





All Things CTF!

Nov 21, 2019

PRESENTER:

Ray Doyle

- Intro by Don Donzal, EH-Net Editor-in-Chief
- Bio – Ray Doyle
 - What are CTFs?
 - Why Play?
 - Demos of Common Challenges
 - Where to play
 - “You had me at CTF...”
 - Designing and Hosting a CTF (optional)
 - Advancing Your Career with CTFs
 - Skill Building Resources to Compete in the Virtual Arena
- Q&A





- Video will be made available on EH-Net
- Style = Interview!
 - Q&A in question tab in GTW
 - Twitter using #EHNet
- Post Game in EH-Net “**CTF**” Group:
<https://www.ethicalhacker.net/groups/ctf/>
- Goal for today – Spark conversation.
Advance your career!

OVERVIEW OF THE NEW EH-NET



- General Layout
 - Magazine side - Columnists, Features, Global Calendar
 - Community side – Members & Profiles, Activity, Forums, Groups, Community Articles
- Building your “Personal Ethical Hacker Network”
- [Hello world! – Get Published in the EH-Net Community](#)
- Limited Time – All new members get a free pen testing course from eLS!!





The man, the myth, the legend; **Ray Doyle**, OSCE, OSCP, GXPN, aka [@doylersec](https://twitter.com/doylersec) is an avid pentester and security enthusiast. He now works as a Senior Staff Adversarial Engineer at Avalara and was formerly a Principal Penetration Testing Consultant at Secureworks. You can visit his blog at <https://www.doyler.net>, where he has been posting for over four years now!

When he's not hacking for work he's, well, hacking for fun as well...Ray has attended various security conferences for the past few years now, and has even spoken at CarolinaCon, BSides Manchester, BrrCon, BSides Denver, and BSides Raleigh/RDU. He has competed in numerous hacking competitions and CTFs over the years, most recently with [Team EverSec](#), and managed to place 1st in the Raleigh BSides CTF, 1st in the DerbyCon CTF (winning the last DerbyCon 'black badge'), 1st in the DEF CON 24 SOHOpelessly Broken CTF (winning a DEF CON 'black badge'), and 1st in the DEF CON 25 Wireless CTF (helping to win another black badge).

Other than security, you can always hit him up for a Super Smash Brothers Melee money match or in City of Heroes ([@doyler](https://twitter.com/doyler)).



What is “CTF”?

CTF

['see, tee, ef]
NOUN

“Capture the flag (CTF) is a traditional outdoor game where two teams each have a flag (or other marker) and the objective is to capture the other team's flag, located at the team's "base," and bring it safely back to their own base.”

Source: [Capture the Flag entry on Wikipedia](#)

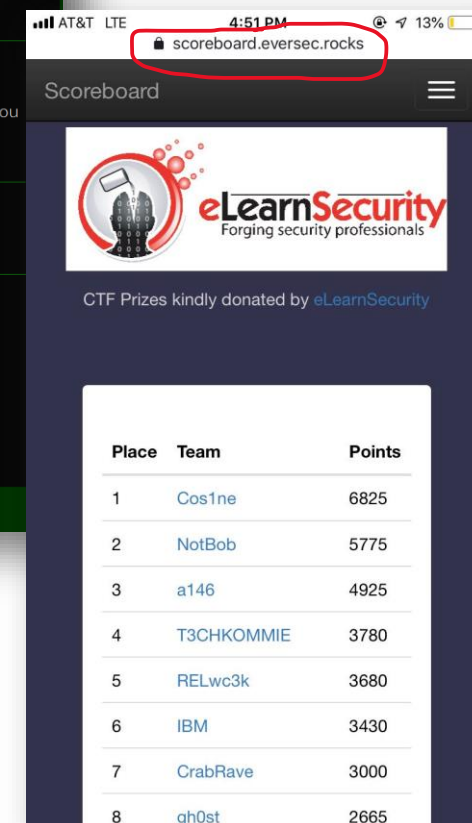
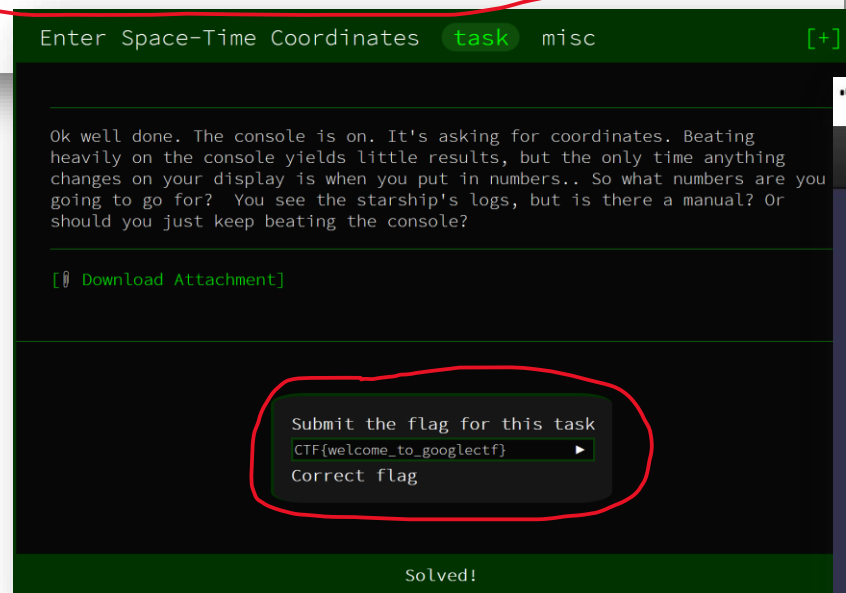
WHAT IS A CTF?



