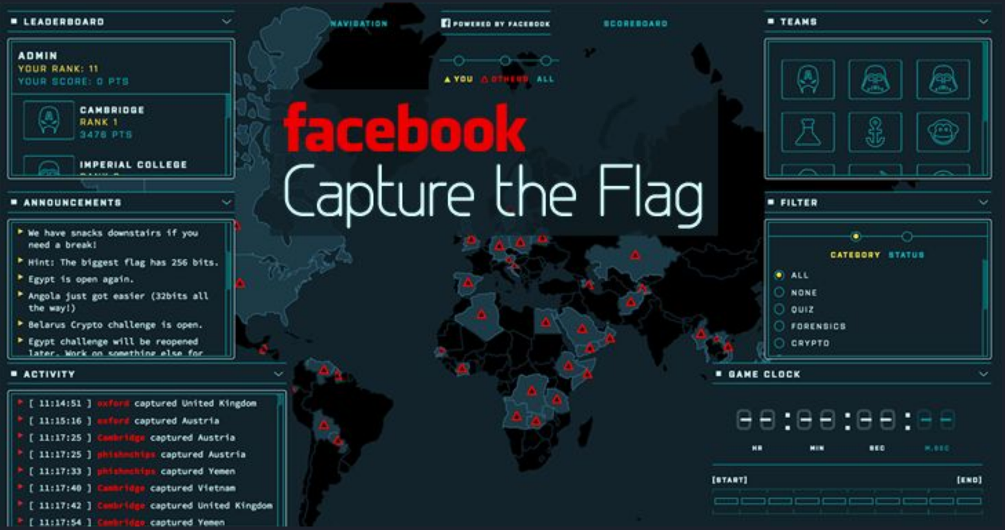
CTF TRACK

An Introduction to CTF

Slides: tinyurl.com/CTFslides1

Introductions

What is CTF?



ADMIN
YOUR RANK: 11
YOUR SCORE: 0 PTS

CAMBRIDGE
RANK 1
3476 PTS

IMPERIAL COLLEGE

● ALL
○ NONE
○ QUIZ
○ FORENSICS
○ CRYPTO

- We have snacks downstairs if you need a break!
- Hint: The biggest flag has 256 bits.
- Egypt is open again.
- Angola just got easier (32bits all the way!)
- Belarus Crypto challenge is open.
- Egypt challenge will be reopened later. Work on something else for

```
[ 11:14:51 ] oxford captured United Kingdom
[ 11:15:16 ] oxford captured Austria
[ 11:17:25 ] Cambridge captured Austria
[ 11:17:25 ] phishnchips captured Austria
[ 11:17:33 ] phishnchips captured Yemen
[ 11:17:40 ] Cambridge captured Vietnam
[ 11:17:42 ] Cambridge captured United Kingdom
[ 11:17:54 ] Cambridge captured Yemen
```

About the Capture the Flag Track

- We're a more informal, chill track that functions more as a study group. We want to consolidate information that would be otherwise difficult to learn.
- We'll be teaching you how to approach CTF problems, which in turn will give you a wide variety of cybersecurity skills.
  - Reverse Engineering: Assembly, GDB: help you learn CS 33 stuff in advance (or help you review it)!
  - Cryptography: Common ciphers and hashing
  - Web Hacking: SQL Injection, XSS scripting,
  - Forensics: Wireshark, tcpdump
  - Linux, Scripting

California CTF

(A first-party advertisement)

BRUINS

NetSec + LUG AT UCLA + ACM Hack + UCLA Residential Life
Capture the Flag
Build a more secure future.

Ucla
BRUINS

NetSec + LUG AT UCLA
+ ACM Hack
+ UCLA Residential Life
C CAPTURE
T THE
F FLAG
GOTTA CAPTURE THEM ALL

Beginner CTFs and Useful Websites

- PicoCTF
- IceCTF
- TU CTF
- overthewire.org
- vulnhub.com
- pentesterlab.com
- ctflearn.com

Wait- what’s a ‘flag’?

The ‘flag’ is basically what we’re looking for!

It’s a phrase often times hidden in a file that we have to find.

It could be a message hidden in a picture, or a hidden phrase in compiled binary.

Types of CTF Questions

Reverse Engineering

Time to understand assembly code!

