Op Indexer/Collection

- iamavu Cyber Collection (The Texts of Athena) - A collection of resources, tricks, techniques , etc.
- CyberSecurity Search Engine - Cheatsheets, Tools & Resources - Cybersecurity spaces with lots of resources
- Pandora - Another cool cyber stuff awesome collection, **but it is not upto date**

CyberSecurity Tools

> Reverse Engineering Tools is also useful in cybersecurity analysis

CLI based

- Zydra - Password Recovery Tool or BruteForce password cracking tool. It can use to recover password of rar,zip and pdf file.
- SSH-Snake - SSH-Snake is a self-propagating, self-replicating, file-less script that automates the post-exploitation task of SSH private key and host discovery

Wordlist

- WeakPass - Collection of wordlist over 700GB (found our rockyou.txt[.gz]!!)

Scanner

- MobSF (Mobile Security Framwork) - Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis... (read more)

Browser Extensions

- Hack Tool | FireFox | Chrome - **The all-in-one Red Team extension for Web Pentester 🛠️.** HackTools, is a web extension facilitating your web application penetration tests, it includes cheat sheets as well as all the tools used during a test such as XSS payloads, Reverse shells and much more.

Website based

- CyberChef | Github - CyberChef is a simple, intuitive web app for carrying out all manner of "cyber" operations within a web browser.

  > credit : TryHackMe Advent of Cyber 4 Task 12(Day 7)

- Rev Shell ⭐ | Github Repo - Online Reverse Shell generator with a ton of functionality. -- (Great for CTFs)

Living off the land ⭐

- GTFOBins (Linux) - GTFOBins is a curated list of Unix binaries that can be used to bypass local security restrictions in misconfigured systems.
- LOLBAS (Windows) - The goal of the LOLBAS project is to document every binary, script, and library that can be used for Living Off The Land techniques.

- LOOBins (macOS) - Living Off the Orchard: macOS Binaries (LOOBins) is designed to provide detailed information on various built-in macOS binaries and how they can be used by threat actors for malicious purposes.

- LOLDrivers (Drivers) - L.O.L. Drivers is a curated list of Windows drivers used by adversaries to bypass security controls and carry out attacks. The project helps security professionals stay informed and mitigate potential threats.

- LOTS (Living Off Trusted Sites) Project - Attackers are using popular legitimate domains when conducting phishing, C&C, exfiltration and downloading tools to evade detection. The list of websites that allow attackers to use their domain or subdomain are listed on website.

- HijackLibs - This project provides an curated list of DLL Hijacking candidates. A mapping between DLLs and vulnerable executables is kept and can be searched via this website. Additionally, further metadata such as resources provide more context.

Misc

- PHP Reverse Shell Script Page - This .php file can use on website which allow access to uploaded file,i.e. website allow .php file upload and allow to accept it eg. https://example.com/uploads/reverse_shell.php

  > Expain : Uploaded file intend to be load as image or get download file in client pc,but .php will get treated as server php page and get executed. It happens if not extension validation is happen when asking for image only upload or preventing .php file to execute from upload folder

- ProjectDiscovery | Community - Open-Source CyberSec company aim to develop security tools (builds tools to detect and remediate vulnerabilities across your modern tech stack.)

Vulnerable VM for practice (or just VM based stuff...)

- CommandoVM - a fully customizable, Windows-based security distribution for penetration testing and red teaming.
- FlareVM - a collection of software installations scripts for Windows systems that allows you to easily setup and maintain a reverse engineering environment on a virtual machine (VM). FLARE VM was designed to solve the problem of reverse engineering tool curation and relies on two main technologies: Chocolatey and Boxstarter. Chocolatey is a Windows-based Nuget package management system, where a "package" is essentially a ZIP file containing PowerShell installation scripts that download and configure a specific tool. Boxstarter leverages Chocolatey packages to automate the installation of software and create repeatable, scripted Windows environments.
- TraceLabs OSINT VM | See It In Action - The Trace Labs team created a specialized OSINT VM specifically to bring together the most effective OSINT tools and customized scripts we saw being used during our Search Party CTF's. Inspired by the infamous Buscador VM, the Trace Labs OSINT VM was built in a similar way, to enable OSINT investigators participating in the Trace Labs Search Party CTF's a quick way to get started and have access to the most popular OSINT tools and scripts all neatly packaged under one roof.

Search engine for hackers/pentesters

- https://shodan.io - Servers
- https://google.com - Dorks
- https://wigle.net - WiFi Networks

- https://grey.app - Code Search
- https://app.binaryedge - Threat Intelligence
- https://onyphe.io - Server
- https://viz.greynoise.io - Threat Intelligence
- https://censys.io - Server
- https://hunter.io - Email Addresses
- https://fofa.info - Threat Intelligence
- https://zoomeye.org - Threat Intelligence
- https://leakix.net - Threat Intelligence
- https://intelx.io - OSINT
- https://app.netlas.io - Attack Surface
- https://searchcode.com - Code Search
- https://urlscan.io - Threat Intelligence
- https://publicwww.com - Code Search
- https://fullhunt.io - Attack Surface
- https://socradar.io - Threat Intelligence
- https://binaryedge.io - Attack Surface
- https://ivre.rocks - Server
- https://crt.sh - Certificate Search
- https://vulners.com - Vulnerabilities
- https://pulsedive.com - Threat Intelligence