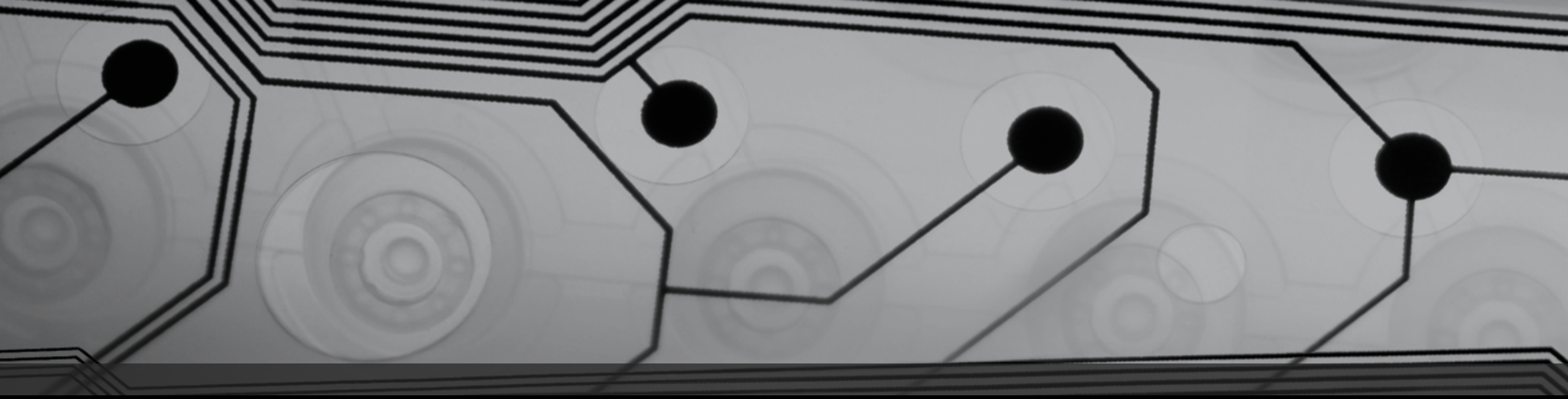


Becoming a Penetration Tester

An attempt to guide you from my mistakes.. By Perla Caston

Introductions …

My name is Perla Caston and I am a Global Security consultant with IBM X-force Red. I have a bachelors degree in Computer Sciences, and an OSCP, CCSE, CCEPE, CSSA, MCTP, CISSP, CCSA.

IBM X-Force Red is an elite, global team that provides security testing services to organizations of all sizes. With over 100 consultants in 26 countries, X-Force Red can easily accommodate any geographic staffing requirement. Services include manual network and application penetration testing, static application analysis, and dynamic vulnerability assessments (automated scans with human validation). Backed by the collective skills of IBM's global organization, X-Force Red can perform expert testing of any technology. Consultants in IBM X-Force Red are widely considered industry leaders, having spoken at high-profile events like RSA, Black Hat, DEF CON, and OWASP conferences

Agenda

- The Path … step by step
- Skills … you will need
- Certifications ... Which ones matter? And why
- Practice makes it perfect…. Where to do it legally?
- Women in Penetration Testing
- Be Humble… and don’t give up!

What is Path to become an Ethical Hacker?

This answer will vary based on who you ask. Penetration Testers come from different backgrounds: Developers, Programmers, Network, System & Security Administrators, Hobbyists, etc..

