Workshop

We are cyber / WoSEC Montreal

What is pentesting?

Who am I?

- Pentester at Okiok
- Blogger, Podcaster, trying to democratize the security of information for all, especially for women.
- Organizer of WoSEC Paris chapter
- Newly organizer of workshops for WeAreCyber aka WoSEC Montreal

- Contact Info:

Gabrielle Botbol

- Twitter:

@Gabrielle_BGB

- Linkedin

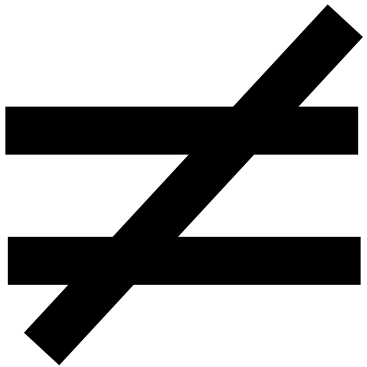
linkedin.com/in/gabriellebotbol

- Blog

https://gabrielleb.fr/blog

What's a hacker?

ETHICAL HACKER



CYBER CRIMINAL

What’s a hacker?

Black

Grey

White

Crédits images:https://www.itpro.co.uk/hacking/30282/what-is-ethical-hacking-white-hat-hackers-explained

What is pentest?

- Trying to get into a system to check its security
- Differents types of pentests

Crédits images:https://image.shutterstock.com/image-vector/furious-frustated-businessman-hitting-computer-260nw-200466014.jpg

External Pentest

Crédits images:https://westoahu.hawaii.edu/cyber/cscc/global-cyber-environment/global-cybersecurity-resources/

Vulnerability assessment

Crédits images:http://www.merule-expert.com/analyse-champignons.ws

Internal pentest

Crédits images: https://www.groovypost.com/howto/connect-netowrks-windows-10/

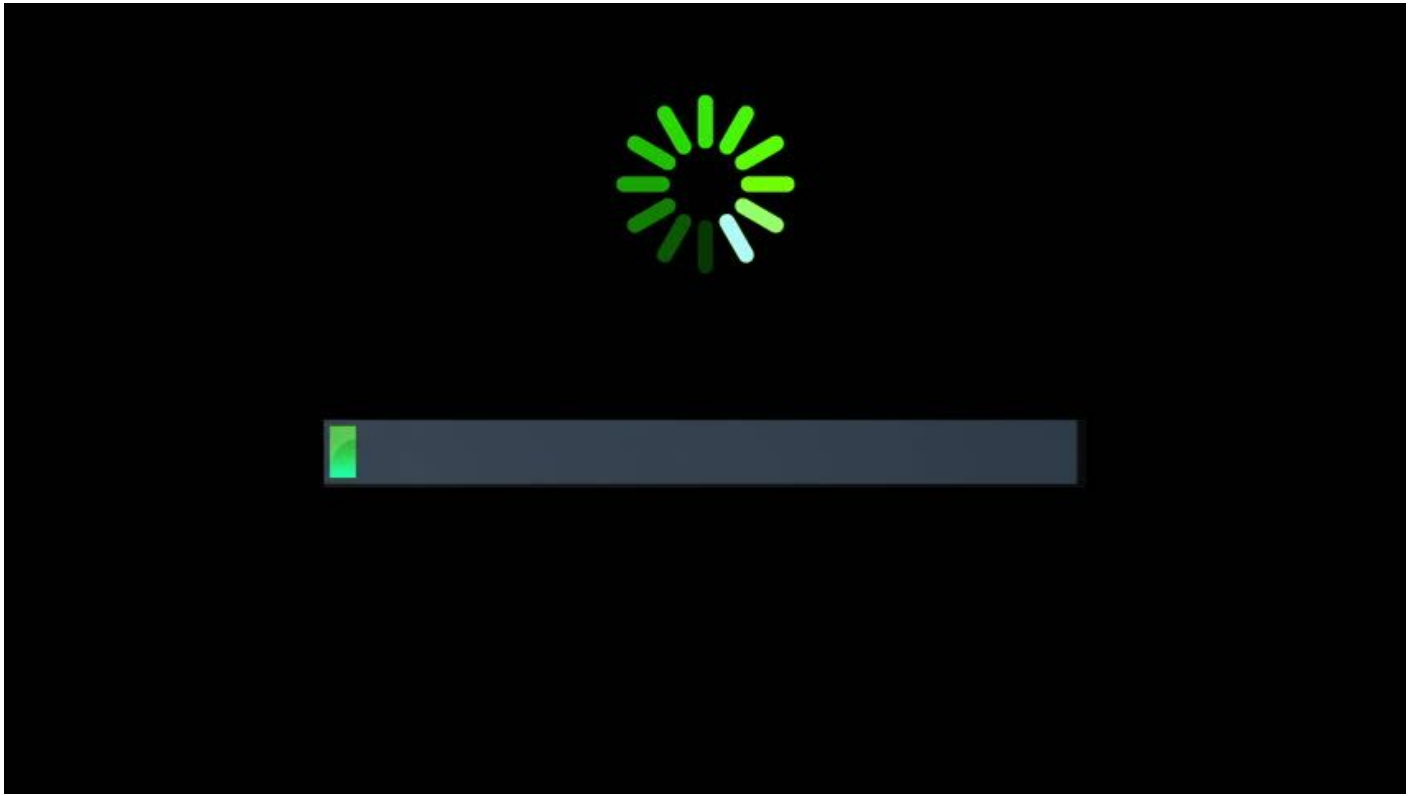
Wifi

Crédits images:https://www.istockphoto.com/ca/photo/business-woman-walking-computer-computing-typing-digital-table-gm166639731-23715417

