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

Изменения конфигурации или программного кода постоянно работающих в ОС сервисов и доступных для взаимодействия с пользователями извне.

Плюсы	Минусы
• Достаточно скрытный, т.к. логирование изменений в сервисах происходит на общем уровне внесения изменений в файловую систему, что сложнее заметить команде реагирования. • На доступность не влияет изменение учетных данных, прав доступа пользователей ОС. • Заложенные backdoor’ы в программный код сервисов могут быть обнаружены только профессионалами, понимающими природу возникновения уязвимостей. • Также одним из способов закрепления может быть обнаружение прочих уязвимостей сервиса без внесения в него изменений.	• При откате версии кода сервиса к последней стабильной, доступ теряется. • Заметен, если в ОС стоит аудит внесения изменения в файловую систему и в файлы конфигурации.

Примеры:

- Внедрение бэкдоров в сервисы ОС
- Внедрение уязвимого поведения в сервисы ОС для последующей эксплуатации уязвимостей
- Запуск внешних программ для получения последующего контроля

Revision #1
Created 6 October 2025 15:32:11 by Admin
Updated 6 October 2025 15:38:05 by Admin