Mažas pradžiamokslis: Programavimas asembleriu Linuxe

Siūlau naudotis:

1) **NASM** (http://nasm.souceforge.net) senas geras kompiliatorius
2) **YASM** (http://www.tortall.net/projects/yasm/) naujas, kažkuo geras, bet stokoja dokumentacijos
3) **ALD** (http://ald.sourceforge.net) assembly Linux debbuger. Irgi šviežias ir jau daug patogesnis naršyti po kodą negu didysis **GDB** (http://www.gnu.org/software/gdb/gdb.html).
4) **VIM** (http://www.vim.org) geriausias geek'o pasirinkimas

Patarimai ir sisteminiai iškvietimai:

1) **BIOS** funkcijų pasiekti negalėsite ir taip pat užmirškite apie **DOS** funkcijas. Dabar jūsų vieninteliai draugai yra int 0x80 (syscalls), **libc** ir svetimas kodas:)
2) Dar kartą: Visos operacijos susijusios su **OS** atliekamos per branduolio syscalls
3) Turėkite savo branduolio išeities kodą.
4) Turėkite arti savęs http://world.std.com/~slanning/asm/syscall_list.html Atkreipkite dėmesį į source kolonėlę, tai kelias prie failo jūsų kernelio išeities kode, kur aprašytas jums reikalingas sisteminis iškvietimas (syscall). Jei jums reikės išsiaiškinti syscall'ų argumentų ar gražinto parametro reikšmę – nebijokite nagrinėti išeities kodą. Taip sutaupysite laiko ir galimas daiktas kad tai bus vienintėlė vieta kur rasite informaciją.
5) Peržvelkite http://www.linuxassembly.org/intro/Assembly-Intro.html
6) Apsilankykite http://www.linuxassembly.org
7) Prisijunkite prie bendraminčių konferencijos http://world.std.com/~slanning/asm/syscall_list.html

Komandinės eilutės parametrai

... perduodami per steką: [esp] yra perduotų parametrų skaičius, [esp +4], pirmas parametras, [esp +8] antras .... Parametrai perduodami eilutėmis, kurios baigiasi 0.

Truputį informacijos apie darbą su failais

Sisteminių iškvietimų sąraše minimas 'mode' yra leidimai, kurie taikomi failams. Neradau informacijos kodėl, bet sys_open ir sys_create neleidžia suteikti a+w arba g+w leidimų.

- sys_open
  int sys_open(const char * filename, int flags, int mode);
  flag parametro žemesnių (low) dviejų bitų reikšmė: 00 – atidaryti tik skaitymui, 01 – atidaryti tik rašymui, 10 – atidaryti ir skaitymui ir rašymui, 11 – specialus režimas.
- sys_lseek
  Pirmas parametras failo yra deskriptorius, antras – poslinkis nuo failo pradžios, 3 – 'orgin' režimas. Orgin reikšmė gali būti: 00 – SEEK_SET pasislinkti kaip nurodyta pirmame parametre, 01 – SEEK_CUR gražinti poslinkio reikšmę, 02 – SEEK_END pasislinkti į galą ir gražinti poslinkį.
- sys_read ir sys_write
  Abu gražina perskaitytų/įrašytų baitų skaičių.

Kodo tarkavimas:) (Debugging)

Esminės komandos yra run, break, examine, continue (RTFM aka help). Patarimas **GDB** naudotojams yra http://www.linuxselfhelp.com/HOWTO/Assembly-HOWTO/faq.html#AEN941.
Dirbant su **NASM** kompiliuoti norinėdami tarkuoti turite taip:
nasm -f elf -g foo.asm
ld -o foo foo.o

Siūlau visiems, kuriems šis dokumentas nors kiek padėjo (ir tiems kuriem ne padėjo), praturtinti jį savo žiniomis.