

The background features abstract, overlapping green geometric shapes, primarily triangles and polygons, in various shades of green, creating a modern, layered effect. The shapes are positioned on the left and right sides of the slide, framing the central text.

OSINT

Beware. Your data is out there

OSINT - Open-source intelligence

Digital Footprint

- ▶ Open-source intelligence (OSINT) is the collection and analysis of data gathered from open sources (overt and publicly available sources) to produce actionable intelligence. ([Wikipedia](#))
- ▶ It's about digital footprint. Gathering information from:
 - ▶ search engines (Google, ...)
 - ▶ social media (Facebook, ...)
 - ▶ government sites
- ▶ The constant battles:
 - ▶ Privacy vs Publicly available information
 - ▶ Convenience vs Security

Disclaimer & Laws



Disclaimer

Boring but necessary

- ▶ Information in this presentation is intended for **educational purposes only**.
- ▶ **Live presentation.** Not a controlled environment and some contents may be inappropriate for some users.
- ▶ **I accept no responsibility** in any kind for the use, misuse, downloading, viewing in whatever way the links in this presentation.
- ▶ This presentation is not related to my work or company.



Disclaimer

Avoid illegal activities

- ▶ Some links, websites, software or other items listed may or **may not be legal**, illegal, a felony, misdemeanor, or worse, in your country.
- ▶ Please make sure that you are **allowed** to browse the websites, download links and software **BEFORE USING!**
- ▶ Ignorance about laws or procedures is **no excuse** for illegal activities or wrongdoing.
- ▶ Illegal activities may get you in **trouble or arrested**.
- ▶ **Always check what is legal, and what laws apply.**



Laws

Portuguese Law and Organizations

- ▶ Diário República Eletrónico ([link](#))
- ▶ ANACOM ([link](#))
- ▶ CNCS – Centro Nacional de Cibersegurança
 - ▶ Incident Notification
 - ▶ CERT.PT ([link](#))
- ▶ Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T) ([link](#))
- ▶ Ministério Público ([link](#))

Search, and then search again



Who Am I

Let's OSINT me 😊

- ▶ Just got a name
 - ▶ Pedro António Oliveira Vieira
- ▶ Google ([link](#))
- ▶ Google “Improved Search” ([link](#))
- ▶ LinkedIn ([link](#))
 - ▶ Public profile was showing way too much
- ▶ Certified **Ethical** Hacker ([link](#))



Who are YOU

Search yourself

- ▶ Search your name on Google and analyze the results
 - ▶ As you saw the search can be improved
- ▶ Some results can/will include:
 - ▶ Friends
 - ▶ Work
 - ▶ School grades
 - ▶ BI - Identity Card Number (yes)
 - ▶ NIF – Tax Identification Number
- ▶ That is typically information to **verify your identity** over a phone call.

Search Engines

Internet is more than Google

- ▶ Different search engine → different rules/crawlers → different results
- ▶ Google ([link](#))
- ▶ Bing ([link](#))
- ▶ Yahoo ([link](#))
- ▶ Ask ([link](#))
- ▶ DuckDuckGo ([link](#))
- ▶ Baidu (China) ([link](#))
- ▶ Yandex (Russia) ([link](#))

Google Dorks

Commonly used searches

- ▶ Google Advanced Search ([link](#))
- ▶ Google Hacking Database ([link](#))
- ▶ gbhackers ([link](#))
- ▶ google-dork-list ([link](#))
- ▶ Google Guide ([link](#))
- ▶ Google Guide ([link](#))

Search operators

Improve the search

- ▶ **filetype:** search your results based on the file extension
- ▶ **cache:** This operator allows you to view cached version of the web page.
- ▶ **allinurl:** This operator restricts results to pages containing all the query terms specified in the URL.
- ▶ **inurl:** This operator restricts the results to pages containing the word specified in the URL
- ▶ **allintitle:** This operator restricts results to pages containing all the query terms specified in the title.
- ▶ **link:** This operator searches websites or pages that contain links to the specified website or page.
- ▶ **info:** This operator finds information for the specified web page.
- ▶ **location:** This operator finds information for a specific location.
- ▶ **42 Advanced Operators** ([link](#))

Search

Dork Examples

- ▶ Google Search ([link](#))
 - ▶ Don't open links just because they are available. It's like entering a house just because the door was open. Would you do that ?
- ▶ `recibo vencimento filetype:pdf`
 - ▶ `recibo` - keyword to look for
 - ▶ `vencimento` - keyword to look for
 - ▶ `filetype:pdf` - only pdf files
- ▶ Available information on receipts
 - ▶ Full name, address, nif, nib, marital status, children number, ...