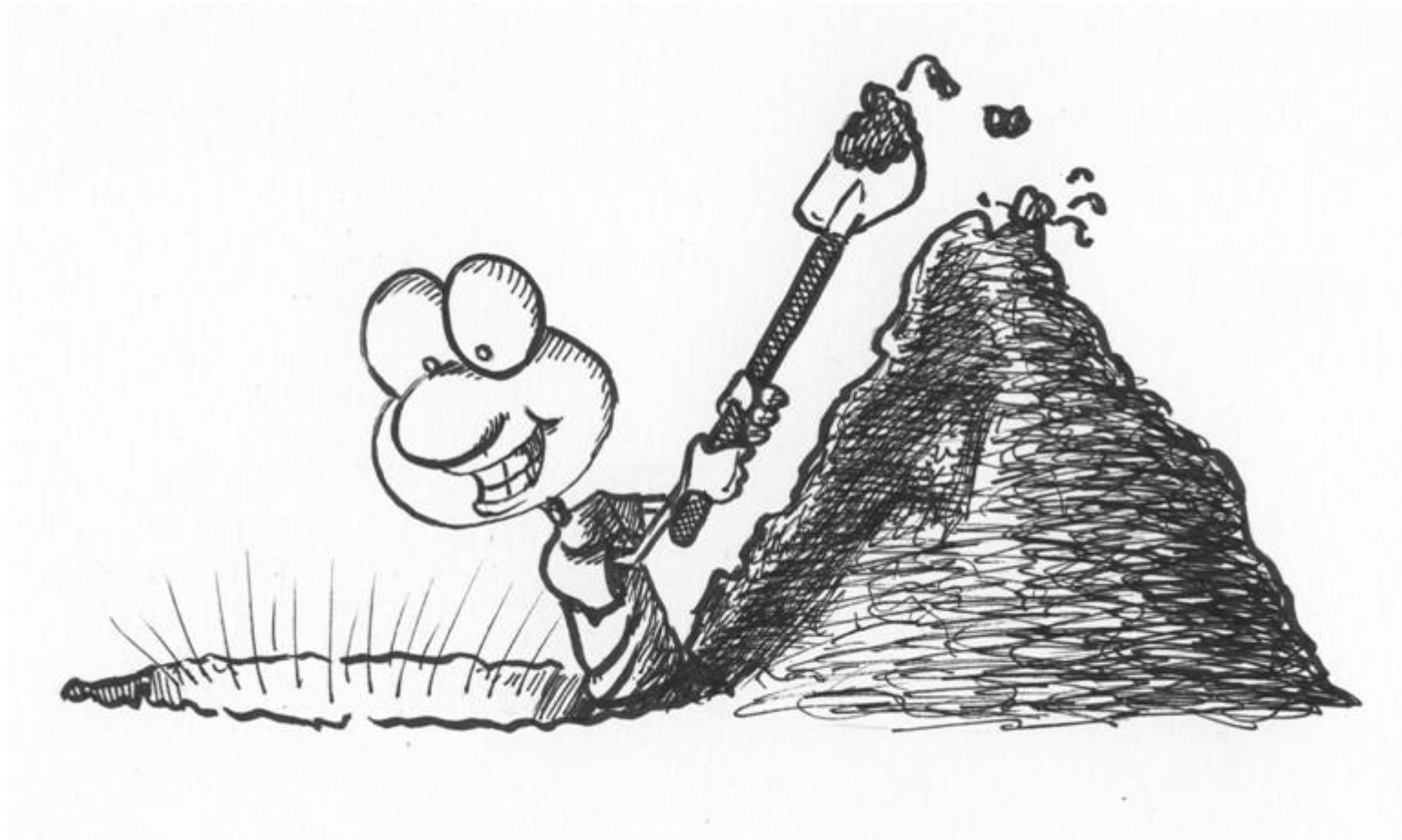
Enter 72bit hex-encoded key:

Correct 😊 The flag is **FARADAY{EverSecForever!!!}**

- CTF competitions are generally on InfoSec topics with challenges, winners, and sometimes even prizes!
- Often a series of puzzles to solve or computers to attack and defend
- Team or individual based
- Solved challenges usually give “flags”
(ther5s_n0_Place_l1ke_h0m3)



LIVE DEMO PART 1 – BEGINNER CHALLENGES X2



WHY DO CTFS?