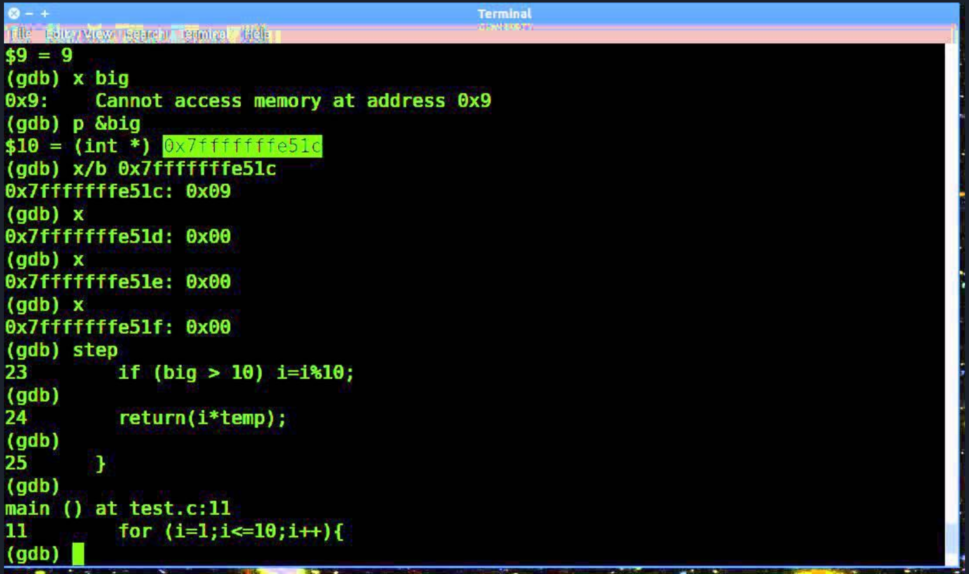
What are you given? An ELF file, an executable, a bin file etc.

Find a hidden phrase in a binary (compiled program) or modify its behavior in unintended ways.

Tools used: GDB, Linux, strings, hexdump, Metasploit framework, objdump, readelf

Useful Knowledge: Registers, Stack frames, Assembly, File types, C, Memory allocation, Overflow, POSIX 2008, Common Optimizations

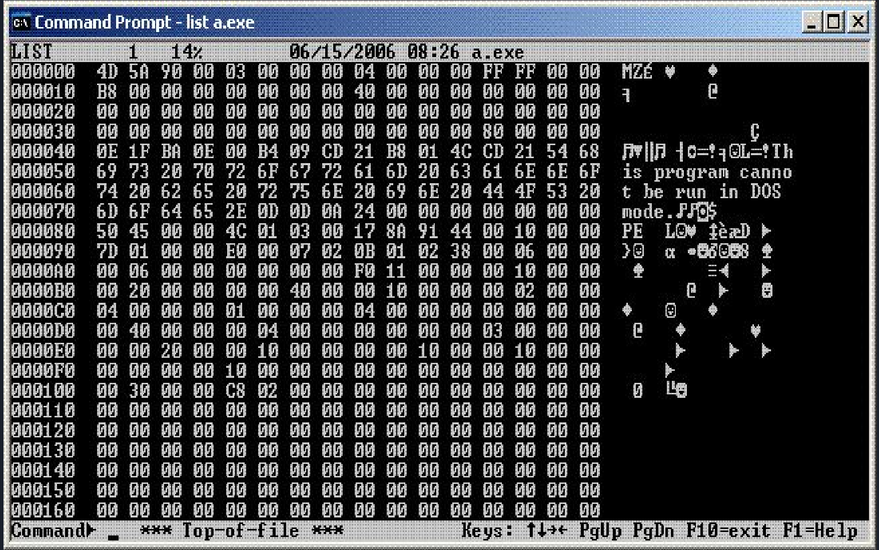
Skills needed: creativity



```
$9 = 9
(gdb) x big
0x9:    Cannot access memory at address 0x9
(gdb) p &big
$10 = (int *) 0x7fffffffe51c
(gdb) x/b 0x7fffffffe51c
0x7fffffffe51c: 0x09
(gdb) x
0x7fffffffe51d: 0x00
(gdb) x
0x7fffffffe51e: 0x00
(gdb) x
0x7fffffffe51f: 0x00
(gdb) step
23          if (big > 10) i=i%10;
(gdb)
24          return(i*temp);
(gdb)
25      }
(gdb)
main () at test.c:11
11          for (i=1;i<=10;i++){
(gdb)
```

