Hacking 101

Filip Holec
$ whoami

- CTO of ENGETO, Ethical Hacking course creator & lecturer
- CTF player [tuna]
- security enthusiast
- former Red Hat Quality Engineer, RHCE
$ whatis

- introduction to ethical hacking
- motivation, required skillset
- resources to get you started
- Q&A
$ ethical hacking

● hacker - originally, someone who makes furniture with an axe
● otherwise, hacking is quite a positive word
  ○ although not in media and specific countries
● red teaming and blue teaming
● pentesting
$ motivation

- challenge one’s abilities
- learn new area in IT - it_skill++
- potential main source of income
  - bug bounty, pentesting, internal security expert
- emerging market for cyber security
  - increase from $3.5B in 2004 to $115B in 2018
$ motivation [H1 report 2018]

- learn tips and techniques
- be challenged
- have fun
- make money
- advance one’s career
- do good in the world & help others
- protect and defend
- show off

$ skillset

- learn how to program.
- get one of the open-source Unixes and learn to use and run it.
- learn how to use the World Wide Web and write HTML.
- if you don't have functional English, learn it.
- try harder / never give up mindset.

src: http://www.catb.org/esr/faqs/hacker-howto.html#basic_skills
$ attitude$

- the world is full of fascinating problems waiting to be solved.
- no problem should ever have to be solved twice.
- boredom and drudgery are evil.
- freedom is good.
- attitude is no substitute for competence.

src: http://www.catb.org/esr/faqs/hacker-howto.html#attitude
resources to learn from

- vulnerable web apps
- online platforms for security education
- ctf s
- written content online - articles, blogs, ...
- books
- podcasts
- conferences
- + bug bounty
- + tools
$ vulnerable web apps

- OWASP - curated list of web applications available
- both online & offline + ISOs

[...] list of vulnerable web applications available to security professionals for hacking and offensive activities, so that they can attack realistic web environments... without going to jail :)
$ web apps - online platforms

● Hack The Box - machines & challenges
  ○ https://www.hackthebox.eu/invite - test to get invite code to HTB

● Avatao - e.g. CrySys 2019
  ○ https://platform.avatao.com/discover/paths

● Over The Wire - online wargames (Bandit, Natanz, ...)
  ○ https://overthewire.org/wargames/

● OWASP Juice Box / DVWA / bWAPP
  ○ available via link on previous slide
$ owasp juice shop

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basket Access</td>
<td>Access someone else's basket.</td>
<td>solved</td>
</tr>
<tr>
<td>Christmas Special</td>
<td>Order the Christmas special offer of 2014.</td>
<td>solved</td>
</tr>
<tr>
<td>Deprecated Interface</td>
<td>Use a deprecated B2B interface that was not properly shut down.</td>
<td>solved</td>
</tr>
<tr>
<td>Five-Star Feedback</td>
<td>Get rid of all 5-star customer feedback.</td>
<td>solved</td>
</tr>
<tr>
<td>Login Admin</td>
<td>Log in with the administrator's user account.</td>
<td>solved</td>
</tr>
<tr>
<td>Login MC SafeSearch</td>
<td>Log in with MC SafeSearch's original user credentials without applying SQL Injection or any other bypass.</td>
<td>solved</td>
</tr>
<tr>
<td>Password Strength</td>
<td>Log in with the administrator's user credentials without previously changing them or applying SQL Injection.</td>
<td>solved</td>
</tr>
<tr>
<td>Security Policy</td>
<td>Behave like any &quot;white-hat&quot; should.</td>
<td>solved</td>
</tr>
<tr>
<td>Weird Crypto</td>
<td>Inform the shop about an algorithm or library it should definitely not use the way it does.</td>
<td>solved</td>
</tr>
</tbody>
</table>
$ dvwa
$ bwapp
$ other online materials

- Hacker news - [https://news.ycombinator.com/](https://news.ycombinator.com/)
  - news curated by community - top posts are most relevant
- Hacksplaining - [https://www.hacksplaining.com/](https://www.hacksplaining.com/)
  - security training for developers
- VulnHub - [https://www.vulnhub.com/](https://www.vulnhub.com/)
  - provide materials that allows anyone to gain practical 'hands-on' experience in security
- Live overflow - [https://liveoverflow.com/](https://liveoverflow.com/)
  - place to learn about topics such as buffer/heap overflows, reverse engineering, vulnerability analysis, debugging, fuzzing and generally hacking
- Smash the stack - [http://smashthestack.org/](http://smashthestack.org/)
  - wargaming network
Capture The Flag
- competition for security professionals and students / enthusiasts
- [https://ctftime.org/](https://ctftime.org/) - aggregator for CTFs
- goal: test one’s skills in a series of challenges
- typically have time constraint (weekend)
- a lot of them have a reward - either reputation or money
$ use case - PicoCTF

