



Features Business Explore Marketplace Pricing

This repository Search

Sign in or Sign up

vitalysim / **Awesome-Hacking-Resources**

Watch

421

★ Star

6,885

🍴 Fork

767

<> Code

🔔 Issues 1

🔗 Pull requests 0

📁 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 collection of hacking / penetration testing resources to make you better!

ctf

hacking

privilege-escalation

reverse-engineering

buffer-overflow

penetration-testing

owasp

exploit

malware

windows-privilege-escalation

privilege-escalation-linux

mitm

📦 190 commits

🌿 1 branch

📦 0 releases

👥 37 contributors

📄 GPL-3.0

Branch: master ▾

New pull request





Find file

Clone or download ▾



vitalysim Merge pull request #90 from dooley1001/master ...

Latest commit 86e826e on Mar 19

 LICENSE	Initial commit	7 months ago
 README.md	Update README.md	2 months ago
 contributing.md	Added Lena's tutorials and a few tools such as BinNavi	7 months ago
 tools.md	Updated tools.md	2 months ago

README.md



Awesome Hacking Resources

awesome **hacking**

awesome **community**

A collection of hacking / penetration testing resources to make you better!

Let's make it the biggest resource repository for our community.

You are welcome to fork and [contribute](#).

We started a new [tools](#) list, come and contribute

Table of Contents

- [Learning the Skills](#)
- [YouTube Channels](#)
 - [Companies](#)
 - [Conferences](#)
 - [NEWS](#)
- [Sharpening Your Skills](#)
- [Reverse Engineering, Buffer Overflow and Exploit Development](#)
- [Privilege Escalation](#)
- [Network Scanning / Reconnaissance](#)
- [Malware Analysis](#)
- [Vulnerable Web Application](#)
- [Vulnerable OS](#)
- [Exploits](#)
- [Forums](#)
- [Archived Security Conference Videos](#)
- [Online Communities](#)
- [Online News Sources](#)
- [Linux Penetration Testing OS](#)

Learning the Skills

Name	Description
------	-------------

Name	Description
Free interactive labs with White Hat Academy	32 labs, easy account sign in with github credentials
Learning Exploitation with Offensive Computer Security 2.0	blog-style instruction, includes: slides, videos, homework, discussion. No login required.
Cybrary	coursera style website, lots of user-contributed content, account required, content can be filtered by experience level
OffensiveComputerSecurity	academic content, full semester course including 27 lecture videos with slides and assign readings
CS 642: Intro to Computer Security	academic content, full semester course, includes assigned readings, homework and github refs for exploit examples. NO VIDEO LECTURES.
Free cyber security training	Academic content, 8 full courses with videos from a quirky instructor sam, links to research, defcon materials and other recommended training/learning
SecurityTube	tube-styled content, "megaprimer" videos covering various topics, no readable content on site.
Seed Labs	academic content, well organized, featuring lab videos, tasks, needed code files, and recommended readings
Hak5	podcast-style videos covering various topics, has a forum, "metasploit-minute" video series could be useful
Mind Maps	Information Security related Mind Maps

Name	Description
OWASP top 10 web security risks	free courseware, requires account
MIT OCW 6.858 Computer Systems Security	academic content, well organized, full-semester course, includes assigned readings, lectures, videos, required lab files.

YouTube Channels

Name	Description
OWASP	see OWASP above
Hak5	see Hak5 above
BlackHat	features talks from the BlackHat conferences around the world
Christiaan008	hosts a variety of videos on various security topics, disorganized
	Companies
0patch by ACROS Security	few videos, very short, specific to 0patch
Detectify	very short videos, aimed at showing how to use Detictify scanner
Kaspersky Lab	lots of Kaspersky promos, some hidden cybersecurity gems
Metasploit	collection of medium length metasploit demos, ~25minutes each, instructional
OpenNSM	network analysis, lots of TCPDUMP videos, instructional,
Rapid7	brief videos, promotional/instructional, ~ 5 minutes

Name	Description
Securelist	brief videos, interviews discussing various cyber security topics
Segment Security	promo videos, non-instructional
SocialEngineerOrg	podcast-style, instructional, lengthy content ~1 hr each
Sonatype	lots of random videos, a good cluster of DevOps related content, large range of lengths, disorganized
SophosLabs	lots of brief, news-style content, "7 Deadly IT Sins" segment is of note
Sourcefire	lots of brief videos covering topics like botnets, DDoS ~5 minutes each
Station X	handful of brief videos, disorganized, unscheduled content updates
Synack	random, news-style videos, disorganized, non-instructional
TippingPoint Zero Day Initiative	very brief videos ~30 sec, somewhat instructional
Tripwire, Inc.	some tripwire demos, and random news-style videos, non-instructional
Vincent Yiu	handful of videos from a single hacker, instructional
nVisium	Some nVisum promos, a handful of instructional series on Rails vulns and web hacking
ntop	network monitoring, packet analysis, instructional
	Conferences
44contv	information security con based in London, lengthy instructional videos