Social Engineering - Phishing

Physical security

Denial of Service

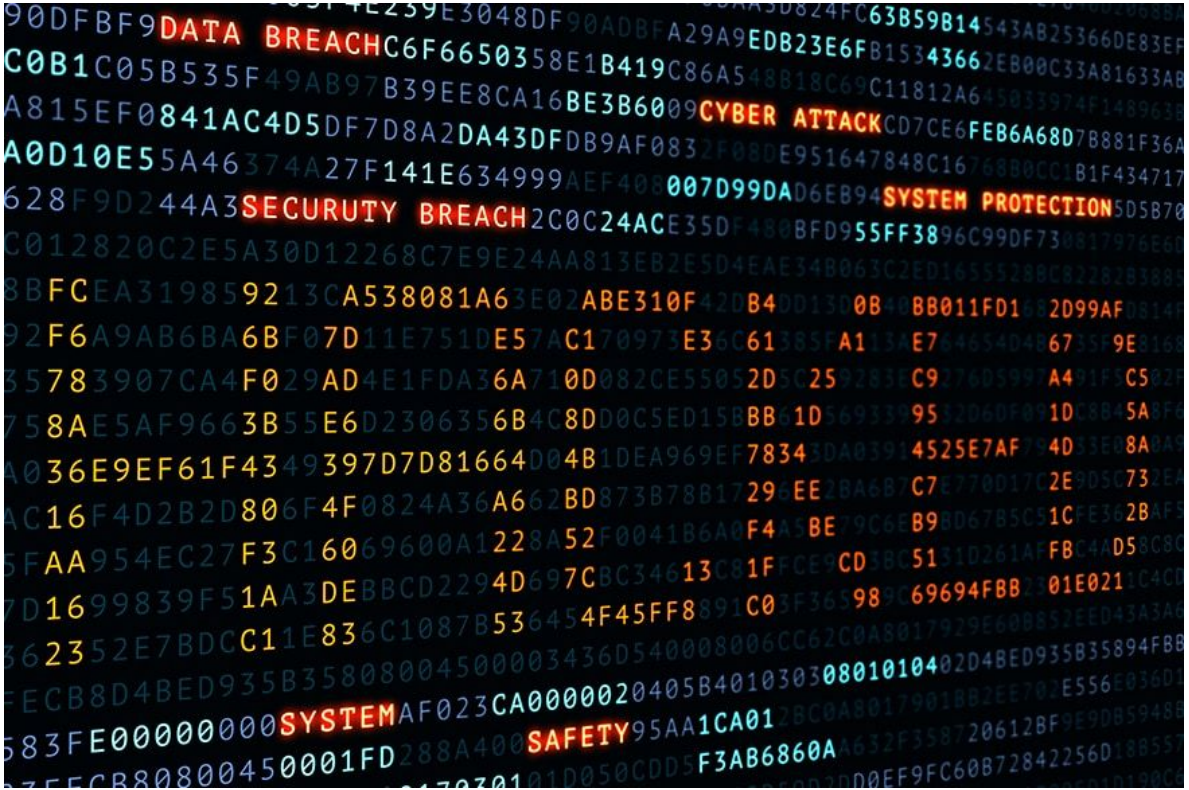


Crédits images: https://www.shutterstock.com/video/clip-12285575-loading-screen-bar-green-0-100-computer

Red Team

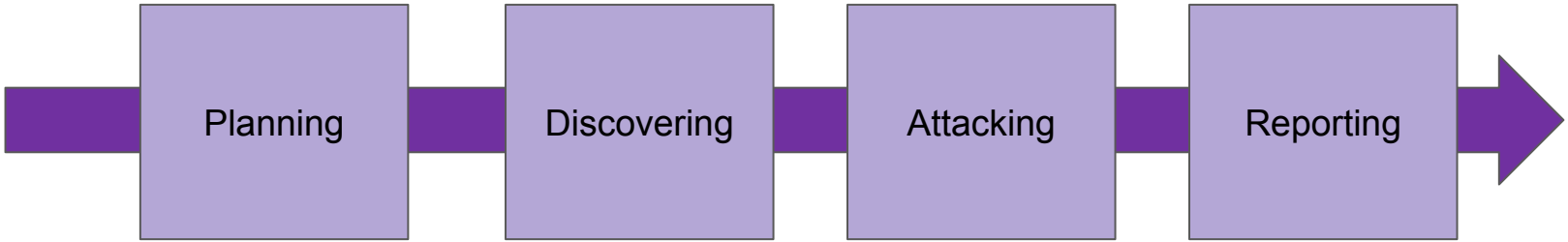
Crédits images: https://www.fourchette-et-bikini.fr/sport/fiche/escrime.html

