Univerza *v Ljubljani*
Fakulteta *za računalništvo in informatiko*

Penetration testing process

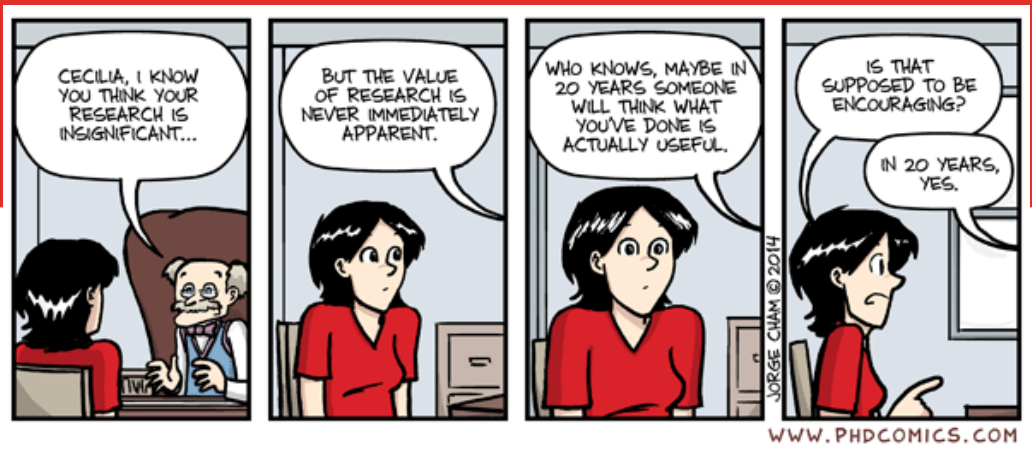
doc. dr. David Modic

28/10/20

Before we start…Homework!

- Everyone submitted! Thanks.
- The aim was to get you into the mind-frame of an attacker. Most of you succeeded quite well.
- The writing standard is quite good and you made me laugh a few times.
- Many of you have practical suggestions that are actually used in real attacks.
- Some of you under- and some of you over-estimate the targets.
- There are some gaps, generally, but we will address them in the future lectures.
- Well done!

Before we start II…



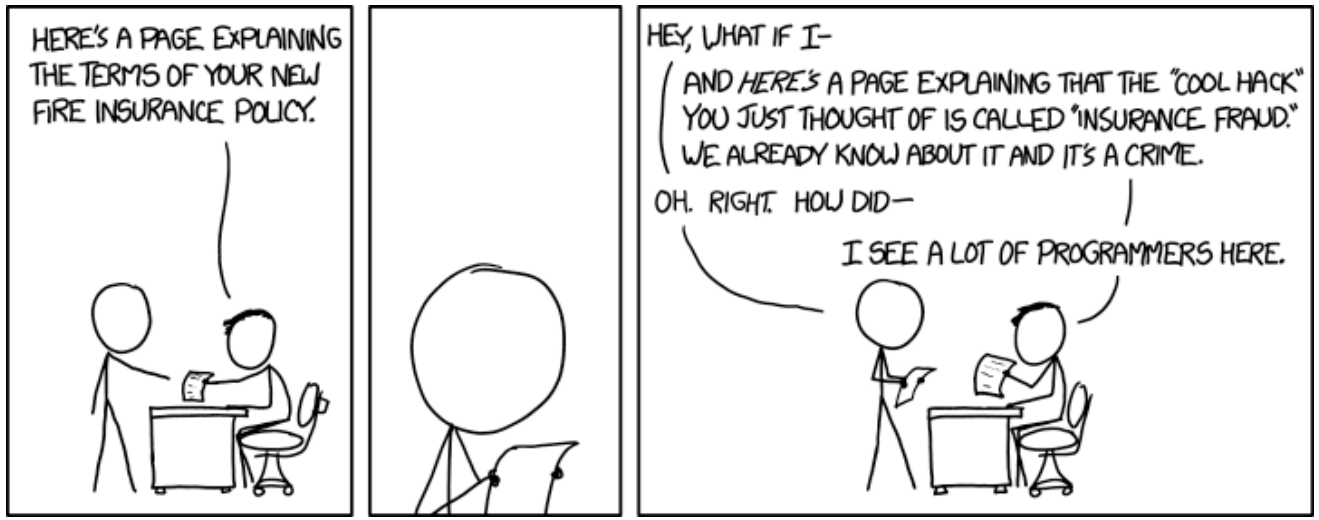
- Assignments. There were a couple of questions.
- All the people who will volunteer Metasploit, will do one presentation together.
- All the people who will do Shodan, will do one presentation together.
- There will be **no penalty** for those who do not do the presentation.
- But we will comment on the presentation of those who do. *Think about it.* How often do you get a room of people assessing your presentation skills? How often do you get a Cambridge academic spending time on your presentation skills?

The story so far…

- We talked about Ethics and how they pertain to hacking last time.
- In summary, the general population won't like you no matter what you do (because they will be afraid of you). But, you can avoid being prosecuted by law.
- For that you need to know the law.
- Today, we shall be talking about the practical process of ethical hacking.

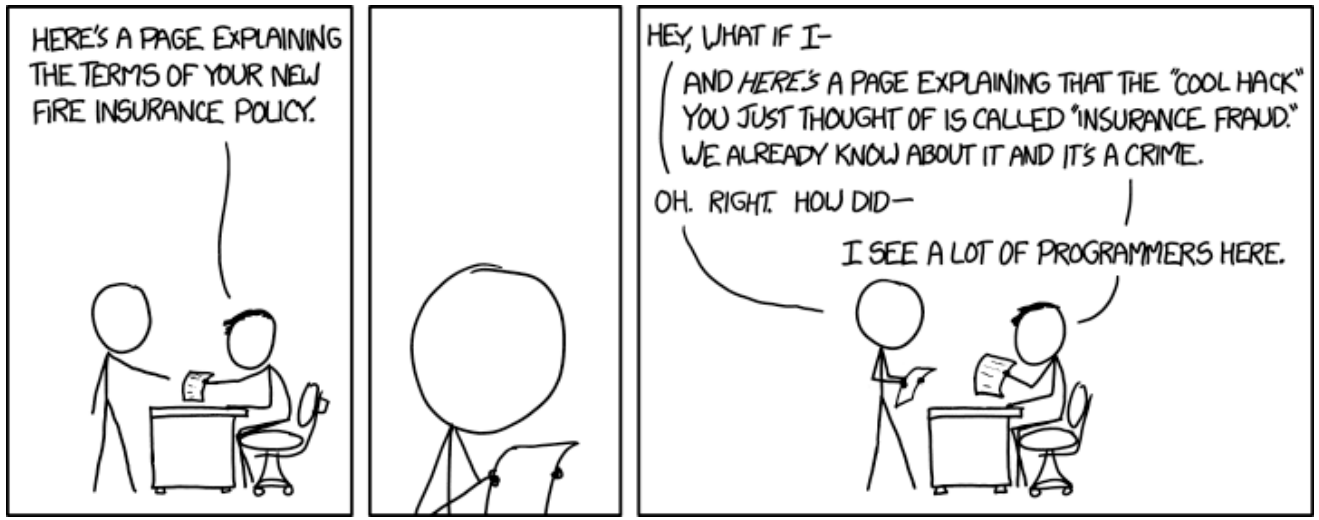
Before you start PENTESTING

- (QUIZ) What do you need for the process to start?



Before you start PENTESTING

- (QUIZ) What do you need for the process to start?
  - Incorporate.
  - Get the infrastructure in place.
  - Secure your machine(s).
  - Follow data safety guidelines.



Incorporate

- Many companies will **not** work with private individuals directly.

Incorporate

- Many companies will **not** work with private individuals directly.
  - Because you can screw them as an individual in many ways unavailable to SME's.
  - This is harder if you are a company.
  - Also you are more liable as a company.
  - And the company can get sued for more money.
  - A breach of contract is easier recouped from a company.
- Look, you just *have* to. And not into an Association. Into a proper company.
- Alternatively, work for a pen testing company. More secure, less money.

Get security policy in place

- This is boring as hell. I should know, I lead the FRI policy team.
- Look them up online.
- You need this. Why?

Get security policy in place

- This is boring as hell. I should know, I lead the FRI policy team.
- Look them up online.
- You need this. Why?
  - Because you need cyber insurance.
  - Because no insurance company will insure you, without a policy they can pester you with.

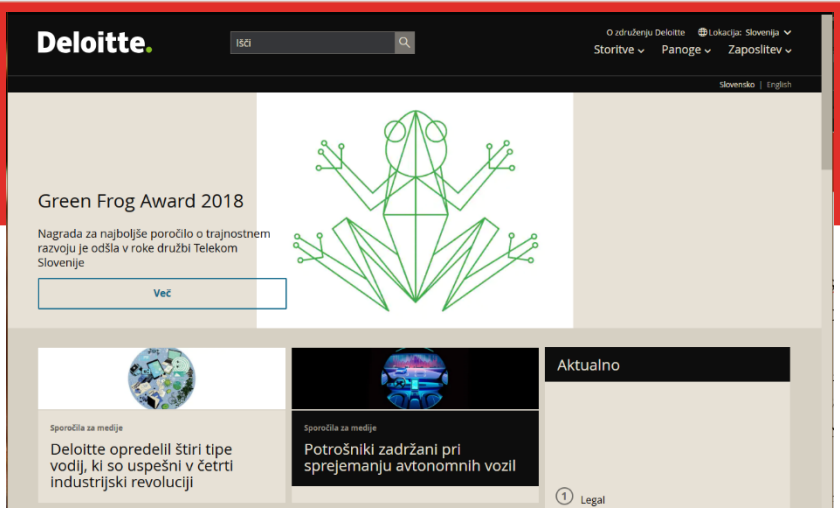
https://info.lse.ac.uk/staff/Services/Policies-and-procedures/Assets/Documents/infSecPol.pdf

Get the infrastructure in place

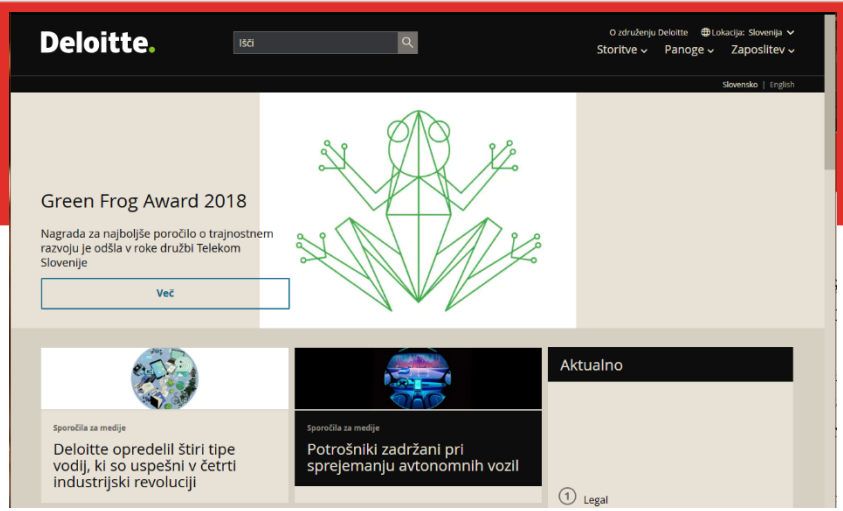
- Buy equipment. A server is preferred. If you are paranoid, follow the UK MOD guidelines (only new equipment directly from the factory, when out of warranty, physically destroy, not sell it).
- Buy tools you figure you might need (card skimmers, pineapples, etc). **Notify the police!**
- Secure licenses for stuff. Most professionals prefer Core Impact (by Core Security).

Secure your machine(s)

- Learn from the example of Deloitte.

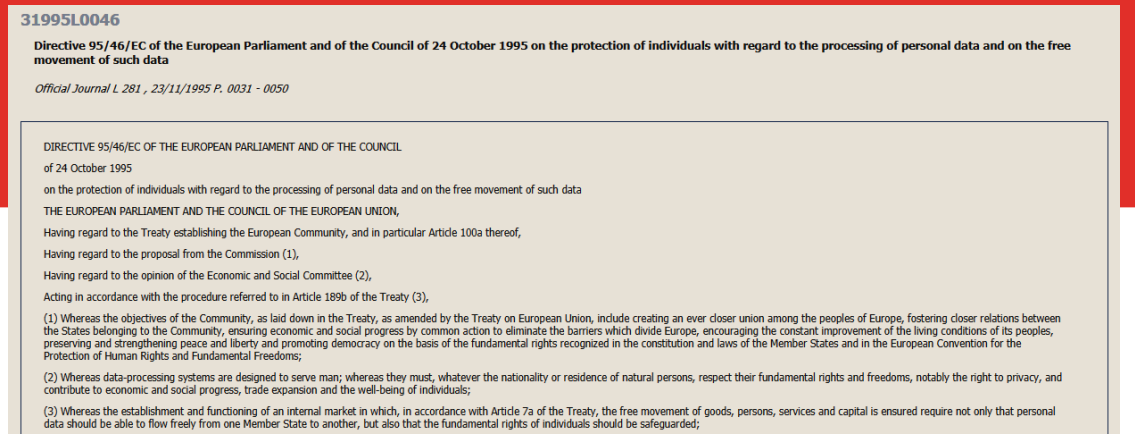


Secure your machine(s)



- Learn from the example of Deloitte.
- One of the most prestigious PenTESTING companies in the world.
- They used Azure for their network. Did not trust Microsoft to administer it for them.
- Had SAMBA access configured with admin/admin.
- Result: 700+ Companies PenTesting reports available to the world.
- We (Cambridge) found the breach. We were their customers, so we contacted them. They promised they already fixed it. Next day, we accessed their cloud again. Same credentials.

Follow data safety directives



31995L0046

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Official Journal L 281 , 23/11/1995 P. 0031 - 0050

DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 24 October 1995

on the protection of individuals with regard to the processing of personal data and on the free movement of such data

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 100a thereof,

Having regard to the proposal from the Commission (1),

Having regard to the opinion of the Economic and Social Committee (2),

Acting in accordance with the procedure referred to in Article 189b of the Treaty (3),

(1) Whereas the objectives of the Community, as laid down in the Treaty, as amended by the Treaty on European Union, include creating an ever closer union among the peoples of Europe, fostering closer relations between the States belonging to the Community, ensuring economic and social progress by common action to eliminate the barriers which divide Europe, encouraging the constant improvement of the living conditions of its peoples, preserving and strengthening peace and liberty and promoting democracy on the basis of the fundamental rights recognized in the constitution and laws of the Member States and in the European Convention for the Protection of Human Rights and Fundamental Freedoms;

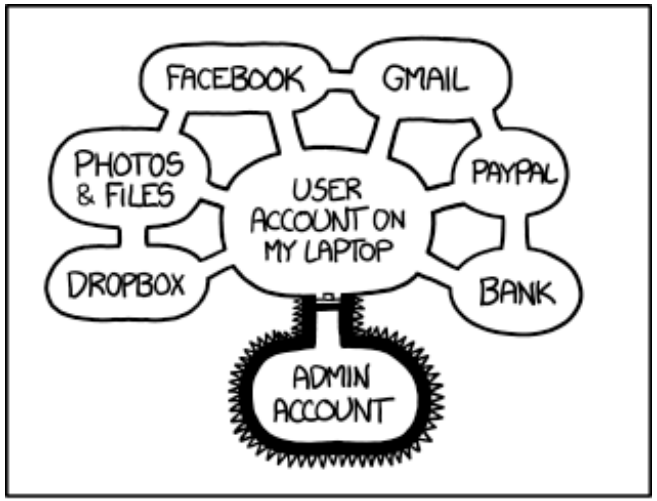
(2) Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals;

(3) Whereas the establishment and functioning of an internal market in which, in accordance with Article 7a of the Treaty, the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded;

- The EU law specifies four levels of data:
  - *Unclassified* – everyone can see that
  - *Internal / sensitive* – data that is sensitive for the business but not overly problematic in the storage sense.
  - *Confidential* – data that cannot be disseminated past those who have clearance. They have to be destroyed after use, copies need to be tracked and they have to be stored "encrypted at rest". Information cannot leave the jurisdiction. *Umm… is the Cloud appropriate for storing that?*
  - *Secret* – data that needs to be stored on an air-gapped machine and copies tracked.

