# PUSHING BOULDERS UPHILL: THE DIFFICULTY OF NETWORK INTRUSION RECOVERY

USENIX LISA 2009

M. Locasto, M. Burnside, & D. Bethea

# Take-home Message



"The problem of network intrusion recovery is a particularly thorny exercise in researching, designing, and creating usable security mechanisms."

# Challenge: Intrusion Recovery

What should I do when my infrastructure is infiltrated on a massive scale?

# Sage Advice

"Damage control is much easier when the actual damage is known. If a system administrator doesn't have a log, he or she should reload his compromised system from the release tapes or CD-ROM."

- Firewalls and Internet Security: Repelling the Wily Hacker (1994)

# Intrusion Recovery: Art, Not Science



- Scenario and attack diversity
  - Institutional and technology differences
- Stigma or legal consequences to admitting breaches
  - Lack of public, documented scenarios

- **Lack of techniques that smoothly handle both technical and human factors involved in recovery**
- Thinking of detection and repair as "accomplished" rather than perpetually "ongoing" is misleading

# Adding to the Lore



- Cliff Stoll's "Stalking the Wily Hacker" (05/88)
- Spafford's analysis of Morris Worm (06/89)
- Cheswick's log of the Berferd case (01/92)
- Abe Singer's experiences (02/05)
- Frields: "Chronicle of a Server Break-in" (03/09)

# Intrusion Incidents



- March 2007
- December 2007
- March 2008

- Many other anecdotes
  - Virginia Prescription Monitoring Database ($10M ransom)
  - Breaches of U.S. electric grid
- Verizon 2008 Data Breach Incident Report

# Organization Details, Pre-Incident



- Mid-sized academic department at large university
- Roughly 1000 heterogeneous workstations
- ~50 infrastructure machines
- Network infrastructure generally not firewalled
- Three to five staff members, single manager
  - Range of experience

# December 2007

| | | | | | | |
|---|---|---|---|---|---|---|
| 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 16 | 17 | 18 | 19 | 20 | 21 | 22 |
| 23 | 24 | 25 | 26 | 27 | 28 | 29 |
| 30 | 31 | | | | | |

# December 2007

| | | | | | | |
|---|---|---|---|---|---|---|
| 2 | 3 | 4 | 5 | 6<br>detection | 7 | 8 |
| 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 16 | 17 | 18 | 19 | 20 | 21 | 22 |
| 23 | 24 | 25 | 26 | 27 | 28 | 29 |
| 30 | 31 | | | | | |

# December 2007

| | | | | | | |
|---|---|---|---|---|---|---|
| 2 | 3 | 4 | 5 | 6 detection | 7 | 8 |
| 9 | 10 detection | 11 | 12 | 13 | 14 | 15 |
| 16 | 17 | 18 | 19 | 20 | 21 | 22 |
| 23 | 24 | 25 | 26 | 27 | 28 | 29 |
| 30 | 31 | | | | | |

# December 2007

| | | | | | | |
|---|---|---|---|---|---|---|
| 2 | 3 | 4 | 5 | 6 detection | 7 | 8 |
| 9 | 10 detection | 11 | 12 | 13 diagnosis | 14 diagnosis | 15 |
| 16 | 17 diagnosis | 18 | 19 | 20 | 21 | 22 |
| 23 | 24 | 25 | 26 | 27 | 28 | 29 |
| 30 | 31 | | | | | |

# December 2007

| | | | | | | |
|---|---|---|---|---|---|---|
| 2 | 3 | 4 | 5 | 6 detection | 7 | 8 |
| 9 | 10 detection | 11 | 12 | 13 diagnosis | 14 diagnosis | 15 |
| 16 | 17 diagnosis | 18 | 19 | 20 | 21 | 22 |
| 23 | 24 | 25 | 26 | 27 | 28 | 29 |
| 30 | 31 | | | | | |

# December 2007

| | | | | | | |
|---|---|---|---|---|---|---|
| 2 | 3 | 4 | 5 | 6 detection | 7 | 8 |
| 9 | 10 detection | 11 | 12 | 13 diagnosis | 14 diagnosis | 15 |
| 16 | 17 diagnosis | 18 | 19 | 20 | 21 | 22 |
| 23 | 24 | 25 | 26 | 27 | 28 | 29 |
| 30 | 31 | | | | | |

# December 2007

| | | | | | | |
|---|---|---|---|---|---|---|
| 2 | 3 | 4 | 5 | 6 detection | 7 | 8 |
| 9 | 10 detection | 11 | 12 | 13 diagnosis | 14 diagnosis | 15 |
| 16 | 17 diagnosis | 18 | 19 | 20 | 21 | 22 |
| 23 | 24 | 25 | 26 | 27 | 28 | 29 |
| 30 | 31 | | | | | |

Last day for half the IT staff.