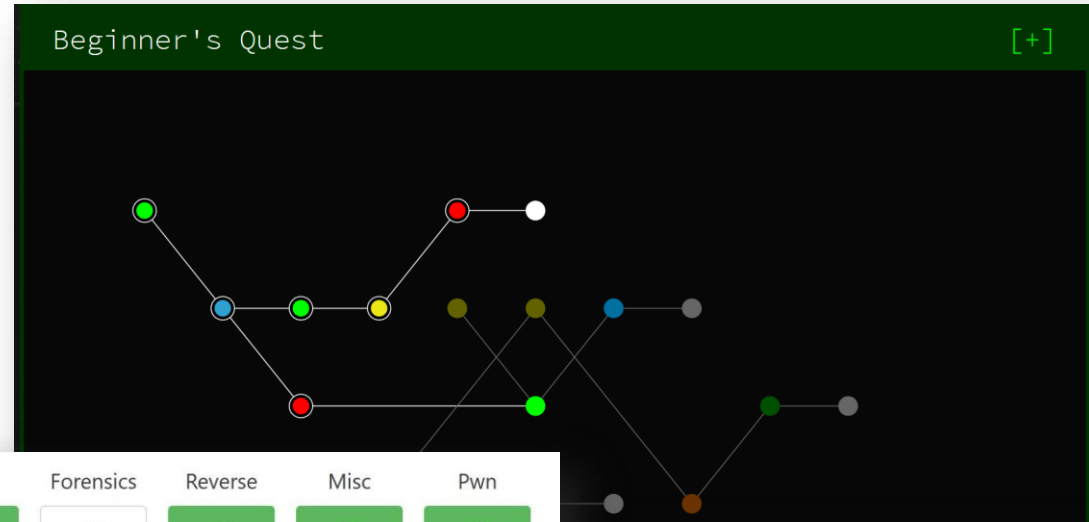
- Closest thing to hacking / pentesting for many people
- Gain experience with tools
- Hone skills, learn new ones
- Competition is fun, motivating, and aggravating
- We learn when we fail! Better here than a in production environment.
- Meet new people, potential employers or co-workers
- CTFs as part of job interviews
- Prizes – Swag, vouchers and sometimes even CASH



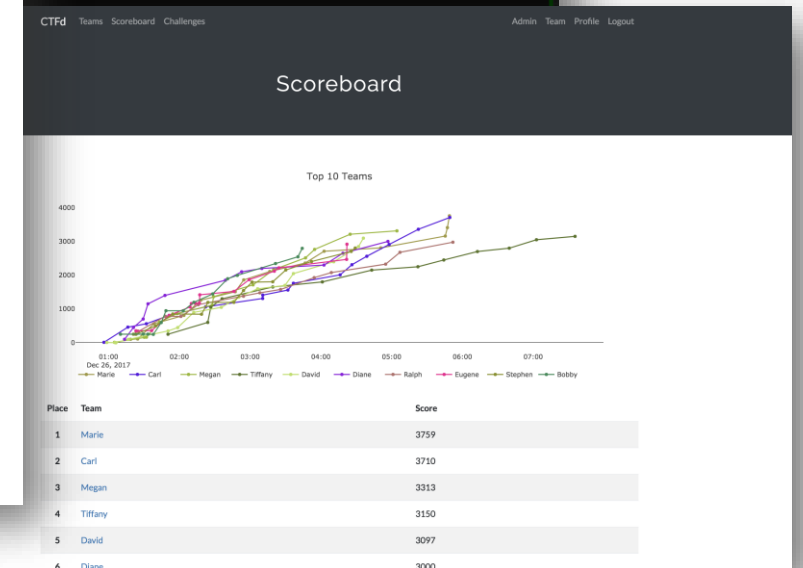
TYPES OF CTFS



- Jeopardy
- Attack-Defend
- Mixed
- Scenario



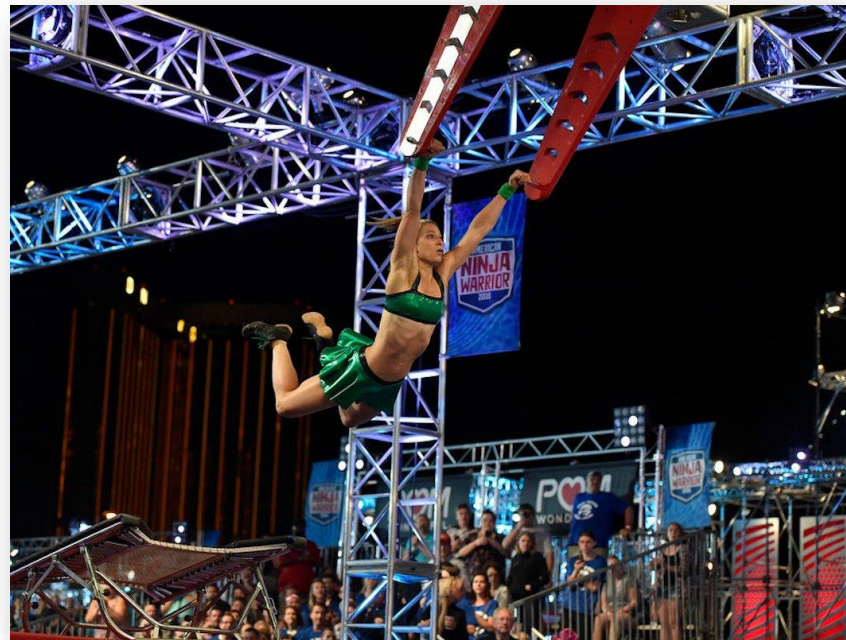
Web	Crypto	Forensics	Reverse	Misc	Pwn
1	165	100	50	50	50
150	150	150	100	100	150
204	150	150	150	165	200
203	200	200	200	150	250
206	257	200	300	200	323
318	334	250	300	300	440
325	400	347	400		
	430	350			



