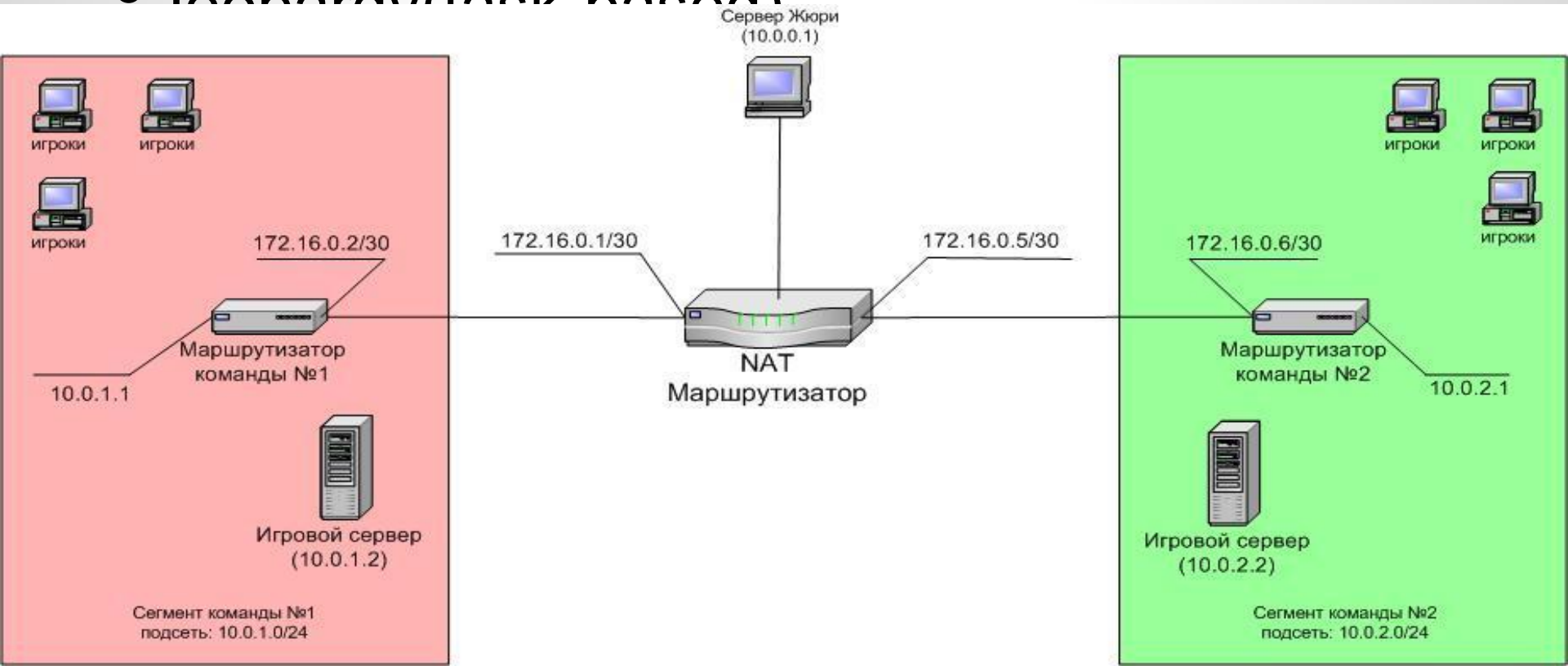

CTF
CAPTURE THE FLAG

# Что такое CTF?

CTF (Capture the flag, Захват флага) — командные соревнования по компьютерной безопасности, в которых участники исследуют заранее заложенные уязвимости предоставленных сервисов, обеспечивают безопасность своих ресурсов и пытаются атаковать ресурсы противников, захватывая «флаги» со скомпрометированных сервисов.

