Od e-sportu dla hakerów do pracy w IT security

Jarosław Jedynak
Mateusz Szymaniec

Warszawskie Dni Informatyki - 29.03.2017

Plan

- Kim jesteśmy i co robimy
- Czym są CTFy
- Jak zacząć zabawę z CTFami
- Praca w bezpieczeństwie IT
- Pytania

Link do tej prezentacji: https://goo.gl/MFxfcR

Kim jesteśmy

Jarosław Jedynak

- Software/Security Researcher @ CERT.pl
- Były programista
- Obecnie w pracy walczy z botnetami i ransomware
- Współzałożyciel P4 team
- Ulubione kategorie na CTF to kryptografia i RE

Mateusz Szymaniec

- Software/Security Researcher @ CERT.pl
- Były programista
- Obecnie w pracy ratuje świat (w tym klientów polskich banków)
- Współzałożyciel P4 team
- Ulubione kategorie na CTF to web/re/pwn

CERT Polska

- Zespół reagujący na incydenty komputerowe naruszające bezpieczeństwo cywilne naszego kraju.
- Analizujemy zagrożenia w polskim internecie.
  - W tym np. złośliwe oprogramowanie (trojany bankowe, ransomware).
- Działamy w ramach instytutu badawczego -

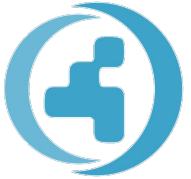
  Naukowej i Akademickiej Sieci Komputerowej.

CERT.PL

p4 team

- Grupa osób zajmujących się bezpieczeństwem IT.
- Znamy się głównie z internetu: nazwa inspirowana forum https://4programmers.net/.

- Przede wszystkim gramy w CTFy.
  - https://p4.team
  - twitter: @p4_team
- Są wśród nas: specjaliści bezpieczeństwa IT, programiści, studenci.



CTF?

Czym są CTFy?

- Drużynowe konkursy dla “entuzjastów bezpieczeństwa komputerowego”.
- Rozwiązywanie różnych zadań związanych z bezpieczeństwem.
  - Na pewno kojarzycie “hackme”, “crackme” - CTFy to dość naturalne rozwinięcie.
- Trwają od 8 do 48 godzin.
- Zazwyczaj organizowane przy okazji konferencji IT security.

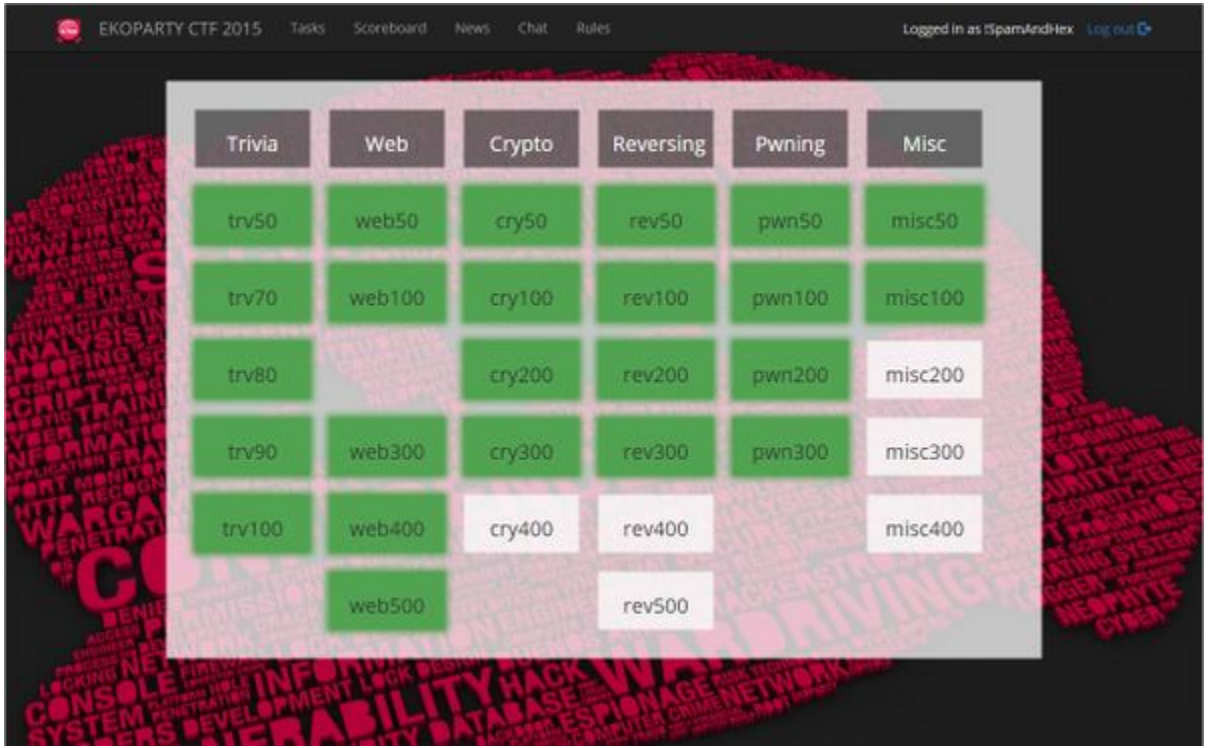
- Potocznie *hakowanie (hack, hack).*
- E-sport, ale bez widowni.

Rodzaje CTFów

- **Jeopardy** (zdecydowana większość)
- **Attack-Defence** (zazwyczaj finały)

- **Online** (zdecydowana większość)
- **Onsite** (zazwyczaj finały)

Jeopardy

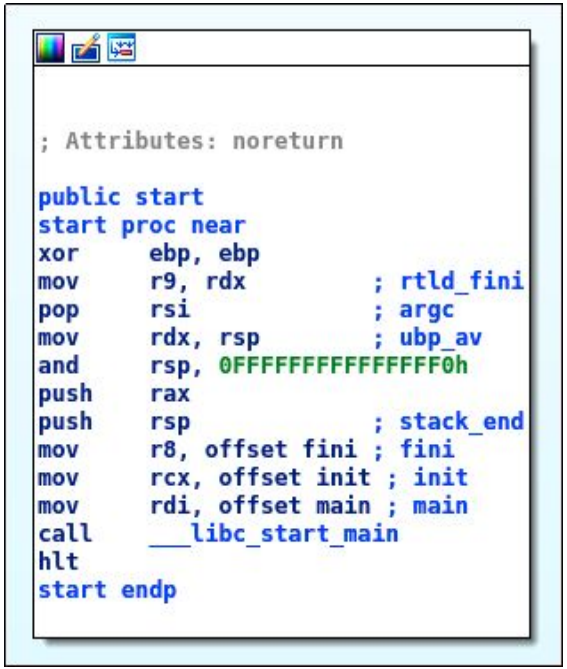

EKOPARTY CTF 2015
Tasks
Scoreboard
News
Chat
Rules
Logged in as !SpamAndHex
Log out
Trivia
Web
Crypto
Reversing
Pwning
Misc
trv50
web50
cry50
rev50
pwn50
misc50
trv70
web100
cry100
rev100
pwn100
misc100
trv80
cry200
rev200
pwn200
misc200
trv90
web300
cry300
rev300
pwn300
misc300
trv100
web400
cry400
rev400
misc400
web500
rev500

Kategorie zadań

Z naszymi subiektywnymi ocenami

Reverse engineering

- *Nasza* ocena kategorii: **10/10** (robimy to codziennie w pracy!)
- Cel: dostajemy skompilowany program i mamy za zadanie go zrozumieć i złamać. (np. znaleźć hasło które program akceptuje, albo wyciągnąć użyty algorytm szyfrowania). Flagą jest hasło, albo dane z pliku.



```
; Attributes: noreturn

public start
start proc near
xor     ebp, ebp
mov     r9, rdx         ; rtld_fini
pop     rsi             ; argc
mov     rdx, rsp        ; ubp_av
and     rsp, 0FFFFFFFFFFFFFFF0h
push    rax
push    rsp             ; stack_end
mov     r8, offset fini ; fini
mov     rcx, offset init ; init
mov     rdi, offset main ; main
call    __libc_start_main
hlt
start endp
```

