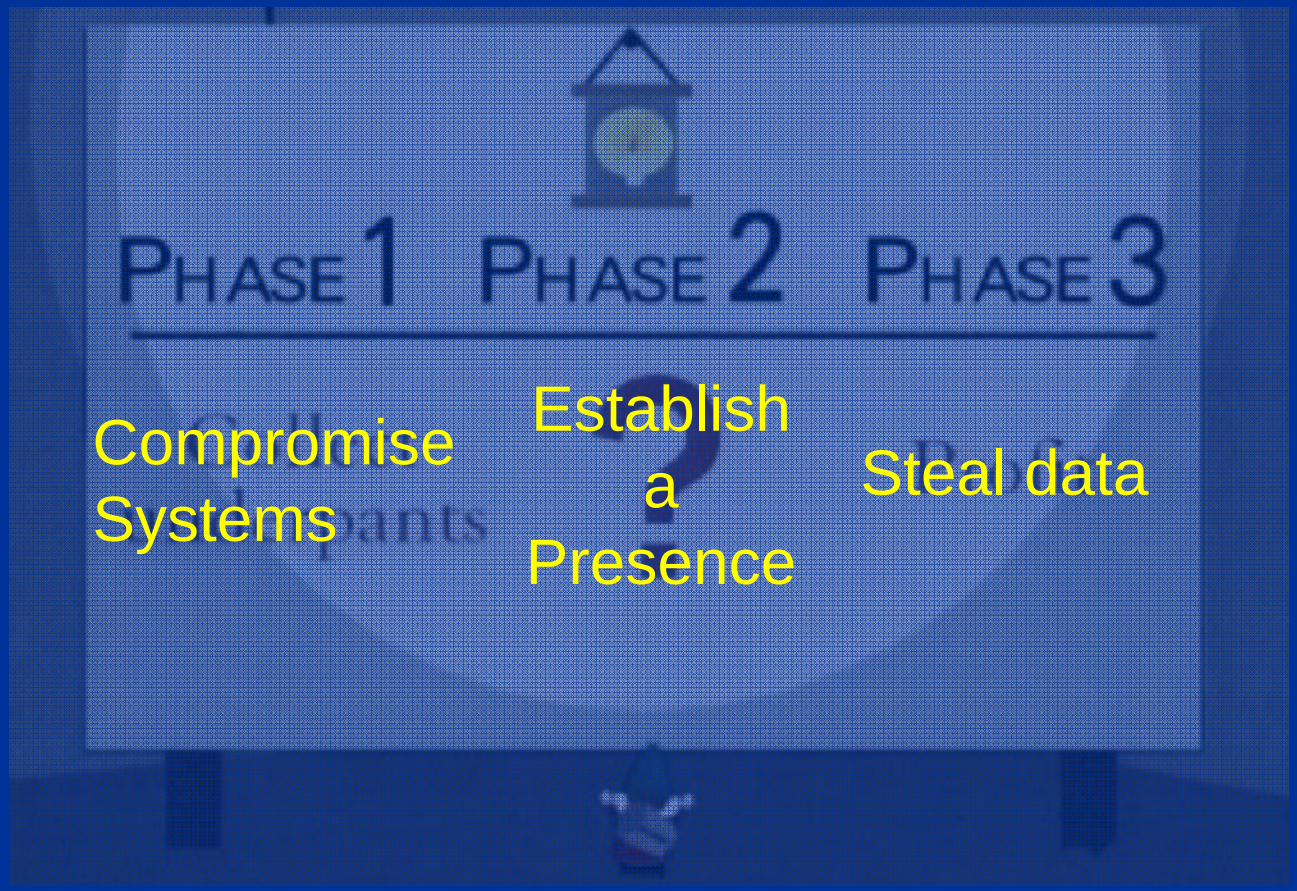
Successful Strategies in Enterprise Intrusion Investigations

