Hi.

Hi.

I'm Aaron.

Hi.

I'm Aaron.
I like CTFs.

Hi.

I'm Aaron.
I like CTFs. I like building CTFs.

Hi.

I'm Aaron.
I like CTFs. I like building CTFs.
It has not always gone well.

Hi.

I'm Aaron.
I like CTFs. I like building CTFs.
It has not always gone well.
Let me tell you how.

UnalloCTF

- or -

How not to write your own CTF scoreboard

~~UnalloCTF~~, OpenSOC

- or -

How not to write your own CTF scoreboard

~~UnalloCTF~~, ~~OpenSOC~~
Zeek Week

- or -

How not to write your own CTF scoreboard

~~UnalloCTF~~, ~~OpenSOC~~ ~~Zeek Week~~, Corelight CTF

- or -

How not to write your own CTF scoreboard

UnalloCTF

Forgotten (@forgottenSec)

- Snort guru
- Played dozens of CTFs
- Unallocated President
- Barcode Shmarcode

Surefire (@_surefire_)

- Full-time network instructor
- Played in a few CTFs
- Unallocated member
- How hard could it be?

Unall{∅}cated

Overview

This was our first attempt at building a CTF.

- Team-based “Network Exploration Challenge”
- Not team-versus-team
- Welcoming visitors into UAS and the world of CTFs.
- Monday, May 27, 2013 (Memorial Day)
- 57 participants (7 local teams, 6 remote teams)
- Six hours (1400-2000 Eastern)

Overview: Infrastructure

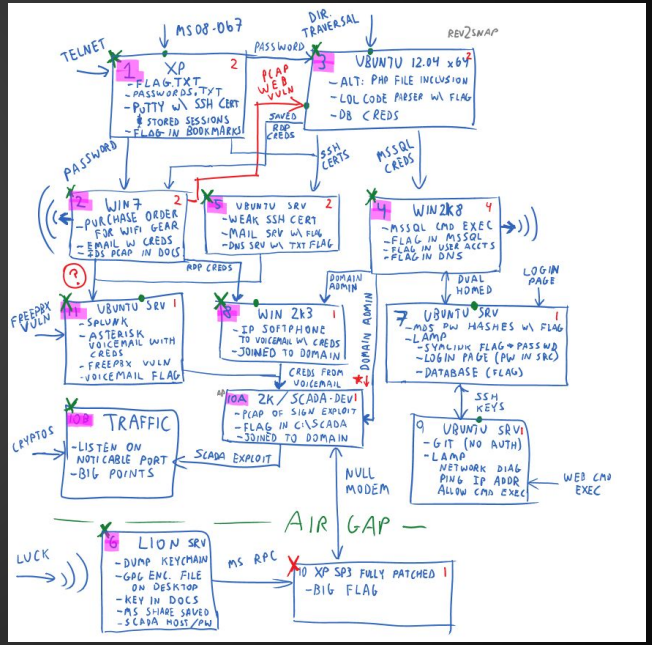
Internet: Comcast (Yeah, I know.)

Two ESX servers, switches

- pfSense firewall
- Windows, Linux, Asterisk

Extra challenges:

- SCADA / Traffic light controller
- Wifi AP / Mac Mini



Overview: Infrastructure

Internet: Comcast (Yeah, I know.)

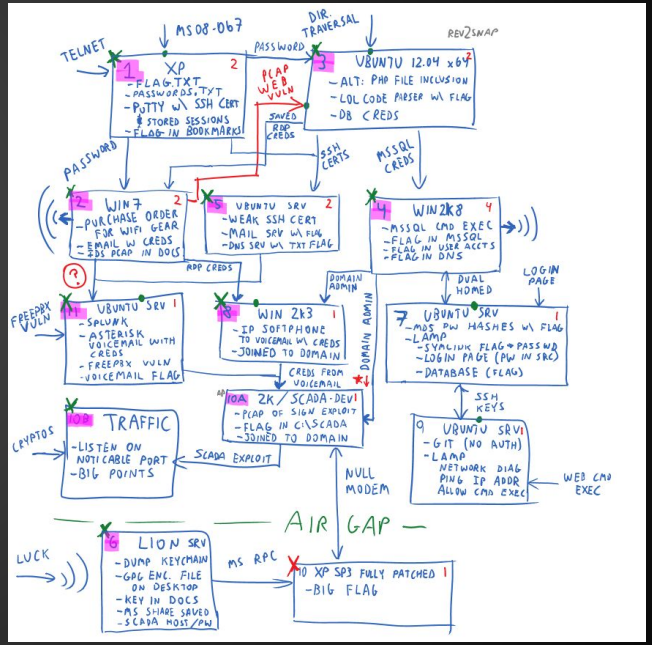
Two ESX servers, switches

- pfSense firewall
- Windows, Linux, Asterisk

Extra challenges:

- SCADA / Traffic light controller
- Wifi AP / Mac Mini

BRICKED



Overview: Infrastructure

Internet: Comcast (Yeah, I know.)

