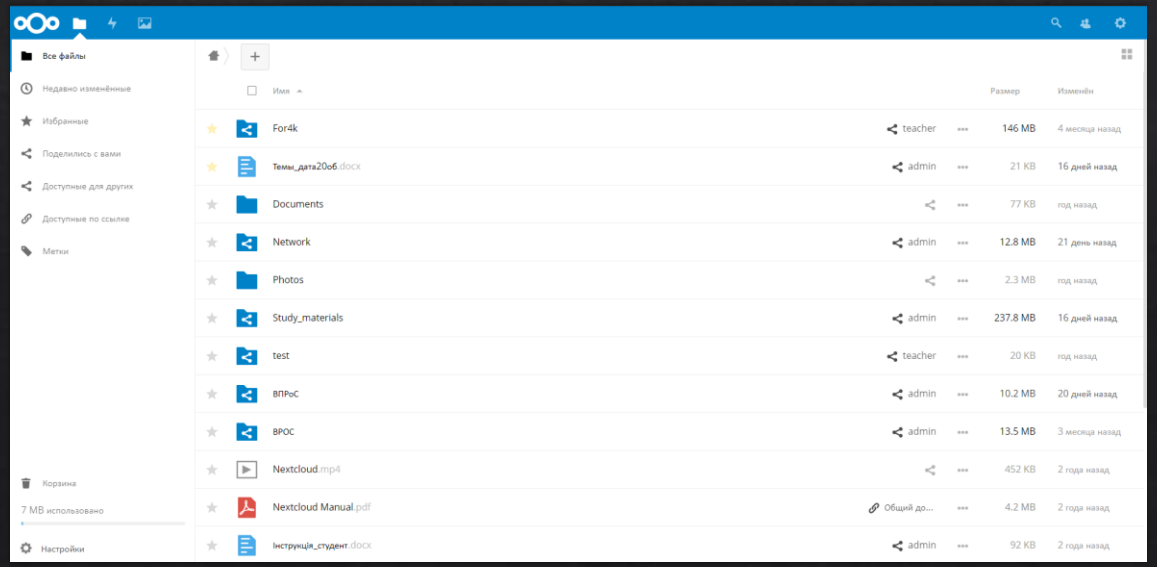
- Необмежений доступ (права користувача root) до контейнера може поставити під загрозу весь хост або кластер.
- Необхідно налаштувати захист хостової машини. Закрити зайві порти, що відкритті для доступу зовні за допомогою файрвола. Особливу увагу приділити портам Docker-демону, які використовуються для отримання доступу над Docker API.
- Для команд Docker потрібні привілеї root. Таким чином, користувачі Docker мають привілейований доступ до хоста та його файлової системи, що робить його вразливим.
- Гарною практикою є створювати окремого користувача з обмеженими привілеями, а також не використовувати root-привілейованого користувача у середині контейнеру.

- Зображення Docker вразливі через спосіб їх побудови або їх вміст.
- Потрібно ретельно вибирати базові (батьківські) образи для створення власних образів. Використовувати образи лише з офіційного реєстру Docker HUB, які створенні видавцями продукту, пройшли перевірку та мають позначку верифікації.
- Деякі контейнери потребують відкриття порту назовні, так у випадку з NextCloud, необхідно тримати відкритий порт для доступу до вебінтерфейсу.
- Для таких контейнерів бажано використовувати Reverse Proxy для фільтрації запитів, наприклад Nginx. Також гарним застережливим засобом є встановлення та використання SSL сертифікату.
- Контейнери, що зберігають файли на хостовій системі шляхом монтування розділу, становлять велику небезпеку.
- У такому випадку має бути встановлена система для перевірки та знешкодження зловісних файлів, які можуть ненавмисно або спеціально бути завантажені до сховища.

