Требования ИСПД на основе Приказа ФСТЭК от 10.02.2013г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

Для 4 уровня защищенности:

|  |  |  |  |
| --- | --- | --- | --- |
| 1. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ) | | | |
| Условное обозначение и номер меры | Содержание мер по обеспечению безопасности персональных данных | Реализация | Комментарий |
| ИАФ.1 | Идентификация и аутентификация пользователей, являющихся работниками оператора | + | При входе в приложение запрашиваются логин и пароль |
| ИАФ.3 | Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов | - | Не ведётся учёт идентификаторов, возможно повторное использование и даже дублирование |
| ИАФ.4 | Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации | - | Нет возможности установления характеристик пароля.  Нет возможности блокировать учётную запись или сменить на ней пароль. |
| ИАФ.5 | Защита обратной связи при вводе аутентификационной информации | - | При вводе пароля он отображается в открытом виде  Использование HTTP предполагает передачу данных в открытом виде, что не приемлемо в принципе  Запрос входа из Бурпа: login=alex&password=alex |
| ИАФ.6 | Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей) | - | Нет разделения на внешних и внутренних пользователей.  Тем более про использование ЕСИА |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. Управление доступом субъектов доступа к объектам доступа (УПД) | | | |
| УПД.1 | Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей | - | Нет временных УЗ  Нет групп УЗ  Нет верификации данных  Нет блокирования/активации УЗ  Нет корректировки УЗ  И все другие пункты |
| УПД.2 | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа | - | Есть разграничение по доступу к таблицам данных, но нет разграничения по правам доступа (RWX) |
| УПД.3 | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами | - | Нет фильтрации информационных потоков  Нет контроля маршрутов  Нет записи во временное хранилище  Во всяком случае внутри самого приложения среду запуска на данном этапе мы не исследуем |
| УПД.4 | Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы | - | Нет разграничения доступа, администраторы имеют доступ к содержимому ПДн |
| УПД.5 | Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы | - | Нет разграничения по чтению/записи, админы имеют полный доступ. |
| УПД.6 | Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) | - | Ограничения нет, можно брутить сколько угодно |
| УПД.13 | Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети | - | Нет фильтрации трафика, HTTP, нет мониторинга |
| УПД.14 | Регламентация и контроль использования в информационной системе технологий беспроводного доступа | - | Контроля маршрутов нет, разграничения прав пользователей нет |
| УПД.15 | Регламентация и контроль использования в информационной системе мобильных технических средств | - | Приложение не отслеживает использование в системе технических средств |
| УПД.16 | Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) | + | Нет API – нет взаимодействия. Полный запрет – тоже управление |

Уязвимости.

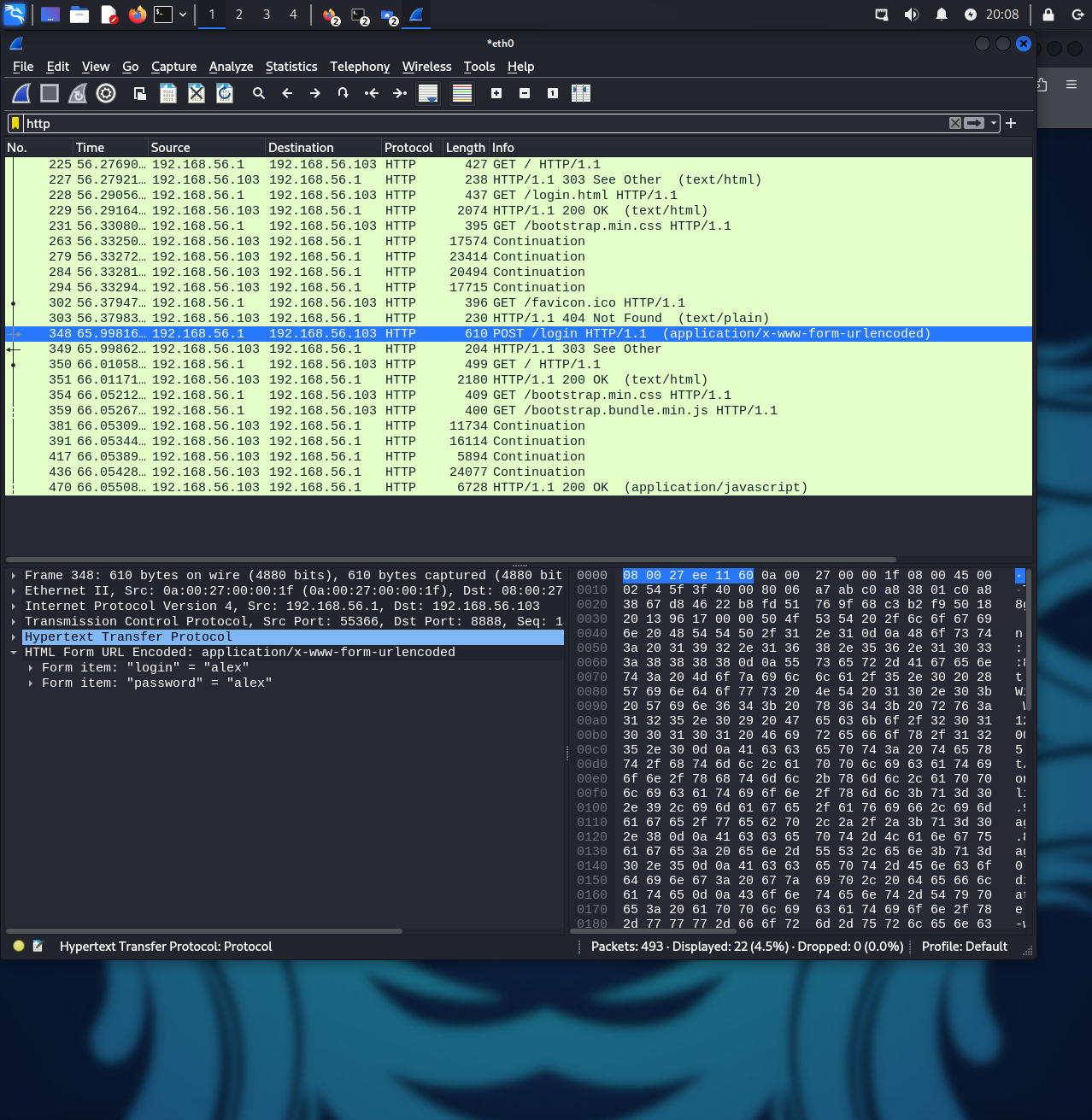
1. CWE-319: Cleartext Transmission of Sensitive Information

