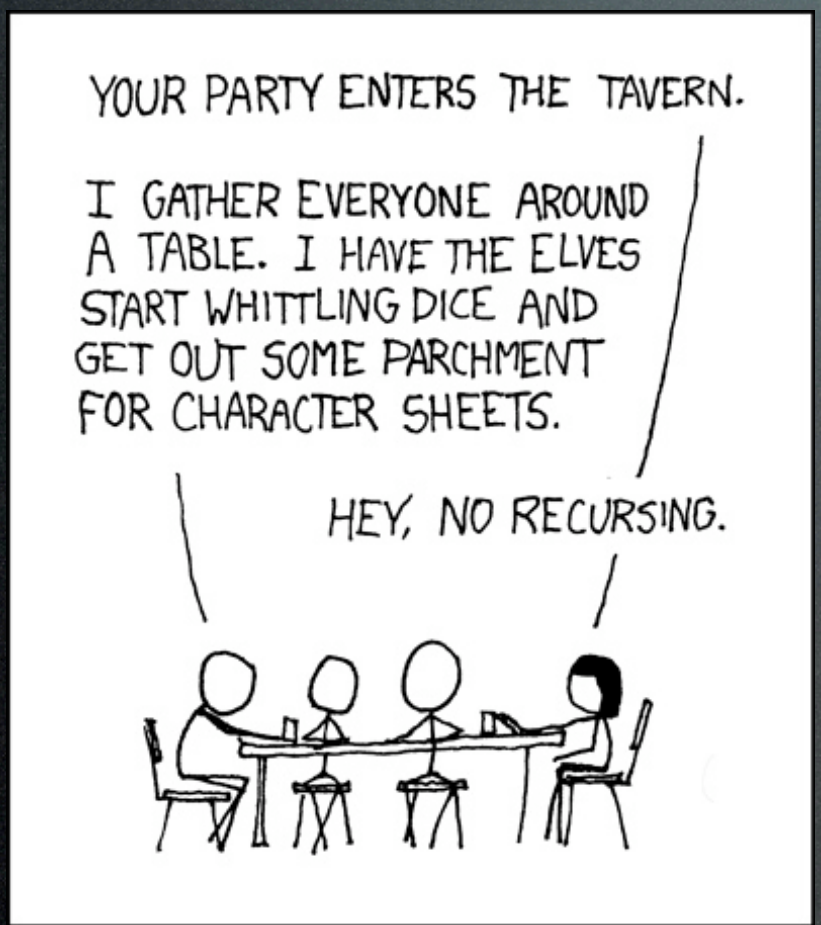
Testing Your Incident Response Process

Brent Huston
MicroSolved, Inc
Security Evangelist (& ceo)

Refresher of Incident Handling Process

- Understand background
- Define communication
- Assess scope
- Decide on evidence handling
- Investigate and Isolate
- Mitigate/repair
- Reporting
- Lessons learned loop

Incident Response Test Process



- Think “D & D”
- Incident director plays “Murphy”, entropy, “dungeon master”
- Independent observer
  - silent
  - performs gap analysis

Testing Scenario 1

- Stolen laptop and case
  - VPN token
  - What was lost? How do you know?
  - Was it encrypted? R U Sure?
- Notification mechanisms
- Asset tracking
- Credential management and social engineering
- Blackmail add-on

Testing Scenario 2

- The web site “isn’t right”!
  - SQL injection in content manager
  - Serving up malware and has been for 8 hours
  - Now what?
- Manage, mitigate, notify infected users?
- What data is exposed? What is the risk? Where do the devices sit?
- Do you have prevention, detection and response for web attacks?
- Customer support work load issues?

Testing Scenario 3

- Worms, Bots and Rootkits, Oh My!
  - Worm on internal network, 0-day Windows, spreading fast and leaving systems infected (possible rootkit) - new admin user & outbound connecting command shells
  - No patches or AV signatures available yet...
- Regain control, limit spread, terminate command shells, trace the infection to source, manage exposures
- “Patchless” mitigation strategies
- Malicious crypto/blackmail add-on
- How is rootkit different and how do you handle it?

Lessons Learned Loop

- Most important part
- Gap analysis
- Board-level or steering committee reporting

Continuing Improvement

- Add training/ resources as needed
- Implement changes
- Train
- Table top again!

Key Take Aways

- Understand your process
- Perform worst-cases
- Prepare for failure/ struggle
- Implement improvements
- Practice, practice, practice

Thanks, Q&A

- bhuston@microsolved.com / @lbhuston
- microsolved.com / stateofsecurity.com
- Table top testing has high value!!!
- Observers are key!!!
- Use random entropy when possible!
- Practice prevents panic!!!!