SANS INCIDENT RESPONSE TACTICS PANEL

Mike Poor & Tom Liston InGuardians, Inc

InGuardians, Inc. Introduction

- Information Security Consulting and Cutting Edge Research
- 14 Technical Consultants – All senior level
- Security architecture, Penetration Testing, Incident Response
- Tools
  - Samurai – Web testing framework
  - Yokoso – Infrastructure fingerprinting and exploitation
  - Spycar – Anti-spyware behavioral testing suite
  - LaBrea – Network Tarpit
  - Bastille UNIX harding scripts
  - B.A.S.E. – Snort front end

Panel Questions

- What are the top 3 analysis techniques
  - Threat vector analysis
  - System, network and application log analysis
  - Deception system monitoring/analysis
- What are the 3 most overrated techniques
  - String searches
  - Match the hash
  - Memory analysis

Panel Questions (2)

- How do you answer the following questions from clients after confirming unauthorized access has occurred:
  - How can we quickly determine what type of data was taken?
  - What are the best ways to determine how the hackers broke into our systems?
  - Our A/V does not seem to be effective; How can we identify malware on hosts on our network?