Search Dork Examples

- ▶ Google Search ([link](#))
- ▶ “hacked by” site:pt
 - ▶ “hacked by” - keyword to look for
 - ▶ site:pt - only “portuguese” sites (registered portuguese domains)
- ▶ About 13.400 results
 - ▶ Sites / pages that were “tagged”/”signed”
 - ▶ Attack and contents changed to show off skills (mainly kids) – compared to street tagging

ONLINE SAFETY



Helping Tools Safety

- ▶ VirusTotal
 - ▶ Check received files ([link](#)) (**don't upload Personal or Company related information**)
- ▶ Netcraft
 - ▶ Sitereport ([link](#)) (check for suspicious sites)
- ▶ Credit Card (online shopping)
 - ▶ Virtual Card
 - ▶ Mbnet
 - ▶ Revolut
 - ▶ PayPal

Helping Tools

Privacy

- ▶ VPN
 - ▶ ProtonVPN, ...
- ▶ Temporary Email (Need to register?)
 - ▶ 10 minute email ([link](#))
 - ▶ 20 minute email ([link](#))
- ▶ Disposable Email
 - ▶ 60 minute email ([link](#))
- ▶ Internet Access (DarkWeb included)
 - ▶ Tor ([link](#)) (internet browser)
 - ▶ Tails ([link](#)) (OS that runs on usb or VM)

Helping Tools

Reverse Tracking

- ▶ Gmail Plus Address ([link](#))
- ▶ Example:
 - ▶ mypersonalemail@gmail.com
 - ▶ If you append a “plus” sign to your email username, Gmail will ignore anything written between the + and @ sign in the email address and still deliver the message to the same mailbox.
- ▶ any email address sent to
 - ▶ mypersonalemail+linkedin@gmail.com
 - ▶ mypersonalemail+continente@gmail.com
 - ▶ mypersonalemail+financas@gmail.com
- ▶ Will still reach the Gmail inbox of mypersonalemail@gmail.com inbox though, technically, they are three different email aliases.

Passwords / Credentials

Please don't share

- ▶ Kaspersky
 - ▶ Check your password ([link](#)) (**or maybe not**)
 - ▶ Check last name – “vieira” or “Vieira” or “Vieira123”
- ▶ Top 10 passwords
 - ▶ “qwerty”, “password”, ...
 - ▶ Country specific: BR example “password” → “senha”
- ▶ Daniel Miessler SecLists
 - ▶ Usernames ([link](#))
 - ▶ Passwords ([link](#))
 - ▶ Default Credentials ([link](#))

OSINT



OSINT

Personal Information

- ▶ Posted information can get publicly and world available
 - ▶ Even private profiles can have their data shared by others
- ▶ When information is posted
 - ▶ Shows where you are at that time (habits & routines)
- ▶ Information on the picture
 - ▶ Metadata
 - ▶ Geolocation
- ▶ What companies know about us ([link](#))
- ▶ Awareness
 - ▶ What do we teach our kids? Do we teach ?
 - ▶ They are exposed to everyone on the internet.

Awareness

True stories

- ▶ Someone posted a photo of healthy meal
 - ▶ Laptop in background: Zoomed in and read emails
 - ▶ Social Media uses OCR. They also read the emails
- ▶ I once posted picture on social media while on trip
 - ▶ My friends knew I was not home (**Not public profile. At least I think it is not**)
 - ▶ Friends on that location called me on the phone
- ▶ Buying book (Buyer's card information)
 - ▶ How I was able to get money just by having the right information
- ▶ Social Media accounts
 - ▶ If you don't have Facebook, I can create one in your name and call your friends

Deadly Social Media

The Final Hours of Pop Smoke

- ▶ Rapper Pop Smoke Murdered in Home Invasion ... By 4 Masked Gunmen ([link](#))
- ▶ Instagram Posts
 - ▶ Location Tag
- ▶ Geolocation
 - ▶ Reverse Image
- ▶ Google Maps
 - ▶ Local Recon
- ▶ Airbnb/Zillow (Rent/Real-estate)
 - ▶ House photos (Outside and Inside)
 - ▶ Layout
- ▶ YouTube Video: The Cyber Mentor ([link](#))

OSINT

Tools & more tools

- ▶ OSINT FRAMEWORK ([link](#))
 - ▶ Yups, only one link is enough



OSINT

Profiling

- ▶ What's my IP? ([link](#))
- ▶ Ip2Location ([link](#))
- ▶ Mylocation ([link](#))
- ▶ Twitter
 - ▶ Twitter Advanced Search ([link](#))
- ▶ Facebook
 - ▶ StalkFace ([link](#))
 - ▶ Sowdust Github ([link](#))
 - ▶ IntelligenceX Facebook Search ([link](#))

OSINT

Profiling

- ▶ Mobile (how long have you been using the same number)
 - ▶ Sync me ([link](#))
- ▶ Usernames (you reuse usernames)
 - ▶ NameChk ([link](#))
 - ▶ WhatsMyName ([link](#))
 - ▶ NameCheckup ([link](#))
- ▶ Tinder
 - ▶ Username reuse ([link](#))
- ▶ New tools are always being created

OSINT

Profiling - Professional

- ▶ LinkedIn ([link](#))
- ▶ Xing ([link](#))
- ▶ Company Information
 - ▶ Technologies described in job adds (leaking information)
- ▶ Professional information phishing
 - ▶ Fake job adds (Is this a thing?)
- ▶ Curriculum Vitae
 - ▶ Sending CV with too much information – what is too much 😊
 - ▶ Home address – Street View

OSINT PT



OSINT

Portugal - Public contracts

- ▶ Base ([link](#))
 - ▶ The example ([link](#))
- ▶ PDF of contract with PII strikethrough ([link](#))
 - ▶ Open with pdf reader and delete the strikethrough boxes
 - ▶ Name of employee who edited the document
 - ▶ Information on UA, LinkedIn, Facebook, ...
 - ▶ Metadata: “KONICA MINOLTA bizhub C454”
- ▶ Information leaked
 - ▶ Full Names, nif, addresses

