|  |  |  |
| --- | --- | --- |
|  |  |  |
| МИНОБРНАУКИ РОССИИ | | |
| Федеральное государственное бюджетное образовательное учреждение  высшего образования  **«МИРЭА – Российский технологический университет»**  **РТУ МИРЭА** | | |
| ИКБ направление «Киберразведка и противодействие угрозам с применением технологий искусственного интеллекта» 10.04.01  Кафедра КБ-4 «Интеллектуальные системы информационной безопасности» | | |
|  |  |  |

Практическая работа 3\_2

по дисциплине

«Управление информационной безопасностью»

Группа:

ББМО-02-22

Выполнил:

Шитов А.В.

Проверил:

Пимонов Р.В.

Москва 2023

# **1 Развёртывание и настройка**

**1.1 Damn Vulnerable Linux (DVL)**

Произведём установку DVL. Для этого создадим новую ВМ (средство виртуализации VMware Workstation Pro 17)

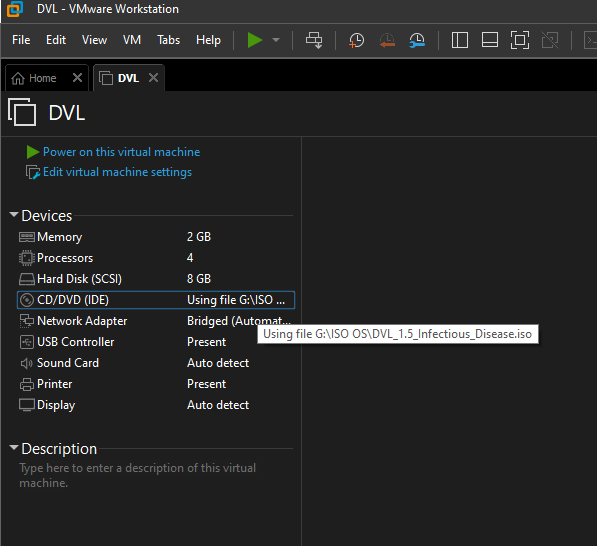


Рисунок 1 – ВМ с DVL

Запускаем и переходим к настройке системы (рисунок 2-4)

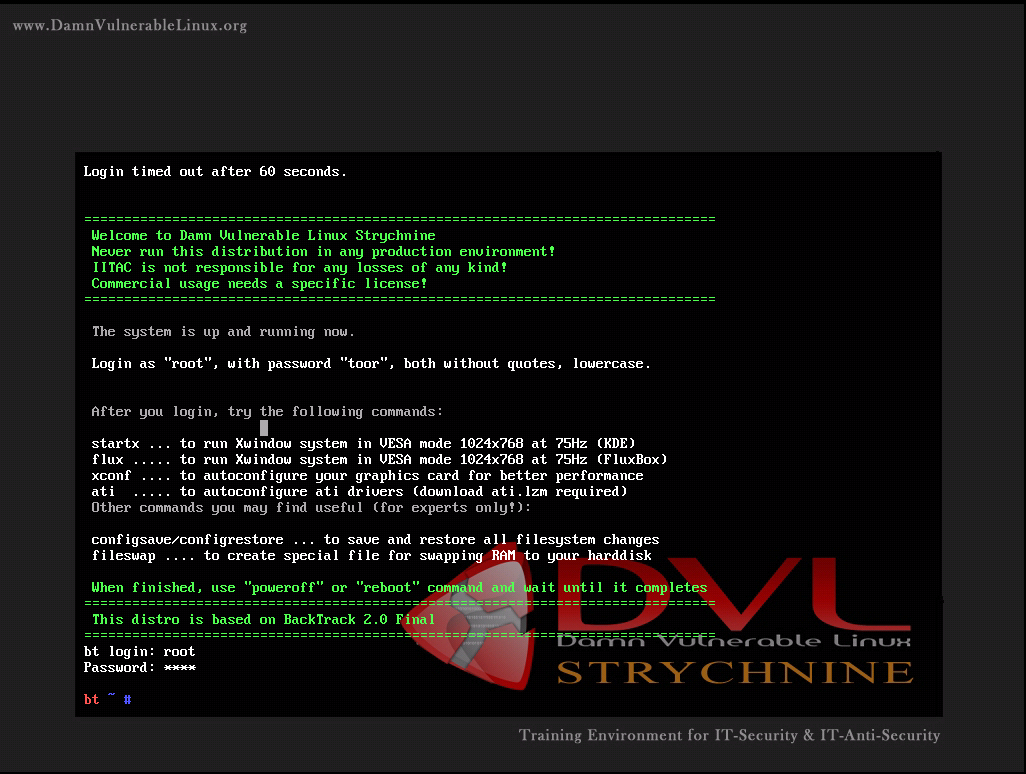


Рисунок 2 - Авторизация (логин root, пароль toor)



Рисунок 3 – Создание разделов при помощи fdisk



Рисунок 4 – Форматирование диска под файловую систему ext3

Далее при помощи последовательности команд необходимо произвести монтирование диска и запуск системы:

* mkdir /mnt/dvl
* mount /dev/sda1 /mnt/dvl
* startx

После выполнения вышеуказанных действий попадаем в графическую оболочку DVL



Рисунок 5 – Графическая оболочка DVL

Для полной установки необходимо запустить BackTrack Installer и выбрать версию Real (рисунок 6-7)

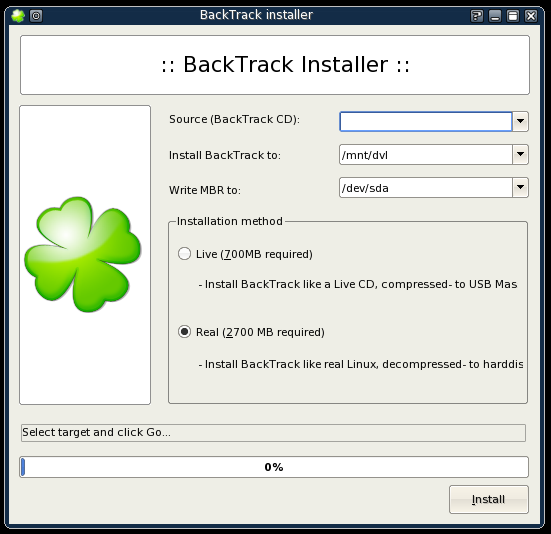


Рисунок 6 – Запуск установки

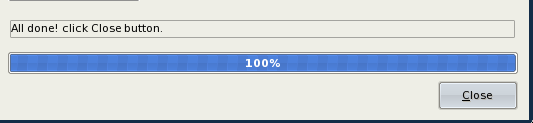


Рисунок 7 – Успешное завершение установки

Далее необходимо узнать IP адрес при помощи команды ip a, который будет использоваться в дальнейшей работе