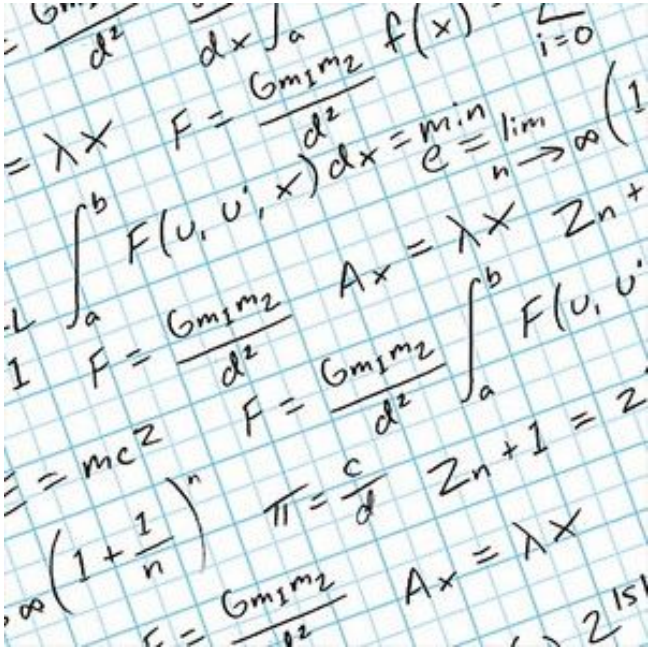
Pwn (binary exploitation)

- Nasza ocena kategorii: **7/10** (dlatego, że jesteśmy w nich słabi)
- Cel: dostajemy skompilowany program i mamy za zadanie znaleźć w nim błąd (np. przepełnienie bufora albo double free), wykorzystać go i włamać się w ten sposób na system organizatorów. Flaga jest zazwyczaj na dysku.

```
root@kali:~/Desktop/ssctf/final# python f1.py
[+] Opening connection to 127.0.0.1 on port 10001: Done
big_chunk addr is: 0xb7bb4000
random is: 0x7742a941
heap addr is: 0x80008000
exe base is: 0x80000000
[*] '/root/Desktop/ssctf/final/final1'
    Arch:     i386-32-little
    RELRO:    Full RELRO
    Stack:    Canary found
    NX:       NX enabled
    PIE:      PIE enabled
    FORTIFY:  Enabled
[+] Loading from '/root/Desktop/ssctf/final/final1': 0xb7fff930
[+] Resolving 'libc.so': 0xb7fff930
[!] No ELF provided.  Leaking is much faster if you have a copy of the ELF being leaked.
libc_base is: 0xb7cb7000
[+] Downloading libc: 0xb7e812d0
[*] Using cached data from '/tmp/pwn-libc.so.cafa8de523249f48aebec877e9f45f904e4d62a4'
[*] '/tmp/pwn-libc.so.cafa8de523249f48aebec877e9f45f904e4d62a4'
    Arch:     i386-32-little
    RELRO:    Partial RELRO
    Stack:    Canary found
    NX:       NX enabled
    PIE:      PIE enabled
[*] Trying lookup based on Build ID: cafa8de523249f48aebec877e9f45f904e4d62a4
[+] Resolving 'swapcontext' in 'libc.so': 0xb7e812d0
[*] Trying lookup based on Build ID: cafa8de523249f48aebec877e9f45f904e4d62a4
swapcontext is: 0xb7cf7940
system is: 0xb7cf53e0
[*] Switching to interactive mode
$ id
uid=0(root) gid=0(root) groups=0(root)
```

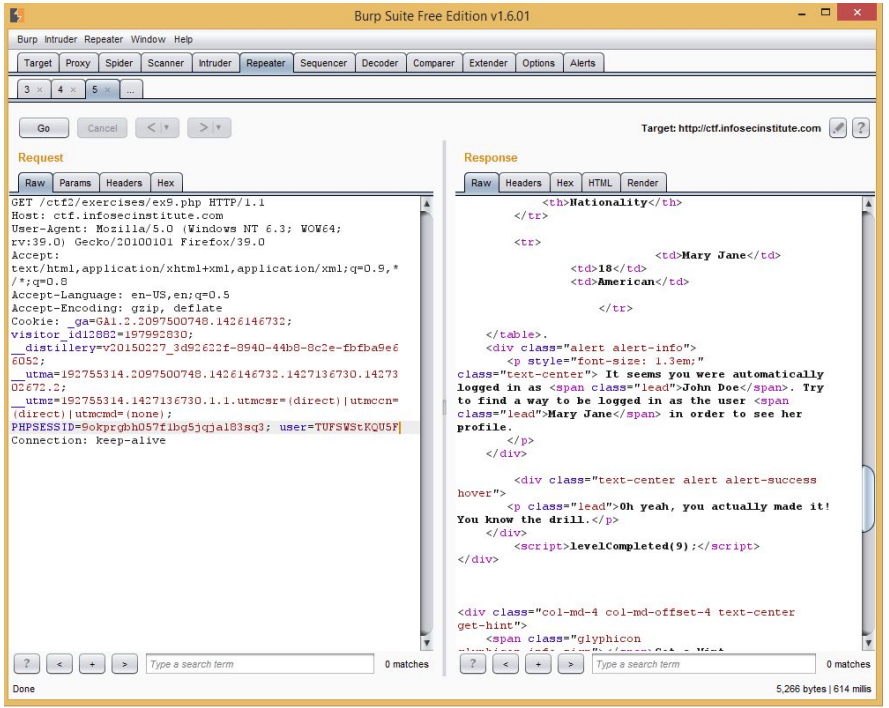
Cryptography

- Nasza ocena kategorii: **9/10**  (dla nielubiących matmy 6/10)
- Dostajemy zaszyfrowane dane, najczęściej też kod który szyfrował te dane, albo serwis/api służące do szyfrowania, i mamy za zadanie odszyfrować dane (w których zazwyczaj znajduje się flaga).



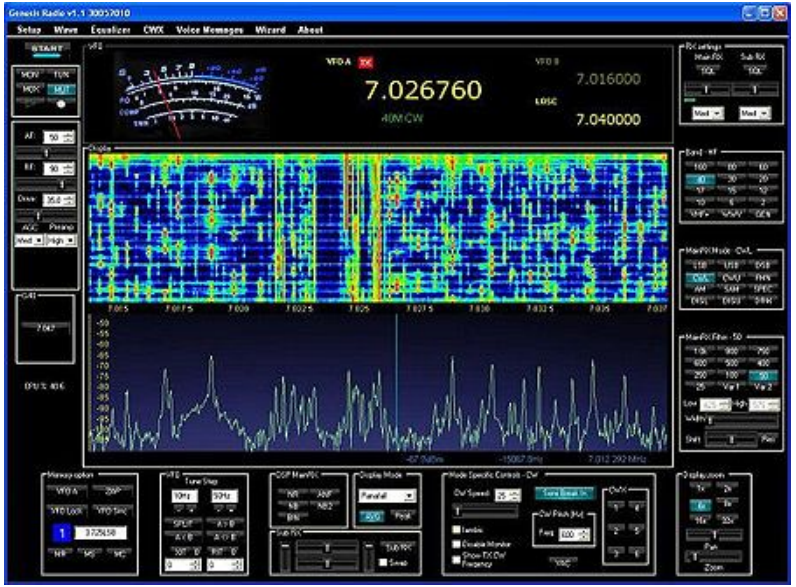
Web

- Nasza ocena kategorii: **8/10** (zależy kogo zapytać)
- Jedna z bardziej życiowych kategorii zadań - dostajemy link do strony organizatorów i naszym zadaniem jest znalezienie na niej błędu i włamanie się. Flaga jest gdzieś w bazie albo na dysku.



Misc

- Nasza ocena kategorii: **5/10** (mieszane uczucia, bardzo różne zadania)
- Wszystko co organizatorom do głowy przyjdzie: pisanie wyrażeń regularnych, słuchanie radia, odtwarzanie logiki programu ze zdjęcia płytki (hardware), dziwne języki, uruchamianie programów z poprzedniej epoki, szukanie ludzi w google, zadania których nie można było wymyślić na trzeźwo.