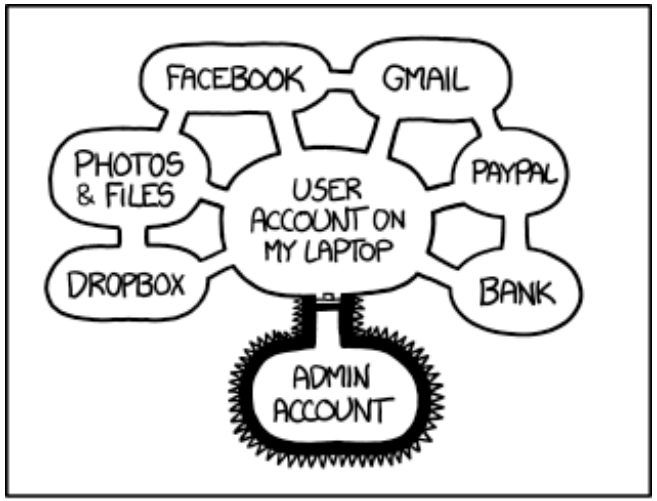
Follow data safety directives - Issues

- Let's say you penetration test and achieve authorized access. You find confidential data. What do you do?
  - (QUIZ) Do you copy them to your machine?



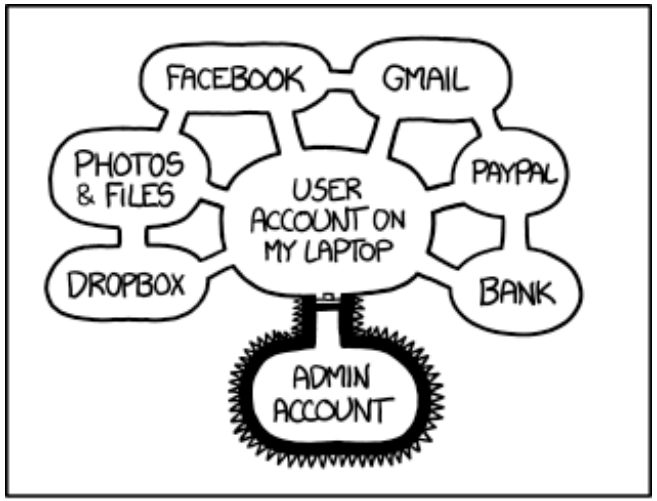
Follow data safety directives - Issues

- Let's say you penetration test and achieve authorized access. You find confidential data. What do you do?
  - (QUIZ) Do you copy them to your machine?
    - No. You would be in breach of EU data safety regulations.
    - Saying that you weren't aware, does not absolve you from prosecution.
  - (QUIZ) Do you disclose the breach to the corporation that hired you?



Follow data safety directives - Issues

- Let's say you penetration test and achieve authorized access. You find confidential data. What do you do?
  - (QUIZ) Do you copy them to your machine?
    - No. You would be in breach of EU data safety regulations.
    - Saying that you weren't aware, does not absolve you from prosecution.
  - (QUIZ) Do you disclose the breach to the corporation that hired you?
    - Yes. In the report. The report needs to be stored encrypted at rest and physically handed over (or sent encrypted). Do not include the data (because you do not have it, anyway ☺).



Follow data safety directives – Issues II.

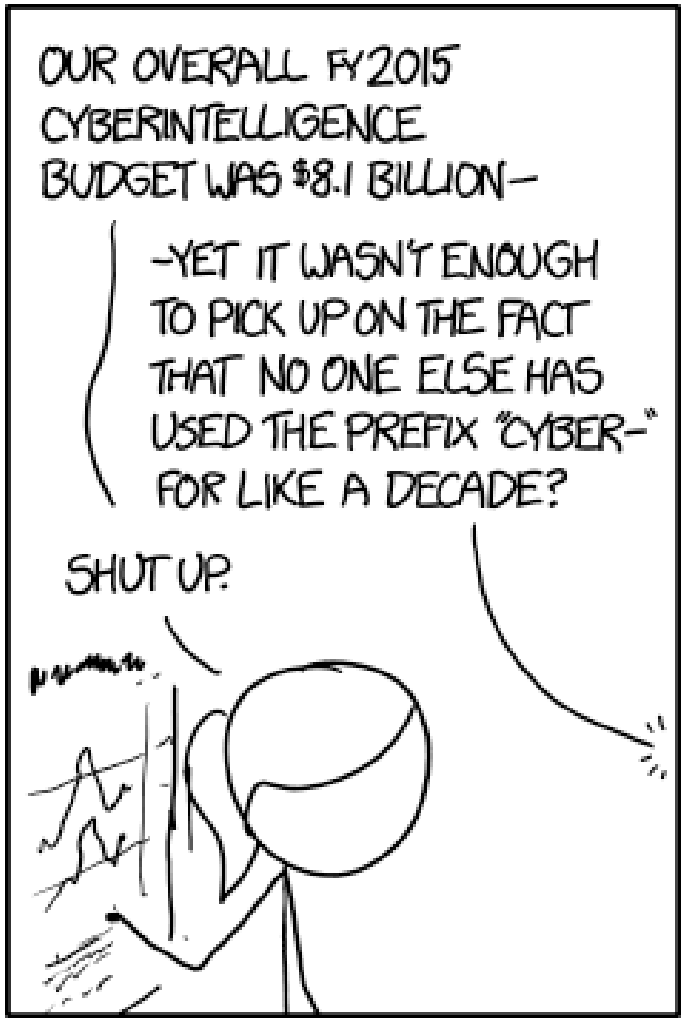
- (QUIZ) A bonus points question. Do you need to encrypt-at-rest all your data to follow GDPR? I mean besides reports.

Follow data safety directives – Issues II.

- (QUIZ) A bonus points question. Do you need to encrypt-at-rest all your data to follow GDPR? I mean besides reports.
  - Yes and no. According to GDPR, you have to follow local storage guidelines. In the UK everything above internal (or TESCO secret as it is called) needs to be encrypted-at-rest. In Slovenia the directive is not that clear. Perhaps, err on the safe side.

The PENETRATION TESTING steps

- In general, there are:
- (a) The preliminary steps – *The pre-action phase.*
- (b) The penetration testing phase.
- (c) The follow-up phase



THE PRE-ACTION PHASE

david.modic@fri.uni-lj.si

The pre-action phase

- (Quiz) What do you need to do in this phase?

The pre-action phase

- (Quiz) What do you need to do in this phase?
  - Get hired by a company / individual to test their defences.
  - Do due diligence
  - Agree on the scope.
  - Agree on the rules of engagement.
  - Agree on the timeline.
  - **Sign a contract**.

Get hired by a company / individual to test their defences

- If you are not hired, then this is *unathorized access*, which is the definition of *Black hat* hacking.
- Slovene law is quite clear on that (KZ-1 §143, §221, §237, §306).
  - §143 Stealing private data (1 – 5 years)
  - §221 Unathorized intrusion (1 – 5 years)
  - §237 Unathorized intrusion into a business system (3 – 5 years)
  - §306 Creating, selling, using tools used in UA (1 – 3 years)

Do due diligence

- Is the person who approached you *authorised* to hire you to pen-test?

Do due diligence

- Is the person who approached you *authorised* to hire you to pen-test?
  - (a) I work for ACME ltd. and want to destroy GoodGuys ltd. I call you, pretend I am from GG, define the scope, pay you, you report to me, I break GG. If caught, you go to prison.
  - (b) I work for the Russian Mafia and hire you as a fake representative of GG. Same deal.
  - (c) I actually work for GG, but I am not the person who can authorize a PENTEST. I sell your report to the competition.

Do due diligence

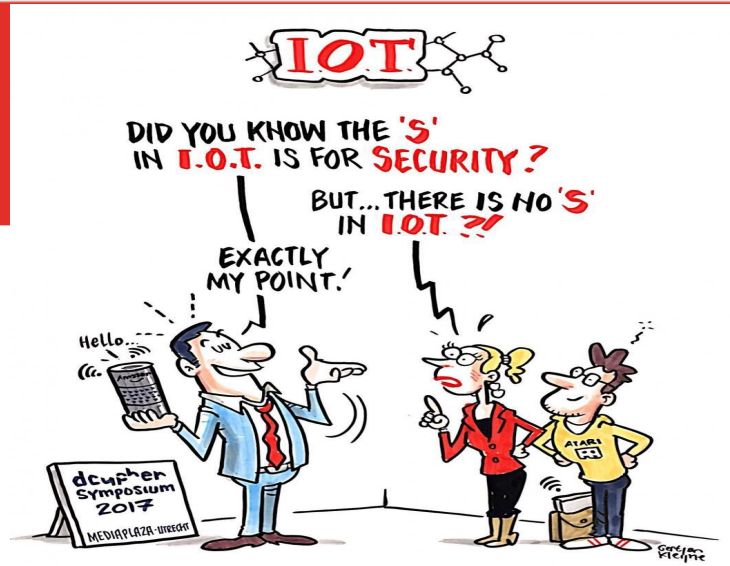
- (Quiz) What if the person who hires you is an evil CEO of GG on their way out?

Do due diligence

- (Quiz) What if the person who hires you is an evil CEO of GG on their way out?
  - Well, you meet with more than one person at GG. Preferably a CISO or a CTO & another board member / the CEO (depending on the size of the company).
  - If your employer is a one-man-band, then they probably cannot afford you in the first place. (Quiz) What if you still pen-test for free?

Do due diligence

- (Quiz) What if the person who hires you is an evil CEO of GG on their way out?
  - Well, you meet with more than one person at GG. Preferably a CISO or a CTO & another board member / the CEO (depending on the size of the company).
  - If your employer is a one-man-band, then they probably cannot afford you in the first place. (Quiz) What if you still pen-test for free?
  - Up to you, *but*. **Liabilities will remain**. An argument in court that you did a crappy job, because they did not pay you, does not hold legal water. And when someone is going under and they are finding it hard to feed their family… you probably cannot count on them being all reasonable and understanding about you just messing about a bit, as it was a free favour.



Agree on the scope and rules of engagement

- Which machines are you allowed to target?
- Which parts of the network are absolutely out of bounds?
- Which vulnerabilities are you allowed to probe? (SQL, Wordpress, Infrastructure…).
- Do you have to be undetected? (*Then passive attacks only*)
- Can you social engineer? If yes, who are the allowed targets?
- Can you probe physical security?

Issues with scope and the rules of engagement

- (Quiz) Why do companies hire you?

Issues with scope and the rules of engagement

- (Quiz) Why do companies hire you?
  - To improve their security.
  - To do damage limitation (usually after a breach ☹).
  - To tick a compliance box.
- If they hire you to tick a box (Banks like to do that), what is the issue?
  - You tend to get pointless scopes and ROE. (Quiz) Do you still follow them?
  - **YES!**

Issues with scope and the rules of engagement

- (Quiz) Why do companies hire you?
  - To improve their security.
  - To do damage limitation (usually after a breach ☹).
  - To tick a compliance box.
- If they hire you to tick a box (Banks like to do that), what is the issue?

Issues with scope and the rules of engagement

- (Quiz) Why do companies hire you?
  - To improve their security.
  - To do damage limitation (usually after a breach ☹).
  - To tick a compliance box.
- If they hire you to tick a box (Banks like to do that), what is the issue?
  - You tend to get pointless scopes and ROE. (Quiz) Do you still follow them?

Issues with scope and the rules of engagement

- (Quiz) Why do companies hire you?
  - To improve their security.
  - To do damage limitation (usually after a breach ☹).
  - To tick a compliance box.
- If they hire you to tick a box (Banks like to do that), what is the issue?
  - You tend to get pointless scopes and ROE. (Quiz) Do you still follow them?
  - **YES!**

- Scope defined by date X
- Testing dates Y – Z
- Report submitted by Date W
- Follow-up by date W + x
- Repeated testing by date XX
- Follow-up report by date YY
- Payment for initial test date W + 30
- Payment for repeat test, if needed by YY + 30

Agree on the timeline

- Discuss the rough time window. As big as possible. Traditionally, companies that do not want to know about their weaknesses will give you an unrealistic time window. *Like, next Monday 9-10am*.
- Push for several days. Do not be an ass – if your attack involves social engineering, do not do it over the weekend, or on a holiday. *No need to*. Do a proof-of-concept and then in the report state that this would be even more effective over the weekend (*which it so would*).
- Agree on everything in advance.

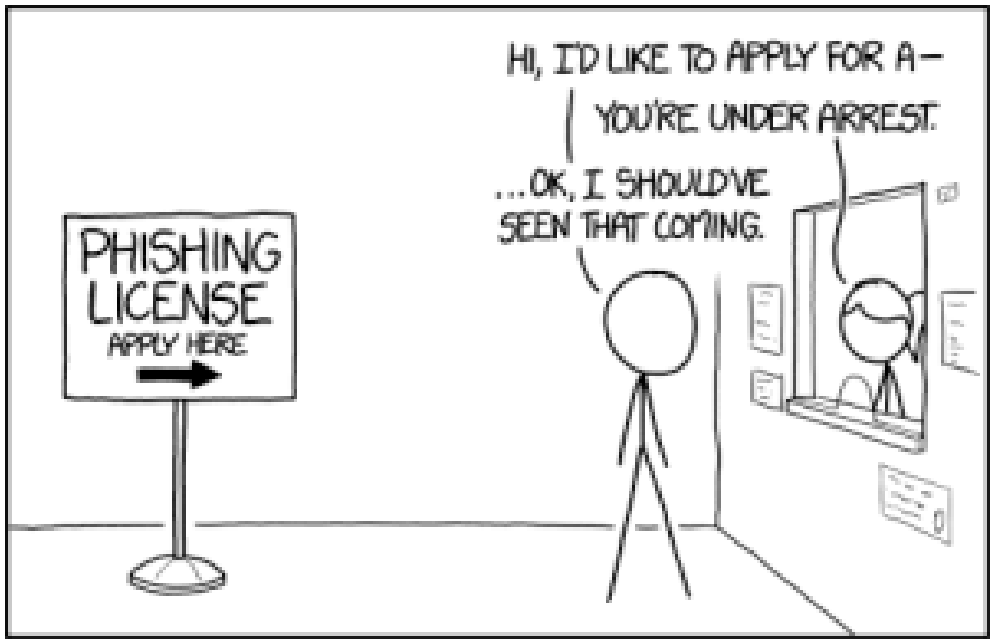
Sign a contract!

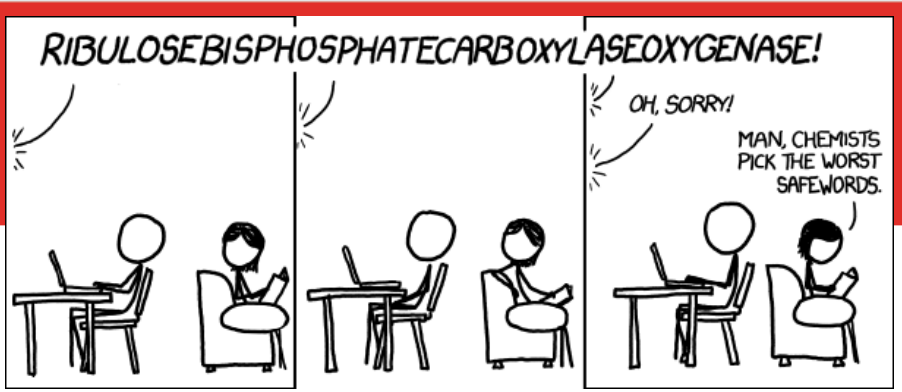
- Before you do anything, sign a contract!
  - Be very precise. *Everything specified on paper!*
  - What you are allowed to do, the dates, the scope, the team, the indemnifying clause (*if we are caught doing what we agreed on, you agree not to persecute*), the fees…
  - Specify your liabilities too (*if sensitive data gets leaked from me, I am on hook for X*). Companies love that.
  - Specify who sees the data and what happens to the report. **NO-ONE else!**
  - Make sure the contract is signed.