# Варианты соревнований

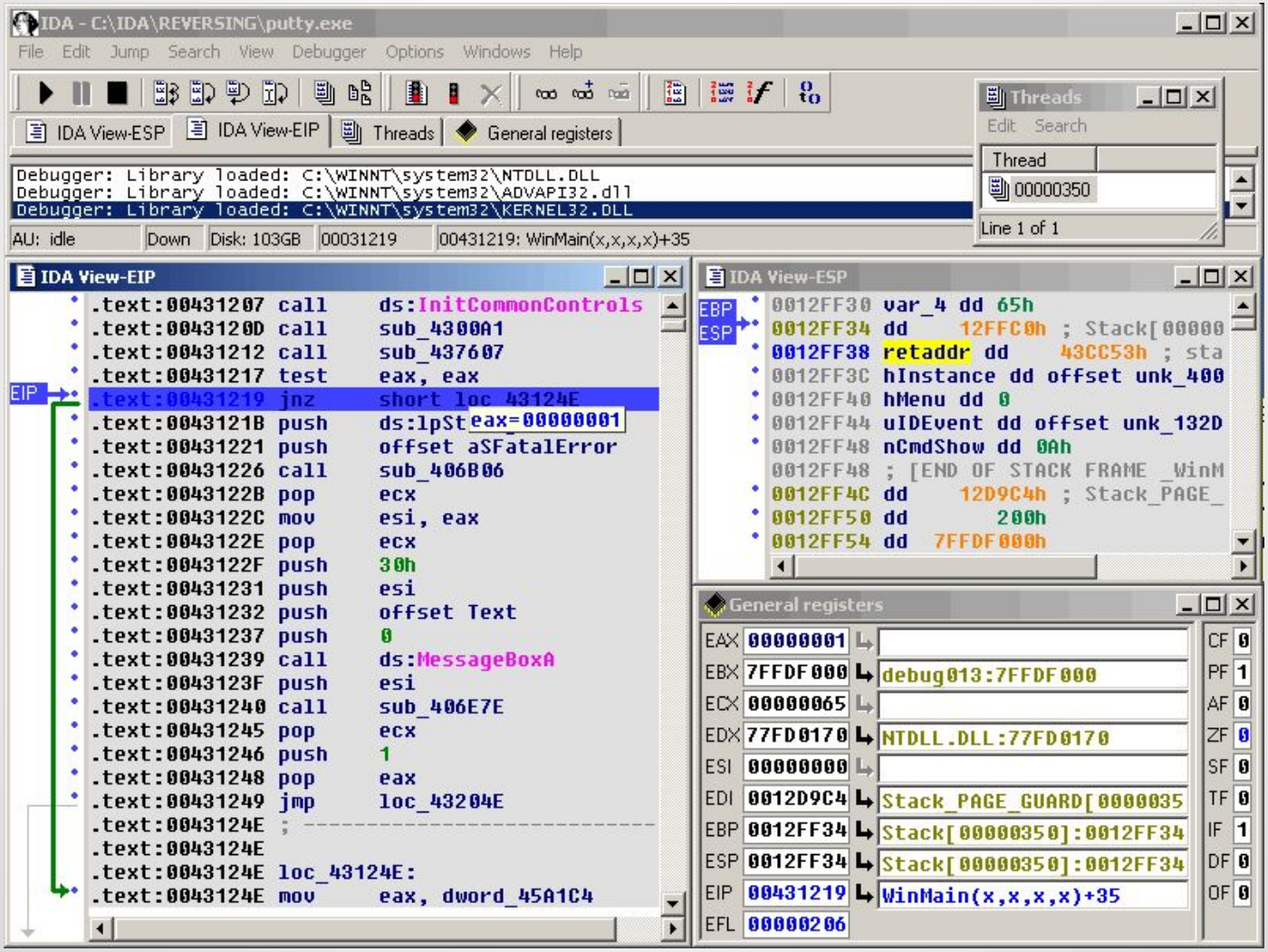
- Attack-defense(classic)
- Jeopardy(task-based)



# Категории task-based CTF

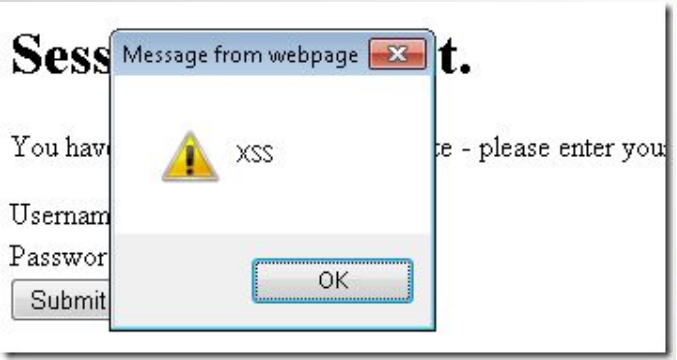
- admin — задачи на администрирование, настройку сети
- joy — различные развлекательные задачи вроде коллективной фотографии или игры в какую-нибудь мини-игру
- ppc — задачи на программирование (professional programming and coding)

