Teoria e Prática de Ataques de Segurança

2025/2026

André Baptista
andre.baptista@fc.up.pt

Miguel Regala
miguel.regala@fc.up.pt

https://tpas.alunos.dcc.fc.up.pt

FACULDADE DE CIÊNCIAS
UNIVERSIDADE DO PORTO

Catch-up

- Tailscale access (VPN) (form link)
- Access to TPAS desafios (https://tpas-desafios.alunos.dcc.fc.up.pt/)
- Groups & CVEs submission (form link) (answers) - until October 2th
  - “flash” presentation October 9th, **remote**

Agenda

- A (little) bit of network
- Recon
- Practice

Class 2

Networks and reconnaissance

FACULDADE DE CIÊNCIAS
UNIVERSIDADE DO PORTO


Weld Pond | Chris Wysopal
@WeldPond
City of Arkansas City, KS faces cybersecurity Incident at water treatment facility. On detection they switched to manual operation and they state that water is safe.
arkcity.org
City of Arkansas City Faces Cybersecurity Incident
The City of Arkansas City encountered a cybersecurity issue early Sunday morning, September 22, 2024, involvin...
12:42 PM · Sep 24, 2024 · 50K Views

Background

OSI model and TCP-IP

https://www.youtube.com/watch?v=2QGgEk20RXM

OSI model

OSI Model			
Layer		Protocol data unit (PDU)	Function[3]
Host layers	7. Application	Data	High-level APIs, including resource sharing, remote file access
	6. Presentation		Translation of data between a networking service and an application; including character encoding, data compression and encryption/decryption
	5. Session		Managing communication sessions, i.e. continuous exchange of information in the form of multiple back-and-forth transmissions between two nodes
	4. Transport	Segment, Datagram	Reliable transmission of data segments between points on a network, including segmentation, acknowledgement and multiplexing
Media layers	3. Network	Packet	Structuring and managing a multi-node network, including addressing, routing and traffic control
	2. Data link	Frame	Reliable transmission of data frames between two nodes connected by a physical layer
	1. Physical	Symbol	Transmission and reception of raw bit streams over a physical medium

From Wikipedia

Devices

- Physical layer (signals):
  - Network cables, fibre optic cables
  - Repeaters, antennas
- Data link layer (logical):
  - Switches, bridges, NICs
- Network layer (routing):
  - Routers, gateways, layer 3 switches

Ethernet

Preamble	SFD	Destination MAC Address	Source MAC Address	EtherType	Payload	FCS

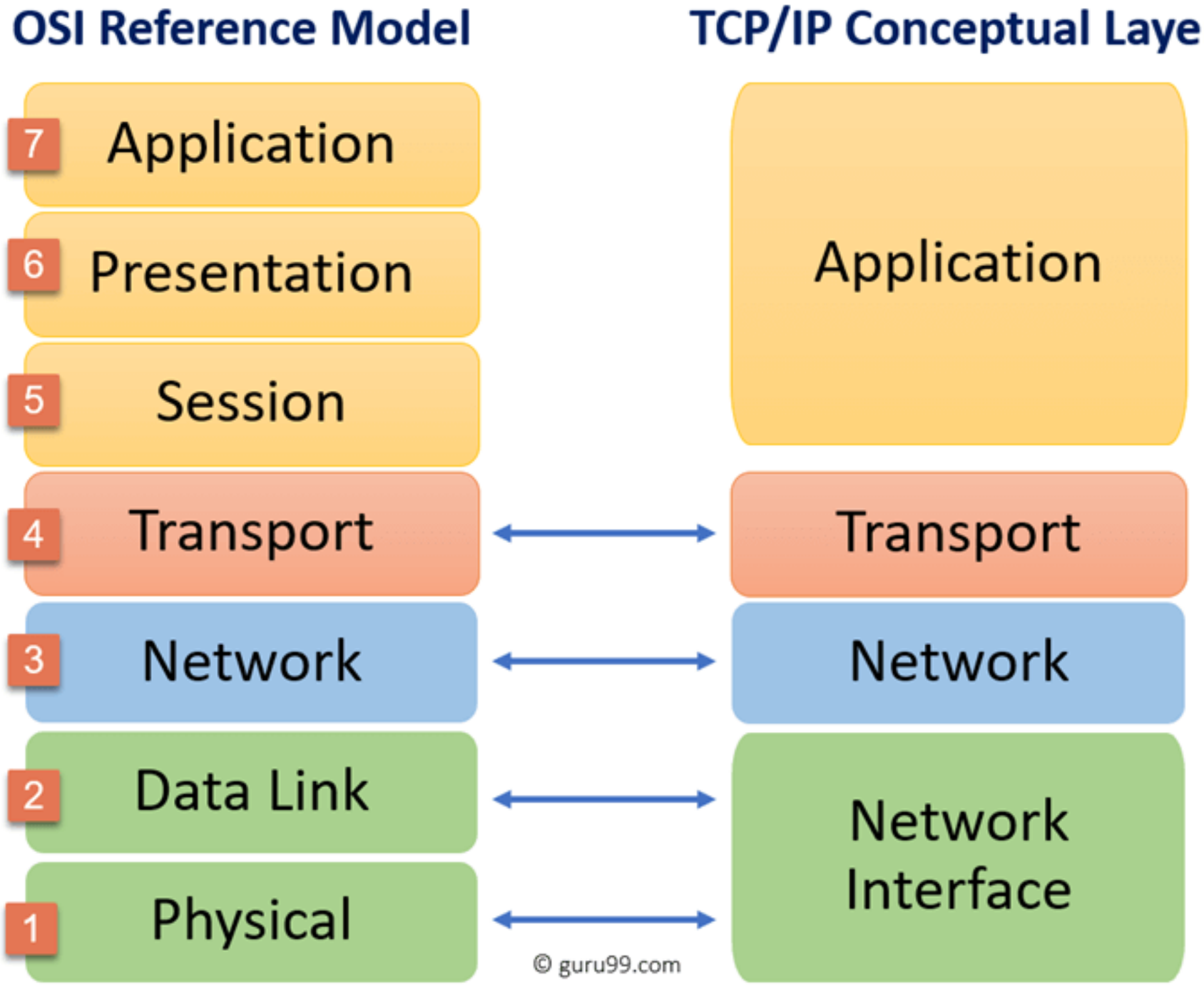
TCP Segment / UDP Datagram -> Transport layer