THE ACTION PHASE

Action

- The practical stuff, we will do in the next lecture(s).
- Here, we will discuss what has to be done in general terms.





Action steps – this is an important slide!!

- Follow the contract!
  - Only the **dates** that are specified in the contract are viable!
  - Only the **scope and ROE** is viable. Negotiate wisely.
- **Agree on a safe-word. If while you are attacking, an actual breach happens, and you get notified, or realize it, immediately send the safe-word and cease all activity, so that the company can deal with the real threat.**
- Record keeping!

Action steps

1. **Open Source Intelligence (OSINT) Gathering.**
2. **Physical probing (if in ROE).**
3. **Deciding on the strategy – developing attack(s).**
4. **Launching the attack(s).**
5. **Write the report.**

1. Open Source Intelligence Gathering

- This is going to be subject of the lecture next week.

2. Physical probing

- If allowed, under ROE, by all means, scout the macro and micro location.
- What are the physical access hurdles?
- Can you incite a crisis (like set off fire alarm, etc)?
- Is there a parking lot? Can you access it without being on cameras?
- Even if there are CCTV's, can you have a legitimate reason to be there?
- What are the companies physical security arrangements? Are they locked after hours, is there a doorperson, how many are there, when do they switch, is there a smoking area, where is the server room, can people walk in unannounced …
- Could you leave rubber duckies around?

2. Physical probing II.

- Is the company hiring? If they are, do OSINT about the hiring committee and apply for job (*surprisingly* you went to the same schools as decision makers, you spend your summer holidays in the similar locations, you have the same hobbies …).
- Once you are in the building for the interview, notice things – security arrangements, operational security, how strictly do they follow security precautions, do they allow tail-gating?

2. Physical probing II - example

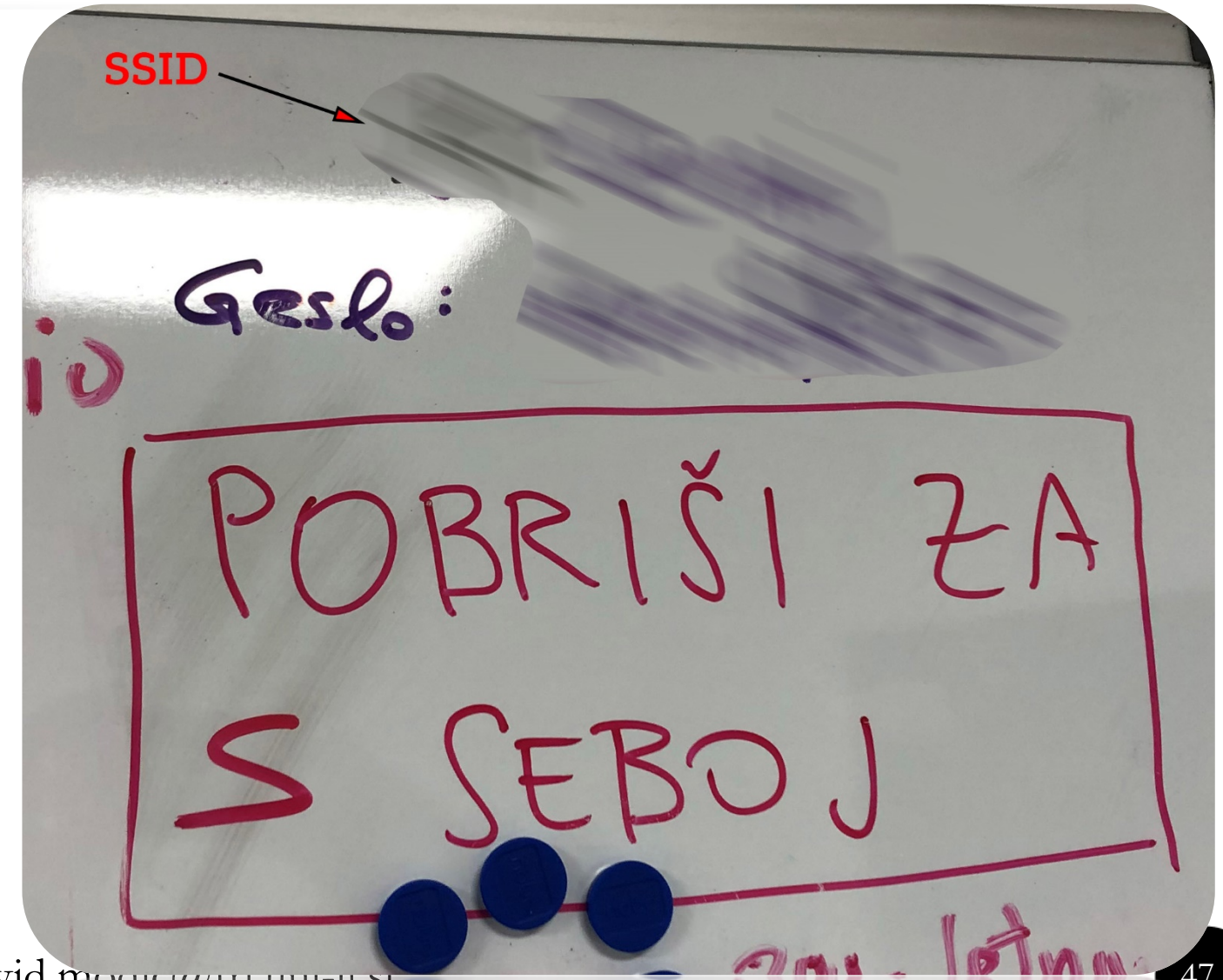
- A few months ago, I was asked to test a company.
- Upon arrival for initial meeting, the person I was meeting was delayed.
- They put me in a meeting room and left me alone.
- This is the result.

2. Physical probing - example

- There was a key in the door of the meeting room. I made an imprint.

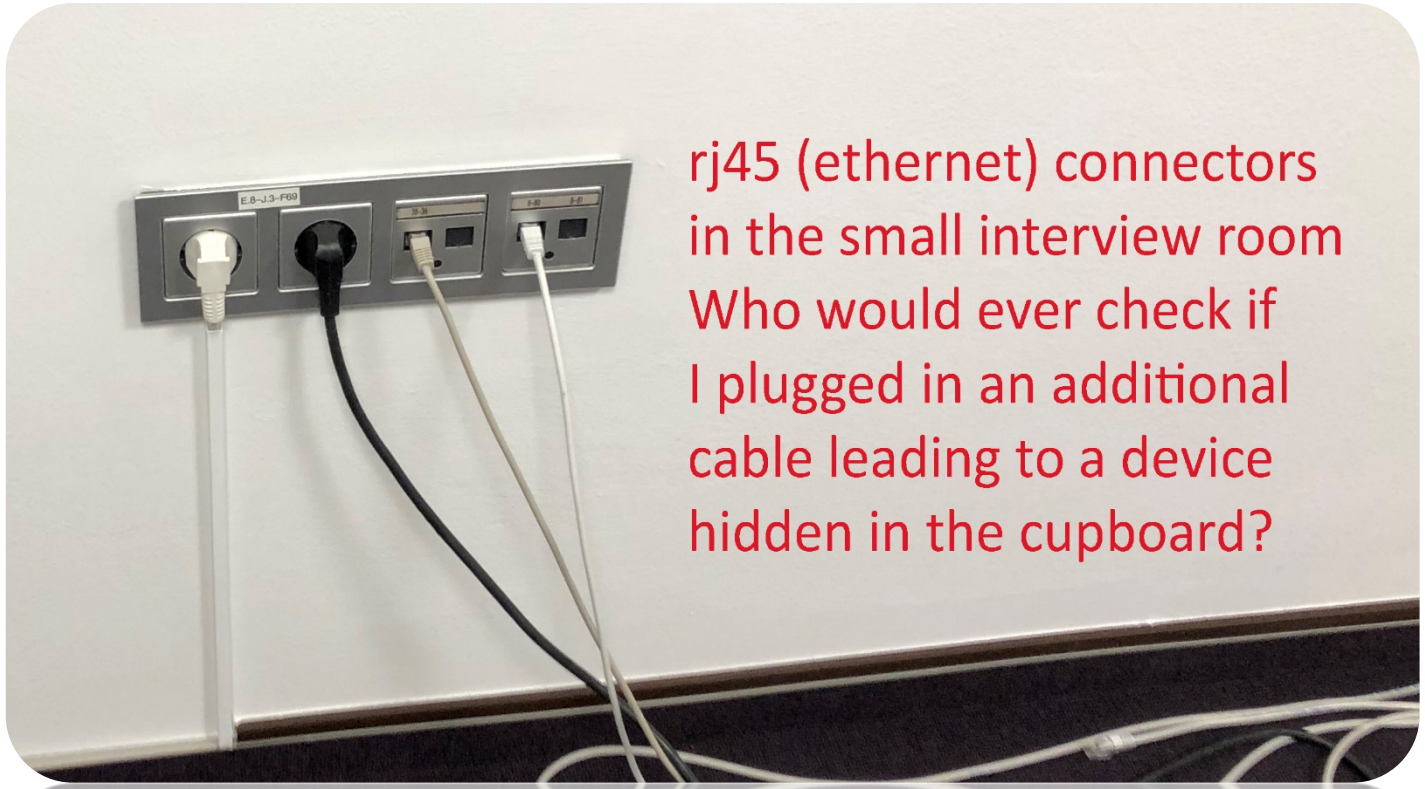
2. Physical probing - example

- The SSID and password were on a whiteboard on the wall.



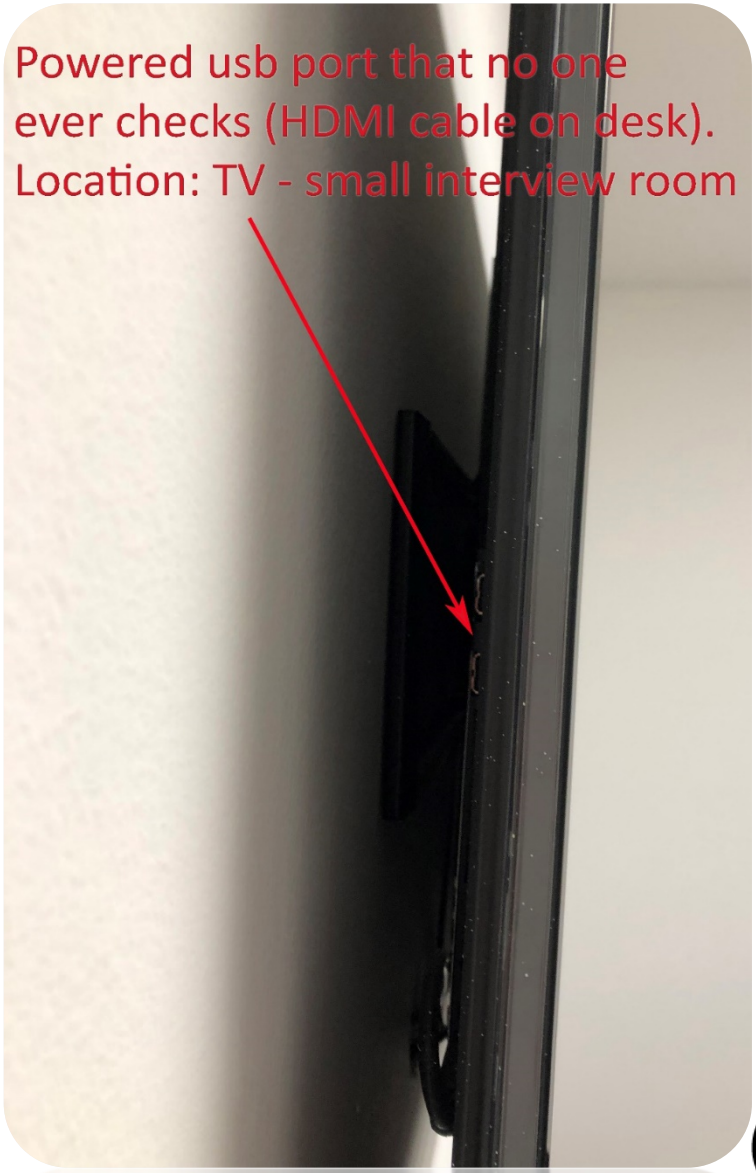
2. Physical probing - example

- There were ethernet sockets on the wall. Some populated.



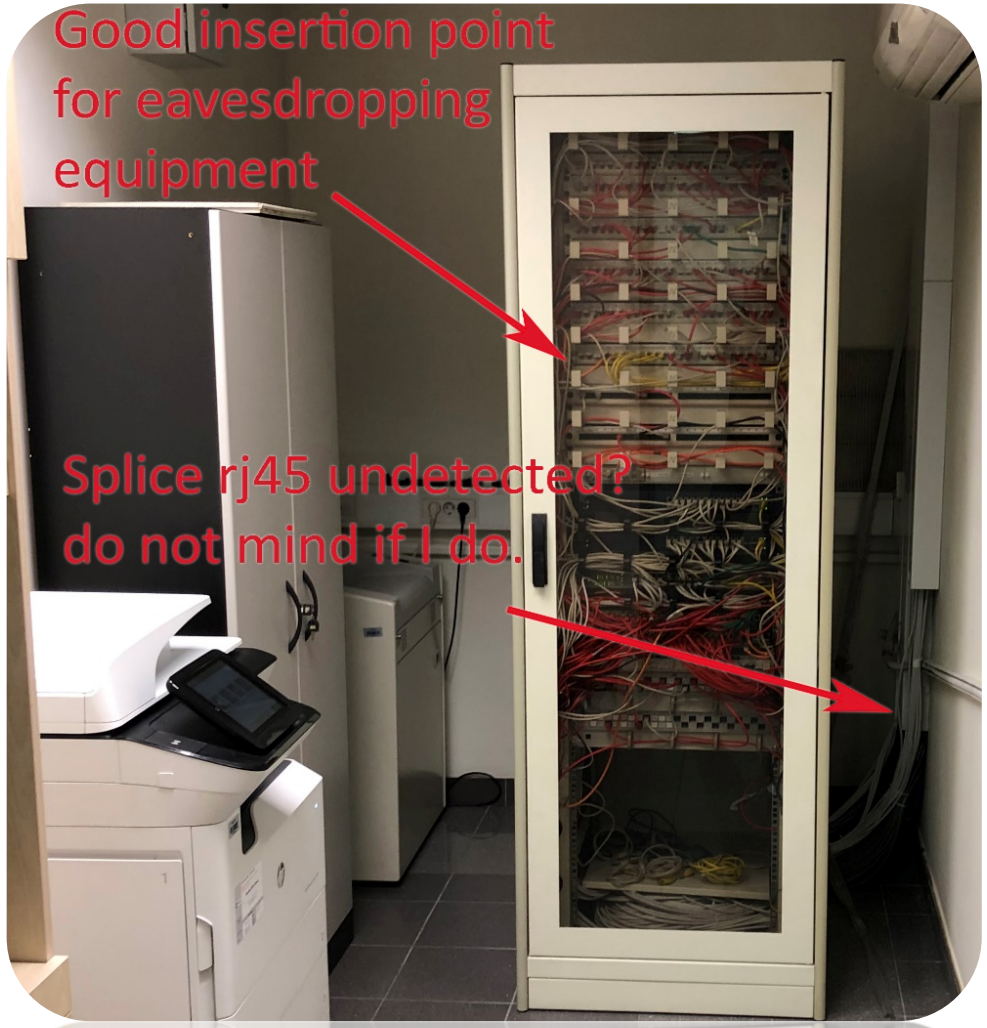
2. Physical probing - example

- There was a smart tv on the wall. It had a powered USB connector.



