Схема аутентификации пользователей с помощью логинов и паролей в UNIX

Доклад к лекции №5

Толстых Александра Андреевна

Содержание

1 Введение

1.1 Актуальность и обоснование

В контексте современного информационного ландшафта, характеризующегося экспоненциальным ростом числа киберугроз, обеспечение безопасности информационных систем является критически важной задачей. В этом докладе рассматривается фундаментальный аспект безопасности — аутентификация пользователей с помощью логинов и паролей.

Этот механизм, исторически использовавшийся в UNIX-подобных операционных системах (ОС), остается широко распространенным и сегодня, несмотря на появление более современных методов аутентификации. Учитывая его широкое применение и, в ряде случаев, недостаточную защищённость, анализ принципов его работы, уязвимостей и современных подходов к усилению безопасности имеет первостепенное значение для повышения общей защищённости информационных ресурсов.

Некорректная реализация или пренебрежение принципами безопасного хранения и проверки паролей могут привести к компрометации учётных записей пользователей и, как следствие, к несанкционированному доступу к конфиденциальной информации, нарушению целостности данных и другим негативным последствиям.

1.2 Объект и предмет исследования

- Объект исследования: схема аутентификации пользователей в UNIX-подобных ОС.
- Предмет исследования: механизмы и методы реализации аутентификации с использованием логинов и паролей, включая методы хранения и проверки паролей, анализ уязвимостей, а также современные подходы к повышению безопасности данной схемы.

1.3 Научная новизна

В рамках этого исследования будет проведён комплексный анализ современных алгоритмов хеширования паролей, таких как bcrypt, scrypt и Argon2, с акцентом на их криптографическую стойкость, устойчивость к различным типам атак (брутфорс, радужные таблицы, атаки с использованием специализированного оборудования) и применимость в контексте UNIX-подобных ОС.

Будет проведено сравнение данных алгоритмов с традиционными методами хеширования (MD5, SHA-1) с целью выявления их преимуществ и недостатков, а также будут предоставлены рекомендации по принципам работы механизмов аутентификации пользователей в UNIX-подобных ОС, выявлению уязвимостей и разработке эффективных стратегий защиты от различных угроз, связанных с компрометацией учётных данных.

Предложенные рекомендации будут способствовать повышению общего уровня безопасности информационных систем и минимизации рисков, связанных с несанкционированным доступом.

2 Цель, гипотеза и задачи исследования:

2.1 Цель исследования

Целью данного исследования является проведение всестороннего анализа схемы аутентификации пользователей с использованием логинов и паролей в UNIX-подобных операционных системах, включающего анализ существующих уязвимостей, рассмотрение современных методов защиты и разработку рекомендаций по повышению безопасности.

2.2 Гипотеза исследования

Использование современных криптографически стойких алгоритмов хеширования, таких как bcrypt, scrypt или Argon2, в сочетании с многофакторной аутентификацией (MFA) значительно снижает вероятность успешного взлома учётных записей пользователей и, как следствие, повышает общий уровень безопасности системы.

2.3 Задачи исследования

Для достижения поставленной цели и проверки выдвинутой гипотезы в рамках данного исследования были сформулированы следующие задачи:

- Изучить и проанализировать архитектуру аутентификации пользователей в UNIX-подобных ОС, включая взаимосвязь между файлами /etc/passwd, /etc/shadow и модулями PAM (подключаемыми модулями аутентификации).
- Подробно рассмотреть методы хранения и проверки паролей в UNIX-подобных ОС, включая используемые алгоритмы хеширования, механизмы добавления соли («salt») и другие средства защиты. Выявить и проанализировать основные уязвимости и риски, связанные с аутентификацией на основе логинов и паролей, включая атаки методом подбора, словарные атаки, атаки с использованием радужных таблиц и другие.
- Рассмотреть современные подходы к усилению безопасности аутентификации, такие как использование многофакторной аутентификации, менеджеров паролей и современных алгоритмов хеширования.
- Сформулировать практические рекомендации по повышению безопасности аутентификации пользователей в UNIX-подобных ОС.

3 Материалы, методы и инструменты исследования, теоретическая база:

3.1 Материалы

В качестве материалов для исследования использовались:

- Документация по UNIX-подобным ОС (man-страницы, руководства по администрированию).
- Научные статьи и публикации в области информационной безопасности.
- Стандарты и рекомендации OWASP (Open Web Application Security Project).
- Открытые исходные коды различных программных продуктов, имеющих отношение к аутентификации.

3.2 Методы

В процессе исследования применялись следующие методы:

- Анализ: Изучение и критический разбор существующей литературы и документации, анализ кода.
- Синтез: Объединение информации из различных источников для получения целостной картины.
- Сравнительный анализ: сопоставление различных методов и алгоритмов для выявления их преимуществ и недостатков.

- Моделирование угроз: оценка потенциальных рисков и уязвимостей на основе различных сценариев атак.

