OVERVIEW

- What is a hacker?
- Prepare
- Find right resource
- Execute
- After
- Q & A
WHAT IS A HACKER?

• Black Hat – criminal
• White Hat – ethical hacker
  • Aim to improve security
  • “Someone paid by businesses to find bugs in systems by trying to hack into them”
PREPARE

• Work with your team to cover some basics
• “Test prep”
• CIS benchmarks
• Vulnerability Scanning
• Static and Dynamic code analysis
• Secure coding practices
• Basic cyber hygiene (shared passwords, password complexity, phishing)
PREPARE (CONTINUED)

- SIEM (Security information & event management)
- Log collection and analysis
- Forensic investigation
- Lean on DHS CSAs, State CISO, state and local cyber resources
FIND THE RIGHT RESOURCE

• Reputable partner with a track record
• Peer references
• Look at PCI assessors
• NDAs
• Contract Ts and Cs – “high risk”
EXECUTE

• Learn Tactics, Techniques, & Procedures (TTPs)
  • (if you have people)
• Exercise your Incident Response (IR) processes
• Detection Success (and failure)
• PICERL (Preparation, Identification, Containment, Eradication, Recovery, Lessons-learned)
POST-MORTEM (JK!)

- A couple notes from Colorado’s experience
- Tech Recap
- Plain Language Recap
- Develop an improvement plan
- Do It Again!
Black Hats are hitting you; why not try the White Hats?

Doesn’t matter whether you control your assets, you are responsible

Tension and Skepticism

need to engage productively
Q & A