Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО

Факультет прикладной информатики (ФПИН)

Лабораторная работа №4

по дисциплине: Основы кибербезопасности

Автор: доцент практики, кандидат технических наук

Кравчук Алексей Владимирович

Санкт-Петербург
2025

Тема занятия: Активный брут-форс сервиса ssh и способы защиты от него.

Цель работы.

- Изучить способы получения несанкционированного доступа (НСД) злоумышленником посредством выполнения им базовой атаки «перебор по словарю» («брут-форс»).
- Изучить базовые способы противодействия угрозе подбора аутентификационной информации.

Краткие теоретические сведения.

В БДУ ФСТЭК эта угроза имеет идентификатор УБИ.008 и заключается в возможности подбора (например, путём полного перебора или перебора по словарю) аутентификационной информации дискредитируемой учётной записи пользователя в системе.

Для закрытия этой угрозы могут применяться различные меры (в т.ч. из Приказа 17 ФСТЭК) и средства, которые эти меры реализуют.

Одним из таких базовых средств защиты является утилита fail2ban и, конечно, корректная (с точки зрения ИБ) настройка ssh-сервера (запрет входа по паролю – только с использованием криптографического ключа).

Практическая часть:

Часть 1: Настройка тестовой среды.

Нужно развернуть 2 виртуальные машины: Kali Linux (с этой машины будем проводить атаку) и Ubuntu (на ней будем настраивать сервер sshd и утилиту fail2ban) и обеспечить между ними сетевую связность (ping должен проходить).

При религиозной непереносимости Kali Linux и Ubuntu можете использовать любые понравившиеся вам дистрибутивы Linux.

Шаг 1.1:

Обновление списка пакетов, доступных к установке:

sudo apt update

Собственно обновление пакетов (если ограничены по времени, то пропускаем)

sudo apt upgrade -y

Установка необходимых утилит для брутфорса

sudo apt install hydra nmap medusa patator -y

Проверка установки

hydra -h

nmap --version

medusa --version

Шаг 1.2: Настройка Ubuntu с уязвимым SSH

Обновляем список доступных пакетов:
sudo apt update

Устанавливаем OpenSSH-сервер (если ещё не установлен):
sudo apt install openssh-server -y

Убеждаемся, что служба SSH запущена и включена в автозагрузку:
sudo systemctl start ssh && sudo systemctl enable ssh

Отредактируйте конфигурацию SSH для имитации небезопасных настроек. Откройте файл /etc/ssh/sshd_config (например, через ***sudo nano /etc/ssh/sshd_config***) и убедитесь, что в нем установлены следующие параметры:

PasswordAuthentication yes – разрешена аутентификация по паролю (если строка закомментирована или имеет значение "***no***", раскомментируйте и установите "***yes***").

PermitRootLogin yes – временно разрешить вход по SSH под пользователем root. По умолчанию Ubuntu запрещает вход root по паролю, поэтому для целей эксперимента включаем эту опцию.

Итого в файле ***/etc/ssh/sshd_config*** параметры должны быть выставлены следующим образом: (для входа по связке логин/пароль):

PasswordAuthentication yes
PermitRootLogin yes
PermitEmptyPasswords no

После внесения изменений сохраните файл и перезапустите SSH-демон:
sudo systemctl restart ssh
sudo systemctl enable ssh

Задайте пароль для пользователя root:
sudo passwd root
и введите простой пароль, например ***princess*** (используем намеренно распространенный слабый пароль для демонстрации).

Создайте тестового пользователя с простым паролем (например, 123456):
sudo useradd -m -s /bin/bash testuser
sudo passwd testuser

Проверяем работу SSH:
sudo systemctl status ssh

ПРИМЕЧЕНИЕ: в реальных системах нельзя разрешать root-вход по паролю или использовать тривиальные пароли – здесь это делается только в учебных целях.