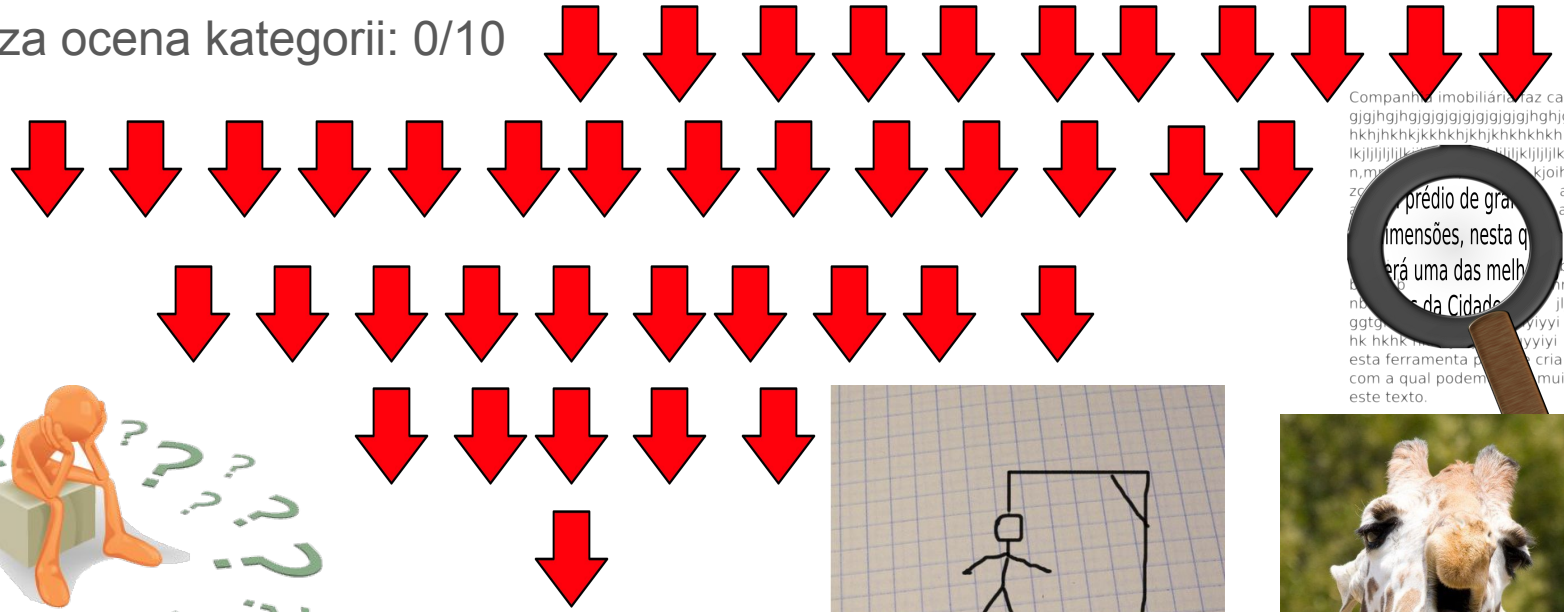


Forensics

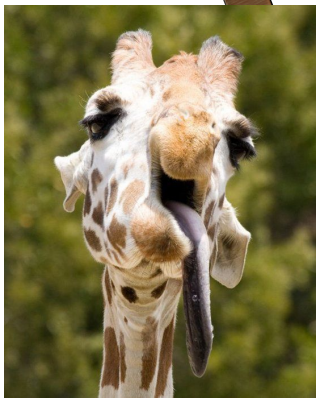
- Nasza ocena kategorii: **3/10** (pomysł dobry, wykonanie zazwyczaj złe)
- Pomysł: **informatyka śledcza**, dostajemy obraz dysku albo zrzut ruchu sieciowego i mamy z niego wyciągnąć "dowód", czyli flagę. Brzmi dobrze, ale w praktyce kończy się na zgadywaniu, użyciu binwalka albo odpakowywaniu 100 warstw zipów. Dla uczciwości: niektórzy lubią tę kategorię.

Steganografia

- Nasza ocena kategorii: 0/10



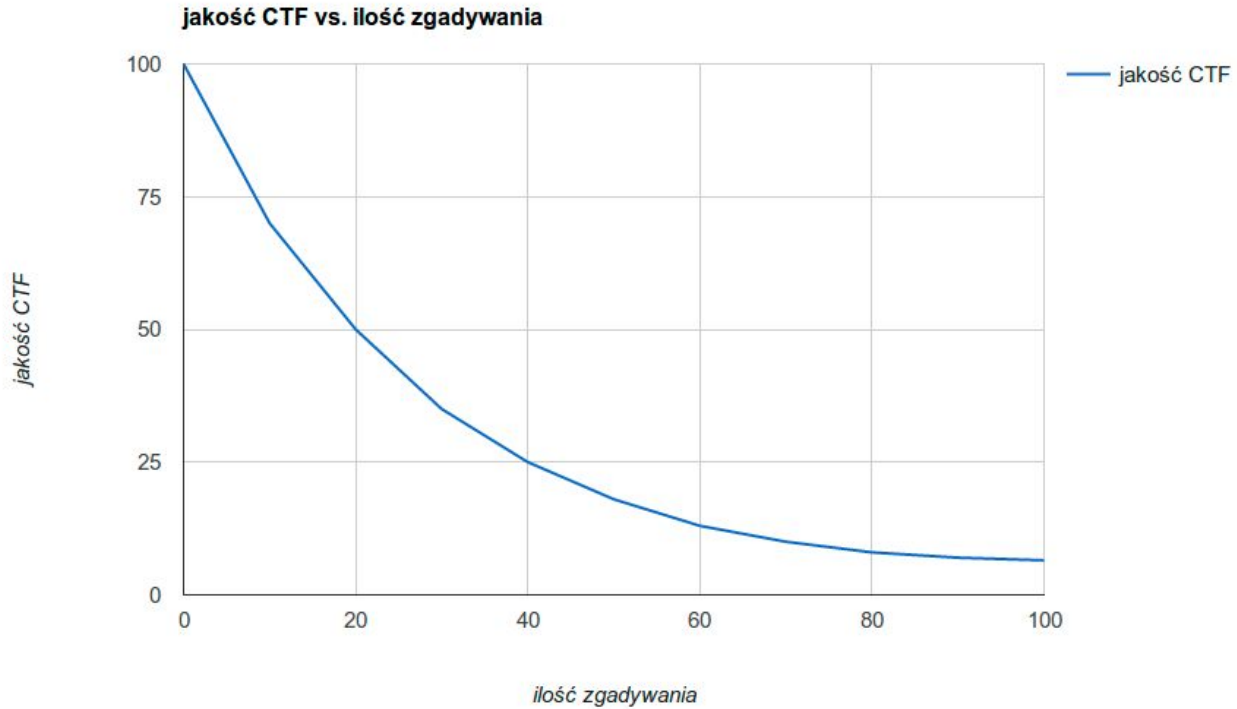
- **Nie**.



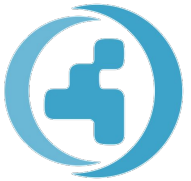
Dygresja: dobre CTFy, kategorie, zadania

- Naukowy wykres:

  Jakość CTF vs ilość zgadywania



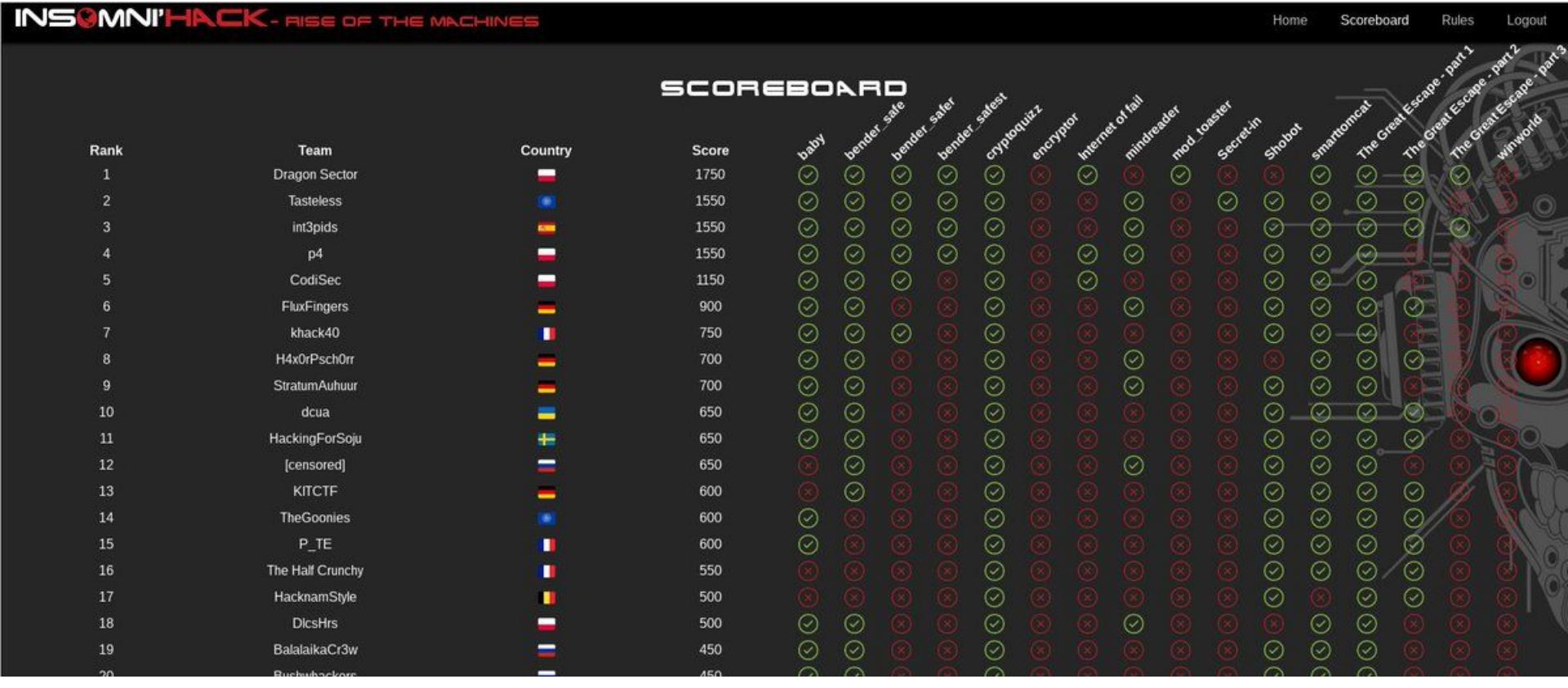
Attack-Defense



- Każda drużyna dostaje identyczną infrastrukturę z pewnymi usługami.
- Usługi mają dziury.
- Trzeba je:
  - znaleźć,
  - naprawić u siebie,
  - wykorzystać u innych i ukraść flagę.