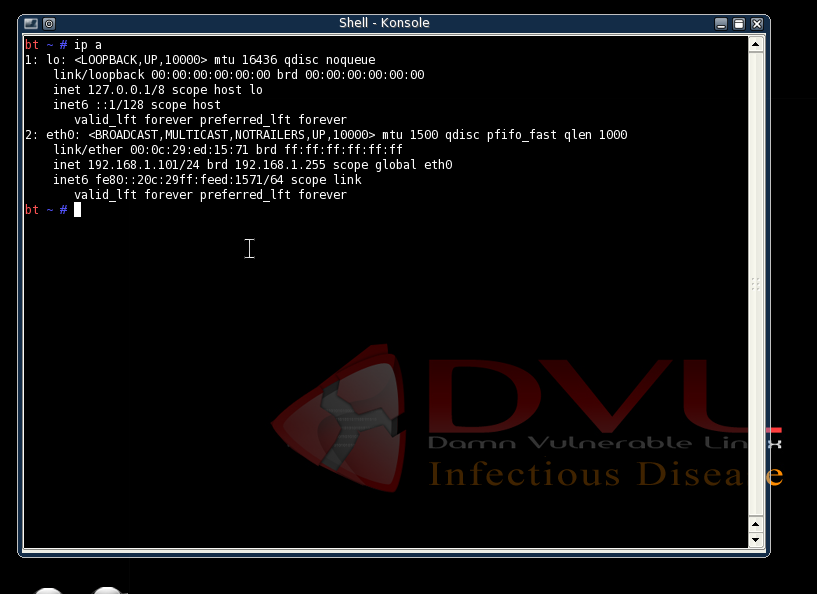


Рисунок 8 – IP адрес

**1.2 Kali linux**

Создадим ВМ с Kali Linux

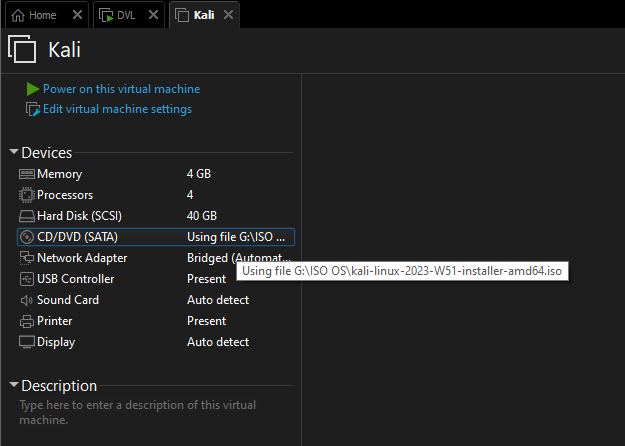


Рисунок 9 – ВМ Kali Linux

После установки необходимо авторизоваться и проверить соединение между Kali и DVL (рисунок 10-11)



Рисунок 10 - Авторизация

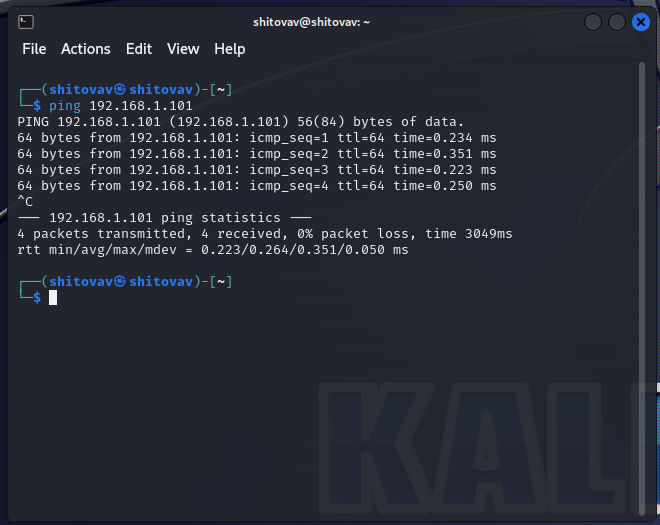


Рисунок 11 – Проверка соединения

# **2 Задачи по анализу защищенности**

**2.1 Сканирование портов и сервисов на DVL с использованием Nmap**

Проверим открытые порты DVL с помощью Nmap

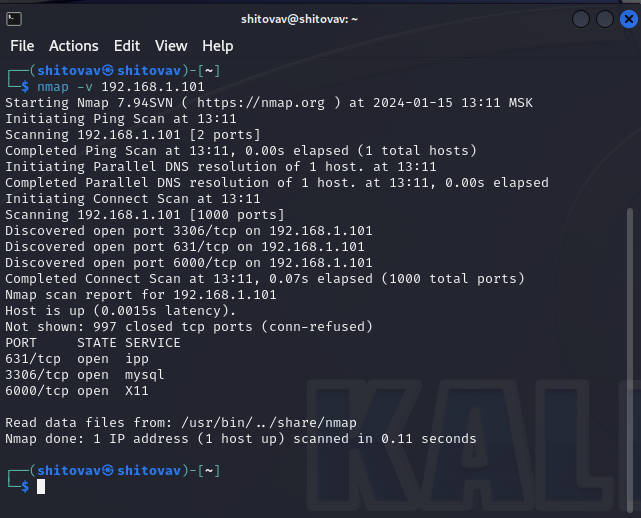


Рисунок 12 – Результат сканирования

Список открытых портов:

* 631/tcp – IPP (протокол для передачи документов на печать)
* 3306 - MySQL
* 6000 – x11 (протокол для связи клиент-сервер)

Для изучения уязвимостей можно воспользоваться скриптом vulners (рисунок 13-15)