Algorithm of Success

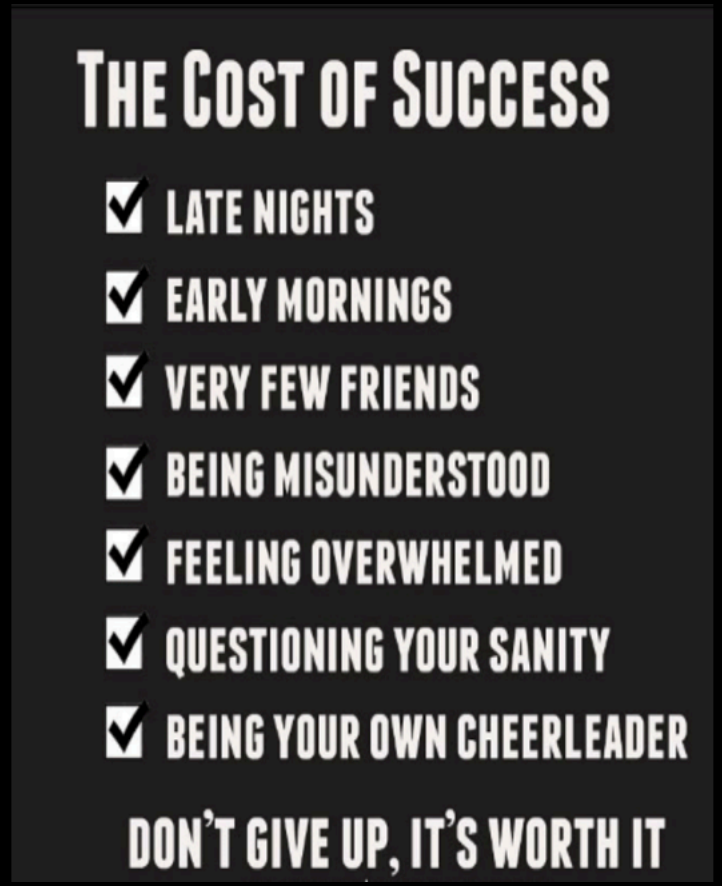
```
while(noSuccess)
{
        tryAgain();

        if(Dead)
                break;
}
```

The main thing we will all agree on is that you need a passion for solving puzzles and the ability to sit for hours working on the same problem until you finally crack it. In the following slides I will attempt to guide you through the path I wish I had taken…

School → Job → Certifications → Penetration Testing

School

- Learn Linux! Learn it well
- Bash, Python, Java, Assembly, Ruby, C++ - you don't need to be a master every language, but you do need to have a general understanding.
- Protocols
- Data Structures
- Computer design ranging from the basics of digital design to the hardware/software interface for application programs
- Networks, network security & privacy
- Wireless
- Cryptography
- …and yes, you do need to learn Windows too!