Jak wygląda CTF?

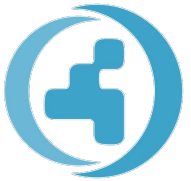
Online



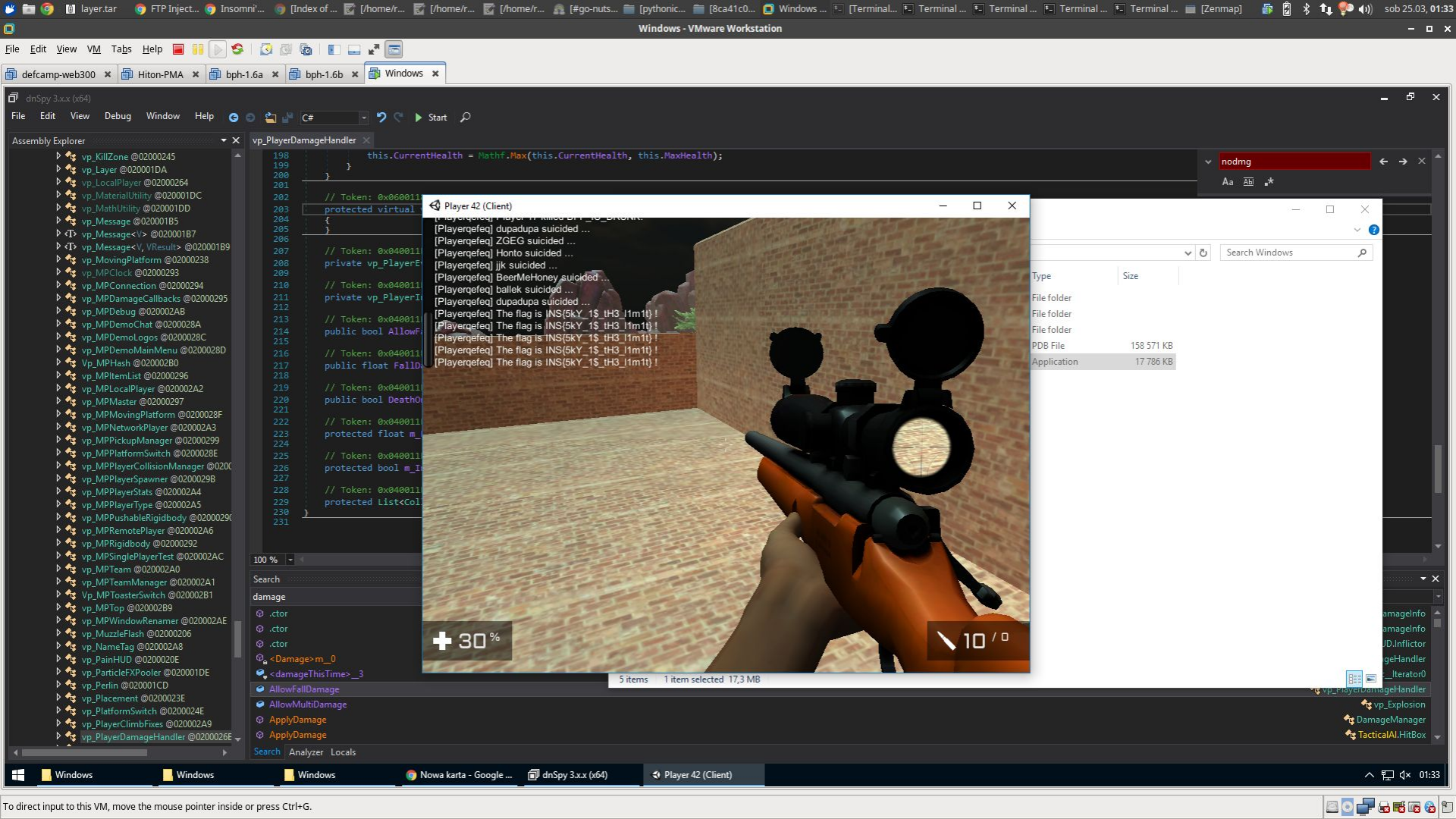
Rank	Team	Country	Score	baby	bender_safe	bender_safer	bender_safest	cryptoquizz	encryptor	Internet of fail	mindreader	mod_toaster	Secret-in	Shobot	smarttomcat	The Great Escape - part 1	The Great Escape - part 2	The Great Escape - part 3	winworld
1	Dragon Sector		1750	✓	✓	✓	✓	✓	✗	✓	✗	✓	✗	✗	✓	✓	✓	✓	✓
2	Tasteless		1550	✓	✓	✓	✓	✓	✗	✗	✓	✗	✓	✓	✓	✓	✓	✓	✗
3	int3pids		1550	✓	✓	✓	✓	✓	✗	✗	✓	✗	✗	✓	✓	✓	✓	✓	✗
4	p4		1550	✓	✓	✓	✓	✓	✗	✓	✓	✗	✗	✓	✓	✓	✗	✗	✗
5	CodiSec		1150	✓	✓	✓	✗	✓	✗	✓	✗	✗	✗	✓	✓	✓	✗	✗	✗
6	FluxFingers		900	✓	✓	✗	✗	✓	✗	✗	✓	✗	✗	✓	✓	✓	✓	✗	✗
7	khack40		750	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗	✓	✓	✓	✗	✗	✗
8	H4x0rPsch0rr		700	✓	✓	✗	✗	✓	✗	✗	✓	✗	✗	✗	✓	✓	✓	✗	✗
9	StratumAuhuur		700	✓	✓	✗	✗	✓	✗	✗	✓	✗	✗	✓	✓	✓	✗	✗	✗
10	dcua		650	✓	✓	✗	✗	✓	✗	✗	✗	✗	✗	✓	✓	✓	✓	✗	✗
11	HackingForSoju		650	✓	✓	✗	✗	✓	✗	✗	✗	✗	✗	✓	✓	✓	✓	✗	✗
12	[censored]		650	✗	✓	✗	✗	✓	✗	✗	✓	✗	✗	✓	✓	✓	✗	✗	✗
13	KITCTF		600	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✓	✓	✓	✓	✗	✗
14	TheGoonies		600	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✓	✓	✓	✓	✗	✗
15	P_TE		600	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✓	✓	✓	✓	✗	✗
16	The Half Crunchy		550	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✓	✓	✓	✓	✗	✗
17	HacknamStyle		500	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✓	✗	✓	✓	✗	✗
18	DIcsHrs		500	✓	✓	✗	✗	✓	✗	✗	✓	✗	✗	✗	✓	✓	✗	✗	✗
19	BalalaikaCr3w		450	✓	✓	✗	✗	✓	✗	✗	✗	✗	✗	✓	✓	✓	✗	✗	✗
20	Bushwhackers		450	✓	✓	✗	✗	✓	✗	✗	✗	✗	✗	✓	✓	✓	✗	✗	✗