OSINT

Portugal - Vehicle Information

- ▶ Automóvel On-line ([link](#))
- ▶ Certidão Permanente Automóvel ([link](#))
 - ▶ License Plate : “01-EF-34”
 - ▶ Result
 - ▶ Brand: MERCEDES-BENZ
 - ▶ VIN: WDD2040081A043326
 - ▶ Example ([link](#))
- ▶ Vehicle Information ([link](#))
 - ▶ Example ([link](#))
 - ▶ Information: Brand, Model, Location, Paint, Delivery Date, Extras, ...
- ▶ Hack across the globe by VIN ([link](#))

OSINT

Portugal - Insurance Information

- ▶ ASF – Autoridade de Supervisão de Seguros e Fundos de Pensões ([link](#))
 - ▶ Example ([link](#))
 - ▶ License Plate : “01-EF-34”
 - ▶ Date : “03-07-2022”
 - ▶ Example 2 ([link](#))
 - ▶ License Plate : “01-EF-34”
 - ▶ Date : “03-07-2012”
- ▶ Insurance Company
 - ▶ Current and Past
 - ▶ Length of the contract
 - ▶ Insurance policy number
 - ▶ Can I get information for all license plates ????

OSINT

Portugal Specific

- ▶ Registo Predial Online ([link](#))
- ▶ DGES - Direção-Geral de Ensino Superior ([link](#))
- ▶ DRE - Diário da República ([link](#))
 - ▶ Search DRE ([link](#))
- ▶ Finanças - Penhorados ([link](#))
 - ▶ Example ([link](#))
 - ▶ Search Penhorados – ([link](#))
- ▶ Ministério da Justiça - Penhorados ([link](#))
- ▶ Plataforma Eletrónica de Compras (Administração Pública) ([link](#))

- ▶ Leaked information:
 - ▶ Full Names, Addresses, NIF, Company, Marital Status, ...

OSINT GEO



OSINT - Photos

Lots of Information

- ▶ Where was this image taken?
 - ▶ Have you been there?
- ▶ When?
 - ▶ Date stamp on photo
 - ▶ Filename with date
 - ▶ Metadata
- ▶ What else?
- ▶ Image search
 - ▶ Identify the castle?




OSINT - Photos Metadata

- Metadata
- GPS ([link](#))

exifdata

SUMMARY
DETAILED
LOCATION
UPLOAD

IMG_20190223_163027.jpg



(click for original)

Camera
Xiaomi Redmi 3

GPS Position
40.989952 degrees N, 7.395051 degrees W

Date of Creation
2019:02:23 16:30:27

Resolution
4160x3120

SUMMARY

Make	Xiaomi
Model	Redmi 3
Aperture	2
Exposure Time	1 / 1506 (0.00066401062416999 sec)
Focal Length	4.2 mm
Flash	Auto, Did not fire
File Size	1447 kB
File Type	JPEG
MIME Type	image/jpeg
Image Width	4160
Image Height	3120
Encoding Process	Baseline DCT, Huffman coding
Bits Per Sample	8
Color Components	3
X Resolution	72
Y Resolution	72
YCbCr Sub Sampling	YCbCr4:2:0 (2 2)
YCbCr Positioning	Centered
Exposure Program	Not Defined
Date and Time (Original)	2019:02:23 16:30:27
Metering Mode	Center-weighted average
Color Space	sRGB
Exposure Index	140
Sensing Method	Unknown (0)
Exposure Mode	Auto
Focal Length In 35 mm Format	0 mm
Scene Capture Type	Standard
Gain Control	Low gain up
ISO	100
Compression	JPEG (old-style)

OSINT

(Reverse) Image search

- ▶ One image is worth 1000 words, maybe more.
 - ▶ What information can be extracted from a photo ?
- ▶ Google Images ([link](#))
- ▶ Bing Images ([link](#))
- ▶ Yahoo Images ([link](#))
- ▶ TinEye ([link](#))
- ▶ Yandex ([link](#))
- ▶ The professionals (video explaining) ([link](#))



OSINT

Street View

- ▶ Google Street View ([link](#))
 - ▶ Identify house by address
 - ▶ Assess security (cameras, fences, ...)
 - ▶ Parked cars (timeline, ...)
 - ▶ People's habits/routines, timetables, ...
- ▶ View the past – timeline ([link](#))
- ▶ Instant Street View ([link](#))



OSINT Maps

- ▶ Google Maps ([link](#))
- ▶ Bing Maps ([link](#))
- ▶ Wikimapia ([link](#))

- ▶ Tips, Tricks and Techniques ([link](#))



Search

Satellite View

- ▶ Zoom Earth ([link](#))
- ▶ Satellites Pro ([link](#))
- ▶ World Imagery ([link](#))
 - ▶ Wayback ([link](#))
 - ▶ Wayback example ([link](#))
- ▶ View the past - timeline



Search Geolocation

- ▶ Digital Cameras/Mobile Phones
 - ▶ Metadata
 - ▶ Geolocation
 - ▶ Camera Model
 - ▶ ...
- ▶ Breasts lead to arrest of Anonymous hacker ([link](#))
 - ▶ Police allege that an Anonymous hacker posted a picture of his presumed girlfriend's breasts as a taunt to U.S authorities. The picture allegedly contained GPS information that led the FBI to her.

