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

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
- Сокрытие 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.

Revision #2
Created 6 October 2025 16:15:18 by Admin
Updated 6 October 2025 16:50:21 by Admin