IP packets -> Network layer

Ethernet packets -> Data link layer

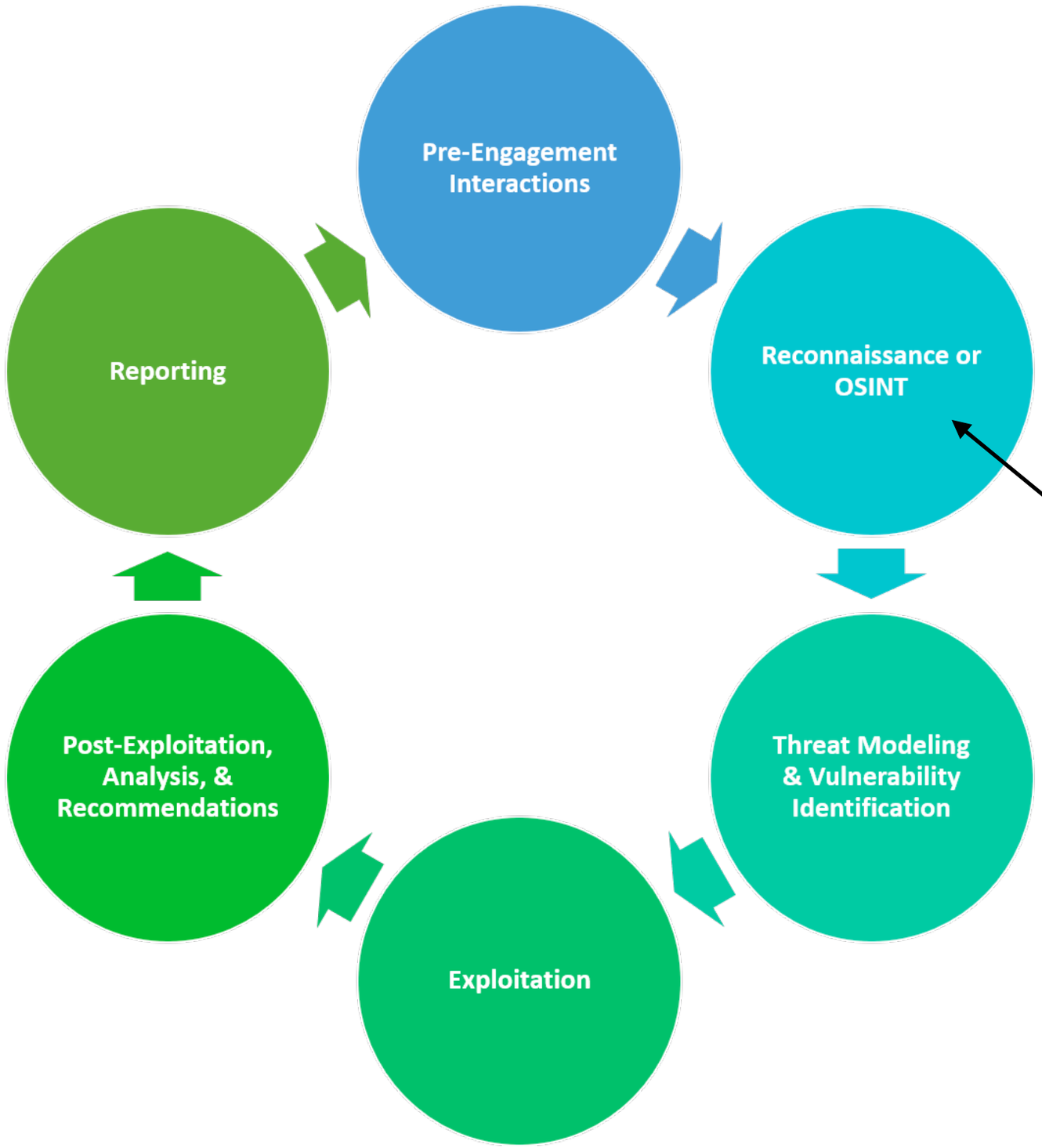
From Wikipedia

OSI <-> TCP/IP


OSI Reference Model
TCP/IP Conceptual Layers
7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data Link
1 Physical
Application
Transport
Network
Network Interface
© guru99.com

Agenda

- Recon
- Search engines
- Network fingerprinting
- Operating systems
- Social engineering and social networks
- Countermeasures



From Cipher blog

Reconnaissance

- Collecting information
  - Passive - public sources: IP addresses, networks, OS, web servers, services, architectures, intrusion detection systems, technologies, etc.
  - Active ⚠️ - subdomain enumeration (active), port scanning, content discovery tools, bruteforce, social engineering, etc.

Reconnaissance

- Information sources:
  - Anonymous - The information provider tries to keep the identity anonymous.
  - Alias - Sources where the provider keeps the same fake name or handle for communication.
  - Organization-based - leveraging resources of an organization to obtain information
  - Internet - using the internet (e.g. social networks, dorks, shodan, wayback machine, and other databases) to retrieve information

