CTF Primer

2013-09-24
Agenda

- CTF?
- CTF!
CTF?
CTF?
What is CTF?

Capture The Flag

„Capture the Flag (CTF) contests are designed to serve as an educational exercise to give participants experience in security related real world problems“

It‘s all about collecting „flags“

... and having fun!

http://net.cs.uni-bonn.de/wg/cs/staff/raphael-ernst/student-ctf-group/
CTF?
What are the Game Modes?

ȝ **Attack / Defense**
  ȝ Every participating team receives the same server image
    ȝ Harden the services in your instance (!= port blocking)
    ȝ Attack vulnerabilities in the other teams' services
  ȝ Mostly pentesting oriented

ȝ **Hacker Jeopardy**
  ȝ Solve challenges to collect flags
    ȝ Different disciplines
    ȝ Various complexity levels
  ȝ Often: First solver receives a bonus
  ȝ More popular version
CTF?
What is a flag?

- Flag == <n> points
- Often a (prefixed) hash
  - C0ffeeb7ce3cb82a05b1b4d57e70f349
  - ^^^^ Dimva CTF, misc100_2
CTF?
What are these disciplines?

- Forensics
- Web
- Crypto
- Trivia
- Reverse Engineering
- Pwning
CTF?
What are these disciplines?

- **Web**
  - (In)Security of web applications
    - SQL injection
    - directory traversal
    - exploiting logical flaws
    - ...

- **Forensics**
  - Needle in a haystack
  - „Broken“ data / files
  - Image recovery
CTF?
What are these disciplines?

- Reverse Engineering
  - Understanding algorithms
  - Defeating anti-analysis mechanisms
  - "crackmes"

- Crypto
  - Implementation flaws
  - Efficient attacks
CTF?
What are these disciplines?

☼ Pwning
  ☼ Exploitation of services
  ☼ Remote Code Execution (RCE)
  ☼ Finding the vector + planting a shell

☼ Trivia
  ☼ Guessing / inference
  ☼ Recognizing network protocols, file formats, ...
CTF!
CTF!
Why should I play?

- Meet nice people & have a good time :)
- Great opportunity to learn
- Extend your horizon
- Fame & Glory
CTF!
Skills needed.

- Creativity!
- Endurance!!
- Communication!

- Previous knowledge welcome :)
  - Coding + Reversing
CTF!

Infrastructure.

We can provide:

- Locality
- Infrastructure (Net access, some boxes)
- Some experience in CTFs
CTF!
Our First Gig!

Hack.lu CTF

- 22nd – 24th October 2013
  - Most likely 11am – 11am (as in previous years)
- Hacker Jeopardy, run by FluxFingers
- Lots of challenges with varying difficulty
Teaser!

A challenge example
CTF!
A challenge example.

❖ Dimva CTF, misc100_2
CTF!
A challenge example.

🔗 APK
- (Android) application package format
- Zip-file / *.jar
- Contains Dalvik VM code (*.dex)

🔗 DEX2JAR!

SMSRemote-dex2jar.jar 18.07.2013 03:01
CTF!

A challenge example.

- JAR = Java?
  - Yes, but only (bytecode-compiled) class files
- JDGUI! (Java Decompiler)
Trigger warning: Powerpoint madness incoming!
CTF!

A challenge example.

(Keyed-)Hash Message Authentication Code

```java
String[] arrayOfString = localSmsMessage.getMessageBody().split(" ");
System.out.println(arrayOfString.length);
String str10 = A2H(localSmsMessage.getOriginatingAddress());
new HMac();
String str11 = HMac.hmacDigest(arrayOfString[0], H2A("44316d5634"), "HmacSHA256");
if (String.valueOf(key).equals(str11)) {
    showToast(paramContext, "HELP -> Show this help\nINFO -> Get device info\nCOORDS -> Get device coords\nEIE -> Close the App");
    while (true) {
        m++;
        break;
    }
    if (arrayOfString[0].equals("HELP")) {
        showToas(paramContext, str1 + \\
        "\n  + str2 + \\
  + str3 + "\n  + str4 + \\
  + str5);
        showToastr(paramContext, str6 + \\
  + str7 + "\n  + str8 + \\
  + str9);
    } else if (arrayOfString[0].equals("COORDS") && arrayOfString[1].equals(str11)) {
        showToastr(paramContext, "LAT: " + \\
  + "122.084095" + "LON: " + "37.422006"));
    } else if ((A2H(arrayOfString[0]).equals("4556494c") && arrayOfString[1].equals(str11)) {
        showToast(paramContext, "Great! You solved this lame level :)");
    } else if ((A2H(arrayOfString[0]).equals("504945") && arrayOfString[1].equals(str11)) {
        System.exit(0);
else if (arrayOfString[0].equals("EIE")) {
    
```

"4556494c".decode(\"Hex\") => EVIL
CTF!

A challenge example.

Solution (Python):

```python
import hmac
import hashlib

key = "D1mV4"
data = "EVIL"
digestmod = hashlib.sha256

hashed = hmac.new(key, data, digestmod).digest()
result = hashed.encode("base64")
print result

Result: vqwYfONxkebWk4SUsmpQenN6ik3uvvoJw3/oq7hQQYg=

$ cat result | netcat dimvactf.0x90.eu 5555
C0ffeeeb7ce3cb82a05b1b4d57e70f349
Conclusion

Final words to wrap things up
CTF

Conclusion.

- **Student CTF group**
  - It's about you! We only offer the framework

- **Expected Skills:**
  - Motivation! Rest will come by itself!

- **Time commitment:**
  - One meeting per week + optional „homework“ + CTF participation

- **Homework?**
  - Voluntary tasks from old CTFs as practice

- **Long-Run:**
  - A platform to publish
CTF
Resources.

- CTFtime.org
  - Archive / Scores / Write-Ups
- Captf.com/practice-ctf
  - Collection of write-ups, challenges, etc.
- Blog.dragonsector.pl
  - Very active write-up blog of a leading team
CTF
Homework! :)

❖ Dimva CTF, crypto100
❖ A bunch of images
  ❖ ... that look the same
  ❖ ... but have a secret
❖ Hints:

https://dl.dropboxusercontent.com/u/1348415/dimva_crypt0100.zip