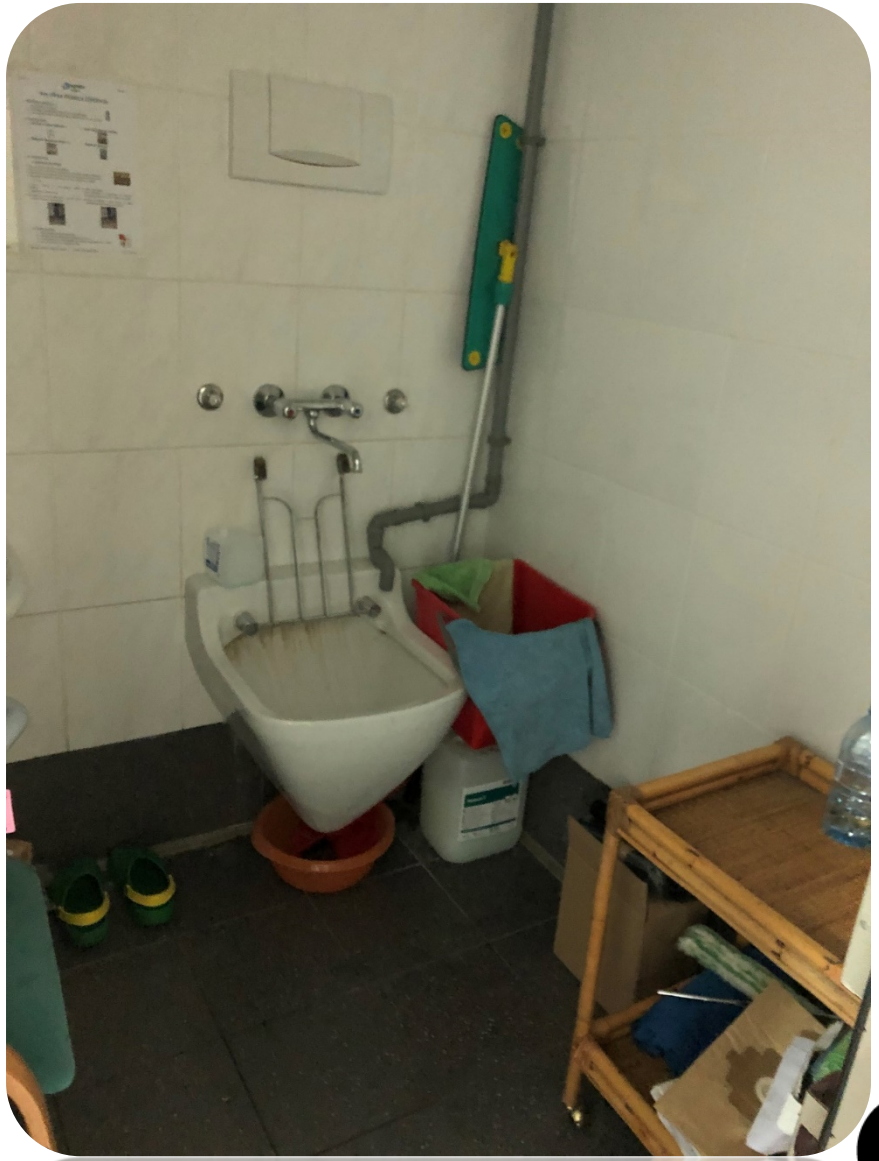
2. Physical probing - example

- The Communications room was unlocked.



2. Physical probing - example

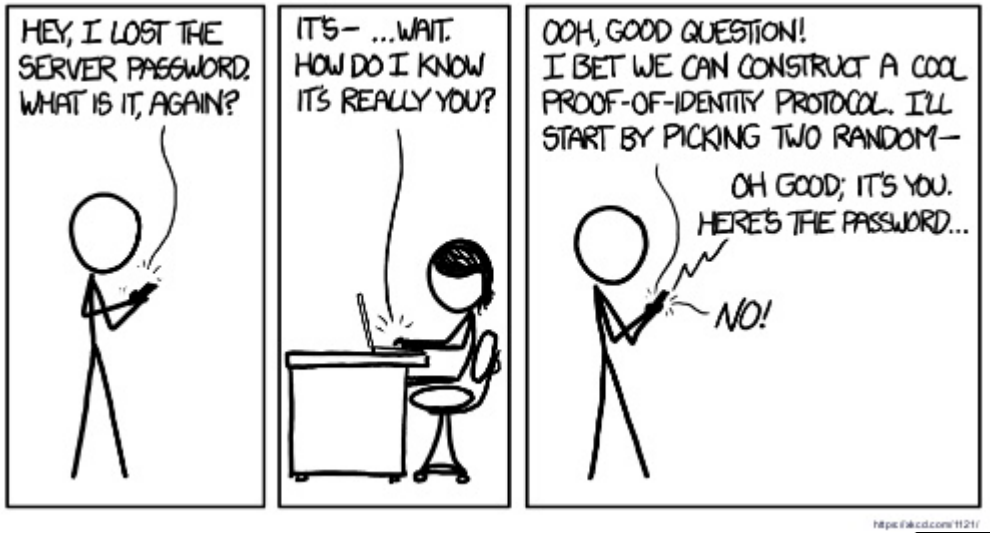
- There was a janitors closet, locked, but with keys in the lock.



3. Developing attack(s)

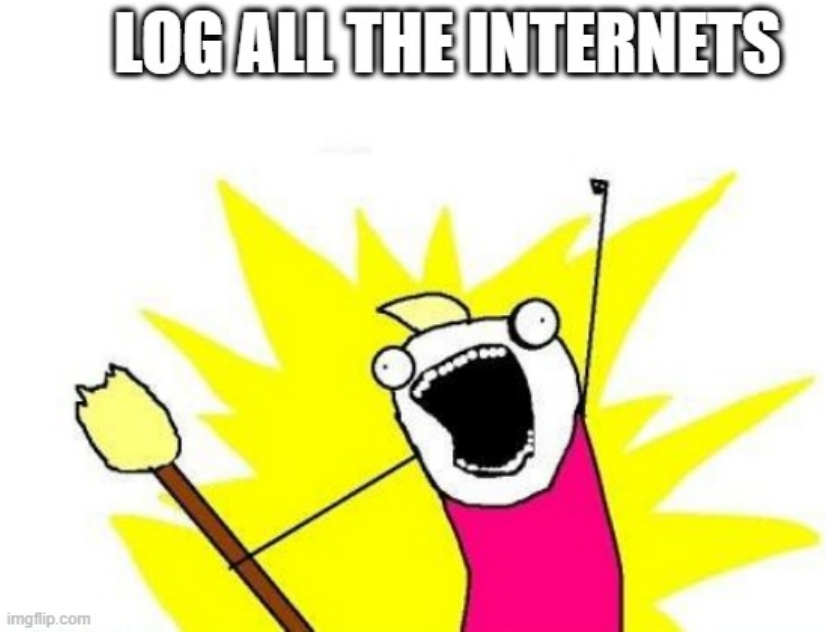
- Once you have all the intelligence you think you need, plan the attack vectors.
- Generally it is smart to do at least two parallel attacks. One is for *misdirection*, the other, the actual attack.

(LOCKED SHIELDS EXAMPLE)



4. Launch

- Once you have the strategy in place and have secured preliminary steps if needed (scripting, fake documents, usb keys, etc), then…
- On the *contract specified window*, launch.
- Religiously track everything. Log it all.



5. Write the report

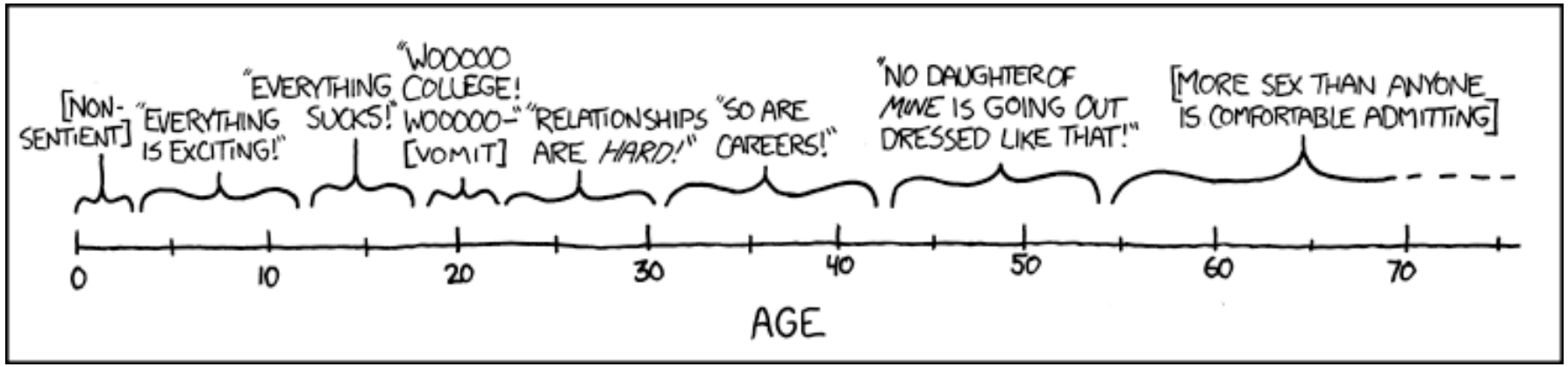
- Look at your logs.
- Write the report. One way to do this is to go to https://www.fedramp.gov/documents/ and use their templates.
- Submit on the agreed upon date.

FOLLOW-UP

david.modic@fri.uni-lj.si

Next steps

- In the contract, you needed to set the timeline.
- Give them at least a week between the report and a meeting.
- Go to a meeting on the specified date.

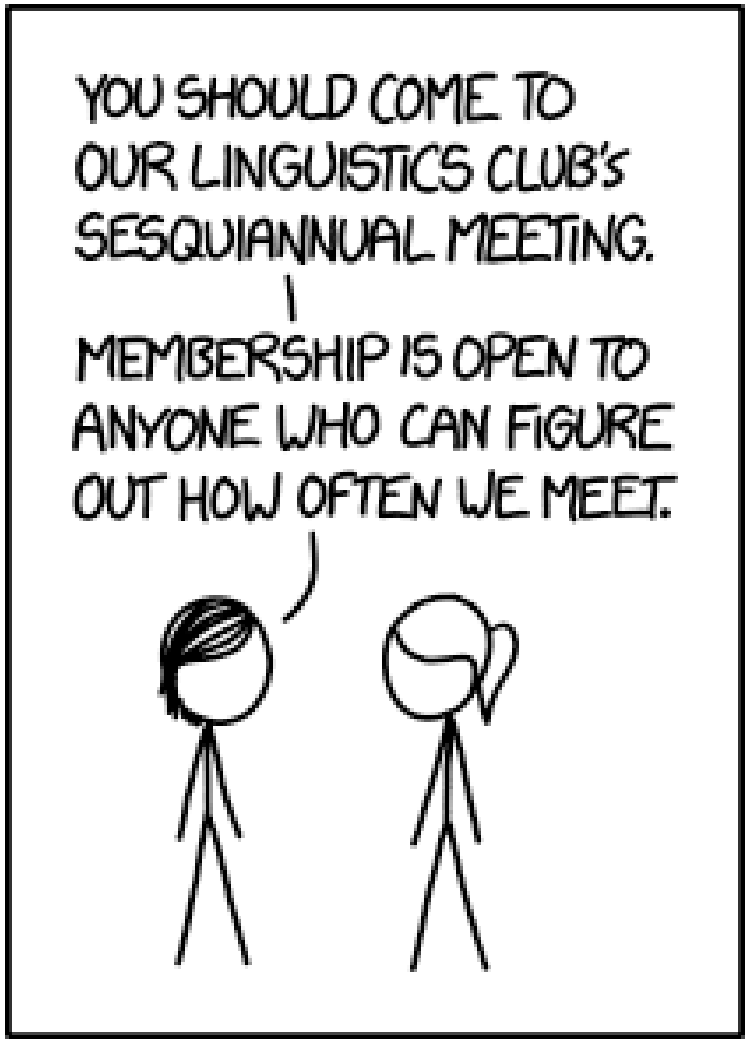


The wrap-up meeting

- Do an **executive summary** and threat assessment.
- Do an overview and propose solutions.
- Depending on the company and their motivation, they will react:
  - Immediately set their teams on patching vulnerabilities and start educating the staff.
  - They will promise everything but do nothing.
  - Only be interested in damage limitation and risk assessment (Finance industry).

The meeting – what you need to get

- Agree on a do-over, specify the timeline if not already, costings etc.
- Push for a firm date of fixes implemented.
- Discuss ethical disclosure.



Follow-up data safety directives - Issues

- Let's say you penetration test and achieve authorized access. You find confidential data.
  - (QUIZ) Do you disclose the breach to the general public?

Follow-up data safety directives - Issues

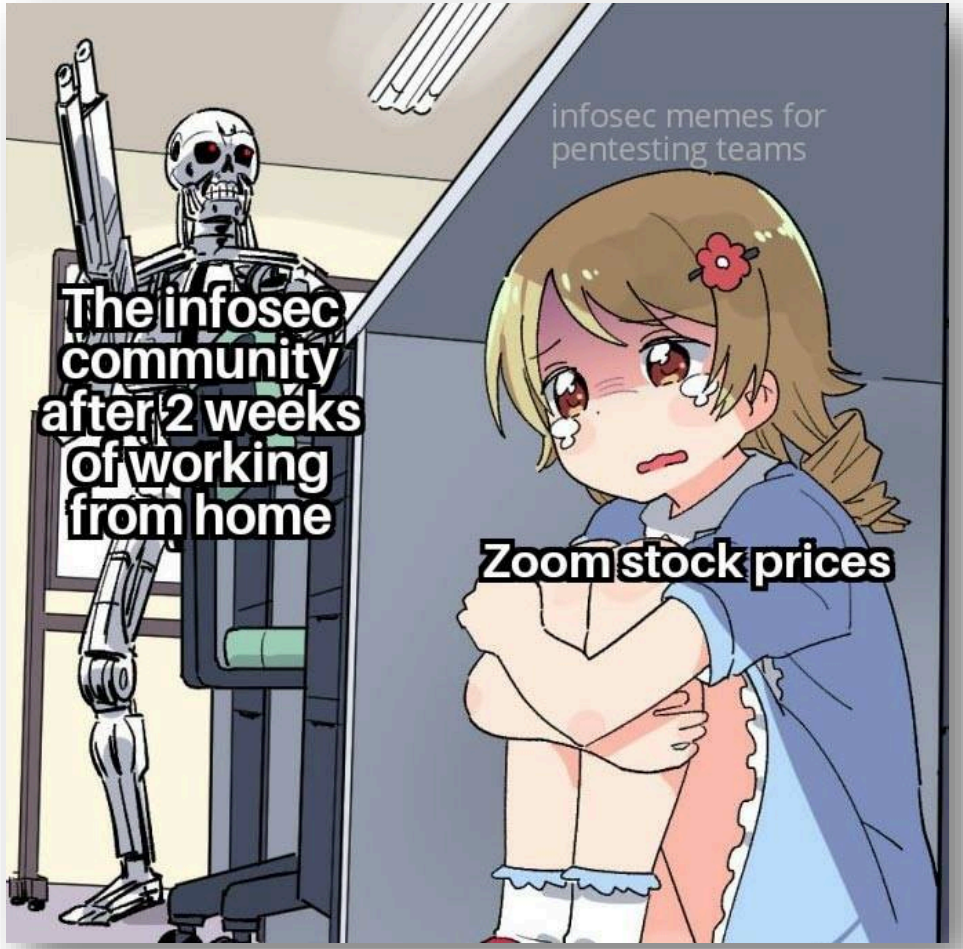
- Let's say you penetration test and achieve authorized access. You find confidential data.
  - (QUIZ) Do you disclose the breach to the general public?
  - Depends on the contract. However, the GDPR guidelines specify that a breach needs to be disclosed in 72 hours from detection. If the company does not, you not liable according to GDPR! You might feel ethically obliged. Discuss it with the employer. Give them time to patch. Follow-up.
  - *There are cases where you cannot disclose a breach: If you discover a vulnerability of the Country's infrastructure, or a defense contractor, disclosure constitutes a breach of the official secrets act and opens you for prosecution (Hitoshi, 2015).*

Once you have submitted a report…

- *It definitively does not end there!*
- Remember a talk about Ethics? If you know an entity is vulnerable, it is your Ethical duty to nudge them.
- Pocketing the money and leaving (*nategn' pa pobegn'* is the Slovene phrase) just makes you an asshole and makes it harder for everyone to have jobs in the future. It also lowers the price of the service.

