# Сканирование ОС Linux и UNIX с минимальными привилегиями

Обновлено 25 мая 2020 г.

В ходе сканирования UNIX-подобных систем, в том числе Linux, для обнаружения большинства уязвимостей достаточно учетной записи без привилегий root. Привилегии root необходимы только для небольшого числа проверок на уязвимости, а также для проверки соответствия конфигураций стандартам. В случае, если планируется сканирование с пользователем без привилегий root, необходимо убедиться, что учетная запись имеет указанные в этом документе права, и понимать, что пользователь без полномочий root не найдет часть уязвимостей.

В следующих разделах приведены рекомендации по настройке учетных записей и информация по ограничениям сканирования без привилегий root. Также важно отметить, что из-за сложности проверок и того, что они часто обновляются, этот список может меняться со временем.

Для обеспечения максимального охвата уязвимостей при сканировании от имени пользователя, не являющегося пользователем root, необходимо выполнить одно из следующих действий:

- Настроить делегирование прав, чтобы пользователь, под которым осуществляется сканирование мог, запускать команды от имени пользователя root без прямого использования учетной записи root.
- Настроить сканируемые системы таким образом, чтобы у пользователя без полномочий root были права на указанные ниже команды и директории.

### Настройка сканируемых узлов

Одним из способов повышения привилегий для сканирования без использования пользователя root является использование повышения прав доступа, такого как sudo или pbrun. Эти параметры требуют особой настройки (например, для pbrun необходимо внести оболочку пользователя в белый список).

### Точечная настройка привилегий для сканирования

Вторым способом является точечная настройка прав для запуска команд, необходимых системе сканирования.

В следующем разделе приведены примеры выполняемых системой сканирования команд. Подавляющее большинство этих команд можно запускать без прав root. Как указано выше, этот список может изменяться по мере добавления новых проверок.

Данные команды необходимы в первую очередь для:

- Получения информации об установленной ОС;
- Получения информации об установленном ПО;
- Запуска проверок аудита конфигураций;

Для сканирования всех UNIX-подобных систем сканеру уязвимостей нужны права на запуск следующих команд:

- ifconfig
- java
- sha1
- sha1sum
- md5
- md5sum
- awk
- grep
- egrep
- cut
- id
- ls
- unzip

Tenable.sc в ходе сканирования также проверяет ряд файлов конфигураций в том случае, если у учетной записи для сканирования есть доступ к этим файлам. Ниже по тексту представлен список файлов и директорий, к которым необходимо предоставить доступ:

- /etc/group
- /etc/passwd
- grub.conf
- menu.lst
- lilo.conf

- syslog.conf
- /etc/permissions
- /etc/securetty
- /var/log/postgresql
- /etc/hosts.equiv
- .netrc
- '/', '/dev', '/sys', and '/proc' "/home" "/var" "/etc"
- /etc/master.passwd
- sshd_config

Также необходимо предоставить права на чтение следующих файлов:

- /etc/debian_release
- /etc/debian_version
- /etc/redhat-release
- /etc/redhat_version
- /etc/os-release
- /etc/SuSE-release
- /etc/fedora-release
- /etc/slackware-release
- /etc/slackware-version
- /etc/system-release
- /etc/mandrake-release
- /etc/yellowdog-release
- /etc/gentoo-release
- /etc/UnitedLinux-release
- /etc/vmware-release
- /etc/slp.reg

- /etc/oracle-release

Следующие команды также должны быть добавлены в белый список для учетной записи, с помощью которой осуществляется сканирование:

- cat
- find
- mysqlaccess
- mysqlhotcopy
- sh
- sysctl
- dmidecode
- perlsuid
- apt-get
- rpm

Ниже представлен перечень специфичных требований к привилегиям учетной записи указанных систем.

**AIX**

**ВАЖНО!**
**Для минимизации ложноположительных срабатываний необходимы привилегии root.**

- lslpp –cL to list packages
- oslevel
- emgr -l

**Blue Coat**

- show version

**Cisco**

Необходимы для поиска уязвимостей:

- show version

Необходимы для проведения аудита конфигураций:

- show version | include Cisco
- show interface
- show running-config
- show snmp host
- show run | include banner login
- show log | incl Trap logging
- show snmp user
- show snmp group
- show ip ssh | incl retries
- show cdp
- show ip ssh | incl timeout
- show running-config | include [ ]*neighbor[ ].[ ]*password
- show run | include banner exec
- show run | include banner motd

### Дистрибутивы на базе Debian

- uname
- dpkg
- egrep
- cut
- xargs

### F5

- "version", "show" или "tmsh show sys version"

### FreeBSD

- Для версий 10 и выше необходимы права на выполнение команды cat freebsd-version
- Для версии 9 и ниже необходимы права на выполнение команды cat /var/db/freebsd-update/tag
- pkg info

**Juniper**

- uname
- show version

**Mac OS X**

- /usr/sbin/softwareupdate
- /usr/sbin/system_profiler
- sw_vers

**Palo Alto Networks PAN-OS**

- show system info

**RPM-ориентированные ОС (Red Hat, SUSE и Oracle)**

- uname
- rpm
- chkconfig

**Solaris**

- showrev
- pkginfo
- ndd

**VMware ESX/ESXi**

- vmware -v
- rpm
- esxupdate -a query || esxupdate query