ZAUFANA TRZECIA STRONA.PL

Bezpieczeństwo serwerów

Hasła

Borys Łącki

28.02.2017

ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

Borys Łącki

Od ponad 10 lat wykonując testy penetracyjne, ***testujemy bezpieczeństwo i zabezpieczamy*** *zasoby Klientów.*

LOGICALTRUST

ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

Agenda

1) Incydenty komputerowe
2) Ataki na hasła: online, offline
3) Bezpieczne hasło, menadżery haseł
4) DEMO: ataki online
5) DEMO: atak offline
6) Podsumowanie
7) Sesja pytań od uczestników

Nasza perspektywa

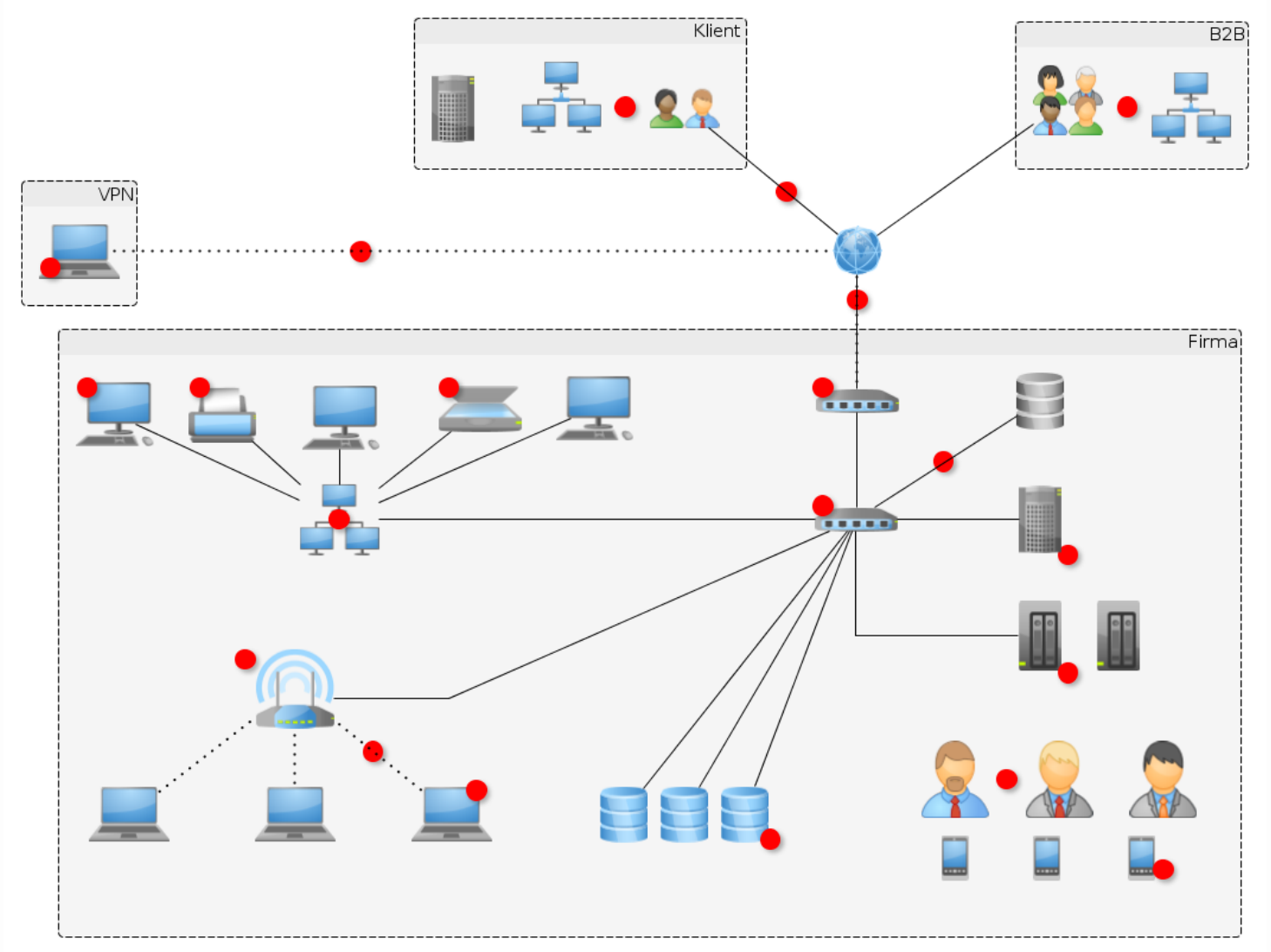
- **Test penetracyjny** – „proces polegający na przeprowadzeniu kontrolowanego ataku na system teleinformatyczny, mający na celu praktyczną ocenę bieżącego stanu bezpieczeństwa (...)”