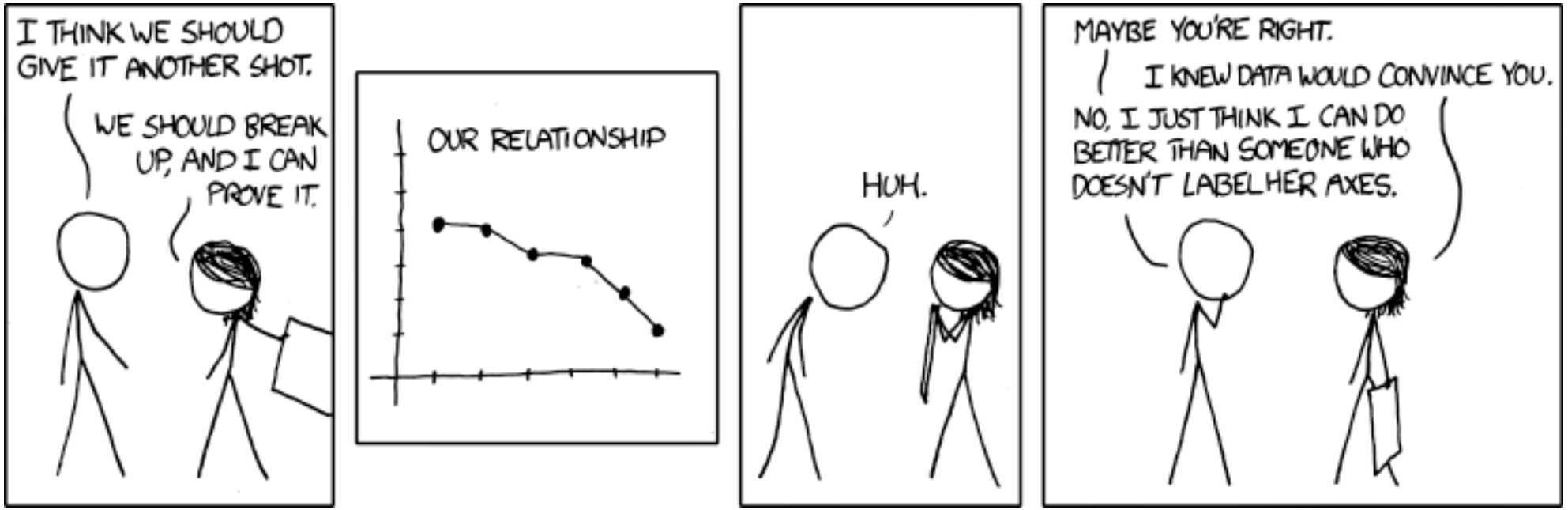
Tales from the field …

- Threats against you and your family (cf. Graham and Saudi Arabia).
- Making you debase yourself (Kieren and me vs. Dubai).
- Unethical behavior of security companies (e.g. reports safety of a Slovene pen-testing company. Expectation of shutdowns, requests for disclosure).



A break

Let's do a short break and then move on to the breach database. 10 minutes?



Univerza *v Ljubljani*
Fakulteta *za računalništvo in informatiko*

Breach database access

doc. dr. David Modic

28/10/20

An Overview

- I'll define a breach database.
- I'll give you access to a Linux Virtual Machine.
- I'll show you how to connect to it.
- I'll go through a practical example of use.
- I'll give you homework ☺.

A breach database

- It is a database of leaked user credentials from a major breach (like linkedin, or yahoo, or Ashley Madison).
- The one we are working with is the one that was leaked in January 2019 and contains 773 million user login details.
- The breach was reported on *ars technica* (*cf.* link on Moodle).
- The database was available on Mega for a while. We have gotten it from Estonian CERT.

Access to the database

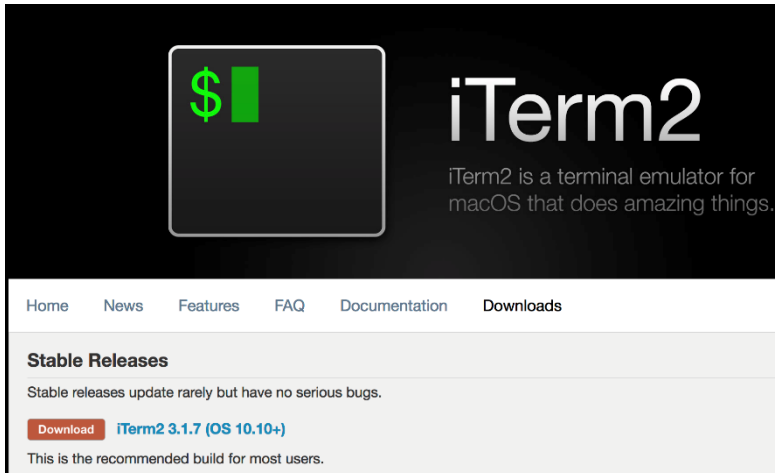
- At your disposal is a fully updated KALI Linux virtual machine. For those of you who are not familiar with KALI – look at: https://www.kali.org/
- It is a distribution that is usually used for penetration testing. There are other solutions, but KALI is the usual one.
- I will **not require you** to install KALI on your machines. No need, we have a virtual machine for that. It runs on 8 Opteron cores, with 16Gb of DDR3 ECC ram (the server is 48 cores, 128 GB DDR3 ECC).
- I will show you how to access it.

Option 1: SSH to the virtual machine

- *A Secure SHell (SSH) connection is a common way to access the command line interface of a remote machine. The connection is encrypted and SSH (if patched) is relatively secure.*
- If you have a *nix machine, you do not need any additional software to do SSH.

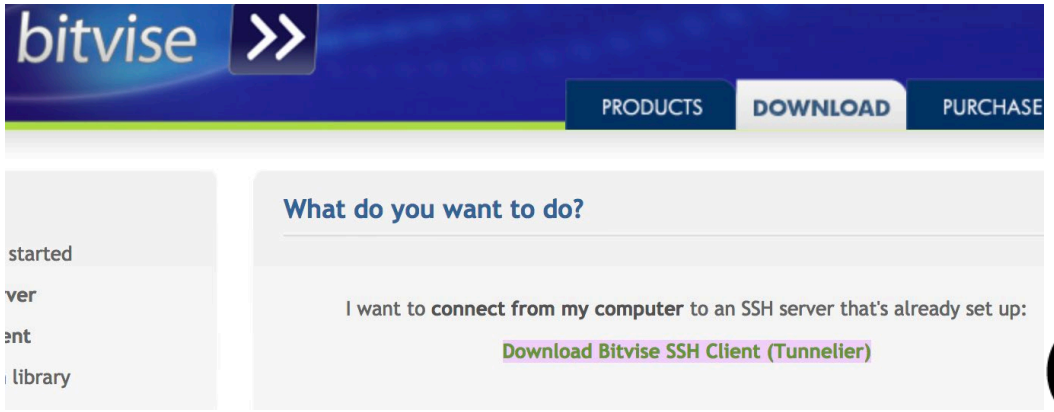
If you have a mac

Download iTerm: https://www.iterm2.com/downloads.html



If you have windows

Download bitTunnelier: https://www.bitvise.com/ssh-client-download



```
u: damjanf        p:[Your STUDENT #]
u: davorh         p:[Your STUDENT #]
u: klemenk        p:[Your STUDENT #]
u: andrazk        p:[Your STUDENT #]
u: aleksanderl    p:[Your STUDENT #]
u: urbann         p:[Your STUDENT #]
u: matejr         p:[Your STUDENT #]
u: andrazs        p:[Your STUDENT #]
u: urbans         p:[Your STUDENT #]
u: evag           p:[Your STUDENT #]
… and so on, you get it.
```

Option 1: SSH to the virtual machine – II.

- *Install your software. AFTER you are done, do this:*

On a mac, open iTerm2

Type:

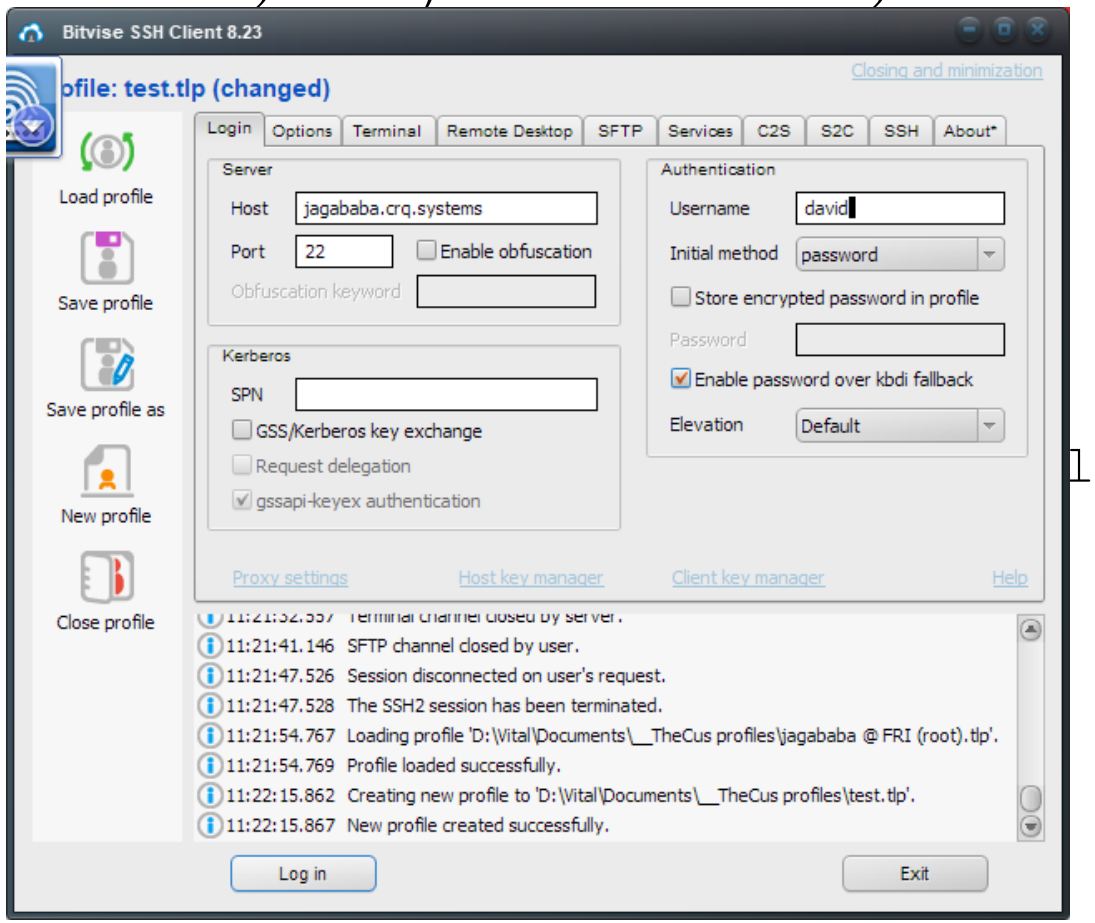
```
User$> ssh jagababa.crq.systems -l
[username]
```

When asked, type: `[your password]`

Option 1: SSH to the virtual machine – II.

- *Install your software. AFTER you are done, do this:*

```
u: damjanf        p:[Your STUDENT #]
u: davorh         p:[Your STUDENT #]
u: klemenk        p:[Your STUDENT #]
u: andrazk        p:[Your STUDENT #]
u: aleksanderl    p:[Your STUDENT #]
u: urbann         p:[Your STUDENT #]
u: matejr         p:[Your STUDENT #]
u: andrazs        p:[Your STUDENT #]
u: urbans         p:[Your STUDENT #]
```

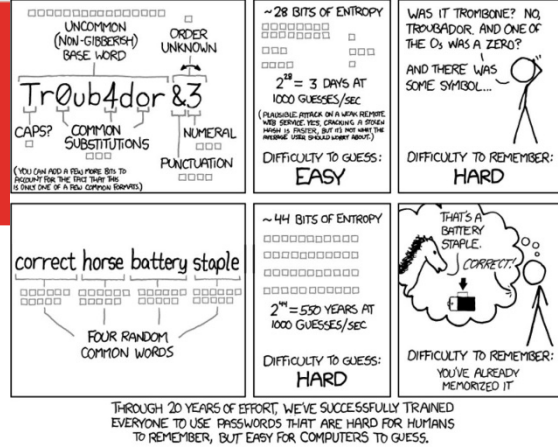


Under HOST: jagababa.crq.systems
Port: 22
Username: *[username]*
Initial method [select]: password
If you want click *Store encrypted password in profile.*
Password: *[your student ID]*

Leave everything else as is.

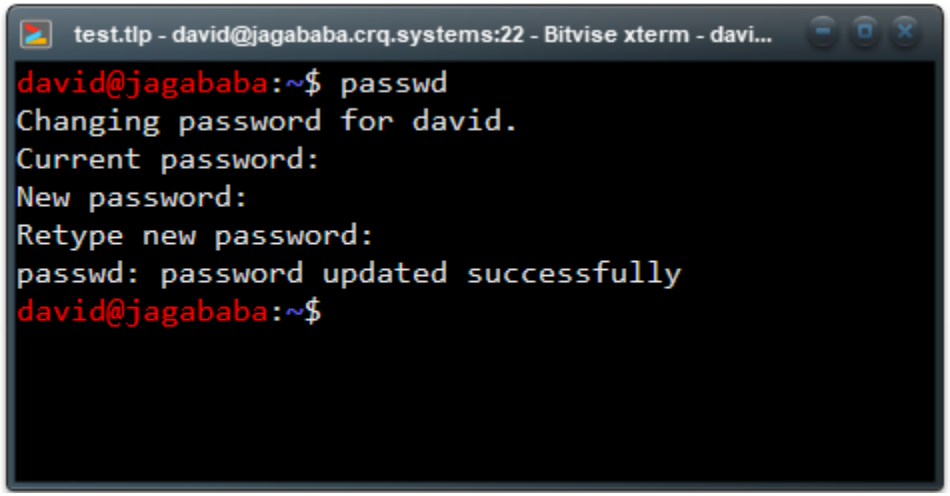
Click *Save profile as*
[Give the profile a name, like FRI_INFOSEC]

Click Login (bottom left)



Option 1: SSH to the virtual machine – III.