Two ESX servers, switches

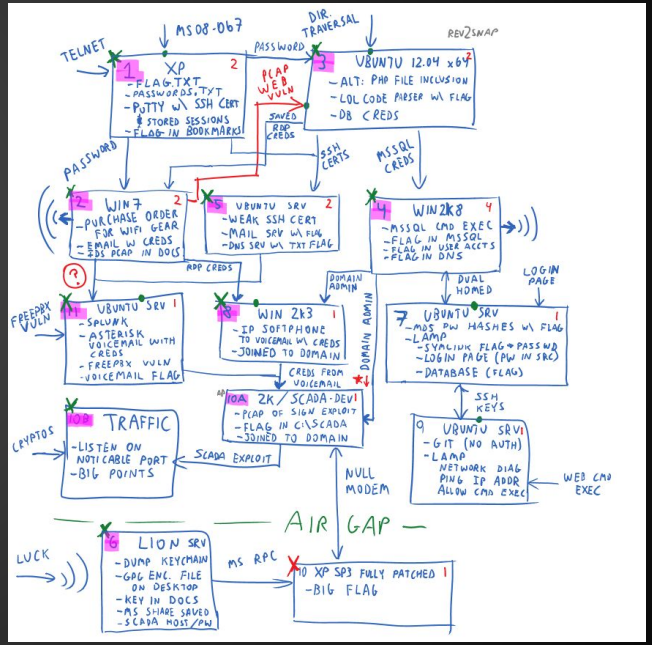
- pfSense firewall
- Windows, Linux, Asterisk

Extra challenges:

- SCADA / Traffic light controller
- Wifi AP / Mac Mini

BRICKED

NOT FOUND



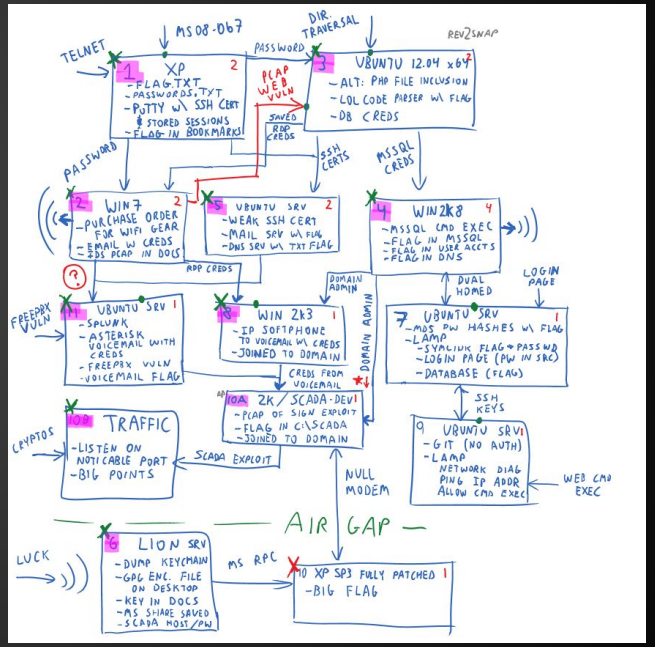
Overview: Challenges

Gaining access:

- Exploits: MS08-067 / MS10-061
- Crappy passwords
- VNC / RDP / Telnet / SSH

Finding flags (approx 3 per target):

- Easy-to-spot (UAS-A8C6B, UAS-643BA)
- User profile, settings, bookmarks
- Web: traversal, SQL, source code



Overview: Scoreboard

Custom-made scoreboard

- Flags assigned to individual hosts, while hiding host information
- Public scoreboards, Private team scoreboards with higher detail
- Countdown timer, announcements, ability to hide scores
- No frills. We just want it to work.

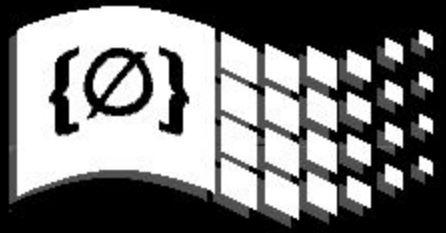
Hey, I know PHP!

- A few hours later...