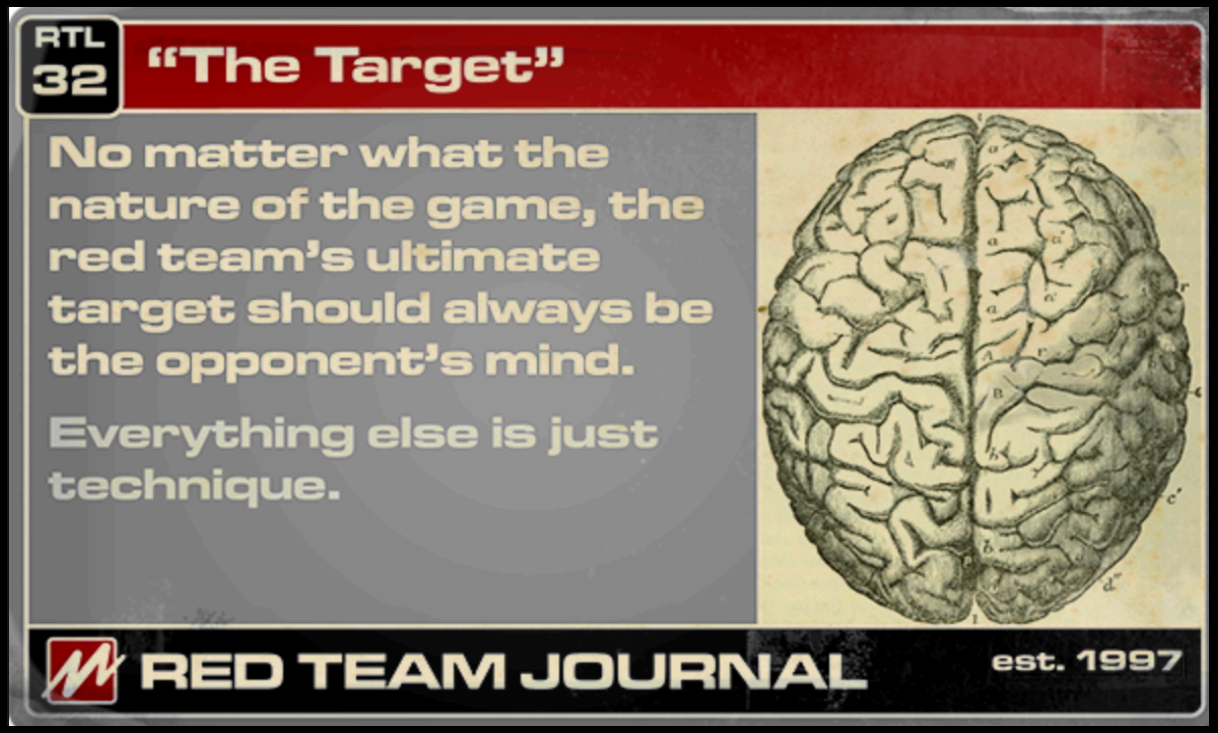
Job

- System Administrator - system administrators learn how to put things together and automate their work for their quality of life. They also learn how to configure different environments, and where most organizations cut corners.

- Security Administrator – deploy security software such as AV, Firewalls, IDS/IPS devices . In this position you will learn how the crown jewels of an organizations will be protected.

- Network Administration – securing network devices, identify improperly configured network devices and risks

- Application Developer - leaning how to write secure application will teach you how to recognize flaws in the application you would be testing.



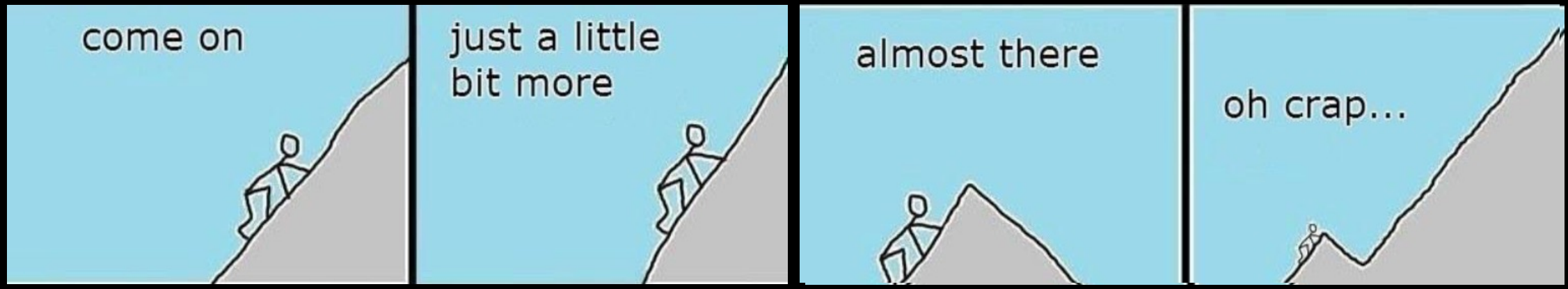
Certifications

- **KLCP: Kali Linux Certified Professional**
- **Course:: Kali Linux Revealed :Mastering the Penetration Testing Distribution Book – FREE for Download!!!** https://www.kali.org/download-kali-linux-revealed-book/
- **Lab Exercises:** https://kali.training/introduction/kali-linux-revealed-book/

- **OSCP : Offensive Security Certified Professional**
- **Course:: Penetration Testing with Kali Linux** https://www.offensive-security.com/information-security-training/penetration-testing-training-kali-linux/
- Live Penetration Testing Labs

- **OSWE : Offensive Security Web Expert**
- **Course:: Hands on web application in depth** https://www.offensive-security.com/information-security-certifications/oswe-offensive-security-web-expert/

- **OSCE : Offensive Security Certified Expert**
- **Course:: Cracking the Perimeter** **https://www.offensive-security.com/information-security-certifications/osce-offensive-security-certified-expert/**



