|  |  |  |
| --- | --- | --- |
| Что было настроено? | Почему это настроено неправильно? | Рекомендации по настройке. |
| 1. vsftpd | В конфигурации /etc/vsftpd.conf включен анонимный доступ anonymous\_enable=YES (без пароля) к директории /etc (где лежат конфигурационные файлы и другие конфиденциальные данные) через опцию anon\_root=/etc/. | Убрать анонимный доступ, или в крайний случай как минимум убрать доступ к этой директории. |
| 1. DNS bind | В конфигурации /etc/bind/named.conf.default-zones неверно настроена зона hackatom.ru: есть доступ на чтение через allow-transfer { any; }; и запись allow-update { any; };.  [https://www.zytrax.com/books/dns/ch7/xfer.html#allow-transfer](https://www.zytrax.com/books/dns/ch7/xfer.html" \l "allow-transfer) [https://www.zytrax.com/books/dns/ch7/xfer.html#allow-update](https://www.zytrax.com/books/dns/ch7/xfer.html" \l "allow-update) | Огранить доступ одним из вариантов:   * полностью через “none”; * указать IP, у кого может быть доступ; * указать ключ key для update. |
| 1. Apache2 | Для сайта /etc/apache2/sites-enabled/000-default.conf включены ServerSignature On и ServerTokens Full, что сообщает злоумышленникам версии сервера (способствует enumeration).  [https://httpd.apache.org/docs/2.4/mod/core.html#servertokens](https://httpd.apache.org/docs/2.4/mod/core.html" \l "servertokens)  [https://httpd.apache.org/docs/2.4/mod/core.html#serversignature](https://httpd.apache.org/docs/2.4/mod/core.html" \l "serversignature) | Отключить (например, ServerTokens Prod и ServerSignature Off). |
| Для того же сайта включена опция Indexes, которая выдает листинг поддиректорий и позволяет выполнять атаку Path Traversal по ним, если в исследуемой директории отсутствует index.html. | Убрать лишнюю опцию. |
| 4. sudo | Пользователь ubuntu в группе sudo, хотя требовался только admin. | Убрать его из группы или убрать пользователя. |
| В /etc/sudoers доступ ALL=(ALL:ALL) ALL для групп sudo и admin, заданный как %sudo и %admin, хотя требовался только один пользователь admin (а еще есть пользователь root). | Ограничить лишний доступ. |
| Файл /etc/sudoers.d/secret\_user с содержимым hacker ALL=(ALL:ALL) ALL | Удалить файл (и пользователя hacker). |
| 5. sshd | В /etc/ssh/sshd\_config включен доступ к пользователю root через PermitRootLogin yes. | Убрать небезопасные настройки. Также ограничить список доступных пользователей (AllowUsers), возможно запретить пароли (PasswordAuthentication) и использовать ключ-файлы (PubkeyAuthentication и т.д.) и/или 2FA вместо них. |
| Разрешены пустые пароли через PermitEmptyPasswords yes. |
| 6. /opt/myscript | Command Injection через неэкранированные переменные в Bash.  <https://unix.stackexchange.com/questions/171346/security-implications-of-forgetting-to-quote-a-variable-in-bash-posix-shells> | Обрамить переменные в кавычки при их использовании. |
| 7. NFS | Открыта доступ к папке /root. | Использовать папку, больше предназначенную для NFS. |
| Права для всех на доступ к папке через rw и no\_root\_squash.  <https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/4/html/security_guide/s2-server-nfs-noroot> | Убрать эти небезопасные настройки (использовать ro, root\_squash, ограничить список пользователей, т.д.).  <https://man.archlinux.org/man/exports.5#EXAMPLE> |