carpedm20 / **awesome-hacking**

Watch 336 | Star 3,726 | Fork 642

<> Code | Issues 5 | Pull requests 3 | Projects 0 | Insights

Join GitHub today

GitHub is home to over 20 million developers working together to host and review code, manage projects, and build software together.

Sign up

Dismiss

A curated list of awesome Hacking tutorials, tools and resources

awesome hacking

91 commits | **1** branch | **0** releases | **32** contributors | MIT

Branch: **master** | New pull request | Find file | Clone or download

carpedm20 Merge pull request #45 from atrestis/master …		Latest commit `212bf65` on Mar 30
LICENSE	First commit	3 years ago

README.md	Added Hack The Box site in Web section	a month ago
books.md	reformat and add sources	3 years ago

README.md

Awesome Hacking awesome

A curated list of awesome Hacking. Inspired by awesome-machine-learning

If you want to contribute to this list (please do), send me a pull request or contact me @carpedm20

For a list of free hacking books available for download, go here

Table of Contents

System

Tutorials

- Corelan Team's Exploit writing tutorial
- Exploit Writing Tutorials for Pentesters

Tools

- Metasploit A computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development.
- mimikatz - A little tool to play with Windows security

Docker Images for Penetration Testing & Security

- `docker pull kalilinux/kali-linux-docker` official Kali Linux
- `docker pull owasp/zap2docker-stable` - official OWASP ZAP
- `docker pull wpscanteam/wpscan` - official WPScan
- `docker pull pandrew/metasploit` - docker-metasploit
- `docker pull citizenstig/dvwa` - Damn Vulnerable Web Application (DVWA)
- `docker pull wpscanteam/vulnerablewordpress` - Vulnerable WordPress Installation
- `docker pull hmlio/vaas-cve-2014-6271` - Vulnerability as a service: Shellshock
- `docker pull hmlio/vaas-cve-2014-0160` - Vulnerability as a service: Heartbleed
- `docker pull opendns/security-ninjas` - Security Ninjas
- `docker pull usertaken/archlinux-pentest-lxde` - Arch Linux Penetration Tester

- `docker pull diogomonica/docker-bench-security` - Docker Bench for Security
- `docker pull ismisepaul/securityshepherd` - OWASP Security Shepherd
- `docker pull danmx/docker-owasp-webgoat` - OWASP WebGoat Project docker image
- `docker-compose build && docker-compose up` - OWASP NodeGoat
- `docker pull citizenstig/nowasp` - OWASP Mutillidae II Web Pen-Test Practice Application
- `docker pull bkimminich/juice-shop` - OWASP Juice Shop

General

- Exploit database - An ultimate archive of exploits and vulnerable software

Reverse Engineering

Tutorials

- Lenas Reversing for Newbies
- Malware Analysis Tutorials: a Reverse Engineering Approach

Tools

- nudge4j - Java tool to let the browser talk to the JVM
- IDA - IDA is a Windows, Linux or Mac OS X hosted multi-processor disassembler and debugger
- OllyDbg - A 32-bit assembler level analysing debugger for Windows
- x64dbg - An open-source x64/x32 debugger for Windows

- dex2jar - Tools to work with Android .dex and Java .class files
- JD-GUI - A standalone graphical utility that displays Java source codes of “.class” files
- procyon - A modern open-source Java decompiler
- androguard - Reverse engineering, malware and goodware analysis of Android applications
- JAD - JAD Java Decompiler (closed-source, unmaintained)
- dotPeek - a free-of-charge .NET decompiler from JetBrains
- ILSpy - an open-source .NET assembly browser and decompiler
- dnSpy - .NET assembly editor, decompiler, and debugger
- de4dot - .NET deobfuscator and unpacker.
- antinet - .NET anti-managed debugger and anti-profiler code
- UPX - the Ultimate Packer for eXecutables
- radare2 - A portable reversing framework
- plasma - Interactive disassembler for x86/ARM/MIPS. Generates indented pseudo-code with colored syntax code.
- Hopper - A OS X and Linux Disassembler/Decompiler for 32/64-bit Windows/Mac/Linux/iOS executables.
- ScratchABit - Easily retargetable and hackable interactive disassembler with IDAPython-compatible plugin API

