Introduction to CTF

Basics, search, and infosec

June 25, 2022

Welcome

Welcome to CTF team training! We are COMPASS CTF Team.

CTF (Capture the Flag) is a kind of competitions in Computer Security.

You can learn from CTF:

- computer science methodology.
- computer security on hacking and defense.
- co-operate with team members.

Overview

Today's topics are include:

- CTF introduction
- Categories
- Tools and resources to CTF
- How to use search engines
- Related books

CTF introduction

"Knowing is not enough; we must apply. Willing is not enough; we must do." - Johann Wolfgang von Goethe

Computer security represents a challenge to education due to its interdisciplinary nature. Topics in computer security are drawn from areas ranging from theoretical aspects of computer science to applied aspects of information technology management. This makes it difficult to encapsulate the spirit of what constitutes a computer security professional.

CTF introduction

Find a CTF:

- PicoCTF and PlaidCTF by CMU
- HSCTF is made for high school students
- Ghost in the Shellcode (GitS)
- CSAW CTF by NYU-Poly
- UCSB iCTF is for academics only
- Defcon CTF

Use CTFtime to find CTFs: https://ctftime.org/event/list/upcoming

CTF introduction

How is a Wargame different?

Wargames are similar to a CTF but are always ongoing. Typically, they are organized into levels that get progressively harder as you solve more of them. Wargames are an excellent way to practice for CTF!

- Micro Corruption
- SmashTheStack
- OverTheWire
- Exploit Exercises

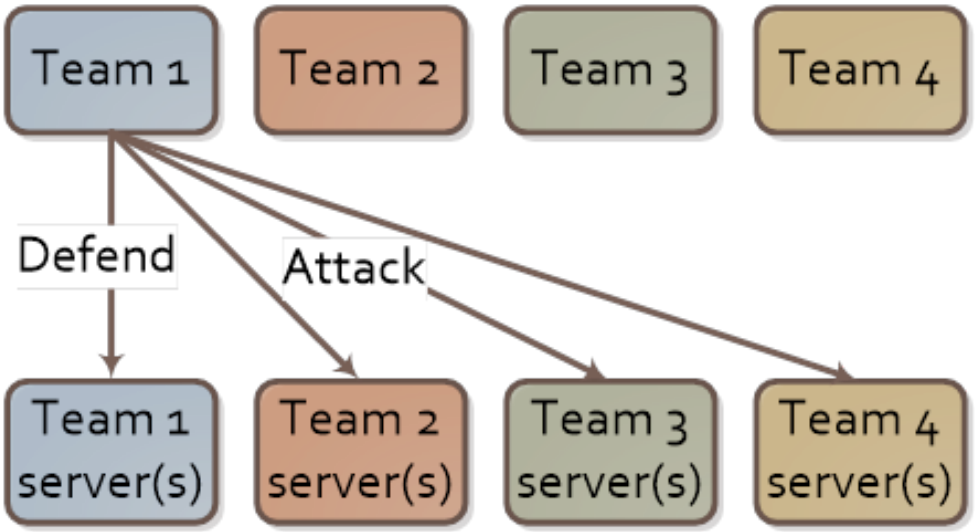
CTF introduction

What about CCDC?

There are some defense-only competitions that disguise themselves as CTF competitions, mainly the Collegiate Cyber Defense Challenge (CCDC) and its regional variations, and our opinion is that you should avoid them. They are unrealistic exercises in frustration and will teach you little about security or anything else. They are incredibly fun to play as a Red Team though!

