ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ КОНТРОЛЮ

Рекомендации по устранению типовых ошибок конфигурации (настройки) общесистемного и прикладного программного обеспечения

2026

1. Использование слабых пользовательских паролей создает угрозы осуществления атак «грубой силы» (T1110, Brute Force), компрометации учетных записей (T1586, Compromise Accounts). В целях предотвращения указанных угроз безопасности информации рекомендуется выполнить следующие мероприятия.

1.1 Установить парольную политику на уровне операционной системы и обеспечить обязательную сложность паролей.

Для операционных систем Windows.

Рекомендуется установить политику паролей с использованием утилиты gpedit.msc на уровне локального компьютера или через Group Policy Object (GPO) в домене (в случае использования Active Directory).

Для запуска редактора локальной групповой политики необходимо нажать сочетание клавиш на клавиатуре «Win» + «R», в открывшемся окне ввести «gpedit.msc» и нажать клавишу «Enter».

В открывшемся окне редактора локальной групповой политики необходимо перейти в разделы «Конфигурация компьютера» - «Конфигурация Windows» - «Параметры безопасности» - «Политика учетных записей» - «Политика паролей».

Установить в разделе «Политика паролей» параметры, представленные в таблице 1.

Таблица 1.

Параметр	Значение
Пароль должен отвечать требованиям сложности	Включить — требует минимум: 1 строчную, заглавную, цифру, спецсимвол
Минимальная длина пароля	Рекомендуется ⩾ 15 символов (по умолчанию — 0)
Максимальный срок действия пароля	60–90 дней (обязывает менять пароль периодически)
Минимальный срок действия пароля	1–2 дня (чтобы избежать мгновенной смены на старый)
История паролей	Не менее 5–10 (запрещает повторное использование)
Хранить пароли, используя обратимое шифрование	Отключить (иначе существует возможность расшифровать пароль)

Для применения настроек необходимо открыть командную строку операционной системы от имени администратора и ввести команду «gpupdate /force» для применения новой групповой политики.

Для проверки текущих локальных политик рекомендуется использовать

утилиту «secpol.msc», или команду «net accounts».

Для операционных систем на базе Linux.

Рекомендуется установить политику паролей с использованием файла /etc/login.defs или модулей Pluggable Authentication Modules (PAM).

Файл /etc/login.defs используется системными утилитами, такими как passwd, useradd, для определения базовых правил политики.

Чтобы открыть указанный файл необходимо выполнить следующую команду в терминале (командной строки) операционной системы:

sudo nano /etc/login.defs.

В открывшемся редакторе «Nano» установить параметры, представленные в таблице 2.

Таблица 2.

Параметр	**Назначение**	**Рекомендованное значение**
PASS_MAX_DAYS	Максимальный срок действия пароля	90
PASS_MIN_DAYS	Минимальное число дней между сменами пароля	1–7
PASS_WARN_AGE	За сколько дней до истечения срока показать предупреждение	7–14
PASS_MIN_LEN	Минимальная длина пароля (не во всех дистрибутивах)	15
ENCRYPT_METHOD	Метод шифрования пароля (SHA512, YESCRYPT, BCRYPT)	SHA512 или YESCRYPT

После внесения изменений необходимо сохранить файл и перезапустить терминал (в некоторых случая понадобится заново создать пользователей), чтобы параметры применились.

Файл /etc/login.defs не всегда гарантирует строгую проверку парольной политики. В качестве усиления проверки парольной политики рекомендуется использовать следующие модули «pam_pwquality» или «pam_cracklib» (в зависимости от дистрибутива).

Расположение конфигураций модулей зависит от дистрибутива:

для Debian/Ubuntu-подобных систем: /etc/pam.d/common-password;

для RHEL/CentOS/Rocky-подобных систем: /etc/pam.d/system-auth или /etc/security/pwquality.conf.