Onsite


You are still the impossibility



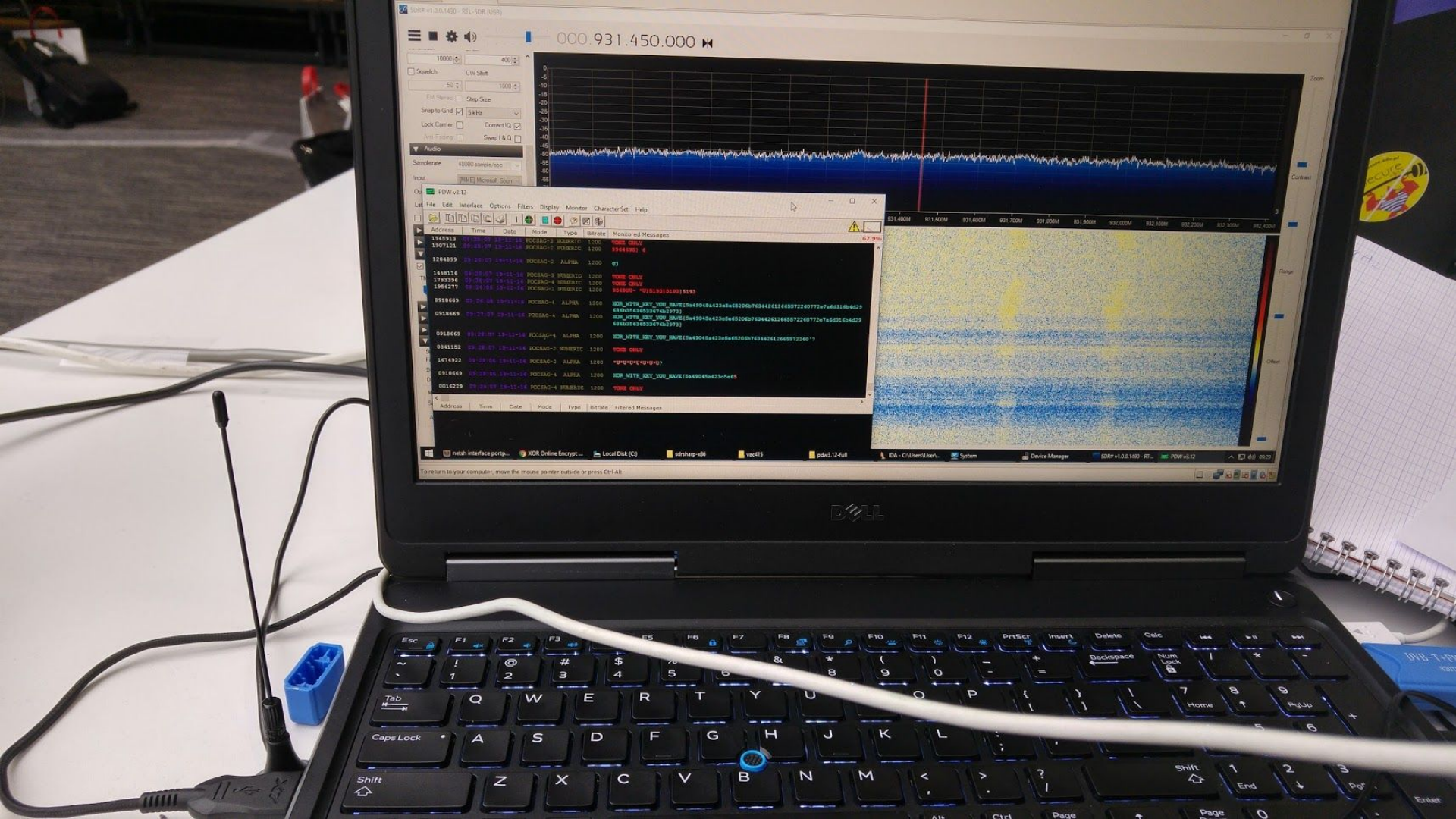
Niestandardowe zadania

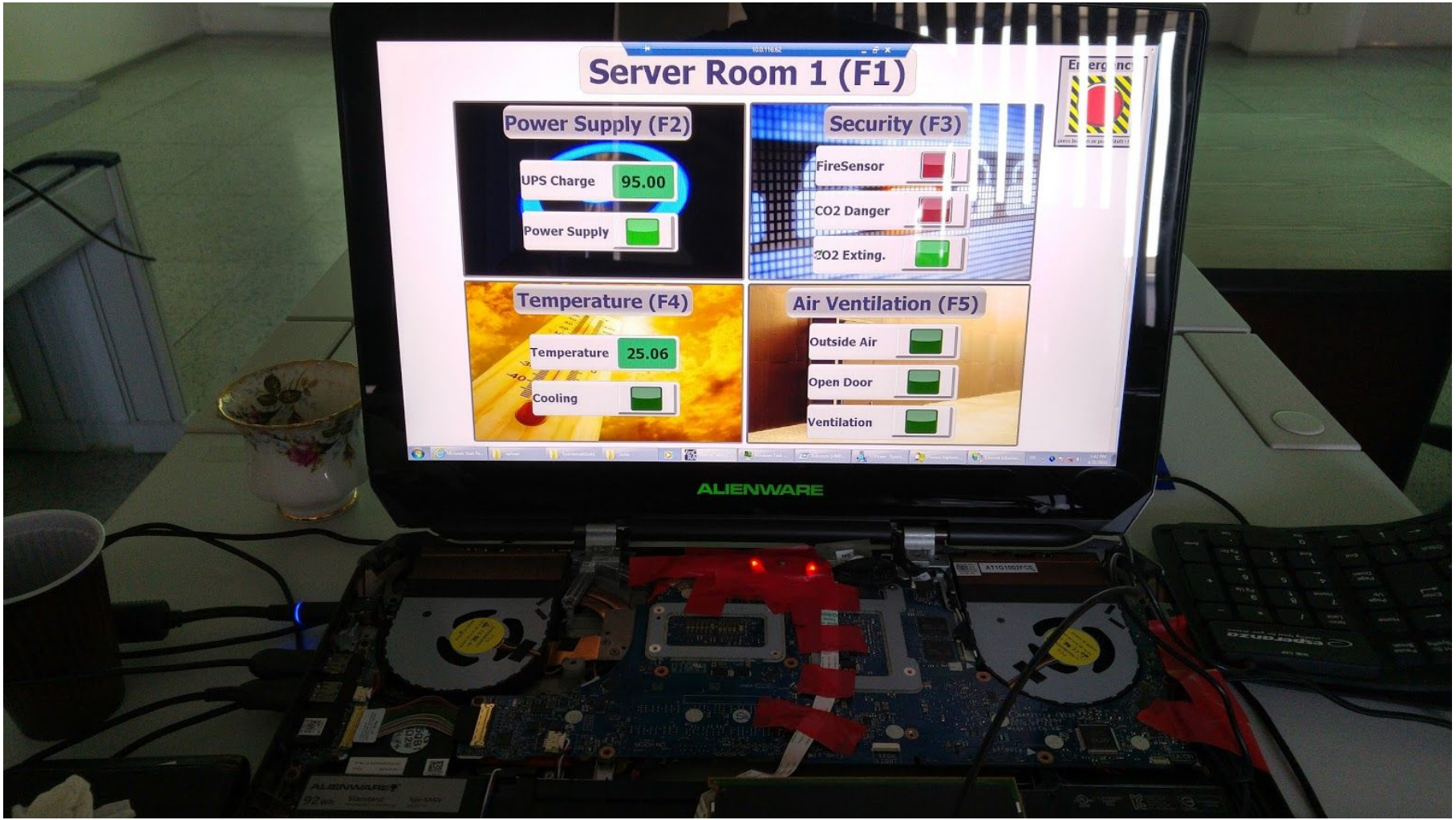

Windows - VMware Workstation
dnSpy 3.x.x (x64)
Assembly Explorer
vp_PlayerDamageHandler
Player 42 (Client)
[Playerqefeq] dupadupa suicided ...
[Playerqefeq] ZGEG suicided ...
[Playerqefeq] Honto suicided ...
[Playerqefeq] jjk suicided ...
[Playerqefeq] BeerMeHoney suicided ...
[Playerqefeq] ballek suicided ...
[Playerqefeq] dupadupa suicided ...
[Playerqefeq] The flag is INS{5kY_1$_tH3_l1m1t} !
[Playerqefeq] The flag is INS{5kY_1$_tH3_l1m1t} !
[Playerqefeq] The flag is INS{5kY_1$_tH3_l1m1t} !
[Playerqefeq] The flag is INS{5kY_1$_tH3_l1m1t} !
30 %
10 / 0
nodmg
Search Windows
Type
Size
File folder
File folder
File folder
PDB File 158 571 KB
Application 17 786 KB
5 items 1 item selected 17,3 MB
damage
AllowFallDamage
AllowMultiDamage
ApplyDamage
ApplyDamage
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Snow Down
Kill the terror of the Snowpocalypse
AngryBear
Bear
Bear
100
0


Unbearable
Open the treasure chest
Angry Bear
Angry Bear
Bear
Bear
Bear
Press 'F' to Crack Chest
100
5
Angry Bear
Angry Bear


Unbearable
Open the treasure chest
1:27
We support the right to arm bears
Angry Bear
Bear
Bear
Bear
Bear
100
1


000.931.450.000
PDW v3.12
DELL


Server Room 1 (F1)
Power Supply (F2)
UPS Charge
95.00
Power Supply
Security (F3)
FireSensor
CO2 Danger
CO2 Exting.
Temperature (F4)
Temperature
25.06
Cooling
Air Ventilation (F5)
Outside Air
Open Door
Ventilation
ALIENWARE

Ciemna strona regexów, lvl 1/8

Please match string that contains "select" as a case insensitive subsequence.