GDB: GNU Project Debugger

Hexdump



```
LIST       1   14%          06/15/2006 08:26 a.exe
000000  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZÉ ♥   ♦
000010  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ╕       @
000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000030  00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00              Ç
000040  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  ♫▼║♫ ┤○═!╕☺L═!Th
000050  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F  is program canno
000060  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20  t be run in DOS
000070  6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00  mode.♪♪◙$
000080  50 45 00 00 4C 01 03 00 17 8A 91 44 00 10 00 00  PE  L☺♥ ↨èæD ►
000090  7D 01 00 00 E0 00 07 02 0B 01 02 38 00 06 00 00  }☺  α •☻♂☺☻8 ♠
0000A0  00 06 00 00 00 00 00 00 F0 11 00 00 00 10 00 00   ♠      ≡◄   ►
0000B0  00 20 00 00 00 00 40 00 00 10 00 00 00 02 00 00        @  ►   ☻
0000C0  04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00  ♦   ☺   ♦
0000D0  00 40 00 00 00 04 00 00 00 00 00 00 03 00 00 00   @   ♦      ♥
0000E0  00 00 20 00 00 10 00 00 00 00 10 00 00 10 00 00       ►    ►  ►
0000F0  00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00      ►
000100  00 30 00 00 C8 02 00 00 00 00 00 00 00 00 00 00   0  ╚☻
000110  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000120  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000130  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000140  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000150  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000160  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Command► _  *** Top-of-file ***          Keys: ↑↓→← PgUp PgDn F10=exit F1=Help
```

Web Hacking

Exploiting fake websites online, escalating privileges

What are you given? A link to a website, a PCAP/packet (rarely)

An online challenge where an up-and-running system must be compromised.

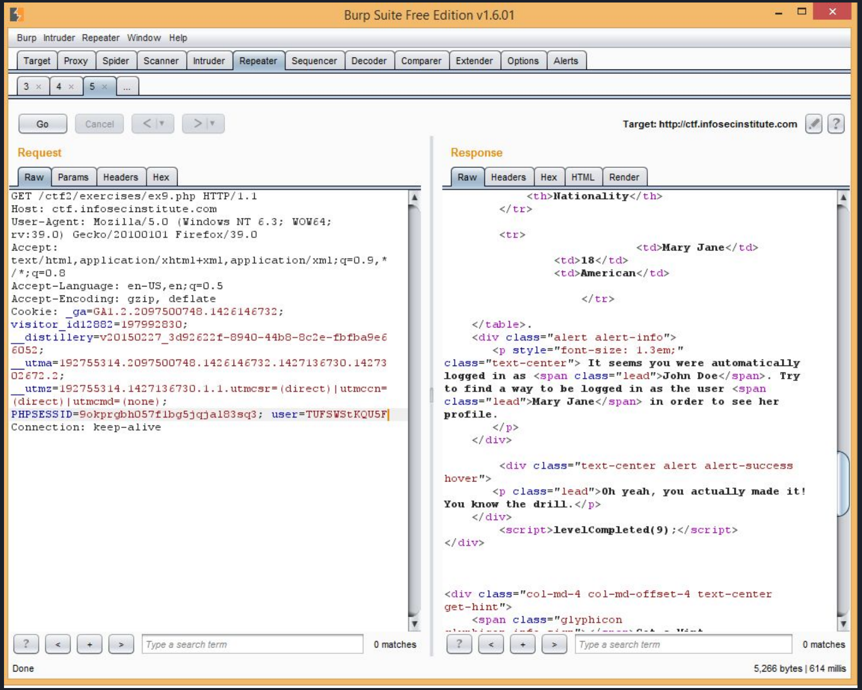
Tools Used: Chrome Dev Tools, Burp Suite, httpie, curl

Useful Knowledge: Cookies, Network Packets, Javascript, HTML/CSS, PHP, SQL, Protocols, curl, netcat

Common web exploits like SQL Injection, XSS (often combined with CSRF)

