Integrating DMA attacks in Metasploit

Rory Breuk rbreuk@os3.nl
Albert Spruyt aspruyt@os3.nl

University of Amsterdam

May 23, 2012
Introduction

Goal:
Metasploit Over Firewire Ownage
Computer architecture

CPU

Northbridge

Southbridge

PCMCIA

FireWire

PCI

SATA

Thunderbolt

RAM
Computer architecture

- CPU
- RAM
- Northbridge
- Southbridge
- PCMCIA
- FireWire
- PCI
- SATA
- Thunderbolt
Computer architecture cont.

Memory divided into 4KiB pages
Virtual / physical addresses
DMA attack vectors

- FireWire
- Thunderbolt
- PCMCIA/CardBus/ExpressCard

- Plug-and-Play and no driver required
Previous work

Encryption key/ password extraction
Winlockpwn/FTWAutopwn/Inception
libforensic1394
Goals

Use DMA attacks with Metasploit

Why?

• Huge potential, but under utilized
• Widespread awareness is lacking
• Making it easy
• Lots of possibilities
Use case

Local attacker

Target

IEEE1394

Internet

Remote attacker
Usecase

Local attacker

169.254.x.x

Target

IEEE1394

Internet

Remote attacker
Metasploit concepts

Exploits
Payloads
Payloads

What to patch

Library call

Patch

12/25
Windows DEMO

Target: Windows 7 SP1 32bit
Find the signature
Inject payload
Problems

Need to interact with the system
Easily user detectable
Detectable by tripwire
Proposed solution

Stage 1:
- Inject stager
- Allocate new page

Stage 2:
- Restore originally patched code

Stage 3:
- Inject second stager
- Restore process
- Execute payload
Stage 1: Inject stager

Find signature
Save code
Inject special stager
Stage 2: Restore code

Find the new page
Restore patched code
Stage 3: Finish

Upload second stager + payload

Directly overwrites running code
Interactionless exploit

Xorg

- root permissions
- runs periodically
Linux DEMO

Target: Ubuntu 12.04
Look ma, no hands!
Stagers, IDS evasion
Target process is kept alive
Mitigation: theoretical

Theoretical:

- IOMMU

No practical implementations
Mitigation: practical

For the consultants:

- Don’t buy them
- Destroy them / glue them
- Disable them
- Deny physical access

Does not guarantee safety
Achievements

Ported libforensic1394 bindings to Ruby
Integrate FireWire exploit into Metasploit
Reusable technique for DMA exploitation
Achievements

Enhanced attack:

- Smaller attack window
- Attack continued over TCP/IP
- Interactionless payload execution
- Use Metasploit functionality

https://github.com/mrbreaker/mofo
Metasploit Over Firewire Ownage

Questions?

https://github.com/mrbreaker/mofo