На вэб сервере не используется шифрование HTTPS. Данные для входа логин/пароль передаются в открытом виде.

Для эксплуатации запускаю ВайрШарк в Кали на интерфейс в сети с приложением.

На хостовой машине ввожу логин/пароль в приложении.

В трафике по фильтру HTTP вижу POST запрос на /login и там, ожидаемо, вижу те самые открытые логин/пароль.

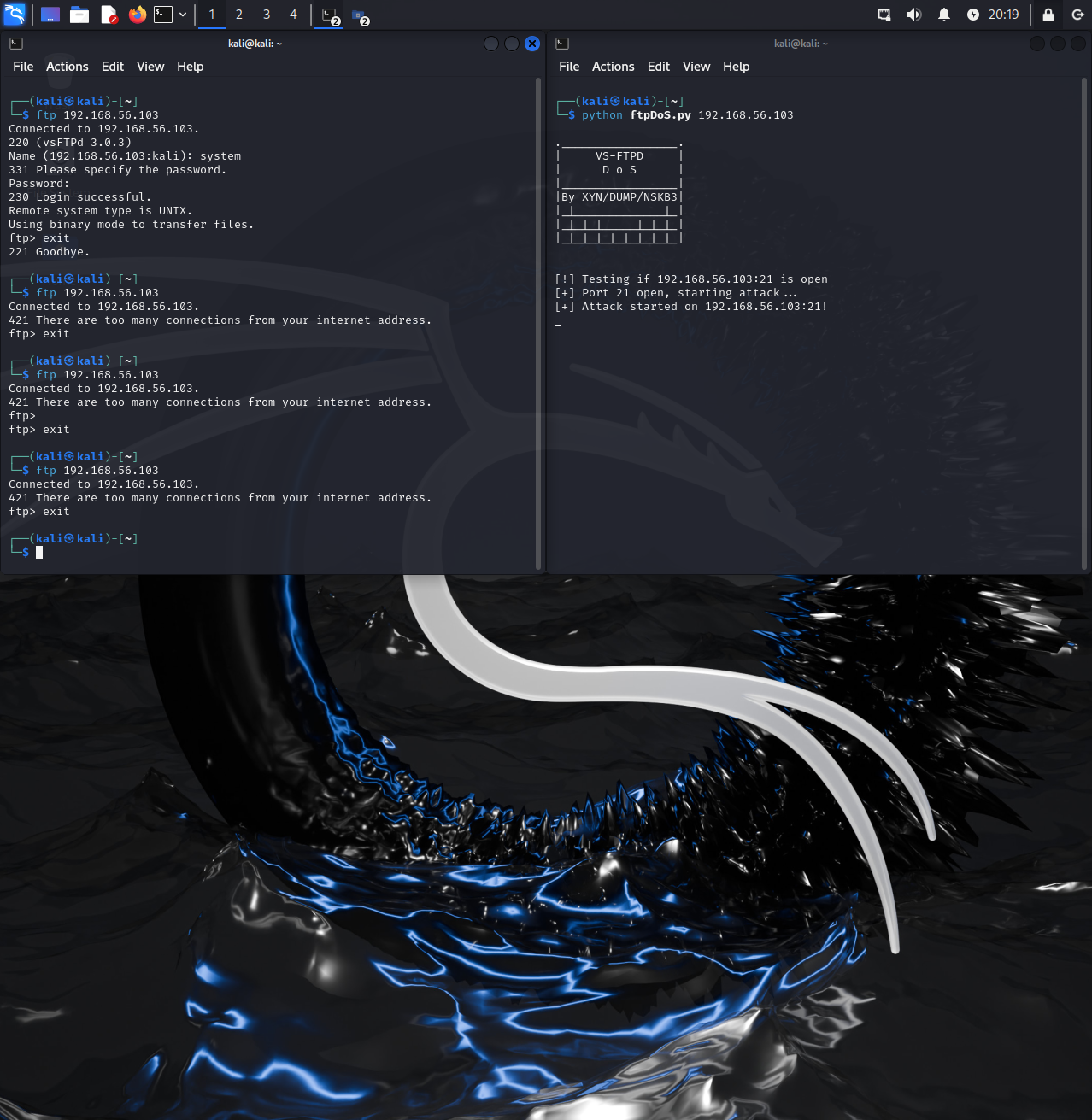


1. EDB-ID:49719

Сканируем НМапом, находим версию vsftpd 3.0.3 далее в интернете находим уязвимость к Remote Denial of Service по средствам эксплойта.

Качаем эксплой с <https://www.exploit-db.com/exploits/49719> и запускаем с параметром IP адреса атакуемой машины.

Видим, что до атаки удалось подключиться, а после начала не удается, так как слишком много подключений. Работа FTP сервера остановлена, хотя приложение продолжает работать.



1. Уязвимость IDOR (Insecure Direct Object Reference)

Не работает(

