Would you like to play a (security) game?

SANS Blue Team
Summit
23-24APR18
Dave Herrald
Ryan Kovar @Splunk
Disclaimer

During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. I often lie. Maybe this is a lie. Wik Alsø wik Alsø alsø wik Wi nøt trei a hølday in Sweden this yér? See the løveli lakes The wøndërful telephøne system And mäni interesting furry animals The characters and incidents portrayed and the names used in this Presentation are fictitious and any similarity to the names, characters, or history of any person is entirely accidental and unintentional. Signed RICHARD M. NIXON

Including the majestik møøse A Møøse once bit my Marcus... No realli! He was Karving his initials on the møøse with the sharpened end of an interspace tøøthbrush given him by Svenge – his brother-in-law – a Canadian dentist and star of many Norwegian møovies: "The Høt Hands of an Canadian Dentist", "Fillings of Passion", "The Huge Møalars of Horst Nordfink"... In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. Splunk undertakës no øbligation either to develøp the features or functionality described or to include any such feature or functionality in a future release.
# whoami > Dave Herrald

CISSP, GIAC G*, GSE #79

- 20+ years IT and security
- Information security officer, security architect, pen tester, consultant, SE, system/network engineer
- Former SANS Mentor
- Co-creator of Splunk Boss of the SOC

Staff Security Strategist
@daveherrald
# whoami > Ryan Kovar

CISSP, MSc(Dist)

- 17 years of cyber security experience
- Current role on Security Practice team
- Co-creator of Splunk Boss of the SOC
- Also investigating why printers are so insubordinate ❗️❗️
Agenda

• Answering some W’s
  • What exactly ARE (Blue Team) CTFs
  • Why are we doing this talk?
  • What are some examples

• Talk about the “H”
  • Hints on making a Blue Team CTF
  • How can I run one myself?

• And now another W
  • Where can I get this awesome stuff!
If you haven’t played a CTF

... Sit Down
If you haven’t played a BOTS

... Sit Down
What is a capture-the-flag (CTF)?
Learning cyber **security** through gamification
K Boopathi, S Sreejith, A Bithin - *Indian Journal of Science and Research*, 2015 - indjst.org
Objectives: Introducing gaming approach in the jeopardy round of InCTF (Indian Capture the Flag). Methods: Present Jeopardy round of InCTF can be compared as take-away assignments, where participants are given set of questions to solve, this is aimed at testing …

Gamification for measuring cyber **security** situational awareness
G Fink, D Best, D Manz, V Popovsky... - *International Conference on Information Security*, 2013 - Springer
Abstract: Cyber defense competitions arising from US service academy exercises, offer a platform for collecting data that can inform research that ranges from characterizing the ideal cyber warrior to describing behaviors during certain challenging cyber defense situations ...

The gamification of education
AM Cohen - *The Futurist*, 2011 - search.proquest.com
The Gamification of Education... McGonigal, the director of game research and development at the Institute for the Future, has designed award-winning games to help ignite real-world solutions to pressing social and environmental challenges, such as global food **security** and a ...

A generic platform for enterprise gamification
P Herzig, M Ameling, A Schili - *Software Architecture (WICSA)*... 2012 - ieeexplore.ieee.org
... be gamified across multiple businesses. For example, a developer can define which events are communicated between enterprise boundaries, which events are relevant for the gamification design, or how **security** is handled ...
CTF? WTF?

Capture the Flag (CTF) is a special kind of information security competitions. There are three common types of CTFs: Jeopardy, Attack-Defence and mixed.

**Jeopardy-style CTFs** has a couple of questions (tasks) in range of categories. For example, Web, Forensic, Crypto, Binary or something else. Team can gain some points for every solved task. More points for more complicated tasks usually. The next task in chain can be opened only after some team solve previous task. Then the game time is over sum of points shows you a CTF winer. Famous example of such CTF is Defcon CTF quals.

Well, **attack-defence** is another interesting kind of competitions. Here every team has own network(or only one host) with vulnerable services. Your team has time for patching your services and developing exploits usually. So, then organizers connects participants of competition and the wargame starts! You should protect own services for defence points and hack opponents for attack points. Historically this is a first type of CTFs, everybody knows about DEF CON CTF - something like a World Cup of all other competitions.