Сервіс NextCloud

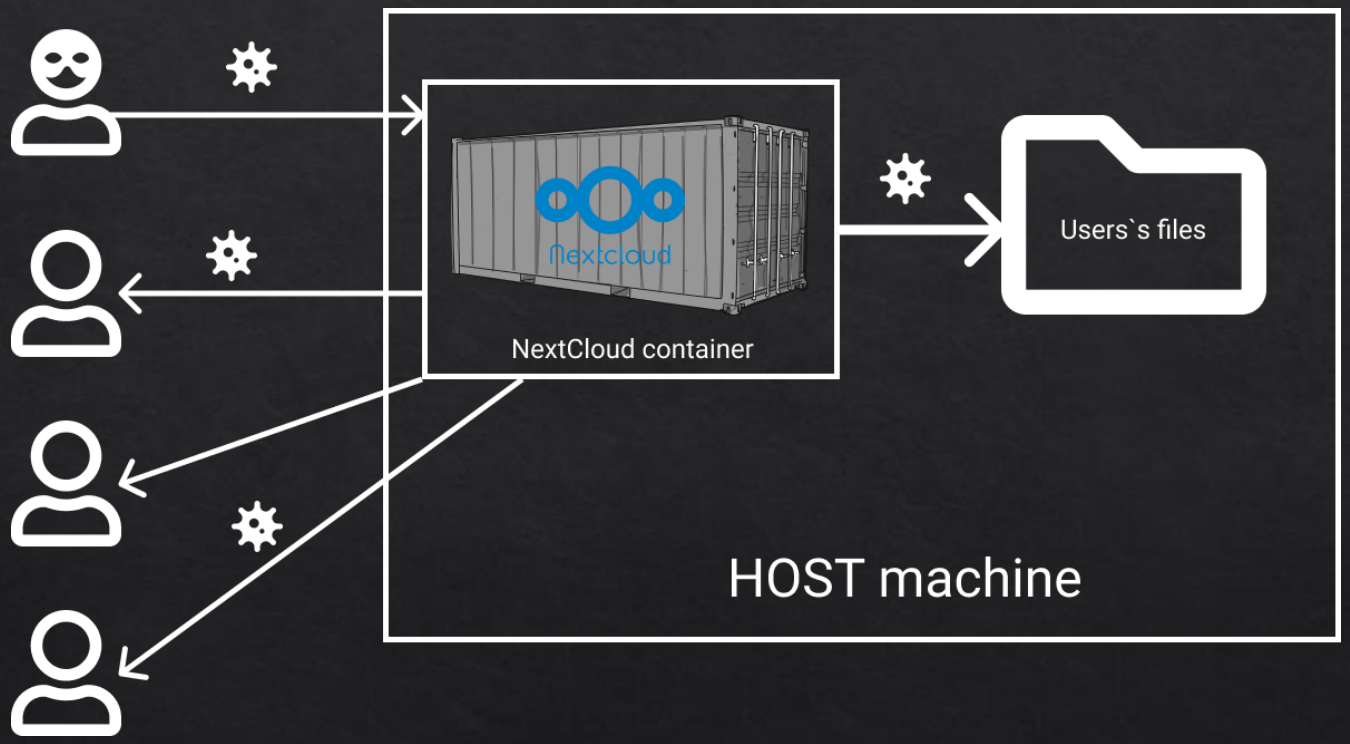
На нашій кафедрі для збереження та розповсюдження навчально-методичних матеріалів використовується сервіс NextCloud. Він дозволяє створювати теки, завантажувати файли та ділитися ними, об’єднувати користувачів у групи і розподіляти права доступу до тек відповідно до групи.





Окрім того додаток забезпечує підтримку усіх стандартних розширень документів docx, doc, xls, xlsx, pdf, з можливістю перегляду у браузері, одночасним доступом та сумісним редагуванням.

Небезпека користування сервісом



Хоча додаток і знаходиться у ізольованому контейнері, файли користувачів завантажуються на хостову машину, аби зберегти їх цілісність у разі виходу з ладу контейнеру. Окрім того, сам процес завантаження та розповсюдження файлів без належного антивірусного захисту наражає на небезпеку не тільки обладнання серверу, а й усіх користувачів системи.