Часть 2: Проведение атаки brute-force

Шаг 2.1: Разведка цели

С Kali Linux сканируем цель:

nmap -sS -sV -p 22 <IP_адрес_Ubuntu>

```
-sS: SYN scan (полуоткрытое TCP-сканирование), отправляет TCP SYN и ждёт ответа.
-sV: version detection (определение сервиса и версии). После обнаружения открытого порта Nmap шлёт набор протокольных запросов, чтобы узнать, какой сервис (например ssh) и часто — версия (например OpenSSH 7.9p1). Может продлить время сканирования и вызвать дополнительные логи на целевой машине.
-p 22: порт(ы) для сканирования.
В данном случае — только TCP порт 22 (обычно SSH). Можно указывать диапазоны/списки: -p 22,80,443 или -p 1-1024.
```

Пример вывода:

22/tcp open ssh OpenSSH 8.9p1 Ubuntu 3

Шаг 2.2: Создаем свои файлы с логинами и паролями (для ускорения испытания):

Создаем файл с логинами

echo -e "testuser\nadmin\nroot\nuser" > users.txt

Создаем файл с паролями

echo -e "123456\npassword\nadmin\n1234\nqwerty\princess" > passwords.txt

В Kali Linux есть популярный словарь rockyou.txt (расположен в /usr/share/wordlists/rockyou.txt.gz). Можно его распаковать и поработать с ним, но это долго.

Шаг 2.3: Атака с помощью Hydra

Базовая атака

hydra -L users.txt -P passwords.txt ssh://<IP_адрес_Ubuntu> -t 4

Можно указать логин напрямую:

hydra -l root -P passlist.txt -t 4 ssh://<IP_Ubuntu>

С дополнительными параметрами

hydra -L users.txt -P passwords.txt ssh://<IP_адрес_Ubuntu> -t 4 -vV -I

Объяснение параметров:

-L users.txt - файл с логинами

-P passwords.txt - файл с паролями

-t 4 - количество параллельных подключений

-vV - подробный вывод
-I - немедленное начало атаки

Шаг 2.4: Атака с помощью Medusa

medusa -h <IP_адрес_Ubuntu> -U users.txt -P passwords.txt -M ssh -t 4
Параметры:
-h - хост цель
-U - файл с пользователями
-P - файл с паролями
-M - модуль (ssh)
-t – потоки

Шаг 2.5: Анализ результатов
Пример успешного результата Hydra:
[22][ssh] host: <IP> login: testuser password: 123456

Проверяем найденные учетные данные
ssh testuser@<IP_адрес_Ubuntu>

Вводим пароль: 123456

Часть 3: Настройка защищенного SSH
Шаг 3.1: Базовая безопасность SSH

Редактируем конфигурацию SSH
sudo nano /etc/ssh/sshd_config

Критически важные настройки:

Port 2222	# Изменяем стандартный порт
PermitRootLogin no	# Запрещаем вход root
PasswordAuthentication no	# Отключаем аутентификацию по паролю
PubkeyAuthentication yes	# Включаем аутентификацию по ключам
MaxAuthTries 3	# Максимум попыток аутентификации
ClientAliveInterval 300	# Таймаут неактивных сессий
AllowUsers testuser	# Разрешаем только конкретных пользователей

Перезапускаем SSH
sudo systemctl restart ssh

Шаг 3.2: Настройка ключевой аутентификации
На Kali генерируем ключ
ssh-keygen -t rsa -b 4096 -f ~/.ssh/ubuntu_key

Копируем публичный ключ на сервер
ssh-copy-id -i ~/.ssh/ubuntu_key.pub -p 2222 testuser@<IP_адрес_Ubuntu>

Тестируем подключение
ssh -i ~/.ssh/ubuntu_key -p 2222 testuser@<IP_адрес_Ubuntu>

Шаг 3.3: Повторная атака на защищенный SSH
Пытаемся провести атаку
hydra -L users.txt -P passwords.txt ssh://<IP_адрес_Ubuntu>:2222 -t 2

Результат будет неудачным:
[ERROR] - all children were disabled
Причина: PasswordAuthentication no

Часть 4: Настройка Fail2ban для защиты
Шаг 4.1: Установка и настройка Fail2ban
Устанавливаем Fail2ban на Ubuntu
sudo apt update
sudo apt install fail2ban -y

После установки запустите службу и добавьте в автозагрузку (если она не запустилась автоматически):
sudo systemctl enable --now fail2ban

Убедитесь, что сервис активен командой:
sudo systemctl status fail2ban
(статус должен быть active (running)

Примечание: Fail2Ban осуществляет блокировку, добавляя правила брандмауэра (iptables) для отказа во входящем трафике с вредоносных IP.

Fail2Ban добавляет динамические правила блокировок поверх существующих. Если UFW не используется, Fail2Ban применит iptables напрямую.