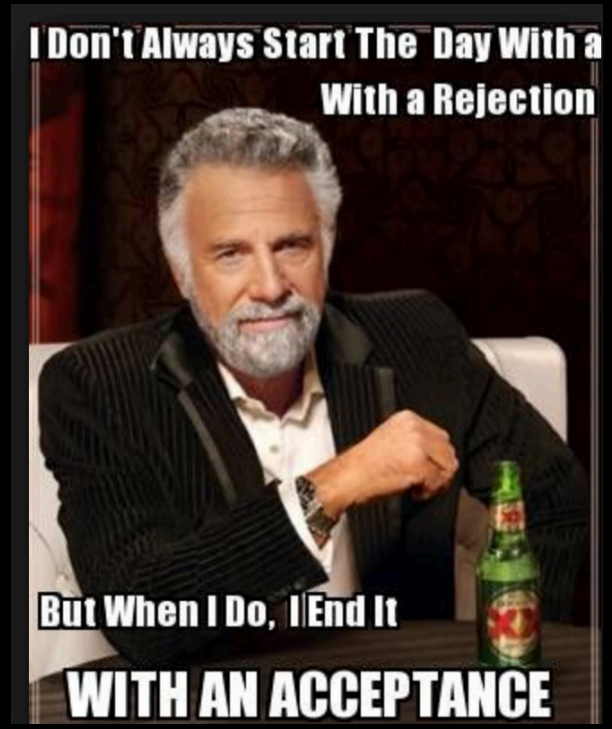
School → Job → Certifications → Penetration Testing

Penetration Testing

- Your skills are the product!
- You are always learning, there is no end to it. Accept it
- Crazy hours… 10-15 hour days followed by 2-3 hour days
- Clients will treat you like auditors… auditors will treat you like clients.
- Sometimes as crazy as the scope may seem all you can do is deliver your best.. Because the client wants what they want.

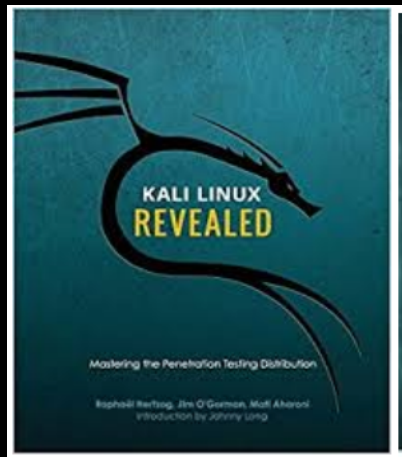
Penetration Testing

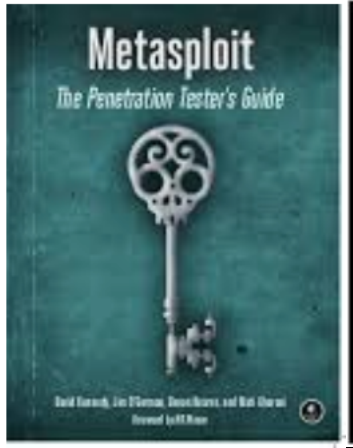
- Meet your new best friend … Reporting. Every organization has a boiler plate template or you may find yourself in the position you need to create one.
- What needs to be on it: Overview, Executive Summary, Scope, Testing Limitations, Engagement Narrative, Risk Ratings, and Findings.
- It's on Testing Limitations, and Engagement narrative that you protect yourself and your employer.
- Accept that not all organizations will hire you to bring value, some of then just want a stamp of approval stating they tested and you found nothing.
- It helps to work in pairs of 2, or to have a counselor as a second pair of eyes. Having an environment or individuals that you can help keep you on track and avoid tunnel vision