Wikipedia

ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

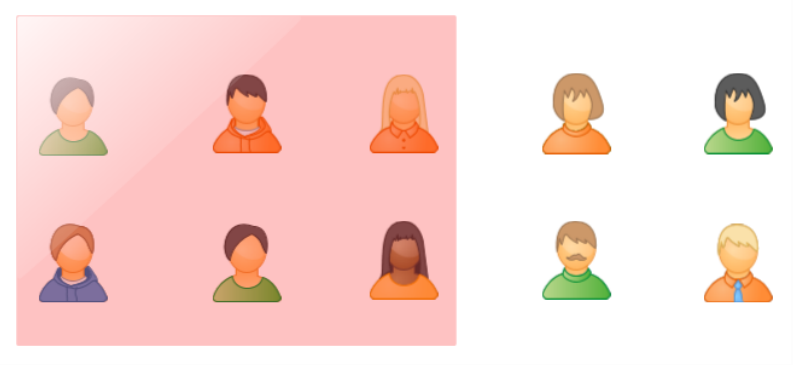
Testy penetracyjne



ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

Testy penetracyjne



PHISHING ~ 60%

ZAUFANA TRZECIA STRONA.PL

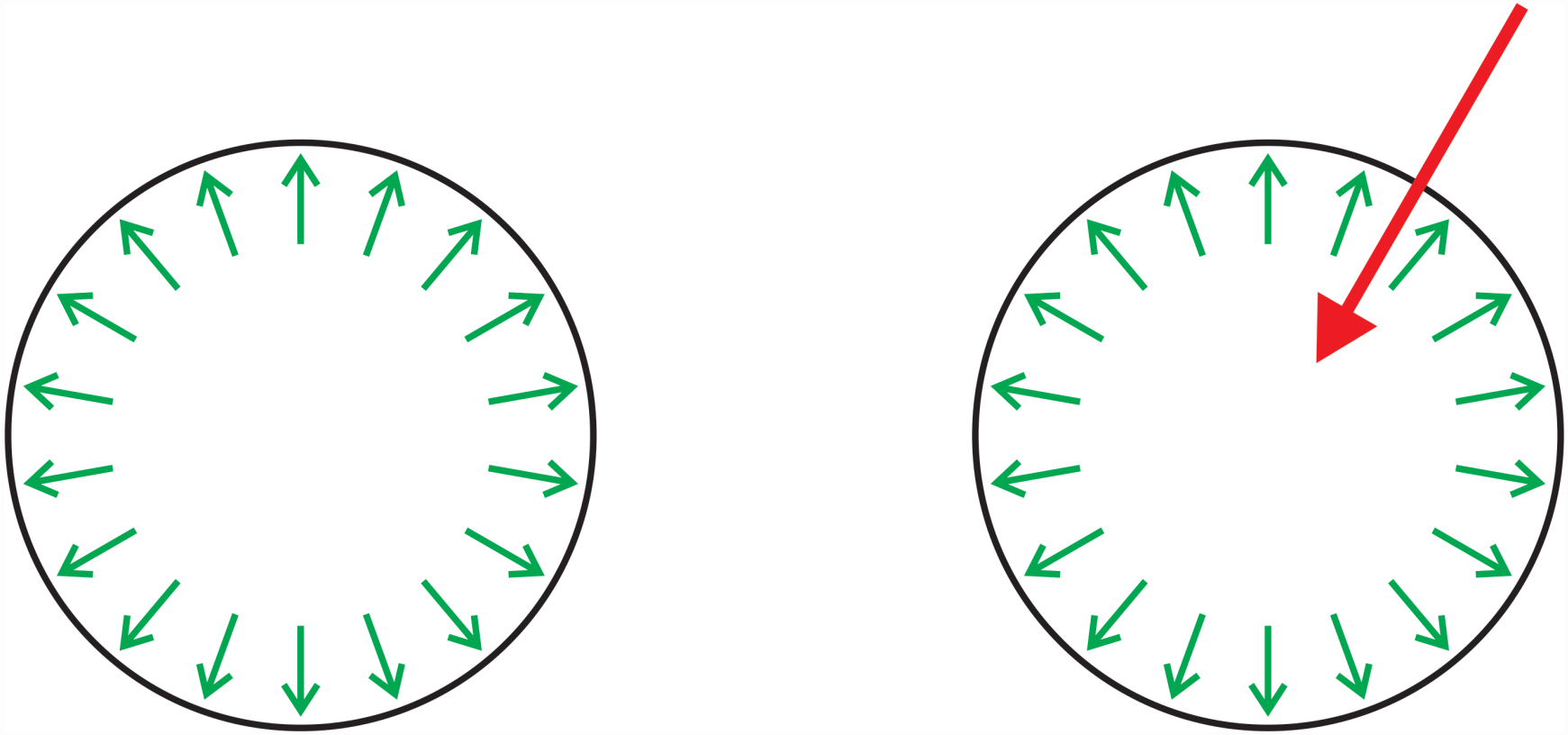
aruba CLOUD

Podatności

ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

Asymetrie i motywacje



ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

Hasło

Hasło – ciąg znaków stosowany powszechnie jako tajny parametr w kryptografii oraz uwierzytelnianiu.