General

- Open Malware

Web

Tools

- sqlmap - Automatic SQL injection and database takeover tool
- tools.web-max.ca - base64 base85 md4,5 hash, sha1 hash encoding/decoding

Network

Tools

- Wireshark - A free and open-source packet analyzer
- NetworkMiner - A Network Forensic Analysis Tool (NFAT)
- tcpdump - A powerful command-line packet analyzer; and libpcap, a portable C/C++ library for network traffic capture
- Paros - A Java-based HTTP/HTTPS proxy for assessing web application vulnerability
- pig - A Linux packet crafting tool
- ZAP - The Zed Attack Proxy (ZAP) is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications
- mitmproxy - An interactive, SSL-capable man-in-the-middle proxy for HTTP with a console interface
- mitmsocks4j - Man-in-the-middle SOCKS Proxy for Java
- nmap - Nmap (Network Mapper) is a security scanner
- Aircrack-ng - An 802.11 WEP and WPA-PSK keys cracking program
- Charles Proxy - A cross-platform GUI web debugging proxy to view intercepted HTTP and HTTPS/SSL live traffic
- Nipe - A script to make Tor Network your default gateway.
- Habu - Python Network Hacking Toolkit
- Wifi Jammer - Free program to jam all wifi clients in range
- Firesheep - Free program for HTTP session hijacking attacks.
- Scapy - A Python tool and library for low level packet creation and manipputalion

Forensic

Tools

- Autospy - A digital forensics platform and graphical interface to The Sleuth Kit and other digital forensics tools
- sleuthkit - A library and collection of command-line digital forensics tools
- EnCase - The shared technology within a suite of digital investigations products by Guidance Software
- malzilla - Malware hunting tool
- PEview - A quick and easy way to view the structure and content of 32-bit Portable Executable (PE) and Component Object File Format (COFF) files
- HxD - A hex editor which, additionally to raw disk editing and modifying of main memory (RAM), handles files of any size
- WinHex - A hexadecimal editor, helpful in the realm of computer forensics, data recovery, low-level data processing, and IT security
- BinText - A small, very fast and powerful text extractor that will be of particular interest to programmers

Cryptography

Tools

- xortool - A tool to analyze multi-byte XOR cipher
- John the Ripper - A fast password cracker
- Aircrack - Aircrack is 802.11 WEP and WPA-PSK keys cracking program.

Wargame

System

- OverTheWire - Semtex
- OverTheWire - Vortex
- OverTheWire - Drifter
- pwnable.kr - Provide various pwn challenges regarding system security
- Exploit Exercises - Nebula
- SmashTheStack

Reverse Engineering

- Reversing.kr - This site tests your ability to Cracking & Reverse Code Engineering
- CodeEngn - (Korean)
- simples.kr - (Korean)
- Crackmes.de - The world first and largest community website for crackmes and reversemes.

Web

- Hack This Site! - a free, safe and legal training ground for hackers to test and expand their hacking skills
- Hack The Box - a free site to perform pentesting in a variety of different systems.
- Webhacking.kr
- 0xf.at - a website without logins or ads where you can solve password-riddles (so called hackits).

Cryptography

- OverTheWire - Krypton

Bug bounty

- Awsome bug bounty resourses by Edoverflow

CTF

Competition

- DEF CON
- CSAW CTF
- hack.lu CTF
- Pliad CTF
- RuCTFe
- Ghost in the Shellcode
- PHD CTF
- SECUINSIDE CTF
- Codegate CTF
- Boston Key Party CTF

General

- Hack+ - An Intelligent network of bots that fetch the latest InfoSec content.
- CTFtime.org - All about CTF (Capture The Flag)
- WeChall
- CTF archives (shell-storm)
- Rookit Arsenal - OS RE and rootkit development
- Pentest Cheat Sheets - Collection of cheat sheets useful for pentesting
- Movies For Hacker - A curated list of movies every hacker & cyberpunk must watch.

OS

Online resources

- Security related Operating Systems @ Rawsec - Complete list of security related operating systems
- Best Linux Penetration Testing Distributions @ CyberPunk - Description of main penetration testing distributions
- Security @ Distrowatch - Website dedicated to talking about, reviewing and keeping up to date with open source operating systems

ETC

- SecTools - Top 125 Network Security Tools