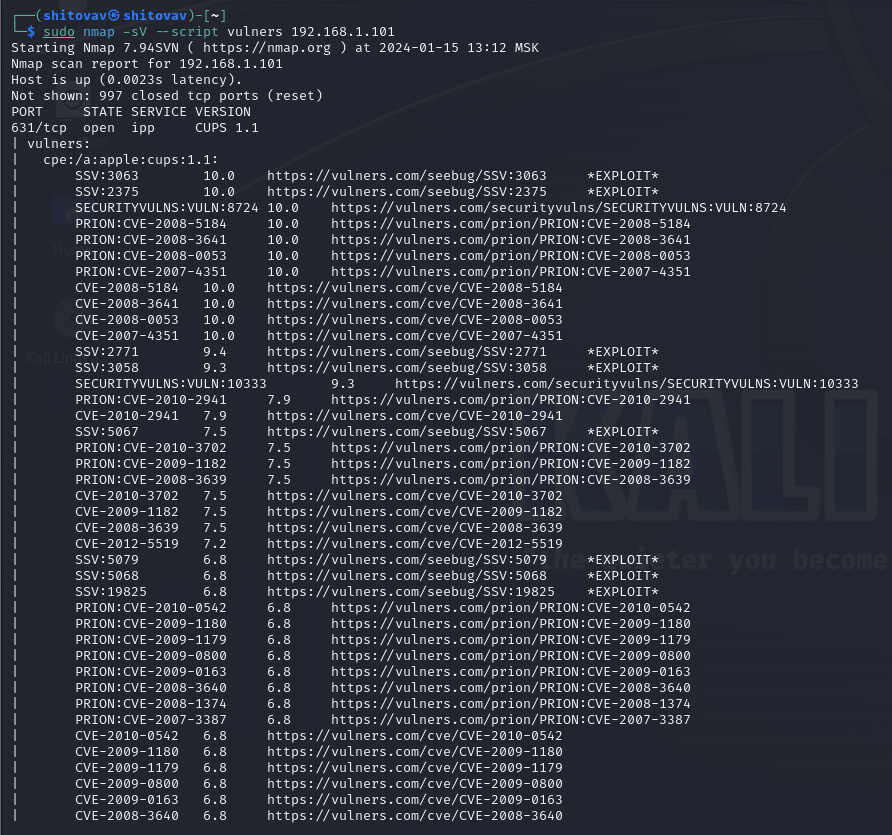


Рисунок 13 – Запуск скрипта

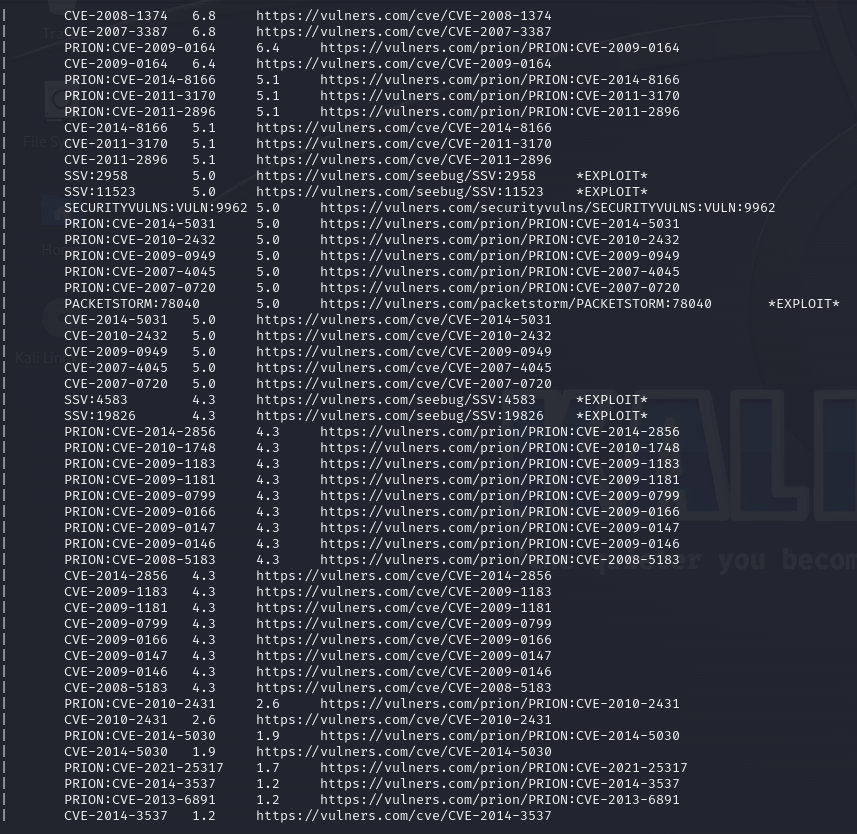


Рисунок 14 – Продолжение списка



Рисунок 15 – Окончание работы скрипта

Список уязвимостей, найденный с помощью Nmap достаточно большой

**2.2 Сканирование портов и сервисов на DVL с использованием OpenVAS**

Проведём установку OpenVAS (GVM), для проверки корректности установки используем gvm-check-setup (рисунок 16-17).

****

Рисунок 16 – Проверка установки

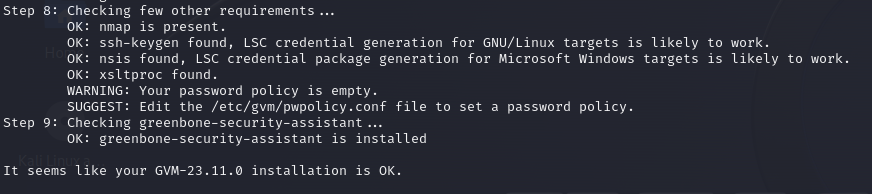
****

Рисунок 17 – Проверка успешно завершена

Далее необходимо обновить фиды, для этого используем greenbone feed sync.