CTF CHALLENGE TOPICS

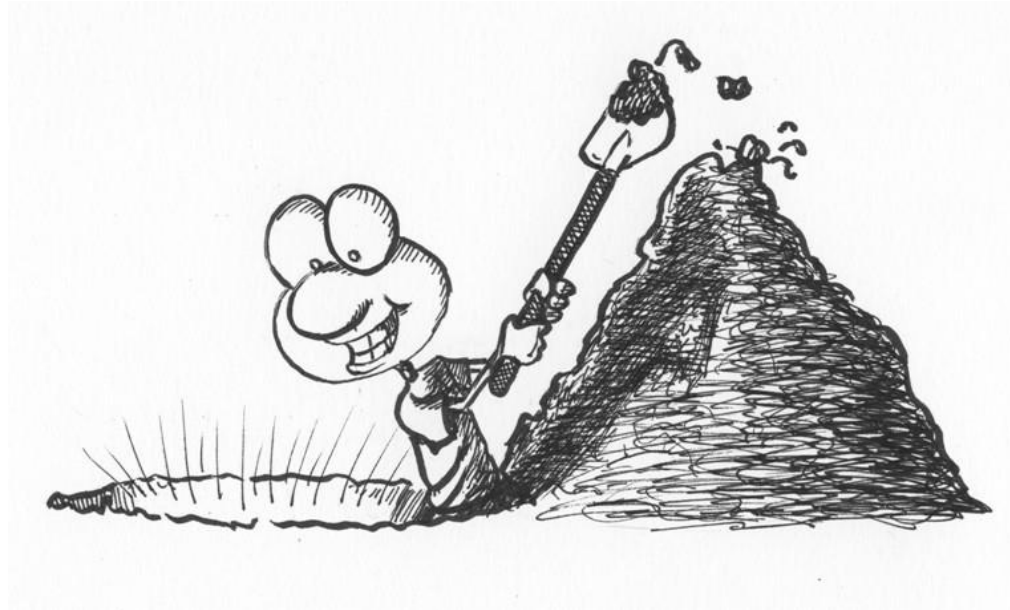


- **Network challenges**
- **WebApp**
- Mobile App
- IoT / Embedded
- Wireless Hacking
- **Cryptography**
- Binary Exploitation
- Forensics
- Games



- **Steganography**
- Physical Attacks
- **Reverse Engineering**
- Packet Analysis
- Obscure systems/languages
- Programming
- Electronics
- And more!

LIVE DEMO PART 2 – INTERMEDIATE CHALLENGES X2



Flag.txt contains:

```
Vm1jblppQmhZbWNnZFc1bGNTQm5ZaUJvWVhGeVpXWm5ibUZ4TENCemRtR  
nhJR2QxY2ICTFFrVWdhblpuZFNCC1ltaGxJSGx5YzJjZ2RXNWhjU0F0SUVKUIY  
zWkJWRk41VFhwWGRrRjZWm1ZNZWsxMIRVcE5ka3gzVjNWTmVrd3pUWHBY  
ZGxveVYzbE1SM2wyVfVwTmRreDNWM1ZDVkUxMIRFZFhka0ZVVTNsTVlzbD  
ZUSHBYZUV4M2NYWk1TbGQzVFVkvGVreDNIRFJDVkv3MVRWUINha3gzZFh  
WQ1NsSnNURXBYZFUxNINyWk1Ta0YyUVVwSU5FeDZUWFZCZEqwOQ==
```


Who's Hosting CTFs? EVERYONE!!



picoCTF





- <https://ctftime.org/>
- CTFs
- Upcoming
- Archive
- Calendar
- Teams
- FAQ

CTFs
Upcoming
Archive
Calendar
Teams
FAQ
Contact us
About
Sign in

Team rating

2019
2018
2017
2016
2015
2014
2013
2012
2011

Place	Team	Country	Rating
1	Dragon Sector		1092.652
2	Balsn		1028.527
3	Plaid Parliament of Pwning		992.151
4	p4		892.113
5	TokyoWesterns		868.981
6	dcua		793.642
7	LC+BC		782.609
8	Tea Deliverers		778.689
9	r3kapig		710.578
10	Bushwhackers		674.898

Full rating
Rating formula

Past events

With scoreboard
All

ASIS CTF Finals 2019

Nov. 17, 2019 17:00 UTC | On-line | Weight voting in progress

Place	Team	Country	Points *
1	perfect blue		164.040
2	Dragon Sector		113.624
3	TokyoWesterns		98.343