Odpowiedź?

```
(?i)s.*e.*l.*e.*c.*t
```

Proste?

Ciemna strona regexów, lvl 2/8

Hmm?

Match a^nb^n

What is the regular expression for the grammar $A^n B^n$?

2 Answers

Sabhya Kaushal, considers Red to be the new Blue.
Updated Feb 14, 2016

Let's start with some background, shall we?

$A^n B^n$ is an example (and a famous one) of a non-regular language, in which a certain number of As is followed by the same number of Bs, some examples being AB, $AAABBB$ etc. In other words, it is a context-free language that can be generated using the context-free grammar $S \rightarrow ASB|AB$.

Now, what is a non- regular language? Simply put, it's a formal language ***NOT*** expressible using a regular expression.

But why is $A^n B^n$ non- regular? Because the pumping lemma says so. In essence, the

Ciemna strona regexów, lvl 2/8

Match a^nb^n

Ale my nie wiedzieliśmy że to niemożliwe:

^(a\g<1>?b)$

(tak naprawdę, po prostu regexy != wyrażenia regularne z teorii języków i automatów)

Ciemna strona regexów, lvl 3/8

```
x^p
A prime is a natural number greater than 1 that has no positive divisors
other than 1 and itself.
```

?????

Ciemna strona regexów, lvl 3/8

x^p
A prime is a natural number greater than 1 that has no positive divisors other than 1 and itself.

A jednak możliwe:

^(?!(xx+)\1+$)xx+$

Swoją drogą, całkiem sprytna metoda:
negacja regexa matchujący liczby złożone

Ciemna strona regexów, lvl 4/8

Palindrome
Both "QQ" and "TAT" are palindromes, but "PPAP" is not.

?????

Ciemna strona regexów, lvl 4/8

Palindrome
Both "QQ" and "TAT" are palindromes, but "PPAP" is not.

I znowu możliwe:

```
^((.)\g<1>?\2|.?)$
```

Rekursywne grupy w wyrażeniu regularnym
to coś co na pewno przyda się pracy
(jeśli bardzo nie lubicie kolegów z pracy)

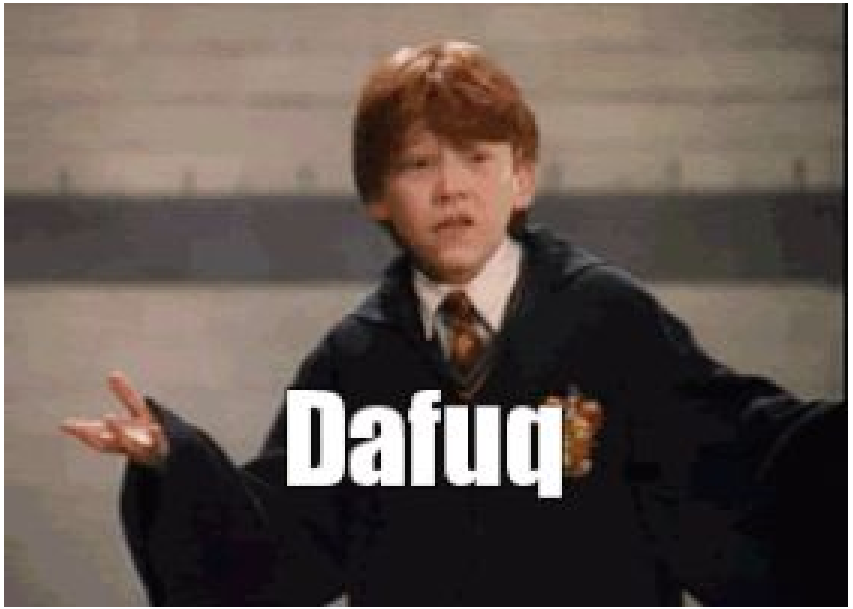
Ciemna strona regexów, lvl 5/8

a^nb^nc^n

Is CFG too easy for you? How about some context SENSITIVE grammer?

?????

Ok, to już na pewno niemożliwe



Ciemna strona regexów, lvl 5/8

a^nb^nc^n
Is CFG too easy for you? How about some context SENSITIVE grammer?

A jednak:

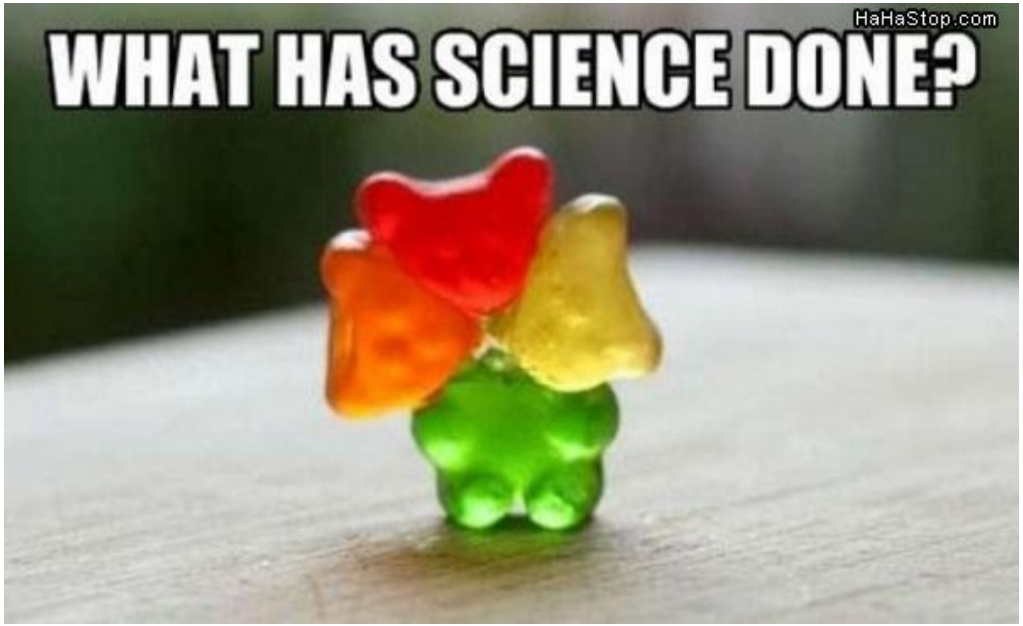
```
^(?=(a\g<1>?b)c)a+(b\g<2>?c)$
```

Już nawet nie pamiętam co ten regex robił.
Ale działa.

Ciemna strona regexów, lvl 7/8

Regex matchujący tylko lata przestępne

Czy to już nie przesada?



Ciemna strona regexów, lvl 7/8

Regex matchujący tylko lata przestępne

```
(?!^0\d)(^\d*((((^|0|[2468])[048])|[13579][26])00$)|^\d*((0[48]|(^0*|[2468])[048]|[13579][26]))$)
```

(Dokładnie tak sprawdzam czy rok jest przestępny)

Ciemna strona regexów, lvl 8/8

Regex matchujący wielokrotności liczby 42

Ciemna strona regexów, lvl 8/8

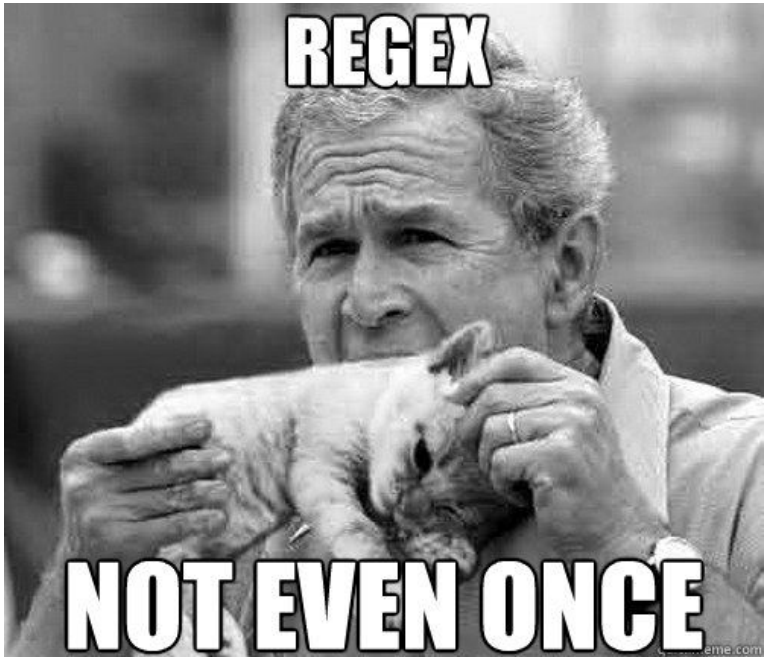
Regex matchujący wielokrotności liczby 42

```
^(?=^-?(\d*[02468])$)(?=^-?((?
!$)(?>(|(?<Y>[147]\g<X>|[0369]
 \g<Y>|[258]\g <Z>))(|(?<Z>[25
8]\g<X>|[147]\g<Y>|[0369]\g<Z>
 )))(?<X>[0369]\g<X>|[258]\g<
Y>|[147]\g<Z>|$))$)(?=^-?((?!$
```

```
)(?>(|(?<B>4\g<A>|5\g<B>|6\g<C
>|[07]\g<D>|[18]\g<E>|[29]\g<F
>|3\g<G>))(|(?<C>[18]\g<A>|[29
]\g<B>|3\g<C>|4\g<D>|5\g<E>|6\
g<F>|[07]\g<G>))(|(?<D>5\g<A>|
6\g<B>|[07]\g<C>|[18]\g<D>|[29
]\g<E>|3\g<F>|4\g<G>))(|(?<E>[
29]\g<A>|3\g<B>|4\g<C>|5\g<D>|
```

```
6\g<E>|[07]\g<F>|[18]\g<G>))(|(?
<F>6\g<A>|[07]\g<B>|[18]\g<C>|[2
9]\g<D>|3\g<E>|4\g<F>|5\g<G>))(|
(?<G>3\g<A>|4\g<B>|5\g<C>|6\g<D>
|[07]\g<E>|[18]\g<F>|[29]\g<G>))
)(?<A>$|[07]\g<A>|[18]\g<B>|[29]
\g<C>|3\g<D>|4\g<E>|5\g<F>|6\g<G
>))$)-?(0|[1-9]\d *)$
```

