MW MS CTF

Nick Marcuzzo & Nico Mariniello

White Hat vs. Black Hat

- White Hat
  - Paid to test systems
  - Experimenting on own servers
- Black Hat
  - Stealing & Breaking
  - Malicious actions
  - ILLEGAL

Who are we?
Why are we doing this?

- Seniors at Millard West
- Computer Science and Robotics
- Independent Study
- Starting Computer Science earlier

What is a CTF?

- Capture the Flag
- Hidden Keys (flags)
- Large range of problems
- Long time
- Stresses self teaching and problem solving

Why CS is important

- Growing need
  - Increasing use of Tech
  - How often tech is used in daily life
- Wide range of employment opportunities

Stats about CS

- 1.4 mil CS jobs by 2020 with only 400,000 CS grads
- AP Comp Sci has one of the lowest enrollment rates of all AP classes (5%)
- Computing occupations are among the highest-paying jobs for new graduates

And now… the stuff you actually care about

What are you going to learn?

- General knowledge that will help in solving problems
- This presentation will be available to download
- We will not show you how to do problems
- Some topics that you need to know will not be covered
- Some concepts will covered, but not explained (thats your job)

Types of data

- Binary
  - 1s and 0s only
  - Ex: 110110 is 54
- Hex
  - 0-9 and A-F
  - Ex: 3E is 62
- ASCII
  - 0-127
  - Ex: 107 is k

- How true and false can be shown (booleans)
    - TRUE vs FALSE
    - T vs F
    - 1 vs 0
    - Y vs N
    - On vs Off

Common CS Stuff

- Epoch
  - Measure of time
  - Seconds since midnight on Jan. 1, 1970 (yup, its a big number)
- EXIF Data
- Binary Merge Archive
- Capturing packet transfers (PCAP files)

Encryption

- Types
  - Caesar
  - Substitution
    - Regular or Keyed
  - Pad
- Encryptions can be stacked on each other

Online resources

- http://rumkin.com/tools/cipher/
- http://google.com
- http://www.kaagaard.dk/service/convert.htm
- http://www.simonsingh.net/The_Black_Chamber/substitutioncrackingtool.html

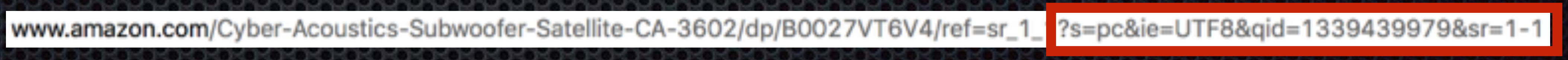
How to google

- Only important words in query
- Don't ask Google questions
- Example:
  - WRONG: “how many petals are on a tulip?”
  - RIGHT: “number of petals on tulip”

How to break web sites

- Google Chrome is your new best friend
- Inspecting element (right click -> inspect element)
- Editing source code
- Cookies
  - Information that your computer gives a web server when you load a page
  - Found on Resources tab on inspect element

- Two types of web requests
  - POST
    - Works in background
    - Very hard to read or modify
  - GET
    - Shown in URL
    - Easy to see and modify
    - What is after the “?” in URLs



www.amazon.com/Cyber-Acoustics-Subwoofer-Satellite-CA-3602/dp/B0027VT6V4/ref=sr_1_?s=pc&ie=UTF8&qid=1339439979&sr=1-1

On to the hard stuff…

How does a computer store info?

- Layers:
  - Binary
  - Hex
  - ASCII or raw data

What is a file?

- Three main parts:
  - Header (tells what type of file it is)
  - Data (can be anything, depends on file type)
  - Footer (tells that file is over)
- Any file can be opened in Notepad, can reveal important info

How can files be broken?

- Bad/missing header or footer (google what the header of a file should look like)
- Corrupted/missing data (very hard to fix)

Closing tips

- Many problems will try to lead you in the wrong direction
- If you get stuck on a problem:
  - Get a teammate and explain in detail everything you know about the problem
  - or, move on and come back to the problem later
- Google google google, google google; GOOGLE!!!!