356 teams total
Tasks and writeups

GreHack CTF 2019

Nov. 16, 2019 06:30 UTC | Grenoble, France | Weight voting in progress

Place	Team	Country	Points *
1	GreHax0r		0.000
2	Sogeti Aces of Spades		0.000
3	sivi-ha-kerez		0.000

32 teams total
Tasks and writeups

Dragon CTF 2019

Nov. 15, 2019 15:00 UTC | Warsaw, Poland | Weight voting in progress

Place	Team	Country	Points *
1	p4		198.000
2	Plaid Parliament of Pwning		121.423
3	ALLES!		101.538

14 teams total
Tasks and writeups

Upcoming events

Open
High-School

Format	Name	Date	Duration
	D*3CTF 2019 On-line	Fri, Nov. 22, 12:00 — Sun, Nov. 24, 12:00 UTC 16 teams	2d 0h
	RuCTFE 2019 On-line	Sat, Nov. 23, 10:00 — Sat, Nov. 23, 19:00 UTC 53 teams	9h

CTFs... Are you ready to play?



- Just enter (CTFtime) or signup early
- Join a random team (in person is easier)
- [/r/OpenToAllCTFteam](#)
- Google
- Read write-ups of older challenges, as well as challenges that you attempted (whether you completed them or not) <https://github.com/ctfs/>
- Watch video write-ups
- Practice, practice, practice





Join a Team

CTF TIME CTFs Upcoming Archive Calendar Teams FAQ Contact us About

How can I join the team

Send membership request using form in your [Profile](#):

Join existing team

Team name

Smoked Chicken

Send request

Create new team

If your team has active members, they will need to approve your request or send you an invitation code:

Join existing team

Team name

Smoked Chicken:5

Send request

Create new team

Invitation code can be found in [Profile](#) -> [Your teams](#) -> [Edit your team](#)

Team members

Use this code to invite new members:
Smoked Chicken:5

If your team has no registered members, administrators will approve your membership request, and then you will be

What does "Academic" team means?

You can mark your team as "Academic" if your team is comprised of university students or academics only and assoc


I don't have a team but wanna play

Well, you can play alone or try to get a team. It's more fun to compete with a team. You can hire people from your uni provide your skills in [Profile](#) name and check "I'm looking for the team" - may be someone will invite you. Also, you can

Read Writeups

doyler.net

SECURITY NOT INCLUDED STEALING FIRST



[← Cracking 256-bit RSA Keys - Surprisingly Simple!](#) [BoFA CTF Part 2 - Climbing the Scoreboard \(DerbyCon 9\) →](#)

BY DOYLER | SEPTEMBER 28, 2019 - 12:00 PM [Jump to Comments](#)


Bank of America CTF – Challenge Coins @ DerbyCon 9

I took part in the Bank of America CTF during the last [DerbyCon](#), and I wanted to share some of my write-ups.

Bank of America CTF - Introduction

Just like [last year's DerbyCon](#), the Bank of America team was hosting a CTF for anyone at the conference.

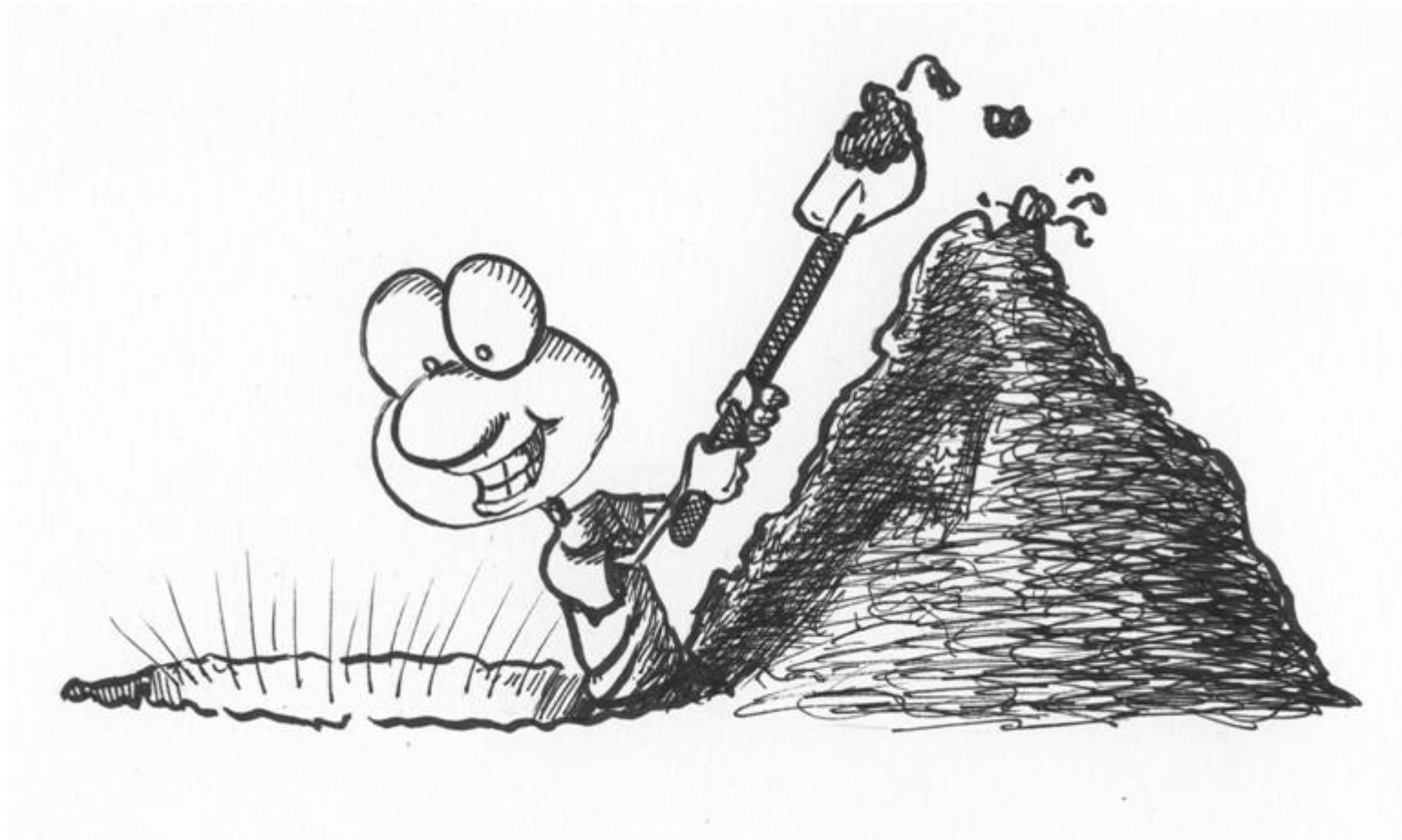
I won a challenge coin from this last year, and it was sweet looking.