OSINT MEMORY



Wayback Machine

Internet in the past

- ▶ Wayback Machine ([link](#))
- ▶ Archive.is ([link](#))
- ▶ Cached Pages ([link](#))
- ▶ Cached View ([link](#))
- ▶ OldWeb.Today ([link](#))
- ▶ Time Travel ([link](#))

OSINT IOT



Shodan

Internet of Things

- ▶ Search Engine for Internet Of Things
- ▶ Explore
 - ▶ Shodan explore ([link](#))
- ▶ Images
 - ▶ Shodan images ([link](#))
- ▶ Maps
 - ▶ Shodan maps ([link](#))
- ▶ Internet Exposure Observatory
 - ▶ Exposure Dashboard ([link](#))



Shodan

Internet of Things

- ▶ Remote Desktop ([link](#))
 - ▶ Total results: 3,482,756
 - ▶ Braga ([link](#))
- ▶ Images
 - ▶ Braga ([link](#))
 - ▶ VNC Remote Access and Loggedin ([link](#))
- ▶ Authentication Disabled
 - ▶ Portugal ([link](#))
 - ▶ Primavera ([link](#))
- ▶ Contabilidade ([link](#))

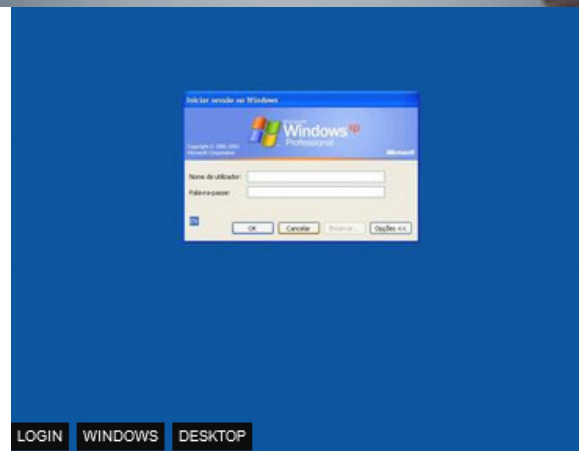
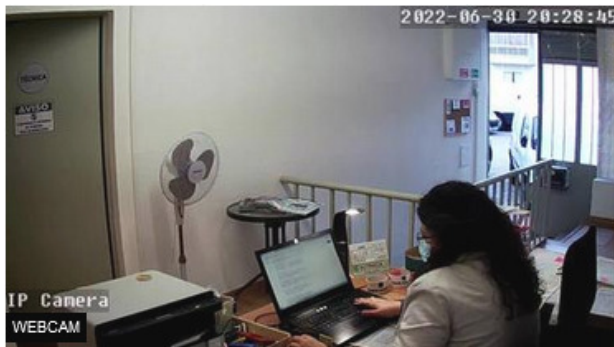
Shodan

Internet of Things

- ▶ Fotos
 - ▶ Portugal ([link](#))
- ▶ IP Cameras
 - ▶ Portugal ([link](#)) (default credentials?)
 - ▶ **Webcams** ([link](#))

Shodan

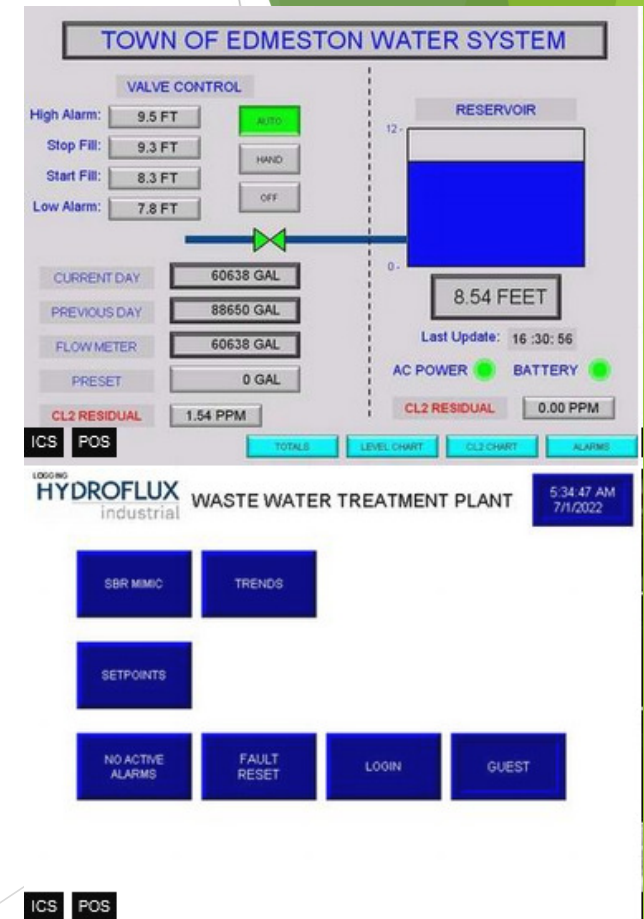
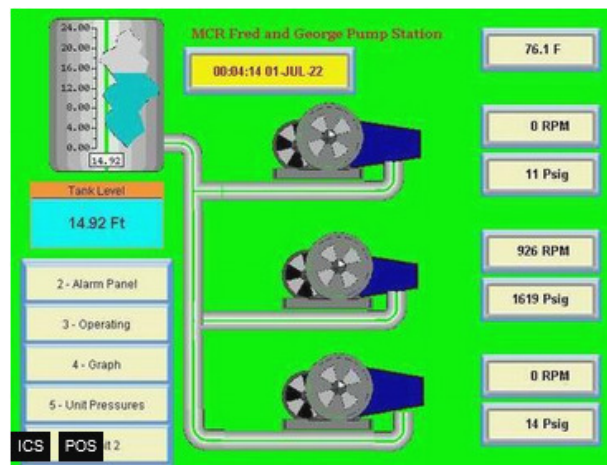
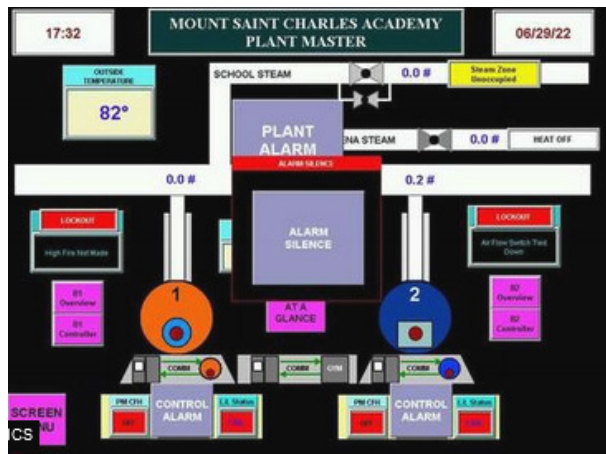
Internet of Things - Images



