Put Your Game Face On: Using InfoSec Challenges to Build Your Skills and Career

By Ed Skoudis

December 9, 2011

Goals of This Talk

- To discuss fun ways to further develop information security skills
- To give you a peek behind the scenes of developing Capture the Flag Games and other infosec challenges
- To share tips on what makes for a good, engaging security challenge
- To point you at some of the best challenges available for developing your skills
My Gaming Background & Some Quick Thank Yous

- I’ve been participating and writing CtF games since 1996
  - Beyond HOPE & several DefCon CtFs by GhettoHackers and Kenshoto
  - I’ve written the 504 and 560 CtFs
  - I’ve coached several CtF teams, including West Point’s CDX groups
  - I’m an advisor & sounding board to several other CtF authors
  - I’m director of SANS NetWars, Cyber Quests, and Cyber Foundations

- Thanks to:
  - My kids, little guinea pigs that they are
  - My mom and my wife, who put up with my games
  - @las & l@stplace for proving my point
  - SANS for the opportunity
  - You for listening and playing!

Put Your Game Face On

- **Overview**
  - Gamification and Game Stigma
  - Characteristics of Challenges
  - Designing Challenges
  - Example Challenges to Savor
  - Conclusions
Motivation

• How do you learn? Really?
• The SANS Promise:
  – “You will be able to apply our information security training the day you get back to the office!”
• Hands-on exercises not only reinforce the concepts of lectures, they also give you skills you can apply directly in your day-to-day job
• How can you expand an exercise to a full day or multiple days? GAMIFY!
• Is there ever a point where you have too much hands-on exercise? As long as you are careful and clever, I think the answer just might be “NO.”

Gamification

• According to the Extra Credits show*, Gamification is “taking the principles of play... such as those used in video games... and using them to make real-world activities more engaging.”
• According to Wikipedia, Gamification, can be used in, “encouraging users to engage in desired behaviors, by showing a path to mastery and autonomy, and by taking advantage of humans' psychological predisposition to engage in gaming.”
• Increasingly, the future of learning (and advertising)
  – Many school teachers are starting to embrace this approach
  – Lego Master Academy – Advance through levels
  – McDonald’s Monopoly Game – Buy high-margin products for points!
• Scoring, progress rewards, and fun are three vital aspects

* Check out the Penny Arcade TV website at penny-arcade.com/patv/episode/gamification
How Can We Use InfoSec Challenges?

- To measure player ability
  - Technical knowledge
  - Analytic skills
  - Creativity
  - Organizational skills
- To identify latent talent in an organization
  - “Who knew that HE was so elite?”
- To train
  - A whole lot of opportunities here
  - Realistic scenarios are key
- To provide motivation
  - “You kicked my... can... this time; next time, I’m gonna kick yours!”

Scorecard

Characteristics of a Game

- Score
  - Consider the difference between educational grading versus scoring
  - Grading starts at 100% and you lose from there
  - Scoring starts at zero and you move up from there!
  - Ultimately the same, but the psychology is reversed and more conducive to learning and fun
- Rewards
  - Show skills mastered and progress regularly
- Solve puzzles
- Fun, smiles, and laughs
  - Have to be careful with the frustration factor
Game Stigma

• Some people are resistant to this concept
  – “I just don’t play games”
  – Some think that it is “childish” or “beneath” them
  – Maybe they are intimidated and don’t want to say so
  – Others
• We can still engage them with a little terminology tweakage
  – “Game” becomes “Challenge” or “Simulation”
  – “Player” becomes “Participant” or “Student”
• Also, people (especially some bosses) don’t want to pay as much for a challenge as they will for a course

Tip: Tell your boss that you need to participate (not play) in a simulation (not game) to build your skills in handling real-world situations.

Knowing That It Can Be Done…
Warps the Scenario

• In CtF games, the player has a reasonable expectation that each challenge can be done
  – That knowledge inspires them to do it
  – Or it frustrates them
  – Either way, it builds a sense of efficacy and a case for action
• In the so-called real world, info sec pros can fall victim to the idea that “It can’t be done.”
  – “I don’t want to beat my head against a wall and waste my time”
  – Vinnie Liu: “Master Pen Testers ARE RELENTLESS… they don’t give up.”