3.3 Инструменты

Для проведения исследования использовались следующие инструменты:

- Утилиты для анализа системных логов (например, grep, awk, journalctl).
- Инструменты для оценки криптографической стойкости (например, John the Ripper, Hashcat) для тестирования различных алгоритмов хеширования.
- Виртуализированные среды (например, VirtualBox, VMware) для создания изолированных тестовых сред.
- Среды разработки и отладки (например, gdb) для анализа кода и разработки рекомендаций.

3.4 Теоретическая база

Исследование опирается на следующие теоретические концепции:

- Основы криптографии: хеширование, симметричное и асимметричное шифрование, криптографические протоколы (подробнее см. в [1]).
- Принципы безопасного проектирования систем: разделение привилегий, принцип наименьших привилегий, минимизация поверхности атаки.
- Архитектура UNIX-подобных ОС: принципы работы ядра, процессы, файловая система, система аутентификации, PAM.
- Методики анализа уязвимостей: моделирование угроз, анализ рисков, тестирование на проникновение.

4 Содержание исследования:

4.1 Обзор архитектуры аутентификации в UNIX-подобных ОС

Аутентификация в UNIX-подобных ОС представляет собой сложный процесс, опирающийся на ряд взаимосвязанных компонентов. Ключевыми элементами являются:

/etc/passwd: Файл, содержащий основную информацию о пользователях: логин, UID, GID, домашний каталог и командную оболочку. Исторически здесь хранился хэш пароля, что было серьезной уязвимостью. В современных системах в этом файле хранится символ «x» или «*», указывающий на то, что информация о пароле хранится в другом файле. Важно отметить, что этот файл доступен для чтения всем пользователям системы, что подчеркивает необходимость отделения информации о паролях в отдельный защищенный файл.

/etc/shadow: Файл, предназначенный для безопасного хранения информации о паролях пользователей. Доступ к этому файлу ограничен только пользователем root, что критически важно для безопасности системы. В этом файле хранится зашифрованный (хешированный) пароль пользователя, дата последней смены пароля, минимальный и максимальный срок действия пароля, а также другие параметры, связанные с управлением паролями. Формат записи в файле /etc/shadow имеет вид: login:hashed_password:last_change:min_days:max_days:warn_days:inactive_days:expire_days:rese

PAM (подключаемые модули аутентификации): гибкая система аутентифи-

кации, позволяющая использовать различные методы проверки подлинности пользователя. PAM позволяет администраторам настраивать систему аутентификации без необходимости перекомпилировать приложения (подробнее см. в [2]).

PAM использует конфигурационные файлы (обычно в каталоге /etc/pam.d/), которые определяют модули, используемые для аутентификации, авторизации, учёта и управления сеансами. PAM состоит из четырёх основных типов модулей:

- auth: Отвечает за аутентификацию пользователя.
- account: Проверяет, может ли пользователь получить доступ к системе (например, проверяет срок действия учётной записи).
- session: Управляет началом и завершением сеансов пользователя.
- password: Отвечает за изменение паролей.

4.2 Анализ методов хранения и проверки паролей

Безопасность хранения и проверки паролей критически важна для обеспечения защиты системы. В современных UNIX-подобных ОС используются следующие механизмы:

Хеширование паролей: вместо хранения паролей в открытом виде они преобразуются в хеши (строки фиксированной длины) с помощью односторонних криптографических функций. Хеширование позволяет системе проверять пароль без необходимости хранить его в незашифрованном виде, что существенно снижает риски, связанные с компрометацией базы данных пользователей.

«Соль» (Salt): случайная строка, добавляемая к паролю перед хешированием. Соль используется для защиты от атак с использованием радужных таблиц, которые представляют собой предварительно вычисленные таблицы соответствия между хешами и возможными паролями. Каждый пользователь имеет свою уникальную соль, которая хранится вместе с хешем пароля в файле /etc/shadow. Длина соли должна быть достаточно большой (не менее 16 байт) для обеспечения

надежной защиты.

Алгоритмы хеширования: выбор надежного алгоритма хеширования является ключевым фактором безопасности. Исторически использовались слабые алгоритмы, такие как MD5 и DES, которые уязвимы для атак. В настоящее время рекомендуется использовать более надежные алгоритмы, такие как:

- SHA-256 и SHA-512: представляют собой надежные алгоритмы хеширования, которые широко применяются в различных приложениях. SHA-256 генерирует 256-битный хеш, а SHA-512 — 512-битный хеш.
- bcrypt: Алгоритм, специально разработанный для хеширования паролей. Он использует «соль» и имеет адаптивную сложность (параметр «cost»), что позволяет увеличивать время вычисления хеша и тем самым усложнять атаки методом подбора.
- scrypt: алгоритм хеширования, который требует значительного объёма памяти для вычисления хеша. Это делает его устойчивым к аппаратным атакам, когда злоумышленники используют специализированное оборудование для быстрого перебора паролей.
- Argon2: современный алгоритм, победитель конкурса Password Hashing Competition, предлагающий три варианта (Argon2d, Argon2i, Argon2id) для различных требований к безопасности и производительности. Argon2id — это гибридный вариант, сочетающий преимущества Argon2d и Argon2i (подробнее см. в [3]).