Skills needed: creativity

Cross Site Scripting (XSS)

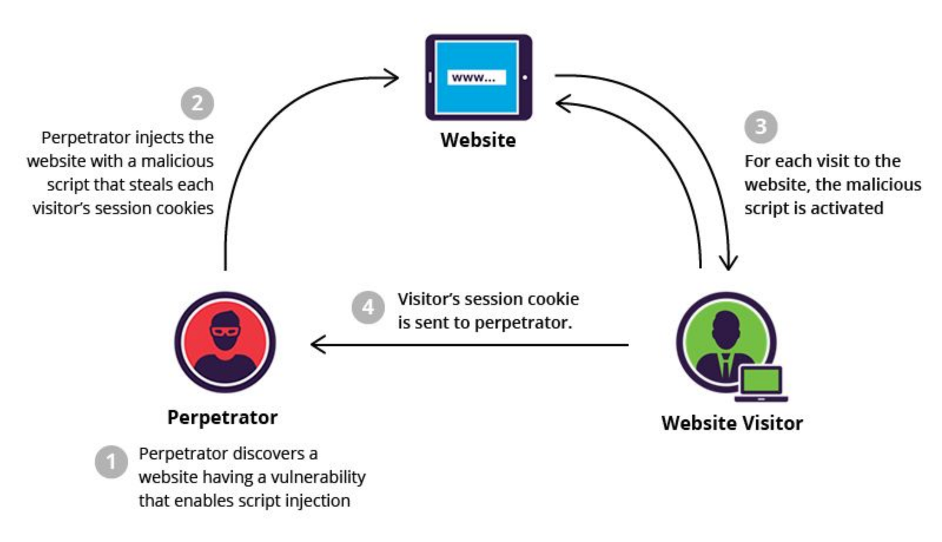


Burp Suite Free Edition v1.6.01
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
3 × 4 × 5 × ...
Go Cancel < >
Target: http://ctf.infosecinstitute.com
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render
? < + > Type a search term 0 matches
? < + > Type a search term 0 matches
Done
5,266 bytes | 614 millis

```
GET /ctf2/exercises/ex9.php HTTP/1.1
Host: ctf.infosecinstitute.com
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64;
rv:39.0) Gecko/20100101 Firefox/39.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*
/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: _ga=GA1.2.2097500748.1426146732;
visitor_id12882=197992830;
__distillery=v20150227_3d92622f-8940-44b8-8c2e-fbfba9e6
6052;
__utma=192755314.2097500748.1426146732.1427136730.14273
02672.2;
__utmz=192755314.1427136730.1.1.utmcsr=(direct)|utmccn=
(direct)|utmcmd=(none);
PHPSESSID=9okprgbh057f1bg5jqja183sq3; user=TUFSWStKQU5F
Connection: keep-alive
```

```
            <th>Nationality</th>
        </tr>

        <tr>
                            <td>Mary Jane</td>
                <td>18</td>
                <td>American</td>

                    </tr>

    </table>.
    <div class="alert alert-info">
        <p style="font-size: 1.3em;"
class="text-center"> It seems you were automatically
logged in as <span class="lead">John Doe</span>. Try
to find a way to be logged in as the user <span
class="lead">Mary Jane</span> in order to see her
profile.
        </p>
    </div>

        <div class="text-center alert alert-success
hover">
        <p class="lead">Oh yeah, you actually made it!
You know the drill.</p>
    </div>
        <script>levelCompleted(9);</script>
</div>



<div class="col-md-4 col-md-offset-4 text-center
get-hint">
    <span class="glyphicon
```

Burp Suite



www...
Website
2
Perpetrator injects the website with a malicious script that steals each visitor's session cookies
3
For each visit to the website, the malicious script is activated
4
Visitor's session cookie is sent to perpetrator.
Perpetrator
Website Visitor
1
Perpetrator discovers a website having a vulnerability that enables script injection