Wikipedia

ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

Hasła - 2016

THE TOP 25 MOST COMMON PASSWORDS OF 2016:

1. 123456
2. 123456789
3. qwerty
4. 12345678
5. 111111
6. 1234567890
7. 1234567
8. password
9. 123123
10. 987654321

ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

Mirai Botnet

DDoS attacks - 1.1 Tbps

ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

Spacja zamiast hasła

Kristoffer was found logging into his fathers Xbox Live account by tapping the space bar into the password field

ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

Stacje benzynowe

5,800 ATGs were found to be exposed to the internet without a password.

ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

TV5

(FRANCE 2)

ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

Syria, Korea Północna

NORTH KOREA

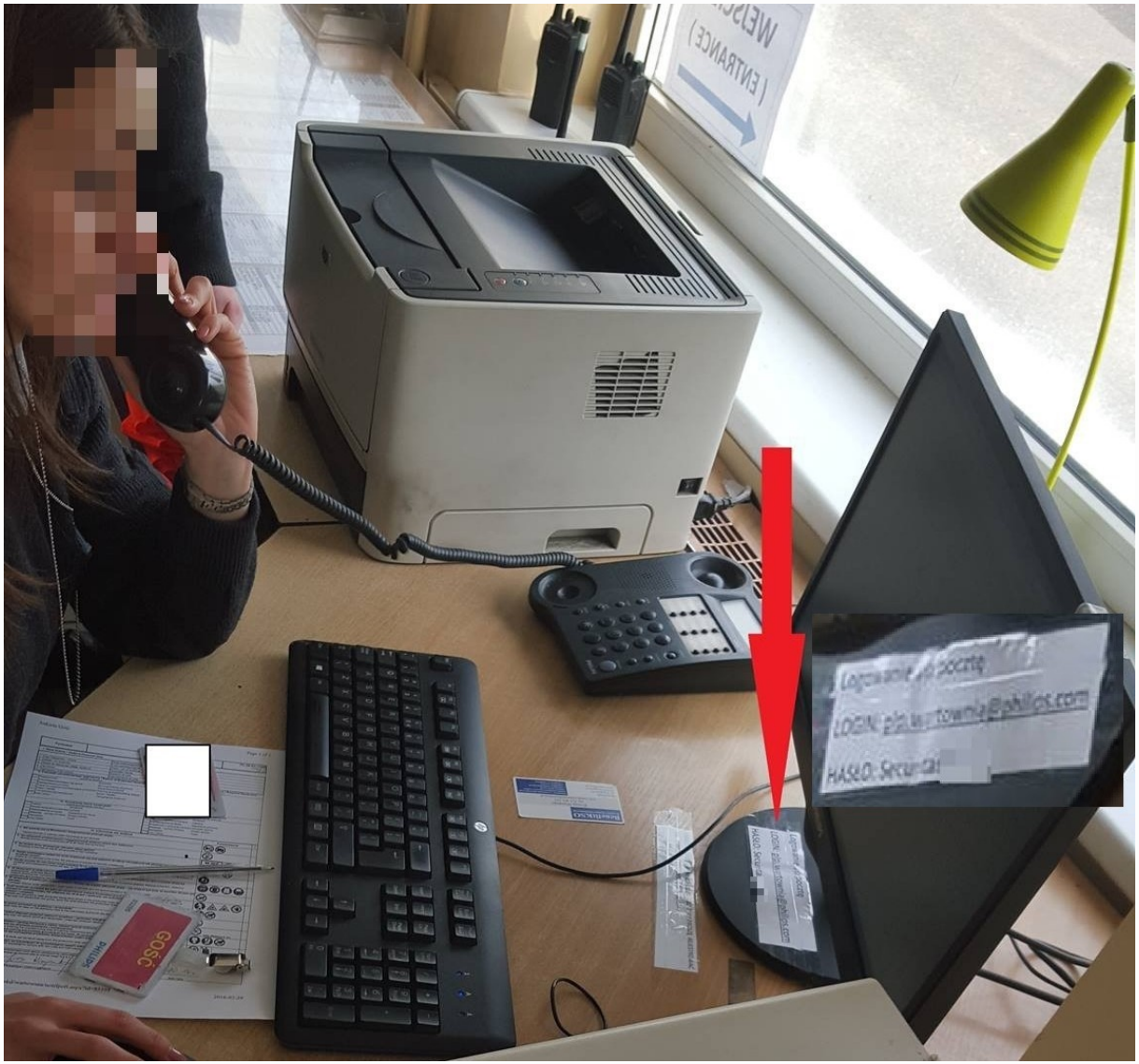
Teen hacks into North Korean Facebook using the password 'Password'

President al-Assad's emails were among 78 other account details from staff members posted on Pastebin by Anonymous, revealing that many of them used two of the worlds least secure passwords: 12345 and 123456.

ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

Philips Lighting Poland



ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

Donald Tusk

ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

Ewa Kopacz

ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

premier.gov.pl

00:32 <@patient> mamy premier.gov.pl

03:21 < GrigoriMaslov> https://www.premier.gov.pl/admin/index.php?do=side&ac=login&id=32%27%20and%201=0%20union%20select%201,uNHex%28Hex%28table_name%29%29,3,5%20FROM%20information_schema.columns--%20and%20%271%27%20=%271

03:22 < GrigoriMaslov> have phun

03:38 < GrigoriMaslov> admin:admin1

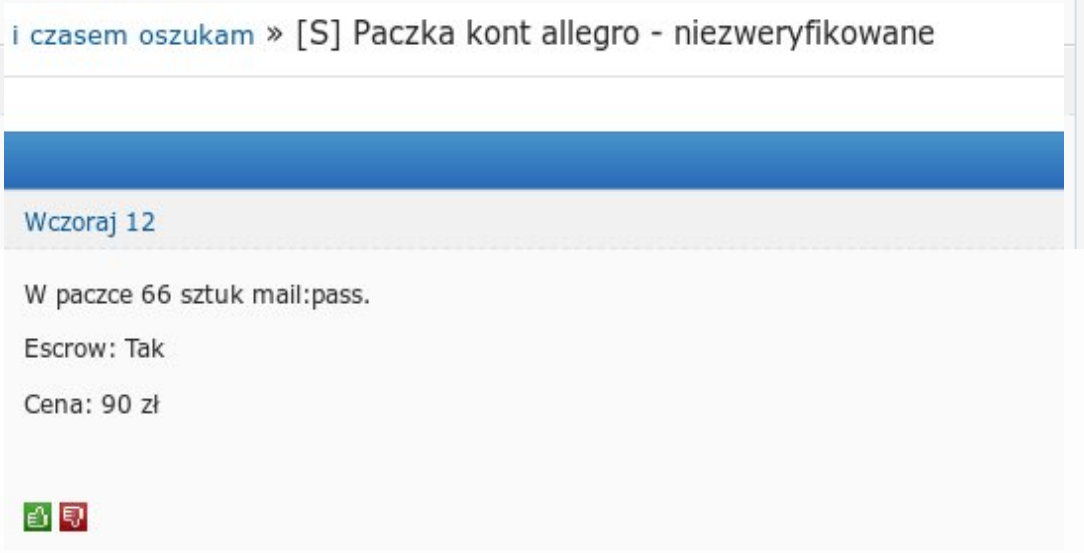
Konta Allegro

Oferuję konta allegro niezweryfikowane, paczka 100 kont (dodaje zawsze kilka więcej) 200 zł w BTC.
Przyjmuję tylko BTC .

"Ponieważ jestem nowym sprzedawcą nalegam wszystkie transakcje ze mną przeprowadzać za pomocą escrow u kogoś zaufanego.
Nie korzystając z escrow narażasz się na wyjebkę z mojej strony.
Jeśli kupujący nie skorzysta z escrow to nie będzie mógł się ubiegać o zadośćuczynienie od sprzedawcy oraz nie będzie miał praw to zakładania sporu "

Dzisiaj 10

Została jeszcze jedna paczka!



ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

Serwery

www. ble.info.pl	24h.pl
Paczka maili	sklep.pl
Baza danych	rolok.pl
357k mail:pass(gmail,yahoo,aol,hotmail)	a.pl
flora.pl	ll.org
Mail;pass	Ruskie maile
Baza danych portalu .pl	ni.pl
Niedawny wyciek bazy danych dużego operatora	4men
Stare bazy danych z PHZ	ns.pl
nbg.info	nos.net

Konta E-mail

Sprzedam paczki mail:pass, konta email (login i haslo), bazy danych (mail, haslo, nick).
Cena w zaleznosci od potrzeb danej osoby

Witam

Nowe paczki na sprzedaz.

Paczki mail:pass zweryfikowane.

1000 rekordow = 200pln

Płatnosc: Only BTC

Zapraszam !!!

Witam. Mam na sprzedaż paczki mail:pass, nowe, nieczesane.

1000rekordów - 150zł w BTC
większe ilości - prv

Płatność tylko w BTC, Pisać na priv, szyfrować(klucz w profilu).

"Ponieważ jestem nowym sprzedawcą nalegam wszystkie transakcje ze
Nie korzystając z escrow narażasz się na wyjebkę z mojej strony.
Jeśli kupujący nie skorzysta z escrow to nie będzie mógł się ubiegać o z
zakładania sporu "

2015-11-06 18

w ramach weryfikacji, dla pierwszych 3 kupujących -50%.

ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

Konta E-mail

Wstawka zawiera dzialajace mail:pass z portalu jak w temacie.

mazdinho@ nis
mpawel@ 365
sylwiuszek@ cin
furmonter@ czek16
janusz.ka33@ da33
arkadiuszklimczyk@ ice1
jacekk00714@ ive1
gabnol@ ola
adrianbol@ ek1
misio@ a11
ziedrzej@ pik
emka00@ lka
nba1234@ a123
sasuke_123-91@ qwww
robert.sudra@ ert
fumagalli@ 15oh
kaczuszkka@ dzia

