



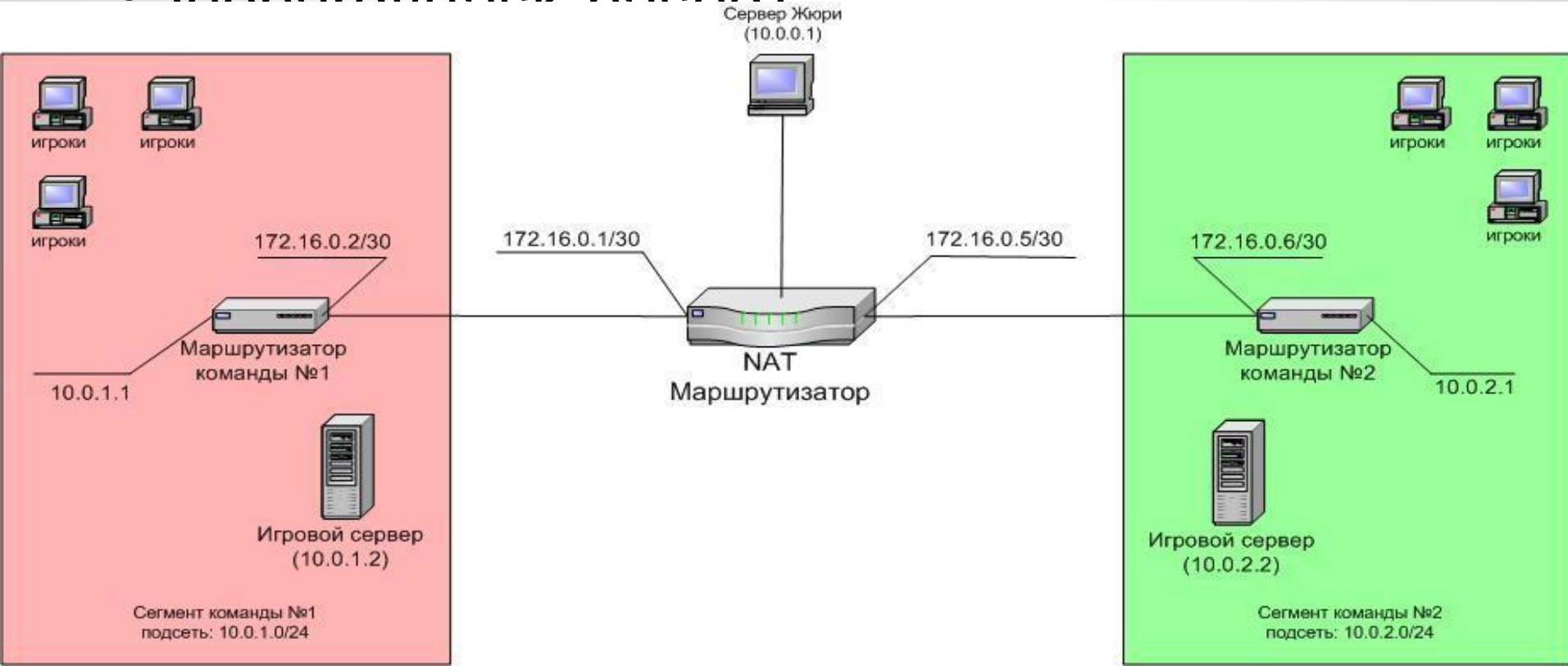
**CAPTURE THE FLAG**

# 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» скомпрометированных сервисов.

# Варианты соревнований

- Attack-defense(classic)
- Looprdy(tool 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

The screenshot displays the IDA Pro interface for a debugger session. The main window shows assembly code for a function named `WinMain(x,x,x,x)+35`. The instruction at address `00431219` is highlighted: `jnz short loc_43124E`. The instruction pointer (EIP) is shown as `00431219`. The stack view (IDA View-ESP) shows the current stack frame, with the return address `retaddr` at `0012FF38` pointing to `43CC53h`. The general registers window shows the state of various registers, including `EAX` (00000001), `EBX` (7FFDF000), `ECX` (00000065), `EDX` (77FD0170), `ESI` (00000000), `EDI` (0012D9C4), `EBP` (0012FF34), `ESP` (0012FF34), `EIP` (00431219), and `EFL` (00000206). The status bar indicates the current instruction is `WinMain(x,x,x,x)+35`.

