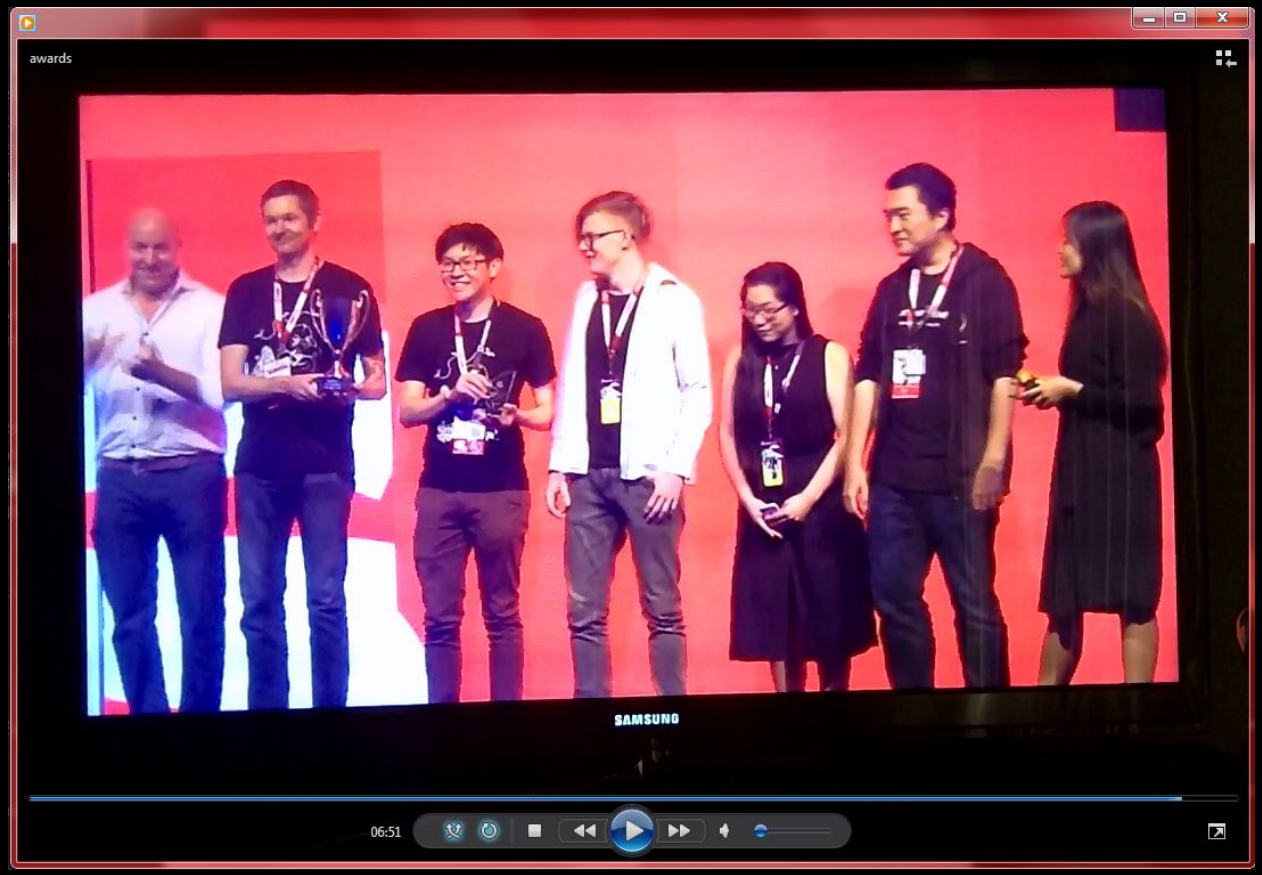
CTF WTF?

CaptureTheSwag // farmingsimulator2015

TOPICS

- What is a CTF
- The context of CTFing – Why CTF?
- Problem categories and skills
- Pre requisites
- CTF workflows and pipelining
- How to get started
- CySCA as a CTF
- A whole world of CTFs

WHO ARE WE?