Overview: Scoreboard

UnalloCTF 2013 Public Scoreboard

Team Name	Points
Cyber Scalpel	4700
Army of the 12 Monkeys!	2400
Team ?	2000
JIT Sh33p Spraying	1800
Kali x	1000
Hacksonville	1000
Shadow Cats	700
Post Office Social Club	500
Sh3LL0 Kitty Requires More Terminals	500



Links

Public Scoreboard
Team Scoreboard
Submit a Flag
Join the Chat

Announcements

Let the games begin!

Lessons Learned: Writing PHP

Teams are assigned a randomized 'hash' (8 digits) to submit flags

Flags are in the form of `'UAS-[...]'`

Lessons Learned: Writing PHP

Teams are assigned a randomized 'hash' (8 digits) to submit flags

Flags are in the form of `'UAS-[...]'`

Scores are tracked via a backend MySQL database

Lessons Learned: Writing PHP

Teams are assigned a randomized 'hash' (8 digits) to submit flags

Flags are in the form of `'UAS-[...]'`

Scores are tracked via a backend MySQL database

What could possibly go wrong?


Submit a Flag
Team Hash:
TEAM-75169131
Flag Hash:
UAS-%%%%%
Moar points please

Lessons Learned: Writing PHP

Note: mysql_real_escape_string() does not escape `%` and `_`. These are wildcards in MySQL if combined with `LIKE`, `GRANT`, or `REVOKE`.

```
//execute the SQL query and return records
$flag = mysql_real_escape_string($_GET['flag']);
$query = "SELECT points FROM flags WHERE hash LIKE '".$flag."'";
$result = mysql_query($query);
```

Lessons Learned: Writing PHP

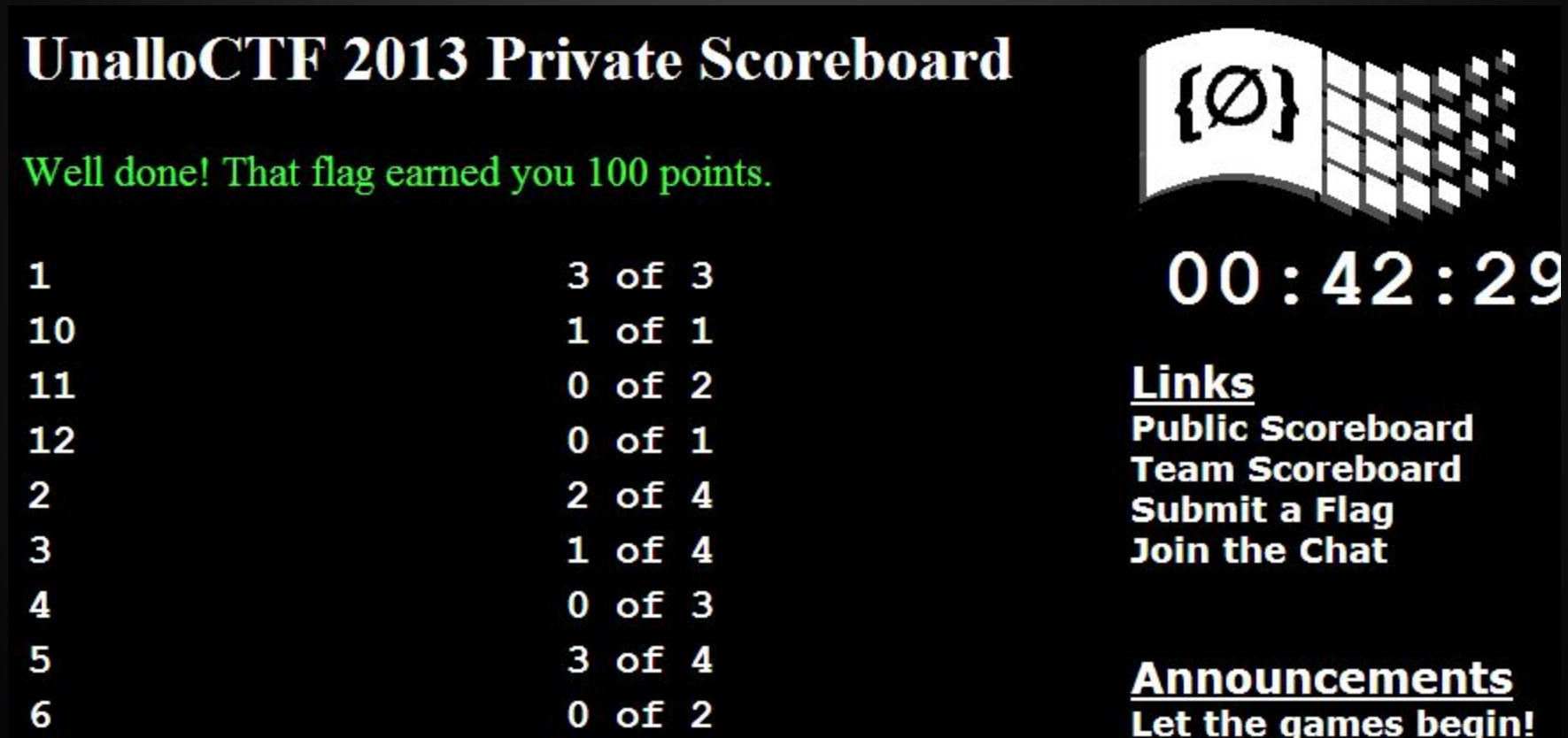
Note: mysql_real_escape_string() does not escape `%` and `_`. These are wildcards in MySQL if combined with `LIKE`, `GRANT`, or `REVOKE`.

```
//execute the SQL query and return records
$flag = mysql_real_escape_string($_GET['flag']);
$query = "SELECT points FROM flags WHERE hash LIKE '".$flag."'";
$result = mysql_query($query);
```