Вибір антивірусного ПЗ

Bitfinder

- Сканування архівів.
- Графічний інтерфейс.
- Підтримка Solaris, Linux и FreeBSD.
- Безкоштовна пробна версія Bitdefender обмежена.
- Деякі функції заблоковані і доступні тільки в платній версії.

ClamAV

- Рішення з відкритим кодом
- Повністю безкоштовне рішення
- Підтримка Unix, Windows, MacOS
- Регулярне оновлення бази данних
- Підтримка різних типів файлів, таких як PDF, Office и Zip.
- Нативна інтеграція з NextCloud.

Типи встановлення

На хостову систему

- Антивірус буде витрачати обчислювальні можливості, скануючи системні директорії, з багатьма системними файлами та вкладеними теками.
- Під час сканування доступ до файлів блокується, а цього не можна допускати для програм - демонів.
- Коли антивірусне програмне забезпечення сканує файли, які використовує Docker, ці файли можуть бути заблоковані таким чином, що сервіси можуть ставати недоступними на деякий час.
- Такий тип встановлення значно уповільнюватиме роботу серверу та підвищить рівень споживання ресурсів.

Docker-контейнер

- Антивірус у контейнері матиме можливість швидко змінювати хостову ОС, тобто таке рішення є абсолютно кросплатформним та незалежне від сімейства ОС.
