OWASP

Open Web Application Security Project

LEARN AND PRACTICE INFOSEC WITH CTF

by Okai Yeboah

OUTLINE

- ❑ InfoSec and CTF intro
- ❑ Styles of CTF
- ❑ Tools and resources for CTF
- ❑ OWASP CTF
- ❑ Getting the best out of CTF
- ❑ Benefits of CTF

Images taken from the almighty internet

INFOSEC

- Information Security
- Preventing, detecting and responding to information or system threats.
- InfoSec Certification [that's not why I am here]

CTF [HISTORY]

- Traditional outdoor game
- Two teams each have a flag
- Objective is to capture the other teams flag

CTF (THE REAL DEAL)

- CTF == Capture The Flag
- InfoSec competition
- Wargame for Hackers
- Hackers are enthusiast software or hardware hobbyist

CTF (THE REAL DEAL)

- Allows you to hack safely
- Challenges – basic to super hard
- Skill level varies between CTF events
- Earn points for completing a challenge

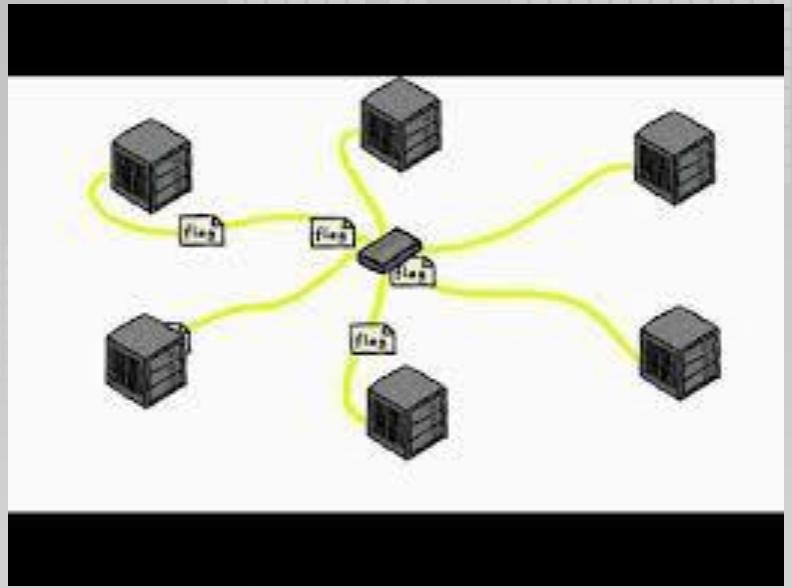
CTF [MYTHS]

- Nerds play CTF
- CTF are for the bad guys
- CTF can not be applied in real life
- CTF == video games // partly false

CTF STYLES

- Attack-Defense
- Jeopardy

CTF STYLES (ATTACK- DEFENSE)



CTF STYLES (ATTACK- DEFENSE)

- Concept like the traditional outdoor game but multiple teams
- Each team is given a machine or network
- Defend the machine or network
- Attack others machine or network

CTF STYLES (ATTACK- DEFENSE)

Teams are scored on:

- Defending the machine from other teams to plant or take their flag
- Attack others machine or network for the flag
- DEFCON usually host it annually

CTF STYLES (JEOPARDY)

- Challenges are divided into categories
- Consist of different points per difficulties
- Don’t attack each other’s machine
- A lot of such competition out there

CTF STYLES (JEOPARDY)

Challenges include:

- Cryptography
- Reverse engineering
- Binary Exploitation
- Web exploitation
- Steganography
- Pwn
- Forensics

Getting Prepared (Tools)

- Fuzzing - afl
- Binary debugger and disassemblers – IDA, GDB, binary ninja, pwndbg
- Analyzing files - binwalk
- Steganography - zsteg
- More on Github – ctftools

Getting Prepared [Resources]

- CTF events tracker
  - http://captf.com/calendar
  - http://ctftime.org/ctfs/
  - http://ctf.forgottensec.com/wiki
- Github repos for learning
  - trailofbits
  - ctfs

Getting Prepared [Resources]

- Archived resources to practice
  - http://ctflearn.com/
  - http://overthewire.org/
  - picoCTF
  - https://owasp.org/
  - http:// captf.com/practice-ctf
  - vulnhub

Getting Prepared [Resources]

- Videos [YouTube channels]
  - OWASP
  - John Hammond
  - Hacker Joe
  - LiveOverflow
  - ShmooCon

OWASP CTF

- Designed during OWASP conferences
- Mostly Web based CTF, Networking and Forensic
- OWASP top 10 web vulnerabilities
- Prices are awarded
- Not Open Sourced Project

https://owasp.org/www-project-ctf/migrated_content.html

OWASP CTF

- CTF based OWASP Projects
  - OWASP Juice Shop
  - OWASP WebGoat
- Open Sourced Project

https://owasp.org/projects/#div-flagships

Getting the best out of CTF

- Take notes when playing CTF
- Research more on what you understand
- Compare write ups to notes taken after the CTF event
- Read more write ups
- Practice more on where you are weak

Benefits of playing CTF

- Job
- Credentials
- Skills
- Meet others and have fun
- Swag and incentives

Maxims of Effective CTF

- We hack for fun, not for frustration
- The scoring mechanism should always be the easiest challenge
- Solutions might be a surprise, but recognizing when you have one shouldn't be
- When the next step requires a leap of faith, be sure to include a bridge
- An homage honors, but duplication doesn't

http://captf.com/maxims.html

Maxims of Effective CTF

- Learners always win even when winners don't learn
- Your point estimates are exactly that until calibrated
- Never rely on the survival of a vulnerable server
- Competitors are more clever than you, they also have more time
- Learning starts where prior knowledge ends

http://captf.com/maxims.html

QUESTIONS

“don’t try to boil the whole ocean”

ECHO ME

Okai Yeboah

[@king_kloy]

Enjoys playing CTF

Loves code

https://twitter.com/king_kloy

THANK YOU

“don’t forget during CTF, Google is your friend, friend”