- *Immediately change your password! Yes, now!*
- In the terminal window type: `passwd`
- Enter your old password.
- Enter your new password.
- Again, enter your new password.



Notes: **Do NOT REUSE passwords**! Follow the password creation guidelines.

- What are they?

(length > 12 characters, best if several words unconnected, like horse staple battery. Do not use those! NO: 1st UPPERCASE, last number).

A bit about information gathering

- `traceroute` *tells you something about the path between you and between your target.*
- Let me give you an example (type with me, if you wish):

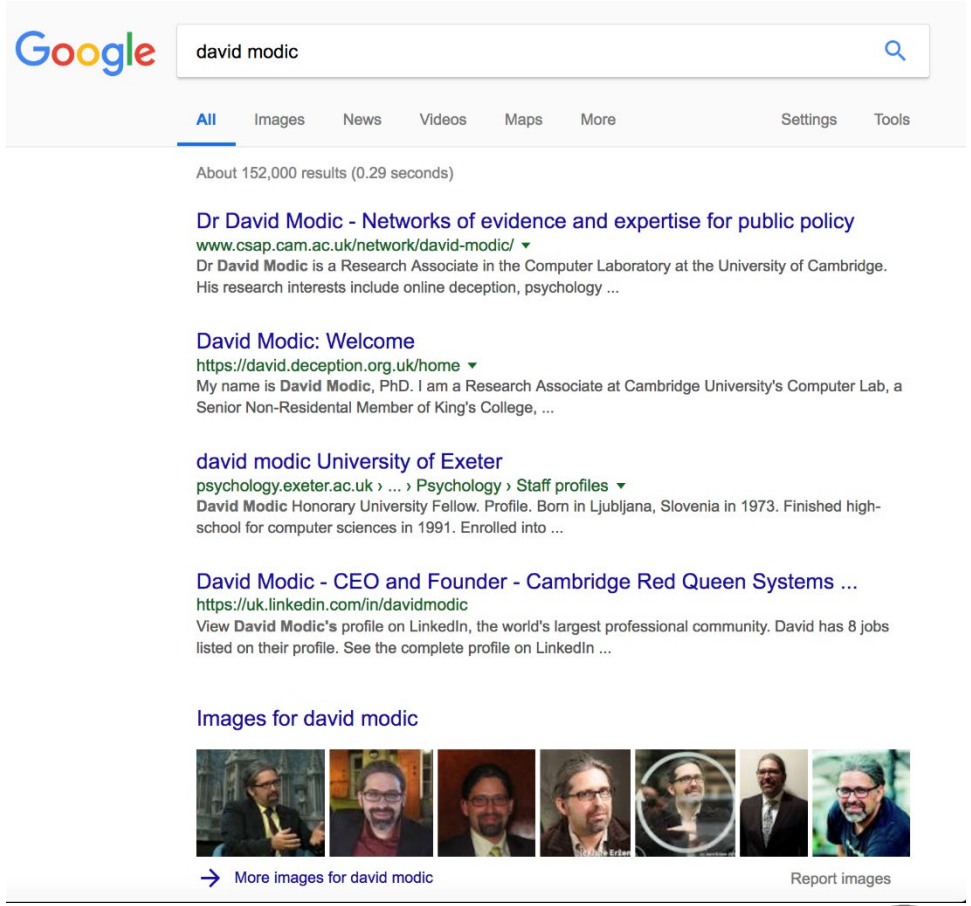
```
traceroute titania.crq.systems
```

- Now, I get an IP. Who is responsible for this IP? I'll use `whois`
- *(IP at the time of writing was: 88.200.24.195)*

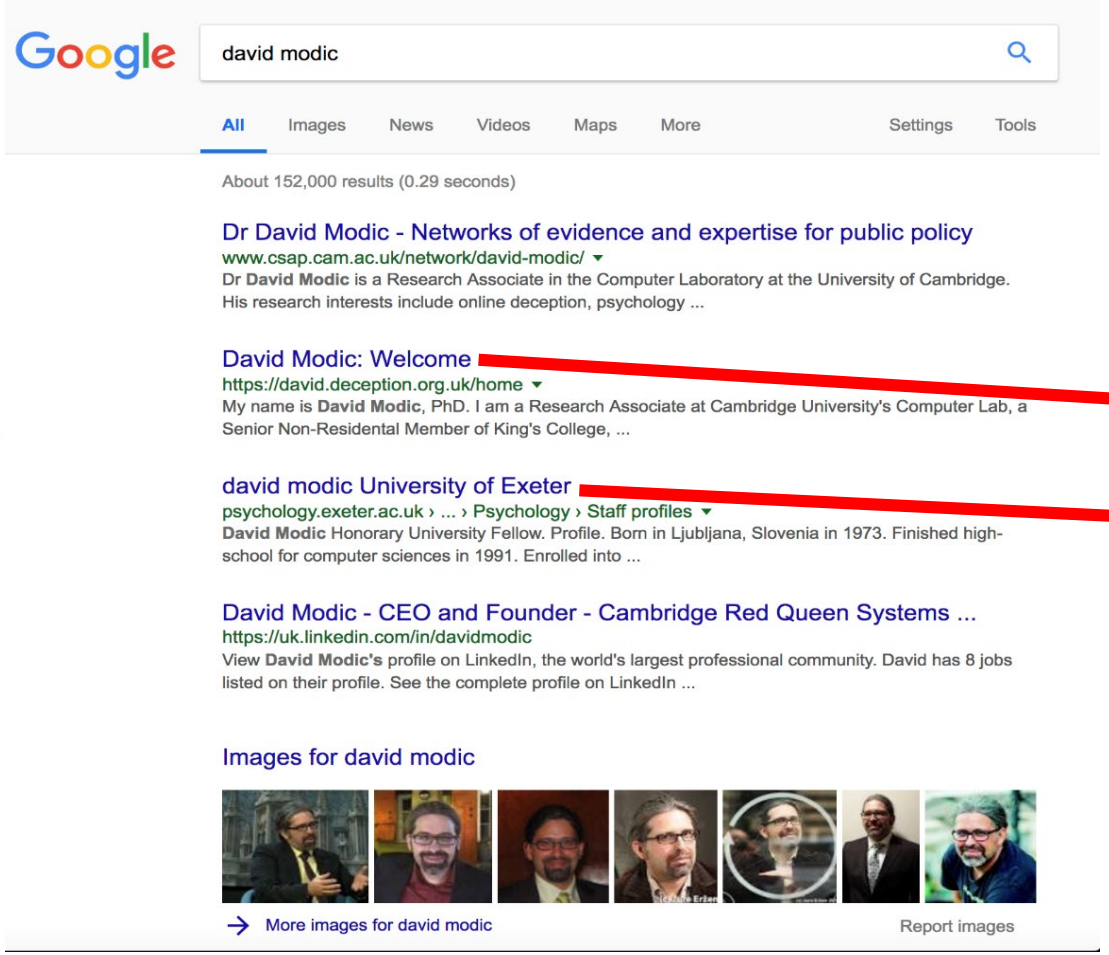
```
whois 88.200.24.195
```

A bit about information gathering

- `whois` output sometimes shows the owner of domain.
- Let's not gather intelligence on them. This is, however, my VM.
- So let's pretend that it was my name that was listed.
- We google my name.



A bit about information gathering



CAMBRIDGE RED QUEEN & UNIVERSITY OF CAMBRIDGE \ DAVID MODIC

home | bio | current work | conferences | teaching | research interests | publications.. | links

Welcome

Hi.

My name is David Modic, PhD. I am a Research Associate at Cambridge University's Computer Lab, a Senior Non-

KulturKontakt (Graz, Austria), an on-line network providing whole field of South – Eastern Europe. The project is spons The Austrian Ministry of Education, Science and Culture. W

Links

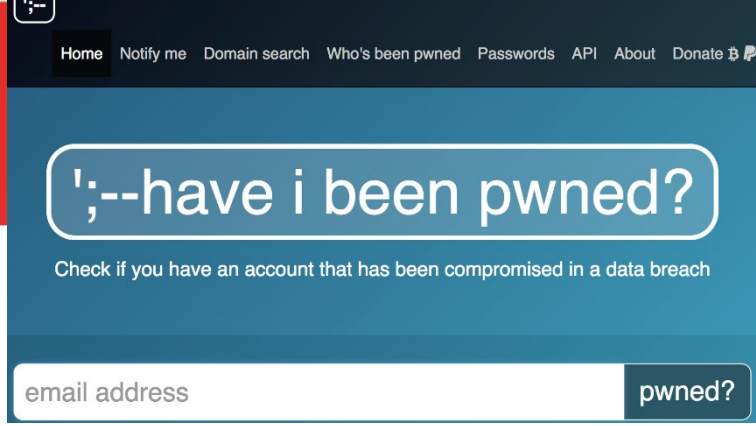
- David's blog

Research group links

- Social, Environmental and Organisational

Contact details

Email	D.Modic@exeter.ac.uk
Tel	+44 759 595 1920
Address	Washington Singer Laboratories University of Exeter Perry Road Prince of Wales Road Exeter EX4 4QG UK
Office	304



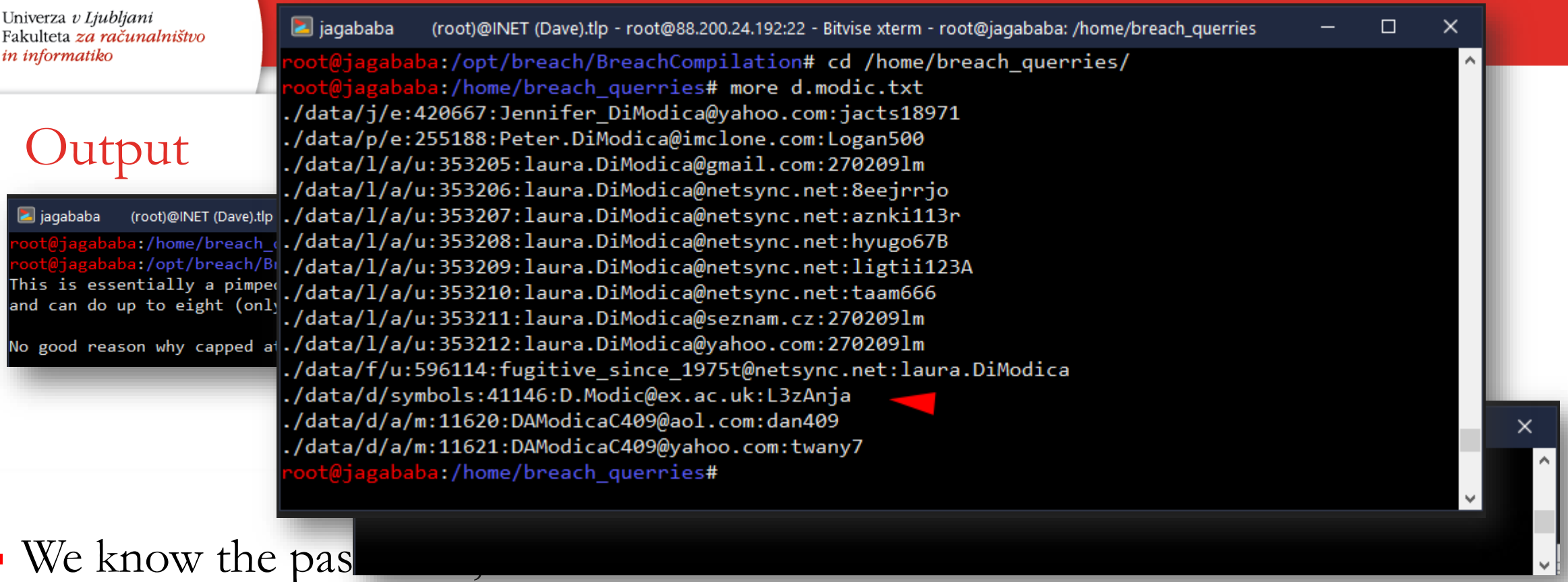
Information gathering

- I now have two email addresses: david.modic@cl.cam.ac.uk and d.modic@exeter.ac.uk.
- I'll do two things:
  - (a) Use the breach database. Our BD does not tell you which site the data comes from.
  - Bonus question. Why is not knowing the origin not a big problem?
  - (b) Because, I can use - https://haveibeenpwned.com, an online resource, where you enter an email and it tells you whether it was breached and on which site.

Information gathering – Breach DB

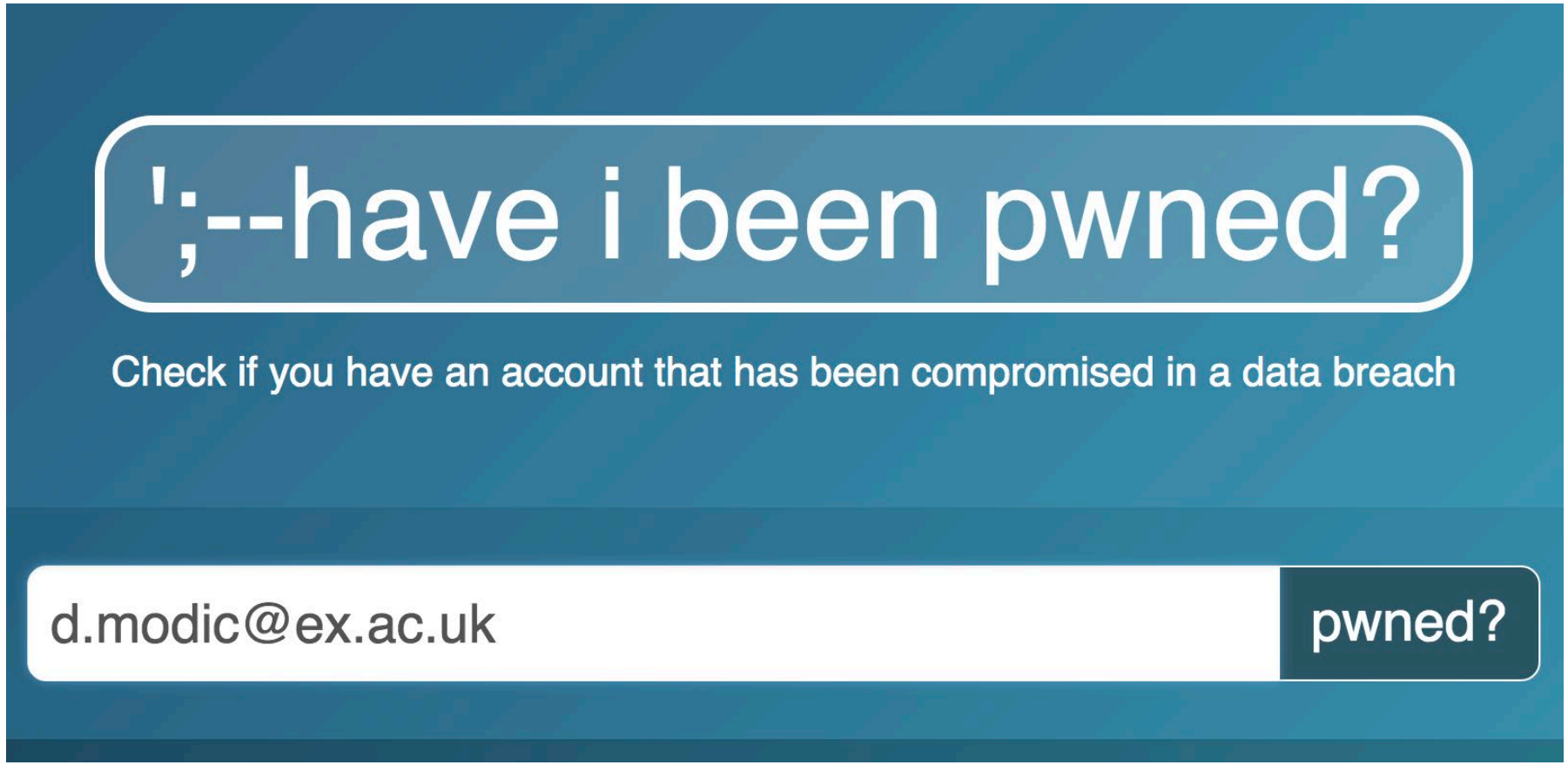
- Use the script in the virtual machine, this is how:
- Connect to the VM with your ssh client (`ssh jagababa.crq.systems -l [your username]`)
- Type in the password, when required.
- david@jagababa:~$ **`cd /opt/breach/BreachCompilation/`**
- david@jagababa:/opt/breach/BreachCompilation$ **`sudo ./multi.query.nomore.sh [term1] [term2] [term3]`** …
- The results are stored in **`/home/breach_querries/[term1].txt`** (e.g. david.modic.txt)
- david@jagababa:/opt/breach/BreachCompilation$ **`cd /home/breach_querries`**
- david@jagababa:/home/breach_querries$ **`more david.modic.txt`**
- ***CAREFUL:*** *unix systems distinguish between lower and UPPER case (*D.Modic, d.Modic and d.modic are three separate entries*).*