Lessons Learned: Writing PHP


```
//execute the SQL query and return records
$flag = mysql_real_escape_string($_GET['flag']);
$query = "SELECT points FROM flags WHERE hash LIKE 'UAS-%%%%%'";
$result = mysql_query($query);
```

Lessons Learned: Writing PHP

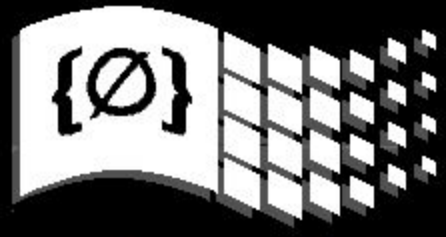


Lessons Learned: Writing PHP

UnalloCTF 2013 Private Scoreboard

WARNING: I'm pretty sure you already submitted that flag.

1	3 of 3
10	1 of 1
11	0 of 2
12	0 of 1
2	2 of 4
3	1 of 4
4	0 of 3
5	3 of 4
6	0 of 2



00:42:29

Links

Public Scoreboard
Team Scoreboard
Submit a Flag
Join the Chat

Announcements

Let the games begin!

Lessons Learned: Writing PHP

I track your submission history.

- First time? Add points and log.
- Already submitted it? Sorry.

Great.

Lessons Learned: Writing PHP

I track your submission history.

- First time? Add points and log.
- Already submitted it? Sorry.

Great.

- What could possibly go wrong?

Lessons Learned: Writing PHP


```
//execute the SQL query and return records
$flag = mysql_real_escape_string($_GET['flag']);
$query = "SELECT points FROM flags WHERE hash LIKE 'UAS-1%%%%'";
$result = mysql_query($query);
```

Lessons Learned: Writing PHP


```
//execute the SQL query and return records
$flag = mysql_real_escape_string($_GET['flag']);
$query = "SELECT points FROM flags WHERE hash LIKE 'UAS-2%%%%'";
$result = mysql_query($query);
```

Lessons Learned: Writing PHP


```
//execute the SQL query and return records
$flag = mysql_real_escape_string($_GET['flag']);
$query = "SELECT points FROM flags WHERE hash LIKE 'UAS-3%%%%'";
$result = mysql_query($query);
```

Lessons Learned: SQLi Prevention

SQL injection is a [censored].

- UAS-#####
- MySQL Prepared Statements

Note: mysql_real_escape_string() does not escape `%` and `_`. These are wildcards in MySQL if combined with `LIKE`, `GRANT`, or `REVOKE`.

Lessons Learned: SQLi Prevention

SQL injection is a [censored].

- UAS-#####
- MySQL Prepared Statements

> **Note:** **mysql_real_escape_string()** does not escape `%` and `_`. These are wildcards in MySQL if combined with `LIKE`, `GRANT`, or `REVOKE`.

```
$stmt=$db->prepare("SELECT points FROM flags WHERE hash LIKE ?");
$stmt->bind_param('s', $_GET['flag'])
$stmt->execute();
```

Enough about pwning yourself with SQLi

Let's talk about other ways to shoot yourself in the foot.
(And a even a few things we got right.)

Lessons Learned: The Targets

VM snapshots are a good thing

- Teams screw up the VMs. (Sometimes intentionally.)
  - Fighting over hosts? Cool.
  - Screwing over other teams? Not cool.