CTF introduction

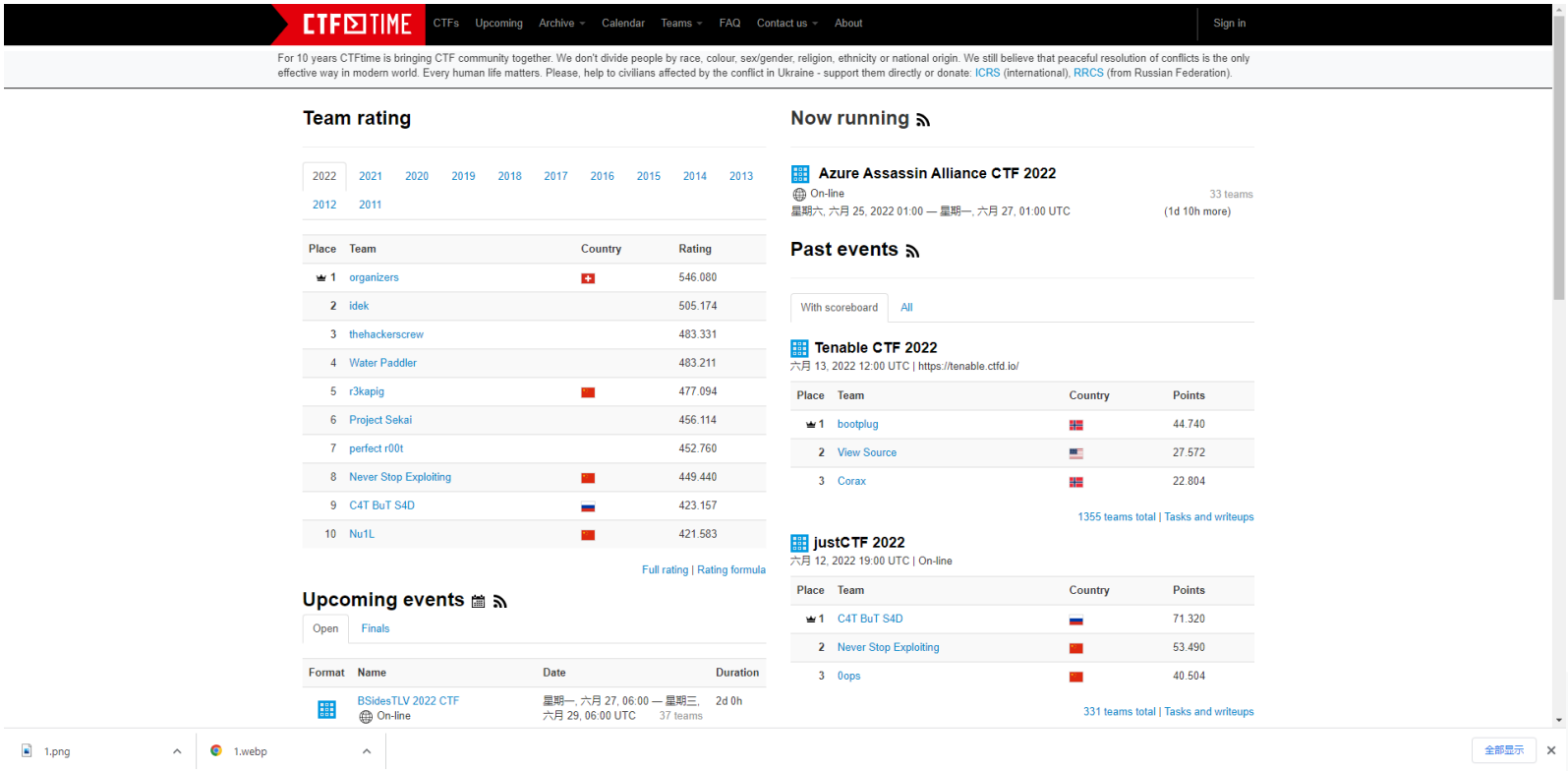
An Attack/Defense Capture the Flag is a type of cybersecurity competition where competing teams attempt to find security vulnerabilities in services run by the opposing teams. Each team works finding vulnerabilities in other team's services while protecting their own, hence "attack/defense".



CTF introduction

Where to find a CTF?

https://ctftime.org/



CTF introduction

Find a Job:

- Application Security (code audits/app assessments)
- Attacker (offensive)
- Compliance
- Forensics
- Incident Handler
- Manager
- Network Security Engineer
- Penetration Tester
- Policy
- Researcher
- Reverse Engineer
- Security Architect

CTF introduction

The Basics

- Linux
- Windows
- Python programming
- GIT
- Firewalls
- Proxies and VPNs

CTF introduction

Linux was first released in September 17, 1991 by Linus Torvalds. Strictly speaking Linux is just the kernel in the GNU/Linux operating system. Linux is the most installed OS in the world, that is mainly due to the fact that android use Linux as its OS. It is leading in pretty much all markets except for the desktop-market.

- Package management program.
- Speed and interval of release
- Desktop environment
- Default GUI
- Community
- Compilation of the Linux Kernel

We typically use kali linux or black arch as environment.