Forensics and Steganography

Recognizing patterns in files, extracting secrets from images

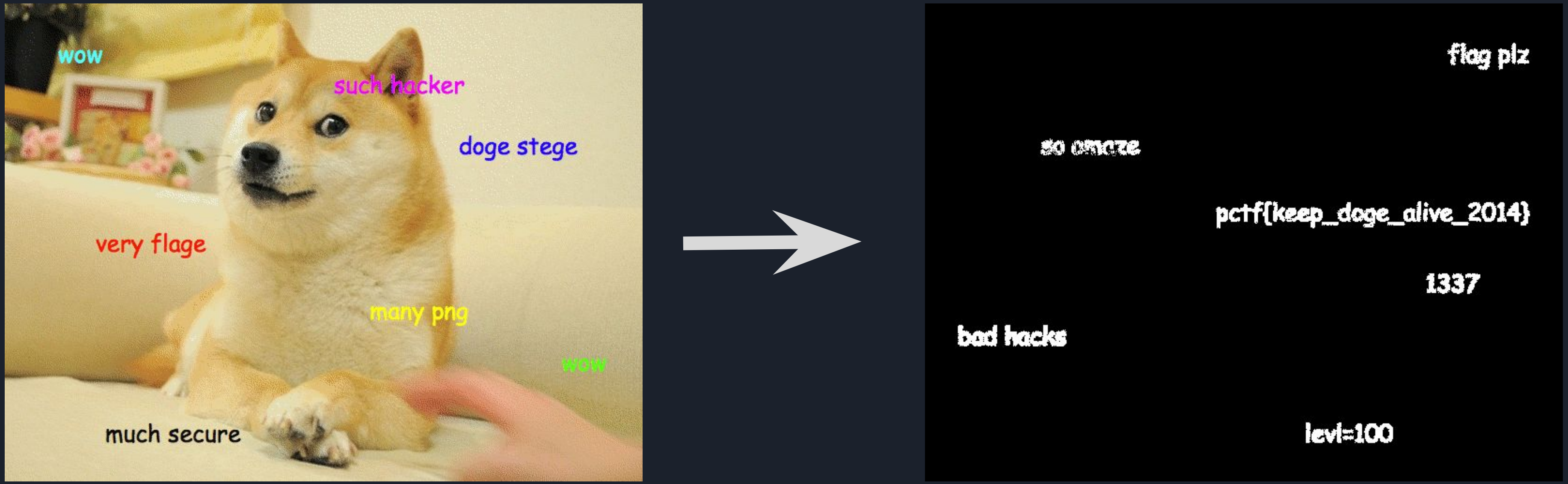
What are you given? Any kind of media file, MS office file, zip/tar, packets, filesystems

Hiding a secret message within an ordinary message (file/audio). Process a hidden piece of information out of static data files.

Tools Used: GIMP/Photoshop, StegSolve, stepic, binwalk, exiftool, Google, Wireshark

Useful Knowledge: Metadata, Scripting, Knowing file formats/encoding, File carving, PCAP analysis, Memory Dumps, Archive files

Skills needed: creativity


wow
such hacker
doge stege
very flage
many png
wow
much secure
flag plz
so amaze
pctf{keep_doge_alive_2014}
1337
bad hacks
levl=100

Cryptography

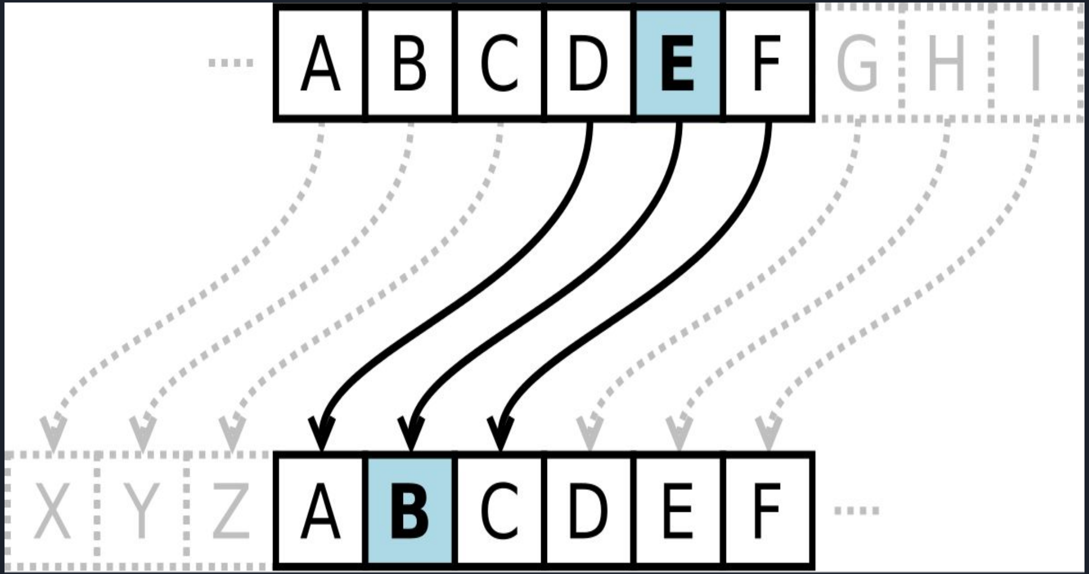
Decoding a message, figuring out which algorithm to use

