Kterak hackúvati

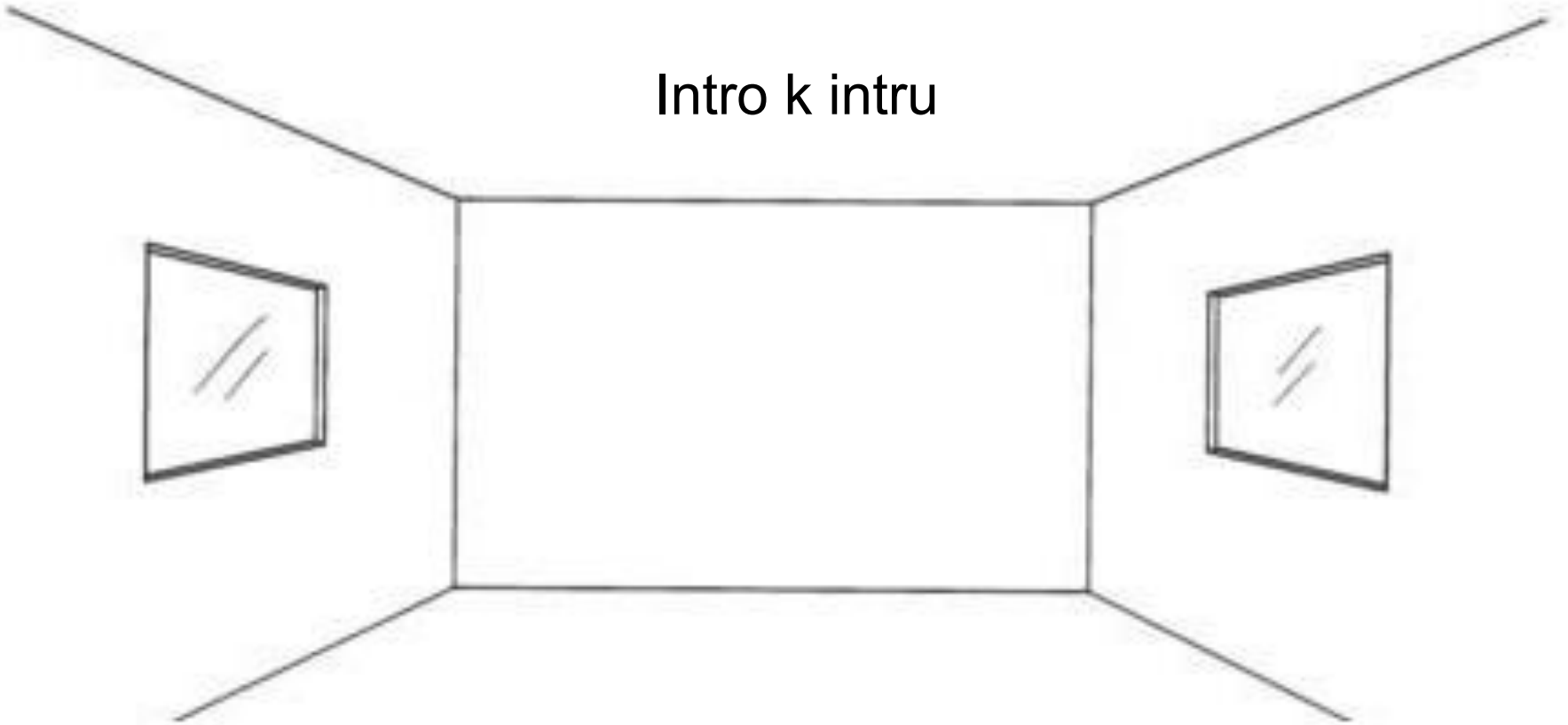
A quick how-to

WTF Hrobky?