- Такий тип встановлення повністю автономний і не потребує додаткових конфігурацій
- Використовуючи Docker можна ізолювати антивірус таким чином, що він не матиме жодного впливу на інші сервіси, які можуть бути встановлені на сервері.
- Швидкість сканування необхідних файлі більша, адже не витрачається час на ієрархічний прохід по текам.
- Продуктивність такого рішення значно вища, бо зникає необхідність сканувати системні фали.

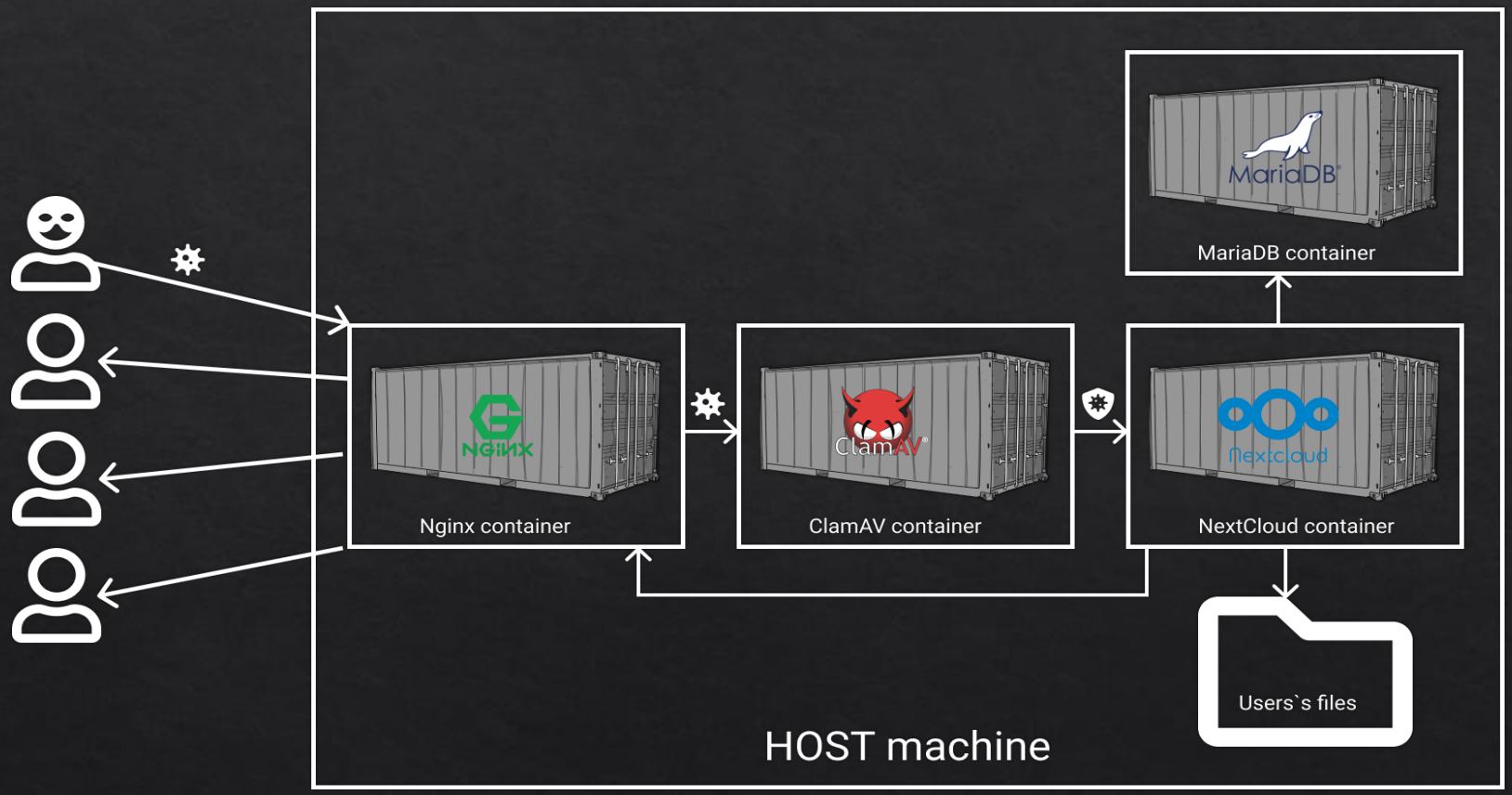
- Наявність антивірусу на хостовій машині лише уповільнить її роботу, а також змусить зависати деякі сервіси. Достатньо дотримуватися вимог безпечної роботи з Docker та інколи незалежно від інших сервісів сканувати файли користувачів на предмет наявності вірусів. До того ж таке рішення абсолютно не кросплатформним.

```
root@test-js:~# clamscan -r /home/kolin/my_files/
/home/kolin/my_files/eicar_com.zip: Win.Test.EICAR_HDB-1 FOUND

----------- SCAN SUMMARY -----------
Known viruses: 6849828
Engine version: 0.102.2
Scanned directories: 1
Scanned files: 1
Infected files: 1
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 21.338 sec (0 m 21 s)
root@test-js:~#
```