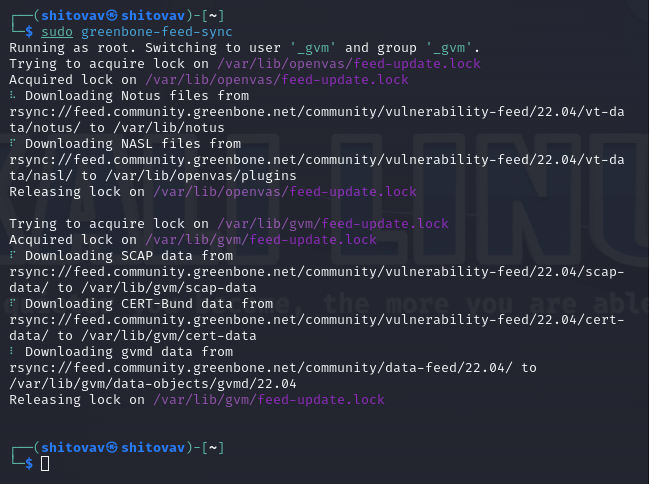
****

Рисунок 18 – Обновление источников

Согласно выполненной команде можно сделать вывод, что обновление завершено успешно. Переходим на 127.0.0.1:9293, логинимся через учетку админа (логин и пароль создаются автоматически при установке), однако при сканировании получаем ошибку, что не найдена конфигурация.

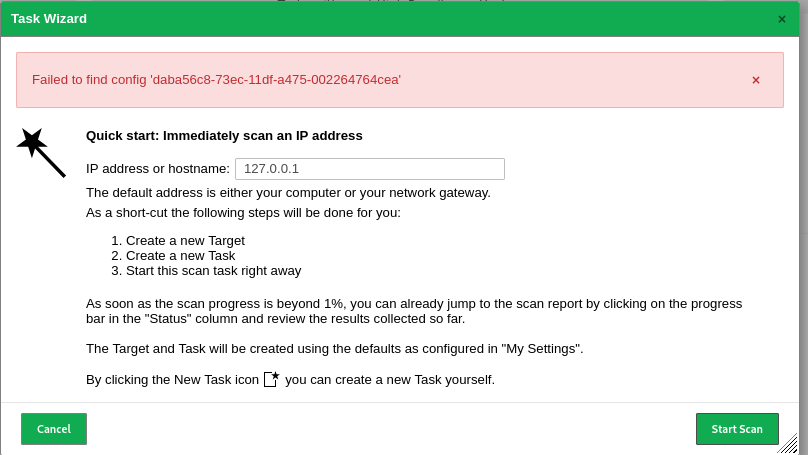
****

Рисунок 19 – Ошибка при запуске скана

Вынюхиваем дальше. Во вкладке administration – подпункт feed status замечаем интересную деталь: 3 источника из 4 находятся в статусе update in progress, однако обновление фидов через команду greenbone-feed-sync, завершается успешно, без каких-либо ошибок, что говорит о некорректности работы скрипта обновления

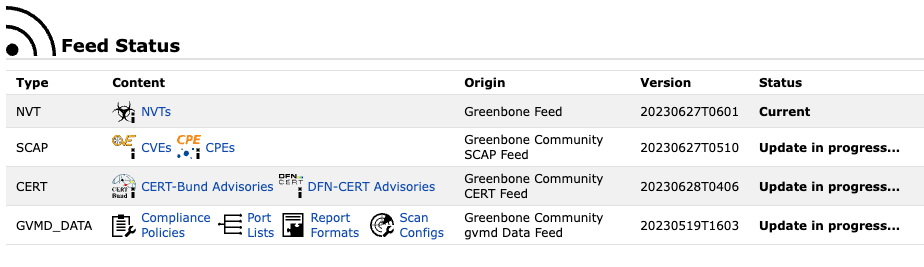
****

Рисунок 20 – Никогда такого не было и вот опять

Спустя множество попыток решения найдено не было, поэтому помогла ВМ одногруппника, на которой были установлены все необходимые обновления и сканирование можно было реализовать. Однако, имя пользователя изменилось с shitovav на kali. IP адрес DVL, разумеется, остался прежним.

Составляем задачу на сканирование, нажав на волшебную палочку (task wizard) на вкладке scans

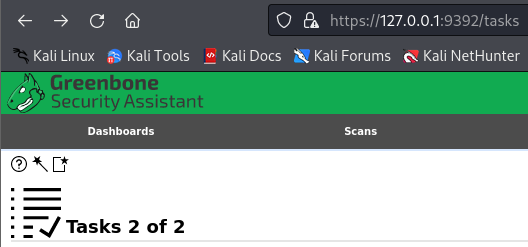


Рисунок 21 – Вкладка scans

Запускаем сканирование. Для этого нужно указать IP адрес DVL в окне task wizard и нажать start scan.