Basics of linux

- The Shell - Bash
  - Navigating
  - Looking at files
  - Working with files
  - Finding files
- Editing text
- User management
- Permissions
- Processes
- Packages
- The Filesystem
- Network basics

Bash-scripting

Bash is also a scripting language, used to programming basically.

The following code will iterate over a file and echo out every single line:

Solution

```
#!/bin/bash
for line in $(cat file.txt);do
echo $line
done
```

Bash-scripting

- For-loops
- If statement
- Command line arguments
- Daemonize an execution
- Use the output of command

Bash is a script language rather than a compilation language.

Vim

http://www.viemu.com/a-why-vi-vim.html

And also this classic answer: https://stackoverflow.com/questions/1218390/what-is-your-most-productive-shortcut-with-vim

- Movement - Motion commands
- Additional Commands
  - :q - Quit.
  - :wq - Save and close.
  - :syntax on - Turn on Syntax highlighting for C programming and other
  - languages.
  - :history - Shows the history of the commands executed
  - :set number - Turn on the line numbers.
  - :set nonumber - Turn off the line numbers.
- Clipboard
- Plugins

Man pages

Online man pages are available at https://man.cx/ if you are curious about some flags and not near a linux terminal

Use man page to find help for commands in Linux.

Windows

Whether you like it or not Windows is the most common OS for desktop users in the world. So for a pentester it is fundamental to understand the ins and outs of it.

So this chapter will contain some basics about Windows and windows networks.

We will also look a bit at **PowerShell** and of course the good old **CMD**.

Basics of windows

Versions of Windows

- Windows desktops OS
- Windows Server

Windows Networks

- User privileges
- Windows domain
- IIS - Windows web server
- File types
  - BAT - Bash Script
  - DLL - Dynamic Link Library

PowerShell

PowerShell is Windows new shell. It comes by default from Windows 7. But can be downloaded and installed in earlier versions.

- PowerShell provides access to almost everything an attacker might want.
- It is based on the .NET framework.
- It is basically bash for windows

Solution

Get-Help <cmdlet name | topic name>

PowerShell Execute scripts

Restricted: PowerShell won't run any scripts. This is PowerShell's default execution policy.

AllSigned: PowerShell will only run scripts that are signed with a digital signature. If you run a script signed by a publisher PowerShell hasn't seen before, PowerShell will ask whether you trust the script's publisher.

RemoteSigned: PowerShell won't run scripts downloaded from the Internet unless they have a digital signature, but scripts not downloaded from the Internet will run without prompting. If a script has a digital signature, PowerShell will prompt you before it runs a script from a publisher it hasn't seen before.

Unrestricted: PowerShell ignores digital signatures but will still prompt you before running a script downloaded from the Internet.

CMD - Windows commands

- Dealing with files and stuff
- Network
- Processes
- Users
- Mounting - Mapping

Scripting With Python

There are many high-level scripting languages that are easy to use. One really popular one is Python.

- Array/list
- Modules
- Pip - package management

GIT

Version Control System, really useful for tracking your changes.

try.github.com 15 mins tutorial.

To use Git on the command line, you'll need to download, install, and configure Git on your computer. You can also install GitHub CLI to use GitHub from the command line. For more information, see "About GitHub CLI."

Firewalls

This basically means that we are filtering outgoing traffic. So egress filtering ensures that malicious, or just prohibited, traffic is not allowed to leave the network. Of course egress filtering then is the enemy of the hacker.

Usually we don't recommend you to install a firewall as you are well at computer science. But if you want to use one, check the different cons & pros.

Proxies and VPNs

Not going to talk here because of some reason. I can only mention that we would use Google and International services a lot. Please make sure you can connect to World Wide Websites.

Offering paid VPN service is illegal, don't sell VPN to others.

Grey or Black areas

Don't play with those dangerous things. Any black aspects would get yourself caught, and even grey sometimes is illegal.

Tor: tor and tor browser, a trick to connect to the "dark net". Sometimes, tor is just a anonymous tool, but if you still can find every dangerous and illegal things on the dark net.

OSINT(*): OSINT is a method to find information from the pictures, photos, and videos. Don't try to steal other's personal information from the leaked social media information.

Phishing: from a fake website to construct a similar page, and get the victims hooked.