Shodan

Industrial Control Systems

- Industrial Control Systems ([link](#))



Shodan

Portugal - Internet Exposure

- ▶ Internet Exposure Dashboard ([link](#))
- ▶ Top Vulnerability
 - ▶ CVE-2015-0204 – CVSS2 4.3 Medium ([link](#))
- ▶ BlueKeep Unpatched ([link](#))
 - ▶ 107 ([link](#))
- ▶ Industrial Control Systems
 - ▶ 516
- ▶ SMB (shared folders)
 - ▶ Authentication Disabled: 2898

Insecure Insecure Cameras

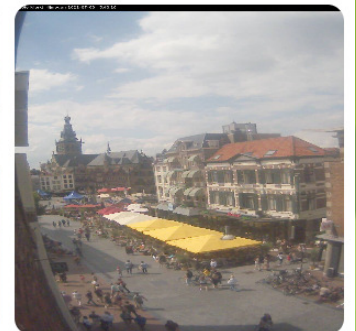
- Browser edit ([link](#))
 - Portugal ([link](#))



Live camera in Lisbon, Portugal



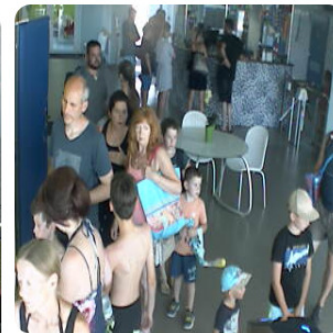
Live camera in Lisbon, Portugal



Live camera in Amsterdam, Netherlands



[Live camera in Kiefersfelden, Germany](#)



[Live camera in PRAGUE, Czech Republic](#)

Databreach



Databreach

Is not a thing of the past

- ▶ Troy Hunt
 - ▶ HaveIBeenPwned ([link](#))
 - ▶ Pwned websites ([link](#))
- ▶ Ashley Madison Breach 2015 ([link](#))
 - ▶ When private data gets public
- ▶ Piracy - Subtitles
 - ▶ Don't think you can hide – **Illegal activities are tracked**
- ▶ Companies are leaking all your information
 - ▶ Compromised data: Dates of birth, Email addresses, Employers, Family structure, Genders, Income levels, Living costs, Marital statuses, Mothers maiden names, Names, Phone numbers, Physical addresses, Places of birth, Religions, Spouses names

Databreach

Company credentials ?

- ▶ Source
 - ▶ Publicly available list of credentials
 - ▶ More than 10k credentials just for Bosch
- ▶ Information gathered
 - ▶ Rule of email/login
 - ▶ (FirstName.LastName)@(Country).(company).com
 - ▶ Rule of password complexity
 - ▶ List of users
 - ▶ Phishing campaigns
 - ▶ Brute force
 - ▶ Look for those users on Social Media
- ▶ Added Problem
 - ▶ Credentials reuse