Tip: When confronting a problem, assume it can be solved. Don’t give yourself the out of saying “This is impossible”. Also, use hints from trustworthy sources.
Tips for Building Your Own CtF

- Select your audience
  - Your kids?
  - Your co-workers?
    - Brown-bag lunch opportunity
  - Your local SANS Mentor group, ISSA chapter, ISACA chapter, etc.
  - Local mentor group
  - Your friends – InGuardians’ PacketWars concept

Tip: Build your own challenge or CtF, as it will help you build your skills and can be a lot of fun.

Audience Skill Set Versus Difficulty of Development

- Some people assume that writing a challenge for advanced participants is harder than writing one for intermediate players
  - In my experience, this is not the case
  - Generally speaking:
    - It is easy to write a challenge for beginners
    - It is easy to write a challenge for technically skilled experts
    - What is hard is writing a challenge for a broad range of people with intermediate skill sets… but it can also have the widest appeal and be the most rewarding!
Methods for Achieving Broader Appeal Across Skill Levels

• Make some challenges relatively easy
  – “Put some cookies on the lower shelf”
  – But, make these relatively easier challenges a foreshadow of much more complex challenges to come later or deeper
  – Have easier challenges build to the more advanced ones
    • That way, the easier ones are building blocks and aren’t throwaway for the advanced players… everyone benefits from them
• Allow advanced players to breeze through easier challenges and rise to the level of their expertise
  – Unlock more advanced levels quickly
  – Interestingly, these players will still hunt for the easy pickins in the lower levels, but they will feel happier knowing that they can jump ahead when they want

Solo versus Team Play

• Solo challenges allow for measuring individual players
  – Provide ample learning opportunities across multiple avenues
  – Can be very satisfying... or very frustrating
• Team challenges add a great extra dimension
  – You can measure leadership, followership, and team dynamics
  – Stronger players can also help weaker players learn
  – Warning! They can also deny weaker players a chance to learn as well
  – Coaching can help a team optimize its human resources
Types of Challenge

- **Offense**
  - Players attack targets, modeling vuln assessment and pen testing
- **Defense**
  - Players stop attackers from compromising targets
- **Offense & Defense**
  - Very exciting, but a lot of work to implement
  - Heavily dependent on players’ skill and capabilities
- **Analysis**
  - Packets, files, malware, and other
- **Others...** Lots of opportunities for innovation here
  - Bot-net control

Flat Games versus Depth

- Challenges can be written to be flat or have depth
- **Flat:** A player can reach all challenges and assets from any point in the game
  - Easier to construct
  - More fault tolerant
  - Can be less frustrating to players (but you should signal which are the easier and which are the harder challenges)
- **Depth:** A participant needs to solve earlier challenges to get access to later ones
  - Unlocking
  - Lends itself to pivoting
  - Leads to richer games and more real-world scenarios
  - Also useful for keeping excitement up and engaging the participant
Visualizing Challenge Architecture

- There are many ways to view an overall CtF challenge architecture, useful for:
  - Designing
  - Verifying
  - Playing
  - Reviewing results with participants
- Two methods I’ve used a lot: Tabular View and Kaleidoscopic View

<table>
<thead>
<tr>
<th>Host 1</th>
<th>Host 2</th>
<th>Host 3</th>
<th>Host 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acct 1</td>
<td>Acct 2</td>
<td>Acct 3</td>
<td>Acct 4</td>
</tr>
<tr>
<td>Vuln 1</td>
<td>Vuln 4</td>
<td>Vuln 7</td>
<td>Vuln 10</td>
</tr>
<tr>
<td>Vuln 2</td>
<td>Vuln 5</td>
<td>Vuln 8</td>
<td>Vuln 11</td>
</tr>
</tbody>
</table>

Close to center implies progress toward ultimate victory.