Important information

- Network: domain names, SSL certificates, IP ranges, internal networks, public websites, exposed services, protocols, ACLs and authentication mechanisms.

- Systems: users and groups, banners, routing tables, architecture. Operating systems, software and versions.

- Organization: employees, collaborators, partners, phones, websites, locations, frontend code (comments, copy-paste), security policies, github, press releases, blog posts, job posts.

Recon risks

- A real attacker while performing successful recon may directly:
  - Obtain sensitive information about a target
  - Perform social engineering
  - Disrupt networks and systems
  - Steal and leak information
  - Impact privacy
  - Obtain business secrets (Industrial espionage)
  - Impact revenue and profit of the organization

Recon

- Recon is the process of collecting all the information that allows an attacker to find potential attack vectors within a scope. As an ethical hacker you should:

  - Retrieve basic information about the target and network

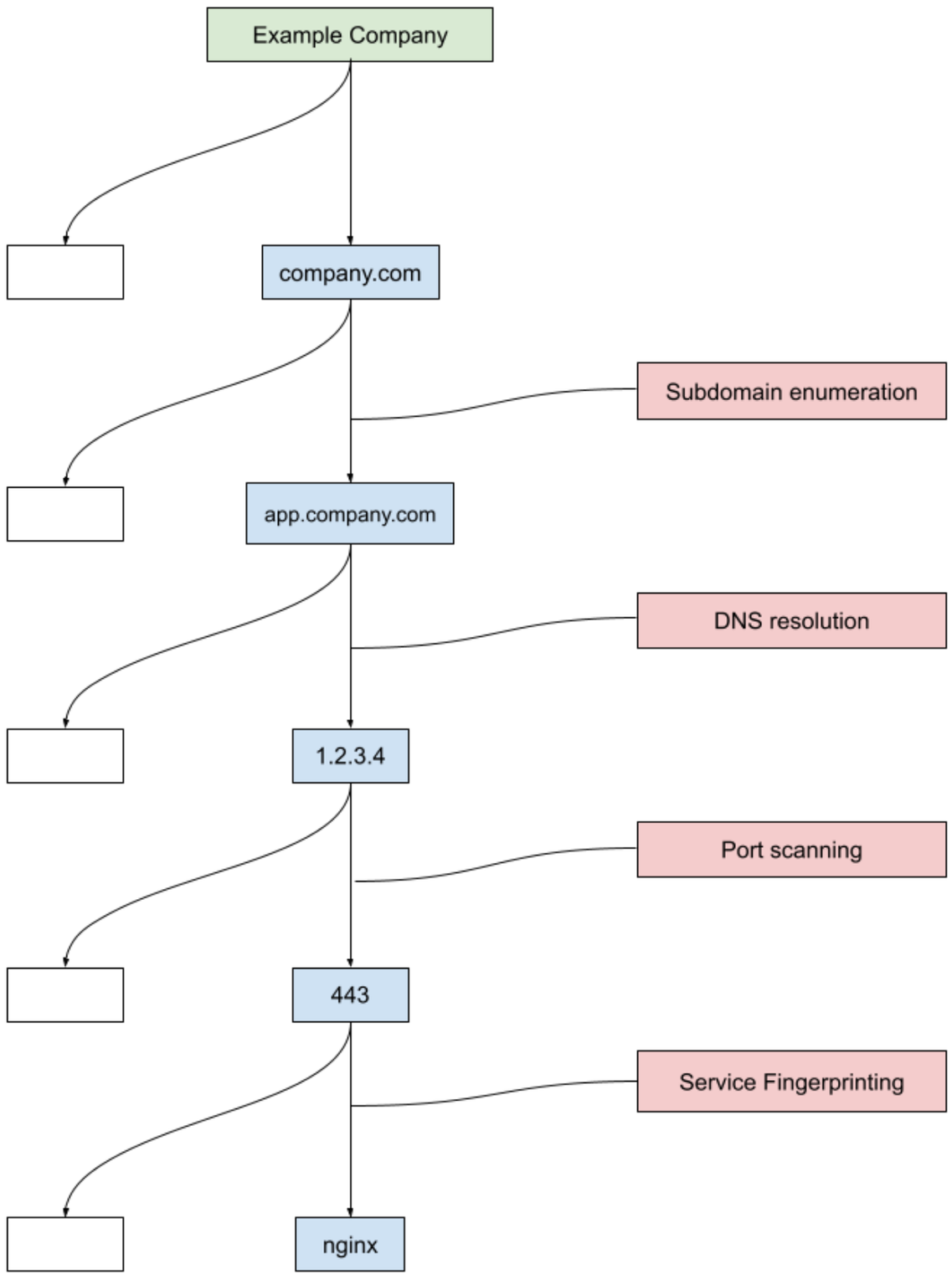
  - Identify operating systems, platforms, technologies, services (http, https, ssh, ftp, etc)

