Linux ASLR Curiosities

Tavis Ormandy
Julien Tinnes
Google Security Team

ASLR

- Address space layout randomization
- First came out as a PaX feature in about 2002
- Makes an attacker's life harder
- Now has reached most mainstream OS

Known info leak ?

- It's well understood that /proc/pid contains information that would defeat ASLR for a local attack
- The kernel developers thought about /proc/pid/maps
- They recently decided to blank /proc/pid/maps if you cannot ptrace attach to pid (2.6.22)

Not so sure

- It's a little known fact that /proc/pid/stat and wchan will leak information such as instruction pointer and stack pointer
- Try ps -eo pid,eip,esp,wchan
- Has been protected in GRSecurity for 7 years

Exploitable to defeat ASLR?

- We only have scarce samples (Kstkeip is only updated during context switches and syscalls)
- An i/o bound or blocking process will leak very few samples
- It's not obvious or intuitive if this is enough information to reconstruct the address space

Let's try

- X86 is a variable width architecture
- We know what code is loaded in the target process
- By dissassembling this code and recording instruction boundaries, we can create a unique ”fingerprint” of the code it contains.
- Are the very few (a dozen or so) samples we can read enough to reconstruct AS layout?

DEMO!