Для применения парольных политик необходимо добавить следующие строки в файлы конфигурации модулей:

password requisite pam_pwquality.so retry=3 minlen=15 ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1,

где retry=3 — попытки ввода пароля, minlen=15 — минимальная длина пароля, ucredit=-1 — минимум 1 заглавная буква, lcredit=-1 — минимум 1 строчная буква, dcredit=-1 — минимум 1 цифра, ocredit=-1 — минимум 1 спецсимвол.

Для RHEL-подобных систем настройка может быть выполнена через утилиту «authselect» или ручное редактирование файла конфигурации /etc/security/pwquality.conf с аналогичными параметрами.

Для проверки действия политики необходимо создать нового пользователя и попытаться задать слабый пароль, в случае отклонения слабого пароля, политика применена и работает.

Для дополнительного усиления рекомендуется применять политику блокировки входа после неудачных попыток. Для этого необходимо установить утилиты «pam_tally2» или «pam_faillock» (в зависимости от дистрибутива) и добавьте в PAM-конфигурацию следующие строки, например для RHEL-подобных систем:

auth required pam_faillock.so preauth audit silent deny=5 unlock_time=900

auth [default=die] pam_faillock.so authfail audit deny=5 unlock_time=900.

1.2 Обеспечить запрет на повторное использование паролей путем ведения журнала использованных паролей в соответствии с парольной политикой.

1.3 Обеспечить применение двухфакторной аутентификации для привилегированных пользователей информационных (автоматизированных) систем.

1.4 Реализовать регулярную проверку паролей на известные утечки с помощью утилит типа HaveIBeenPwned API или OpenVAS.

1.5 Реализовать регулярную проверку паролей на соответствие парольным словарям OpenVAS.

2. Отсутствие обязательной аутентификации для доступа к базам данных создает угрозы получения несанкционированного доступа, утечки защищаемой информации. В целях предотвращения указанных угроз безопасности информации рекомендуется выполнить следующие мероприятия.

2.1 Отключить возможность неавторизованного доступа в настройках систем управления базами данных (далее — СУБД) (MySQL, PostgreSQL, MS SQL).

Для MySQL (MariaDB):

необходимо осуществить проверку наличия анонимных пользователей командой на языке SQL:

SELECT User, Host FROM mysql.user WHERE User = '';

в случае наличия строк с пустым значением «User» подтверждается факт наличия анонимных пользователей;

необходимо удалить анонимных пользователей СУБД командами на языке SQL:

DELETE FROM mysql.user WHERE User = '';

FLUSH PRIVILEGES.

Кроме того, необходимо убедиться, что остальные пользователи имеют установленные пароли командой на языке SQL:

SELECT User, Host, authentication_string FROM mysql.user.

А также отключить удаленный доступ для «root»-пользователя командой на языке SQL:

UPDATE mysql.user SET Host='localhost' WHERE User='root'.

Для PostgreSQL:

PostgreSQL по умолчанию не поддерживает неавторизованный вход, но неправильная настройка конфигурации файла pg_hba.conf может допустить это;

файл конфигурации находится в директориях /etc/postgresql/<version> /main/pg_hba.conf или /var/lib/pgsql/<version>/data/ pg_hba.conf;

для запрета подключения без аутентификации необходимо заменить строки следующего вида, так как значение «trust» разрешает подключение без аутентификации, например:

host all all 0.0.0.0/0 trust

на:

host all all 0.0.0.0/0 scram-sha-256;

после осуществления замены необходимо выполнить команду перезапуска СУБД:

sudo systemctl restart postgresql.

Для Microsoft SQL Server:

в целях проверки возможности входа в SQL Server с анонимным или пустым паролем необходимо подключиться к SQL Server Management Studio (SSMS);

выполнить команду на языке SQL:

SELECT name, is_disabled, type_desc

FROM sys.sql_logins

WHERE name NOT IN ('sa');

найти учетные записи без пароля, а также с общими именами (guest, test, user, anon);

отключить или удалить найденные учетные записи (отключение пользователя производится командой ALTER LOGIN [имя_пользователя] DISABLE, удаление пользователя производится командой DROP LOGIN [имя_пользователя]);

осуществить проверку настройки аутентификации в СУБД путем просмотра

в разделе «Properties» - «Security», что выбран режим SQL Server and Windows Authentication mode.