Email/Login	Password
data/m/i/c:michele@de.bosch.com	\$HEX[576569c3
data/m/i/c:michele@de.bosch.com	er@de.bosch.com:weißer
data/m/i/c:michele@de.bosch.com	zkus@de.bosch.com:shannon
data/m/i/c:michele@de.bosch.com	tke@bosch.com:lumpi007
data/m/i/c:michele@de.bosch.com	der@de.bosch.com:a6fc6b19
data/m/i/c:michele@de.bosch.com	z4@de.bosch.com:jaguar
data/m/i/c:michele@de.bosch.com	@us.bosch.com:ultra06
data/m/i/c:michele@de.bosch.com	@cz.bosch.com:micsis
data/m/i/c:michele@de.bosch.com	ll@uk.bosch.com:frances
data/m/i/c:michele@de.bosch.com	@bosch.com:petros69
data/m/i/c:michele@de.bosch.com	us.bosch.com:mike5920
data/m/i/c:michele@de.bosch.com	n@us.bosch.com:radar123
data/m/i/c:michele@de.bosch.com	om@us.bosch.com:2af415a2174b1
data/m/i/c:michele@de.bosch.com	om@us.bosch.com:hardrock
data/m/i/c:michele@de.bosch.com	rger@za.bosch.com:mikel23
data/m/i/c:michele@de.bosch.com	cn.bosch.com:Mikomido
data/m/i/c:michele@de.bosch.com	@us.bosch.com:bulldog3120
data/m/i/c:michele@de.bosch.com	@de.bosch.com:maccaroni
data/m/i/c:michele@de.bosch.com	mann@de.bosch.com:\$HEX
data/m/i/c:michele@de.bosch.com	mann@de.bosch.com:asdfjklö
data/m/i/c:michele@de.bosch.com	mann@de.bosch.com:asdfjklR
data/m/i/c:michele@de.bosch.com	comcast.net:mojopapa
data/m/i/c:michele@de.bosch.com	comcast.net:mojopapal
data/m/i/c:michele@de.bosch.com	s.bosch.com:bogey
data/m/i/c:michele@de.bosch.com	cz.bosch.com:koqugeti
data/m/i/c:michele@de.bosch.com	cz.bosch.com:wunazaqu
data/m/i/c:michele@de.bosch.com	zak@pl.bosch.com:igi74mick77
data/m/i/c:michele@de.bosch.com	z.bosch.com:hyqokibu
data/m/i/c:michele@de.bosch.com	@fr.bosch.com:CHOISNE
data/m/i/c:michele@de.bosch.com	@be.bosch.com:elsclaes
data/m/i/c:michele@de.bosch.com	de.bosch.com:janlasse79
data/m/i/c:michele@de.bosch.com	nl.bosch.com:Killer1
data/m/i/c:michele@de.bosch.com	ey@us.bosch.com:leander65
data/m/i/c:michele@de.bosch.com	r.bosch.com:ro67vsh5
data/m/i/c:michele@de.bosch.com	nte@it.bosch.com:michele
data/m/i/c:michele@de.bosch.com	lli@us.bosch.com:radica4
data/m/i/c:michele@de.bosch.com	de@br.bosch.com:mls2g3a4
data/m/i/c:michele@de.bosch.com	hi@br.bosch.com:Talita
data/m/i/c:michele@de.bosch.com	@br.bosch.com:Orquideas1

Databreach

Portuguese domain examples (2018)

- ▶ uminho.pt - Universidade do Minho
- ▶ adv.oa.pt - Ordem dos Advogados
- ▶ pj.pt - Policia Judiciária
- ▶ mail.exercito.pt - Exército
- ▶ cm-braga.pt - Câmara Municipal de Braga
- ▶ cm-guimaraes.pt - Câmara Municipal de Guimarães
- ▶ psd.pt - Partido Social Democrata
- ▶ ps.pt - Partido Socialista
- ▶ fcporto.pt - Futebol Clube do Porto
- ▶ min.justiça - Ministério da Justiça

- ▶ Were these the sources for criminal “hacker” Rui Pinto ?

Wifi



Wifi

World Map - WiFi Networks

- ▶ Wigle – shell5
- ▶ <https://wile.net/map?maplat=41.53443897842117&maplon=-8.437174307569958&mapzoom=21&coloring=density>
- ▶ mac address lookup
- ▶ <https://dnschecker.org/mac-lookup.php?query=68-cc-6e-c0-c7-e1>



Hacker Mentality



Penetration Test

Portugal - Ministério da Justiça

- ▶ How safe is our information?
- ▶ Site URL: `https://www.automovelonline.mj.pt/AutoOnlineProd/`
 - ▶ Is there a **DEV** site?
 - ▶ Error shows software and version (Apache Tomcat/8.0.41)
 - ▶ Are there exploits? Exploit Database ([link](#))
- ▶ Automatic testing website ([link](#))
- ▶ Are these tests legal?
 - ▶ If you don't own the site, it's usually not legal or allowed.