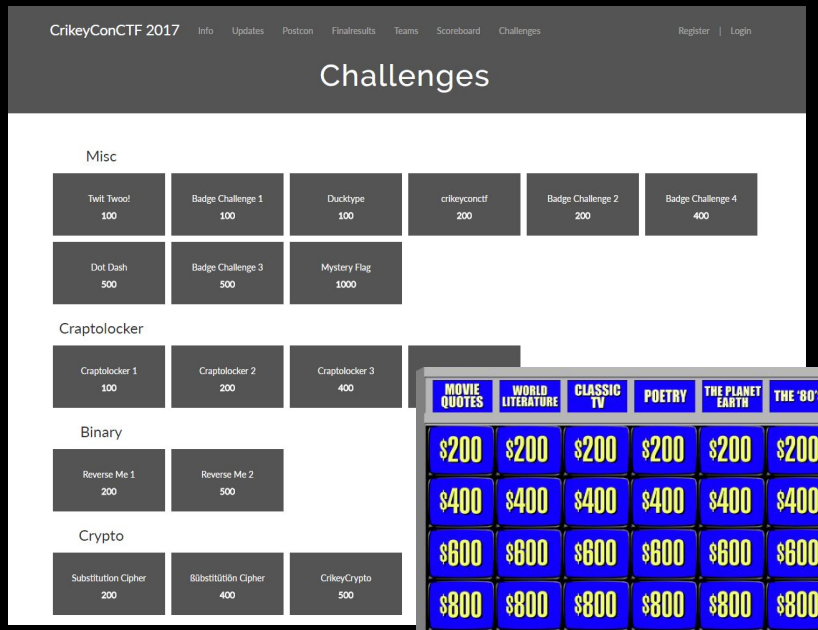
CTF WTF - WHAT IS A CTF?

- CTF (Capture the Flag) competitions are a kind of information security competition
- Generally held over a 24 – 48 hour period
- Competitors are given challenges covering many facets of security
- Three types of CTF competitions in order of popularity are:
  - Jeopardy Style
  - Attack defense
  - Mixed
- Solving challenges in the competition awards flags which are submitted for points – typically flags look like:

flag{1337_sp34k_fl4gs_4r3_c0mm0n}

JEOPARDY STYLE CTF

- Concept based on the TV game show “Jeopardy”
- Choose the category and attempt the challenges ranked in order of difficulty by point value
- Point values generally from 50 – 1000 points
- Most common CTF by miles

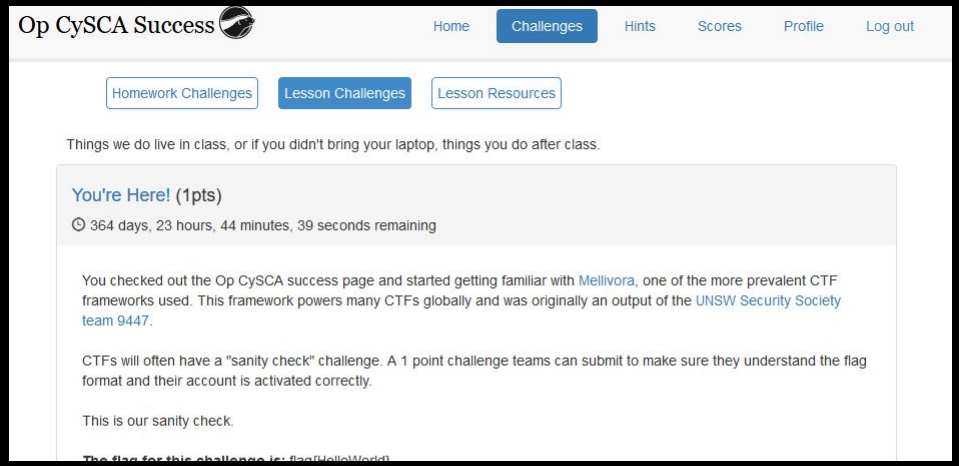


ATTACK DEFENSE CTF

- Teams are assigned services and a virtual environment for those services to run on
- Each team must attack the other team's services to recover flags
- Each team must also PATCH their own services to remove vulnerabilities while maintaining uptime and functionality
- Flags change regularly and must be re-exploited and submitted to continue to gain points once per round
- Rounds last 5 – 10 minutes
- If one of your services is down or doesn't pass unit tests you get less points for that round

SIGNUP TO THE CLASS JEOPARDY CTF

- Visit the below URL now and register yourself, think of a cool CTF team name.
- URL: https://cysca.ctf.rip
- Claim your first flag:
  - Lesson Challenges Cat
  - Flag: flag{HelloWorld}



WHY CTF?

Don’t you have better things to do?

WHY WOULD I CTF?

