00401020 push ebp

00401021 mov ebp,esp

00401023 sub esp,40h

00401026 push ebx

00401027 push esi

00401028 push edi

00401029 lea edi,[ebp-40h]

0040102C mov ecx,10h

00401031 mov eax,0CCCCCCCCh

00401036 rep stos dword ptr [edi]

6: while(1)

00401038 mov eax,1

0040103D test eax,eax

0040103F je pri+30h (00401050)

7: {

8: printf("attack!\n");

00401041 push offset string "attack!\n" (0042201c)

00401046 call printf (004010a0) 相对寻址，5a

0040104B add esp,4

9: }

0040104E jmp pri+18h (00401038)

10: }

00401050 pop edi

00401051 pop esi

00401052 pop ebx

00401053 add esp,40h

00401056 cmp ebp,esp

00401058 call \_\_chkesp (00401120)

0040105D mov esp,ebp

0040105F pop ebp

00401060 ret

0012FECA push ebp

0012FECB mov ebp,esp

0012FECD sub esp,40h

0012FED0 push ebx

0012FED1 push esi

0012FED2 push edi

0012FED3 lea edi,[ebp-40h]

0012FED6 mov ecx,10h

0012FEDB mov eax,0CCCCCCCCh

0012FEE0 rep stos dword ptr [edi]

0012FEE2 mov eax,1

0012FEE7 test eax,eax

0012FEE9 je 0012FEFA

0012FEEB push offset string "attack!\n" (0042201c)

0012FEF0 call 0012FF4A相对5a

0012FEF5 add esp,4

0012FEF8 jmp 0012FEE2

0012FEFA pop edi

0012FEFB pop esi

0012FEFC pop ebx

0012FEFD add esp,40h

0012FF00 cmp ebp,esp

0012FF02 call 0012FFCA

0012FF07 mov esp,ebp

0012FF09 pop ebp

0012FF0A ret