Be Careful About Concurrency

- In creating CtF challenges in particular, one of the toughest issues I’ve seen is building resilience in light of concurrency
- You do plan on having multiple players, right?
- Watch out for deadlocks and resource hogging
  - Even inadvertent action here can cause big problems
  - Port usage, file locks, file move (instead of copy), service hanging under exploitation, etc.
- Watch out for “King of the Hill” challenges, which encourage players to beat up on each other
  - Leads to a lot of frustration, and little learning
Automate Healing of Invariants

- For active challenge environments (especially CTF), I strongly recommend that you identify a set of resources in your challenges that must not change for your challenges to work
  - I call these invariants
- Write small scripts to check and automatically fix the invariants every 5 seconds
  - The Linux watch command is very helpful here
  - The Windows "FOR /L %i in (1,0,2) do" loop is useful as well
- Be careful that your healing scripts do not reveal too much information about the challenge
  - Construct scripts so that players who grab a copy of a script don't gain any more info than they'd already have with the privileges needed to read the script
  - Yes, this can be tricky

Scenarios Rock!

- Provide a narrative to engage players
  - People like stories, especially those that unfold over time and due to their efforts
- Create characters
  - User accounts with artifacts
  - Provide each character with a personality
    - "What would Susan do here?"... allows participants to think through and utilize character behaviors and motivations
    - Can also be good for a laugh or smile
- Create a backstory
  - What happened before to make things this way?
- Helps make your challenge seem more real-world
Challenge Pacing

- For a rewarding experience, there should be times of building intensity and release
  - With an overall increasing trajectory
  - A nice denouement at the end also helps
- Consider Star Wars, Episode IV: A New Hope
  - Build this structure into your challenges

Scenarios and Asset Construction

- With your scenario, you are creating a small world
  - Give your world a sense of rules, forethought, prehistory, and depth, and try to be consistent within them
  - Timestamps, logs, geo-location, character habits, etc.
- Never underestimate the time it takes to develop really good game assets!
Red Herrings, Diversions, Head Fakes, and Rabbit Holes

• Real life is full of red herrings, diversions, and head fakes
  – Misdirection, lies, dirty tricks
  – Contradictory messages
• Should your challenges be as well?
  – They can test participants’ ability to focus on what is really important
  – But, they can also frustrate players big time
  – There are always unintended diversions, no matter how much you try to avoid them
    • Clever players will see patterns where they weren’t intended

Avoid Puzzles for Puzzles’ Sake and Needles in the Haystack

• Sometimes, it can be tempting to put in a puzzle just for fun
  – Example: ROT-14, silly poems, needless information shuffling
  – These may seem fun, but could get you branded as a waste of time
• Such puzzles can:
  – Seem rather random
  – Lead to frustration
  – Don’t lead to developing real-world skills
• Similarly, “needle-in-a-haystack” problems are often less useful as they involve random luck
  – However, if your goal is to stress some form of automation in iteration, they could be useful... but watch out for performance impacts
Scoring

- Participants should have a real-time method for determining their progress
- This may be an automated scoreboard, map, score card, poll, etc.
- Positive points, of course
- Negative points? Can be controversial or frustrating
  - Make sure player can’t mess up one thing so bad that they are prohibited entirely from progressing in the challenge
  - Consider capping negative points
  - People also like “Jeopardy-style” score boards or color, animated game maps

Dealing with Hints

- Some players want hints, while others do not want them
- Many approaches to dealing with hints:
  - “Suck it up and do it on your own, babe!”
  - Ask the Game Master for a manual hint
  - Automated hint system
    - Should it penalize players’ scores or progress?
- How can you be fair?
  - Give hints to everyone at the same time, or...
  - Automate, and allow players to ask for hints
Frustration

• Offer ways for your players to burn off a little frustration
  – Build your challenges so that they have “More than one way to do it”
    • Even if you don’t try to do this, it is still very likely the case
    • But, increase that likelihood by building multiple paths through your challenges
    • This approach also increases reliability and concurrency
  – Contact with game master (e-mail, chat, etc.)
  – Hints
  – Build a community of players