- PicoCTF - [https://2018game.picoctf.com/](https://2018game.picoctf.com/)
  - **PICOCTF IS A FREE COMPUTER SECURITY GAME TARGETED AT MIDDLE AND HIGH SCHOOL STUDENTS. THE GAME CONSISTS OF A SERIES OF CHALLENGES CENTERED AROUND A UNIQUE STORYLINE WHERE PARTICIPANTS MUST REVERSE ENGINEER, BREAK, HACK, DECRYPT, OR DO WHATEVER IT TAKES TO SOLVE THE CHALLENGE**
$ use case - 35C3 Junior

- 35c3 Junior CTF - [https://junior.35c3ctf.ccc.ac/](https://junior.35c3ctf.ccc.ac/)
  - Some of them are working - mainly to see the concept of CTF
$ use case - Czech CTF example

● The Catch - [https://www.thecatch.cz/](https://www.thecatch.cz/)
  ○ 1-4 members
  ○ Czech round in Prague, finals in Japan

● CTFs at/for conferences
  ○ [https://konferencesecurity.cz/](https://konferencesecurity.cz/)
  ○ Catch The Qubit for [https://qubitconference.com/](https://qubitconference.com/)
$ use case - Slovak CTF example

- Guardians 2019 - [https://wargame.sk/](https://wargame.sk/)
- only for individuals - no teams
- storyline - elections: compromised security
  - prevent data leak that could harm candidates
$ online written resources

● OWASP Top Ten Project

● write-ups from disclosed bug bounties

● awesome-bug-bounty, awesome-security and awesome-pentest lists
  ○ e.g. [https://github.com/djadmin/awesome-bug-bounty](https://github.com/djadmin/awesome-bug-bounty)

● write-ups of past CTFs

● + written/video write-ups on retired Hack The Box machines
  ○ Valentine - [https://www.youtube.com/watch?v=XYXNvemgJUo](https://www.youtube.com/watch?v=XYXNvemgJUo)
$ books

● the web application hacker's handbook: finding and exploiting security flaws
  ○ 2nd edition [Dafydd Stuttard, Marcus Pinto]
● OWASP testing guide v4
● the hacker playbook 3: practical guide to penetration testing [Peter Kim]
● hacking: the art of exploitation [Jon Erickson]
● web hacking 101 [Peter Yaworski] - bug bounties
$ podcasts

- hackable - [https://hackablepodcast.com/](https://hackablepodcast.com/)
  - view on security from consumer point of view, recommended for beginners

- unsupervised learning - [https://danielmiessler.com/podcast/](https://danielmiessler.com/podcast/)
  - content curation as a service
  - ~30 minute overview of news in security, technology and humans
  - senior IT Security researcher
  - Creator and leader of the OWASP IOT security project & SecLists project
$ others

- Pentester Land - [https://pentester.land/](https://pentester.land/)
  - really nice resource with news, cheatsheets, conference news etc.
- Zero Daily - [https://www.hackerone.com/zerdaily](https://www.hackerone.com/zerdaily)
  - Hacking, AppSec, and Bug Bounty newsletter
- The Secure Developer
  - [https://www.heavybit.com/library/podcasts/the-secure-developer/](https://www.heavybit.com/library/podcasts/the-secure-developer/)
  - podcast about security for developers, covering tools and best practices
$ certifications

- OSCP, OSCE by offensive security
- CEH - certified ethical hacker
- CISSP, Security+
- ... + a lot more
- **not needed if starting with security/bug bounty**
- mainly a **formal** requirement in job descriptions
$ conferences

- OWASP Local Chapters
- DEFCON & BlackHat - largest ones, LV, US (+ onsite/online CTF)
- Chaos Communication Congress - every year, DE (+ onsite/online CTF)
- **Security Session** - Brno, CZ (+ onsite CTF)
- Def Camp - important sec conference in CEE, RO (+ onsite CTF)
- Hacktivity - Budapest, HU
- nearly all of them publish talks & materials online
  - e.g. [https://media.ccc.de/](https://media.ccc.de/) and others
$ bug bounty

● break software & get paid in the process
● earn $ and reputation
● everyone can start, just register at a bug bounty platform
  ○ https://www.hackerone.com/start-hacking
● start with public programs, then get invites into private ones
  ○ or use https://ctf.hacker101.com/
$ bug bounty platforms

● hackerone
  ○ https://hackerone.com/bug-bounty-programs
● bugcrowd
  ○ https://bugcrowd.com/programs
● hacktropy [SK]
● bountysource
● ... plus private programs
  ○ facebook
  ○ google
$ tools used by security experts

- OWASP ZAP - active scanner + proxy
- burp suite - proxy
- firefox - web browser
- nmap - network scanner
- wireshark - network traffic analyzer
- hydra - bruteforce password cracker
- sqlmap - SQL Injection checker
- gobuster/dirb - enumerate endpoints
- nikto - web application scanner
- SPARTA - GUI application to simplify network penetration testing
- binwalk - analysis of a resource (img/zip) to see resources within
$ tips and hints

- find a team you can work with
- challenge yourself
- try harder attitude
- ... add your own in

$ q&a
NOT SURE IF THEY'RE CLAPPING FOR MY PRESENTATION

OR BECAUSE ITS FINISHED