- GJH, MatFyz
- Admin (2004 - 2010)
- Vyučujúci (Informatika, Počítačové Systémy)
- Tempest, Telekom

Upratovanie prázdnej izby

Intro k intru



Upratovanie prázdnej izby

- Zbytočné samoupresňujúce prvoprednáškové kecy
  - Sme na strednej škole
  - Nemáme čas
  - Hlavne prakticky a nepresne ;)

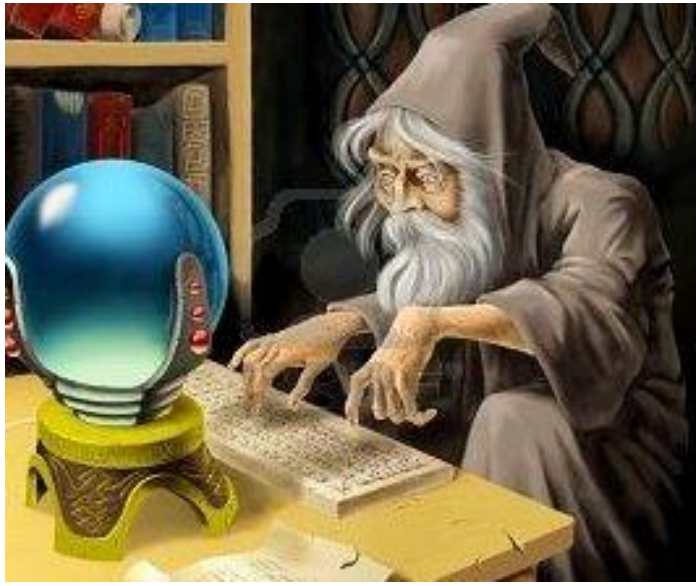
- Aj tak treba intro
  - Kto je Hacker?
  - Počítačová bezpečnosť

Hacker

- to hack = udrieť
- Lichôtka
  - Búchač, Dávač
  - Naozaj *používa* počítač
  - Slovom Macher :)
- Zneúctené novinármi
  - Záporák, Kazisvet
  - Nové pozitívne výrazy: White Hat, Etický hacker, PenTester
- Človek, ktorý sa vyzná v niečom obvykle technickej povahy
  - Zámočník

Hacker

- Dokáže spraviť niečo z užívateľského pohľadu neočakávané
  - Prihlásiť sa ako ktokoľvek s heslom **’ or ’a’=’a**



Počítačová bezpečnosť

Webové Aplikácie

- XSS
- SQL injection
- Session stealing

Číra zloba

- DoS
- Social Engineering
- Spam

Lokálne Aplikácie

- Buffer overflow
- Ransomware
- Cracking

Kryptografia

- Šifrovanie
- Identita
- Autenticita

Siete

- Spoofing/Poisoning
- Rougue AP
- MitM

Základné pojmy

Nárečje **HTML**uo
alebo
Potreba písaňja v tomto nárečí

- Pôvodná idea: HyperText - ideálny náučný text
- Dnešné využitie: Webové Aplikácie
  - JavaScript (<script>, href=, onmouseover=, ...)
  - CSS
  - Obrázky
  - iFrame

HTTP

- Stateless (potreba cookies)
- Objemný plain-textový protokol

```
GET /appka?p1=xx HTTP/1.1
Host: domena.sk
User-Agent: Mozilla/5.0
Accept: application/json, text/javascript, */*; q=0.01Referer:
http://inyserver.sk/view-zmluva/7019400031
X-Requested-With: XMLHttpRequest
Cookie: session=83h8hlalsu56ho13vnmpr603d4
```

```
HTTP/1.1 200 OK
Content-Length: 15564
Date: Wed, 18 Jan 2017 17:07:16 GMT
Content-Type: text/html; charset=utf-8
Server: Apache/2.4.18 (Red Hat) OpenSSL/1.0.1e-fips
Set-cookie: session=x; Secure; HttpOnly; Expires=Thu, 01 Jan 1970 00:00:01
GMT
↲
...
```