Output



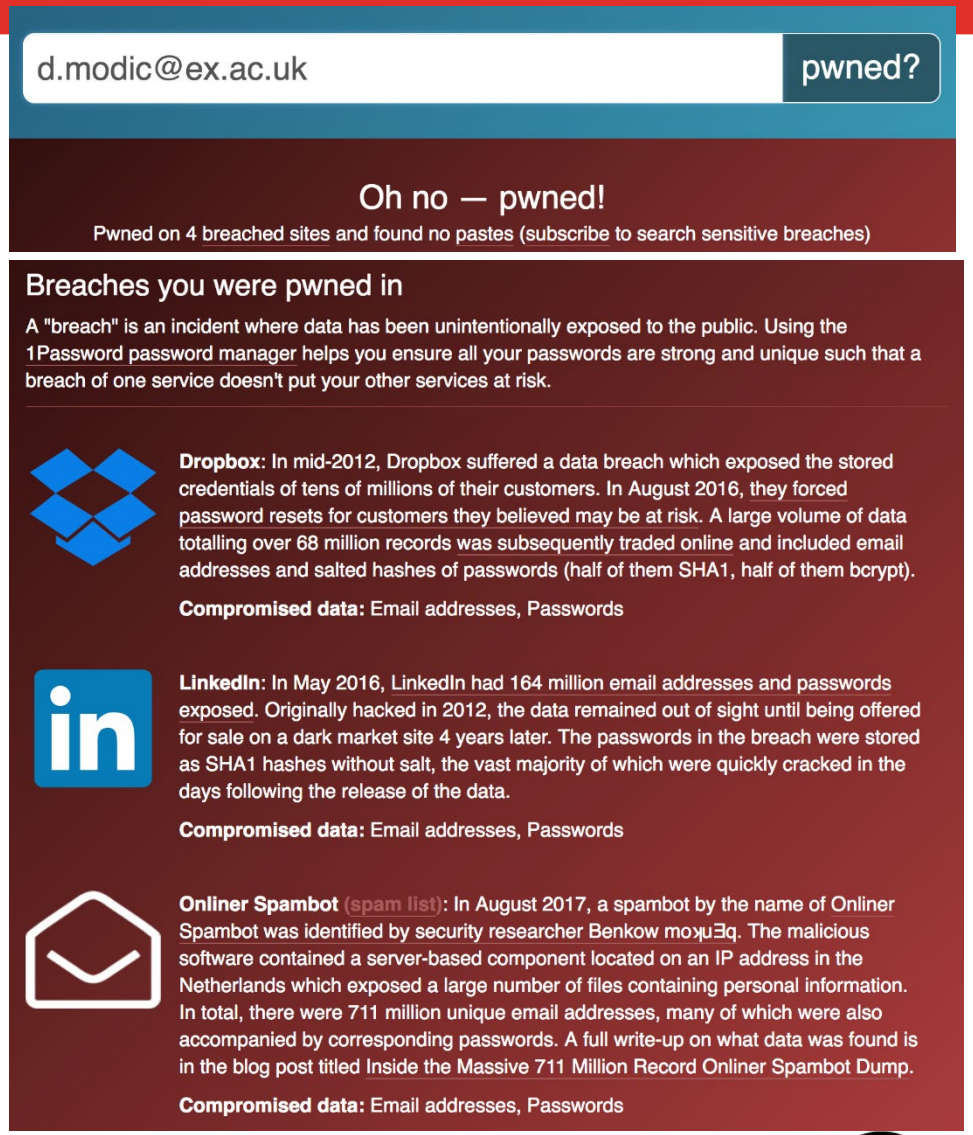
- We know the pas
- **Bonus question: Is it ethical and lawful to use this password to log-in somewhere as me?**

Visit https://haveibeenpwned.com and enter my email address:



Haveibeenpwned?

- Ah schucks I am toast ☹. We now know my LinkedIn password.
- (This is not news to me. The password has been changed long ago, and email is not in use anymore.)
- But, you might want to check to see whether you have been pwned.
- Bonus question: If my password is listed, do I have to change it every-where or just on breached sites?



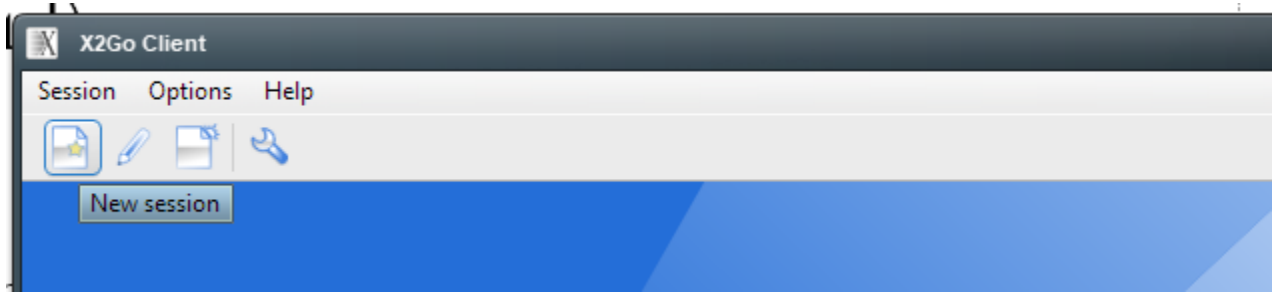
Another useful tool - nmap

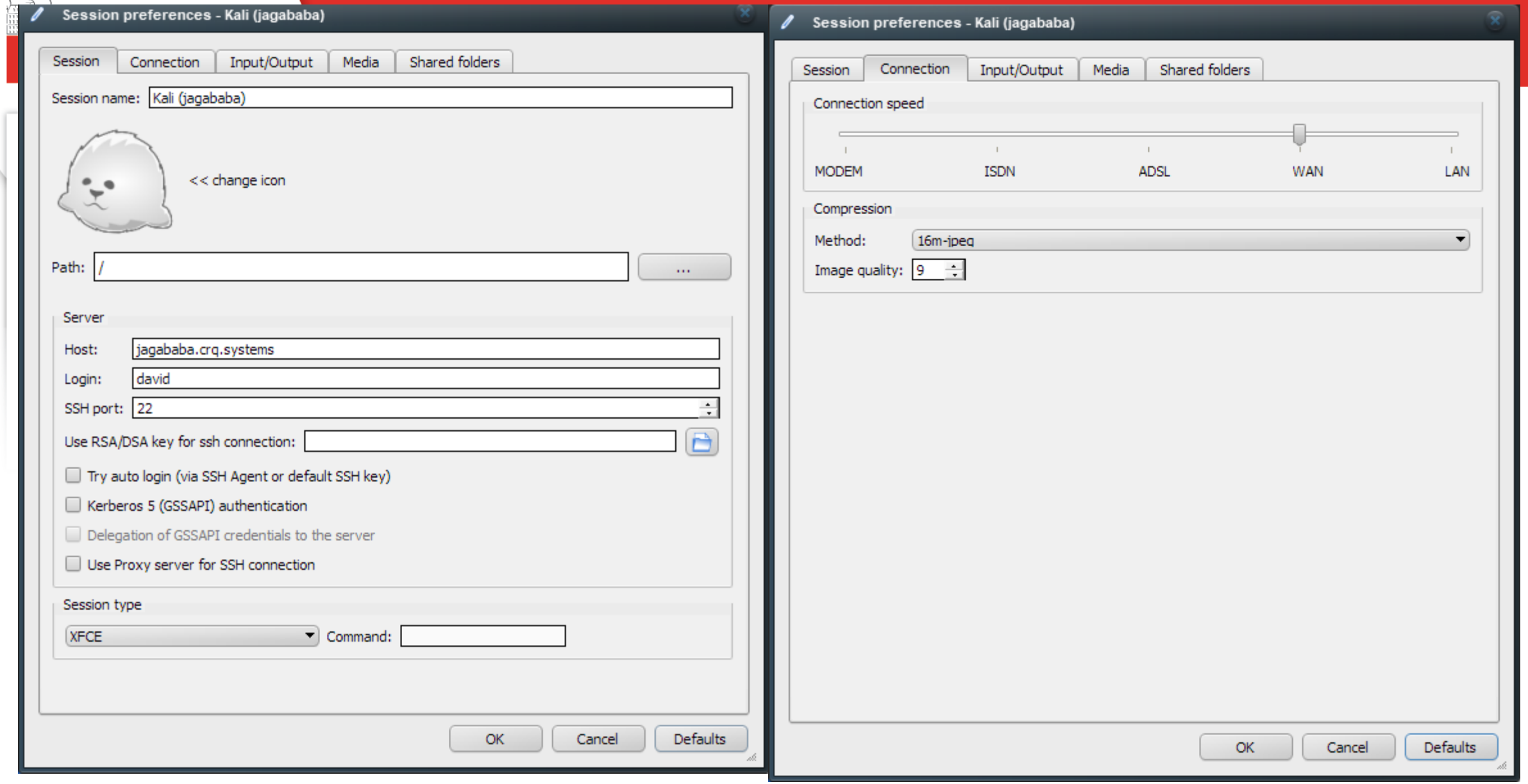
- `nmap` scans a given network. Here is the link to an online manual: https://highon.coffee/blog/nmap-cheat-sheet/
- nmap is a network mapper, or a *scanner*. They are *not passive*. They do get detected. You will light up like a Christmas tree on an IDS'.
- (There are ways around that, but they are not needed for this course).
- You will get detected at Cambridge, but they will let me know, and I'll OK it, during the course. But not after ;).
- **NOTE that you will need to sudo nmap!**

