Internet Security Systems

SANS Forensic Summit Tactics Panel

Tactics Panel, Question 1

Have advances in memory analysis affected Forensics/IR tactics?

Without a doubt. A great deal extremely valuable information is available in memory that allows questions to be answered; questions that could not even be entertained in a post-mortem-only analysis methodology.

- **Process list, network connections**
- **Exited processes, expired connections**
- **Clipboard contents, window messages (possible)**
- **N. Petroni – answer new questions later**

Tactics Panel, Question 2

Given the fact that many hackers are versed in anti-forensics techniques:

- **What anti-forensics techniques are being seen? What is the most effective?**
- **What are some workarounds or techniques to aid in the investigation to still gather evidence with this in mind?**

Anti-forensics techniques haven't had to be employed in many incidents; response and examinations have illustrated a lack of visibility into systems/infrastructure such that AF techniques do not need to be employed, and some may actually give intruder away (i.e., poorly written rootkit causes BSoD, etc.)

Questions?

Harlan Carvey

hcarvey@us.ibm.com