Categories

CTF events usually have 5 categories:

- Forensics
- Cryptography
- Web Exploitation
- Reverse Engineering
- Binary Exploitation

Forensics

Forensics is the art of recovering the digital trail left on a computer. There are plently of methods to find data which is seemingly deleted, not stored, or worse, covertly recorded.

An important part of Forensics is having the right tools, as well as being familair with the following topics:

- File Formats
- EXIF data
- Wireshark & PCAPs
- What is Wireshark
- Stegonagraphy
- Disk Imaging

Cryptography

Cryptography is the reason we can use banking apps, transmit sensitive information over the web, and in general protect our privacy. However, a large part of CTFs is breaking widely used encryption schemes which are improperly implemented. The math may seem daunting, but more often than not, a simple understanding of the underlying principles will allow you to find flaws and crack the code.

The word "cryptography" technically means the art of writing codes. When it comes to digital forensics, it's a method you can use to understand how data is constructed for your analysis.

- XOR
- Cesear Cipher
- Substitution Cipher
- Vigenere Cipher
- Hashing Functions
- Block Ciphers
- Stream Ciphers
- RSA

Web Exploitation

Websites all around the world are programmed using various programming languages. While there are specific vulnerabilities in each programming langage that the developer should be aware of, there are issues fundamental to the internet that can show up regardless of the chosen language or framework.

These vulnerabilities often show up in CTFs as web security challenges where the user needs to exploit a bug to gain some kind of higher level privelege.

Common vulnerabilities to see in CTF challenges:

- SQL Injection
- Command Injection
- Directory Traversal
- Cross Site Request Forgery
- Cross Site Scripting
- Server Side Request Forgery

Reverse Engineering

Reverse Engineering in a CTF is typically the process of taking a compiled (machine code, bytecode) program and converting it back into a more human readable format.

Very often the goal of a reverse engineering challenge is to understand the functionality of a given program such that you can identify deeper issues.

- Assembly / Machine Code
- The C Programming Language
- Disassemblers
- Decompilers

Categories

Binary Exploitation

Binaries, or executables, are machine code for a computer to execute. For the most part, the binaries that you will face in CTFs are Linux ELF files or the occasional windows executable. Binary Exploitation is a broad topic within Cyber Security which really comes down to finding a vulnerability in the program and exploiting it to gain control of a shell or modifying the program's functions.

Common topics addressed by Binary Exploitation or 'pwn' challenges include:

- Registers
- The Stack
- Calling Conventions
- Global Offset Table (GOT)
- Buffers
- Return Oriented Programming (ROP)
- Binary Security
- The Heap
- Format String Vulnerability

Attacks

Tools used for performing various kinds of attacks

- Bettercap - Framework to perform MITM (Man in the Middle) attacks.
- Yersinia - Attack various protocols on layer 2.

Crypto

Tools used for solving Crypto challenges

- CyberChef - Web app for analysing and decoding data.
- FeatherDuster - An automated, modular cryptanalysis tool.
- Hash Extender - A utility tool for performing hash length extension attacks.
- padding-oracle-attacker - A CLI tool to execute padding oracle attacks.
- PkCrack - A tool for Breaking PkZip-encryption.
- QuipQuip - An online tool for breaking substitution ciphers or vigenere ciphers (without key).
- RSACTFTool - A tool for recovering RSA private key with various attack.
- RSATool - Generate private key with knowledge of p and q.
- XORTool - A tool to analyze multi-byte xor cipher.

Bruteforcers

Tools used for various kind of bruteforcing (passwords etc.)

- Hashcat - Password Cracker
- Hydra - A parallelized login cracker which supports numerous protocols to attack
- John The Jumbo - Community enhanced version of John the Ripper.
- John The Ripper - Password Cracker.
- Nozzlr - Nozzlr is a bruteforce framework, trully modular and script-friendly.
- Ophcrack - Windows password cracker based on rainbow tables.
- Patator - Patator is a multi-purpose brute-forcer, with a modular design.
- Turbo Intruder - Burp Suite extension for sending large numbers of HTTP requests

Exploits

Tools used for solving Exploits challenges

- DLLInjector - Inject dlls in processes.
- libformatstr - Simplify format string exploitation.
- Metasploit - Penetration testing software.
- one_gadget - A tool to find the one gadget execve('/bin/sh', NULL, NULL) call.
- Pwntools - CTF Framework for writing exploits.
- Qira - QEMU Interactive Runtime Analyser.
- ROP Gadget - Framework for ROP exploitation.
- V0lt - Security CTF Toolkit.