2.2 Удалить гостевые (общие) учетные записи СУБД.

2.3 Ограничить IP-адреса, с которых возможен доступ, с помощью средств межсетевого экранирования или параметров «bind-address».

2.4 Включить режимы «TLS/SSL» для клиентских соединений.

Для PostgreSQL:

Необходимо настроить шифрование трафика между клиентом и сервером базы данных путем внесения следующих изменений в конфигурационные файлы СУБД (postgresql.conf для standalone или postgres.yml для cluster):

ssl: true

ssl_ca_file: /home/postgres/ssl/root.crt

ssl_cert_file: /home/postgres/ssl/server.crt

ssl_key_file: /home/postgres/ssl/server.key

ssl_min_protocol_version = 'TLSv1.2'

В случае использования внешней аутентификация (LDAP) необходимо обеспечить шифрование клиентских подключений к базе данных (hostssl) и подключения СУБД к контроллеру домена (ldapscheme=ldaps).

Для MSSQL:

Необходимо запустить SQL Server Configuration Manager и перейти в разделы «SQL Server Network Configuration» – «Protocols for MSSQLSERVER (имеющейся экземпляр сервера)».

Открыв свойства «Protocols», во вкладке «Certificate» выбрать нужный сертификат из списка.

Во вкладке «Flags», установить следующее значение для принудительного шифрования всех соединений:

Force Encryption = Yes.

Для применения указанных настроек необходимо перезапустить SQL Server с использованием оболочки выполнения сценариев Windows «PowerShell» командой Restart-Service MSSQLSERVER (имеющейся экземпляр сервера).

2.5 Организовать аудит событий доступа к СУБД.

Для PostgreSQL:

Аудит событий возможен с использованием расширения с открытым исходным кодом «pg_audit», настроенного в соответствии с рекомендациями разработчика (https://github.com/pgaudit/pgaudit/blob/main/README.md).

Для Microsoft SQL Server:

Аудит MSSQL доступен для версий SQL Server Enterprise и SQL Server Standard (2016+) и включается на уровне сервера и на уровне базы данных.

Для включения аудита на уровне сервера необходимо запустить SQL Server

Management Studio, подключиться к имеющемуся экземпляру SQL Server и перейти в разделы «Security» - «Audits».

Создать SQL Server Audit (аудит-файл или журнал Windows) путем выбора «New Audit…» и указать его параметры.

Audit name: например, Audit_Server_Activity

Audit destination:

File (Рекомендовано. Необходимо указать путь к директории, например C:\AuditLogs\);

Application log (для Event Viewer);

Security log (требует запуск SQL Server с привилегиями Generate Security Audits);

Максимальный размер файла и ротация (с учетом имеющихся вычислительных возможностей);

Создать Server Audit Specification (спецификацию аудита) в разделе «Security» - «Server Audit Specifications» путем нажатия на «New Server Audit Specification…» и указания следующих параметров.

Name: например, Spec_LoginAudit

Audit: выбирать ранее созданный (Audit_Server_Activity).

В блоке «Actions», необходимо добавить события аудита с учетом того, что должен быть включен аудит уровня сервера следующих действий:

BACKUP_RESTORE_GROUP;
SERVER_OBJECT_PERMISSION_CHANGE_GROUP;
SERVER_PERMISSION_CHANGE_GROUP;
SERVER_PRINCIPAL_IMPERSONATION_GROUP;
FAILED_LOGIN_GROUP;
SUCCESSFUL_LOGIN_GROUP;
LOGOUT_GROUP;
DATABASE_CHANGE_GROUP;
SERVER_OBJECT_CHANGE_GROUP;
SERVER_PRINCIPAL_CHANGE_GROUP;
SERVER_OPERATION_GROUP;
LOGIN_CHANGE_PASSWORD_GROUP;
SERVER_STATE_CHANGE_GROUP;
SERVER_OBJECT_OWNERSHIP_CHANGE_GROUP;
TRACE_CHANGE_GROUP.

