

Индивидуальный проект 2

Информационная безопасность

Волчок Кристина Александровна НПМбд-02-21

25 сентября 2024

Российский университет дружбы народов, Москва, Россия

Информация

- Волчок Кристина Александровна, студентка кафедры прикладной информатики и теории вероятностей
- Российский университет дружбы народов
- [1032215007@rudn.ru]

Вводная часть

Hydra — это инструмент, широко применяемый для подбора логинов и паролей к различным сервисам. Он поддерживает множество протоколов, включая HTTP, FTP, SSH и другие, что делает его универсальным решением для тестирования безопасности систем. Одним из основных его применений является подбор паролей методом грубой силы (brute-force). ##

Актуальность

Актуальность использования Hydra заключается в необходимости обеспечения безопасности информационных систем. Современные веб-приложения часто становятся целями атак, поэтому регулярное тестирование безопасности, в том числе подбор паролей, является критически важным для предотвращения несанкционированного доступа. Hydra предоставляет возможность автоматизации этих проверок.

Объектом исследования является веб-приложение с HTML-формой авторизации, а предметом исследования — методы подбора пароля с использованием Hydra. Исследование сосредоточено на уязвимостях в системе аутентификации, которые могут быть выявлены через атаку методом грубой силы.

Цель работы — продемонстрировать использование утилиты Hydra для автоматизированного подбора пароля к веб-форме авторизации через метод POST. Задачами являются установка и настройка Hydra, запуск подбора паролей, а также анализ результатов для выявления уязвимостей в системе.

Для выполнения работы используется сервер с IP-адресом 178.72.90.181, предоставляющий сервис HTTP на 80 порту. Для авторизации используется HTML-форма, отправляющая POST-запрос с параметрами `username=root` и `password=test_password`. В случае неудачной попытки аутентификации сервер возвращает сообщение об ошибке. Используемая команда для подбора пароля выглядит следующим образом:

```
hydra -l root -P  
~/pass_lists/dedik_passes.txt -o ./hydra_result.log -f -V -s 80 178.72.90.181 http-post-form  
"/cgi-bin/luci:username=USER&password=PASS:Invalid username"
```


Hydra показала свою эффективность в автоматизированном подборе паролей через веб-форму авторизации. Это мощный инструмент, который должен использоваться для выявления уязвимостей в системах безопасности и повышения уровня защиты веб-приложений.

- Hydra успешно подбирает пароли при правильной настройке и наличии подходящих словарей.
- Важно понимать процесс: сервер возвращает сообщение об ошибке при неудачных попытках, и его отсутствие может означать успешную авторизацию.
- Логическая структура между слайдами: от описания инструмента к выполнению задания и анализу результата.
- Результат — найденный пароль — помогает выявить уязвимости и укрепить защиту.

- Главный вывод: тестирование с помощью Hydra выявляет слабые места, что помогает своевременно усилить безопасность системы.

Рекомендации

- Используйте сложные пароли и ограничьте количество попыток входа.
- Внедрите двухфакторную аутентификацию.
- Регулярно обновляйте систему безопасности и отслеживайте подозрительные попытки входа.