# Reverse Engineering



# Web

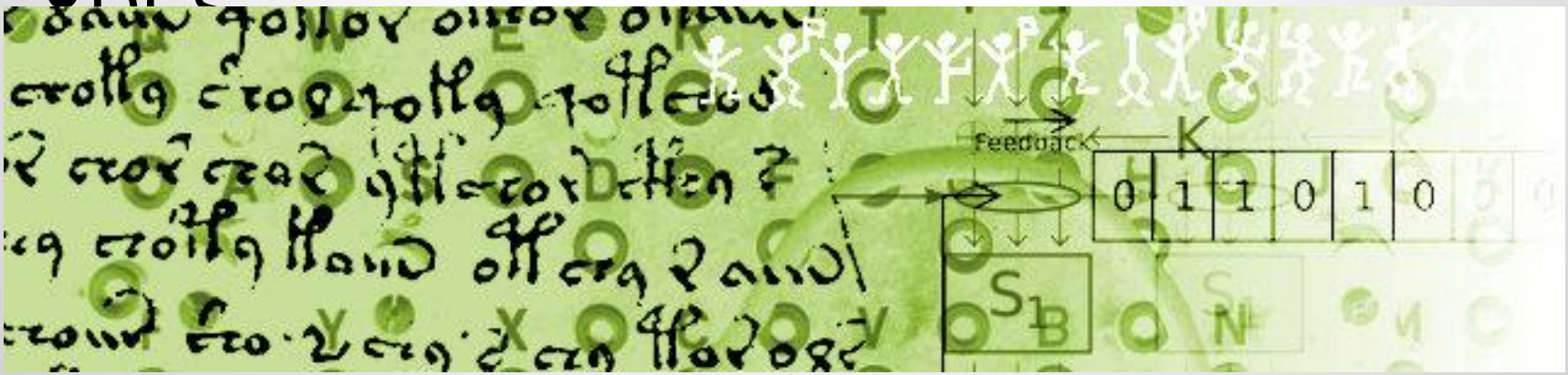
- SQL injection
- XSS
- CSRF
- Directory traversal


```php
<?
if(is_numeric($_GET['show'])&&isset($_GET['ver'])){
    if($_GET['ver']===phpversion()){
        if(!is_numeric($_REQUEST['show'])&&is_numeric($_REQUEST['ver'])){
            die('Flag: FLAGISHERE');
        }
        die("<script>alert('Failed #2')</script>");
    }
    die("<script>alert('Failed #1')</script>");
}
die("<script>alert('Failed #0')</script>");
?>
```

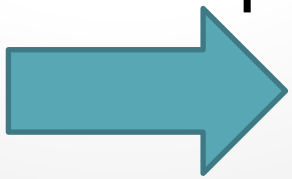
# Crypto

- AES
- RSA
- ГОСТ 28147-89
- DES



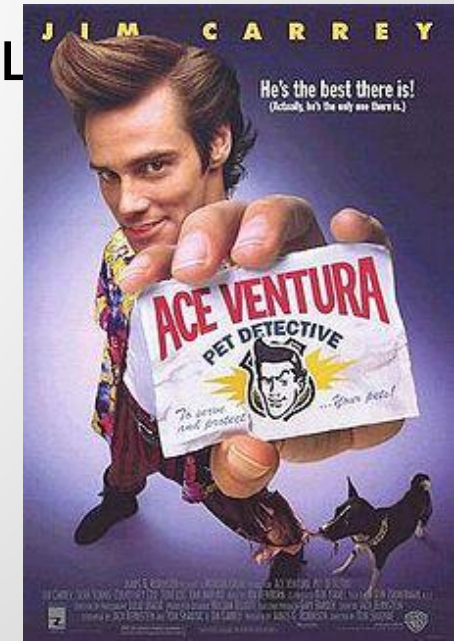
# Steganography

- Стеганография - это наука о скрытой передаче информации путём сохранения в тайне самого факта передачи.
- Преимущество – сообщение не привлекает к себе внимания.
- Отли няется кри й.



# Forensics

- Ответвление криминалистики, сочетающее в себе восстановление и расследование материалов, найденных на электронных носителях.
- Криминалистика – наука, исследующая закономерности приготовления, соверш и раскрытия преступлений.



# Exploit

- **Эксплойт**, **эксплоит**, **сплоит** (англ. *exploit*, эксплуатировать) — компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему. Целью атаки может быть как захват контроля над системой (повышение привилегий), так и нарушение её функционирования (DoS-атака).


Capture The Flag!