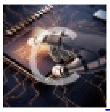
CTF比赛中必备的瑞士军刀ctf-tools

转载

不改长流 于 2016-06-26 17:37:07 发布 13736 收藏 11
分类专栏： CTF 文章标签： CTF 安全


CTF 专栏收录该内容
6 篇文章 0 订阅
订阅专栏

---

ctf-tools

CTF：全称Capture The Flag，即夺旗比赛，衍生自古代军事战争模式，两队人马前往对方基地夺旗，每队人马须在保护好己方旗帜的情况下将对方旗帜带回基地。ctf-tools 集合了很多黑客ctf大赛中需要使用的工具。

下载地址
官方主页

ctf-tools是一个集合了各种安全研究工具的管理脚本，使得大家能够一键轻松的安装并使用这些工具，目前覆盖的列表包括：

Category	Tool	Description
binary	afl	State-of-the-art fuzzer.
binary	barf	Binary Analysis and Reverse-engineering Framework.
binary	bindead	A static analysis tool for binaries.
binary	checksec	Check binary hardening settings.
binary	crosstool-ng	Cross-compilers and cross-architecture tools.
binary	gdb	Up-to-date gdb with python2 bindings.
binary	peda	Enhanced environment for gdb.
binary	preeny	A collection of helpful preloads (compiled for many architectures!).
binary	villoc	Visualization of heap operations.
binary	qemu	Latest version of qemu!
binary	pwntools	Useful CTF utilities.
binary	python-pin	Python bindings for pin.
binary	radare2	Some crazy thing crowell likes.
binary	shellnoob	Shellcode writing helper.
binary	taintgrind	A valgrind taint analysis tool.

Category	Tool	Description
binary	qira	Parallel, timeless debugger.
binary	xrop	Gadget finder.
binary	rp++	Another gadget finder.
forensics	binwalk	Firmware (and arbitrary file) analysis tool.
forensics	dislocker	Tool for reading Bitlocker encrypted partitions.
forensics	firmware-mod-kit	Tools for firmware packing/unpacking.
forensics	testdisk	Testdisk and photorec for file recovery.
forensics	pdf-parser	Tool for digging in PDF files
crypto	cribdrag	Interactive crib dragging tool (for crypto).
crypto	hashpump	A tool for performing hash length extension attaacks.
crypto	hashpump-partialhash	Hashpump, supporting partially-unknown hashes.
crypto	hash-identifier	Simple hash algorithm identifier.
crypto	littleblackbox	Database of private SSL/SSH keys for embedded devices.
crypto	pemcrack	SSL PEM file cracker.
crypto	reveng	CRC finder.
crypto	sslsplit	SSL/TLS MITM.
crypto	python-paddingoracle	Padding oracle attack automation.
crypto	xortool	XOR analysis tool.
web	burp	Web proxy to do naughty web stuff.
web	dirs3arch	Web path scanner.
web	sqlmap	SQL injection automation engine.
stego	sound-visualizer	Audio file visualization.
stego	stegdetect	Steganography detection/breaking tool.
stego	steganabara	Antoher image steganography solver.
stego	stegsolve	Image steganography solver.
android	APKTool	Dissect, dis-assemble, and re-pack Android APKs

也带了一些不是ctf相关工具的小彩蛋，哈哈

Category	Tool	Description
game	Dwarf Fortress	Something to help you relax after a CTF!

下载

```
[root@localhost software]# git clone https://github.com/zardus/ctf-tools.git
```

用法

```
# set up the path
/path/to/ctf-tools/bin/manage-tools setup
source ~/.bashrc

# list the available tools
manage-tools list

# install gdb, allowing it to try to sudo install dependencies
manage-tools -s install gdb

# install pwntools, but don't let it sudo install dependencies
manage-tools install pwntools

# uninstall gdb
manage-tools uninstall gdb

# uninstall all tools
manage-tools uninstall all
```

新增工具

```
1. 创建一个`工具名称`的目录
2. 创建一个`install`的安装脚本
3. 如果需要特殊的卸载步骤，还要创建一个`uninstall`的脚本，用来卸载
```

原文地址: http://www.codefrom.com/c/43

转载自http://www.tasfa.cn/index.php/2016/01/29/ctf-tools-2/