Web



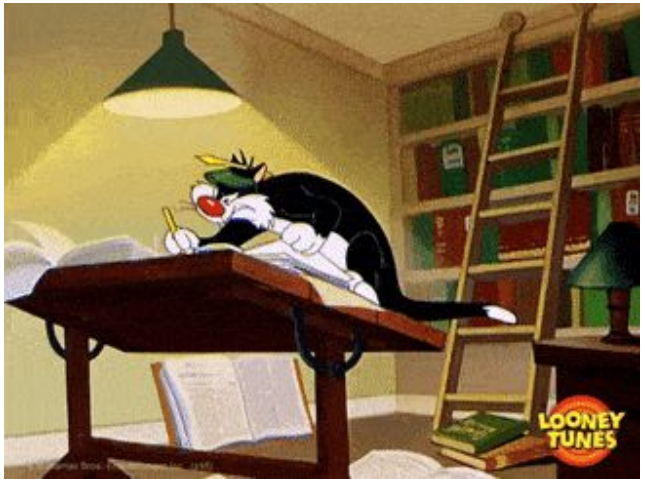
Crédits images: https://hackercombat.com/cyber-criminals-are-selling-hacking-tools-on-the-dark-web/

Steps of a pentest



Planning

- Communication with customer
- Defining the scope
- Defining goals of the pentest
- NDA
- Will a retest be done or not after patch applied by customer?
- etc.



Discovering

- Gathering informations about the target
- How does it works
- Trying to find out technologies in use
- Etc.

Attacking

- Based on the previous step we can attack
- We try to do what a cybercriminal would do

Reporting

- We deliver a report
- Every flaws with score of criticallity
- How to reproduce the attack
- How to patch

Practice: Case Study

Exercise:

Mr Flaw needs you to test his brand new fancy website.

Describe what you will do (with him and on your own) to help him in regards of the pentesting steps we talked about previously.

Possible solution for the Planning phase

You make an appointment with Mr Flaw:

a. Scope
b. Goals
c. Plan with deadlines
d. Explanation of the process
e. Constraints
f. Expected delivery
g. NDA Signing
h. Authorisation form signed
i. Time tracking table (Ganttchart like)

Possible solution for the Planning phase

Tools needed for this phase:

- A prepared NDA contract
- A prepared Engagement Protocol
- Something to take some notes
- A presentation of an anonymised previous similar project if Mr Flaw is not used to pentest

Possible solution for the Discovering phase

You start to get to know your target

- How does it work
- Inspect request response
- What are the technologies used

Possible solution for the Discovering phase

Tools for this phase:

- Burp Suite or OWASP ZAP
- OWASP testing guide: https://owasp.org/www-project-web-security-testing-guide/
- Freemind or libre office draw something to help you visually organize your observations

Possible solution for the attacking phase

You will test as many things as you can but methodically

You can use guides like the OWASP testing guide (again):
https://owasp.org/www-project-web-security-testing-guide/

You will take note of all your findings for the report:

You can use cherrytree or amy other tool you want for this:
https://www.giuspen.com/cherrytree/

In case of critical vulnerabilities you need to contact the customer immediately

Kali Linux to effectively attack the target

Possible solution for the reporting phase

Describe every vulnerabilities you can get help in the OWASP testing guide or on Mitre website:

- http://capec.mitre.org/data/lists/2000.html

Order your vulnerabilities by criticality using cvss or wasc:

- http://projects.webappsec.org/w/page/13246978/Threat%20Classification
- https://www.first.org/cvss/

Explain how to reproduce
Explain how to patch
Include a part for the executive of the company you are testing for

Generally useful Resources

- The penetration testing execution standard: http://www.pentest-standard.org/index.php/Main_Page
- Examples of pentest reports:
  - https://radicallyopensecurity.com/portfolio.htm
  - https://cure53.de/#publications
- CVSS:
  - What is it: https://en.wikipedia.org/wiki/Common_Vulnerability_Scoring_System
  - Resource: https://www.first.org/cvss/
- References for vulnerabilities and attacks:
  - http://capec.mitre.org/data/lists/2000.html
  - https://attack.mitre.org/
- Kali Linux a set of tools for pentest in a VM: https://tools.kali.org/

Other resources: How to learn

- You can read my story here: https://gabrielleb.fr/blog/
- Continue to attend our workshop :D :D :D :D
- Mosse Institute (free for women contact me if you are interested i can enroll you): https://www.mosse-institute.com/
- Cybrary (free): https://www.cybrary.it/
- Certifiedsecure (free): https://www.certifiedsecure.com/frontpage
- Hackthebox (free): https://www.hackthebox.eu/
- Root-me (free): https://www.root-me.org/
- Over the wire (free): https://overthewire.org/wargames/
- Ringerzer0 (free): https://ringzer0ctf.com/
- Practice with lives ctf (free): https://ctftime.org/
- Go to conferences (free): https://en.wikipedia.org/wiki/Computer_security_conference

Questions?