Forensics

Tools used for solving Forensics challenges

- Aircrack-Ng - Crack 802.11 WEP and WPA-PSK keys.
- Audacity - Analyze sound files (mp3, m4a, whatever).
- Bkhive and Samdump2 - Dump SYSTEM and SAM files.
- CFF Explorer - PE Editor.
- Creddump - Dump windows credentials.
- DVCS Ripper - Rips web accessible (distributed) version control systems.
- Exif Tool - Read, write and edit file metadata.
- Extundelete - Used for recovering lost data from mountable images.
- Fibratus - Tool for exploration and tracing of the Windows kernel.
- Foremost - Extract particular kind of files using headers.

Forensics

Tools used for solving Forensics challenges

- Fsck.ext4 - Used to fix corrupt filesystems.
- Malzilla - Malware hunting tool.
- NetworkMiner - Network Forensic Analysis Tool.
- PDF Streams Inflater - Find and extract zlib files compressed in PDF files.
- Pngcheck - Verifies the integrity of PNG and dump all of the chunk-level information in human-readable form.
- ResourcesExtract - Extract various filetypes from exes.

Forensics

Tools used for solving Forensics challenges

- Shellbags - Investigate NT_USER.dat files.
- Snow - A Whitespace Steganography Tool.
- USBRip - Simple CLI forensics tool for tracking USB device artifacts (history of USB events) on GNU/Linux.
- Volatility - To investigate memory dumps.
- Wireshark - Used to analyze pcap or pcapng files
- OfflineRegistryView - Simple tool for Windows that allows you to read offline Registry files from external drive and view the desired Registry key in .reg file format.
- Registry Viewer® - Used to view Windows registries.

Networking

Tools used for solving Networking challenges

- Masscan - Mass IP port scanner, TCP port scanner.
- Monit - A linux tool to check a host on the network (and other non-network activities).
- Nipe - Nipe is a script to make Tor Network your default gateway.
- Nmap - An open source utility for network discovery and security auditing.
- Wireshark - Analyze the network dumps.
- Zeek - An open-source network security monitor.
- Zmap - An open-source network scanner.

Reversing

Tools used for solving Reversing challenges

- Androguard - Reverse engineer Android applications.
- Angr - platform-agnostic binary analysis framework.
- Apk2Gold - Yet another Android decompiler.
- ApkTool - Android Decompiler.
- Barf - Binary Analysis and Reverse engineering Framework.
- Binary Ninja - Binary analysis framework.
- BinUtils - Collection of binary tools.
- BinWalk - Analyze, reverse engineer, and extract firmware images.
- Boomerang - Decompile x86/SPARC/PowerPC/ST-20 binaries to C.
- ctf_import – run basic functions from stripped binaries cross platform.
- cwe_checker - cwe_checker finds vulnerable patterns in binary executables.
- demovfuscator - A work-in-progress deobfuscator for movfuscated binaries.

Tools and resources to CTF

Reversing

Tools used for solving Reversing challenges

- Frida - Dynamic Code Injection.
- GDB - The GNU project debugger.
- GEF - GDB plugin.
- Ghidra - Open Source suite of reverse engineering tools. Similar to IDA Pro.
- Hopper - Reverse engineering tool (disassembler) for OSX and Linux.
- IDA Pro - Most used Reversing software.
- Jadx - Decompile Android files.
- Java Decompilers - An online decompiler for Java and Android APKs.

Reversing

Tools used for solving Reversing challenges

- Krakatau - Java decompiler and disassembler.
- Objection - Runtime Mobile Exploration.
- PEDA - GDB plugin (only python2.7).
- Pin - A dynamic binary instrumentaion tool by Intel.
- PINCE - GDB front-end/reverse engineering tool, focused on game-hacking and automation.
- PinCTF - A tool which uses intel pin for Side Channel Analysis.
- Plasma - An interactive disassembler for x86/ARM/MIPS which can generate indented pseudo-code with colored syntax.
- Pwndbg - A GDB plugin that provides a suite of utilities to hack around GDB easily.
- radare2 - A portable reversing framework.
- Triton - Dynamic Binary Analysis (DBA) framework.