  - Use techniques such as WhoIS and DNSdumpster

  - After recon, we can try to find vulnerabilities and run exploits against services or systems

Recon

- Recon should be performed carefully.
- Main goals are:
  - Understanding the security posture of the target
  - Mapping the attack surface
  - Building a knowledge base
  - Mapping the target systems, networks and services


Example Company
company.com
Subdomain enumeration
app.company.com
DNS resolution
1.2.3.4
Port scanning
443
Service Fingerprinting
nginx

Subdomain enumeration

- **Passive tools:** subfinder, assetfinder, chaos, https://crt.sh
- **Active tools:** dnsx, puredns, massdns, amass ⚠️

```
→  /tmp subfinder -d up.pt

                __     _____           __
   _______  __/ /_  / __(_)___  ____/ /__  _____
  / ___/ / / / __ \/ /_/ / __ \/ __  / _ \/ ___/
 (__  ) /_/ / /_/ / __/ / / / / /_/ /  __/ /
/____/\__,_/_.___/_/ /_/_/ /_/\__,_/\___/_/ v2.5.0

                projectdiscovery.io

Use with caution. You are responsible for your actions
Developers assume no liability and are not responsible for any misuse or damage.
By using subfinder, you also agree to the terms of the APIs used.

[INF] Loading provider config file /Users/0xacb/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for up.pt
www.overleaf.fe.up.pt
www.lome.inegi.up.pt
cmup.fc.up.pt
foton.fe.up.pt
www.tic.up.pt
mx02.up.pt
www.rec-mat.up.pt
khero.dcc.fc.up.pt
www.mil.up.pt
[INF] Found 3336 subdomains for up.pt in 20 seconds 244 milliseconds
```

Search engines

- We can find a lot of information on search engines: platforms, collaborators, login pages, intranet portals, etc.

- Discussion forums, github/gitlab repositories, stack overflow, etc can disclose PII and concerns of IT personnel and other employees, device vendors, software and technologies used by the target, firewalls, etc.

- Search engines store and **cache** information. This means that if the information is deleted or changed, a cached version may still be available. Check wayback machine as well.

- Exposed URLs may reveal important information about the target organization.

- Internal URLs and private files may disclose relevant information, since those are usually for collaborators, employees or partners.

- Public published vulnerability reports are always important to understand what vulnerabilities have been found so far, and to identify technologies.

Search engines

- PII is also important: phone numbers, birth dates, credit card data, passwords/hashes. May lead to easy ATO (account takeover), impersonation, theft.

- There are specific websites for retrieving information about someone: (pipl, anywho). However, there are OSINT specific tools like SocialPwned, sherlock and others.

- Manual research should be done for better results, social networks (twitter, facebook, instagram, LinkedIn), username search, mobile phone search (e.g. sync.me, adding a contact on WhatsApp to retrieve photo, etc), credential dump research (haveibeenpwned).