Ciemna strona regexów, lvl 8/8



Wniosek A: na CTF są zadania bardziej i mniej praktyczne
Wniosek B: można się nauczyć rzeczy których samemu nigdy by się nie ruszyło

Nagrody

Są, ale:

- raczej jako miły dodatek
- pokrycie części kosztów podróży
- czasem nagrodą jest t-shirt
- (są pewne wyjątki)

Ale z roku na rok jest lepiej!


Second place
¥300,000
Trend Micro CTF 2016
RS
aspberry Pi 3


Trend Micro CTF 2016
The Final
November 19-20, 2016
Tokyo, Japan
Presented by
TREND MICRO
Second place
¥300,000
Trend Micro CTF 2016


KR-03-0164
CONFIDENCE
CTF
5.000 PLN
19-20 V 2016 KRAKOW
PROGRAM REGIONALNY
PLAZA KRAKOW
Projekt współfinansowany przez Unię Europejską
w ramach Małopolskiego Regionalnego
Programu Operacyjnego na lata 2007-2013

WCTF 2016 (Belluminar Beijing) is an international CTF hacking contest cosponsored by 360Vulcan Team and PoC Security. WCTF 2016 will be held June 1-3rd, 2016 at Crowne Plaza Beijing Lido Hotel & Resort in Chaoyang District, Beijing.

Ten of world top CTF hacking teams including the ones in China are invited to battle for a total bonus of USD 100000. The top three teams of WCTF will be awarded with USD 50,000, USD 30,000 and USD 20,000 respectively.

$2.75m 1. miejsce
$1.75m 2. miejsce
$1.5m 3. miejsce
$0.75m 4-7 miejsca

Drużyny CTFowe

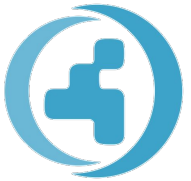
Dlaczego lepiej w zespole?

- Razem raźniej!
- Zróżnicowanie umiejętności
- Zróżnicowane ulubione kategorie
- Szybsza nauka/brainstorming
- Wspólna motywacja (bardzo ważne!)
- Lepsze wyniki (do pewnej ilości osób)

Czym jest właściwie zespół

- Grupa 8-12 osób
  - choć czasem są 2 albo 30
  - najlepiej o zróżnicowanych umiejętnościach, choć częściowo pokrywających się
- 1-2 team-leaderów (sprawy organizacyjne, etc)
- Narzędzia do wspólnej pracy
  - **Czat** (Slack, self-hosted Mattermost, Rocket Chat, IRC, etc)
  - **Wymiana kodu, plików** (Slack, Google Drive)
  - **Arkusz organizacyjny per CTF** (Google Sheet)

Rodzaje zespołów



- Akademickie
  - całe wydziały, roczniki, koła naukowe
  - **PPP** - Carnegie Mellon (kilkukrotnie mistrzowie świata)
  - **Just Hit The Core** - Akademia Górniczo-Hutnicza
- Firmowe
  - **Codisec** - Codilime
  - **DeliciousHorse** - (początkowo) ESET
- Ogólne (internetowe / lokalne - hackerspace'y)
  - mniej lub bardziej narodowe, czasem międzynarodowe
  - **Dragon Sector** (aktualnie najlepszy polski zespół)
  - **p4** (to my!)

Światowy ranking z 2016 roku

Place	Team	Country	Rating
1	dcua		1625.714
2	Dragon Sector		1435.461
3	LC↯BC		1419.805
4	Plaid Parliament of Pwning		1419.410
5	p4		1138.729
6	217		1088.393
7	TokyoWesterns		882.254
8	Tasteless		874.920
9	0daysober		850.763
10	Eat, Sleep, Pwn, Repeat		780.327

Polskie zespoły w 2016

Position	Country position	Name	Points
2	1	Dragon Sector	1435.461
5	2	p4	1138.729
20	3	Snatch The Root	515.628
29	4	DeliciousHorse	392.655
37	5	CodiSec	333.137
61	6	Just Hit the Core	231.320
72	7	Raccoons	191.333
94	8	Shady Hats	151.908


Carnegie Mel
SCHOOL OF COMPUTER SCI
1337
1970


ZuriHac
2015
INSOMNIHACK
CTF WINNER

Dlaczego warto?

- **Nauka!**
- Zdobycie doświadczenia.
  - Dobre wyniki w CTF można wpisać do CV!
  - Grają wszyscy - i licealiści i najlepsi specjaliści w branży
- Fajna zabawa i rywalizacja.

- Podróże, poznawanie ludzi i branży.

Trzeba jednak pamiętać, że:

- Zadania na CTFach nie są bezpośrednim przełożeniem tego, co specjalista IT security robi na co dzień w pracy.
- Czym więcej gramy w CTFy tym.. lepiej gramy w CTFy.

- Ale część umiejętności i podejście do rozwiązywania problemów **mogą** nam pomóc w pracy!
- Czy mówiliśmy już, że to super zabawa?
    - skutki uboczne: zmęczenie, uzależnienie od kawy, wątroba zniszczona energetykami, irytacja.


CERT.PL
551788


JAPAN CUP
TOKYU
SHIBUYA community bus HACHIKO

Jak zacząć?

Można...

Założyć team

- minimum to druga zmotywowana osoba
- kilka osób z uczelnianego koła naukowego? najprościej!

Dołączyć do teamu

- część drużyn prowadzi okresowo rekrutacje
- szukać (IRC, twitter) i pytać!

Trzeba...

Ćwiczyć:

- https://www.root-me.org/en
- https://www.wechall.net/
- https://www.enigmagroup.org/
- https://www.tdhack.com/
- http://crackmes.de/ ['']
- prawdziwe CTFy w weekendy
  - https://ctftime.org

Czytać/oglądać:

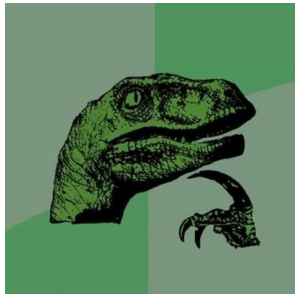
- https://www.youtube.com/user/GynvaelColdwind
- https://github.com/p4-team/ctf/
- https://github.com/ctfs

Jeździć na:

- CONFidence
- Security BSides Warsaw
- PWNing
- SECURE

Praca?

Nie chcę pracować w IT security
i jestem **programistą**



Po co mi wiedza o security?

Ponieważ,

- nie będziemy popełniać błędów bezpieczeństwa w swoich programach,
- będziemy na pierwszy rzut oka rozpoznawać już istniejące błędy bezpieczeństwa,

- lepiej wygląda CV,
- bezpieczeństwo jest ciekawe!

Nie chcę pracować w IT security
i jestem **administratorem**

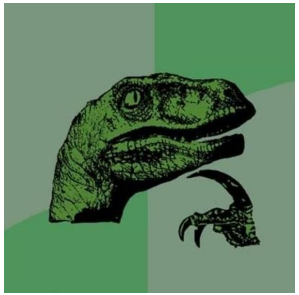
Po co mi wiedza o security?