- Антивірусне ПЗ у контейнері – це оптимальне рішення, хоч і при одиночному скануванні швидкість трохи менша, але таке рішення не викликає проблем у роботі серверного обладнання, а на довгій дистанції споживає менше системних ресурсів та швидше справляється з поставленою ціллю.

```
bash-5.0# clamscan -r /folder_to_scan/
/folder_to_scan/eicar_com.zip: Win.Test.EICAR_HDB-1 FOUND

----------- SCAN SUMMARY -----------
Known viruses: 9062947
Engine version: 0.102.2
Scanned directories: 1
Scanned files: 1
Infected files: 1
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 40.669 sec (0 m 40 s)
bash-5.0#
```

Структура залежних сервісів



Окрім Антивірусного ПЗ, NextCloud потребує деяких додаткових сервісів:

1. Reverse Proxy (Nginx)
2. Database (MariaDB)

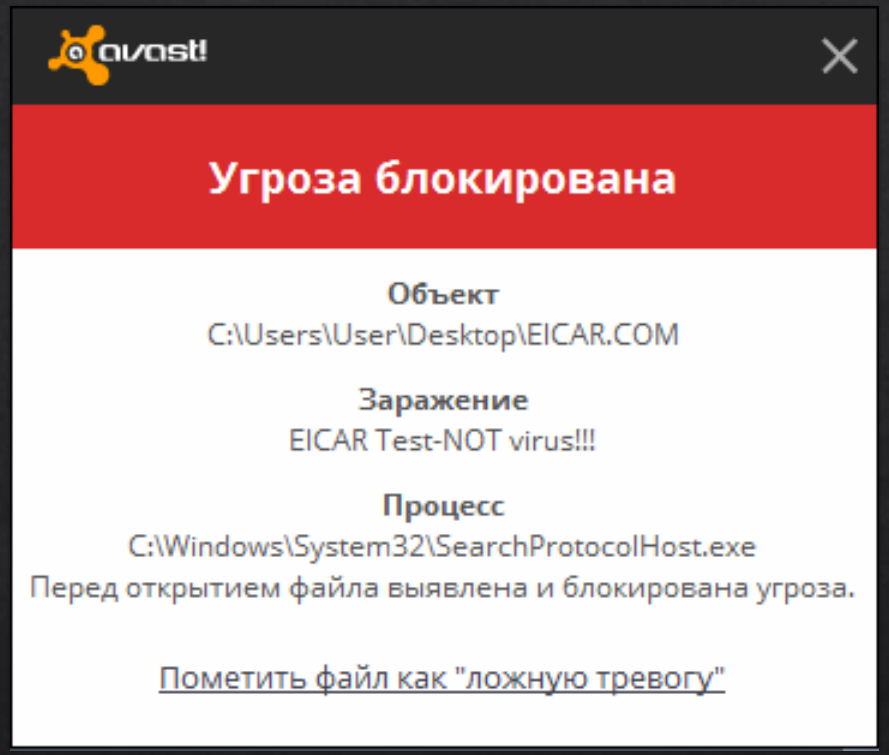
У результаті отримуємо наступну структуру.
Веб-інтерфейс проксується через Nginx, завантажені файли скануються на льоту і лише потім потрапляють до сховища, гарантуючи безпеку користувачам та обладнаню на якому розміщено сервіс.

Лабораторний вірус

EICAR (Або **EICAR-Test-File**) — це спеціальний тестовий файл для перевірки АВ-систем. Стандартний файл аби впевнитись у коректній роботі антивірусу.

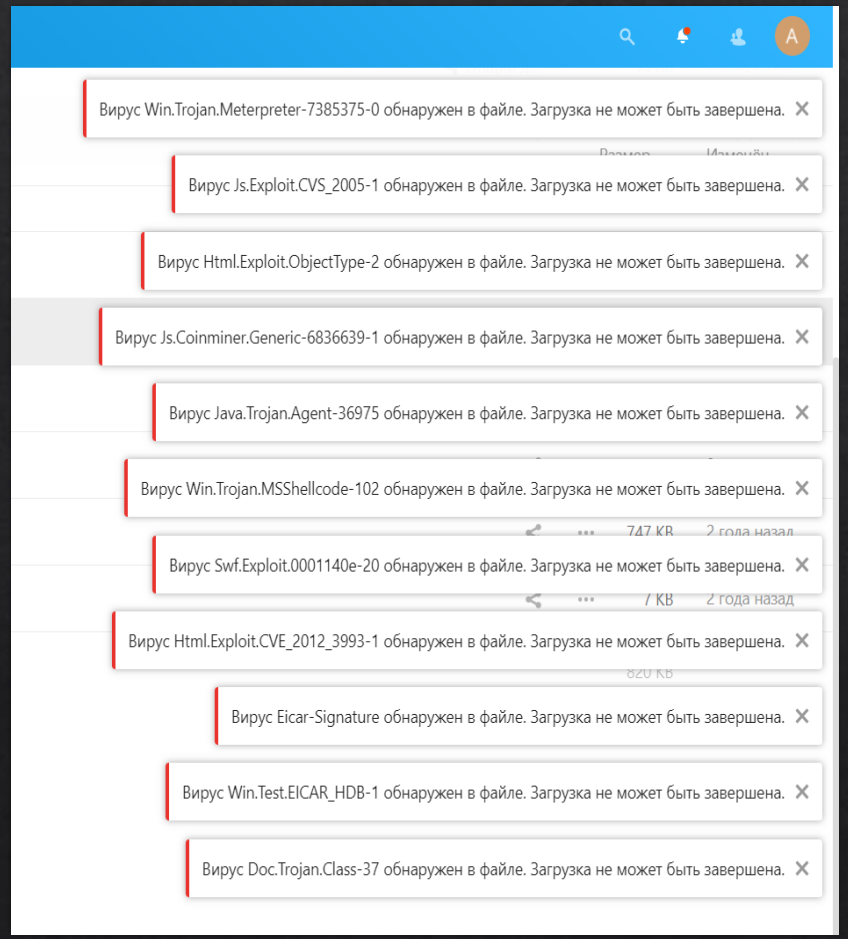
Ним можна безпечно користуватися, оскільки це не вірус і не містить фрагментів вірусного коду. Більшість продуктів реагують на нього так, ніби це вірус (хоча вони, як правило, повідомляють про це з очевидною назвою, наприклад „EICAR-AV-Test“).