Debugger: Library loaded: C:\WINNT\system32\NTDLL.DLL  
Debugger: Library loaded: C:\WINNT\system32\ADVAPI32.dll  
Debugger: Library loaded: C:\WINNT\system32\KERNEL32.DLL

ALU: idle    Down    Disk: 103GB    00031219    00431219: WinMain(x,x,x,x)+35

Threads: 00000350

General registers:

EAX	00000001		CF	0
EBX	7FFDF000	debug013:7FFDF000	PF	1
ECX	00000065		AF	0
EDX	77FD0170	NTDLL.DLL:77FD0170	ZF	0
ESI	00000000		SF	0
EDI	0012D9C4	Stack_PAGE_GUARD[0000035]	TF	0
EBP	0012FF34	Stack[00000350]:0012FF34	IF	1
ESP	0012FF34	Stack[00000350]:0012FF34	DF	0
EIP	00431219	WinMain(x,x,x,x)+35	OF	0
EFL	00000206			



# Web

- SQL injection
- XSS
- CSRF
- Directory traversal

## WEB SECURITY: SQL INJECTION

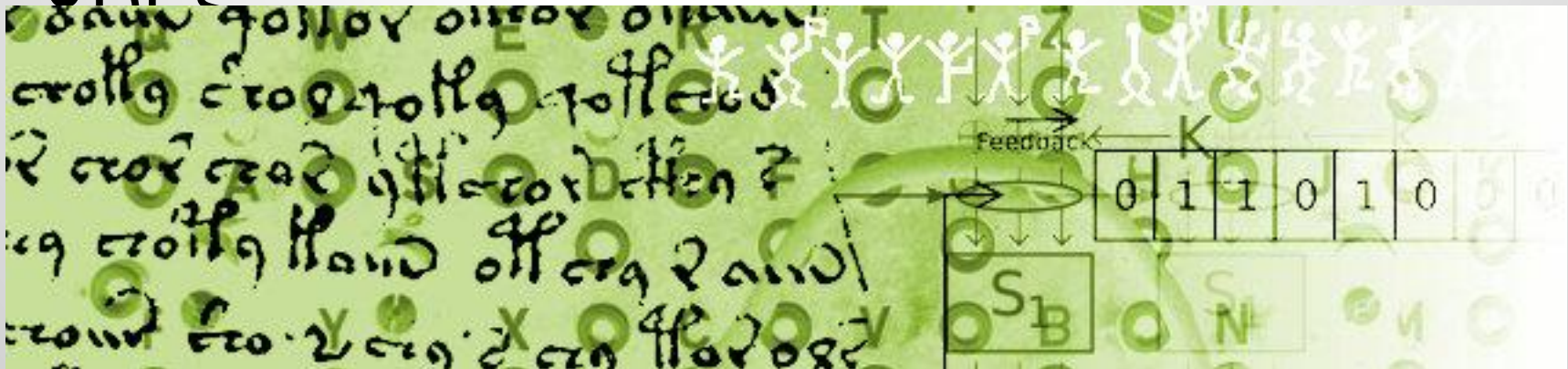


```
<?
if(is_numeric($_GET['show'])&&isset($_GET['ver'])){
    if($_GET['ver']==phpversion()){
        if(!is_numeric($_REQUEST['show'])&&is_numeric($_REQUEST['ver']))){
            die('Flag: FLAGISHERE');
        }
        die("<script>alert('Failed #2')</script>");
    }
    die("<script>alert('Failed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

# Crypto

- AES
- RSA
- ГОСТ 28147-89

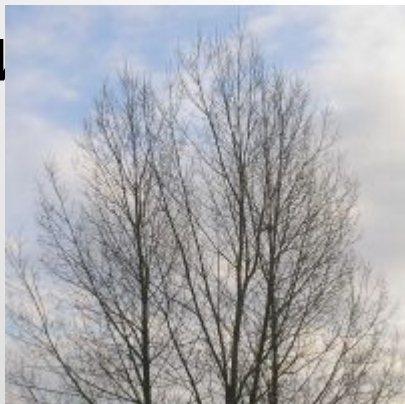
- DES



# Steganography

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

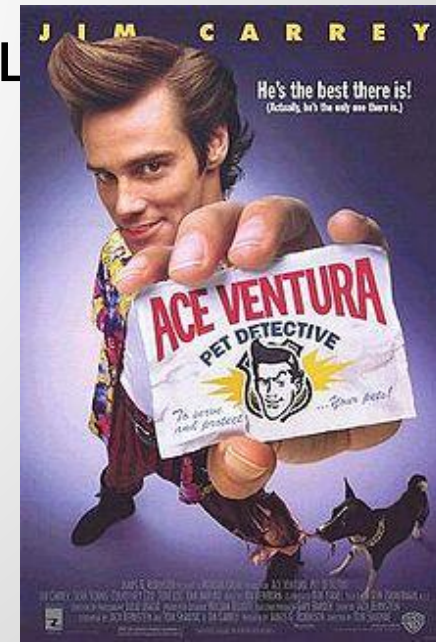
- Отличительная особенность – не привлекает к себе внимания кри...





# Forensics

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



# Exploit

- **Эксплойт, эксплоит, спloit** (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!**

