Guy Fawkes Starting Pack

Roberto A. Foglietta
GNU/Linux Expert and Innovation Supporter

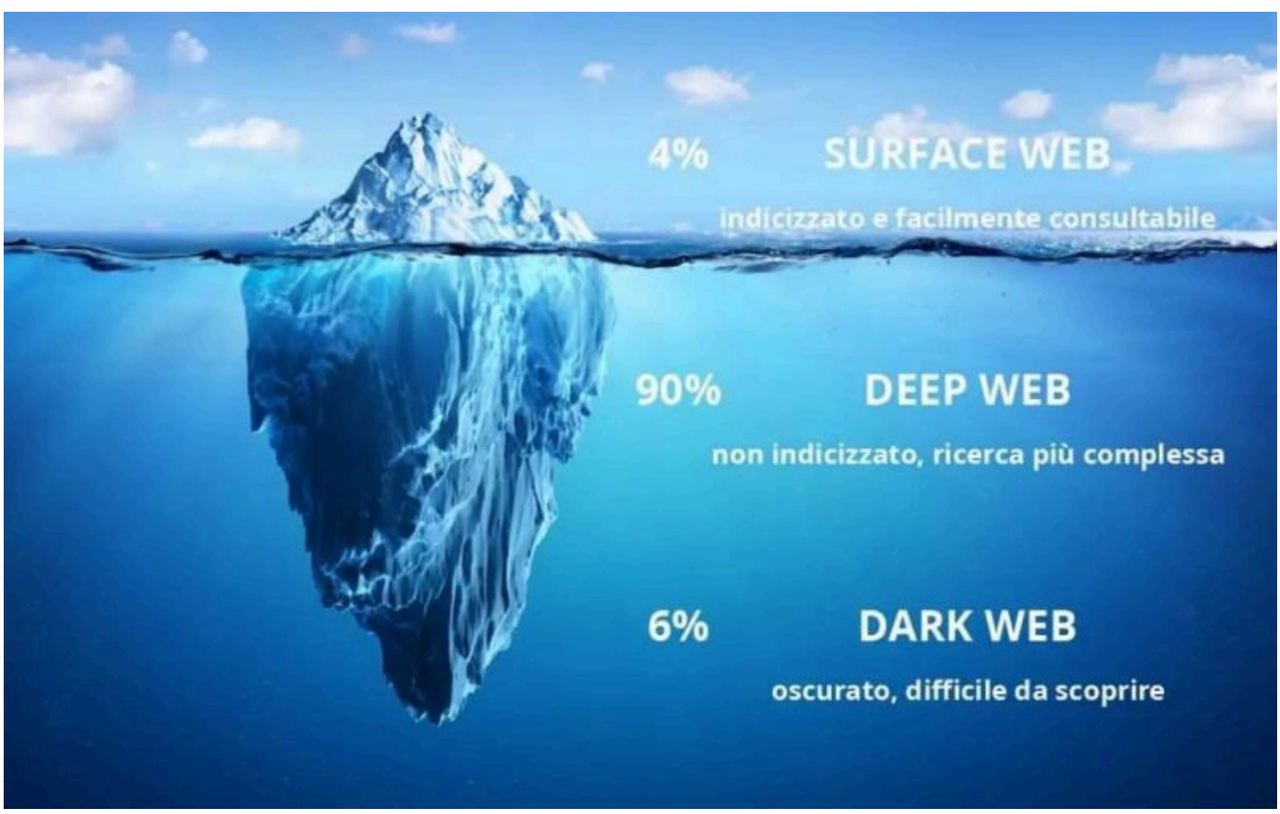
Published Jan 15, 2024

22nd draft, based on previous LinkedIn posts.

Published and updated since 15th Jan 2024.

Il darkweb per principianti

Il darkweb è una dimensione pericolosa per i principianti e il rischio di imbattersi in attività criminali o di essere loro vittima aumenta di molto rispetto al surface web e al deep web.



La differenza fra il surface web e il deep web è l'indicizzazione: tutto il materiale che in qualche modo si può reperire con una ricerca sui vari motori di ricerca. Nel deep web, manca l'indicizzazione e quindi se non si ha il link diretto non si può accedere ai contenuti.