Video Walkthroughs



LIVE DEMO PART 3 – ADVANCED CHALLENGE X1



Pro Tips: Advanced CTF Tactics



- Slack
- Trello
- Specialization
- Out-of-band tactics and resource gathering

Derbycon 2016 Eversec ☆ Team Visible

Todo

- Index of /
 - [tiki-15.0/](#)
 - [tiki/](#)
- 172.30.1.248 - port 22,37,80, 111, 113

In Progress

- helpberkz
 - Account Login
 - Search in Knowledgebase
 - Knowledgebase
 - Most popular articles
- 172.30.1.247 - 80,135,139,443,1026,3306
- Easy Chat Server
- 172.30.1.252 - port 80,135,139,445,3389

Possibly Done?

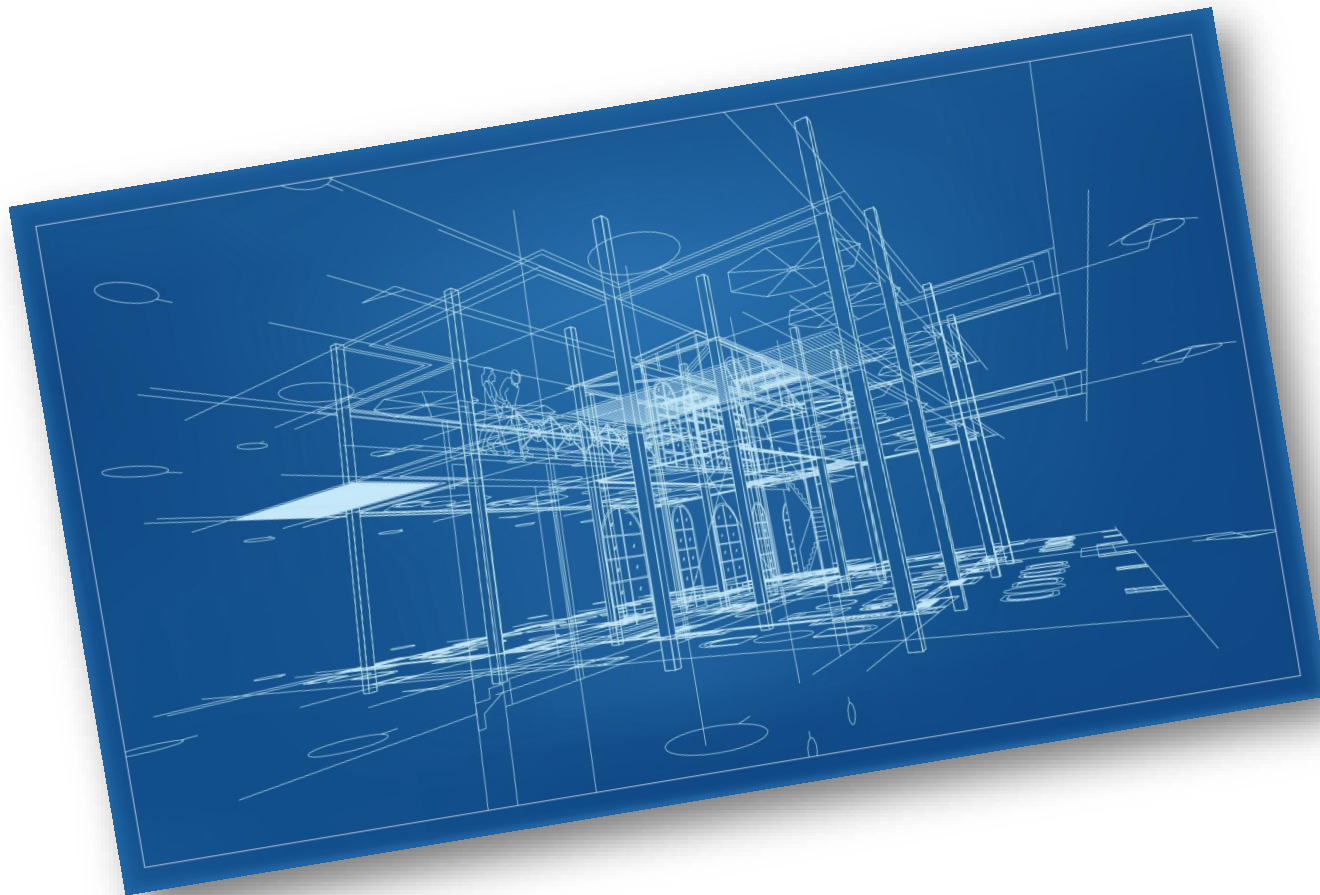
- Cisco ASDM 7.1(4)
- 172.30.1.253 - port 22,80,443

