CTF Techniques

Por Carlos Velez
Introduction
What is it, why is it important?

Types of CTF
Many options with different difficulty levels

Challenges
Some of the challenges of the most important CTFs

Statistics
It is growing and recruiters are looking for talent

Tools
Some of the essential tools for CTF Competitions

Resources
Lots of information, writeups, repos
INTRO

Children game where each team attempt to capture the opposing team’s flag (Persil).

CTF

What is it?

British soldiers capturing French flag (Pinterest).
INTRO

What is it?

- ...is a computer security competition where teams/individuals compete to solve challenges of varying difficulty (usually increasing) to score points.
- Realistic problems with realistic solutions.
- Some of the famous CTFs (CTFtime).
TYPES OF CTFs

Wargames
overthewire

Hack quest
SANS holyday Challenge

Jeopardy
National Cyber League

Attack & Defend
National Collegiate Cyber Defense

- Single-user vs. multi-user
- Single targets vs. multiple targets
- Competitive vs. collaborative
- Short and focused vs. long-term
- Local vs. remote
- Defensive, offensive, analytical
TYPES OF CHALLENGES (CATEGORIES)

Cryptography
Lots of math!

Exploitation
Break it!

Reverse Engineering
How it works, what can you get?

Forensics
Looking for evidence

Web Applications
Get information!
CTF Characteristics:

- divides a problem into smaller pieces (challenges, flags)
- measure progress (score)
- create a sense of accomplishment (rewards, achievements)
- instill a sense of competition (leader board)
- directly applies theory
- is great fun!
Why CTF?

• To practice your hacking skills in a realistic environment
• Compete with other hackers
• Getting good at it = find a good job opportunity
• Is great fun!
CTFtime.org Teams Total

Number of Competitions

Top 10 countries by team count

- US — 3437
- IN — 2786
- RU — 1198
- CN — 1069
- ID — 918
- FR — 807
- VN — 683
- KR — 669
- JP — 639
- DE — 588

35976 teams total
Nacional Cyber League (NCL) (Spring 2017) Report

- Must be affiliated to a US institution
- Defensive and offensive puzzles
- Based on CompTIA Security+ and EC-Council CEH exams

<table>
<thead>
<tr>
<th>Category</th>
<th>Bracket</th>
<th>Bracket Rank</th>
<th>National Rank</th>
<th>Total Score</th>
<th>Total Flag Capture</th>
<th>Total Flag Attempts</th>
<th>Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cryptography</td>
<td>Silver</td>
<td>5</td>
<td>10</td>
<td>580</td>
<td>17</td>
<td>22</td>
<td>77.27%</td>
</tr>
<tr>
<td>Enumeration and Exploitation</td>
<td>Silver</td>
<td>1</td>
<td>3</td>
<td>310</td>
<td>4</td>
<td>4</td>
<td>100.00%</td>
</tr>
<tr>
<td>Log Analysis</td>
<td>Silver</td>
<td>3</td>
<td>9</td>
<td>450</td>
<td>15</td>
<td>19</td>
<td>78.95%</td>
</tr>
<tr>
<td>Network Traffic Analysis</td>
<td>Silver</td>
<td>13</td>
<td>28</td>
<td>310</td>
<td>17</td>
<td>23</td>
<td>73.91%</td>
</tr>
<tr>
<td>Open Source Intelligence</td>
<td>Silver</td>
<td>8</td>
<td>13</td>
<td>185</td>
<td>22</td>
<td>27</td>
<td>81.48%</td>
</tr>
<tr>
<td>Password Cracking</td>
<td>Silver</td>
<td>9</td>
<td>26</td>
<td>515</td>
<td>24</td>
<td>24</td>
<td>100.00%</td>
</tr>
<tr>
<td>Scanning</td>
<td>Silver</td>
<td>5</td>
<td>17</td>
<td>330</td>
<td>17</td>
<td>25</td>
<td>68.00%</td>
</tr>
<tr>
<td>Web Application Exploitation</td>
<td>Silver</td>
<td>6</td>
<td>13</td>
<td>85</td>
<td>2</td>
<td>2</td>
<td>100.00%</td>
</tr>
<tr>
<td>Wireless Access Exploitation</td>
<td>Silver</td>
<td>17</td>
<td>43</td>
<td>235</td>
<td>12</td>
<td>12</td>
<td>100.00%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>Silver</td>
<td>5</td>
<td>15</td>
<td>3150</td>
<td>131</td>
<td>159</td>
<td>82.39%</td>
</tr>
</tbody>
</table>
Requirements:

• Problem solving skills
• Network knowledge
• Web vulnerabilities
• Programming (no language preference) **python**
• *Keep up with the* **Tools**
• *In addition: math, algorithms, protocols, Linux, shell script, automation*
Forensic Challenge Tools

- **Network**
  - Wireshark (packet analyzer)
  - Tcpdump (packet analyzer)
  - Network Miner (network forensics analysis tool)

- **File**
  - 010 (hex editor)
  - Scalpel (file system recovery)

- **Disk Image**
  - Autopsy
  - VMs
  - FTK

- **Image Steganography**
  - Stegsolve
  - Zsteg
RE Tools

- Decompilers
- IDA Pro
- Binary Ninja
- Gidra (free... from NSA)
- programmer knowledge and patience
Encoding vs Ciphers vs Hashing

- Encoding
  - Base64
  - Morse
  - Braille
  - Fictional language

- Ciphers (Classic)
  - Atbash
  - ROT13
  - Caesar
  - Vigener

- Ciphers (Mechanical)
  - Enigma cipher
  - Lorenz ciphers

- Ciphers (Modern)
  - Block ciphers
  - Stream ciphers

- Tools
  - John (pass. Cracking)
  - Hashcat (lots of hash types, GPU)
  - OphCrack (rainbow tables)
  - THC Hydra (online)
Tools for web app security

- Web Browser!
- Web Proxying Tool(s)
  - Burp Suite
  - Fiddler
  - mitmproxy
  - Nikto
  - ZapProxy
- SQLMap - Automatic SQL injection and database takeover tool
- Ysoserial - tool for exploiting unsafe object deserialization vulnerabilities
- SSLyze - deep analysis of the SSL/TLS configuration of web servers/applications.
RESOURCES

- https://github.com/zardus/ctf-tools
- https://github.com/MrMugiwara/CTF-Tools (Repos of useful tools)

- http://icyberchef.com/ (encrypt, decrypt, base conversion, more, open source on GitHub)

- https://www.kali.org/ (pentesting tools already installed on a Linux environment)

- https://overthewire.org/wargames/ (practice Linux command line interface)
REFERENCES

Annual Security Conference Proceedings

ACM

IEEE
THANKS!

Do you have any questions? velez.carlos.y@gmail.com