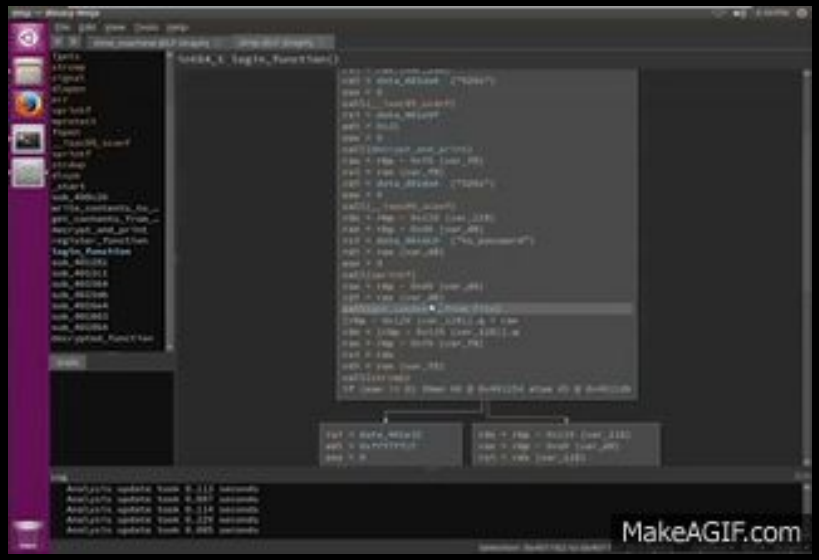
- CTFs are now becoming recognized by leading tech companies in the infosec and tech industries
- Facebook, Google, PaloAlto, FireEye, TrendMicro, Riscure hold annual CTF events
- Many more tech and financials are sponsoring big name CTFs
- Hiring managers put CTFers on the top of the interview pile in info sec job opportunities
  - And if they don't yet…
- The biggest win is learning
  - New techniques, new skills
  - "Learning to attack helps you better defend"

PROBLEM TYPES

What can you expect to see CTFing?

PROBLEM CATEGORIES

- These are the “Jeopardy” categories we talked about – these are the “staples” that you see in most CTFs
  - Pwn (Exploitation)
  - Reverse Engineering
  - Digital Forensics
  - Web
  - Cryptography
  - Professional Programming Challenges
  - Misc / Trivia



PWNABLES

- Pwning is “owning” or exploiting some software or hardware to gain some access. Like RCE or information disclosure
- Generally you will be delivered a binary file and a hostname and port combination for a service running somewhere
- The idea is to:
  - Reverse engineer the binary until you find a vulnerability

    - OR -
  - Fuzz test until you find a vulnerability
  - Develop an exploit, usually that works locally
  - Attack the remote target with your exploit
- Occasionally the binary is not given to you (you might need to “leak” it)
- Occasionally a “libc” will also come along with the binary

REVERSE ENGINEERING

- Reverse engineering is the process of analyzing compiled or otherwise complex or obfuscated computer code in order to uncover its function
- In the context of a CTF we're usually reversing some algorithm or set of steps a program takes to validate that some input is what it is expecting
- Generally the ONLY input that validates successfully in that program is the flag
- So we need to "reverse engineer" how the validation takes place so we can deduce the correct input
- Many parallels can be drawn between software copy protection cracking and this type of RE
- Common sub categories of RE are "CrackMe", "ReverseMe" and "ExploitMe"

WEB CHALLENGES

- Finding and exploiting vulnerabilities in web applications
- Everything from common or obscure misconfigurations, to fiendish logic / evaluation vulnerabilities
- Some sub-types of this category:
  - Server side language attacks (PHP, templating languages)
  - Directory traversal
  - File inclusion attacks (Local/Remote)
  - Cookie tampering
  - Combination web / crypto challenges (e.g. encrypted cookies)

CRYPTOGRAPHY CHALLENGES

- Challenges involving cryptanalysis of known or bespoke cryptosystems
- Generally with the goal of decrypting a given ciphertext or gaining access to some system by forging a cryptographic token
- Some of the sub categories of crypto:
  - Classical ciphers
  - Symmetric key attacks
  - Asymmetric crypto implementation flaws
  - Eliptic curve
  - Padding oracles / LSB oracles
  - Hash extensions

PROFESSIONAL PROGRAMMING CHALLENGE

- PPC for short, these challenges test competitors ability to design algorithms to solve problems quickly and accurately
- Generally ask many questions of the same category with short timeouts so only building computer recognition and solving algorithms can get the flag
- Types of PPC:
  - Math equation solving
  - Maze / Snake / Dalek ASCII art games
  - QR Codes / Bar codes
  - Computer vision challenges

MISC / TRIVIA / RECON

- General questions or challenges that don’t fit into the other information security categories
- Generally not directly computer science problems but are tangentially related.
  - Hacker movie trivia
- Generally just Googling hard enough is the answer
- Looking back in time (archive.org)
- Example:
  - Find Eric Liang (CSAW 2015)…

DID YOU CATCH THE OTHER FLAG

- We’ve seen two flags so far in the slides.
- Make sure you cap both of them on the site.