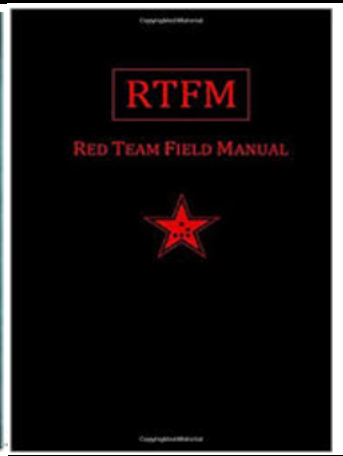


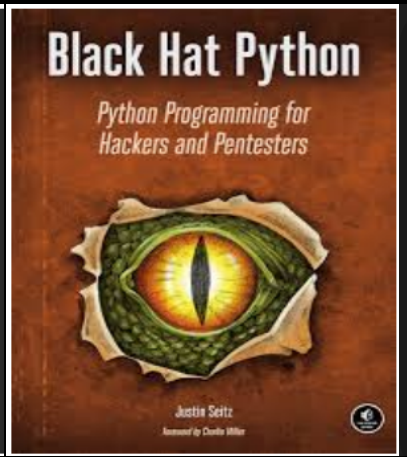
Free Resources & My favorite books:

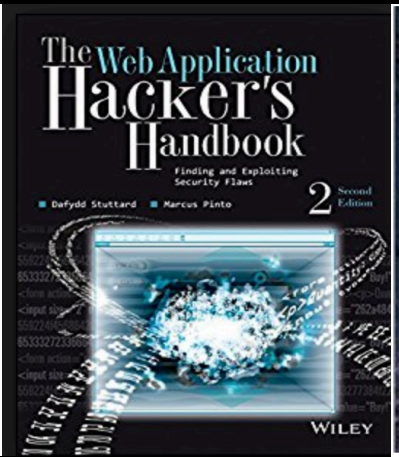
- Download Metasploitable, the virtual machine to test Metasploit by Rapid7: https://information.rapid7.com/metasploitable-download.html
- HackThisBox: https://www.hackthebox.eu/
- bWAPP: http://www.itsecgames.com/
- HackThis: https://www.hackthis.co.uk/
- Hellbound Hackers: https://www.hellboundhackers.org/
- HackThisSite: https://www.hackthissite.org/