Для включения аудита на уровне базы данных необходимо запустить SQL Server Management Studio, подключиться к имеющемуся экземпляру SQL Server и перейти в разделы «Security» - «Audits».

Создать новое правило аудита путем нажатия на «New Audit...» и настройки

его параметров:

Audit name: например, Audit_DB_Level

Destination: File (Рекомендовано. Необходимо указать путь к директории, например C:\AuditLogs\);

Максимальный размер файла и ротация (с учетом имеющихся вычислительных возможностей).

Для создания спецификации аудита базы данных необходимо в SQL Server Management Studio открыть базу данных, для которой устанавливается аудит. Перейти в разделы «Security» - «Database Audit Specifications», создать спецификацию путем выбора «New Database Audit Specification…» и заполнить её следующими параметрами

Name: например, DBAudit_ReadWrite

Audit: Audit_DB_Level (ранее созданное)

В блоке «Actions», необходимо добавить события аудита с учетом того, что должен быть включен аудит уровня базы данных следующих действий (за исключением версий MSSQL Standart и Express):

DATABASE_PERMISSION_CHANGE_GROUP;

DATABASE_OBJECT_PERMISSION_CHANGE_GROUP;

SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP;

DATABASE_PRINCIPAL_IMPERSONATION_GROUP;

DATABASE_CHANGE_GROUP;

DATABASE_OBJECT_CHANGE_GROUP;

DATABASE_PRINCIPAL_CHANGE_GROUP;

DATABASE_OBJECT_OWNERSHIP_CHANGE_GROUP;

SCHEMA_OBJECT_OWNERSHIP_CHANGE_GROUP.

Для проверки работы аудита необходимо выполнить событие (например, неудачную авторизацию) и открыть журнал аудита.

В случае, если был выбран FILE, то необходимо выполнить следующую команду на языке SQL:

```
SELECT *
FROM sys.fn_get_audit_file('C:\AuditLogs\*.sqlaudit', default, default);
```

В случае, если был выбран журнал Windows, то необходимо открыть следующие разделы Event Viewer:

«Application and Services Logs» - «Microsoft» «SQL Server» - «Audit».

Кроме того, необходимо убедиться, что права доступа к директориям журнала аудита (например, C:\AuditLogs\) ограничены.

3. В операционной системе Windows используется устаревший протокол SMBv1, который создает угрозы осуществления атак, направленных на получение несанкционированного доступа (EternalBlue, WannaCry). В целях предотвращения указанных угроз безопасности информации рекомендуется выполнить следующие мероприятия.

3.1 Отключить протокол SMBv1 с использованием оболочки выполнения сценариев Windows «PowerShell» командой:

Disable-WindowsOptionalFeature -Online -FeatureName "SMB1Protocol".

3.2 Убедиться, что используется протокол SMBv2 или SMBv3:

Для операционной системы Windows необходимо:

открыть оболочку выполнения сценариев Windows «PowerShell» от имени администратора и ввести команду:

Get-SmbServerConfiguration | Select EnableSMB1Protocol, EnableSMB2Protocol;

вывод результата выполнения команды должен быть следующим:

EnableSMB1Protocol — False

EnableSMB2Protocol — True (это подтверждает использованием проколов SMBv2 и SMBv3).

Для операционных систем на базе Linux (проверка, что протокол SMBv1 отключён в Samba) необходимо:

открыть файл /etc/samba/smb.conf и убедиться, что указаны минимальные версии:

[global]

min protocol = SMB2

max protocol = SMB3;

перезапустить Samba командой:

sudo systemctl restart smbd.

3.3 Организовать проведение регулярной инвентаризации сетевых устройств, на предмет выявления использования протокола SMBv1 (например, устаревшие принтеры).

3.4 Обновить или изолировать устаревшие устройства, использующие протокол SMBv1.

3.5 Осуществить (по возможности) блокировку протокола SMBv1 на уровне сети с помощью средств межсетевого экрана (например, блокировкой портов 137, 138, 139, 445).