ZAUFANA TRZECIA STRONA.PL

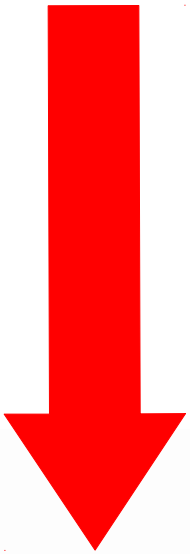
BugBounty - Snapchat

aruba CLOUD

21 #128114 **Administrator access to a Django Administration Panel on *.sc-corp.net via bruteforced credentials**

State	● Resolved (Closed)
Disclosed publicly	July 14, 2016 11:08pm +0200
Reported To	Snapchat
Types	Authentication, Information Disclosure, Privilege Escalation
Bounty	$1,000

Participants



username: admin and password: research

ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

BugBounty – Pornhub

hackerone About Product Resources Contact Directory Blog Try HackerOne Sign in | Sig

131 #72243 **Publicly exposed SVN repository, ht.pornhub.com** Share:

State ● Resolved (Closed) Participants

Disclosed publicly June 26, 2016 12:53am +0200

Reported To Pornhub

Types Authentication, Information Disclosure, Missing Best Practice, Remote Code Execution

Bounty $10,000

Collapse

SUMMARY BY PORNHUB

The researcher accessed a publicly visible .svn repository which enabled him to gave credentials to log into production servers.

TIMELINE

mak submitted a report to Pornhub. Jun 23rd

After I found the subversion repository I visited the following location https://netreact.eu/hubtraffic

I could see the usernames in the repo and the following weak credentials gave me access:

stefan:123456

An attacker can commit code to this location which could be mirrored on the main site and result in full remote code execution. This also has all

ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

Najczęstsze problemy

- Proste hasła
- Te same hasła
- Hasła “na chwilę”

Skuteczność hasła

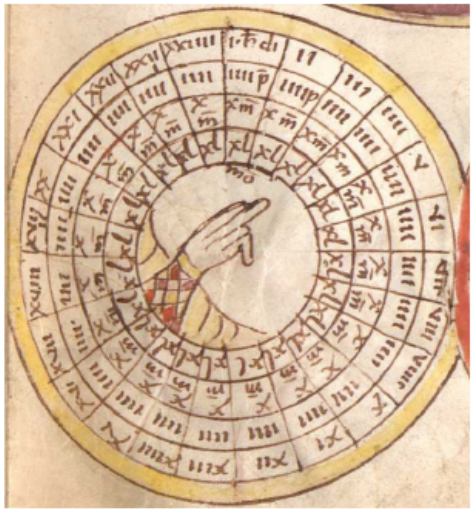
O sile czyli skuteczności hasła decydują:

- jego długość (każdy dodatkowy znak, zwiększa jego użyteczność kilkukrotnie)
- jego losowość (niezgodność ze słownikiem lub znanymi powszechnie wyrażeniami)
- rodzaj użytych znaków (litery, cyfry, znaki specjalne)

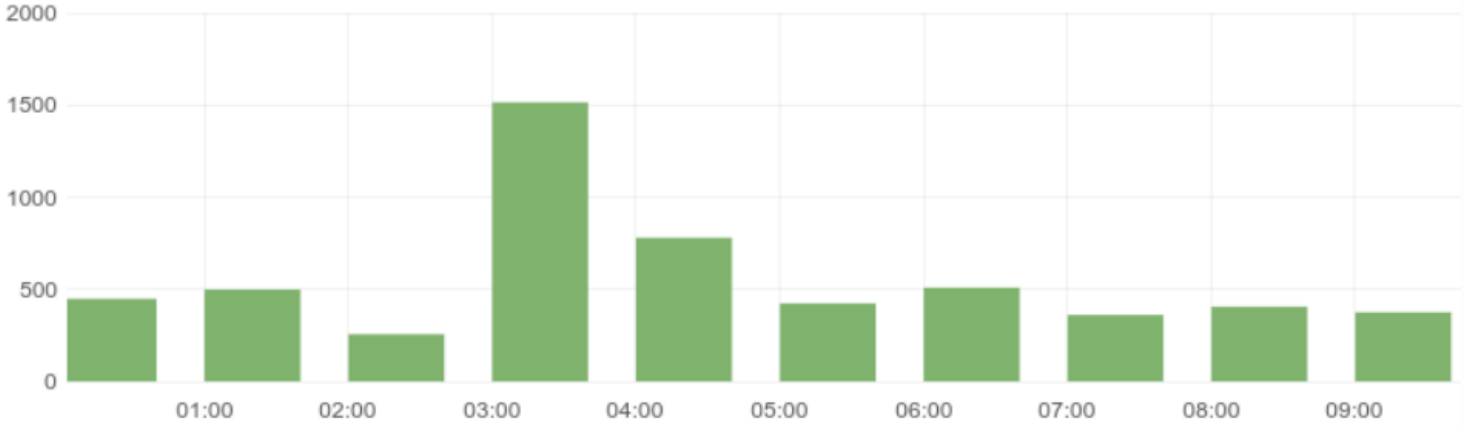
Do tego trzeba dodać starania o tajność hasła.