Need to incorporate automated monitoring of VMs

- Monitoring service ports?
- Monitoring processes through Hypervisor? VMware Tools?

Lessons Learned: The Targets

VM snapshots are a good thing

- Teams screw up the VMs. (Sometimes intentionally.)
  - Fighting over hosts? Cool.
  - Screwing over other teams? Not cool.

Need to incorporate automated monitoring of VMs

- Monitoring service ports?
- Monitoring processes through Hypervisor? VMware Tools?
- What could possibly go wrong? *(future work)

Lessons Learned: The Network

Per-Team VLANs are a Good Thing™

- Have fun ARP poisoning yourselves.

pfSense floating rules are a Bad Thing™

- No that's alright. Don't block the attackers from port 80.

Need better host / network monitoring

- NetFlow monitoring?
- Zeek monitoring?

Lessons Learned: Planning

Enforcing intra-team deadlines / project management

- Building 11 VMs in 36 hours is not… ideal.

We both suck at this.

- More testing
- Less panicking

	Owner	Start Date	Due Date	Status
Advertising	Forgotten	3/10/2013	3/15/2013	Yes
-- WP static page	Forgotten	3/10/2013	3/15/2013	Yes
-- Flyer / Manning CCDC table	Forgotten		4/9/2013	No
-- Registration Page (EventBrite)	Forgotten	3/10/2013	3/15/2013	Maybe
Build Environment	S / F		5/10/2013	
-- Refactor ToDo List	Surefire	3/18/2013	3/20/2013	No

Lessons Learned: Registration

Registration / Costs / Scholarships

- Free is ideal, but difficult

- People show up if they payed a small fee ($5?)
  - Always waive the fee at even the slightest request

- Eventbrite ~6.5% is so worth avoiding the hassle
  - Eventbrite API is The. Worst.

Lessons Learned: Rules

Disqualifications / Rule Enforcement

- Players will attempt to hack the scoreboard

- Threat of Disqualifications will not change anything

- Honorable mentions for cool attempts are perfect

- Be ready to kick a team off the board. (Even if they're winning)

Ideas for Next Time...

More challenges

Broader challenges

- Cryptography
- Reverse Engineering

Formal Hints & Tips (with penalties?)

Best Write-up challenge is occurs the night of Walkthrough

Immediate Feedback / Survey

Next time: OpenSOC

@eric_capuano - Concieved of the idea, bought the NUCs
@shortxstack - DevOps Master Extraordinaire
@mbromiley_DFIR - Brilliant Scenario Writer
@_surefire_ - Jack of all trades, breaker of things
@megan_roddie - Herding cats and keeping us on track
@cyberGoatPsyOps - Filling in as we slipped behind

(many, many more)

OpenSOC

OpenSOC


DTF
DOWN TO FORENSICATE
OPEN SOC
NETWORK DEFENSE SIMULATION
SHADY CLOUD
NETGEAR
ProSAFE JGS524E
TAP
OOB

OpenSOC Overview

Joining a team of CTF-building veterans:

- Team-based “Defensive Incident Response Exercise"
- Not team-versus-team, but definitely more competitive
- Welcoming newcomers into the world of DFIR
- In-person at various local conferences and BSides events
- We had a blast. People learned things. It was fun.

OpenSOC @ BSidesAusitn

OpenSOC @ BSidesDC

Use an open-source scoreboard

Build a solid team

OpenSOC Overview

Joining a team of CTF-building veterans:

- Team-based “Defensive Incident Response Exercise"
- Not team-versus-team, but definitely more competitive
- Welcoming newcomers into the world of DFIR
- In-person at various local conferences and BSides events
- We had a blast. People learned things. It was fun.

We should take it to DEF CON?

- What could possibly go wrong?

Use an open-source scoreboard

Use an open-source scoreboard

OpenSOC @ DEFCON 2018

We should take it to DEF CON?

- What could possibly go wrong?

271 players

115 teams

OpenSOC @ DEFCON 2018

We should take it to DEF CON?

- What could possibly go wrong?

271 players

115 teams

People who would stay up 72 hours, with the resolve to solve every single challenge you threw at them

OpenSOC @ DEFCON 2018

What did we learn?

- Scoreboards don't scale
- Many defensive tools don't scale
  - Tools like Elastic are written so 5 people can query 100GBs of data
  - They are NOT written so 100's of people can query 5GB of data

OpenSOC @ DEFCON 2018

What did we learn?

- Scoreboards don't scale
- Many defensive tools don't scale
  - Tools like Elastic are written so 5 people can query 100GBs of data
  - They are NOT written so 100's of people can query 5GB of data
- People who play CTFs at DEFCON are insane
  - You will never have enough content to keep them satisfied

OpenSOC @ DEFCON 2018

What did we learn?