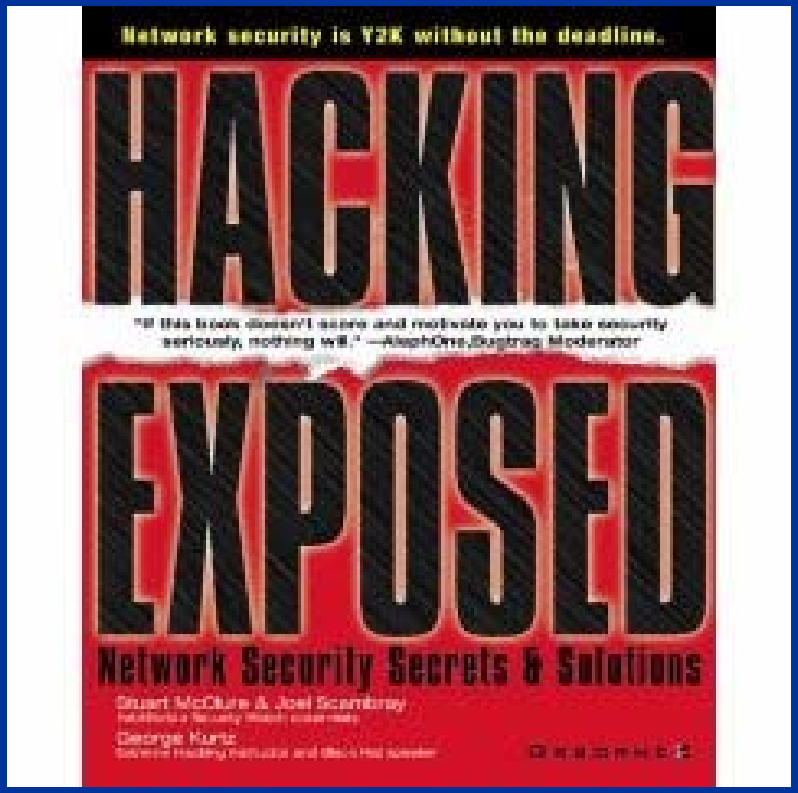
SANS WhatWorks in Forensics and Incident Response Summit 2008

Michael Cloppert
Member Technical Staff
Lockheed Martin Computer Incident Response Team

Phase 2: Establish a presence



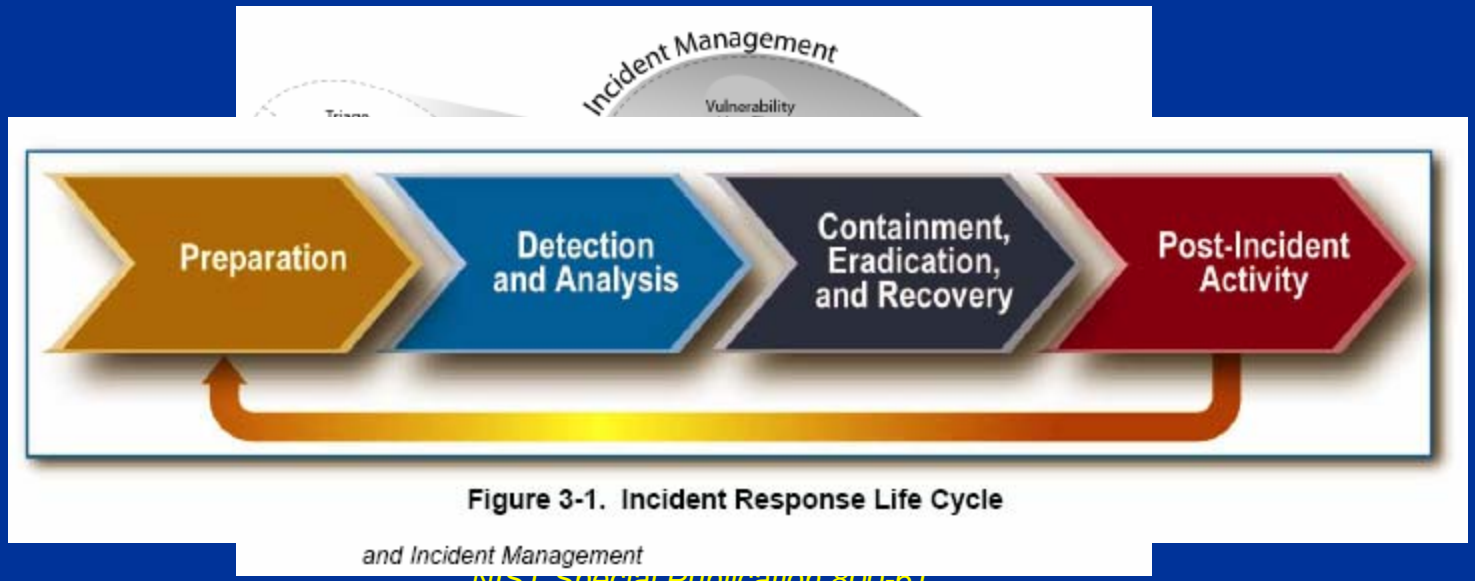
But how?


Network security is Y2K without the deadline.
HACKING
EXPOSED
Network Security Secrets & Solutions
Stuart McClure & Joel Scambray
George Kurtz

So what now?

We have a process!

Oh you mean this one?



NIST Special Publication 800-61: Computer Security Incident Handling Guide

CMU-SEI-2004-TR-015 Defining Incident Management Processes: A Work In Progress

Yeah, it's broken.

Get Intelligent

Integration of intelligence acquired through analysis and collaboration is key to successfully managing incidents