DNS

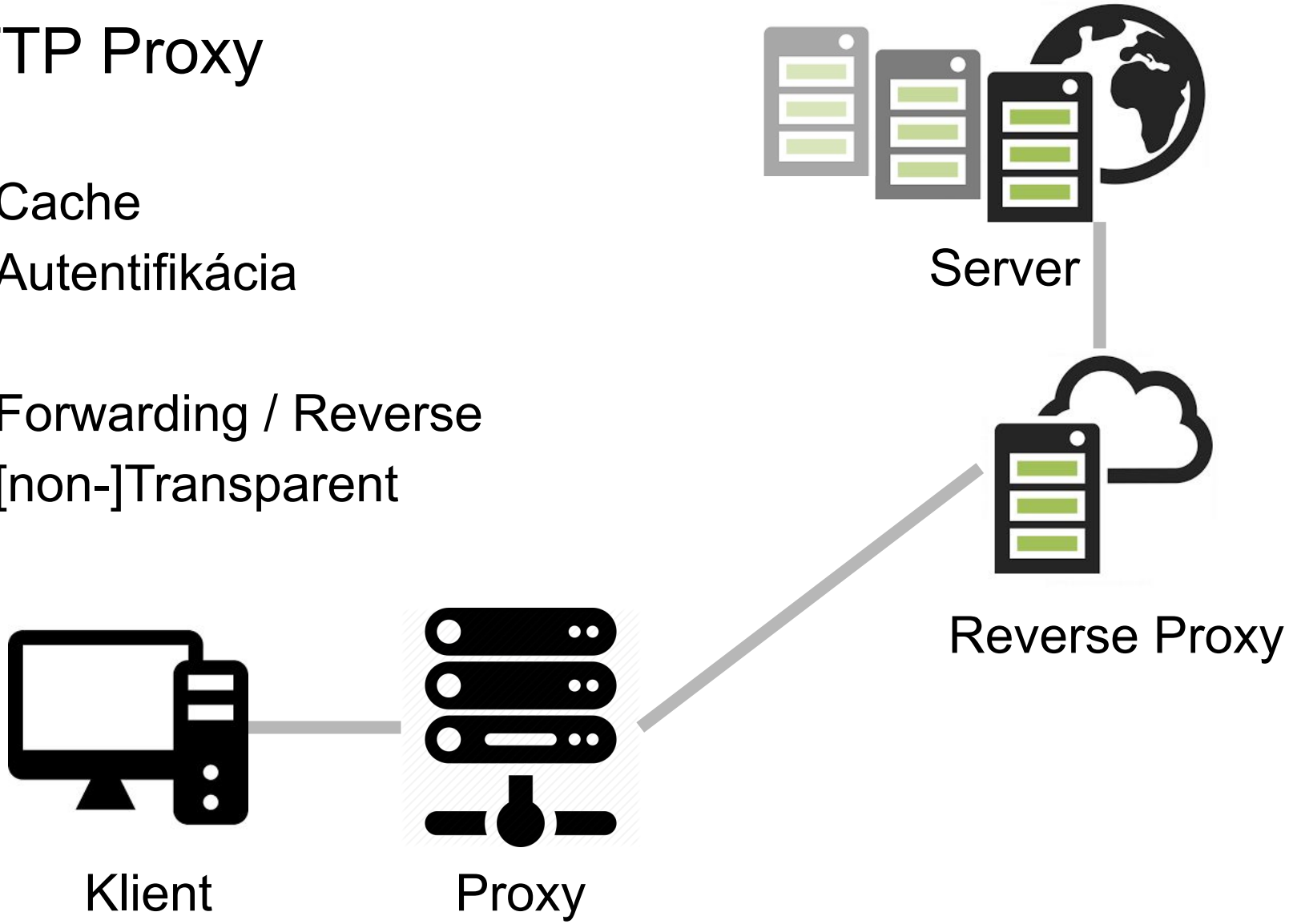
Domain Name System

- Preklad pekného názvu na IP adresu
  - www.gjh.sk → 193.87.79.100
- Punycode
  - šľahačka.gjh.sk → xn--ahaka-jya35ajj.gjh.sk