Mixed competitions may vary possible formats. It may be something like wargame with special time for task-based elements (e.g. UCSB iCTF).

CTF games often touch on many other aspects of information security: **cryptography, stego, binary analysis, reverse engeneering, mobile security** and others. Good teams generally have strong skills and experience in all these issues.
What is Jeopardy style CTF?
ATTACK / DEFENSE CTF
NetWars: Cyber Defense NetWars

What is Cyber Defense NetWars?

The all-new Cyber Defense NetWars challenge is a defense-focused competition aimed at testing your ability to solve problems and secure your systems from compromise. Cyber Defense NetWars is a truly unique experience, and an opportunity to test your skills in Administration, Threat Hunting, Log Analysis, Packet Analysis, Cryptography, and much more.

Topics Include:
- Windows Administration
- Linux Administration
- Packet Analysis
- Network Security Monitoring
- Continuous Security Monitoring
- Logfile Analysis
- Cryptography
- Steganography

The SANS Cyber Defense NetWars Experience:
- Consists of an interactive, Internet-based environment that tests a player's ability to secure systems and detect compromises
- Is designed to be accessible to a broad level of player skill ranges
- Is split into separate levels so players may quickly advance through earlier levels to the level of their expertise.

The entire challenge involves four levels:
- Level 1: Defending and Securing the wall
- Level 2: Defend against wilding attacks
- Level 3: Defending against undead attacks
- Level 4: Defending against the dreaded Night King

Who Should Attend:
- Security Administrators
The 2015 SANS Holiday Hack Challenge
Don't miss the chance to be educated and trained in critical skill areas like incident response, forensic investigation and analysis, file systems, memory layout, and malware analysis. University of Missouri students, alumni, faculty and staff are welcome to participate!

TracerFIRE Schedule:
Missouri/Ozark Room - Havener Center
Friday, August 28th: 5:30pm - 9:30pm
Catered Pizza Dinner Provided
Saturday, August 29th: 10:00am - 6:00pm
Catered Donuts, Lunch, and Afternoon Snacks Provided
Sunday, August 30th: 10:00am - 6:00pm
Catered Donuts, Lunch, and Afternoon Snacks Provided

Visit acmsigsec.mst.edu to sign up!
WHY

a Mystery Game

presented by ALFRED HITCHCOCK
“And now for something completely different.”

Monty Python
We wanted to tell a story.
We wanted “chains” of events
So we made a different mousetrap
Goals of our CTF

- Training
- Realistic Competition
- FUN!
KEEP IT REAL
TAEDONGGANG ART

BOSS OF THE SOC 2017
A special thanks to:

**ADVERSARY**
- Nation state sponsored adversary
- Located (+8.5 time zone)
- Uses Korean encoded language
- Uses Hancom Thinkfree Office

**CAPABILITIES**
- PowerShell Empire
- Spear phishing

**TECHNICAL AXIS**
- Documents with .hwp suffix
- PS exec lateral movement
- YMLP
- Self signed SSL/TLS certificates
- +8.5 hour time zone
- Korean fonts for English
- Korean text google translated to English
- Naenara user agent string

**INFRASTRUCTURE**
- European VPS servers

**VICTIMS**
- Western innovative Brewers and Home Brewing companies

- +8.5 hour time zone
- Korean fonts for English
- Korean text google translated to English
- Naenara user agent string

A special thanks to THREATCONNECT.
• Advance Persistent Threat
• Web Attacks
• Ransomware
• Insider Threat
• Fraud
A Maltego Graph of the APT group infrastructure
Lessons learned in making our CTF
Create Realistic Scenarios
Write Clear Questions
Now Get A Copy Editor
Avoid Time Zone questions
How to make a CTF