- If we are a company, public information on recruitment/jobs websites or career pages may disclose information about internal procedures, technologies, frameworks or even upcoming features

```
→  sherlock git:(master) python3 sherlock johndoe1337
[*] Checking username johndoe1337 on:

[+] 9GAG: https://www.9gag.com/u/johndoe1337
[+] Academia.edu: https://independent.academia.edu/johndoe1337
[+] Apple Discussions: https://discussions.apple.com/profile/johndoe1337
[+] Archive.org: https://archive.org/details/@johndoe1337
[+] AskFM: https://ask.fm/johndoe1337
[+] BitBucket: https://bitbucket.org/johndoe1337/
[+] BodyBuilding: https://bodyspace.bodybuilding.com/johndoe1337
[+] Chess: https://www.chess.com/member/johndoe1337
[+] Clubhouse: https://www.clubhouse.com/@johndoe1337
[+] Codecademy: https://www.codecademy.com/profiles/johndoe1337
[+] Cults3D: https://cults3d.com/en/users/johndoe1337/creations
[+] DeviantART: https://johndoe1337.deviantart.com
[+] Disqus: https://disqus.com/johndoe1337
[+] Dribbble: https://dribbble.com/johndoe1337
[+] Fameswap: https://fameswap.com/user/johndoe1337
[+] Fiverr: https://www.fiverr.com/johndoe1337
[+] Flipboard: https://flipboard.com/@johndoe1337
[+] Freesound: https://freesound.org/people/johndoe1337/
[+] G2G: https://www.g2g.com/johndoe1337
[+] Genius (Users): https://genius.com/johndoe1337
[+] GitHub: https://www.github.com/johndoe1337
```

URL scanning

- A website, frontend source code, cookies, HTTP headers, may reveal:
  - OS, technologies and versions
  - Directory structure, filenames
  - Code editor information
  - Information about sysadmins, emails, internal IP addresses and hostnames, and much more

URL scanning

- Multiple tools are available to scan URLs, we'll explore some in the next assignment. Some even crawl websites to find more endpoints (Linkfinder, relative-url-extractor, Burp Suite).

- Worst case scenario, we can replicate a website for offline analysis (client-side only).

- Other tools and plugins allow us to research caching mechanisms (wayback machine) and find more URLs.

- Content discovery tools ⚠️: gobuster, dirsearch, ffuf, and more

- `/robots.txt`, `/sitemap.xml`

URL scanning

```
fisher@fishers-MacBook-Pro-2 wordlist % ffuf -c -w raft-large.txt -u https://paypal.com/FUZZ -fc 301

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.5.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : https://paypal.com/FUZZ
 :: Wordlist         : FUZZ: raft-large.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
 :: Filter           : Response status: 301
```

Email analysis

- Email is a very important vector to conduct social engineering, launching attacks and (spear-)phishing campaigns.

- Understanding the profile of a email user (application, OS, etc) is very important for this process.

- Email headers contain important data, such as timestamps, applications, versions, IP addresses, email providers, DKIM signatures, etc.