4. В операционной системе Windows используется устаревший протокол NTLMv1, что создает угрозы осуществления атак, направленных на получение несанкционированного доступа. В целях предотвращения указанных угроз безопасности информации рекомендуется выполнить следующие мероприятия.

Рекомендуется установить политику, отключающую использование протокола NTLMv1, с использованием утилиты gpedit.msc на уровне локального компьютера или через Group Policy Object (GPO) в домене (в случае использования Active Directory).

Для запуска редактора локальной групповой политики необходимо нажать сочетание клавиш на клавиатуре «Win» + «R», в открывшемся окне ввести «gpedit.msc» и нажать клавишу «Enter».

В открывшемся окне редактора локальной групповой политики необходимо перейти в разделы «Конфигурация компьютера» - «Конфигурация Windows» - «Параметры безопасности» - «Локальные политики» - «Параметры безопасности». Перейти в свойства «Сетевая безопасность: уровень проверки подлинности LAN Manager» и установить значение политики «Отправлять только NTLMv2-ответ. Отказывать LM и NTLM».

Аналогичные изменения возможно осуществить через запись реестра Windows HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa с помощью параметра DWORD с именем LmCompatibilityLevel и значением от 0 до 5, где значению 5 соответствует значение политики «Отправлять только NTLMv2-ответ. Отказывать LM и NTLM».

5. Наличие учетной записи «Гость» в локальной группе «Администраторы» создает угрозы получения несанкционированного доступа с повышенными привилегиями. В целях предотвращения указанных угроз безопасности информации рекомендуется выполнить следующие мероприятия.

5.1 Отключить учетную запись «Гость» с помощью утилиты lusrmgr.msc путем перехода в раздел «Пользователи» и удаления пользователя с именем «Гость».

5.2 Удалить также пользователя с именем «Гость» из группы «Администраторы», если он был добавлен.

5.3 Проверить членство пользователя в группах возможно с помощью команды:

net localgroup Администраторы.

5.4 Организовать внедрение групповой политики, запрещающей автоматическое добавление учетных записей в группу «Администраторы».

5.5 Организовать журналирование событий, связанных с попытками входа под учетной записью «Гость».

6. Хранение учетных данных в открытом виде создает угрозы утечки аутентификационных данных. В целях предотвращения указанных угроз безопасности информации рекомендуется выполнить следующие мероприятия.

6.1 Запретить пользователям информационной (автоматизированной) системы хранить учетные данные в файлах «.env», «.txt», «.ini» без шифрования.

6.2 Использовать отечественные хранилища паролей и учетных данных, например, Kaspersky Password Manager.

6.3 При необходимости применения учетных данных в скриптах необходимо использовать переменные окружения, а не прямой ввод учетных данных.

6.4 Ограничить доступ к конфигурационным файлам, содержащим учетные данные, ведением списков доступа (ACL) для операционных систем Windows или с использованием утилиты chmod для операционных систем Linux.

Для операционных систем Windows:

Например, для ограничения доступа к файлу C:\App\config.json необходимо открыть оболочку выполнения сценариев Windows «PowerShell» от имени администратора удалить все существующие разрешения командой:

icacls "C:\App\config.json" /inheritance:r

icacls "C:\App\config.json" /remove:g "Users" "Authenticated Users" "Everyone";

предоставить доступ только Admin и SYSTEM командой:

icacls "C:\App\config.json" /grant:r "Administrators:F" "SYSTEM:F",

где F — полный доступ, R — только чтение, /grant:r — замещает предыдущие разрешения;

для установки флага «только для чтения» необходимо выполнить команду:

attrib +R "C:\App\config.json".

Для применения групповой политики (GPO) в случае использования Active Directory с использованием утилиты gpmc.msc необходимо:

создать новую политику;

перейти в раздел «Computer Configuration» - «Windows Settings» - «File System»;

добавить путь к файлу или каталогу;

настроить разрешения следующим образом Администраторы и SYSTEM — полный доступ, остальным — запрет.

Для операционных систем на базе Linux права доступа настраиваются с использованием утилит chmod, chown.

