

Сохранение вредоносного кода

Сабина Жигальская

Специалист по комплексной защите информации

Skillbox

Сохранение вредоносного кода

Цель урока

Узнаем о сохранении вредоносного кода в системе.

«Вирусов под Unix не бывает»

Большинство вирусов и иных вредоносных средств ПО создавались под Windows.

В Linux для того чтобы нанести глобальный вред системе или внести в неё фундаментальные изменения, вредоносная программа должна получить root-доступ к целевой системе в целом.

Root-доступ в Linux

Получить привилегии суперпользователя можно с помощью:

- эксплойтов, эксплуатирующих незакрытые уязвимости в ядре Linux или в сервисах, имеющих root-привилегии для собственной деятельности
- методов социальной инженерии (например, попытки выдать вирус за легальное приложение, требующее административных полномочий)

Способы заражения Linux-систем

- 1 Бинарные файлы и исходные коды
- 2 При помощи Wine

Класс файловых вирусов практически перестал существовать, уступив место троянам и бэкдорам.

Основные типы вредоносного ПО

- 1 Вирусы — это вид вредоносных программ, способных внедряться в код других программ, системные области памяти, загрузочные секторы и распространять свои копии по разнообразным каналам связи. Основная цель вируса — распространение

Яркий представитель этого семейства — червь Морриса.



Основные типы вредоносного ПО

- 2 Трояны — разновидность вредоносной программы, проникающая в компьютер под видом легитимного программного обеспечения в отличие от вирусов и червей, которые распространяются самопроизвольно

Яркий представитель этого семейства — AIDS Trojan.



Выводы урока

- ✓ Концептуальный подход к заражению систем UNIX и Windows кардинально различается
- ✓ В UNIX для внедрения с максимальным эффектом необходим тотальный контроль над системой, то есть получение root-прав в системе