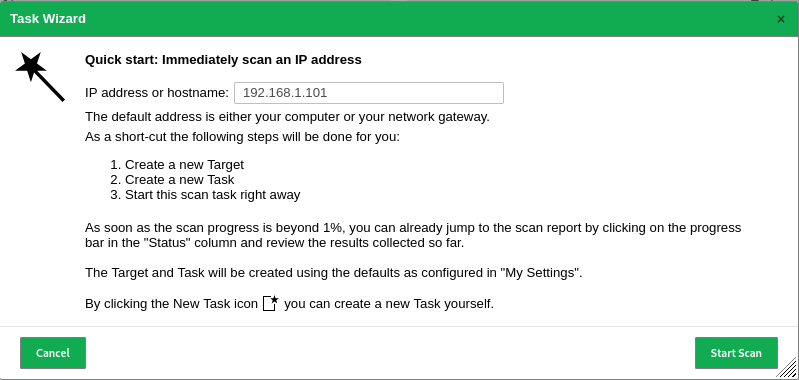
****

Рисунок 22 – Параметры сканирования

Результат сканирования отображён на рисунках 23-24

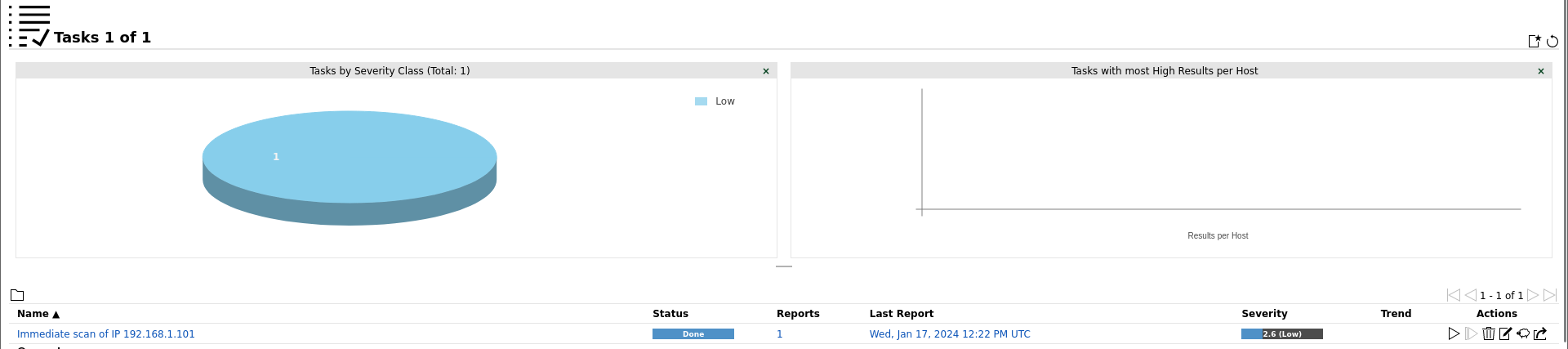
****

Рисунок 23 – Результат сканирования

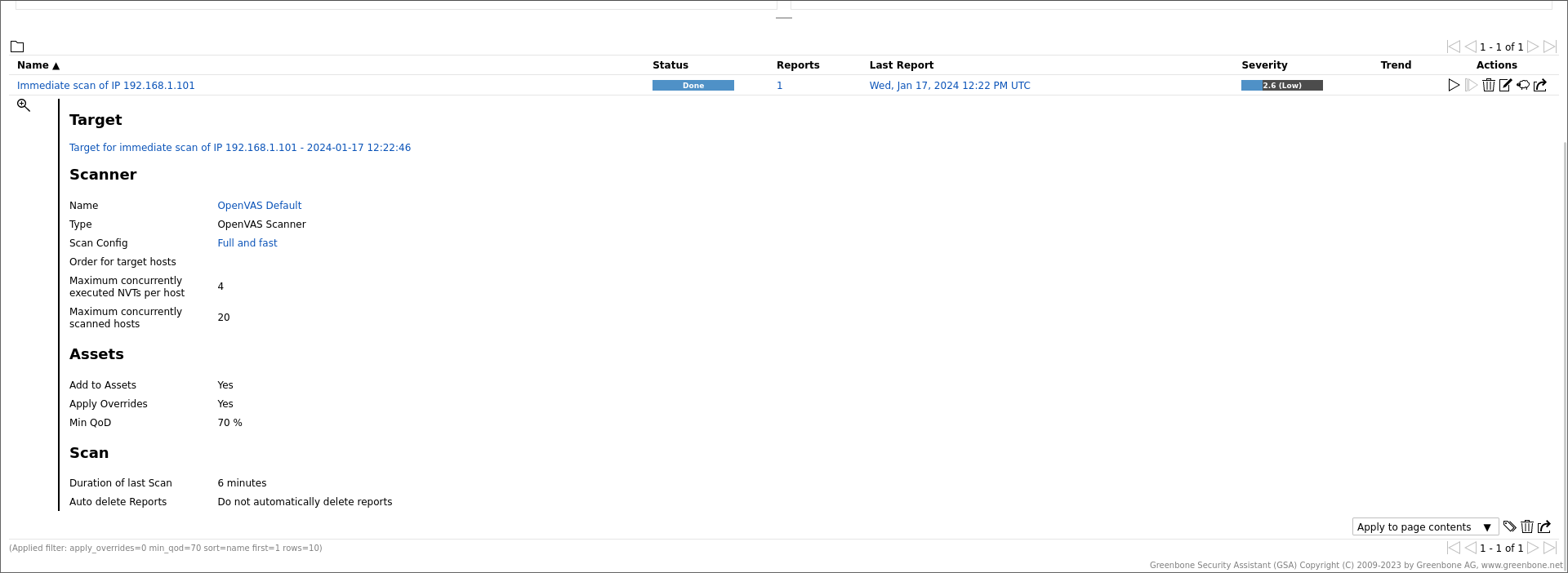
****

Рисунок 24 – Результат сканирования

В отличии от Nmap сканирование показало, что уязвимостей не обнаружено. Запустим несколько сервисов, которые удобно расположены в левом верхнем углу рабочего стола DVL (HTTPD, SSH, Mysql, PHPMyAd)