Email analysis

```
Delivered-To: miguel@regala.im
Received: by 2002:a17:505:4acf:b0:1be8:e389:5ae0 with SMTP id ay15csp447131njc;
        Wed, 25 Sep 2024 09:44:26 -0700 (PDT)
X-Forwarded-Encrypted: i=2; AJvYcCVDiRslnAG/9KrUSma4lYnfBuBVFoDWrsaGkYjm0has4OKuCa31pBQcdMIH2sSMEke3280utis=@regala.im
X-Google-Smtp-Source: AGHT+IEDqzITWMHyDS+WTbpqF636Ja3+u2xnT2kg9xc8oMnQj8K5a40xgKmeeS67NLzsay13aJVE
X-Received: by 2002:a05:6870:8090:b0:268:880c:9de3 with SMTP id 586e51a60fabf-286e13874b0mr2865840fac.14.1727282666714;
        Wed, 25 Sep 2024 09:44:26 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1727282666; cv=none;
        d=google.com; s=arc-20240605;
        b=HeWDQD4J1TLLnAmUWDownEN3J1NoVZKyAtTcGkUz+iDm6CrScLjNOYkZSiqTnaNORa
         x3NAvXG93lL7ZrA/XC8mgOAC9gtgk4Bupv0AVTiZddHJ3+nfB6wbQTVRdqE9kGoNHDEy
         cGZWG69ZXU1esV6/F57l05xbqBeE30rieqFg2Q7LBksZqYpKeqk3quHYzPGSR3qmkNJk
         NSVpp9A2YuPbOwtN4X8t4AwWcMSOXlyxuNtJAnVWQTQInYvFKAiVwiQILWmozOcwPiDP
         WrOXQGAHwkyGlbSqkkbxVl2yhgL2IpNWWaJd853odJOlinlvVbU+Wn18PDKvaYiVFN9q
         neRA==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20240605;
        h=feedback-id:message-id:to:reply-to:subject:mime-version:from:date
         :content-transfer-encoding:dkim-signature:dkim-signature;
        bh=85AHTwqZrafObTmEcAwMA4du/MMf+rJ25vJcVChWdhE=;
        fh=KCSJVVitPXnIgH0ngAY3HsW2dBBi6YKpK2fySjMTBnw=;
        b=GyQHUhH64U+ESKRAn32iXWkGQR5XKCHtbQvdFp+ch6WxuyBMFH5/TwDafnYbEy5JY8
         HjKoPxvOEyDLlS8dnx75SzZfxKP3a90C1LwG3Olrm4ph3ZLLONaoprMbG/GTdM93F/Si
         1PGXZv7mCbho0+ldEc4lWlnkFbNhxvOB2XlZI0X3EupOU2w8x6P8qgxyH+uLN5+SeoZH
         IukcYsqPn27sRBhQ2DvPUAyfDoegzFgiGxN8X77p0jCUZfK2g33NGn7j0mngc7poQEJI
         jNIhWg87Yr6bBHEvuYziZe0dpEQezSp0NylUKpbLtQKMEs9kNacOT1NRRMjV0sHtLCnj
         utcQ==;
        dara=google.com
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@wearehackerone.com header.s=sqifkb7463btg37d52maffmml773iddp header.b=P1ka3n82;
       dkim=pass header.i=@amazonses.com header.s=7v7vs6w47njt4pimodk5mmttbegzsi6n header.b=AQy3m8Ey;
       spf=pass (google.com: domain of 010101922a11d6ca-25d914f4-9734-4dd0-9682-cd9ed47708d4-000000@us-west-2.amazonses.com designates
54.240.27.214 as permitted sender) smtp.mailfrom=010101922a11d6ca-25d914f4-9734-4dd0-9682-cd9ed47708d4-000000@us-west-2.amazonses.com;
       dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=wearehackerone.com
Return-Path: <010101922a11d6ca-25d914f4-9734-4dd0-9682-cd9ed47708d4-000000@us-west-2.amazonses.com>
Received: from a27-214.smtp-out.us-west-2.amazonses.com (a27-214.smtp-out.us-west-2.amazonses.com. [54.240.27.214])
        by mx.google.com with ESMTPS id 46e09a7af769-713beb730d3si1761921a34.246.2024.09.25.09.44.26
        for <miguel@regala.im>
        (version=TLS1_3 cipher=TLS_AES_128_GCM_SHA256 bits=128/128);
        Wed, 25 Sep 2024 09:44:26 -0700 (PDT)
Received-SPF: pass (google.com: domain of 010101922a11d6ca-25d914f4-9734-4dd0-9682-cd9ed47708d4-000000@us-west-2.amazonses.com
designates 54.240.27.214 as permitted sender) client-ip=54.240.27.214;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@wearehackerone.com header.s=sqifkb7463btg37d52maffmml773iddp header.b=P1ka3n82;
       dkim=pass header.i=@amazonses.com header.s=7v7vs6w47njt4pimodk5mmttbegzsi6n header.b=AQy3m8Ey;
```

Email analysis

- Tools like MX Toolbox and https://www.ip-tracker.org/ can help understanding the collected information.

- Tools like whoreadme.com and other tracking services allow email tracking and understand what happens with email messages sent by us.

- Google and other email providers use proxies to retrieve external resources, to protect user's privacy (IP address). But most don't.

Google dorking

- Google has been restricting access to advanced search tools that allow information gathering.

- Sometimes, Google shows errors and warnings, and asks the user to solve a captcha.

- We can still use dorks to retrieve indexed information: *site, inurl, intitle, ext, intext, inanchor, cache*, *filetype.*

Google dorking

- A few dorks (Credits Miguel Santareno):
  - Example: `intitle:intranet inurl:intranet + intext: “human resources” site:example.com`
  - Example: `ext:txt | ext:sql | ext:log & intext:"admin" | intext:"root" | intext:"administrator" & intext:"password" | intext:"root" | intext:"admin" | intext:”administrator” site:example.com`

Networking: Whois

- WHOIS databases are maintained by Internet registrars.
- They keep information about the owner of a domain, DNS servers, multiple information about creation and expiration dates, network ranges: bgp.he.net
- This data can help mapping the attack surface
- We can query online services, e.g. whois.domaintools.com or just use specific tools, such as the command: **`whois example.com`**