Il dark web invece è tutt'altra cosa. Prima di tutto non è accessibile con un normale browser web connesso a Internet ma serve accedervi tramite, ad esempio le reti TOR che comunque da sole non forniscono il 100% della garanzia di essere anonimi o non tracciabili.

Sul dark web si possono trovare link il cui contenuto non è indicizzato e magari è protetto da una password per garantire che non venga indicizzato. Il link e la password possono essere entrambe pubbliche ovvero esposte sul dark web. Anche se il contenuto è accessibile dal deep web non significa che sia sicuro o che sia legale o che corrisponda alla descrizione.

Già questo dovrebbe farvi capire che non è una dimensione per principianti ma non si diventa senior o esperti stando seduti sul divano a guardare Netflix. Quindi se si vuole esplorare questa dimensione occorre prudenza, un po' di paranoia e ovviamente coraggio.

Ma anche strumenti e accorgimenti specifici per questa attività:

1. non usare MAI-E-POI-MAI il computer di casa o di lavoro per accedere la dark e neanche al deep web ad esso relativo.

2. Dal punto **#1** deriva la necessità di dotarsi di un laptop dedicato SOLO-ED-ESCLUSIVAMENTE per quelle attività.

3. Dai primi due punti deriva la conclusione che MAI-E-POI-MAI si devono trasferire contenuti dal computer di casa o lavoro a quello di esplorazione e viceversa.

4. Perciò tutte le unità dati esterne che si usano per l'esplorazione DEVONO-ASSOLUTAMENTE essere contrassegnate con un bel nastro adesivo ROSSO per evitare pericolosi errori.

5. Un laptop da esplorazione può essere comprato spendendo da €150 (T460) a €300 (X280) e i ThinkPad sono i più adatti perché garantiscono la massima compatibilità hardware con Linux scordatevi Windows e anzi radetelo subito al suolo meglio ancora se all'inizio togliete anche lo SSD.

6. La distribuzione più adatta all'esplorazione è TAIL Linux [1] da usare via USB (suggerita: Sandisk Ultra USB 3.0 130Mb/s) [2], inizialmente senza possibilità di salvare dati in modo permanente. Poi con la sua partizione dati e una volta raggiunta una certa seniority potete rimontare lo SSD.

7. Quando o se decidete di usare lo SSD interno, procuratevi una chiavetta USB di wiping [3] e testatela sulla SSD come prima cosa. Se avete la sensazione che qualcosa stia andando storto o scaricate del materiale che ASSOLUTAMENTE-NON volete conservare - reboot & erase - piallate tutto senza esitazione.

8. Trust your gut and never panic.

Links

- [1] **tails.net**

- [2] **www.amazon.it/gp/product/B00P8XQPY4**
- [3] **github.com/PartialVolume/shredos.x86_64**
- [4] **wikileaks.org**

PhotoRec, Digital Picture and File Recovery

PhotoRec is file data recovery software designed to recover lost files including video, documents and archives from hard disks (Mechanical Hard drives, Solid State Drives...), CD-ROMs, and lost pictures (thus the Photo Recovery name) from digital camera memory. PhotoRec ignores the file system and goes after the underlying data, so it will still work even if your media's file system has been severely damaged or reformatted.

- **https://www.cgsecurity.org/wiki/PhotoRec**

Signal App + /e/OS for TOR encrypted messages

Signal is an end-to-end encrypted instant messaging service for instant messaging, voice, and video calls. The application uses a centralized computing architecture and is cross-platform software. It is developed by the non-profit Signal Foundation and its subsidiary Signal Messenger LLC. Signal's software is free and open-source. It uses mobile telephone numbers as identifiers for users and includes mechanisms by which users can independently verify the identity of their contacts and the integrity of the data channel. --Wikipedia

Using TOR and faking the GPS position.

