Шеллкоды

Сабина Жигальская
Специалист по комплексной защите информации

Skillbox

Цели урока

- Узнать, что такое шеллкод
- Разобрать его особенности

Ядро Linux

Ядро операционной системы — это её основа.

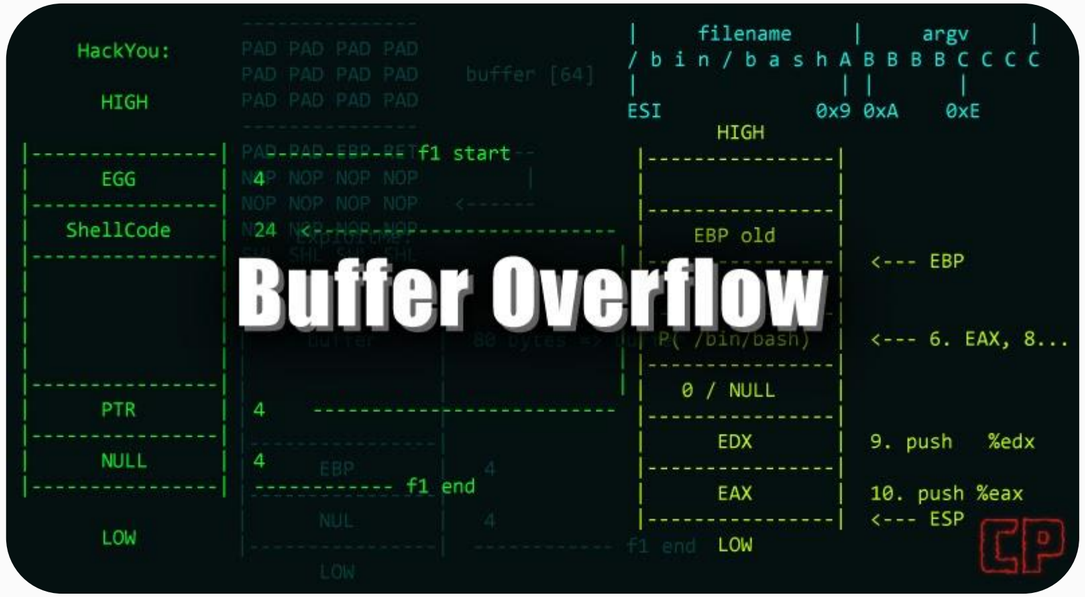
Скомпрометированное ядро представляет опасность для работы всех служб.

Шеллкод

Шеллкод — это двоичный исполняемый код, который передаёт управление командному процессору.

Шеллкод

Одним из популярных шеллкодов является переполнение буфера (стека).



Особенности шеллкода

- Можно встроить в любой процесс
- Не должен иметь глобальные переменные
- Не должен содержать системных вызовов и функций

Выводы урока

- Узнали, что такое шеллкод
- Разобрали его особенности

Выводы модуля

- Ядро — это главная часть абсолютно любой операционной системы. Оно является приоритетным и запускается первым
- В операционной системе Linux можно выбрать версию загружаемого ядра
- Ядро Linux позволяет настраивать большинство параметров
- GRUB — основной загрузчик Linux, который позволяет выбрать, какую операционную систему загружать
- Безопасность ядра — залог бесперебойной работы системы
- Узнали, как шеллкод встраивается в процесс и какие у него особенности