Networking: Whois

```
Nome de dom?nio / Domain Name: up.pt
Data de registo / Creation Date (dd/mm/yyyy): 11/10/1991
Data de expira??o / Expiration Date (dd/mm/yyyy): 30/05/2021
Estado / Status: ACTIVE

Titular / Registrant
   Universidade do Porto
   Reitoria - Pra?a Gomes Teixeira, Porto, 4099-002 Porto, PT
   Email: contacto_dnsup@reit.up.pt;fmc@uporto.pt;jorge@uporto.pt;jasousa@uporto.pt

Entidade Gestora / Billing Contact
   Universidade do Porto
   Reitoria - Pra?a Gomes Teixeira, Porto, 4099-002 Porto, PT
   Email: contacto_dnsup@reit.up.pt;fmc@uporto.pt;jorge@uporto.pt;jasousa@uporto.pt


Nameserver Information
   Nameserver: up.pt    NS      ns4.up.pt.
   Nameserver: up.pt    NS      ns3.up.pt.
   Nameserver: up.pt    NS      ns1.up.pt.
   Nameserver: up.pt    NS      ns2.up.pt.
   Nameserver: ns4.up.pt.       A       193.137.55.33
   Nameserver: ns3.up.pt.       AAAA    2001:690:2200:a10::32
   Nameserver: ns1.up.pt.       A       193.137.55.30
   Nameserver: ns3.up.pt.       A       193.137.55.32
   Nameserver: ns2.up.pt.       A       193.137.55.31
   Nameserver: ns4.up.pt.       AAAA    2001:690:2200:a10::33
   Nameserver: ns1.up.pt.       AAAA    2001:690:2200:a10::30
   Nameserver: ns2.up.pt.       AAAA    2001:690:2200:a10::31

Information Updated: 2018-09-22 12:28:38
```

Networking: DNS

- DNS records contain very important information for mapping networks.

- Different types: A (IP address), AAAA (ipv6), MX (mail), NS (DNS), CNAME (alternative name), SOA (authority), TXT (text), HINFO (Information about the host - machine, OS), PTR.

- They allow us to identify email services easily, IP addresses, cloud providers, third-party services and more.

Networking: Addresses

- By inspecting multiple IP address, we can sometimes retrieve network ranges used by a given organization.
- It's a very important step while fingerprinting network architecture.
- It's possible to retrieve network ranges by identifying the subnet mask used my a given target: official records.
- Some whois related services also publish and store this information: ARIN.

ARIN

You searched for: **8.8.8.8**

Network	
Net Range	8.8.8.0 - 8.8.8.255
CIDR	8.8.8.0/24
Name	LVLT-GOGL-8-8-8
Handle	NET-8-8-8-0-1
Parent	LVLT-ORG-8-8 (NET-8-0-0-0-1)
Net Type	Reallocated
Origin AS	
Organization	Google LLC (GOGL)
Registration Date	2014-03-14
Last Updated	2014-03-14
Comments	
RESTful Link	https://whois.arin.net/rest/net/NET-8-8-8-0-1
See Also	Related organization's POC records.
See Also	Related delegations.

Networking: Traceroute

- The **`traceroute`** tool can help us understand the route our traffic follows to reach a given host in a network.