Capture The Flag



CTF

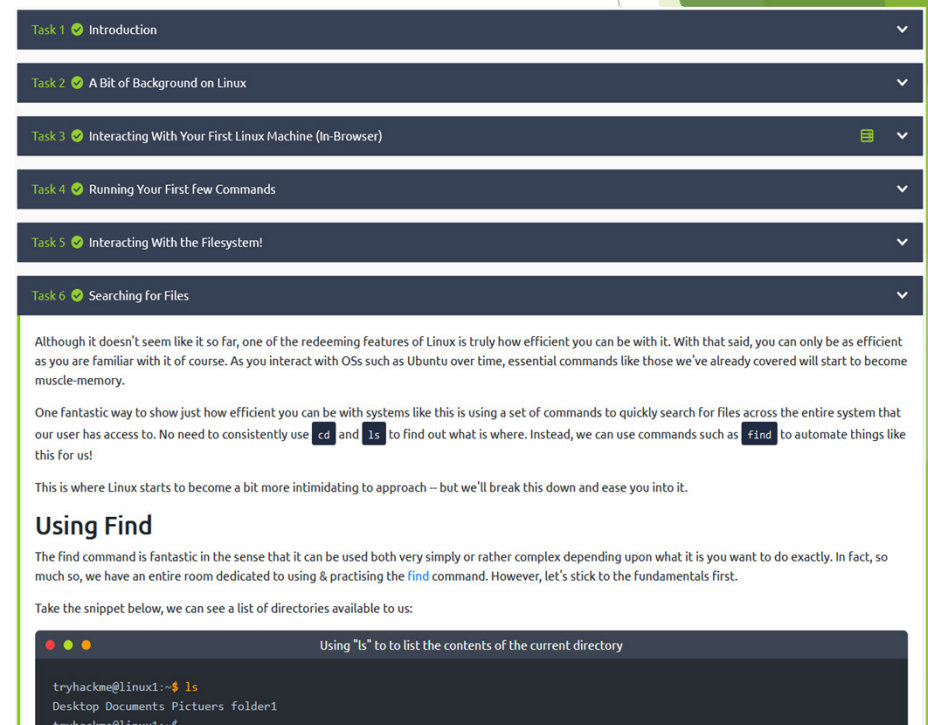
Capture The Flag

- ▶ TryHackMe - <https://tryhackme.com/>
- ▶ HackTheBox - <https://www.hackthebox.eu/>
- ▶ VulnHub - <https://www.vulnhub.com/>
- ▶ OTW - <https://overthewire.org/wargames/>
- ▶ PicoCTF - <https://picoctf.org/>
- ▶ CryptoPals - <https://cryptopals.com/>
- ▶ CryptoHack - <https://cryptohack.org/>

CTF

THM - Try Hack Me

- ▶ Try Hack Me ([link](#))
 - ▶ TryHackMe is a free online platform for learning cyber security, using hands-on exercises and labs, all through your browser!
- ▶ Learn
 - ▶ Our content is guided with interactive exercises based on real world scenarios, from hacking machines to investigating attacks, we've got you covered.
- ▶ Practice
 - ▶ Put your knowledge into practice with gamified cyber security challenges.
- ▶ Cost - Free or \$10/month



The screenshot displays the TryHackMe web interface. At the top, there is a list of tasks: Task 1 Introduction, Task 2 A Bit of Background on Linux, Task 3 Interacting With Your First Linux Machine (In-Browser), Task 4 Running Your First Few Commands, Task 5 Interacting With the Filesystem!, and Task 6 Searching for Files. Task 6 is selected and expanded, showing its content. The text explains the efficiency of Linux and introduces the 'find' command. It includes a terminal snippet demonstrating the 'ls' command to list directory contents.

Task 1 Introduction

Task 2 A Bit of Background on Linux

Task 3 Interacting With Your First Linux Machine (In-Browser)

Task 4 Running Your First Few Commands

Task 5 Interacting With the Filesystem!

Task 6 Searching for Files

Although it doesn't seem like it so far, one of the redeeming features of Linux is truly how efficient you can be with it. With that said, you can only be as efficient as you are familiar with it of course. As you interact with OSs such as Ubuntu over time, essential commands like those we've already covered will start to become muscle-memory.

One fantastic way to show just how efficient you can be with systems like this is using a set of commands to quickly search for files across the entire system that our user has access to. No need to consistently use `cd` and `ls` to find out what is where. Instead, we can use commands such as `find` to automate things like this for us!

This is where Linux starts to become a bit more intimidating to approach – but we'll break this down and ease you into it.

Using Find

The find command is fantastic in the sense that it can be used both very simply or rather complex depending upon what it is you want to do exactly. In fact, so much so, we have an entire room dedicated to using & practising the `find` command. However, let's stick to the fundamentals first.

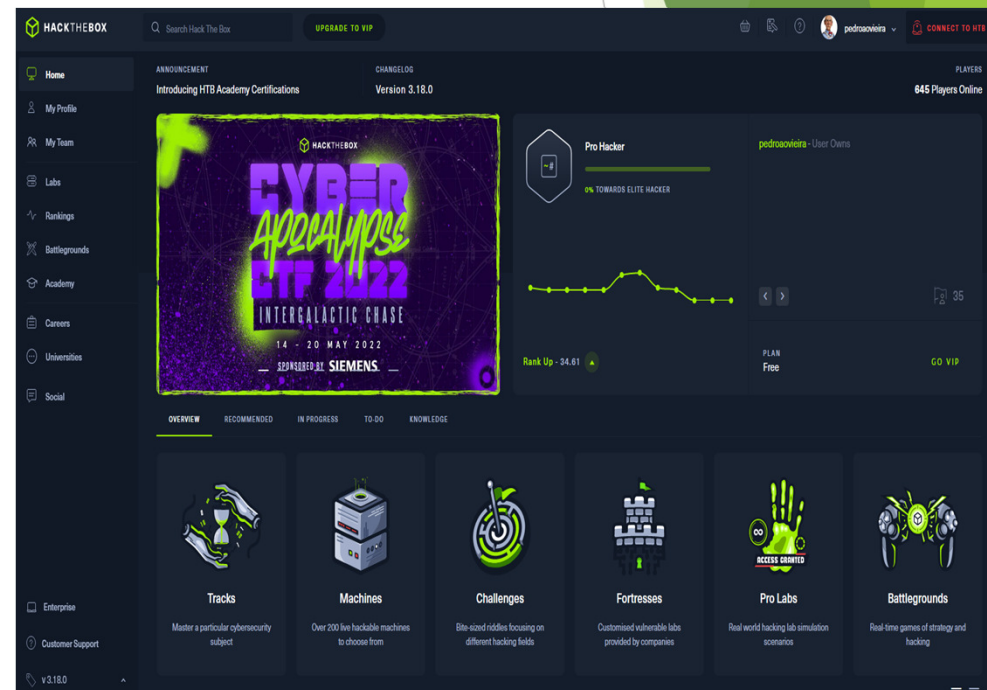
Take the snippet below, we can see a list of directories available to us:

```
tryhackme@linux1:~$ ls
Desktop Documents Pictures folder1
tryhackme@linux1:~$
```