/e/OS is a fork of LineageOS, an Android-based mobile operating system, and associated online services. /e/ is presented as privacy software that does not contain proprietary Google apps or services, and challenges the public to "find any parts of the system or default applications that are still leaking data to Google." --Wikipedia

- -> **doc.e.foundation/support-topics/advanced_privacy**

Advanced Privacy is using an implementation of the Tor project. We extracted the core functionality from the Orbot application, and added a user interface on the top of it. When Hide My IP is activated, all the device’s internet traffic, or just the one of some selected app, is redirected through the Tor network. In the end, the user’s primary (and read) IP address is masked by a random IP address that belongs to the TOR network

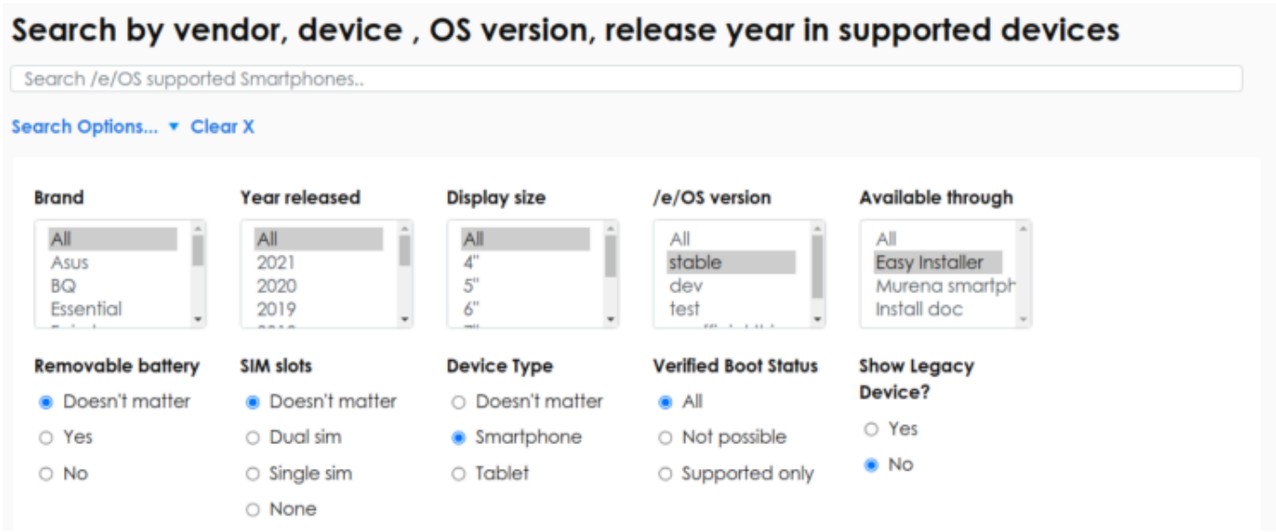
In Advanced Privacy, Fake my location takes advantage of existing low-level operating system features that we have connected to the Advanced Privacy User Interface to make it easy to use and hidden from applications. Fake my location bypasses the real location provided by the satellite radio navigation system or the network, and instead sends the one set by users to applications that are requiring location.

Smartphones /e/OS compatibili

Scegliere in preferenza quelli contrassegnati con l'etichetta STABLE e dotati di Easy Installer preferibilmente anche di Roll Back (opzionale) oppure i Murena Smartphone che arrivano già preinstallati.

- -> **doc.e.foundation/devices**

Per facilitare la selezione queste impostazioni mostrate nello screenshot ridurranno la lista a quelli preferiti come sopra.



In ordine secondo il più recente rilasciato sul mercato troviamo:

TeraCube 2e, Fairphone 4, OnePlus 8 and 8 pro, Google Pixel 4a, Gigaset GS290, OnePlus Nord, Google Pixel 5 -- *before 2020* -- Fairphone 3 and 3+, OnePlus 7 pro and 7T, Google Pixel 4 and 4XL, Samsung Galaxy S9, S9+ S8, S7 and S7 edge.