Ponieważ,

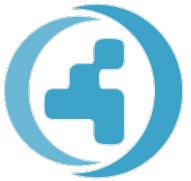
- monitoring zagrożeń jest coraz ważniejszy,
- znając zagrożenia możemy je lepiej wykrywać i analizować,

- lepiej wygląda CV,
- bezpieczeństwo jest ciekawe!

Uczę się **programować** od roku / dwóch / dziesięciu lat



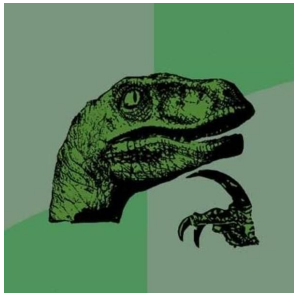
Czy jest sens zaczynać **karierę** w security?



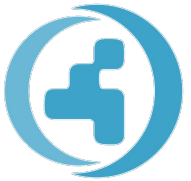
- Ludzie mający dużą wiedzę z programowania mają prostszy start.
  - doświadczenie w programowaniu się nie marnuje
  - "myślenie jak programista" to cenna umiejętność, bo często szukamy błędów w kodzie programistów

- Wiedza z bezpieczeństwa w połączeniu ze specyficznymi technologiami to bardzo duże zarobki, np. bezpieczeństwo ICS/SCADA.

Jestem **administratorem** i nie umiem programować



Czy jest sens zaczynać **karierę** w security?



- Ludzie z doświadczeniem administrowania sieciami oraz systemami stanowią dużą część specjalistów IT security.
  - większość administratorów prędzej czy później styka się z bezpieczeństwem
  - wiele zagrożeń to właśnie część sieciowa / systemowa

- Doświadczenie w zapobieganiu zagrożeniom pomaga je lepiej analizować (i vice-versa).

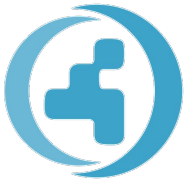
Czyli dlaczego warto?

- Próba nauki bezpieczeństwa nic nie kosztuje: nie ma nic do stracenia.
- W Polsce (i na świecie) jest teraz coraz większe zapotrzebowanie na specjalistów od bezpieczeństwa.
    - Podobnie jak kilkanaście lat temu było z zapotrzebowaniem na programistów.

- Coraz więcej zagrożeń, coraz więcej skradzionych danych i pieniędzy, **coraz więcej pracy** i coraz większe **zarobki**.
    - Coraz większe wymagania zapewnienia prywatności (również prawne).

No dobra, co właściwie się robi w IT security?

- Najwięcej zależy od firmy oraz branży.
- My na przykład ratujemy świat :).
  - Staramy się wiedzieć jak najwięcej o zagrożeniach w .pl i dzielimy się tą wiedzą (systemy wymiany informacji, blog, szkolenia, konferencje, ćwiczenia).
  - Łagodzimy skutki działalności przestępców.
  - Analizujemy złośliwe oprogramowanie, monitorujemy poczynania przestępców, etc



Co **konkretnie** można robić w security

Bronienie (blue teaming)

- SOC - Security Operations Center
  - monitorowanie systemów
  - korelowanie logów, zdarzeń, alertowanie (to ciekawsze niż może się wydawać)
  - może służyć jako pierwsza praca w IT security

- CERT - Computer Emergency Response Team
  - reakcja na incydenty i koordynacja
  - spojrzenie na bezpieczeństwo z szerszej perspektywy
  - analityka (w tym techniczna, np. złośliwego oprogramowania)
  - wyciąganie wniosków, wydawanie zaleceń, standardów, polityk
  - różne CERTy działają na różnym poziomie - firmy, sektora, kraju

Atakowanie (red teaming / pentesting)

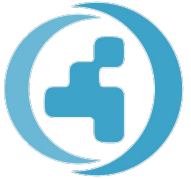
- testowanie zabezpieczeń w całych organizacjach / sieciach
- szukamy luk, wykorzystujemy je i piszemy raport

- na zamówienie bądź wewnątrz własnej firmy

Purple teaming

- Najlepiej mieć doświadczenie zarówno w blue teamingu i red teamingu.

Szukanie podatności w oprogramowaniu



- W ramach programów bug bounty.
- We własnej firmie / organizacji.
- W produktach innych firm.
  - Google *Project Zero*
  - Pwn2Own
  - Zero Day Initiative

Tworzenie produktów IT security

Czyli: antywirusy, zapory sieciowe, systemy monitorujące / detekcji zagrożeń (IDS), zapobiegania zagrożeniom (WAF/IPS), systemy antyfraudowe.

Zadania:

- Opracowywanie metod detekcji.
- Analiza złośliwego oprogramowania.
- Może być sporo fajnego programowania zarówno low- i high-level.

Threat intelligence

Czyli: zbieranie informacji na temat działalności zagrożeń mogących zagrozić firmie / organizacji, przestępców oraz używanych przez nich narzędzi (złośliwe oprogramowanie, spam, maile phishingowe) - ogólnie wszystkiego co dzieje się w sieci.

Zadania:

- Korelowanie informacji w złożony sposób.
- Analiza złośliwego oprogramowania.
- Tworzenie baz danych informacji (i czasem sprzedawanie ich).

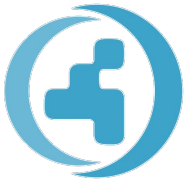
Szerzenie wiedzy

- Prowadzenie szkoleń, warsztatów, kursów.
- Organizowanie ćwiczeń.
- Prowadzenie zajęć na uczelniach.
- Występowanie na konferencjach.
    - Niektórzy już tak zarabiają na życie.

Zarządzanie ryzykiem

- Tworzenie polityk, standardów oraz procedur bezpieczeństwa w organizacjach.
- Przeprowadzanie audytów.
- Doradztwo.
- "Menedżerskie security"

Gdzie można pracować w security



- Właściwie **każda duża firma** w dowolnej branży.
  - Póki co zwłaszcza finansowa oraz IT.
- Firmy z branży IT security :) - rosną jak na drożdżach.

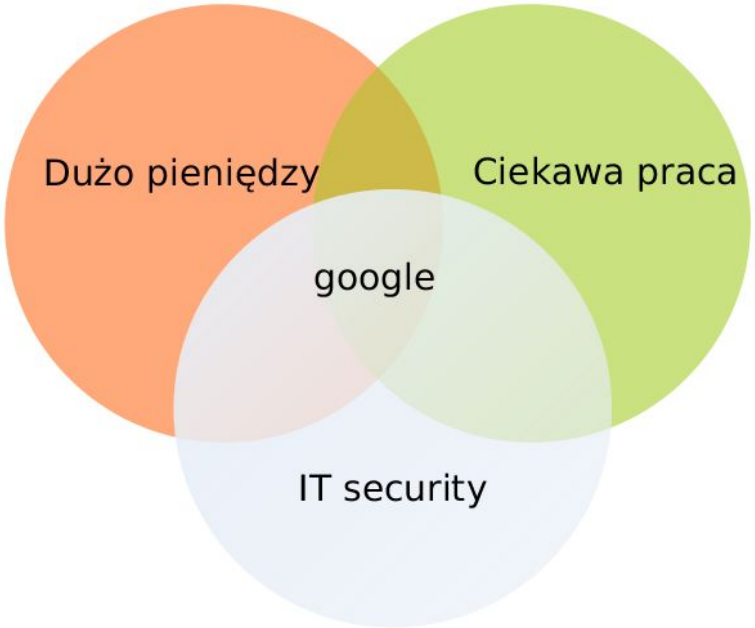
- Administracja publiczna.
  - organy ścigania
  - służby specjalne (w Polsce: Agencja Bezpieczeństwa Wewnętrznego)
  - wojsko (również potrzebuje cywilnych specjalistów)

Gdzie fizycznie można wykonywać pracę

- W Polsce jeszcze właściwie tylko Warszawa i Kraków.
- Jest jeszcze opór w kwestii pracy zdalnej

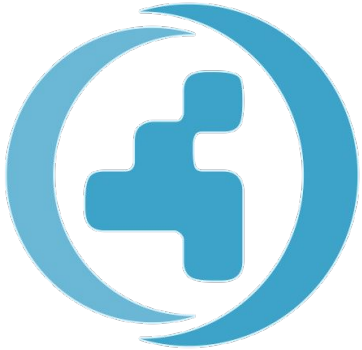
- Ciekawe miejsca za granicą:
  - Szwajcaria
  - UK
  - USA

Rynek pracy IT: diagram Venna



Zaciekawieni?

- 31 marca – 14 kwietnia
- CTF dla początkujących
  - https://**picoctf**.com/



https://p4.team

twitter: @p4_team

https://cert.pl

twitter: @CERT_Polska_en

Mateusz Szymaniec rev@p4.team twitter: @RevToJa

Jarosław Jedynak msm@p4.team twitter: @MsmCode

Link do tej prezentacji: https://goo.gl/MFxfcR