Копируем конфигурационный файл для SSH
sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local

Редактируем конфигурацию
sudo nano /etc/fail2ban/jail.local

Добавляем секцию для SSH:
[sshd]
enabled = true
port = 2222
filter = sshd
logpath = /var/log/auth.log
maxretry = 3
bantime = 600
findtime = 600

Создаем фильтр для нестандартного порта
sudo nano /etc/fail2ban/filter.d/sshd.conf

Перезапускаем Fail2ban
sudo systemctl enable fail2ban
sudo systemctl start fail2ban

Шаг 4.2: Проверка работы Fail2ban
Смотрим статус
sudo fail2ban-client status
sudo fail2ban-client status sshd

Проводим тестовую атаку с Kali:
hydra -L users.txt -P passwords.txt ssh://<IP_адрес_Ubuntu>:2222 -t 1

На Ubuntu проверяем блокировки:
sudo fail2ban-client status sshd
sudo iptables -L -n

Смотрим логи Fail2ban:
sudo tail -f /var/log/fail2ban.log

Шаг 4.3: Мониторинг и управление
Разблокировка IP вручную
sudo fail2ban-client set sshd unbanip <IP_адрес>

Добавление IP в белый список
sudo nano /etc/fail2ban/jail.local

Добавить: ignoreip = 127.0.0.1/8 <ваш_IP>

Часть 5: Анализ и выводы

До защиты:

- Hydra быстро подбирает простые пароли
- Неограниченное количество попыток
- Легкий доступ к системе

После базовой защиты SSH:

- Атаки по паролю невозможны
- Измененный порт скрывает сервис
- Только ключевая аутентификация

С Fail2ban:

- Автоматическая блокировка атакующих IP
- **Логирование попыток** неавторизованного доступа
- Временные блокировки снижают эффективность брутфорса

Рекомендации по безопасности:

- Всегда использовать ключевую аутентификацию
- Изменять стандартный порт SSH
- Регулярно обновлять SSH и операционную систему
- Настраивать Fail2ban или аналогичные системы
- Использовать сложные пароли для sudo
- Регулярно мониторить логи аутентификации

Часть 6. Приложение по использованию встроенных словарей в Kali Linux

Встроенные словари паролей в Kali Linux

Kali Linux содержит обширную коллекцию словарей, расположенных в различных директориях:

Шаг 6.1: Обзор доступных словарей

Поиск словарей паролей
find /usr/share/wordlists -name "*.txt" -type f | head -20

Просмотр популярных словарей
ls -la /usr/share/wordlists/

Основные директории со словарями:
ls -la /usr/share/wordlists/rockyou.txt
ls -la /usr/share/wordlists/fasttrack.txt

ls -la /usr/share/wordlists/nmap.lst
ls -la /usr/share/wordlists/dirbuster/
ls -la /usr/share/wordlists/metasploit/

Шаг 6.2: Подготовка словаря rockyou.txt

# Распаковка знаменитого словаря rockyou (если не распакован)
sudo gunzip /usr/share/wordlists/rockyou.txt.gz

Проверка размера словаря
wc -l /usr/share/wordlists/rockyou.txt
Результат: ~14 миллионов паролей

Просмотр первых 20 строк
head -20 /usr/share/wordlists/rockyou.txt

Создание уменьшенной версии для тестов
head -1000 /usr/share/wordlists/rockyou.txt > rockyou_top1000.txt

Шаг 6.3: Атака с использованием встроенных словарей

Вариант 1: Использование rockyou.txt

Атака с полной версией rockyou (очень долго!)
hydra -L users.txt -P /usr/share/wordlists/rockyou.txt ssh://<IP_адрес_Ubuntu> -t 4 -vV

Атака с уменьшенной версией
hydra -L users.txt -P /usr/share/wordlists/rockyou_top1000.txt ssh://<IP_адрес_Ubuntu> -t 4 -vV

Вариант 2: Использование fasttrack.txt

Fasttrack - популярные пароли для пентеста
hydra -L users.txt -P /usr/share/wordlists/fasttrack.txt ssh://<IP_адрес_Ubuntu> -t 4

Просмотр содержимого fasttrack
head -50 /usr/share/wordlists/fasttrack.txt

Вариант 3: Использование директории dirbuster

Словари из DirBuster
hydra -L users.txt -P /usr/share/wordlists/dirbuster/common-passwords.txt ssh://<IP_адрес_Ubuntu> -t 4

Использование нескольких словарей
hydra -L /usr/share/wordlists/dirbuster/apache-user-enum-1.0.txt -P /usr/share/wordlists/dirbuster/common-passwords.txt ssh://<IP_адрес_Ubuntu> -t 4