CTF

HTB -Hack The Box

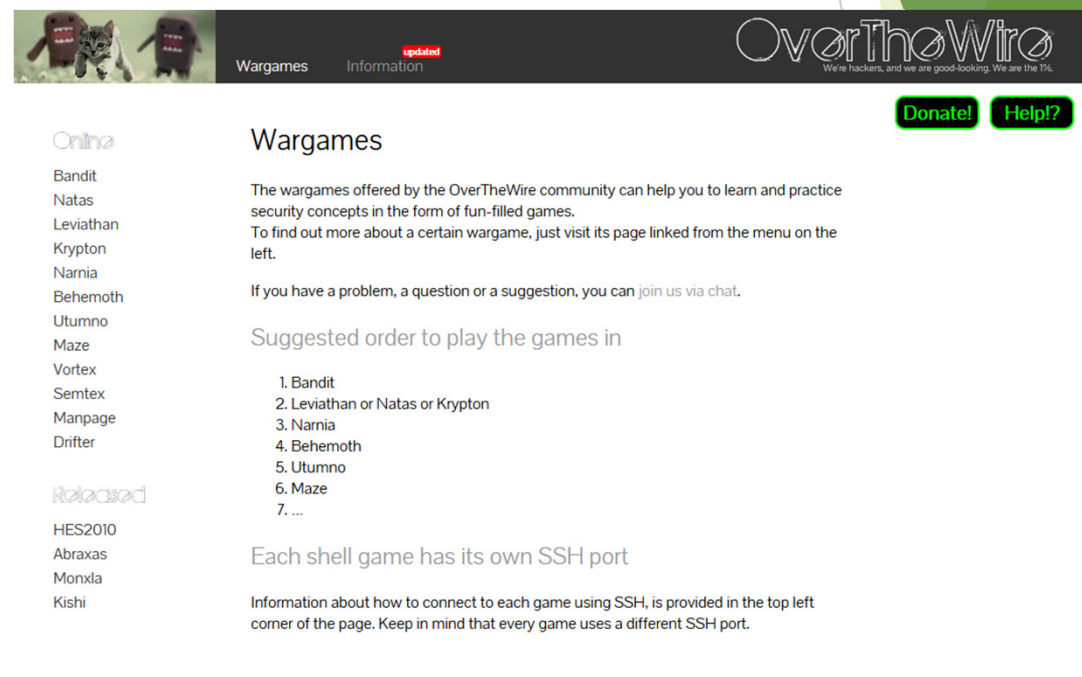
- ▶ Hack The Box ([link](#))
 - ▶ Hack The Box is a massive, online cybersecurity training platform, allowing individuals, companies, universities and all kinds of organizations around the world to level up their hacking skills.
- ▶ Challenges
 - ▶ Hardware, Crypto, Pwn, Mobile, Reversing, Web, ...
- ▶ Machines / Tracks
- ▶ Cost - Free / €12/month
- ▶ Job Board



CTF

OTW -Over The Wire

- ▶ Over The Wire ([link](#))
- ▶ Linux and Web based games
 - ▶ Linux - Bandit
 - ▶ Web - Natas



The screenshot shows the OverTheWire website. The header features a navigation bar with 'Wargames' and 'Information' (marked as 'updated'). The 'OverTheWire' logo is on the right, with the tagline 'We're hackers, and we are good-looking. We are the OW.' Below the header, there are 'Donate!' and 'Help!?' buttons. The main content area is titled 'Wargames' and includes a description of the wargames offered, a link to a chat, and a suggested order to play the games. A sidebar on the left lists 'Online' and 'Released' games. The 'Online' games listed are Bandit, Natas, Leviathan, Krypton, Narnia, Behemoth, Utumno, Maze, Vortex, Semtex, Manpage, and Drifter. The 'Released' games listed are HES2010, Abraxas, Monxdia, and Kishi. The 'Wargames' section text states: 'The wargames offered by the OverTheWire community can help you to learn and practice security concepts in the form of fun-filled games. To find out more about a certain wargame, just visit its page linked from the menu on the left. If you have a problem, a question or a suggestion, you can join us via chat.' The 'Suggested order to play the games in' list is: 1. Bandit, 2. Leviathan or Natas or Krypton, 3. Narnia, 4. Behemoth, 5. Utumno, 6. Maze, 7. ... The 'Each shell game has its own SSH port' section states: 'Information about how to connect to each game using SSH, is provided in the top left corner of the page. Keep in mind that every game uses a different SSH port.'

Wargames Information ^{updated}

OverTheWire
We're hackers, and we are good-looking. We are the OW.

Donate! Help!?

Online

Bandit
Natas
Leviathan
Krypton
Narnia
Behemoth
Utumno
Maze
Vortex
Semtex
Manpage
Drifter

Released

HES2010
Abraxas
Monxdia
Kishi

Wargames

The wargames offered by the OverTheWire community can help you to learn and practice security concepts in the form of fun-filled games.
To find out more about a certain wargame, just visit its page linked from the menu on the left.

If you have a problem, a question or a suggestion, you can join us via chat.

Suggested order to play the games in

1. Bandit
2. Leviathan or Natas or Krypton
3. Narnia
4. Behemoth
5. Utumno
6. Maze
7. ...

Each shell game has its own SSH port

Information about how to connect to each game using SSH, is provided in the top left corner of the page. Keep in mind that every game uses a different SSH port.

License

- ▶ Feel free to use/modify/share
- ▶ teach

