

AHA! 0X12

Eighteen is the loneliest number that you'll ever do.
(AKA: OSX, Firewire and a whole lot of FAIL)

OSX Memory and Firewire

- Dumping process virtual memory pages using Mach VM API
- Dumping physical memory via firewire
- OSX memory profiling
- Loginwindow.app memory sanitization bug

OSX Virtual Memory

- `/usr/bin/vmmap`
 - display processes' virtual memory infos
- `/System/Library/PrivateFrameworks/vmutils.framework/Versions/A/vmutils`
 - This is where the magic happens
 - Still 'magic' to me - more work to do here

OSX Virtual Memory

- `otool -tvV <vmutils framework>`
 - symbolic disassembly / poor man's IDA
- `otx` - nice `otool` frontend that resolves all those `_obj_msgSend()` calls
- `class-dump <vmutils framework>`
 - generate the `.h` files for the framework

VMemory Scanner

- Uses the Mach virtual memory API
 - `vmscan()` `vmread()` `vmprotect()`
- Creates files of all contiguous process virtual memory
- Starting point for future memory profiling of processes
- `vmscan` must minimally run as `gid procview`

OSX

FW Memory Dumper and Scanner

- Python wrapper around OSX
- [http://c0re.23.nu/c0de/pyfw/
pyfw-20041111.tar.gz](http://c0re.23.nu/c0de/pyfw/pyfw-20041111.tar.gz)
- Dumper 'works'
- Password scanner 'in the works'

Linux FW Memory Scanner

- Python library for firewire
- Goal is to get running on iPod linux
- Bucket of fail with extra slaw

Loginwindow.app

- LoginWindow is the (duh) process that shows the login UI
- It doesn't clear your password from memory
- For the life (?) of being logged in
- Even when screen locked
- Filevault passwords too :)

/* XXX TODO: Linux iPod Password Dumper */

- Still have to get this working
- Basic idea is to get the python code working and run it on a gen3 ipod to dump password from OSX over firewire
- Stealthy (kinda)

/* XXX TODO: Profiling Memory */

- Want to be able to know 'what kind' of memory is at a given location(data/code)
- Use vmutils framework?
- Eventually put shellcode into memory and trigger
- Looking over LoginWindow code (bypass authentication)

Resources

- OSX Internals - Amit Singh
- Weasel iPhone Debugger
- otx.osxninja.com
- <http://metasploit.com/dev/trac/wiki/Firewire>
- Codes will be posted somewhere