Hasło „na moment”

Zmienię hasło na ”moment”



- 40 momentów na godzinę (90 sekund)
- co najmniej 256 ataków na godzinę
- ponad 6 prób logowania w „momencie”



Hasła są jak majtki

Hasła są jak majtki – należy je zmieniać często, nie zostawiać na widoku i nie pożyczać obcym.
GIODO

ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

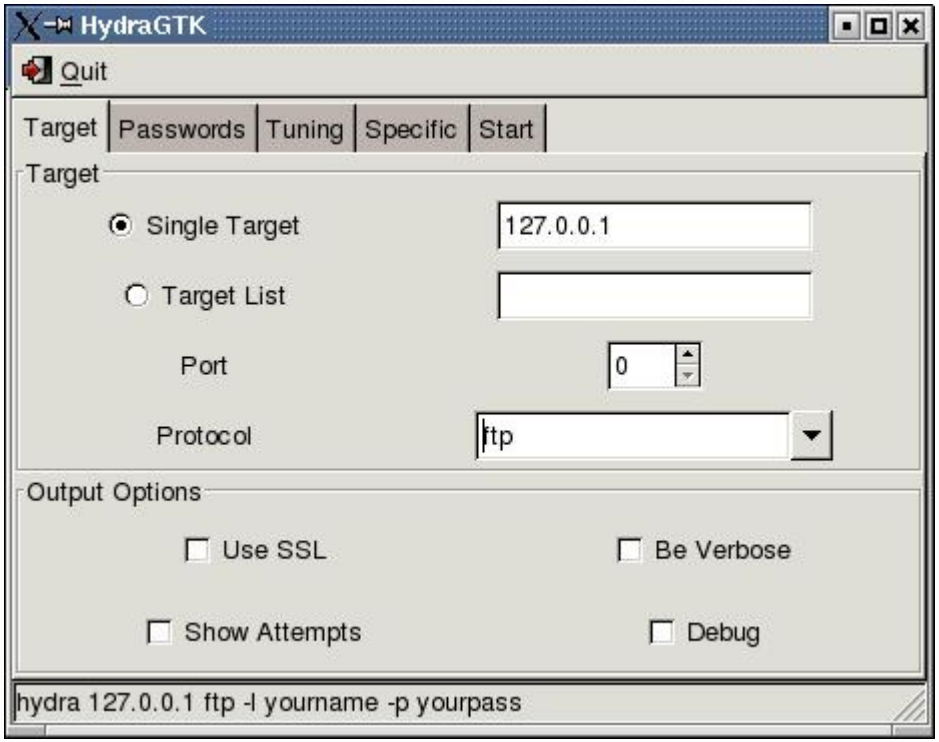
Password reuse

Grupa OurMine przejęła profil założyciela Facebooka na Twitterze i serwisie Pineterest. Włamywacze twierdzą, że hasła poznali dzięki wyciekowi z LinkedIn (hasło Zuckerberga miało brzmieć “dadada”).

ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

Narzędzia




```
root@sf:~/oclHashcat-1.32# ./oclHashcat64.bin -m 8900 -a 3 ?a?a?a?a?a?a?a -n 512 hash

Device #1: Hawaii, 3072MB, 1000Mhz, 44MCU

Hashes: 1 hashes; 1 unique digests, 1 unique salts
Bitmaps: 8 bits, 256 entries, 0x000000ff mask, 1024 bytes
Applicable Optimizers:
* Zero-Byte
* Single-Hash
* Single-Salt
* Brute-Force
Watchdog: Temperature abort trigger set to 95c
Watchdog: Temperature retain trigger set to 80c

SCRYPT tmto optimizer value set to: 2

Device #1: Kernel ./kernels/4098/m08900_1024_1_1_2.Hawaii_1573.4_1573.4 (VM).kernel
Device #1: Kernel ./kernels/4098/markov_le_v1.Hawaii_1573.4_1573.4 (VM).kernel
Device #1: Kernel ./kernels/4098/amp_a3_v1.Hawaii_1573.4_1573.4 (VM).kernel

SCRYPT:1024:1:1:NjM0OA==:TWU9Rx1o8AnB1A7CC/jUoTsLE6RaVZkuLGzDudgdJaA=:gra2020

Session.Name...: oclHashcat
Status.........: Cracked
Input.Mode.....: Mask (?a?a?a?a?a?a?a) [7]
Hash.Target....: SCRYPT:1024:1:1:NjM0OA==:TWU9Rx1o8AnB1A7CC/jUoTsLE6RaVZkuLGzDudgdJaA=
Hash.Type......: scrypt
Time.Started...: Thu Jan 15 15:59:44 2015 (5 mins, 46 secs)
Speed.GPU.#1...:   862.1 kH/s
Recovered......: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.......: 295567360/69833729609375 (0.00%)
Skipped........: 0/295567360 (0.00%)
Rejected.......: 0/295567360 (0.00%)
HWMon.GPU.#1...:  0% Util, 76c Temp, 100% Fan

Started: Thu Jan 15 15:59:44 2015
Stopped: Thu Jan 15 16:05:31 2015
```

ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

Algorytmy haseł

./john .htaccess-crypt
(Traditional DES [128/128 BS SSE2-16])

c/s: 2907K 19 godzin

./john .htaccess-bcrypt
(OpenBSD Blowfish [32/64 X2])

c/s: 1412 > 4 lata

ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

Demo

ZAUFANA TRZECIA STRONA.PL

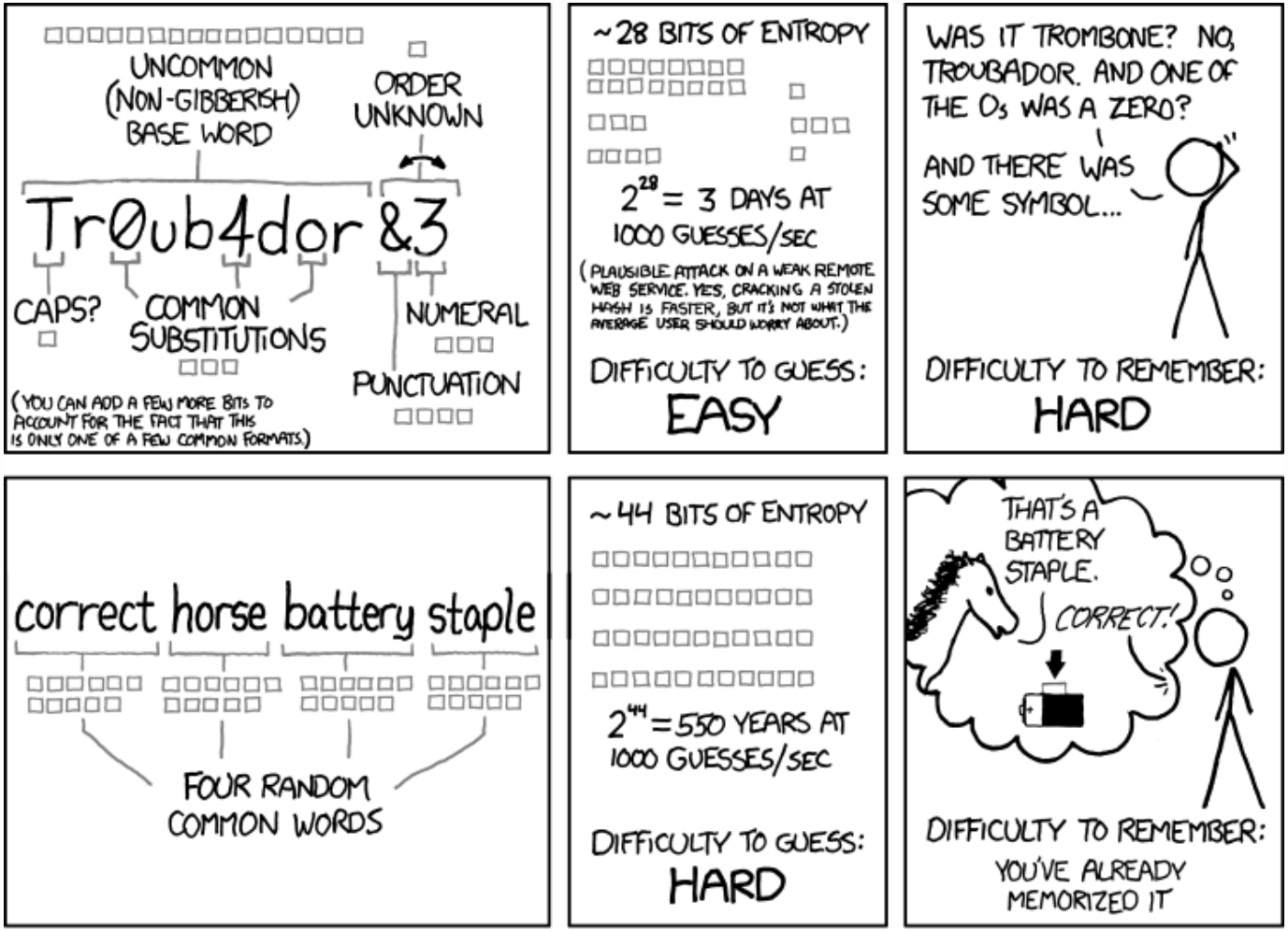
aruba CLOUD

Tworzenie haseł

ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

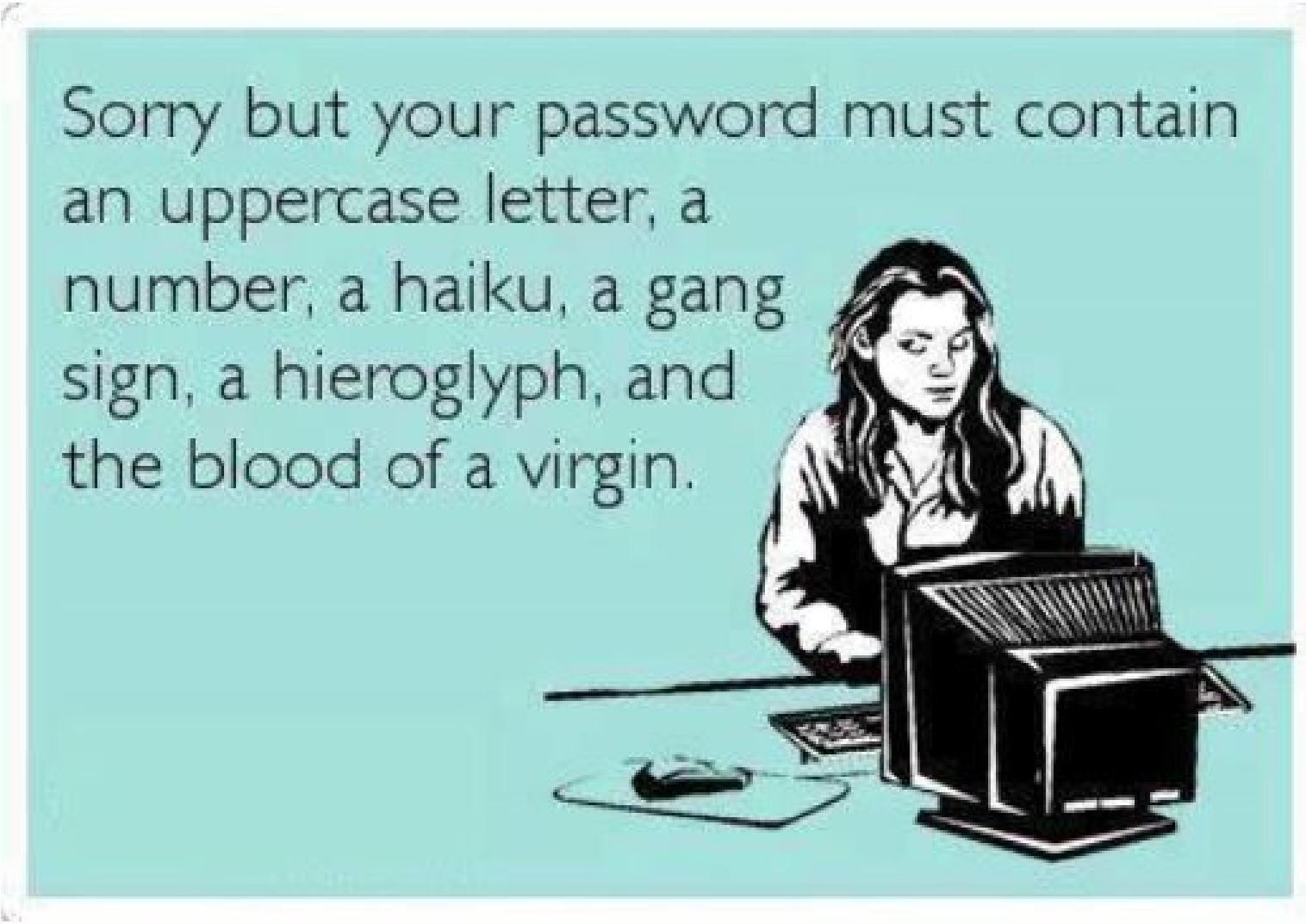
Tworzenie haseł



ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

Menadżery haseł



ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

Menadżery haseł

+ skomplikowane, losowe, różne hasła

+ wygoda

- w wersji online – hasła w chmurze

- złośliwe oprogramowanie

ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

Inne rozwiązania

- 2 Factor Authentication
- One Time Password
- Aplikacja mobilna
- Biometria
- Firewall (Fail2ban, klucze)

ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

Źródła

http://www.huffingtonpost.com/entry/2016-most-common-passwords_us_587f9663e4b0c147f0bc299d

https://zaufanatrzeciastrona.pl/post/a-haslo-zapisujemy-pod-monitorem/

