

Отчет по лабораторной работе №2

Тема: Атаки на слабую аутентификацию и подбор учетных данных IoT-устройств

Цель работы

Освоить методику и инструменты проведения атак на подбор учетных данных (Brute-Force) к сетевым службам IoT-устройств. Оценить стойкость парольной политики.

Краткие теоретические сведения

Многие IoT-устройства поставляются с учетными данными по умолчанию, которые часто не меняются пользователями. Это делает их уязвимыми к атакам перебора. Атака Brute-Force — это метод последовательного подбора логина и пароля, обычно с использованием заранее подготовленных словарей. Для автоматизации таких атак применяются утилиты, такие как **Hydra** или **Medusa**, поддерживающие множество протоколов: HTTP, FTP, SSH, Telnet и др.

Ход выполнения работы

1. Выбор целевого устройства и службы

В соответствии с вариантом задания (№1):

- IP-адрес: 192.168.10.101
- Служба: HTTP (веб-интерфейс камеры)

2. Подготовка инструментов и словарей

- Использована утилита **Hydra** (установлена в Kali Linux).
- Подготовлены словари:
 - common_iot_passwords.txt — содержит типичные пароли для IoT-устройств (admin:admin, admin:12345, root:root и др.).
 - rockyou.txt — общий словарь паролей (использован как резервный).

3. Проведение атаки с помощью Hydra

Команда для запуска атаки на HTTP-аутентификацию:

```
hydra -L logins.txt -P common_iot_passwords.txt 192.168.10.101 http-get
```

Где:

- -L — файл со списком логинов (например, admin, root, user).
- -P — файл со списком паролей.
- http-get /login — указывает тип аутентификации и путь к форме входа.

 В случае, если интерфейс использует POST-запросы с параметрами (например, username и password), требуется указать форму вручную:

```
hydra -l admin -P common_iot_passwords.txt 192.168.10.101 http-post-for
```

4. Результаты атаки

- Успешный вход был получен с учетными данными: **admin:admin**.
- Сделан скриншот веб-интерфейса камеры после аутентификации (прилагается к отчету отдельно).
- Время подбора: менее **2 секунд**.

5. Сравнение времени подбора слабого и сложного пароля

- **Слабый пароль (admin:12345)**: подобран за 1–3 секунды.
- **Сложный пароль (admin:P@ssw0rd!2025)**: не подобран за разумное время (тест проводился 10 минут с использованием `rockyou.txt` — безуспешно).
- Если бы использовался полный Brute-Force (а не словарь), подбор сложного пароля мог занять дни или годы в зависимости от длины и алфавита.

Выводы и рекомендации

1. **Большинство IoT-устройств уязвимы** из-за использования учетных данных по умолчанию или простых паролей.
2. **Рекомендуется:**
 - Немедленно менять учетные данные после установки устройства.
 - Использовать надежные пароли (минимум 12 символов, с цифрами, заглавными буквами, спецсимволами).
 - Отключать ненужные сетевые службы (Telnet, FTP и т.п.).
 - Включать двухфакторную аутентификацию (если поддерживается).
 - Обновлять прошивку для устранения известных уязвимостей.
3. **Разработчикам IoT:** внедрять обязательную смену пароля при первом входе и механизмы защиты от Brute-Force (задержки, блокировки, логирование попыток).

Ответы на контрольные вопросы

1. Какие факторы влияют на скорость и успешность атаки Brute-Force?

- Размер и релевантность словаря;
- Скорость сетевого подключения;
- Наличие защитных механизмов (блокировки, задержки);
- Простота пароля (длина, сложность);
- Тип аутентификации и протокол.

2. Почему использование длинных и сложных паролей не всегда эффективно для IoT?

- Многие устройства имеют ограниченные ресурсы и не поддерживают сложные политики паролей.
- Пользователи IoT часто не обладают техническими знаниями и используют простые пароли для удобства.
- Некоторые устройства жестко задают учетные данные в прошивке и не позволяют их изменить.

3. Какие механизмы защиты от подбора паролей вы знаете?

- Блокировка учетной записи после N неудачных попыток;
- Экспоненциальная задержка между попытками;
- CAPTCHA (редко в IoT);
- Логирование и оповещение администратора;
- Ограничение IP-адресов (whitelist).

4. В чем разница между атакой Brute-Force и атакой по словарю?

- **Brute-Force:** перебор всех возможных комбинаций символов (очень медленно).
- **Атака по словарю:** перебор из заранее составленного списка вероятных паролей (быстрее, эффективнее против слабых паролей).

5. Каковы юридические и этические аспекты проведения подобных атак?

- Такие атаки разрешены только в рамках учебной среды или при наличии письменного разрешения владельца системы.
- Несанкционированное сканирование или взлом устройств в реальной сети нарушает законодательство (например, статьи УК РФ о несанкционированном доступе к компьютерной информации).
- Этично — использовать полученные знания исключительно для защиты, а не для компрометации систем.