Operatori 4G suggeriti

- in Italia con EU roaming, Iliad - **www.iliad.it**
- internazionale, giffgaff - **www.giffgaff.com**

100 free Cyber Security Tools

For ethical hackers and forensic investigators

- -> **original LK post from HRC**
- -> **PDF download from LK media**

The Hacker Manifesto

Il Manifesto Hacker di Loyd Blankenship presentato in un video sul canale youtube di Red Hot Cyber.

- -> **youtu.be/nr02_ELQsbI**

Era una giornata fredda dell'8 gennaio 1986 quando The Mentor scrisse il breve saggio dal titolo "the hacker manifesto". Si tratta di un altro pezzo fondamentale della cultura hacker, che tra poco comprerà 35 anni. Un manifesto, preso in prestito da tutti gli hacker, vecchi e nuovi e che rappresenta una descrizione scritta della filosofia hacker che la raffigura sia dal punto di vista ideologico, psicologico che sociale. Ed è questo che vi racconterò oggi.

Steganografia

La **steganografia** è una tecnica che si prefigge di nascondere la comunicazione tra due interlocutori. [...] Generalmente, i messaggi nascosti sembrano essere (o fanno parte di) qualcos'altro: immagini, articoli, liste della spesa o un altro testo di copertura.

Ad esempio, il messaggio nascosto può essere un inchiostro invisibile tra le linee di una lettera privata. Alcune implementazioni della steganografia che non utilizzano un segreto comune sono forme di ***security through obscurity***, mentre gli schemi steganografici a chiave dipendono dal **principio di Kerckhoffs**.

La steganografia, a differenza della **crittografia**, consente di nascondere un messaggio all'interno di un vettore che possa consentirne il trasporto senza destare sospetti.

Ad esempio, un mittente potrebbe inviare un file di immagine innocuo e regolare il colore di un pixel ogni cento per farlo corrispondere a un carattere alfabetico. La modifica è così lieve che è improbabile che qualcuno la noti, a meno che non la stia cercando in modo specifico.

Plausible deniability

The **plausible deniability** is the ability of people, typically senior officials in a formal or informal chain of command, to deny knowledge of or responsibility for actions committed by or on behalf of members of their organizational hierarchy.

Combinando queste diverse tecniche, ad esempio mediante errori ortografici o declinazioni di verbi in tempi incorretti rispetto al contesto si possono inviare brevissimi messaggi (hook codes) che oltre a passare generalmente inosservati hanno il beneficio di essere plausibilmente negabili di essere messaggi di comunicazione.

Hook codes

Hooking code that handles such intercepted function calls, events or messages *is called a hook. Hook methods are of particular importance in the Template Method Pattern where common code in an abstract class can be augmented by custom code in a subclass.*

Gli hook codes possono servire a molti scopi quali:

- informare e/o validare un messaggio
- determinare mittente e/o destinatario
- indicare la tipologia di codifica usata

- indicare dove si trova il messaggio

Gli hook codes più efficaci sono quelli non strettamente codificati ovvero quelli che sono diretti alle persone e non a degli algoritmi. La combinazione di questo tipo di hook codes con altre tecniche permette di creare un sistema di comunicazione che può essere, anche se scoperto, decifrato solo dalle persone che ne conoscono i meccanismi e le informazioni di contesto relative.

- -> **La steganografia e le sue possibili implementazioni**

Breve articolo divulgativo riguardo a un progetto che permette di salvare files dentro a dei video di youtube e la struttura frattale dei numeri primi.

Bare conductive electric paint

- -> **lnkd.in/dQwP8Xyd**

There are many version of it. Another one is Liquiwire™. However, making this product as DIY is quite simple and requires two ingredients: graphite powder and Elmer's glue, mixed together.

Here two interesting links about DIY conductive painting:

- -> **lnkd.in/dkyFT674**
- -> **lnkd.in/dYaNWPQK**

Combining the instructions from these two links, it is possible to produce large quantities of this conductive paint for a small amount of money: BBQ charcoal briquettes $16 for 5lb + Elmer's glue $21 per gallon.

Please notice that the briquettes need to be broken in small fragments before being put into the blender and the blender should be designed for crushing ice. Such blender starts to be priced from $25. While a press-on refillable pen can be bought for $1 each.

Prices collected on Amazon as reference.