Файл є законною програмою DOS і дає заздалегідь сприятливі результати (він друкує повідомлення „EICAR-STANDARD-ANTIVIRUS-TEST-FILE!”).



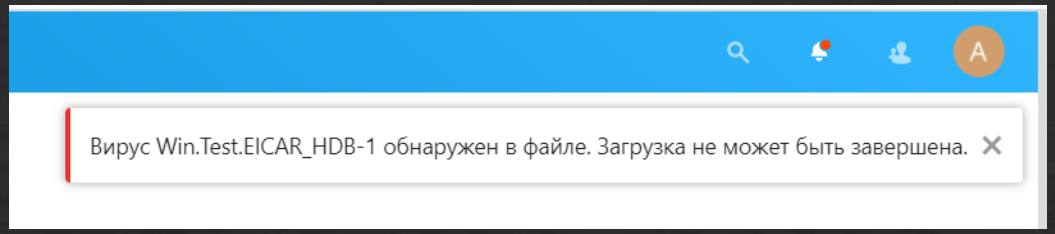
EICAR – це стандарт у тестуванні антивірусів, але він перевіряє лише одну з багатьох вразливостей системи. Тому, аби точно бути впевненим у надійності антивірусу, скористаймося файлами, що визначаються як модифіковані відомі віруси