Done

- UNC Portal Secure Login
- 172.30.1.243 - port 80
- Password List
- Other user
- 172.30.1.250 - 3389
- RNC - 172.30.1.242 - 22,80



- To “story” or not to “story”
- Designing Challenges
- Making them *virtually* real
- Submission Interface
- Scoreboard
- Promotion
- Prizes
- Expenses



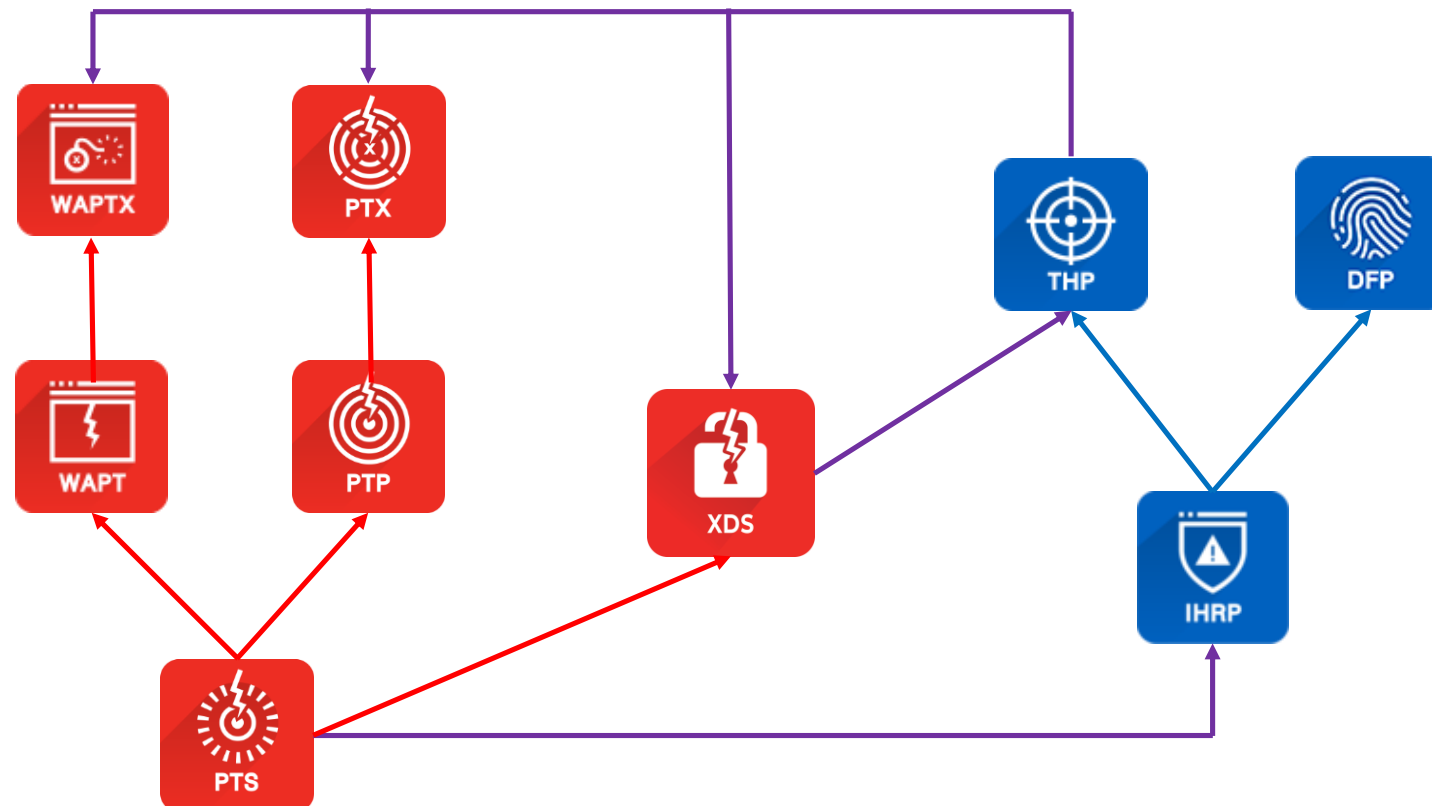


- Incident Responder
- SOC Analyst
- SE (Visher, Phisher, etc.)
- OSINT Investigator
- Secure Code Reviewer
- Project Manager
- Penetration Tester
- Red Team Member
- Reverse Engineer
- Malware Analyst

HOW DO I GET THERE?



- Experience – CTFs, Employment, Home lab, Non-profits, Open source projects, etc.
- Practical Training – eLearnSecurity Training Paths (NIST-NICE Role-based Training)
- Will playing CTFs get me a job?

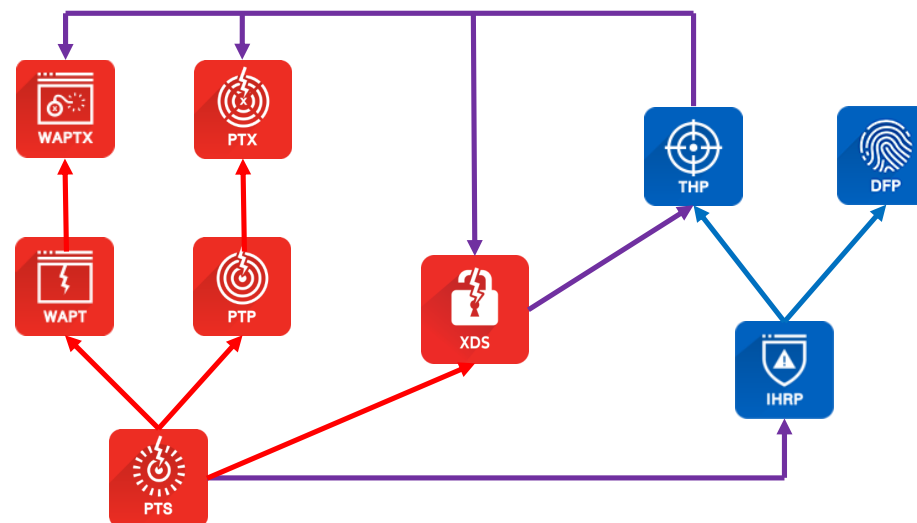


<https://www.elearnsecurity.com/course/>

EARLY BLACK FRIDAY DEAL



eLearnSecurity
Forging security professionals



<https://www.elearnsecurity.com/course/>

BUILDING YOUR SKILLSET – CTF RESOURCE LIST



- [Ray's List!!](#)
- [ctftime.org](#)
- github.com/zardus/ctf-tools - long list of tools separated by challenge category by Yan Shoshitaishvili
- [CTF>101](#), [CTFlearn](#), [CTF Field Guide](#) – Thanks Pico!
- Practice CTFs
 - [picoCTF](#) by Carnegie Mellon
 - [Pwn Adventure](#) – MMO client / server you can run
 - [OWASP Juice Shop](#) – Vuln webapp and CTF
 - [VulnHub](#), [Hack.me](#) – Vuln practice VMs
