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

Самые продвинутые и, зачастую самые надежные подходы по закреплению доступа, - это серия методов, позволяющих проникать глубоко в ядро ОС и изменять стандартные службы удаленного доступа, аутентификации, обработки событий и пр.

Плюсы	Минусы
• Некоторые из методов почти невозможно обнаружить при использовании стандартных средств анализа ОС, только используя глубокий анализ дампа памяти ОС (существуют методы, которые скрывают свое наличие при входе на сервер администратора и потом возвращают свое присутствие). • Такие методы зачастую могут действовать даже после обновления ОС, и, в частных случаях, даже после переустановки ОС. • Реализовать такой метод без действий, которые могут быть замечены в ходе выполнения, может быть непросто.	• Высокая сложность реализации таких методов, а также сложность их отладки. • Разница в версии ОС или дистрибутиве может быть критически важной для выбора метода закрепления из этой категории.

Rootkit

Вид вредоносного программного обеспечения, которое скрывает свою присутствие на компьютере или другом
устройстве, изменяя функциональность операционной системы и скрывая свои следы от пользователей и системных программ.

TripleCross - Linux eBPF-руткит с открытым исходным кодом по технологии eBPF*.

eBPF (Extended Berkeley Packet Filter) - технология ядра Linux, расширяющая функциональность стандартного фильтра Berkeley Packet Filter (BPF) для обработки пакетов и мониторинга событий в ядре.

Работа eBPF осуществляется через специальное виртуальное машинное окружение (VM), которое запускается внутри ядра Linux.Оно позволяет загружать и исполнять программы на языке C, которые могут обрабатывать пакеты на уровне ядра, принимать решения о пересылке или отбрасывании пакетов, создавать и мониторить события в ядре и многое

другое.

Remote Admin Tool

Похоже на RootKit, но менее скрытная. Утилиты RAT (Remote Access Tool) — это программные инструменты, которые позволяют удаленно управлять компьютером или устройством без ведома пользователя. RAT-утилиты могут быть использованы для различных целей, в том числе для управления компьютером из удаленного места, сбора конфиденциальной информации, мониторинга активности пользователя и т.д.

Revision #1
Created 6 October 2025 15:40:09 by Admin
Updated 6 October 2025 15:48:10 by Admin