Awesome coolkaveh advisory

Penetration test is my keyservice

coolkaveh@rocketmail.com

•?((¯°·._.• ČÕÕĹĶÃüĘĤ •._.·°¯))؟•

http://twitter.com/coolkaveh

MOV DWORD PTR DS:[ECX],EAX
MOV DWORD PTR DS:[EAX+4],ECX

connection timeout

```
"\x2d\x4a\x83\xe8\xfc\x31\x58\x14\x03\x58\xee\x2f\xd8\xb6" +
"\xe6\x39\x23\x47\xf6\x59\xad\xa2\xc7\x4b\xc9\xa7\x75\x5c" +
"\x99\xea\x75\x17\xcf\x1e\x0e\x55\xd8\x11\xa7\xd0\x3e\x1f" +
```

server is too busy

running out of swap space

Access violation at address

segmentation fault

```
EAX 41414141
ECX 41414141
EDX 00050740 ASCII "AAAAAAAAAAAAAAAAAAAA
EBX 00000024
ESP 0012F814
EBP 0012F82C
ESI 00050740 ASCII "AAAAAAAAAAAAAAAAAAAA
EDI 00050000
EIP 77F6256F ntdll.77F6256F
C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 1  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 0038 32bit 7FFDE000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_ENVVAR_NOT_FOUND (00
EFL 00010246 (NO,NB,E,BE,NS,PE,GE,LE)
```

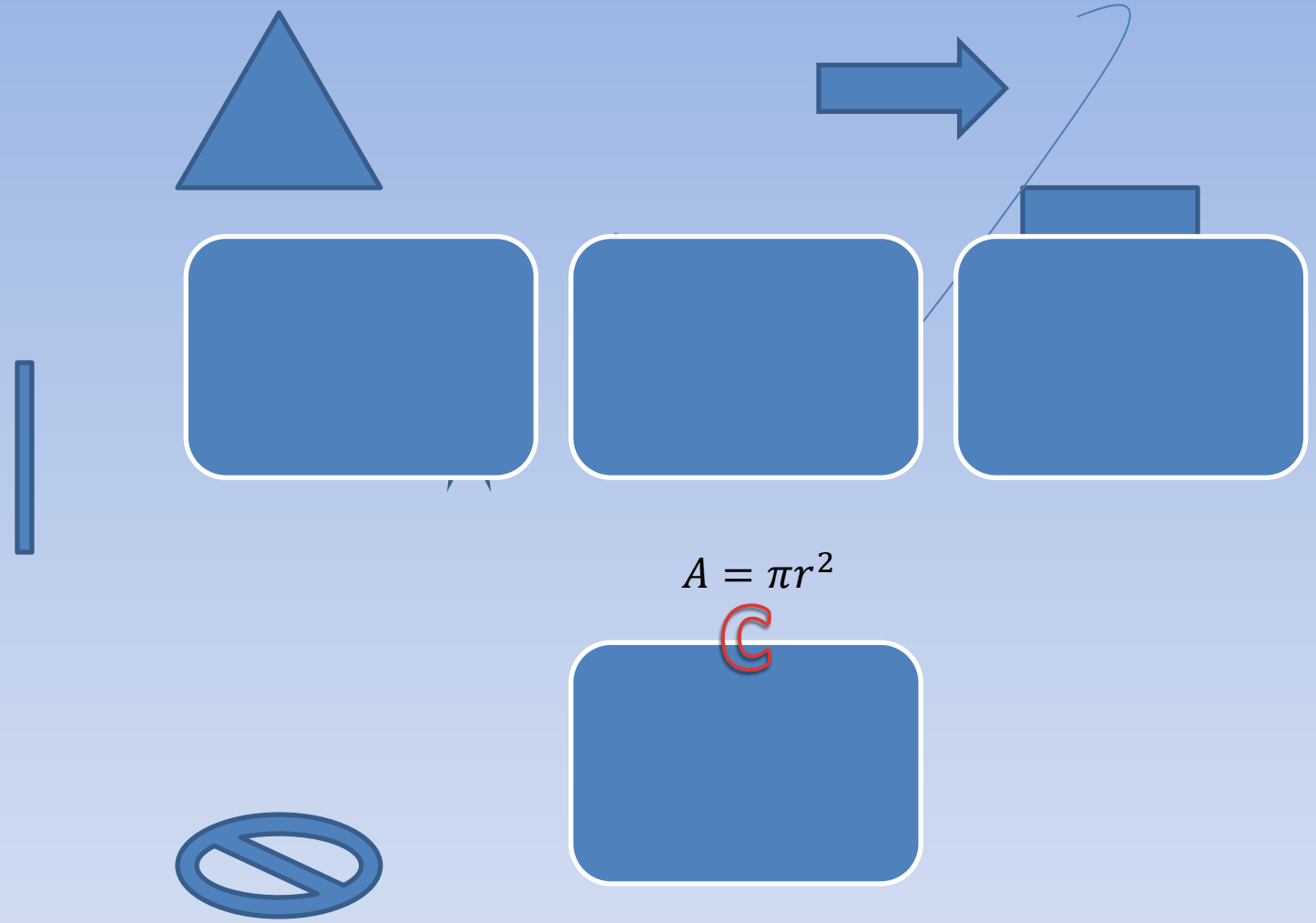
who am i ?
root

Heap ThaiChi

ROP + Leak + Heap FengShui

Use-After-Free

Heap Spray


$A = \pi r^2$