****

Рисунок 25 – Сервисы DVL

Повторим сканирование

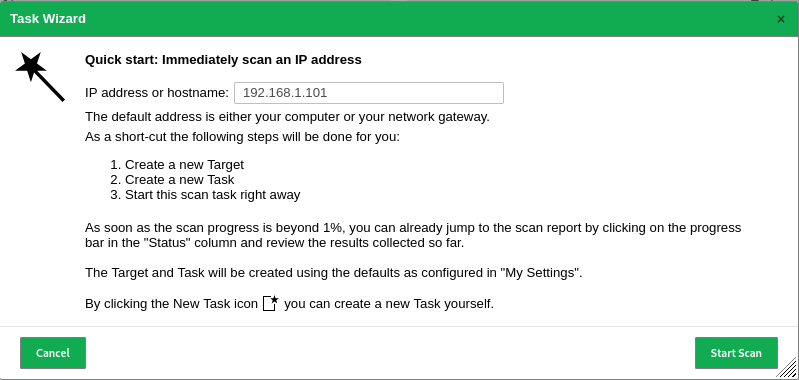
****

Рисунок 26 – Вторая задача на сканирование

Результат сканирования отображён на рисунке 27

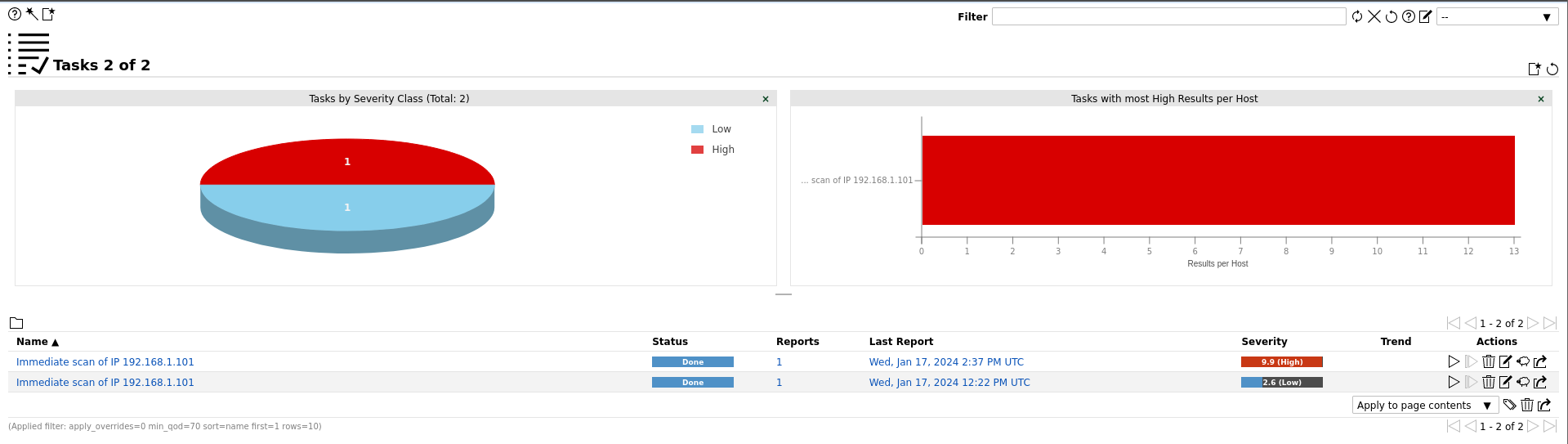
****

Рисунок 27 – Результат сканирования

Повторное сканирование обнаружило значительно больше уязвимостей. Рассмотрим критические, их было выявлено 13.

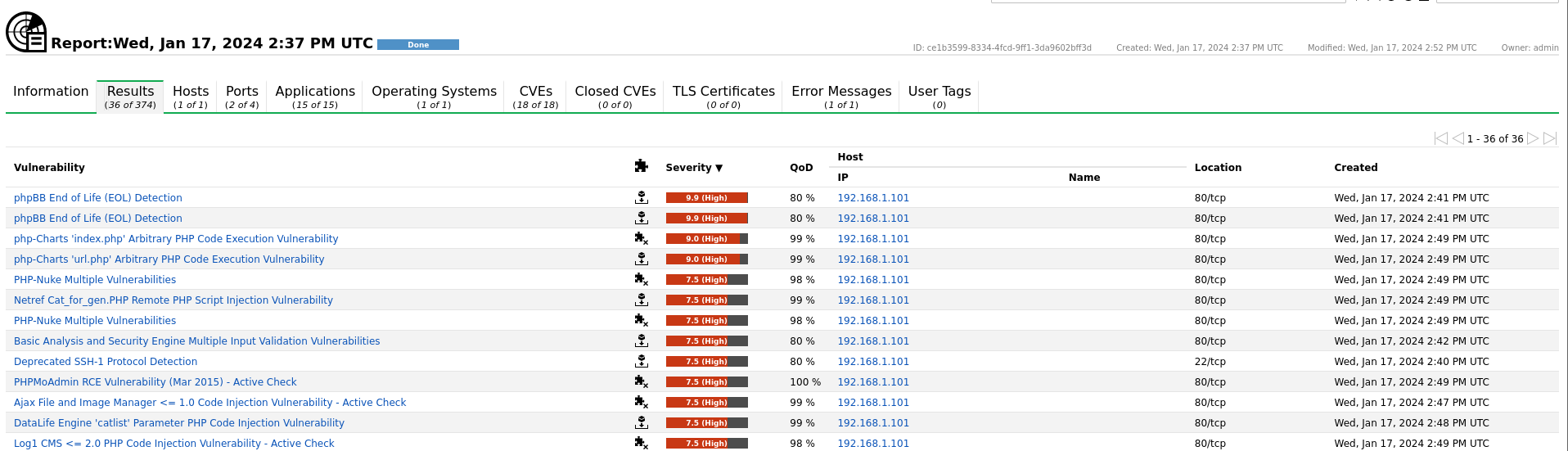
****

Рисунок 28 – Список уязвимостей

В таблице 1 приведён обзор найденных критических уязвимостей.