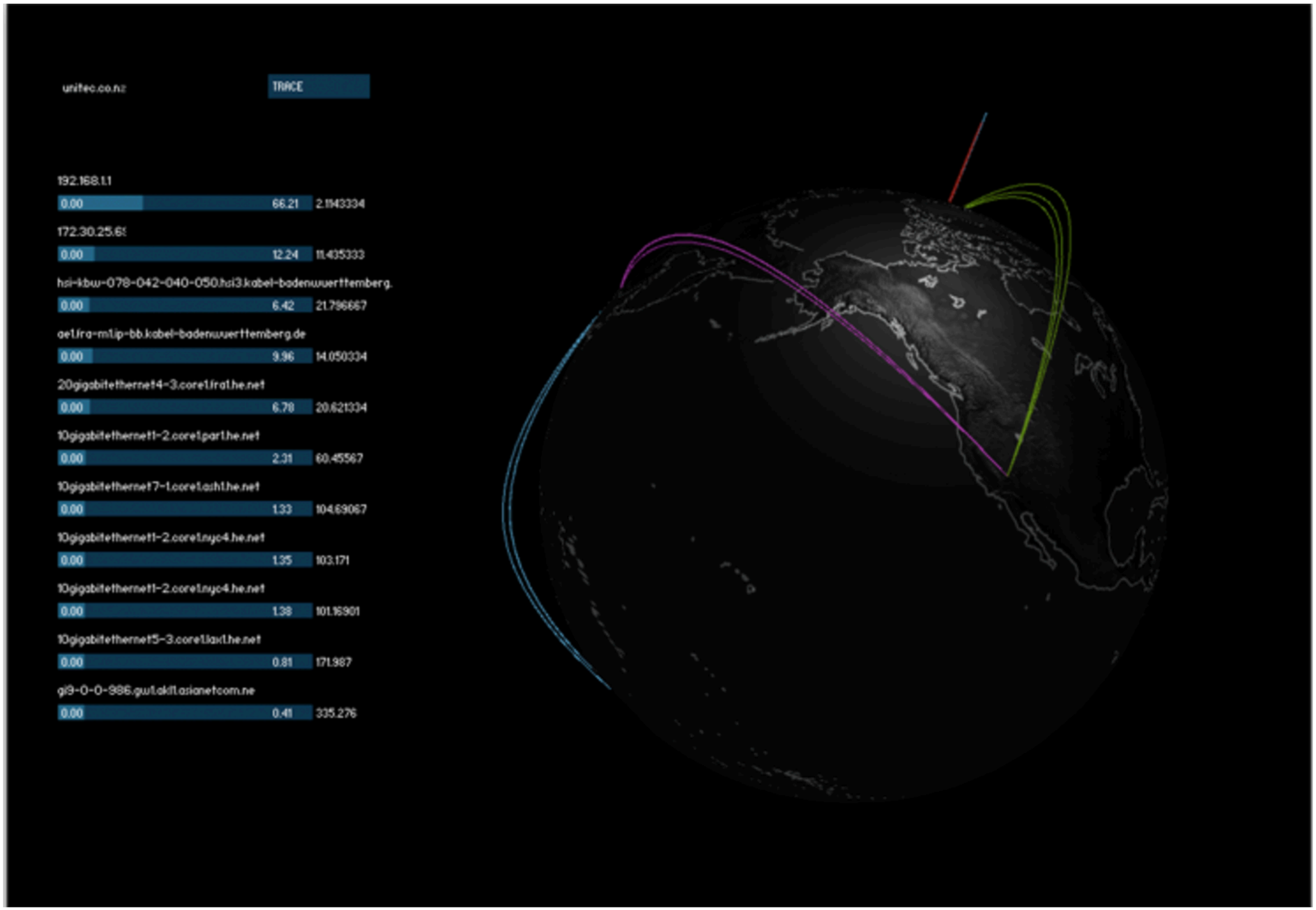
- How it works: The TTL (time to live) field of IP packets to explore the path until reaching the destination:

  - TTL = 0 -> The packet is sent back to the sender after 1 hop, with identification from “who” returned it

  - TTL = 2 -> The packet is sent back to the sender after 2 hops, with identification from “who” returned it, …

- visual-traceroute

Rede: Traceroute



Services and OS

- After finding the target IP addresses, the next step is about identifying operating systems and exposed services on those machines.

- `nmap`, `masscan` ⚠️

- https://www.shodan.io, smap ✅

- We'll get back to this later: identifying versions and operating systems are an essential step for identifying known vulnerabilities.

Social Engineering

- Social engineering is the art of persuading a human to reveal confidential information.
- The target should not understand that he/she is compromising the security of their systems or organisations.
- Some techniques:
  - Eavesdropping, shoulder surfing
  - Dumpster diving
  - **Pretending to be other person on a phone call, email message or social network interaction**
- Usually compromised: PII, ID numbers, birth dates, passwords/hashes, information about systems, network information, credit card or banking credentials and much more.

Social Networks

- A good vector for social engineering.
- An attacker can easily obtain information to pretend to be a friend of the victim.
- Sometimes, basic information can be used to perform actions on behalf of victims on other systems, such as **birth date, driver license, national ID**.
- Messages on social networks can be sent from accounts that can look legitimate, but now we have message requests, which is good for common users.
- By sending links, someone can be targeted and multiple information can be disclosed, including credentials.
- On LinkedIn, collaborators share information about products, jobs, etc. What if those job offerings are fake and an attack is deployed? A nice rule to follow: we shouldn't trust information that shows up on our inboxes.

Some more tools

- The tools and website services presented are just a subset of many options available.

- There are paid tools to retrieve privileged information about people and targets.

- Explore: social-engineer-toolkit

- Another example: maltego is a tools that allows an high-level approach to understand the fingerprint of an entity on the Internet.

Countermeasures

- How can we, as an organisation, protect us from these attacks?

Countermeasures

- Properly configuring network devices, such as routers, to restrict query responses
- Using firewalls, ID(P)S software and hardware, configure web servers correctly
- Control exposed information
- Educate the collaborators and employees
- Avoid exposing links for internal use
- Don’t use the same DNS for public servers and internal servers, network segmentation
- The best way is to actually try to perform recon on our own organization, as an attacker would do! Offensive security.
- Perform pentests, create internal security teams, incident response teams, implement policies, bug bounty programs and responsible disclosure…