Capture The Flag 101

By a bunch of random people

Why are we doing this talk?

While some of you have played in CTFs before, not all of you have.

We’ll also be hosting a CTF at UMBC during the spring semester! More details to come after we actually plan it.

We need y’all to be good, because we’re going to invite UMD and we don’t want them to get first place.

WTF IS CTF?!?!?!?!

Capture The Flag competitions are information security competitions that test a wide variety of skills, usually with a time limit.

They usually attempt to be somewhat realistic, but sometimes realism is thrown out for the sake of fun.

CTFs are usually held online, and sometimes in person (ex. Kaizen, CTF’s at conferences, NetWars)

Types of CTFs

- Jeopardy
  - Most common
  - CSAW, DEFCON qualifiers, PicoCTF, etc
- Attack and defend
  - Hardest, typically need to qualify for these
  - Almost always in person CTFs (some exceptions)
  - DEFCON CTF Finals, Point3 A3 CTF, iCTF (online!)
- King of the Hill
  - Fun, but often has technical issues
  - Old MDC3 format
- Hack quest
  - New hipster jeopardy with levels
  - Has a story attached usually
  - NetWars etc

Jeopardy

Jeopardy style CTFs are usually composed of a bunch of mostly unrelated challenges, each worth a different amount of points. Whichever team has the most points when the time is up wins!

Usually the challenges are unrelated and there is no theme, occasionally there will be 2 or 3 stage challenges that each have their own flag.

Points are generally in the 100-500 point range (with 50 point increments), sometimes really easy challenges are 50 points, or even 1 point (‘sanity check’)

Attack and Defend

The hardest of all CTF competitions. This is DEFCON CTF, iCTF, etc.

Each team gets an identical network with challenges running on them, and attack the other teams.

They need to patch their own services while simultaneously creating exploits for them.

Usually all of the challenges are binary exploitation (occasionally crypto or reverse engineering).

Often need to qualify for these competitions, and they are usually in person events.

King of the Hill

An underused format, in this game type all the teams attack one network of vulnerable hosts.

Every five minutes (or so) each host is checked and whichever team ‘owns’ it gets points.

None of the hosts are terribly hard to get into (challenges are easy), the difficulty in these competitions is keeping control of what you already have.

MDC3 used to be run this way, Panoply (side event at CCDC) is this.

Hack quest

An offshoot of jeopardy CTFs, Hack quest’s usually have some sort of progression and story behind them.

While these can be very thematic and fun, the challenges are often cookie cutter and not difficult. (this is so less skilled teams don’t get stuck).

This is what NetWars is, and some Kaizen scenarios. Most paid training CTFs are set up this way.

Categories

- Crypto
- Forensics
- Web Exploitation
- Recon
- Reverse Engineering
- Binary Exploitation (also called pwn)
- Miscellaneous

Cryptography

Crypto problems can be really easy or really hard, depending on how many points the problem is worth.

An easy problem might be decoding base64, a harder problem might be doing a padding oracle attack on AES.

Forensics

These are an absolute crapshoot

Example challenges

- They give you a network capture in the form of a pcap. You have to extract a file from there. You then have to find the magic nonstandard separators, and split it into three files. You then figure out what each file is and decode it.
- You have to run volatility on a memory dump
- You have to figure out a puzzle to find a password, then use steghide to retrieve the flag

Web Exploitation

These are about what they sound like. They give you a URL to a web application, you have to exploit it. Usually the goal is to log in as admin, then it gives you the flag

Common things you might have to do

- Take advantage of client-side validation
- SQL injection
- Command injection
- Exploit some random framework vulnerability that you Google

Recon

These can vary depending on what people mean by ‘recon’

- A simple recon challenge may involve combining aspects of simple crypto and puzzles in order to gather information on a person or company
- More robust examples involve using scanning tools in order to launch an attack
    - Some of these challenges may also give you information that’s crucial to another problem later on

Some tasks you may need to perform:

- Scan a website/ip to find available attack vectors
- Perform whois/whereis lookups on a person/company of interest
- Solve puzzles (possibly crypto related)

Could very well cascade into other categories! Depends on how far they want you to go...

Reverse Engineering

These challenges involve downloading a (usually standalone) binary, for some platform and finding a flag within it.

There is a lot of variety in RE challenges, you will run into everything from standard Linux x64 userland binaries to PowerPC boot loaders.

Many RE challenges are Crypto challenges with a layer of RE! Some crypto knowledge is a must for this category.

Most pwn challenges involve some reverse engineering as well.

Binary Exploitation/pwn/pwnables

This is typically the hardest category. Top level CTFs (such as DEFCON) typically only have challenges in this category and reverse engineering (and sometimes crypto).

Usually you are given some executable, which you must reverse engineer and find a bug in. Then, you need to write an exploit for that bug which will give you a shell on the target where you can read the flag.

Typically the bugs are memory corruption bugs. Simple challenges may be stack based buffer overflows, harder challenges may involve advanced techniques such as heap overflows, type confusion, and chaining multiple bugs together.