Таблица 1 – Критические уязвимости

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № | Название | Описание | Влияние | Исправление | CVE |
| 1 | phpBB End of Life (EOL) Detection | Установленная на удаленном хосте версия phpBB достигла окончания срока службы (EOL) и больше не должна использоваться. | Устаревшая версия phpBB не получает обновлений безопасности от производителя. Неисправленные уязвимости безопасности могут быть использованы злоумышленником для нарушения безопасности этого узла. | Обновите phpBB на удаленном хосте до поддерживаемой версии. | https://www.phpbb.com/community/viewtopic.php?t=2373956 |
| 2 | phpBB End of Life (EOL) Detection | Аналогично №1 | | | |
| 3 | php-Charts 'index.php' Arbitrary PHP Code Execution Vulnerability | php-Charts 1.0 является уязвимым. Другие версии также могут быть затронуты. | Злоумышленник может использовать эту проблему для выполнения произвольного PHP-кода  в контексте затронутого приложения. | Обновление до более новой версии, отключение соответствующих функций, удаление продукта или замена его на другой. | http://www.securityfocus.com/bid/59987 |
| 4 | php-Charts 'url.php' Arbitrary PHP Code Execution Vulnerability | php-Charts 1.0 является уязвимым. Другие версии также могут быть затронуты. | Злоумышленник может использовать эту проблему для выполнения произвольного PHP-кода   в контексте веб-сервера. | Запрос на обновление информации от поставщика | http://www.securityfocus.com/bid/57448 |
| 5 | PHP-Nuke Multiple Vulnerabilities | PHP-Nuke подвержен многочисленным уязвимостям.  Множественные недостатки связаны с:   * Неправильной проверкой вводимых пользователем параметров 'chng\_uid', 'sender\_name' и 'sender\_email' в файлах 'admin.php' и 'modules.php' * Неправильная проверка вводимых пользователем данных для добавления учетных записей пользователей или предоставления административных привилегий в файле 'mainfile.php'. | Успешная эксплуатация позволит злоумышленнику выполнить произвольные SQL-команды, внедрить произвольный веб-скрипт или перехватить аутентификацию администраторов. | Обновление до более новой версии, отключение соответствующих функций, удаление продукта или замена его на другой. | CVE-2011-1480  CVE-2011-1481  CVE-2011-1482 |
| 6 | Netref Cat\_for\_gen.PHP Remote PHP Script Injection | В установленной версии Netref существует уязвимость, позволяющая удаленному злоумышленнику передать произвольный PHP-код скрипта через параметры 'ad', 'ad\_direct' и 'm\_for\_racine' скрипта 'cat\_for\_gen.php'. | Этот код будет выполнен на удаленном хосте под привилегиями идентификатора пользователя веб-сервера. | Обновление до Netref 4.3 или более поздней версии | CVE-2005-1222 |
| 7 | PHP-Nuke Multiple Vulnerabilities | Аналогично №5 | | | |
| 8 | Basic Analysis and Security Engine Multiple Input Validation Vulnerabilities | Basic Analysis and Security Engine (BASE) подвержен многочисленным уязвимостям, связанным с проверкой правильности ввода, поскольку не обеспечивает адекватную проверку вводимых пользователем данных. Эти уязвимости включают в себя проблему SQL-инъекции, проблему межсайтового скриптинга и проблему включения локальных файлов. | Эксплуатация этих проблем может позволить злоумышленнику украсть учетные данные аутентификации на основе cookie, просмотреть и выполнить локальные файлы в контексте веб-сервера, скомпрометировать приложение, получить доступ к данным или изменить их, а также использовать скрытые уязвимости в базовой базе данных. Возможны и другие атаки. | Обновление | CVE-2009-4590  CVE-2009-4591  CVE-2009-4592  CVE-2009-4837  CVE-2009-4838  CVE-2009-4839 |
| 9 | Deprecated SSH-1 Protocol Detection | Хост работает под управлением SSH и предоставляет/принимает одну или несколько устаревших версий протокола SSH, которые имеют известные криптографические недостатки. | Успешная эксплуатация может позволить удаленным злоумышленникам обойти ограничения безопасности, получить открытый ключ хоста клиента при попытке подключения и использовать его для открытия и аутентификации SSH-сессии на другом сервере с тем же доступом. | Переконфигурация службы SSH так, чтобы она предоставляла/принимала только протокол SSH версии SSH-2 | CVE-2001-0361  CVE-2001-0572  CVE-2001-1473 |
| 10 | PHPMoAdmin RCE Vulnerability (Mar 2015) - Active Check | PHPMoAdmin подвержен уязвимости удаленного выполнения кода (RCE), поскольку приложение не обеспечивает достаточной санации пользовательского ввода. | Эксплуатация этой проблемы позволит злоумышленникам выполнить произвольный код в контексте затронутого приложения. | Обновление до более новой версии, отключение соответствующих функций, удаление продукта или замена его на другой. | CVE-2015-2208 |
| 11 | Ajax File and Image Manager <= 1.0 Code Injection Vulnerability - Active Check | Злоумышленник может использовать эту проблему для внедрения и выполнения произвольного PHP-кода в контексте затронутого приложения. | Это может способствовать компрометации приложения и базовой системы. Возможны и другие атаки. | Обновление до более новой версии, отключение соответствующих функций, удаление продукта или замена его на другой. | CVE-2011-4825 |
| 12 | DataLife Engine 'catlist' Parameter PHP Code Injection Vulnerability | DataLife Engine подвержен уязвимости удаленной инъекции кода PHP. Уязвимым является DataLife Engine 9.7. Другие версии также могут быть затронуты. | Злоумышленник может использовать эту проблему для внедрения и выполнения произвольного PHP  код в контексте затронутого приложения. Это может способствовать  компрометации приложения и базовой системы. Другие атаки  также возможны. | Обновление | CVE-2013-1412 |
| 13 | Log1 CMS <= 2.0 PHP Code Injection Vulnerability - Active Check | Log1 CMS подвержена уязвимости удаленной инъекции PHP-кода. | Внедрение и выполнение произвольного PHP-кода в контексте затронутого приложения. Это может способствовать компрометации приложения и базовой системы, возможны и другие атаки. | Обновление до более новой версии, отключение соответствующих функций, удаление продукта или замена его на другой. | CVE-2011-4825 |

**2.3 Сходства и различия инструментов Nmap и OpenVAS (GVM)**

Сходства: OpenVAS и Nmap оба являются инструментами для сканирования уязвимостей. Оба инструмента также предоставляют возможность сканирования сети для выявления уязвимостей и открытых портов на устройствах.

Различия: OpenVAS - это инструмент для сканирования уязвимостей в сети, который предоставляет отчеты о найденных уязвимостях, и может предложить рекомендации по их устранению. Nmap, с другой стороны, это инструмент для сканирования сети, который преимущественно сфокусирован на определении активных узлов, открытых портов, а также определении операционных систем и служб на удаленных узлах.

Сферы применения: OpenVAS идеально подходит для сканирования и анализа уязвимостей в сетях. Зачастую его используют в предприятиях для регулярного сканирования сетевых устройств и серверов на предмет уязвимостей, а также для обеспечения соответствия стандартам безопасности. Он также хорошо подходит для аудита сети и оценки безопасности.

Nmap, с другой стороны, является универсальным инструментом для сетевого сканирования. Он может использоваться для обнаружения устройств в сети, проверки открытых портов, определения операционных систем и версий служб (что делает его прекрасным выбором для анализа сети и поиска уязвимостей), но не предоставляет такую детализированную информацию о конкретных уязвимостях, как OpenVAS.

Для сканирования уязвимостей OpenVAS потребуется для более глубокого анализа, а Nmap нужен, чтобы получить общий обзор состояния сети, однако наилучшим выбором будет комбинированное использование этих средств.

**3 Анализ безопасности системы с помощью Metasploit**

Используем Metasploit для эксплуатации одной из уязвимостей. Проведём запуск инструмента с помощью sudo msfdb init && msfconsole (установка не треуется, так как данная утилита встроена в Kali Linux).



Рисунок 29 – Запуск Metasploit

Выбор пал на уязвимость Log1 CMS <= 2.0 PHP Code Injection Vulnerability - Active Check (таблица 1 пункт 13). В OpenVAS был отображён адрес, по которому была обнаружена данная уязвимости (Vulnerable URL: http://192.168.1.101/info/admin/libraries/ajaxfilemanager/inc/data.php), попробуем найти что-то по словам ajax file manager.

