Don’t touch that system

A quick primer on incident response

Rikard Bodforss, Omegapoint
Commercial break!

- If you understand Swedish…
  Listen to our podcast on security:
  www.sakerhetspodcasten.se

  Also available on iTunes

  …oh, and I work for Omegapoint.
Agenda

- The bare essentials
- What is evidence
- Handling evidence
- Myth busting
- What to do
- Demo
The bare essentials
Tools
Incident response checklist

• S.T.O.P!
• Stop, Think, Observe, Plan
• Start taking notes
• Collect evidence in order of volatility
• Analyze
• Report
Process

- Document everything!
- Take pictures
- Take notes
- Label all seized items
Everything you do...

Will have an impact on the system!
What is evidence?
Order of volatility

- RAM
- Open network connections
- Open encrypted volumes
- Hard drives
- Other storage media
- Hard copies etc
Best evidence
Evidence handling
Integrity is key

- Cryptographic checksums
- Chain of custody
- Secure storage
- Clean media
Myth busting
Forensic myths

- MD5 is broken and can’t be used
- You have to use a forensic write blocker
- Touching a live system is forensic suicide
- You must use clean media
What to do
42?

"The answer to every question within the field of forensics is: It depends..."
– Rob Lee
Make sure acquisition is done “by the book”

• If you do the acquisition right you can always go back for more analysis
• You never know if a case will end up in court
• You seldom know what jurisdiction that court will reside in...
Demo time
Thank you for listening!

Rikard Bodforss
Twitter: @rbodforss
http://www.sakerhetspodcasten.se/