- Scoreboards don't scale
- Many defensive tools don't scale
  - Tools like Elastic are written so 5 people can query 100GBs of data
  - They are NOT written so 100's of people can query 5GB of data
- People who play CTFs at DEFCON are insane
  - You will never have enough content to keep them satisfied
- Your team will burn out.

OpenSOC @ DEFCON 2018

Lessons learned

- Load test your scoreboard.
- Anticipate double the number of expected players.
- Have open lines of communication with tool developers
  - Seriously, they'd love the opportunity to see their tools stress tested
  - (and they also want to save face)
- Don't expect to keep players 100% occuplied
- Shut down the event at night.
- Schedule so your team gets stretch/food/destrss breaks.

OpenSOC @ DEFCON 2019

OpenSOC @ DEFCON 2019

541 players
220 teams
Using ZeroTier

Finals round
- shutdown on Saturday
- rebuild everything overnight
- all-new scenarios on Sunday

OpenSOC @ DEFCON 2019

541 players

220 teams

Using ZeroTier

Finals round

- shutdown on Saturday
- **rebuild everything overnight**
- all-new scenarios on Sunday

OpenSOC @ DEFCON 2019

541 players

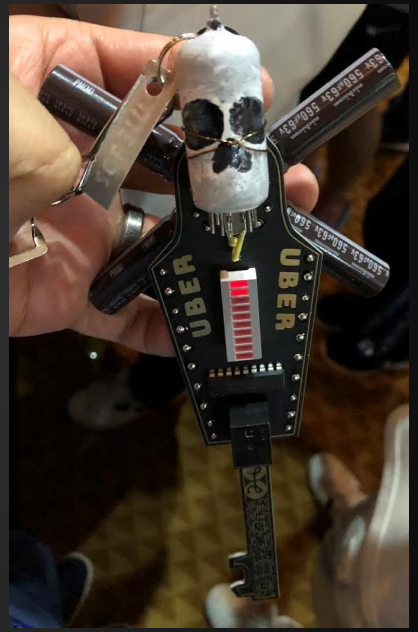
220 teams

Using ZeroTier

Finals round

- shutdown on Saturday
- **stay up all night rebuilding and testing everything**
- all-new scenarios on Sunday

OpenSOC @ DEFCON 2019



OpenSOC @ DEFCON 2019

Hey folks - just wanted to give a specific THANK YOU to the crew for BTV.

This year was my very first DEFCON.

Three weeks after the con, one of my clients was breached - big time.

Using some of the skills I picked up at the [OpenSOC] CTF and more importantly, the CONFIDENCE to get in the trench and work, I not only stopped the attack but found the specific person responsible for the attack and created a dossier for the LEO cyber guys - it lead to an arrest!

I know this might be insignificant in the grand scheme but has been a career highlight for me. Wanted to extend my thanks for putting on the village!

OpenSOC @ DEFCON 2020

CANCELLED

OpenSOC @ DEFCON 2020

OpenSOC @ DEFCON 2020

Fully remote, via ZeroTier

Kept the Finals Round

Moved to Discord (OMG yes plz)

Open to all timezones (OMG plz no)

Decentralized team

- Makes it really difficult to cooperate
- Tensions were high. Things slipped through the cracks

OpenSOC @ DEFCON 2020

Fully remote, via ZeroTier

Kept the Finals Round

Moved to Discord (OMG yes plz)

Open to all timezones (OMG plz no)

Decentralized team

- Makes it really difficult to cooperate
- Tensions were high. Things slipped through the cracks

No Black Badge :-(

Lessons Learned

ZeroTier is pretty badass

Use finals rounds to separate:

- people just having fun
- people who want to win a badge

CTFd scoreboard was pretty darn solid

Custom front-ends to tools to rate-limit and prevent dumb queries

Scheduling shifts was important, and we missed it

Corelight Zeek CTF

In-person at conferences, but also fully-remote via Zoom

Just for fun, give folks a brief tutorial at the beginning

- Winners gonna win (offer some prizes, sure)
- Make it enjoyable for n00bs

Help available via Zoom breakout rooms

- Trained volunteers to answer questions
- Share screens, give personal walkthroughts