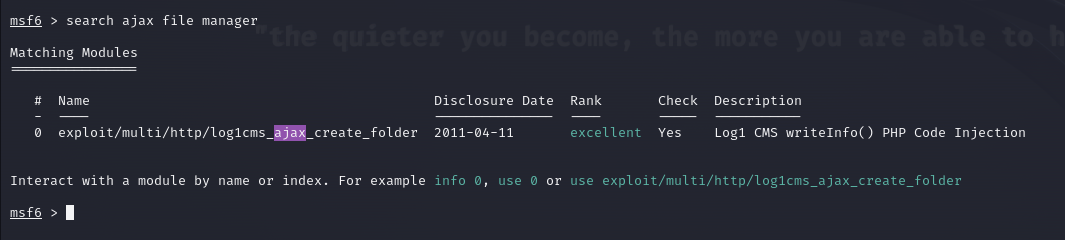


Рисунок 30 – Результаты поиска

Посмотрим более подробную информацию о модуле (рисунок 31-32)

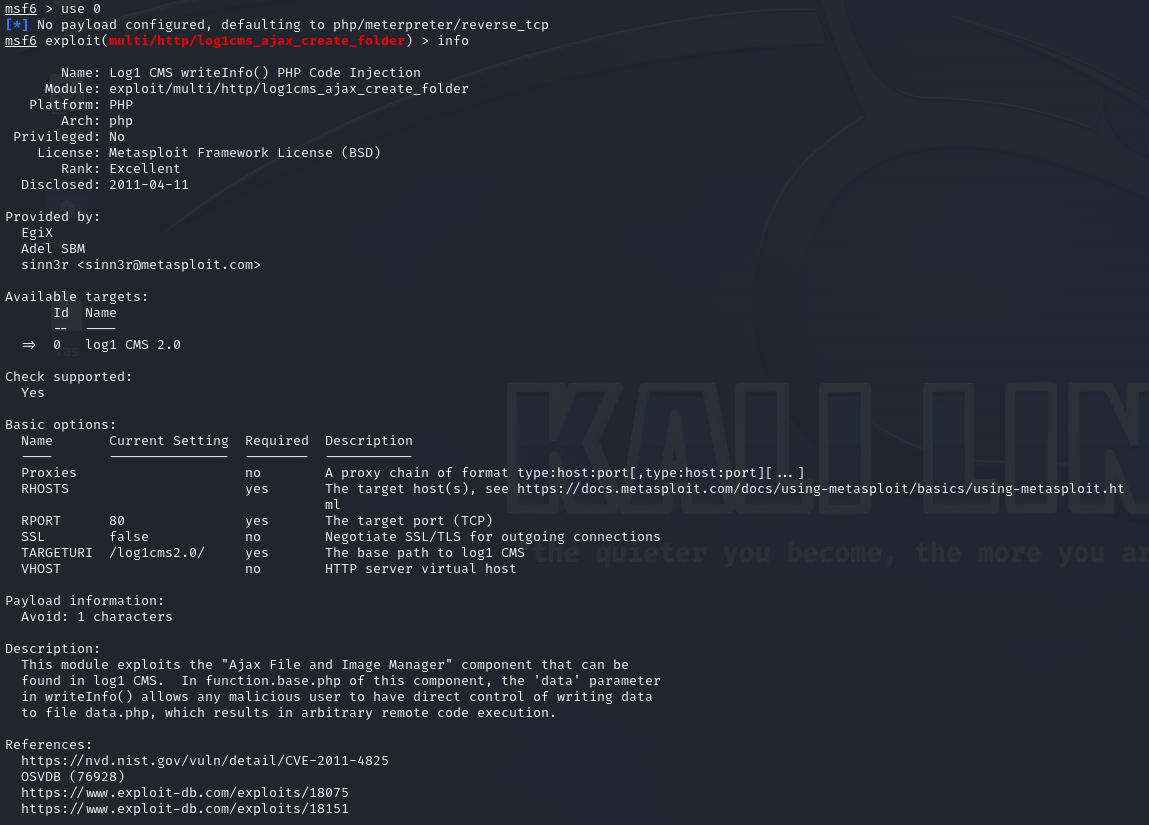


Рисунок 31 – Информация о модуле

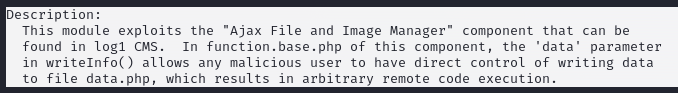


Рисунок 32 – Описание модуля

Согласно описанию, данный модуль использует компонент «Ajax File and Image Manager», который может быть найден в log1 CMS. В файле function.base.php этого компонента параметр 'data' в функции writeInfo() позволяет любому злоумышленнику получить прямой контроль над записью данных в файл data.php, что приводит к произвольному удаленному выполнению кода.

Укажем IP адрес DVL в качестве цели (RHOSTS) и запускаем скрипт

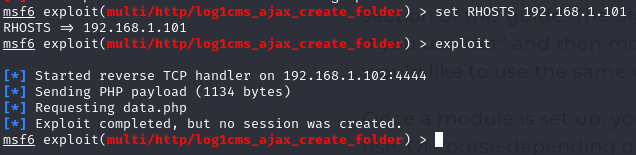


Рисунок 33 – Запуск скрипта

Эксплуатация уязвимости проведена успешно, было передано 1134 байта данных и получен доступ к файлу data.php.

Рекомендации по исправлению: прямого решения нет, поэтому единственное решение использовать более новую версию Log1 CMS, в которой данная уязвимости устранена.

# **Вывод**

Были установлены ВМ Kali Linux и Damn Vulnerable Linux (DVL)

Проведено сканирование портов и сервисов на DVL с помощью Nmap и OpenVAS. Также выполнен анализ результатов сканирования: выявлены критические уязвимости, предложены меры по их устранению.

Проведён сравнительный анализ инструментов Nmap и OpenVAS

Был использован для Metasploit для эксплуатации уязвимости Log1 CMS <= 2.0 PHP Code Injection Vulnerability - Active Check, проведён анализ результатов и сформированы рекомендации по устранению уязвимости.

Поставленные задачи выполнены в полном объёме.