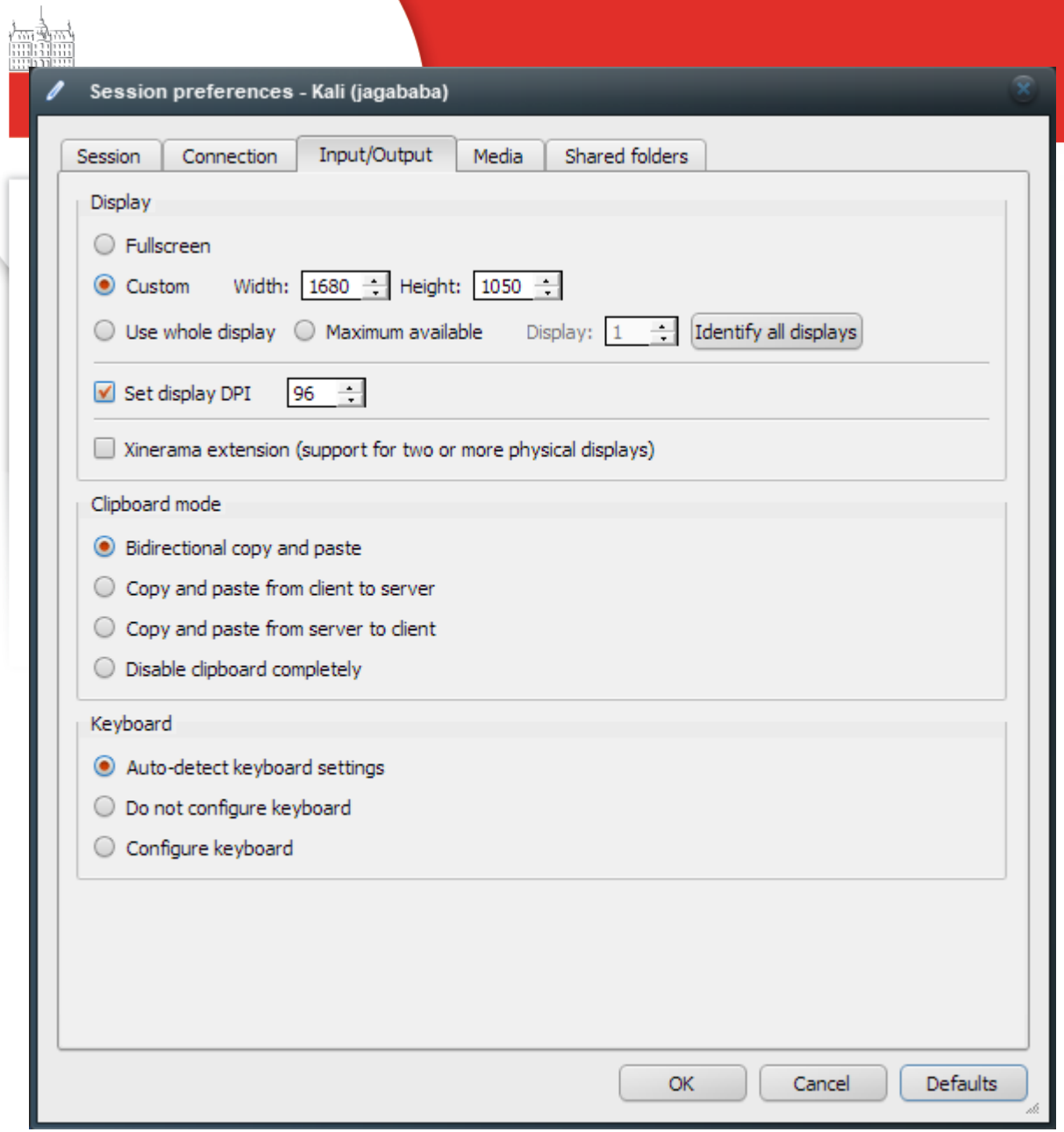
GUI access to the virtual machine

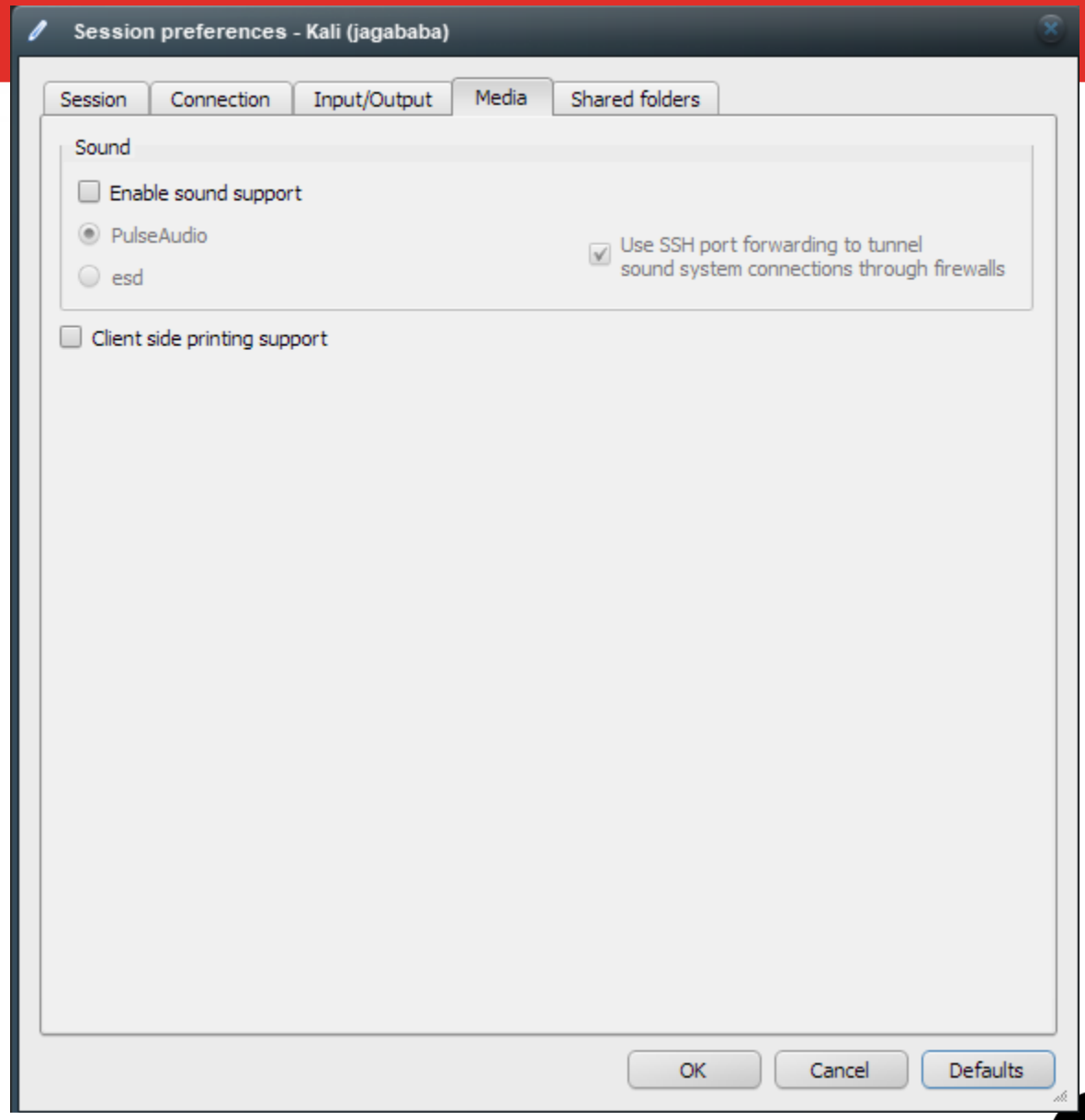
- You can connect through secure shell (as you did).
- Or by using a graphical interface. Some tools at your disposal have GUI's .
- We will use X2GO client. NoMachine would also work.
- Connect to the: https://wiki.x2go.org/doku.php
- This is an x-windows server (I know, it should be a client. It is a **nix thing*).
- It runs on Windows, MAC and Linux.
- *Follow instructions on the page*. For the x2go client.
- Once installed do run it and do this:

GUI access to the virtual machine

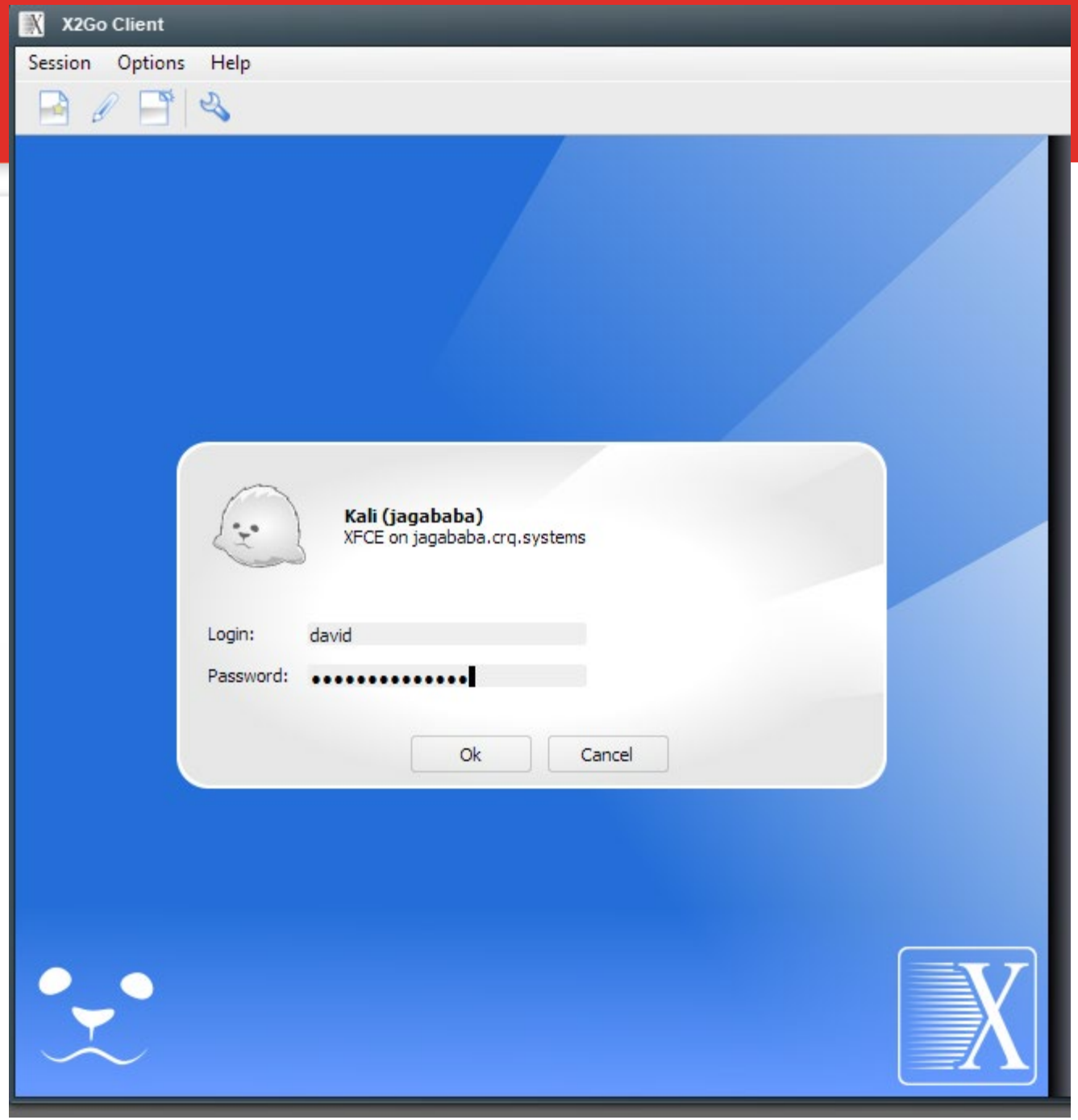


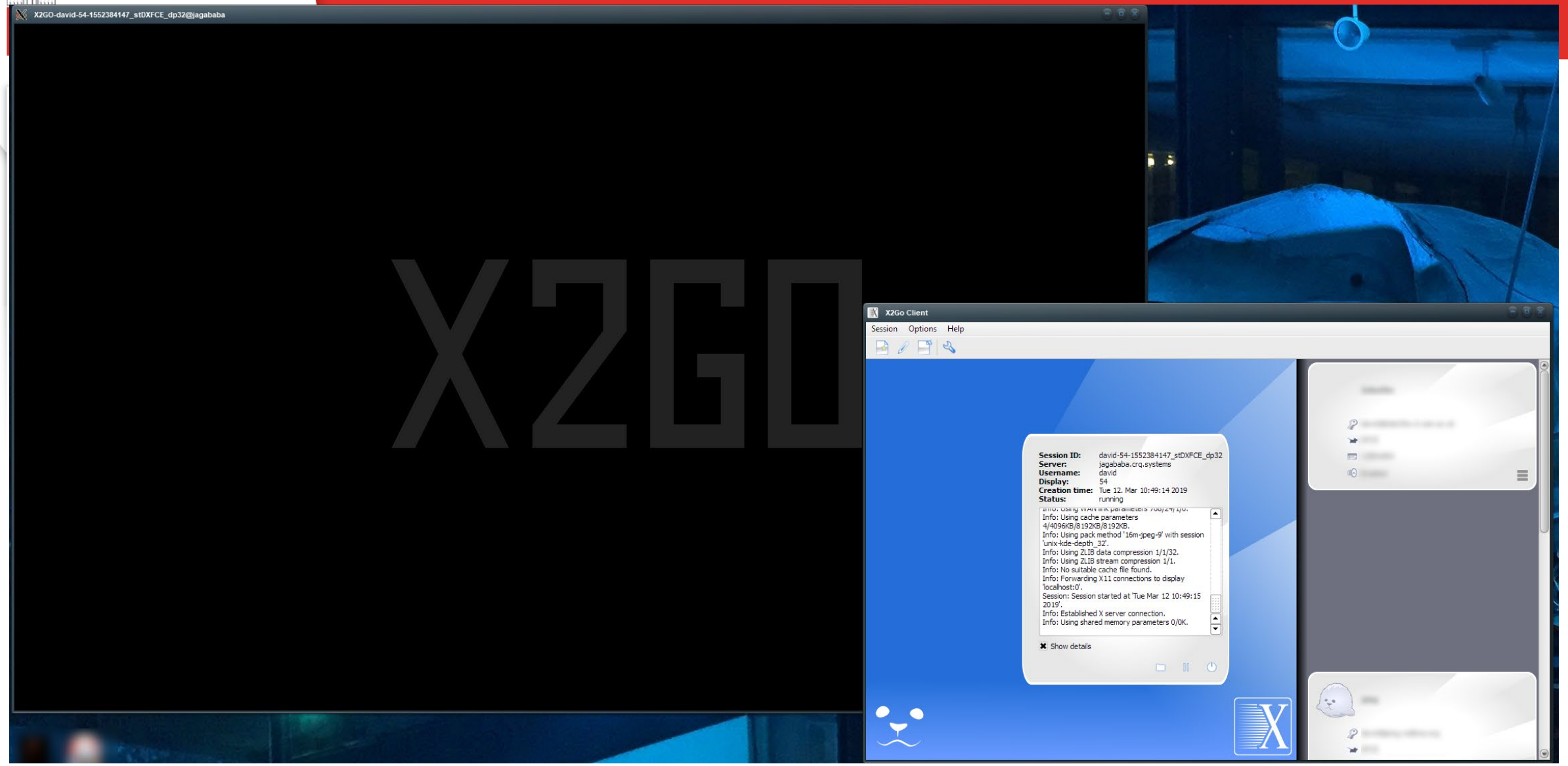

Session preferences - Kali (jagababa)
Session
Connection
Input/Output
Media
Shared folders
Session name: Kali (jagababa)
<< change icon
Path: /
...
Server
Host: jagababa.crq.systems
Login: david
SSH port: 22
Use RSA/DSA key for ssh connection:
Try auto login (via SSH Agent or default SSH key)
Kerberos 5 (GSSAPI) authentication
Delegation of GSSAPI credentials to the server
Use Proxy server for SSH connection
Session type
XFCE
Command:
OK
Cancel
Defaults
Session preferences - Kali (jagababa)
Session
Connection
Input/Output
Media
Shared folders
Connection speed
MODEM
ISDN
ADSL
WAN
LAN
Compression
Method: 16m-jpeg
Image quality: 9
OK
Cancel
Defaults


Session preferences - Kali (jagababa)
Session
Connection
Input/Output
Media
Shared folders
Display
Fullscreen
Custom
Width:
1680
Height:
1050
Use whole display
Maximum available
Display:
1
Identify all displays
Set display DPI
96
Xinerama extension (support for two or more physical displays)
Clipboard mode
Bidirectional copy and paste
Copy and paste from client to server
Copy and paste from server to client
Disable clipboard completely
Keyboard
Auto-detect keyboard settings
Do not configure keyboard
Configure keyboard
OK
Cancel
Defaults


Session preferences - Kali (jagababa)
Session
Connection
Input/Output
Media
Shared folders
Sound
Enable sound support
PulseAudio
esd
Use SSH port forwarding to tunnel sound system connections through firewalls
Client side printing support
OK
Cancel
Defaults

GUI access to the




X2GO-david-54-1552384147_stDXFCE_dp32@jagababa
X2GO
X2Go Client
Session Options Help
Session ID: david-54-1552384147_stDXFCE_dp32
Server: jagababa.crq.systems
Username: david
Display: 54
Creation time: Tue 12. Mar 10:49:14 2019
Status: running
Info: Using cache parameters 4/4096KB/8192KB/8192KB.
Info: Using pack method '16m-jpeg-9' with session 'unix-kde-depth_32'.
Info: Using ZLIB data compression 1/1/32.
Info: Using ZLIB stream compression 1/1.
Info: No suitable cache file found.
Info: Forwarding X11 connections to display 'localhost:0'.
Session: Session started at 'Tue Mar 12 10:49:15 2019'.
Info: Established X server connection.
Info: Using shared memory parameters 0/0K.
Show details


X2GO-david-54-1552384147_stDXFCE_dp32@jagababa
Applications
10:50
David Modic
Run Program...
Terminal Emulator
File Manager
Mail Reader
Web Browser
Settings
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
13 - Social Engineering Tools
14 - System Services
Accessories
Development
Graphics
Internet
Multimedia
Office
Other
System
About Xfce
Log Out
• DNS Analysis
• IDS/IPS Identification
• Live Host Identification
• Network & Port Scanners
• OSINT Analysis
• Route Analysis
• SMB Analysis
• SMTP Analysis
• SNMP Analysis
• SSL Analysis
dmitry
dnmap-client
dnmap-server
ike-scan
maltego
netdiscover
nmap
p0f
recon-ng
sparta
zenmap
CAMBRIDGE
RED QUEEN

jagababa.crq.systems

- As mentioned, this is a rolling Kali install – updated every few days.
- Amongst *many* other things, it offers Armitage, which is a GUI to access Metasploit.
- Metasploit is an exploit framework and vulnerability scanner – constantly updated.
- For many intents and purposes this is all you will ever need to probe mechanical vulnerabilities.
- Whether you need to do this at all will be the topic for the next lecture.

Homework 2 (by Monday November 2nd 12:00) – PART 1

- Check yourself in the *breach_db* **and** on the https://haveibeenpwned.com. Check all the email addresses you use (each is a separate query).
- Example

```
./multi.query.nomore.sh joe.blow joe@example.com joe.blow@gmail.com
more /home/breach_querries/joe.blow.txt
```

- Change passwords if you've found yourself anywhere.
- Submit to me in the form of:

  Your name.

  Homework 2

  [syntax used]

  <actions taken, if any> i.e. if you needed to change your passwords, report doing so).

- Do NOT send passwords ☺!

Homework 2 (by Monday November 2nd 12:00) – PART 2

- use nmap
- Task 3: Which operating system is running on titania.crq.systems?
  - Bonus points if you find you can tell me which version.
- Task 4: Which standard ports are open on titania.crq.systems?
  - Bonus points if you tell me whether all are accessible to everyone.

- Submit the results to me, containing:
- Homework 2, Part 2, [Your name].
- Task 3: Command used Task 1: result
- Task 4: Command used Task 2: results

Before you go…

- **I some people have contacted me already about shodan and metasploit. I will create a slack channel for those specific folks.**
- One to prepare a talk about Shodan (https://www.shodan.io/).
- One to prepare a talk about Metasploit / Armitage (runs on jagababa).
- Send me an email or slack DM if interested.

Next Time…

- **4th November, 2020 @ 16:30**
- We will talk about open source intelligence (OSINT) gathering, with examples.