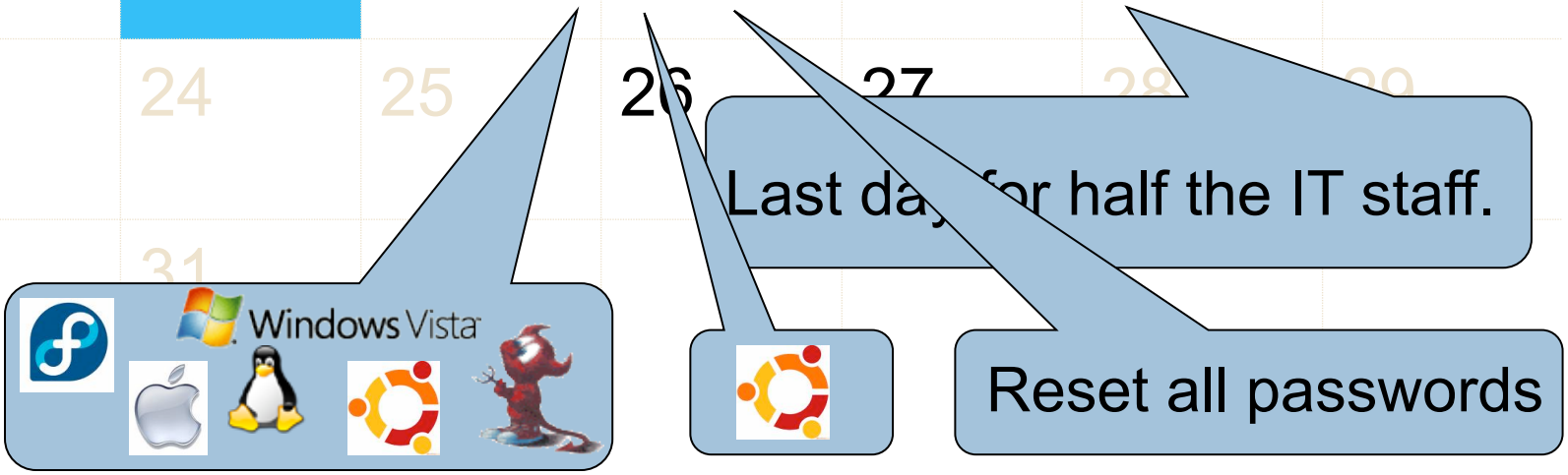
# December 2007

| | | | | | | |
|---|---|---|---|---|---|---|
| 2 | 3 | 4 | 5 | 6 detection | 7 | 8 |
| 9 | 10 detection | 11 | 12 | 13 diagnosis | 14 diagnosis | 15 |
| 16 | 17 diagnosis | 18 | 19 | 20 | 21 | 22 |
| 23 | 24 | 25 | 26 | 27 | 28 | 29 |
| 30 | 31 | | | | | |


Last day for half the IT staff.

# December 2007

| | | | | | | |
|---|---|---|---|---|---|---|
| 2 | 3 | 4 | 5 | 6 detection | 7 | 8 |
| 9 | 10 detection | 11 | 12 | 13 diagnosis | 14 diagnosis | 15 |
| 16 | 17 diagnosis | 18 | 19 | 20 | 21 | 22 |
| 23 | 24 | 25 | 26 | 27 | 28 | 29 |
| 30 | 31 | | | | | |



# December 2007

| | | | | | | |
|---|---|---|---|---|---|---|
| 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 16 | 17 | 18 | 19 | 20 | 21 | 22 |
| 23 | 24 | 25 | 26 | 27 | 28 | 29 |
| 30 | 31 | | | | | |

# Lessons Learned



- Intrusions discovered through manual examination of puzzling symptoms and side effects of attacks, not Snort or a commercial anti-virus tool

- Complete forensics difficult to achieve
  - Try balancing risk of analyzing a running server providing both essential services as well as service to the attacker
  - Operational demands can preclude the opportunity to learn from incidents

# Tension: Forensics

| | **Disable Host** | **Keep Host Up** |
|---|---|---|
| **Staff** | Reputation | Can observe host; provides service |
| **ISP** | Reputation | Field less service calls |
| **Users** | Risk to confidentiality, integrity, privacy, & availability | Keep service |

# Lessons Learned (cont.)



- We rely on human memory too much:
  - "…goals, suggestions, or objections [can be] misunderstood, warped, or forgotten, leaving potentially large gaps in the actual level of security achieved after repairs complete."
  - Having no single complete & coherent forensics analysis gives rise to multiple viewpoints
  - Planning for future attacks requires a pervasive, unobtrusive recording system

# Lessons Learned (cont.)



- Intrusions present opportunities for the good guys!
  - Creative ways of distributing new credentials out of band
  - Replace an outdated, slow, or weak authentication system

# Lessons Learned (cont.)



- Recovery decisions can be driven by informal preferences rather than objective, quantitative comparison of security properties
  - E.g., switching OS platforms
- Improvisation seems to rule the day
  - Challenge: design tools that meet the engineering challenges of repairing a network and the management and usability challenges of dealing with humans

# Research Directions



- Education!
  - Educated users are great IDS systems
  - Educating students on how to put a network back together again can be even more instructive than CTF exercises
  - Need an "Incident Archive" based on a standardized encoding of intrusion scenarios and testbed / "internet range" scenarios
- Pervasive recording infrastructure: "recovery trees"
- Objective technical comparisons of alternatives
  - NLP on release notes
  - Query bug databases & mailing lists

# Concluding Caveat



"We do not aim to lay blame with individuals…our goal is to present the facts, disposition of the network, and decisions…as a way to motivate tools that ease the burden on IT staff."

# Conclusion



"We believe the community should focus on creating mechanisms that deal with recovery as a system composed of both humans and computers."

- Contact: mlocasto@gmu.edu

- Many thanks to our shepherd, Nicole, for her help, patience, and assistance

# Links: Verizon Report & Fedora Saga



- http://securityblog.verizonbusiness.com/2008/06/10/2008-data-breach-investigations-report/

- http://www.linux-magazine.com/Online/News/Update-Fedora-Chronicle-of-a-Server-Break-in

# Tension: Forensics



- ISP: wants machine taken down
- Staff: keep machine operational to observe it
- Staff & Users: Machine must be operational b/c it provides a vital service
- Users: want machine taken down (e.g., it represents an invasion of privacy)
- Staff: want machine disabled (e.g., no mess in my backyard!)