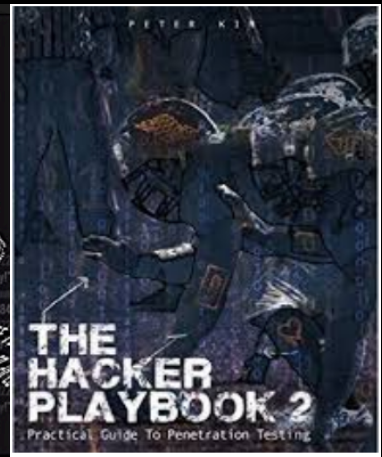






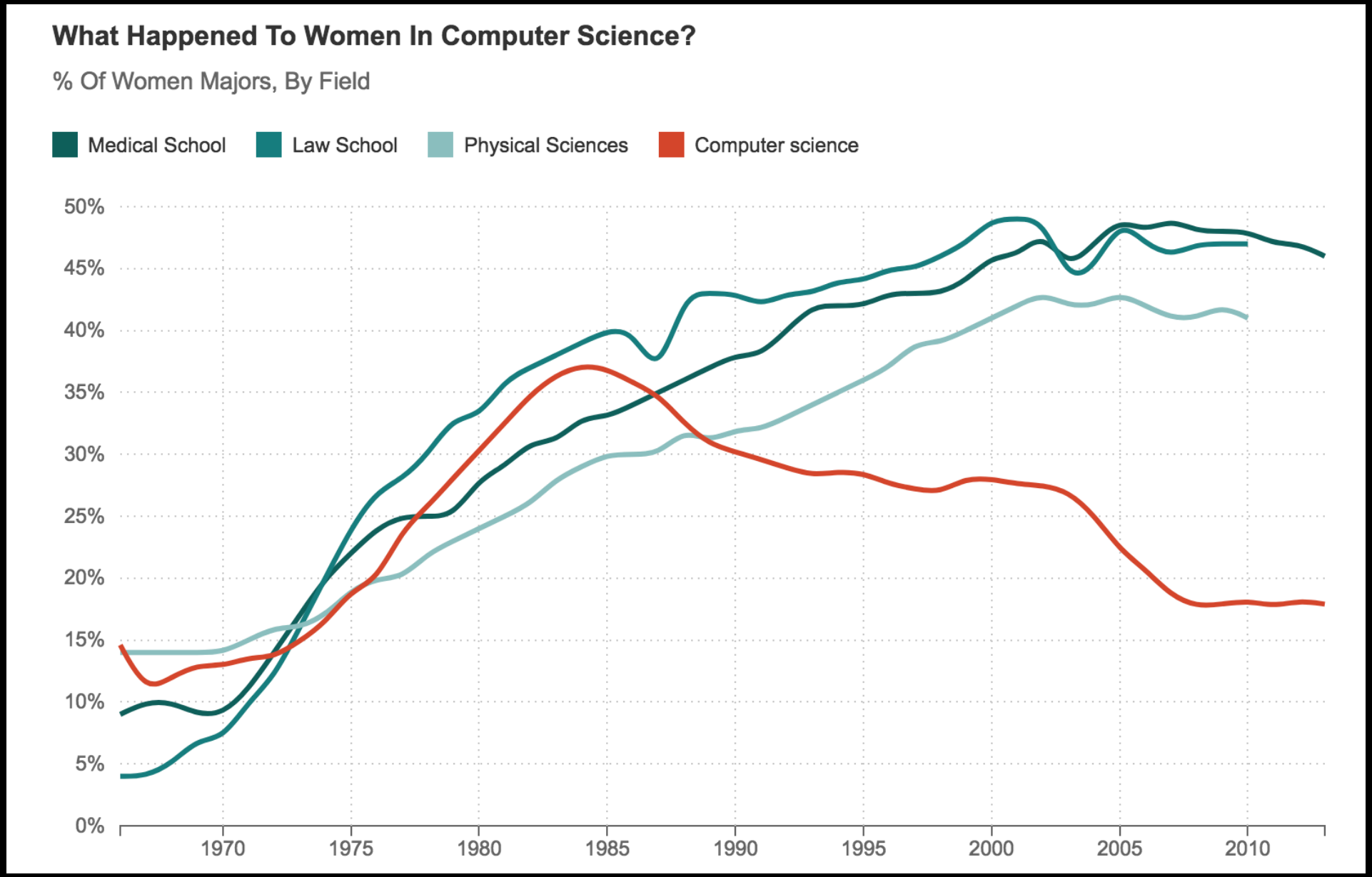




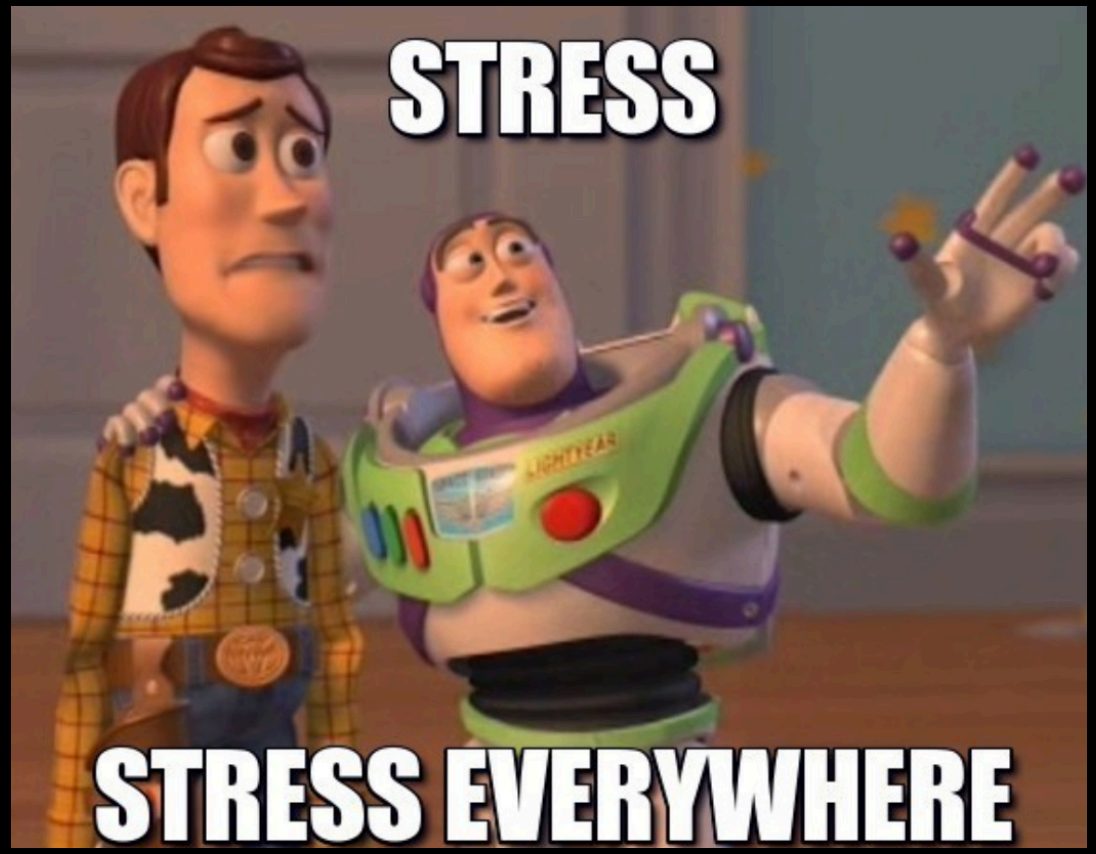


Women in Penetration Testing..

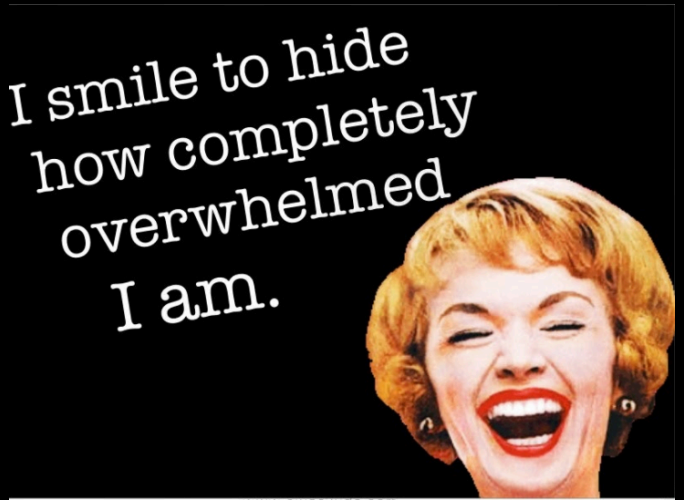
- This field still primarily dominated by men
- Expect to be asked silly technical questions on interviews
- Expect to put in at least 6 months into a job before you “earn” the same respect.
- Workplace harassment.. It’s going to happen be prepared to deal with it.
- There is hope!


What Happened To Women In Computer Science?
% Of Women Majors, By Field
Medical School
Law School
Physical Sciences
Computer science
50%
45%
40%
35%
30%
25%
20%
15%
10%
5%
0%
1970
1975
1980
1985
1990
1995
2000
2005
2010

In Summary…



1. You need to be passionate and enjoy what you do otherwise you will never make it in this business.
2. The skills you will need to be a successful tester.
3. You need to be extremely curious...research is 70% of the job.
4. Keep your knowledge fluid… don't stale! Get the right certifications and keep training.
5. Practice makes it perfect! The more tests you do the more you will improve.
6. Find a non- computer related hobby. Playing soccer, yoga, dancing, whatever… you need to be able to mentally disconnect to keep you from burning out.
7. Finally, be humble along the way… and once you make it help the next generation of hackers.



If you would like to hire us to test your organization please email us at:

pcaston@us.ibm.com

If you have questions or want to keep in touch feel free to use the methods below:

perla.caston@gmail.com

https://twitter.com/castonperla

https://www.linkedin.com/in/perlacaston