Reversing

Tools used for solving Reversing challenges

- Uncompyle - Decompile Python 2.7 binaries (.pyc).
- WinDbg - Windows debugger distributed by Microsoft.
- Xocopy - Program that can copy executables with execute, but no read permission.
- Z3 - A theorem prover from Microsoft Research.
- Detox - A Javascript malware analysis tool.
- Revelo - Analyze obfuscated Javascript code.
- RABCDAsm - Collection of utilities including an ActionScript 3 assembler/disassembler.
- Swftools - Collection of utilities to work with SWF files.
- Xxxswf - A Python script for analyzing Flash files.

Tools and resources to CTF

Services

Various kind of useful services available around the internet

- CSWSH - Cross-Site WebSocket Hijacking Tester.
- Request Bin - Lets you inspect http requests to a particular url.

Steganography

Tools used for solving Steganography challenges

- AperiSolve - Aperi'Solve is a platform which performs layer analysis on image (open-source).
- Convert - Convert images b/w formats and apply filters.
- Exif - Shows EXIF information in JPEG files.
- Exiftool - Read and write meta information in files.
- Exiv2 - Image metadata manipulation tool.
- Image Steganography - Embeds text and files in images with optional encryption. Easy-to-use UI.
- Image Steganography Online - This is a client-side Javascript tool to steganographically hide images inside the lower "bits" of other images
- ImageMagick - Tool for manipulating images.
- Outguess - Universal steganographic tool.
- Pngtools - For various analysis related to PNGs.

Steganography

Tools used for solving Steganography challenges

- SmartDeblur - Used to deblur and fix defocused images.
- Steganabara - Tool for stegano analysis written in Java.
- SteganographyOnline - Online steganography encoder and decoder.
- Stegbreak - Launches brute-force dictionary attacks on JPG image.
- StegCracker - Steganography brute-force utility to uncover hidden data inside files.
- stegextract - Detect hidden files and text in images.
- Steghide - Hide data in various kind of images.
- StegOnline - Conduct a wide range of image steganography operations, such as concealing/revealing files hidden within bits (open-source).
- Stegsolve - Apply various steganography techniques to images.
- Zsteg - PNG/BMP analysis.

Web

Tools used for solving Web challenges

- BurpSuite - A graphical tool to testing website security.
- Commix - Automated All-in-One OS Command Injection and Exploitation Tool.
- Hackbar - Firefox addon for easy web exploitation.
- OWASP ZAP - Intercepting proxy to replay, debug, and fuzz HTTP requests and responses
- Postman - Add on for chrome for debugging network requests.
- Raccoon - A high performance offensive security tool for reconnaissance and vulnerability scanning.
- SQLMap - Automatic SQL injection and database takeover tool. pip install sqlmap
- W3af - Web Application Attack and Audit Framework.
- XSSer - Automated XSS testor.
- CHYbeta/Code-Audit-Challenges - vulnerable code snippets can be used for source code audit challenges (in Chinese)

Operating Systems

Penetration testing and security lab Operating Systems

- Android Tamer - Based on Debian.
- BackBox - Based on Ubuntu.
- BlackArch Linux - Based on Arch Linux.
- Fedora Security Lab - Based on Fedora.
- Kali Linux - Based on Debian.
- Parrot Security OS - Based on Debian.
- Pentoo - Based on Gentoo.
- URIX OS - Based on openSUSE.
- Wifislax - Based on Slackware.
- Flare VM - Based on Windows.
- REMnux - Based on Debian.

Starter Packs

Collections of installer scripts, useful tools

- CTF Tools - Collection of setup scripts to install various security research tools.
- LazyKali - A 2016 refresh of LazyKali which simplifies install of tools and configuration.

Not recommend to use

As a CTF player, don't use those stupid software

- CMD. We have an alternative: PowerShell. Forget CMD.
- winrar, 2345 compress, or 360 compress. It's not good at all. If you don't want to use command, use 7-zip or something else.
- Any anti-virus. Don't run un-trusted software on your computer.
- Baidu. Don't know why this search engine exists.
- CSDN. Medium, Stack overflow are much better.
- Gitee. Do you like some code check about the "sensitive words"? Don't use it.
- ...to be add.