HTTP Proxy

- Cache
- Autentifikácia

- Forwarding / Reverse
- [non-]Transparent



Drobné príklady zo života

tzv. ani-nie-hacky

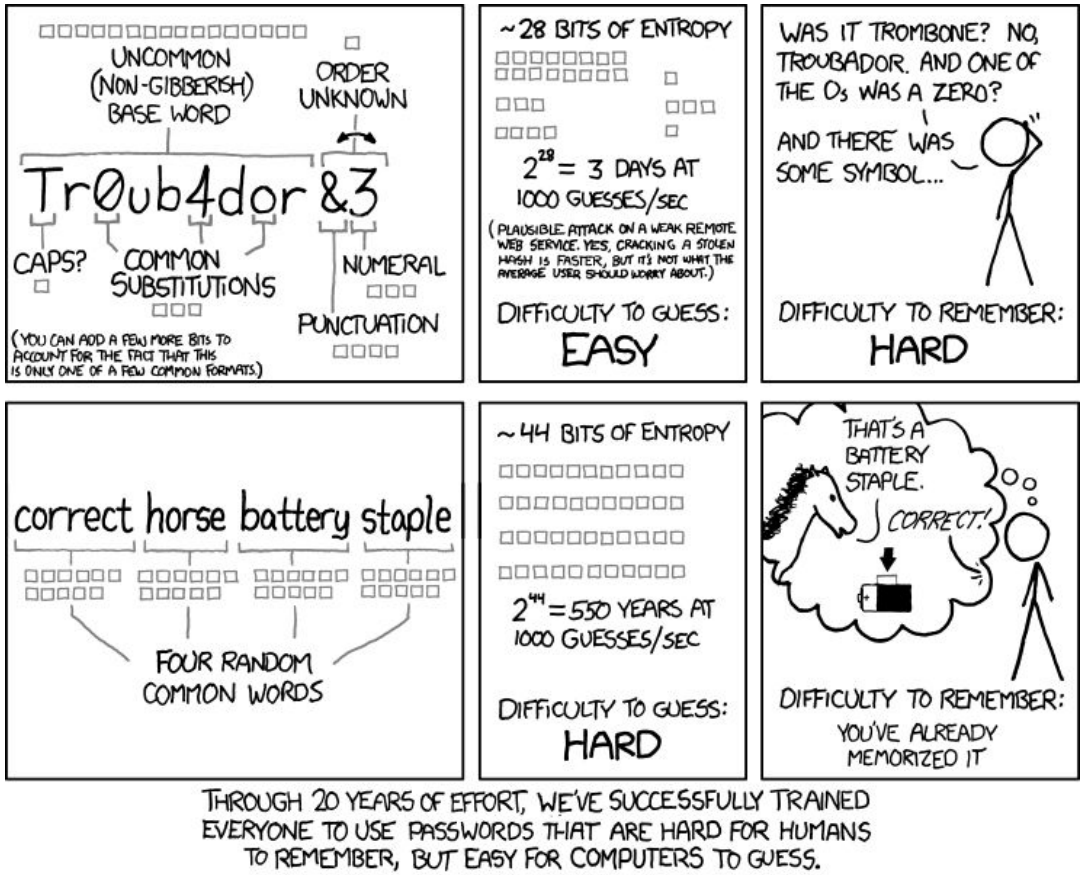
Password reminder mailom

- V horšom prípade
  - Zabudnuté heslo v plain-texte (???)
  - Nevymazaný mail
- V lepšom prípade
  - Vygenerované heslo
  - “Forgot password” ako metóda na prihlasovanie
  - Heslo od mailového konta sa stáva ultimátnym nadheslom :)

- Stačí prísť a stlačiť ctrl-v
  - Používajte password managery (napr. KeePass)

Heslá

- Jednoduché
  - “Veď tam nič nemám”
- Opakujúce sa
  - Kto už niekedy vyplnil heslo do loginu?