Например, чтобы установить файлу владельца и группу /etc/app/config.yml необходимо выполнить следующую команду в терминале:

sudo chown root:app /etc/app/config.yml;

чтобы установить права на чтение только владельцем необходимо выполнить следующую команду в терминале:

sudo chmod 640 /etc/myapp/config.yml,

где 640 означает: 6 (rw-) для владельца (root), 4 (r--) для группы (app), 0 (---) для всех остальных.

Также возможно создать специализированную группу и предоставить доступ к файлу через неё путем выполнения следующих действий.

Создать группу, выполнив следующую команду в терминале, например:

sudo groupadd app.

Добавить в группу нужного пользователя, выполнив следующую команду в терминале:

sudo usermod -aG app serviceuser.

Назначить владельцем группу для файла, выполнив следующую команду в терминале:

chgrp app myfile.txt.

Рекурсивно сменить группу для всех файлов в директории, выполнив следующую команду в терминале:

chgrp -R app /project.

Для обнаружения конфигурационных файлов, доступных для всех рекомендуется выполнить следующую команду в терминале:

find /etc -type f -name "*.conf" -perm -004 -exec ls -l {} \;

Для усиления контроля ограничения доступа к файлам возможно использование SELinux.

Пример ограничения доступа к конфигурационному файлу Nginx с использованием SELinux (для RHEL/CentOS-подобных систем):

semanage fcontext -a -t httpd_config_t "/etc/nginx/nginx.conf"

restorecon -v /etc/nginx/nginx.conf.

Мониторинг изменений прав доступа к файлу возможно осуществить с помощью утилиты auditd.

Для мониторинга доступа к файлу необходимо выполнить следующую команду в терминале:

auditctl -w /etc/app/config.yml -p war -k config_watch.

Для просмотра записанных событий необходимо выполнить следующую команду в терминале:

ausearch -k config_watch.

6.5 Периодически производить сканирование репозиториев хранимых файлов на наличие в них учетных данных с помощью инструментов truffleHog, git-secrets, gitleaks.

7. Наличие открытых неиспользуемых портов создает угрозу их использования злоумышленниками. В целях предотвращения указанных угроз безопасности информации рекомендуется выполнить следующие мероприятия.

7.1 Организовать проведение регулярного аудита открытых портов с использованием инструментов nmap, netstat, ss.

7.2 Осуществить блокировку неиспользуемых портов.

7.3 Использовать для блокировки (открытия и закрытия) портов политики безопасности (firewalld, iptables, Windows Firewall, bpfilter, nftables).

7.4 Организовать мониторинг активных соединений и автоматическое оповещение администраторов безопасности в случае подозрительной активности.

8. Активированный автовход пользователя на сервере Windows создает угрозу получения несанкционированного доступа внутренним нарушителем. В целях предотвращения указанных угроз безопасности информации рекомендуется выполнить следующие мероприятия.

8.1 Отключить автовход пользователя Windows путем удаления ключей AutoAdminLogon из реестра.

8.2 Осуществлять проверку конфигурации служб удаленного доступа (RDP, SSH).

8.3 Принудительно включить ввод пароля при входе в систему.

9. SSH-сервер разрешает вход по паролю и привилегированный доступ (root), что создает угрозу получения несанкционированного доступа. В целях предотвращения указанных угроз безопасности информации рекомендуется выполнить следующие мероприятия.

9.1 Отключить авторизацию пользователей по паролю и доступ с «нулевым» паролем путем внесения следующих изменений в файл /etc/ssh/sshd_config:

PermitEmptyPasswords no

PermitRootLogin no

PasswordAuthentication no.

9.2 Обеспечить доступ только по SSH-ключам.

9.3 Ограничить IP-адреса, которые используются для входа с помощью политик AllowUsers/AllowGroups.

8.4 Организовать мониторинг событий SSH-доступа и анализ полученных событий.

В операционной системе Linux SSH-логирование осуществляется с использованием утилиты sshd, а события записываются в системный журнал.