Tutorials

Tutorials to learn how to play CTFs

- CTF Field Guide - Field Guide by Trails of Bits
- CTF related notes - Personal CTFs and beyond notes (in Chinese)
- CTF Resources - Start Guide maintained by community
- CTF Tricks by Phithon - CTF tricks about Web (in Chinese)
- CTF-pwn-tips - Some tips about pwn
- firmianay/CTF-All-In-One - all CTF related tutorials complied in one book (in Chinese)
- How to Get Started in CTF - Short guideline for CTF beginners by Endgame
- Intro. to CTF Course - A free course that teaches beginners the basics of forensics, crypto, and web-ex.
- IppSec - Video tutorials and walkthroughs of popular CTF platforms.
- LiveOverFlow - Video tutorials on Exploitation.
- MIPT CTF - A small course for beginners in CTFs (in Russian)
- OWASP Mutillidae 2 Project - a free, open source, deliberately vulnerable web-application providing a target for web-security enthusiest
- RITSEC - RITSEC is a student run club at Rochester Institute of Technology. There are some CTF writeups and shares in this team repository.

Wargames

Always online CTFs

- 247ctf - A learning oriented real CTF platform with challenges covering across web, cryptography, networking, reversing and exploitation.
- Backdoor - Security Platform by SDSLabs.
- buuoj - A CTF training platform with challenges collected from the past real CTF contests around the world. (in Chinese)
- Crackmes - Reverse Engineering Challenges.
- CryptoHack - Fun cryptography challenges.
- echoCTF.RED - Online CTF with a variety of targets to attack.
- Exploit Exercises - Variety of VMs to learn variety of computer security issues.
- Exploit.Education - Variety of VMs to learn variety of computer security issues.
- Gracker - Binary challenges having a slow learning curve, and write-ups for each level.

Wargames

Always online CTFs

- Hack The Box - Weekly CTFs for all types of security enthusiasts.
- Hack This Site - Training ground for hackers.
- Hacker101 - CTF from HackerOne
- Hacking-Lab - Ethical hacking, computer network and security challenge platform.
- Hone Your Ninja Skills - Web challenges starting from basic ones.
- IO - Wargame for binary challenges.
- jarvisoj - A CTF training platform developed by Jarvis from USSLab in ZJU.
- Microcorruption - Embedded security CTF.
- Over The Wire - Wargame maintained by OvertheWire Community.
- PentesterLab - Variety of VM and online challenges (paid).
- PicoCTF - All year round ctf game. Questions from the yearly picoCTF competition.
- PWN Challenge - Binary Exploitation Wargame.

Wargames

Always online CTFs

- Pwnable.kr - Pwn Game.
- Pwnable.tw - Binary wargame.
- Pwnable.xyz - Binary Exploitation Wargame.
- Reversin.kr - Reversing challenge.
- Ringzer0Team - Ringzer0 Team Online CTF.
- Root-Me - Hacking and Information Security learning platform.
- ROP Wargames - ROP Wargames.
- SANS HHC - Challenges with a holiday theme released annually and maintained by SANS.
- SmashTheStack - A variety of wargames maintained by the SmashTheStack Community.
- Viblo CTF - Various amazing CTF challenges, in many different categories. Has both Practice mode and Contest mode.

Wargames

Always online CTFs

- VulnHub - VM-based for practical in digital security, computer application & network administration.
- W3Challs - A penetration testing training platform, which offers various computer challenges, in various categories.
- WebHacking - Hacking challenges for web.
- CTFTraining - CTF challenge's source code, writeup collected from the past real CTF contests around the world. (in Chinese)
- My CTF Web Challenges - CTF challenge's source code, writeup and some idea explanation. All about Web.
- Pikachu - PHP web application with some common delibrated vulnerabilities. (in Chinese)

Tools and resources to CTF

Websites

Various general websites about and on CTF

- Awesome CTF Cheatsheet - CTF Cheatsheet.
- CTF Time - General information on CTF occuring around the worlds.
- Reddit Security CTF - Reddit CTF category.