Corelight Zeek CTF

In-person at conferences, but also fully-remote via Zoom

Just for fun, give folks a brief tutorial at the beginning

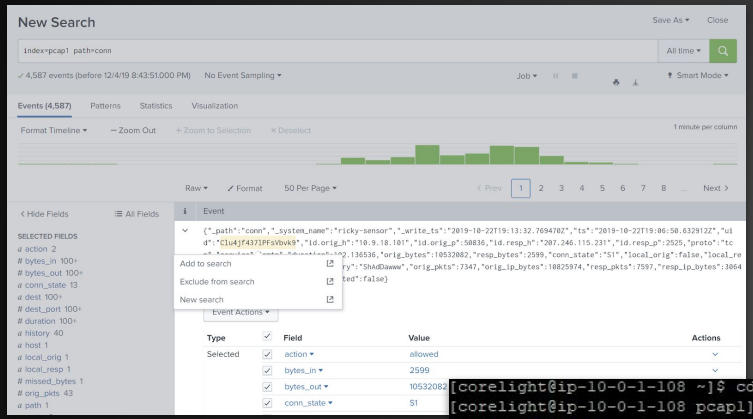
- Winners gonna win (offer some prizes, sure)
- Make it enjoyable for n00bs

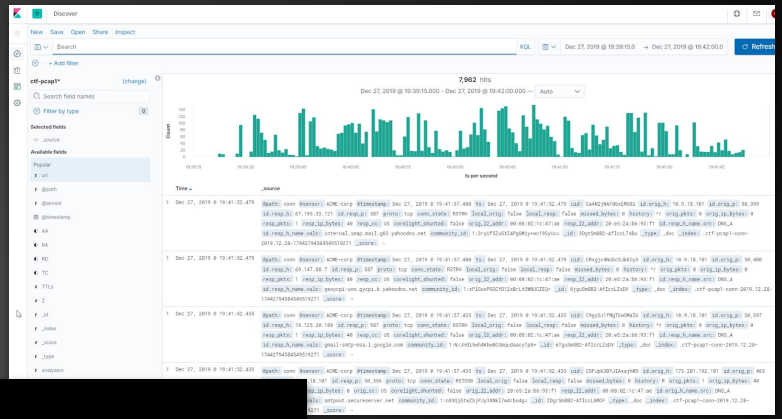
Help available via Zoom breakout rooms

- Trained volunteers to answer questions
- Share screens, give personal walkthroughts

Give players choices on how to solve flags

Corelight Zeek CTF






```
[corelight@ip-10-0-1-108 ~]$ cd tsv_logs/pcap1
[corelight@ip-10-0-1-108 pcap1]$ ls -1
capture_loss.log
conn.log
dns.log
files.log
http.log
known_hosts.log
known_services.log
loaded_scripts.log
notice.log
packet_filter.log
pe.log
smtp.log
software.log
ssl.log
stats.log
weird.log
x509.log
[corelight@ip-10-0-1-108 pcap1]$ cat ssl.log | zeek-cut id.resp_h ja3 ja3s
```