Advanced electronic devices

Flipper Zero is a portable multi-tool for pentesters and geeks in a toy-like body. It loves hacking digital stuff, such as radio protocols, access control systems, hardware, and more. It's fully open-source and customizable, so you can extend it in whatever way you like. -- source: **flipperzero.one**

- -> **amazon.it/gp/product/B0BFXKSFNT** (ref. price: €200 c.a.)

Wifi Deauther, deauthing a network means to forcibly disconnect all the devices connected to a network. This is possible as the Management frames used to administrate a WiFi connection are unencrypted. So a 3rd party can inject false Management Frames into a network, disconnecting clients.

- -> **Aursinc dstike WiFi deauther & bad USB watch V4** €140 c.a.

- -> **Seamuing dstike WiFi deauther & test tool watch** €70 c.a.
- -> **Seamuing ESP32 dev board WiFi w/OLED 0.96"** €23 c.a.
- -> **LilyGo T-Deck ESP32-S3 blackberry-like dev board** $53 c.a.

Portable products and prepared kits based on ATMega 32 are available. Using Amazon Italia as price reference, starting from €23 up to €140.

Radio frequency gadgets

Moreover, about the radio frequency hacking and signal analyzing, there are nice OSHW/SW projects as much interesting as the Flipper Zero.

- -> **HackRF One FROM Great Scott Gadgets** in a €170 - €340 range

HackRF One is a Software Defined Radio (SDR) peripheral capable of transmission or reception of radio signals from 1 MHz to 6 GHz. Designed to enable test and development of modern and next generation radio technologies, HackRF One is an open source hardware platform that can be used as a USB peripheral or programmed for stand-alone operation.

- -> **HackRF Portapack H4M** with **mayhem firmware** from $152

HackRF Portapack H4M is a Receiver and Spectrum Analyzer based on HackRF One but assembled with other stuff to made it portable. Because it is an Open Hardware and Open Software project many forks and producer are available but not all of them are necessarily deserve our attention or money. Revisions and models variety is explained in **this video**.

- -> Quansheng UV-K5 or UK-K6 with **F4HWN custom firmware** from €16

Quansheng UV-Kx radios are not professional quality transceivers, their performance is strictly limited. The RX front end has no track-tuned band pass filtering at all, and so are wide band/wide open to any and all signals over a large frequency range.

Quansheng UV-K5 and UV-K6 with F4HWN custom firmware

Despite this limitations, they can offer also a basic spectrum analyser and considering the very very cheap price on Chinese online market places, it is a great starting point.

Quansheng UV-K5 out-of-band spurious harmonics explanation:

- **YouTube video** (04m22s - 08m24s)

List of the most common antennas available:

- Antenna SRH805 city range UHF only
- Abbree AR-805S city range VHF also
- Antenna NA-771 outdoor range
- Antenna NA-F30 72cm long range

Note that some antennas can create spurious harmonics also out side the legit bands even when used in combination with FCC compliant ham radios transmitting on the legit bands.

- **Handheld ham radio antennas comparison**

The most wide-spread ham radio is based on the Baofeng UV-5R model:

- **Baofeng UV-5R resources file**

This PDF file collects some interesting resources based mainly on YouTube videos about how to start using them, how to deal with all the config and also how to unlock extended features.

WARNING

Please, pay attention to not create interference or transmitting on forbidden bands.

Customized wi-fi routers

The **OpenWrt Project** is a Linux operating system targeting embedded devices. Instead of trying to create a single, static firmware, OpenWrt provides a fully writable filesystem with package management. This frees you from the application selection and configuration provided by the vendor and allows you to customize the device through the use of packages to suit any application. For developers, OpenWrt is the framework to build an application without having to build a complete firmware around it; for users this means the ability for full customization, to use the device in ways never envisioned.

- -> **openwrt.org**

Alternative for penetration testing over WiFi networks

- -> **DIY WiFi Router using Kali Linux on a Raspberry Pi 3 Model B[+]**

The specific tool is name airgeddon:

- -> **kali.org/tools/airgeddon**

- -> **github.com/v1s1t0r1sh3r3/airgeddon**

The **airgeddon** is a menu driven 3rd party tools wrapper to audit wireless networks with many features and can be installed on many distributions.