Основные файлы, содержащие записи событий представлены в таблице 3.

Таблица 3.

Файл	Назначение	Дистрибутив
/var/log/auth.log	Аутентификация, включая SSH	Debian, Ubuntu
/var/log/secure	Аналогично (аутентификация, sudo)	RHEL, CentOS, Rocky
journalctl -u ssh	Лог systemd-юнита SSHD	Все systemd-дистрибутивы

По умолчанию sshd осуществляет запись следующих событий:

успешные и неуспешные попытки входа;

ошибки аутентификации (неверный логин, пароль, ключ);

попытки входа с отключёнными пользователями;

использование команд sudo, su, scp, sftp.

Пример строк в файле /var/log/auth.log:

Jun 18 12:43:22 server sshd[17245]: Accepted password for alice from 192.168.1.25 port 52914 ssh2;

Jun 18 12:45:00 server sshd[17252]: Failed password for invalid user admin from 192.168.1.30 port 52788 ssh2.

Настройку уровня записи событий возможно осуществить путем внесения следующих изменений в файл конфигурации: /etc/ssh/sshd_config:

LogLevel VERBOSE.

В качестве дополнительных уровней допускается использование:

QUIET, FATAL, ERROR — минимальные;

INFO — по умолчанию;

VERBOSE — включает запись ключей при аутентификации (без самих ключей).

Для того, чтобы применить настройки, необходимо выполнить следующую команду в терминале:

sudo systemctl restart sshd.

Для ручного анализа SSH-логов рекомендуется использовать следующие команды:

grep "Accepted" /var/log/auth.log (для нахождения всех успешных авторизаций);

grep "Failed password" /var/log/auth.log (для нахождения всех неудачных авторизаций);

Подсчёт количества попыток по IP:

grep "Failed password" /var/log/auth.log | awk '{print $(NF-3)}' | sort | uniq -c | sort -nr (для подсчета количества попыток авторизации по IP);

Подсчёт по пользователям:

grep "Failed password" /var/log/auth.log | awk '{print $(NF-5)}' | sort | uniq -c | sort -nr (для подсчета количества попыток авторизации по пользователям);

Для автоматического анализа записей событий SSH рекомендуется использовать утилиту fail2ban, которая также автоматически блокирует IP-адреса с частыми ошибками входа.

Для установки fail2ban необходимо выполнить следующие команды в терминале:

Для Debian/Ubuntu-подобных систем:

sudo apt install fail2ban;

Для RHEL-подобных систем:

sudo yum install fail2ban;

Для настройки указанного инструмента необходимо выполнить следующие изменения в файле конфигурации /etc/fail2ban/jail.local:

[sshd]
enabled = true
port = ssh
filter = sshd
logpath = /var/log/auth.log
maxretry = 5
bantime = 3600.

Для более глубокого аудита рекомендовано использовать утилиту Auditd со следующими правилами:

auditctl -w /usr/sbin/sshd -p x -k ssh_exec;
ausearch -k ssh_exec.

10. Отсутствие назначенных прав доступа на файлы и директории создает угрозу их несанкционированной модификации любыми пользователями. В целях предотвращения указанных угроз безопасности информации рекомендуется выполнить следующие мероприятия.

10.1 Организовать проведение регулярного аудита прав доступа файлов и директорий (для операционных систем на базе Linux командой ls -l, для операционных Windows командой icacls).

10.2 Использовать для разграничения доступа принципы наименьших привилегий.

10.3 Ограничить доступ к файлам конфигурации, выполняемым скриптам и журналам событий информационной инфраструктуры.

10.4 Осуществить настройку ACL и наследование прав по аналогии с пунктом 5 настоящих рекомендаций.

10.5 Организовать регулярное сканирование инфраструктуры на наличие

«world-writable» директорий и файлов.

Для этого рекомендуется использовать утилиту Auditd со следующим правилом:

auditctl -w / -p w -k world_write_watch.

Кроме того, в качестве дополнительного инструмента контроля рекомендуется использовать Lynis.