Now Featuring...
The Real World

• Real-world devices are often controlled by computer equipment
  – “How can you structure a challenge to show that cyber action can have kinetic effects?”
  – Let’s include computer-controlled kinetic game assets!
  – Computer oriented-overlays of the real world: Webcams, videos, telephony, geo-location, wireless, etc.
  – Actual kinetic devices: SCADA systems, HVAC infrastructure, etc.
  – Models of larger equipment: trains, rocket-launchers, etc. – THE WAR ROOM!
  – Be careful of latency (remote control cars and helicopters) and resetting physical infrastructure
Free Challenge Environments You Can Download

- There are numerous downloadable test environments for building skills
  - You could easily turn any of these into a challenge or game
- Damn Vulnerable Web App
  - http://www.dvwa.co.uk
- Iron Geek’s Mutillidae
- OWASP WebGoat
- Metasploitable
  - https://community.rapid7.com/community/metasploit/blog/2010/05/19/introducing-metasploitable
- Damn Vulnerable Linux: Currently being rebuilt, but you can find older versions
  - http://www.damnvulnerablelinux.org/
- Don’t forget the VMware appliance marketplace!
  - http://www.vmware.com/appliances/

Free Challenges You Can Play

- SkullSpace Winnipeg Secret Challenge
  - www.skullspace.net/2011/01-level/secchotchallenge.php
- High Schoolers: USCC Cyber Foundations
  - http://workforce.cisecurity.org
  - Next run in Spring 2012
- College Students: Cyber Quests
  - U.S. Cyber Challenge (USCC)
    - Check out http://uscc.cyberquests.org
    - Run approximately 4 times per year
Additional Challenges for You to Check Out

- **Smash the Stack Wargaming Network**
  - Several games (IO, TUX, LOGIC, Blackbox, etc.) of various levels of difficulty
  - www.smashthestack.org

- **OverTheWire challenges**
  - www.overthewire.org
  - In Sept 2011, they released their Abraxas game as freely downloadable virtual appliances, so you can host it and play locally
  - They also have several other games there to play

- **And, also, don't forget:**
  - Cyber Patriot high school competition: http://www.highschoolcdc.com
  - Several different games: http://p6dread-teel.net/~windo/wargame
  - Even more games: http://hack.thebackupbox.net
  - Vulnerable code & exploit dev! http://community.corest.com/~gera/InsecureProgramming

Great Write-Ups on Earlier Challenges

- **Fantastic SANS Forensics Challenges, including answers, are available at:**
  - http://computer-forensics.sans.org/community/challenges

- **Previous DefCon CTF Quals:**
  - 2008 (B300 write-up in cartoon form!): http://hackerschool.org/DefconCTF/17/B300.html

Awesome cartoon of the Sap Heads team from http://hackerschool.org/DefconCTF/17/B300.html
Free Counterhack.net Movie & Christmas Challenges

- At my personal website, I have 34 different challenges, most including very detailed answers
  - Written by me and my friends (Kevin Johnson, Yori Kvitchko, Tom Liston, Mike Poor, Tom Hessman, etc.)

The Nightmare Before Charlie Brown’s Christmas
Miracle on Thirty-Hack Street
Santa Claus is Hacking To Town
It Happened One Friday
Brady-Bunch Boondoggle

A New Challenge!

- Grandma Got All Hax0red By a Reindeer... Or Did She?
- Match wits with Rudolph and Grandma to determine the truth!
- In-depth packet and evidence analysis
  - Multiple levels of fun!
- Help make sure justice is served
- Available at pen-testing.sans.org/holiday-challenge
- Download now, analyze over holidays, and submit answers before Jan 9, 2012!
Conclusions

• Gamification is happening, and you can use it to help improve your skills
  – Not in just participating, but also in creating challenges
• Try out the challenges we’ve described here
• And, write your own! Share with the community
• Have fun and learn!
  – Really, folks... this is the future