4.3 Выявление уязвимостей и рисков

Несмотря на применение современных методов защиты, аутентификация на основе логинов и паролей остаётся уязвимой для различных типов атак:

1. Атаки методом перебора (Brute-force атаки): перебор всех возможных комбинаций паролей до тех пор, пока не будет найден правильный. Эффек-

тивность этой атаки зависит от сложности пароля (длины, использования различных символов).

2. Словарные атаки (Dictionary attacks): перебор паролей из списка часто используемых паролей (словаря). Эти атаки эффективны против пользователей, использующих простые и предсказуемые пароли.
3. Атаки с использованием радужных таблиц (Rainbow table attacks): использование заранее подготовленных таблиц хешей для быстрого поиска пароля по хешу. Использование соли усложняет проведение таких атак, но не исключает их полностью.
4. Фишинг (Phishing): обман пользователей с целью получения их логинов и паролей. Эта атака нацелена на человеческий фактор и требует от пользователей повышенной бдительности.
5. Уязвимости в программном обеспечении: наличие уязвимостей в коде, обрабатывающем данные аутентификации. Такие уязвимости могут позволить злоумышленнику обойти систему аутентификации или получить доступ к файлу /etc/shadow.
6. Атаки на файл /etc/shadow: Получение несанкционированного доступа к файлу /etc/shadow позволяет злоумышленнику получить хеши паролей всех пользователей и в дальнейшем попытаться их взломать.

4.4 Рассмотрение современных подходов к защите

Для повышения безопасности аутентификации пользователей в UNIX-подобных ОС рекомендуется использовать следующие подходы:

Использование сложных и уникальных паролей: регулярное обновление паролей, требование соблюдения минимальной длины пароля (не менее 12 символов), использование различных символов (букв верхнего и нижнего регистра, цифр, специальных символов).

Использование менеджеров паролей (например, KeePass, LastPass) для генера-

ции и хранения сложных паролей.

Ограничение количества неудачных попыток входа: блокировка учетной записи после определенного количества неудачных попыток аутентификации. Использование таких инструментов, как fail2ban, для автоматической блокировки IP-адресов, с которых осуществляются попытки подбора паролей.

Многофакторная аутентификация (MFA): использование нескольких факторов аутентификации (например, пароль + одноразовый код, отправленный на мобильный телефон, или биометрические данные). Наиболее распространенными методами MFA являются:

- Использование одноразовых паролей (OTP), генерируемых приложениями-аутентификаторами (например, Google Authenticator, Authy).
- Использование аппаратных ключей безопасности (например, YubiKey).
- Использование биометрических данных (например, отпечатки пальцев).

Применение современных алгоритмов хеширования: использование bcrypt, scrypt или Argon2, обеспечивающих высокую криптографическую стойкость. Важно правильно настроить параметры этих алгоритмов (например, «cost» для bcrypt, параметры памяти и времени для scrypt и Argon2), чтобы обеспечить оптимальный баланс между безопасностью и производительностью.

Мониторинг и аудит безопасности: регулярный анализ журналов событий, выявление аномалий, своевременное реагирование на инциденты. Использование систем обнаружения вторжений (IDS) и систем предотвращения вторжений (IPS) для автоматического выявления и блокирования подозрительной активности. Следование рекомендациям OWASP (подробнее см. в [4]).

5 Анализ и практическая значимость полученных результатов

В ходе данного исследования был проведён всесторонний анализ схемы аутентификации пользователей в UNIX-подобных ОС, выявлены основные уязвимости, рассмотрены современные методы защиты и разработаны практические рекомендации по повышению безопасности. Была подтверждена гипотеза о том, что использование современных стойких алгоритмов хеширования, таких как bcrypt, scrypt или Argon2, в сочетании с многофакторной аутентификацией значительно снижает вероятность успешного взлома учётных записей пользователей и, как следствие, повышает общий уровень безопасности системы.

Практическая реализация предложенных мер позволит организациям и частным лицам значительно повысить уровень своей кибербезопасности.

6 Общее заключение и выводы

В заключение следует отметить, что аутентификация с использованием логинов и паролей является фундаментальным аспектом безопасности UNIX-подобных ОС. Несмотря на свою простоту, эта схема подвержена различным уязвимостям, требующим постоянного внимания и совершенствования.

Проведенное исследование показало, что использование современных алгоритмов хеширования (bcrypt, scrypt, Argon2), многофакторной аутентификации, а также соблюдение передовых методов обеспечения безопасности является необходимым условием для надежной защиты от современных угроз.

Результаты работы позволяют сделать вывод о необходимости постоянного совершенствования подходов к управлению доступом и непрерывном повышении уровня осведомленности пользователей. Дальнейшие исследования могут быть направлены на анализ новых векторов атак и разработку более совершенных механизмов аутентификации, таких как беспарольная аутентификация (passwordless authentication) и использование биометрических данных.

Список литературы

1. Ferguson N., Schneier B. Practical Cryptography. Wiley, 2003. 416 с.
2. Nemeth E. и др. UNIX and Linux System Administration Handbook, 5th Edition. Pearson, 2017.
3. Argon2 Password Hashing Competition.
4. OWASP (Open Web Application Security Project). Password Storage Cheat Sheet. OWASP, n.d.