### Game Pieces
- H-Ray Specter
- Mr. Rogue XP
- The Clipboard of Authority
- Light Sword of Holding
- Black Magic Wand of SEC
- SANS NetWars Energy Drink
- My First Burner Phone
- The Hero's Slingshot
- Cyber Net Dealer of Cyber

### Game Modifiers
- Build a Home
- Additional game pieces, and game modifiers at www.sans.org/boardgame
- Scoping & Rules of Engagement
- Reconnaissance

### Scoping & Rules of Engagement
- Scoping call went great!
- Target organization provides lists of systems to attack
- Target organization gives your "victory conditions"
- Client wants to modify scope
- Go back to start

### Reconnaissance
- Shodan.io helps you find potential vulnerabilities
- You interacted with a honey pot
- Target organization DNS server allows external zone transfers
- Search engines reveal data exposure

### Password Attacks
- Cracked service account password
- Target organization's admin accounts use multi-factor authentication
- Go back 2 spaces

### Exploitation
- Find Github repo with working exploit
- Exploit causes app to crash, client mad
- Skip next turn
- You use a honey account and get caught
- Crack passwords with Hashcat
- Skip next turn

### Post-Exploitation
- Host Blue Team catches you
- DLP is only looking at email, so you can exfiltr data with ease
- You find SQL injection on internal web app
- Get additional credentials from configuration files
- Look through local system and network shares for interesting files

### Reporting
- Use your packet capture to help show network trust relationships
- You realize you didn't take enough screenshots: PANIC!
- Roll dice, skip that many turns
- Your proofreader has the week off, skip next turn while you find a replacement
- You add the target organization's alerts to show they have detection capabilities
- Target organization likes draft report! It gives feedback in a timely manner
- Target organization wants you to present the findings to the board of directors
- Skip next turn to prepare

### Scanning
- Discover unpatched remote exploit
- Verify findings from search engine recon
- Target organization MSSP detects your scans
- Go back 2 spaces

---

**PIVOTS & PAYLOADS**

**SIMULATE A FULL-SCALE HIGH-VALUE PENETRATION TEST**