Wikis

Various Wikis available for learning about CTFs

- Bamboofox - Chinese resources to learn CTF
- bi0s Wiki - Wiki from team bi0s.
- CTF Cheatsheet - CTF tips and tricks.
- CTF-Wiki - Open Wiki for beginners in CTFs (in Chinese and English)
- ISIS Lab - CTF Wiki by Isis lab
- OpenToAll - Open To All Knowledge Base

Writeups Collections

Collections of CTF write-ups

- 0e85dc6eaf - Write-ups for CTF challenges by 0e85dc6eaf
- Captf - Dumped CTF challenges and materials by psifertex.
- CTF write-ups (community) - CTF challenges + write-ups archive maintained by the community.
- CTFTime Scrapper - Scraps all writeup from CTF Time and organize which to read first.
- HackThisSite - CTF write-ups repo maintained by HackThisSite team.
- Mzfr - CTF competition write-ups by mzfr
- pwntools writeups - A collection of CTF write-ups all using pwntools.
- SababaSec - A collection of CTF write-ups by the SababaSec team
- Shell Storm - CTF challenge archive maintained by Jonathan Salwan.
- Smoke Leet Everyday - CTF write-ups repo maintained by SmokeLeetEveryday team.

How to use search engines

Keywords to explore

- tips - ex: exploit tips php / exploit tips java / exploit tips python
- tricks
- cheatsheet - ex: php security cheatsheet
- checklist - ex: php security checklist
- bypass - ex: bypass WAF / bypass sql injection prevention
- vulnerability database - find known vulnerabilities related to challenge's runtime
- Feature Keywords in CTF challenges - find known or similar challenges and writeups

Common search techniques

Search social media

Put in front of a word to search social media. For example: twitter.

Search for a price

Put $ in front of a number. For example: camera $400.

Search hashtags

Put # in front of a word. For example: #throwbackthursday

Exclude words from your search

Put - in front of a word you want to leave out. For example, jaguar speed -car

Common search techniques

Search for an exact match

Put a word or phrase inside quotes. For example, "tallest building".

Search within a range of numbers

Put .. between two numbers. For example, camera $50..$100.

Combine searches

Put "OR" between each search query. For example, marathon OR race.

Common search techniques

Search for a specific site

Put "site:" in front of a site or domain. For example, site:youtube.com or site:.gov.

Search for related sites

Put "related:" in front of a web address you already know. For example, related:time.com.

See Google's cached version of a site

Put "cache:" in front of the site address.

Important: Not all search operators return exhaustive results.

Related books

https://stackoverflow.com/questions/1711/what-is-the-single-most-influential-book-every-programmer-should-read/1713%231713

If you could go back in time and tell yourself to read a specific book at the beginning of your career as a developer, which book would it be?

I expect this list to be varied and to cover a wide range of things.

To search: Use the search box in the upper-right corner. To search the answers of the current question, use inquestion:this. For example:

inquestion:this "Code Complete"

Related books

https://github.com/EbookFoundation/free-programming-books

This list was originally a clone of StackOverflow - List of Freely Available Programming Books with contributions from Karan Bhangui and George Stocker.

The list was moved to GitHub by Victor Felder for collaborative updating and maintenance. It has grown to become one of GitHub's most popular repositories, with 200,000+ stars, 6100+ commits, 1600+ contributors, and 43,000+ forks.

The Free Ebook Foundation now administers the repo, a not-for-profit organization devoted to promoting the creation, distribution, archiving, and sustainability of free ebooks. Donations to the Free Ebook Foundation are tax-deductible in the US.

Related books

https://github.com/justjavac/free-programming-books-zh_CN

Chinese version of programming books recommend.

Summary

Topics that we covered:

- CTF introduction
- Categories
- Tools and resources to CTF
- How to use search engines
- Related books

That's a lot of things, make sure you review today's contents.

Summary

The time schedule of CTF team can be access:

https://wiki.compass.college/Tutorial/Schedule/2022Summer/

Now we are under a training process of 2 months and don't upset if you feel it's confusing today. And we are not yet ask you to master anything today.

Also, you can use our platform to solve challenges:

https://compass.ctfd.io/

How to join COMPASS CTF team?

We do have some grading principles related to following:

- Evaluation of the weekly challenges, and competitions: 30%.
- Remark from the team members: 10%.
- The sharing and the report score: 15%.
- The final exam: 100%.

Glad to have you in CTF team!

Summary

What you should do today:

1. Try to use some Linux distribution, or try some codes on the VPS.
2. Connect to Google, and search something related to the CTF.
3. Write some Python codes.
4. Talk with your teammate.