Clockwork uConsole

- -> **clockworkpi.com/product-page/uconsole-kit-r-01**

Clockwork uConsole R-01 is a kit easy to DIY assembly (12+ y.o.) that equipped with 4G + WiFi module and based on RISC-V architecture can provide a full features mobile GNU/Linux device. The peculiarity of this board is being emancipated by ARM or INTEL architectures. However, ARM64 core modules can be bought separately.

Disaster radio

The disaster radio is an idea based on carrying on communications off the traditional network grids during natural disasters. The idea is to deploy a grid of nodes that can be powered by small batteries and recharged by small solar panels in order to be completely independent and self sufficient.

The **disaster radio** architecture is based on the LoRa (Low Energy Radio) mesh networking technology and a grid of low costs embedded device acting as nodes that can receive, transmit and repeat the data on that network.

- **Reticulum** - is a cryptography-based networking stack for building local and wide-area networks with readily available hardware. Reticulum can continue to operate even in adverse conditions with very high latency and extremely low bandwidth.

- **RNode** - is a handheld device that can be assembled DIY with easily to find components and embedded within a 3D printable case. When bought read-to-go, it is priced €139 or the equivalent in some cryptocurrencies.

- **MeshTastic** - is an open source, off-grid, decentralized, mesh network built to run on affordable, low-power devices. It enables you to use inexpensive LoRa radios as a long range off-grid communication platform in areas without existing or reliable communications infrastructure.

- **T-Echo** - is a MeshTastic LoRa handheld module ($54) for Arduino (not included) that can be coupled with a T-keyboard ($19) to DIY a dedicated mobile device.

A LoRa board with LCD and antenna can be bought for a price between €24 and €40 while a MeshTastic T-beamer can be priced upto €90 but a RF module is priced between €7 and €12. Instead, a BlackBerry like mobile device is available for $53 or €56 in Europe.

- -> **Generic LoRa UART module** €7 c.a.

- -> **Arduino RF module w/antenna** €12 c.a.

- -> **Arduino LoRa+WiFi+BLE add-on w/antenna** €24 c.a.

- -> **LilyGo LoRa ESP32 dev board w/antenna** €40 c.a.
- -> **LilyGo Meshtastic T-Beam ESP32 dev board w/antenna** €90 c.a.
- -> **LilyGo T-Deck ESP32-S3 LoRa+WiFi+BLE mobile device** $53 c.a.

Amazon used as price reference e-commerce platform.

3-3-3 Radio SHTF Communications

The 3-3-3 Radio Plan for SHTF Communications resources:

- **3-3-3-radio-plan-for-shtf-communications**
- **shtf_frequency_list_2013e_print.png**
- **prepper_and_survivalist_frequency_list_333_plan.pdf**

The SHTF communications and plans are ways to communicate and prepare for situations when conventional communication methods fail. Ham Radio isn't discussed much on survival websites, but it plays a crucial role in preparedness during these times. Knowledge is the most valuable asset in a survival situation.

Urban warfare and sabotage

John W. Spencer is a retired United States Army officer, researcher of urban warfare, and author. [...] During the Russian invasion of Ukraine in 2022, he started to give "how to resist the Russian invasions" through Twitter. This culminated in him releasing "The Mini-Manual for the Urban Defender: A Guide to the Strategies and Tactics of Defending a City", which was translated in more than 10 languages.

- -> **Mini Manual for the Urban Defender v.5** (PDF)
- -> **John W. Spencer Urban Warfare bibliography**

The CIA's *Simple Sabotage Field Manual*: A Timeless Guide to Subverting Any Organization with "*Purposeful Stupidity*". It has been distributed in 1944 by the Strategic Services for the information and guidance of all concerned and will be used as the basic doctrine for Strategic Services training for this subject.

- -> **Simple Sabotage Field Manual** on Gutenberg Project

Questo manuale è stato scritto nel 1944 ed è stato de-secretato nel 2008.