Установка Lynis осуществляется путем выполнения следующей команды в терминале:

sudo apt install lynis.

Для формирования отчета по аудиту инфраструктуры с использованием Lynis необходимо выполнить следующую команду в терминале:

sudo lynis audit system.

Указанный отчет будет содержать информацию о «world-writable» объектах. Для обнаруженных объектов в указанном отчете необходимо осуществить разграничение доступа в соответствии с пунктом 5 настоящих рекомендаций.

11. Наличие в информационной инфраструктуре неиспользуемых служб и компонентов операционной системы создает угрозу их использования злоумышленниками. В целях предотвращения указанных угроз безопасности информации рекомендуется выполнить следующие мероприятия.

11.1 Проводить периодическую инвентаризацию активных служб:

для операционной системы Windows рекомендуется использовать утилиту services.msc, а также команду Get-Service оболочки выполнения сценариев Windows «PowerShell»;

для операционных систем на базе Linux рекомендуется использовать утилиту systemctl, а также команду терминала service --status-all.

11.2 Отключить неиспользуемые службы, например, Telnet, FTP, SNMPv1/v2c.

11.3 Осуществить настройку контроля запуска критичных служб, например, GPO, systemd.

11.4 Осуществлять периодический мониторинг автозагрузки и изменения запущенных служб.

12. Наличие в информационной инфраструктуре неиспользуемых учетных записей, а также учетных записей с избыточными правами создает угрозу их использования злоумышленниками. В целях предотвращения указанных угроз безопасности информации рекомендуется выполнить следующие мероприятия.

12.1 Проводить периодическую инвентаризацию учетных записей и отключать неиспользуемые учетные записи.

Для операционных систем Windows:

инвентаризацию учетных записей рекомендуется проводить с использованием утилиты net путем выполнения следующей команды оболочки выполнения сценариев Windows «PowerShell»:

net имя_пользователя;

для просмотра всех локальных пользователей необходимо выполнить следующую команду оболочки выполнения сценариев Windows «PowerShell»:

Get-LocalUser;

для просмотра последнего входа пользователя в систему необходимо выполнить следующую команду оболочки выполнения сценариев Windows «PowerShell»:

```
Get-LocalUser | foreach {
   $lastLogon = $_.LastLogon
   "$($_.Name) - $lastLogon"
}
```

для просмотра журнала событий Windows, связанных с успешной авторизацией пользователей рекомендуется использовать команду Get-WinEvent или просмотр событий Безопасности Windows (ID 4624 — успешный вход).

Для отключения пользователей необходимо выполнить следующую команду оболочки выполнения сценариев Windows «PowerShell»:

для локальных пользователей:

Disable-LocalUser -Name "UserName";

В случае использования Active Directory:

Disable-ADAccount -Identity "username".

Для операционных систем на базе Linux:

инвентаризацию учетных записей рекомендуется проводить с использованием команды терминала getent passwd, которая показывает список всех пользователей из /etc/passwd или централизованного источника (например, LDAP);

для просмотра даты последнего входа всех пользователей рекомендуется использовать команду терминала:

sudo lastlog;

для просмотра журнала неудачных попыток входа рекомендуется использовать команду терминала:

sudo faillog -a;

для просмотра информации о сроке действия пароля рекомендуется использовать команду терминала:

sudo chage -l username;

для проверки активных и предыдущих сессий пользователей рекомендуется

использовать утилиты who, w, last.

Для блокировки учетных записей используется следующая команда терминала:

usermod -L <user>.

Для блокировки входа пользователя используется следующая команда терминала:

passwd -l <user>.

Для запрета shell-доступа используется следующая команда терминала:

usermod -s /sbin/nologin <user>.

Для установки даты истечения действия учетной записи на «сейчас» используется следующая команда терминала:

chage -E 0 <user>.

12.2 Произвести минимизацию пользовательских привилегий.

12.3 Обеспечить использование выделенных привилегированных учетных записей для администрирования информационных (автоматизированных) систем, а также реализовать запрет использования для этих целей обычных пользовательских учетных записей.