 - <https://overthewire.org/wargames/>
 - [Google CTF – Beginner](#)
- Previous [CTF writeups](#)
- [GynvailColdwind YouTube Ch](#) – Video CTF Walkthroughs
- [Building Your Own Kickass Home Lab](#) by Jeff McJunkin
- [Top tools & resources for running a CTF](#) by Larry Seltzer



EVERYBODY LOVES RAYMOND!



- Follow Ray [@doylersec](https://twitter.com/doylersec)
- Website/blog - <https://www.doyler.net>
- Follow EverSec CTF [@EverSecCTF](https://twitter.com/EverSecCTF)



Avalara



“WepApp Pentesting FTW”

Thursday December 19, 2019 @ 1:00 PM EST

[@PhillipWylie](#), CISSP, NSA-IAM, OSCP, GWAPT is a Principal InfoSec Engineer on the Assessment Services Penetration Testing Team. Phillip is also an Adjunct Instructor at Richland College teaching Ethical Hacking and System Defense, a Bugcrowd Ambassador and the founder of [The Pwn School Project](#). Phillip has over 21 years of experience in InfoSec and IT and has performed pentests on networks, wireless networks, applications including thick client, web application and mobile. His passion for sharing, mentoring and educating led to the founding of The Pwn School Project, a free monthly educational meetup with a focus on hacking. He is also featured in “Tribe of Hackers – Red Team”.



Guests, Dates & Topics Subject to Change

Q&A

POST GAME IN EH-NET GROUPS

THANK YOU FOR JOINING

 **EH-NET
Live!**



Follow us:



www.ethicalhacker.net
team@ethicalhacker.net

