Introduction to CTFs

Week 6

Slides by @kathyra

ETHICS - LET'S *NOT* GET ARRESTED

- The skills you learn doing CTFs are similar in many ways to the skills you need to do real hacking/auditing.
- What you are learning can be used for malicious purposes.
- Neither I, the society, or the university are responsible for your actions.
- Never attempt to illegally gain access to a system you do not own.
- You're all smart people. Use common sense!

SO WHAT *ARE* CTFS?

- Capture The Flag challenges
- A CTF will involve some sort of system (an executable, a web server, etc.) that has a vulnerability written in
- Your job is to figure out what the vulnerability is, and how to exploit it
- A successful exploitation will give you a ‘flag’ - often a text string

BUT HOW DO I *DO* CTFS?

- CTFs will normally hint at what the intended exploit is. Read any text that comes with the challenge carefully (sometimes even just the name of the challenge can give away what the vulnerability is).
- Scope out the system. If you're given an executable with code, you'll want to read the code carefully. If you're doing an easy web CTF, a good place to start with is checking the source code.
- Finding the vulnerability is half the battle. After that, you figure out how to exploit it to gain access to the system.

OK, FINE. *NOW WHAT?*

- The best way to understand how CTFs work is to just do them.
- On the next slides I'll be listing some more or less beginner friendly CTFs with a brief overview of how to approach them.
- They're not arranged in any order of difficulty. Feel free to start with whatever ones look more interesting to you.
- *Collaborate with the people around you!* Sometimes you might miss a really obvious solution, and getting another perspective is incredibly valuable. (also, the more you talk to others, the less work I need to do. thanks.)

OverTheWire - Bandit

- http://overthewire.org/wargames/bandit/
- Absolute beginner challenges - basically teaches you your way around a terminal

OverTheWire - Web Hacking

- http://overthewire.org/wargames/natas/ - web challenges. These are in ascending order of difficulty.
- Writeup is here: https://infamoussyn.com/2014/02/05/overthewire-natas-level-0-16-writeup-updated/ (don't look unless you're SUPER lost)
- If you're using Google Chrome, Postman + Postman Interceptor are useful for web hacking
- In Firefox, the Inspect Element function can get you through most things - but Postman is much more robust
- (if you wouldn't touch Chrome with a 10ft pole, look into Burpsuite)

Installing Postman + Postman Interceptor

- Postman: https://chrome.google.com/webstore/detail/postman/fhbjgbiflinjbdggehcddcbncdddomop?hl=en
- Postman Interceptor: https://chrome.google.com/webstore/detail/postman-interceptor/aicmkgpgakddgnaphhhpliifpcfhicfo?hl=en
- Postman Interceptor has a button in your toolbar - click it and turn Interceptor on
- Open the Postman app (select “I’ll create an account another time”), and near the top right, click the “Postman Interceptor” button to link Interceptor to the Postman app

Using Postman

- Load a page in your browser
- Interceptor will capture your request and keep it from transmitting for now. You can fiddle around with it in Postman before sending it off.
- You'll see your pending requests in the left sidebar of Postman
- Select a request, change what you need to in the "Headers" tab, then click the "Send" button to send the request

Backdoor

- https://backdoor.sdslabs.co/beginner
- Assortment of various challenges