Corelight Zeek CTF: Lessons Learned

It's more fun to teach people than to elevate pros

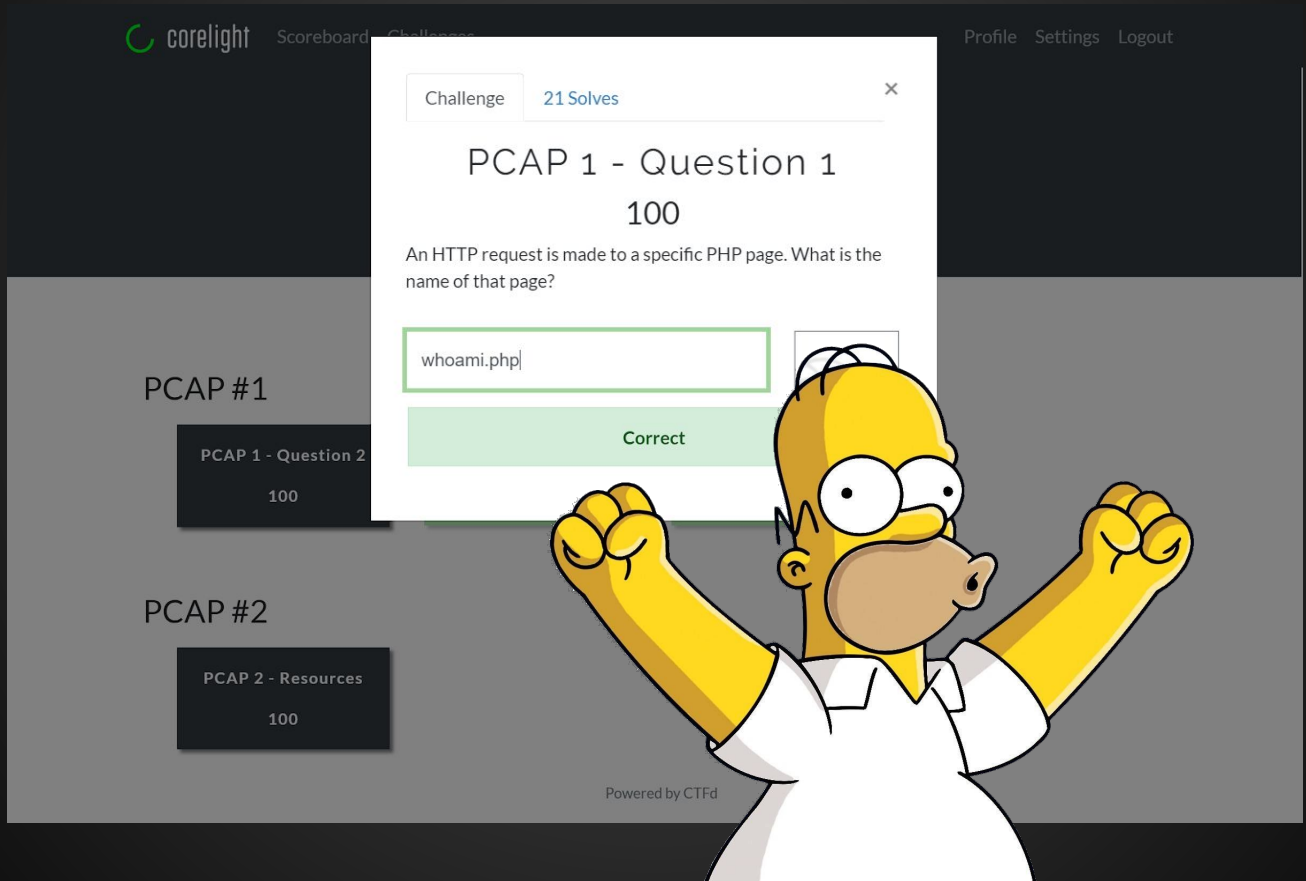
Having a structured way to teach volunteers is key

Build it, and they will come

Focus on making it a fun environment

- CTF playlist
- Banter between hosts
- Scoreboard shoutouts

Let the games begin!



Corelight Zeek CTF: Lessons Learned

CloudFormation means we can scale:

```
AWSTemplateFormatVersion: 2010-09-09
Description: A Capture The Flag (CTF) scoreboard and named point-of-access
Parameters:
  Subdomain:
    Description: The xxx in xxx.ctf.corelight.io
    Type: String
    MinLength: 2
    MaxLength: 30
    AllowedPattern: '^[a-zA-Z][a-zA-Z0-9\-_]+$'
    ConstraintDescription: 'Must be a valid DNS subdomain matching [a-z][a-z0-9]+'
 ScoreboardAmi:
    Description: The scoreboard AMI to be provisioned
    Type: String
    MinLength: 2
    MaxLength: 30
    AllowedPattern: '^ami-[a-fA-F0-9]+$'
    ConstraintDescription: 'Must be a valid AMI (eg. ami-03dc0bf2e05c193c3)'
```

Corelight Zeek CTF: Lessons Learned

CloudFormation means we can scale:

```
AWSTemplateFormatVersion: 2010-09-09
Description: A Capture The Flag (CTF) scoreboard and named point-of-access
[...]

Resources:
  ScoreboardInstance:
    Type: 'AWS::EC2::Instance'
    Properties:
      ImageId: !Ref ScoreboardAmi
      InstanceType: t2.medium
      AvailabilityZone: us-east-2c
      UserData: { "Fn::Base64" : { "Fn::Join" : ["", [
        "#!/bin/bash\n",
        [...]
      SecurityGroupIds:
        - sg-05452113259120957
```

Here's what I've learned

Building CTFs is more fun than playing them

Writing well-balanced challenges is key
(not to obvious, but it should be clear how to solve)

Helping people learn is more fun than torturing them

Strive for tested, open-source solutions (CTFd)

Make it approachable and fun!

Be prepared to screw up and learn

Want to write your own CTF?

Get comfortable playing a few. Learn what makes it fun.

Find your niche. It may be challenge writing, devops, organizing, getting sponsors, helping folks 1:1, or more...

Start small. It's easier to load test for 20 people than for 200.

Make it easy for people to join, eg. via web browser. No building environments, getting Kali, paid (or pirated) tools

Build a team around you and care for each other.

Want to write your own CTF?

I'm happy to chat, always. Hit me up:

Email: aaronsoto@gmail.com

UT-CTF slack: @surefire

Twitter: @_surefire_