- Známy komix XKCD
  - “Po 20 rokoch úpenlivej snahy sme úspešne všetkých naučili vytvárať si ťažko zapamätateľné ľahko strojovo uhádnuteľné heslá”

Netradičné použitie stránky

- Nesprávne ošetrenie vstupov
- Zlý návrh
- Použitie stránky, ako by to väčšine ľudí nenapadlo
  - Stalking n-tého rádu

- Vyhľadávanie v nezobrazených poliach
  - Dajú sa po znakoch natipovať (tzv. blind prístup)
- Dôverovanie vstupu z combo-boxu
- Predvídateľné identifikátory

Útočné techniky

Phishing

- Vytvorenie podobnej stránky
- MitM - obalamutí aj autentifikáciu SMSkou
- Spam / Scam (všetci sa prihláste, lebo bude zle!)
- Použitie plekrepu
  - googlw.com
- Punycode
  - znak “o” vyzerá ako znak skladania zobrazení
  - microsoft.com, passport.com
- Data:
  - data:text/plain;base64,SGVsbG8sfK39amcsfwbpzL...

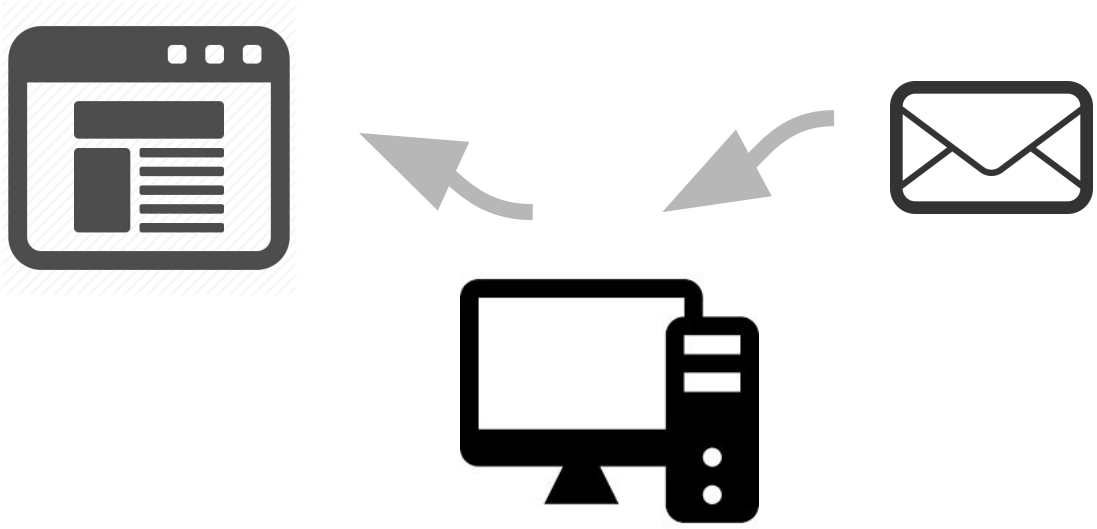
XSS (cross-site scripting)

- Ja to napíšem, tebe sa to vykoná
- Zobrazuje sa tvoje Meno ako Me**no**?
  - Skúsme to aj so <script>...
- Reflected / Stored / DOM based

- CMS systémy
- iframe-ové návštevné knihy

CSRF (cross-site request forgery)

- Linka v maile do prihláseného portálu
  - Session Riding
- CSRF pomocou XSS
  - Session Stealing
  - TRACE metóda na získanie HttpOnly cookie



SQL injection

- SQL overenie hesla

```
SELECT count(*) FROM users
WHERE userlogin = '$login'
AND userpwd = '$pwd';
```

- if prihlas($login, $pwd) then ...
  - 0 = false, nenulová hodnota = true

$pwd:= `' OR 'a'='a`

Vysledok: `AND userpwd = '' OR 'a'='a';` a to je true vždy!

Scan podsiete CSSkom :)

- Bez JS sieťových spojení

…

...

- CSS: display:none
- JS: už len zistiť, ktorá linka je fialová

Kam ďalej?

Nejaké tie softwary

- BurpSuite
- JuiceShop / DVWA / WebGoat
- Pentester Lab

- Notpron (hra)
  - Pekná kratochvíľka aj pre netechnikov

- Sqlmap.py
- Metasploit
- cve.mitre.org, www.cvedetails.com

Demo