Add clues
Ages: Tier 1+
How to put it all together
Platforms

Projects that can be used to host a CTF

- **CTFd** - Platform to host jeopardy style CTFs from ISISLab, NYU Tandon
- **FBCTF** - Platform to host Capture the Flag competitions from Facebook
- **HackTheArch** - CTF scoring platform
- **Mellivora** - A CTF engine written in PHP
- **NightShade** - A simple security CTF framework
- **OpenCTF** - CTF in a box. Minimal setup required
- **PicoCTF Platform 2** - A genericized version of picoCTF 2014 that can be easily adapted to host CTF or programming competitions.
- **PyChallFactory** - Small framework to create/manage/package jeopardy CTF challenges
- **RootTheBox** - A Game of Hackers (CTF Scoreboard & Game Manager)
- **Scorebot** - Platform for CTFs by Legitbs (Defcon)
- **SecGen** - Security Scenario Generator. Creates randomly vulnerable virtual machines
Take the sh out of IT.
Platforms

Projects that can be used to host a CTF

- CTFd - Platform to host jeopardy style CTFs from ISISLab, NYU Tandon
- FBCTF - Platform to host Capture the Flag competitions from Facebook
- HackTheArch - CTF scoring platform
- Mellivora - CTF scoring platform
- NightShade - A simple security CTF framework
- OpenCTF - CTF in a box. Minimal setup required
- PicoCTF Platform 2 - A genericized version of picoCTF 2014 that can be easily adapted to host CTF or programming competitions.
- PyChallFactory - Small framework to create/manage/package jeopardy CTF challenges
- RootTheBox - A Game of Hackers (CTF Scoreboard & Game Manager)
- Scorebot - Platform for CTFs by Legitbs (Defcon)
- SecGen - Security Scenario Generator. Creates randomly vulnerable virtual machines

CTF Scoring Engine on Splunk!
Initial Splunk CTF Scoring Engine Requirements

✅ Keep score
✅ Do that^ securely (yes, we have stories)
✅ Manage users/teams
✅ Manage questions/answers/hints
✅ Provide instructions and help
✅ Control and visibility for admins
✅ Do it on Splunk
4378 players
Up to 350+ users simultaneously tested
2.32 “person” years of BOTS
Community Chest

GET FREE STUFF FROM THE GUYS AT SPLUNK - CARD

THIS CARD MAY BE KEPT UNTIL NEEDED, OR SOLD

©1936, 1996 Hasbro
What can we contribute back to the community?

- Dataset
- Scoring app
- Questions, answers & hints
### Real Data Sources

- **Sysmon**
- **Windows Events**
- **Windows Registry**
- **IIS**
- **Splunk Stream (wire data)**
- **Suricata**
- **Fortigate (NGFW)**
Real Data Sources

Download today

Scoring App
Scoring App

Download today

- https://github.com/splunk/SA-ctf_scoreboard
- https://github.com/splunk/SA-ctf_scoreboard_admin
### Questions

**BOTS slayer**

Click `>` below to see your team's entire submission history for this question.

<table>
<thead>
<tr>
<th>f</th>
<th>Number</th>
<th>Question</th>
<th>Status</th>
<th>Base Points Avail</th>
<th>Base Points Earned</th>
<th>Speed Bonus</th>
<th>Additional Bonus</th>
<th>Penalty</th>
<th>Hints Available</th>
<th>Hints Received</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>This is a simple question to get you familiar with submitting answers. What is the name of the company that makes the software that you are using for this competition? Just a six-letter word with no punctuation.</td>
<td>Correct</td>
<td>50</td>
<td>50</td>
<td>10</td>
<td>5</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>100</td>
<td>What's my favorite color?</td>
<td>Incorrect</td>
<td>500</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>10</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>101</td>
<td>What's the answer to the ultimate question of life, the universe and everything?</td>
<td>Unanswered</td>
<td>1000</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Questions, etc.

BOTS slayer

Request today

Drop us a line at bots <at> splunk.com
Conclusion

- Gamifying blue-team activities is an awesome way to increase skills
- Anyone can make a CTF!
- Don’t reinvent the wheel. Many different resources to help you.
Special Thanks

- Splunk!!!!
- SANS Netwars
- DOE Tracer FIRE
- DEFCON CTF
- Ed Skoudis and crew
Contact info

Dave Herrald
@daveherrald

Ryan Kovar
@meansec

CTF Server - [https://github.com/splunk/SA-ctf_scoreboard](https://github.com/splunk/SA-ctf_scoreboard)
CTF Server - [https://github.com/splunk/SA-ctf_scoreboard_admin](https://github.com/splunk/SA-ctf_scoreboard_admin)
Questions - bots [@] splunk.com