Si vis Pacem, para Bellum

Si vis pacem, para bellum - se vuoi la pace, prepara la guerra - è una locuzione latina. Usata soprattutto per affermare che uno dei mezzi più efficaci per assicurare la pace consiste nell'essere armati e in grado di difendersi, possiede anche un significato più profondo che

è quello che vede proprio coloro che imparano a combattere come coloro che possono comprendere meglio e apprezzare maggiormente la pace. --**Wikipedia**

- Allievo: maestro perché parli di pace e mi insegni a combattere?
- Bruce Lee: perché preferisco avere un guerriero in un giardino che un giardiniere in un campo di battaglia.

Oppure detto in altre parole: un popolo inerme è un popolo già sconfitto.

Interesting works

Hacking a Smart Home Device - How I reverse engineered an ESP32-based smart home device to gain remote control access and integrate it with Home Assistant.

- **https://jmswrnr.com/blog/hacking-a-smart-home-device**

BitLocker encryption broken in 43 seconds with sub-$10 Raspberry Pi Pico. The key can be sniffed when using an external TPM. The youtube video presents some others links.

- **https://www.youtube.com/watch?v=wTl4vEednkQ**
- **https://github.com/stacksmashing/pico-tpmsniffer**
- **https://github.com/stacksmashing/LPCClocklessAnalyzer**
- **https://labs.withsecure.com/publications/sniff-there-leaks-my-bitlocker-key**
- **https://www.secura.com/blog/tpm-sniffing-attacks-against-non-bitlocker-targets**
- **https://pulsesecurity.co.nz/articles/TPM-sniffing**
- **https://blog.scrt.ch/2021/11/15/tpm-sniffing**

ssh-chat, a chat over SSH. Custom SSH server written in Go. Instead of a shell, you get a chat prompt. Just an working PoC as example rather than a prdocut.

- **https://github.com/shazow/ssh-chat?tab=readme-ov-file#ssh-chat**

Search Engines for Pen-testers

List provided by **Hacking Articles** in a public post

1. **shodan.io** (Server)
2. **Google Dorks** (Queries)
3. **wigle.net** (WiFi Networks)
4. **grep.app** (Codes Search)
5. **app.binaryedge.io** (Threat Intelligence)

6. **onyphe.io** (Server)
7. **viz.greynoise.io** (Threat Intelligence)
8. **censys.io** (Server)
9. **hunter.io** (Email Addresses)
10. **fofa.info** (Threat Intelligence)
11. **zoomeye.org** (Threat Intelligence)
12. **leakix.net** (Threat Intelligence)
13. **intelx.io** (OSINT)
14. **app.netlas.io** (Attack Surface)
15. **searchcode.com** (Codes Search)
16. **urlscan.io** (Threat Intelligence)
17. **publicwww.com** (Codes Search)
18. **fullhunt.io** (Attack Surface)
19. **socradar.io** (Threat Intelligence)
20. **binaryedge.io** (Attack Surface)
21. **ivre.rocks** (Server)
22. **crt.sh** (Certificate Search)
23. **vulners.com** (Vulnerabilities)
24. **pulsedive.com** (Threat Intelligence)

OSINT tools and engines

Experts can often collect significant artifacts related to the authors behind the analyzed scenarios during cybersecurity exercises, including details such as emails, usernames, IP addresses, domains, and so on. This article will provide you with a list of online tools to help you discover and track criminals' identities, their secrets, or even geolocation.

1. **github.com/coldvisionz/osint-investigation**
2. **github.com/sherlock-project/sherlock**
3. **github.com/smicallef/spiderfoot**
4. **github.com/p1ngul1n0/blackbird**

5. **instantusername.com**
6. **haveibeenpwned.com**
7. **whois.domaintools.com**
8. **viewdns.info**
9. **breachdirectory.org**
10. **data.occrp.org**
11. **usa-official.com**
12. **thatsthem.com**
13. **searchpeoplefree.com**
14. **knowem.com**
15. **namecheckr.com**
16. **social-searcher.com**
17. **whatsmyname.app**

Share alike