http://www.foxnews.com/tech/2016/06/01/teen-hacks-into-north-korean-facebook-using-password-password.html

http://www.techspot.com/news/47364-anonymous-hacks-syrian-presidents-email-reveals-weak-password.html

https://niebezpiecznik.pl/post/haslo-do-youtuba-bylo-haslem-zhackowanej-francuskiej-telewizji/

https://niebezpiecznik.pl/post/twitter-marka-zuckerberga-przejety/

https://pl.pinterest.com/pin/97671885645540424/

https://xkcd.com/936/

http://www.goodpassword.info/sila_hasla.php

http://www.giodo.gov.pl/259/id_art/7321/j/pl

https://pixabay.com/

https://www.malwaretech.com/2016/10/mapping-mirai-a-botnet-case-study.html

https://zaufanatrzeciastrona.pl/post/internet-zbiornikow-z-paliwem/

https://freedomhacker.net/2014-04-5-year-old-finds-vulnerability-in-microsoft-xbox-password-system/

ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

Szkolenia – rabat

https://z3s.pl/szkolenia/

Atak i obrona:

- **Bezpieczeństwo aplikacji WWW**
- **Bezpieczeństwo aplikacji mobilnych**

-10%

Obowiązuje 10 dni

Hasło: 3d92b6f0

ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

Pytania

Dziękuję za uwagę

Borys Łącki

b.lacki@logicaltrust.net