Process Freezer

cnoize@chroot.org

Dec 2004

Outline

Checkpoint
Process Freezer
Demo
Other Checkpointing Packages

- CheckPoint

  http://www.checkpointing.org/
- Checkpoint/Restart

  Suspend/Resume
- Software Suspend

  http://swsusp.sf.net/

  suspend-to-disk - Linux

  hibernate - Windows

- CryoPID

  A Process Freezer for Linux

  http://cryopid.berlios.de/

  CryoPID allows you to capture the state of a running process in Linux and save it to a file.

  This file can then be used to resume the process later on, either after a reboot or even on another machine.

- No root privileges needed.
- Can start & stop a process multiple times.
- Migrate processes between machines
  and between kernel.
  (save all libraries to the image)

Demo

- ptrace()
- stub.c
- ELF writer
- get_one_vma (/proc)
- do_syscall() // get_file_offset
- get_termios()

- open_self()
- seek_to_image()
- resume_image_from_file()
- put_shell_code()

```
int get_one_vma(pid_t target_pid, char* map_line,
struct map_entry_t* m, int get_library_data) {
/* Parse a line that looks like one of the following:
08048000-080ab000 r-xp 00000000 03:03 1309106
/home/b/dev/sp/test
080ab000-080ae000 rw-p 00062000 03:03 1309106
 /home/b/dev/sp/test
080ae000-080db000 rwxp 00000000 00:00 0
40000000-40203000 rw-p 00000000 00:00 0
bfffe000-c0000000 rwxp 00000000 00:00 0
*/
```

```
int do_syscall(pid_t pid, struct user_regs_struct *regs)
ptrace(PTRACE_GETREGS, pid, NULL, &orig_regs);
old_insn = ptrace(PTRACE_PEEKTEXT();
PTRACE_POKETEXT
PTRACE_SETREGS
PTRACE_SINGLESTEP /* Execute call */
PTRACE_GETREGS
PTRACE_SETREGS /* Return everything back to normal */
PTRACE_POKETEXT
```

- root privileges
- modifications to the kernel
- recompiling/relinking your software
- using an LD_PRELOAD when you start your program.

- Ckpt - A process checkpoint library

  http://www.cs.wisc.edu/~zandy/ckpt/

- Paradyn Project Papers

  http://www.cs.wisc.edu/paradyn/papers/#hijack

  ftp://ftp.cs.wisc.edu/paradyn/technical_papers/hijack.pdf

  Process Hijacking (PDF)

- http://appcap.ihaquer.com/

- Appcap is a tricky application for x86 Linux which allows the user with enough power (usually the superuser) on a Linux machine to attach and redirect standard input and output of any application to his actual tty.

- file descriptor passing

END