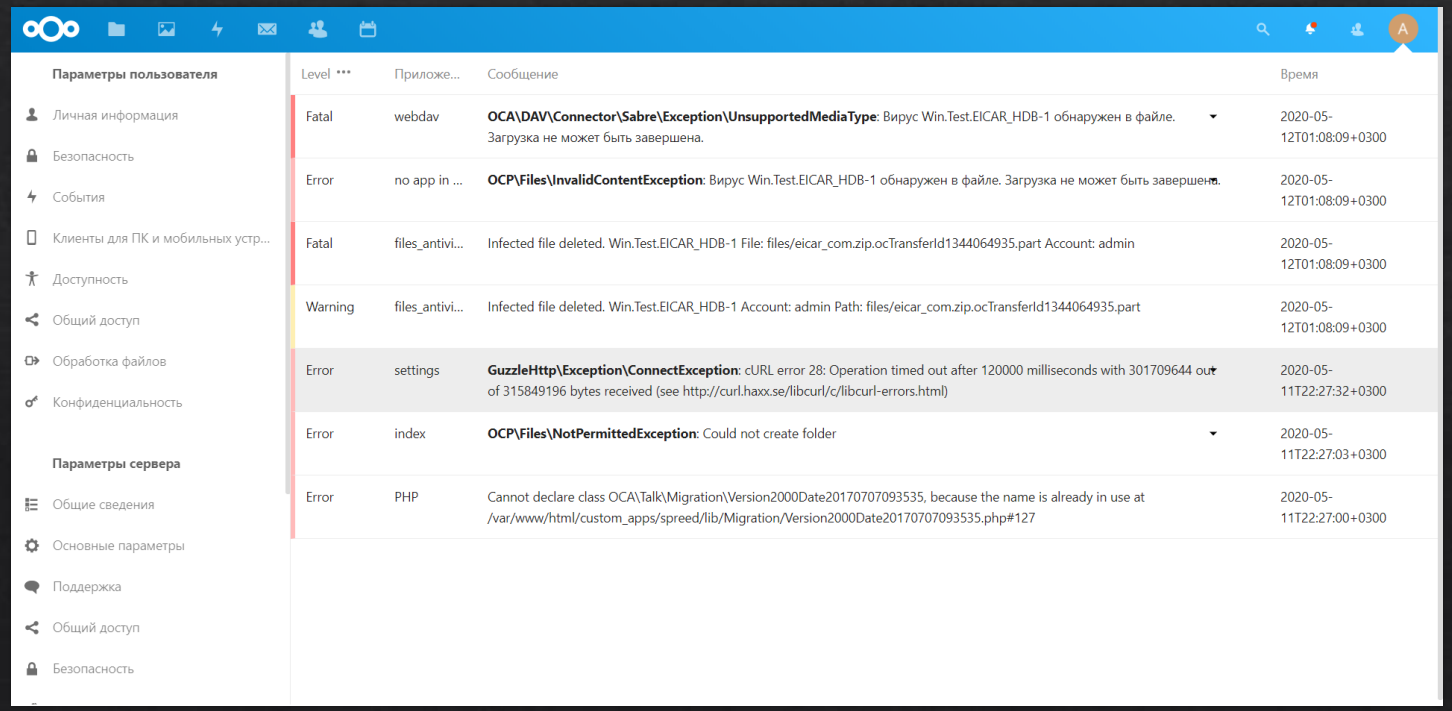
Тестування антивірусу



- CVE-2014-6332 – Вірус з подібною сигнатурою дозволяє віддаленим зловмисникам виконувати довільний код через створений веб-сайт, також відомий як «Уразливість виконання віддаленого коду Windows OLE Automation Array.
- Doc.Trojan.Class-37 – моделює поводження фішинг-трояна – файлом документа, який призначений виглядати законним, але насправді служить засобом доставки шкідливих програм.
- CVE-2010-3275 – у VideoLAN VLC Media Player до 1.1.8 дозволяє віддаленим зловмисникам виконувати довільний код через створену ширину у файлі AMV, пов’язану з "уразливістю вказівника".
- CVE-2015-5119 – в Linux дозволяє віддаленим зловмисникам виконувати довільний код або викликати відмову в обслуговуванні (пошкодження пам’яті) через створений Flash-вміст, який перекриває функцію valueOf.
- CVE-2012-4681 Багаторазові вразливості в компоненті середовища Java Runtime Environment (JRE) в Oracle Java SE 7 Update 6 і новіших версій дозволяють віддаленим зловмисникам виконувати довільний код через створений аплет, який обходить обмеження.

Під час спроби завантажити вірус через вебінтерфейс отримуємо помилку, а процес завантаження переривається, через те що система виявила підозрілу сигнатуру і заблокувала процес.





У той самий час у системному журналі з’являється відповідний запис, який сигналізує про те, що додаток files_antivirus знайшов загрозу. Також він повідомляє тип вірусу, час спроби завантаження, шлях завантаження та ім’я користувача який почав процес завантаження.

Висновки

- Проведено аналіз і складено перелік наявних вразливостей технології контейнеризації та способів їх вирішення.
- На основі аналізу пропозицій ринку та тестування вибрано антивірусне програмне забезпечення, а саме ClamAV.
- Протестовано декілька варіантів встановлення та використання антивірусу з платформою Docker та сервісами NextCloud.
- У процесі дослідження складено compose файл з описом налаштувань всіх компонентів, необхідних для функціонування системи.
- Продемонстровано роботу антивірусного ПЗ інтегрованого у додаток NextCloud.

ПЕРСПЕКТИВИ ПОДАЛЬШОГО РОЗВИТКУ

- Впровадження сервісів NextCloud HUB у навчальний процес.
- Планування та організація структури каталогів.
- Розмежування прав користувачів та груп користувачів.
- Збільшення можливостей та захищення системи за рахунок сторонніх додатків, або створювати їх самостійно.
- Створення інтеграцій для автоматизації рутинних операцій.

ДЯКУЮ ЗА УВАГУ!