Introduction to Offensive Security

CS-UY 3943-G / CS-GY 9223-H

Agenda for today

- What is this course?
- What is CTF?
- Syllabus overview
- Environment Setup
- Start the first unit (Web)

What is this course?

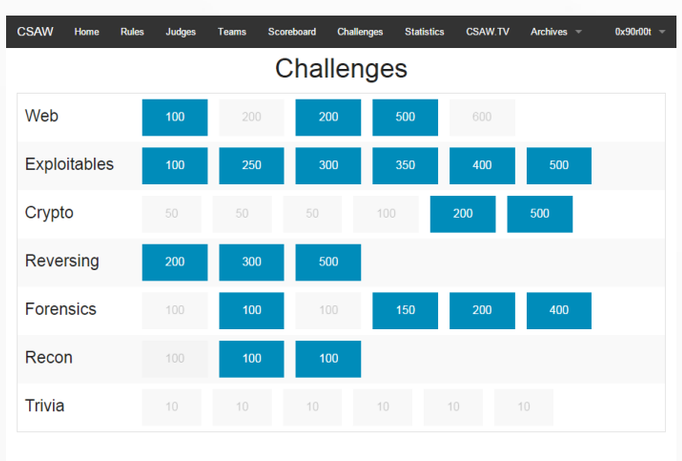
- This course aims to teach offensive security in the context of Capture-the-Flag (CTF) competitions.
- We are:
  - Brendan Dolan-Gavitt
  - John Cunniff
- Course originally developed by
  - Nick Gregory
  - Josh Hofing

What is CTF?

- Learn security topics (mostly offensive) in a controlled, competitive environment
  - Guide people to discovering tricks
- Many categories of problems:
  - Web, Reversing, Pwning, Crypto, PPC, Forensics, etc.
- A large community of Security people trying to prove their skills

CTF Formats

- Jeopardy
  - A board of challenges divided into categories and point values
  - Get a flag to complete a challenge, move on to the next one



- Attack/Defense
  - Each team has a server with vulnerable services
  - Find bugs, Patch them, Exploit everyone else

CTF Culture Stuff

- Generally, CTFs have IRC channels where you can ask questions from the admins
- Problems that run on a remote service will frequently tell you where the service is hosted like:
  - `nc some.server.address port`
- You'll see some magic numbers all over:
  - 1337
  - 0xdeadbeef
    - and basically anything else you can spell with hex

What we'll be covering

- Web
- RE
- Pwning
- Crypto

What we expect you to know

- Basic Javascript
- C/C++
- Python
- Basics of x86 (we will give a crash course)
- Be quick at picking things up

Web Problems

- Finding and exploiting bugs in websites
- Sometimes, you get source, sometimes you don't
- Frequently PHP or Python servers
- Usual vuln types:
  - XSS
  - SQLi
  - Command Injection
  - (Basically anything in the OWASP top 10)

Reversing (RE) Problems

- Understanding code, systems
- Usually compiled binaries
- Typical problem types:
  - Crackmes
  - Bytecode Interpreters
  - “Supercomputer” problems (Figure out the algo, rewrite it faster)
  - Weird languages
  - Weird architectures
  - Weird machines

Pwning (Binary Exploitation) Problems

- Exploit a vulnerable service
- Usual goal is to read a file called “flag” or “flag.txt”
  - Normally by getting a shell
- Typical problem types:
  - Stack-based buffer overflow
  - Heap-based buffer overflow
  - Write-What-Where
  - Heap corruption
  - Shellcoding
  - Basically any other kind of memory corruption you could think of

Crypto Problems

- Decrypt a message
- Given encrypted message(s) (and usually what was used to create them), decrypt them by exploiting an issue in the cryptography
- Typically
  - Attacks against RSA
  - Logic flaws
  - Giving bad parameters to (otherwise-secure) algorithms
  - Crazy math stuff

Programming Problems

- Everyone likes implementing algorithms, right?
- These are normally warmup problems
  - Your homework this week has a programming problem
- Typically implementing algorithms or such
- Some examples:
  - Provide a string that matches this regex
  - Solve some math problems
  - Basically anything you can imagine scripting

Forensics Problems

- Given device/memory image, find something in it
- File forensics – we've hidden stuff in some weird part of a file format, go find it!
- We won't really be covering this in detail, and it tends to be quite varied.