CTF PRE-REQS

YOUR SKILLS

- Anyone can get into CTFing as long as you possess at least some level of these skills
  - Curiosity
  - General problem solving ability
  - Willingness to take responsibility for teaching yourself a new skill
    - i.e. wanting to learn
- It is advantageous to know:
  - Basic programming in Python and a knowledge of C
  - Linux stuff
  - Memes

YOUR HACKBOX – THE HARDWARE

- CTFing is possible on a shoe-string hardware budget. A Surface or an older Macbook works
- You can always benefit from more CPU and GPU especially for challenges involving offline brute force attacks against hashes / passwords
- The more RAM you can scrape together the better, especially if you prefer to deploy multiple VMs (or anything like the Android SDK)

YOUR HACKBOX – THE OS

- You'll need a platform upon which you're comfortable enough to get results quickly
- Linux is the most versatile CTF attack platform as most CTF tools are developed targeting Linux
  - Distro's like Kali, BlackArch, Santoku, Parrot, DEFT, Pentoo, SIFT and others come bundled with loads of tools
- MacOSX is a close seconds as most tools compile or run with minimal changes natively
- Windows is certainly possible as a preferred attack platform. Windows 10 even has bash built in now…
- Tactical use of virtual machines can overcome any shortcomings in your main operating system

HOW TO CTF

effective internet points capturing methods

APPROACHING PROBLEMS

- A great deal of CTFing can be boiled down to “How do you approach problems”
- A well practiced problem solving approach can streamline finding a solution
- So just like with many problem types in technology, over time a process emerges
- In CTFing, we can treat each challenge, irrespective of type / category as the input to this process
- We call this the “challenge pipeline”

CHALLENGE PIPELINE

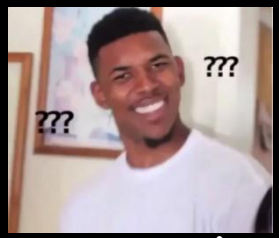
- Consists of a few simple steps, that you execute in approximate order, for every challenge
  - Get motivated to attempt something
  - Clues / Challenge text / read between the lines
  - Quick Analysis steps – Spend 2 – 3 minutes only
    - Files, download them, what are they?
    - Executables, run them (inside a VM please), observe their behavior, send inputs that quickly test edge cases
    - Network services, connect to them, observe
    - Web challenges, visit the links
- Let's run through a few of these points more, and a then few example uses of a pipeline

GET MOTIVATED TO TRY...

- Sounds obvious but its hard
  - “I’m no good with crypto”
  - “I’m only good enough to do the easy ones”
  - “This is too hard for me…”
- It’s easy to talk yourself out of trying a challenge
- You get over this by exposure and succeeding occasionally
- Sometimes it’s luck, sometimes you land on something you find intuitive and discover a new skill
- Check this example…

VOLGA CTF 2015 - CARRY

- Five hundred points in the Crypto category
- Bespoke crypto function with an 8 byte key, too large for brute force ?
- Algorithm essentially unknown but we begin analysis…
- We notice a “def sanity_check():” function
- Inside sanity_check() is “key = ‘324dfwer’”



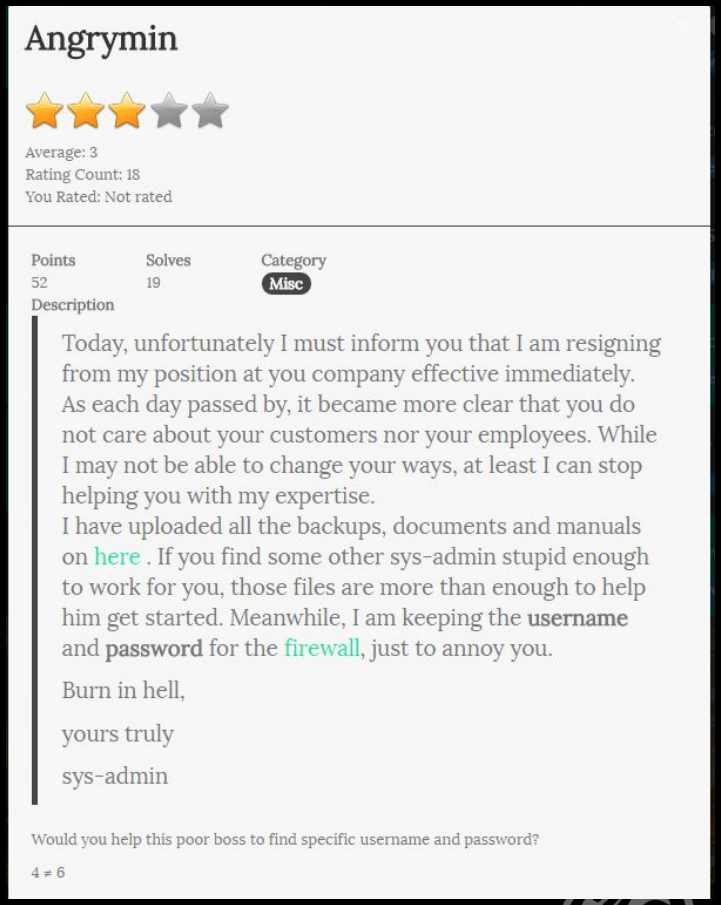
- It’s the key, problem solved within 5 minutes for 500 points
- Only 30 or so of the HUNDREDS of playing teams solved this challenge
- Get motivated to try!!!