What do you get? A jumbled text file

A challenge in which you need to decode a file or plaintext

Tools Used: Google, base64, Online decoders, md5sum, shasum, openssl

Useful Knowledge: Names of ciphers and how to identify them, Keys, Basic math, Identifying hash prefixes



Caesar Cipher

RSA

Quizzes

Becoming a trivia buff with the power of Google.

What are you given? Just a question, but try to decipher it carefully for extra clues.

A short question to which you input an answer.

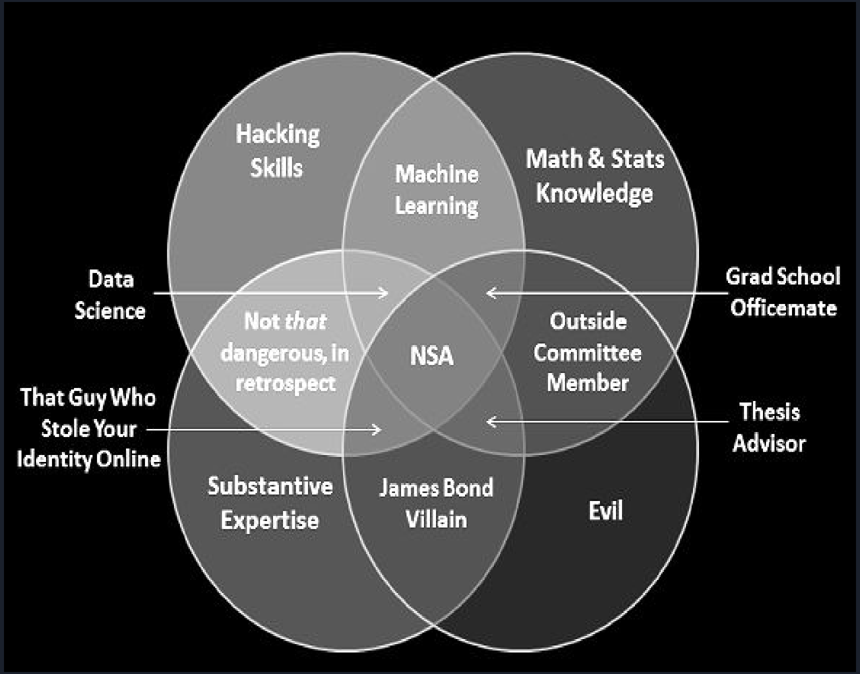
Tools Used: Google, Google, Google, Google, Google, man, Chrome dev tools

Useful Knowledge: Network, Protocols, How to Google stuff, Linux, History

We’ll be going over all of this in our upcoming sessions from the very basics! :)

Time to form groups!

tinyurl.com/ctfproblems1



A meme, as we wait for all the shuffling around.

Upcoming CTFs

- School CTF (Beginner Friendly)
  - Nov 5, Sunday, Week 6
  - https://school-ctf.org/
- RC3 CTF 2017 (Intermediate)
  - Nov 18, Saturday, Week 7
  - https://rc3ctf.rc3.club/
- TU CTF (Beginner friendly)
  - Nov 26, Sunday, Week 9
  - https://tuctf.asciioverflow.com/
- Check out ctftime.org for more CTF dates! Let me know if there's one that catches your eye :)

Walkthroughs/Demos

Let’s work on questions together!

tinyurl.com/CTFproblems1

Thank you for coming!

Feedback form: http://tinyurl.com/ctfsession1