What does CTF not teach?

- There are skills that playing in CTFs will *not* teach you:
  - How to find vulnerable code in a large application
  - Post-exploitation: what do you do once you're inside?
  - Communication: how do you report your findings responsibly and comprehensibly?
- Also, outside of attack/defend classes, usually will not teach you much about *defense*
  - Secure coding practices
  - System administration / configuration

Homework

- We will be running a CTF throughout the course
  - https://class.osiris.cyber.nyu.edu
  - Go there and login now, let us know if something doesn't work
- Homework will be a set of "hot" CTF problems each week
  - Homework is Pass/Fail each week
  - Pass = at least 300 CTF points
  - You will have one week for each homework set
    - We will tally the scores for a set at the beginning of class each week
  - Problems stay up after, but you will not receive credit after they are due

CTF Participation

- In addition to the class CTF, you will be required to participate in at least one other CTF
  - The CTF must be ranked on ctftime.org
- You must submit a writeup for at least one non-trivial problem that you solved during the CTF.
- You may form teams – but we expect more hands make better writeups
- Your writeup should be more than just a script
  - You should explain the problem you solved well enough that someone who didn't look at it would fully understand how it worked
- You ***must*** submit a writeup to pass this class

Grading

- 90% Homework
- 10% CTF Participation + Writeup
  - But this is required to pass the class
  - Please don’t put it off to the end

Materials

- You'll need a reverse-engineering toolkit during the RE and Pwning sections of the class
  - We recommend Binary Ninja, which is friendly and is cheap
  - You can also use some free tooling, but it's a lot less user-friendly
    - objdump
    - Radare2
- We're also providing a VM with a bunch of handy tools pre-installed
  - See https://class.osiris.cyber.nyu.edu/vm for installation instructions

Office Hours

- BDG's office hours: 1pm-3pm Fridays, 2 Metrotech 10.081A
- John Cunniff's office hours
  - Tuesdays & Thursdays RH 219, 11:30am-3:30pm
  - Fridays RH 219 from 12:00pm-6:00pm
- We are also available via e-mail!

Office Hours

- We're in the OSIRIS lab (RH 219)
  - Office hours will be there
    - Tuesdays & Thursdays: 11:30am – 3:30pm
    - Fridays: 12:00pm - 6:00pm
  - If our availability decreases, we'll send an email.
  - If that timing is bad for you, let us know, and we'll work out another time we can be available that works for you.

Collaboration Policy

- While CTF is a team sport, we believe that all members of a team should be able to solve problems
  - Therefore, collaboration on homework assignments is not permitted
    - Feel free to share answers and techniques *after* the homework is due
- If we catch you cheating, we will report you to academic affairs.
  - If you need to ask if it's cheating, it probably is.
- If you have questions about homeworks, show up to office hours, or send an email

Schedule

- Schedule for the course:
  - Weeks 2-4: Web
  - Weeks 5-8: Reversing
  - Weeks 9-11: Pwning
  - Weeks 12-13: Crypto
  - Week 14: Side Channels
- Details for what we plan to cover in each section on the Syllabus

Questions?

What to do now

- Log into the website
  - https://class.osiris.cyber.nyu.edu
- Solve the “Are you alive” problem
  - It’s very, very easy :)
- Let us know if there are any issues

Homework for this week

- There will be 2 challenges put up at the end of class today
  - One Warmup, one Programming
- Due at the beginning of class next week
  - These should be a pretty basic warmup for everyone