HOW TO READ A CLUE

- Clues are any artifact that contributes to a challenges description or execution
  - Includes the challenge text from the CTF page
  - Includes any files you download
  - Includes any network connection banners / websites you connect to.
- Some are obvious and explanatory
  - In these cases generally the techniques are well known but hard to execute correctly
    - PPC challenges are usually this
- Some are oblique and purposefully vague
  - Be extremely careful of reading such clues

ASIS CTF - 2016

- The clue is a resignation letter
- A link to the firewall references “juniper.asis-ctf.ir” which doesn’t seem to respond to connections on the internet
- We need to find the username and password
- In tiny text: 4 ≠ 6
- To solve we need 3 parts from the clue:
  - “juniper”
  - 4 ≠ 6
  - The download



QUICK ANALYSIS STEPS – ALL FILES

- Download each and every file
- Decompress them to a new folder named for the challenge it relates to
- Filenames? Anything stand out?
- Use “file” command to identify the file types
  - If there are images, use “exiftool” “checkpng”, “stegdetect” & “Stegosolve.jar”
- Use “binwalk” to identify embedded files
- Use “strings”, grep for the “flag format” this works more often than you’d think
- Depending on the outcome of the above, branch here into other parts of your pipeline

EXECUTABLES

- Extract or download each executable into a new folder named for the challenge
- From the output of “file” in the previous steps you determined the binary architecture and format
- If possible execute the binary to find out what the most obvious inputs and outputs are
- Is a libc provided?
- Does it identify as a .NET binary?
- Is there a menu with “Delete item?”
- Is it echoing your input? Try %x
- Try long strings
- Any crashes?

WEB CHALLENGES

- Visit the URL via an intercepting proxy (Burp)
- Check the response packet for:
  - Cookies
  - Forms
  - Comments in the source
- Check for the existence of:
  - Directory indexes
  - robots.txt
  - .git, .svn folders (even if they return 403)

WRITE-UPS

- After you solve a CTF challenge you have never encountered before, write about it.
- Writing about it serves as a great source of reference material for yourself if you ever encounter a similar problem
- Writing helps cement the concepts you learned in your mind so you recall them more easily.
- Writing is a great creative outlet
- Writing gets seen by potential future employers…

HOW TO START PRACTICING

resources and ideas

START A TEAM

- Either go solo or get together with a group of friends
- Think of a cool name
- Sign up “CTFTime.org”
- Start playing CTFs to train your skills
- Begin training montage

ALWAYS ON CTFS

- CTFs like the ones we've discussed so far are generally run by different organizations annually
- In general there's one, maybe two of those CTFs a week
- Always on CTFs are a way to learn CTF skills by completing challenges without a time pressure
- You still get flags, still get internet points, but you don't have to ruin your sleep schedule or forsake your loved ones to participate
- Check them out:
  - Ringzer0team.com
  - backdoor.sdslabs.co
  - wechall.net
  - pwnable.kr
  - ctfs.me
  - SANS Holiday Hack Challenge archive

HOMEWORK

get your feet wet this week

HOMEWORK

- Signup to Op CySCA Success Mellivora at: https://cysca.ctf.rip
- Check the “Homework Challenges” category and complete all available challenges there.
  - They are all super easy but it will lead you to some external sites you might find interesting

RESOURCES

- CTFTime – Global CTF leaderboard / calendar / writeups
- WeChall / ringzer0team.com / Backdoor SDSLabs – Always on CTFs
- What is a CTF? Youtube / LiveOverflow – This guys entire channel is a great resource
- ctf.rip – @ctfkris' writeups
- advancedpersistentjest.com - @lin_s' writeups
- Github writeups repo – contributed by many teams and individuals globally

THANKS FOR LISTENING TO US RANT!

questions? @ctfkris / @lin_s