Name	Description
BruCON Security Conference	security and hacker conference based in Belgium, lots of lengthy instructional videos
BSides Manchester	security and hacker con based in Manchester, lots of lengthy videos
BSidesAugusta	security con based in Augusta, Georgia, lots of lengthy instructional videos
CarolinaCon	security con based in North Carolina, associated with various 2600 chapters, lots of lengthy instructional content
Cort Johnson	a handful of lengthy con-style talks from Hack Secure Opensec 2017
DevSecCon	lengthy con videos covering DevSecOps, making software more secure
Garage4Hackers - Information Security	a handful of lengthy videos, About section lacks description
HACKADAY	lots of random tech content, not strictly infosec, some instructional
Hack In The Box Security Conference	lengthy con-style instructional talks from an international security con
Hack in Paris	security con based in paris, features lots of instructional talks, slides can be difficult to see.
Hacklu	lots of lengthy con-style instructional videos
Hacktivity	lots of lengthy con-style instructional videos from a con in central/eastern europe
Hardwear.io	handful of lengthy con-style video, emphasis on hardware hacks

Name	Description
IEEE Symposium on Security and Privacy	content from the symposium; IEEE is a professional association based in the us, they also publish various journals
LASCON	lengthy con-style talks from an OWASP con held in Austin, TX
Marcus Niemietz	lots of instructional content, associated with HACKPRA, an offensive security course from an institute in Germany
Media.ccc.de	The real official channel of the chaos computer club, operated by the CCC VOC - tons of lengthy con-style vids
NorthSec	lengthy con-style talks from an applied security conference in Canada
Pancake Nopcode	channel of Radare2 whiz Sergi "pancake" Alvarez, Reverse Engineering Content
Psiinon	medium length instructional videos, for the OWASP Zed Attack Proxy
SJSU Infosec	handful of lengthy instructional videos from San Jose State university Infosec
Secappdev.org	tons of lengthy instructional lectures on Secure App Development
Security Fest	medium length con-style talks from a security festival in Sweden
SecurityTubeCons	an assortment of con-style talks from various cons including BlackHat and Shmoocon
ToorCon	handful of medium length con videos from con based in San Diego, CA
USENIX Enigma Conference	medium length "round table discussion with leading experts", content starts in 2016
	News

Name	Description
Corey Nachreiner	security newsbites, 2.7K subscribers, 2-3 videos a week, no set schedule
Error 404 Cyber News	short screen-shot videos with loud metal, no dialog, bi-weekly
Latest Hacking News	10K followers, medium length screenshot videos, no recent releases
Pentester Academy TV	lots of brief videos, very regular posting, up to +8 a week
SecureNinjaTV	brief news bites, irregular posting, 18K followers
Troy Hunt	lone youtuber, medium length news videos, 16K followers, regular content
Samy Kamkar's Applied Hacking	brief to medium length instructional vids from the creator of PoisonTap for the Raspberry Pi Zero, no recent content, last updated in 2016
danooct1	lots of brief screenshot, how-to vids regarding malware, regular content updates, 186K followers
DedSec	lots of brief screenshot how-to vids based in Kali, no recent posts.
DEFCON Conference	lots of lengthy con-style vids from the iconic DEFCON
DemmSec	lots of pen testing vids, somewhat irregular uploads, 44K followers
Don Does 30	amateur pen-tester posting lots of brief screenshot vids regularly, 9K Followers
Geeks Fort - KIF	lots of brief screenshot vids, no recent posts
iExplo1t	lots of screenshot vids aimed at novices, 5.7K Followers, no recent posts
HACKING TUTORIALS	handful of brief screenshot vids, no recent posts.

Name	Description
LiveOverflow	Lots of brief-to-medium instructional vids, covering things like buffer overflows and exploit writing, regular posts.
Metasploitation	lots of screenshot vids, little to no dialogue, all about using Metasploit, no recent vids.
NetSecNow	channel of pentesteruniversity.org, seems to post once a month, screenshot instructional vids
Open SecurityTraining	lots of lengthy lecture-style vids, no recent posts, but quality info.
BalCCon - Balkan Computer Congress	Long con-style talks from the Balkan Computer Congress, doesn't update regularly
Penetration Testing in Linux	DELETE
rwbnetsec	lots of medium length instructional videos covering tools from Kali 2.0, no recent posts.
Security Weekly	regular updates, lengthy podcast-style interviews with industry pros
Seytonic	variety of DIY hacking tutorials, hardware hacks, regular updates
Shozab Haxor	lots of screenshot style instructional vids, regular updates, windows CLI tutorial
SSTec Tutorials	lots of brief screenshot vids, regular updates
Waleed Jutt	lots of brief screenshot vids covering web security and game programming
webpwnized	lots of brief screenshot vids, some CTF walkthroughs
JackkTutorials	lots of medium length instructional vids with some AskMe vids from the youtuber

Name	Description
Zer0Mem0ry	lots of brief c++ security videos, programming intensive
LionSec	lots of brief screenshot instructional vids, no dialog
Adrian Crenshaw	lots of lengthy con-style talks
HackerSploit	regular posts, medium length screenshot vids, with dialog
Derek Rook - CTF/Boot2root/wargames Walkthrough	lots of lengthy screenshot instructional vids, with

Sharpening Your Skills

Name	Description
OWASP Security Shepherd	BROKEN AS OF 11/6
CTFLearn	an account-based ctf site, where users can go in and solve a range of challenges
CTFs write-ups	a collection of writeups from various CTFs, organized by
CTF365	account based ctf site, awarded by Kaspersky, MIT, T-Mobile
Pentestit	acocunt based CTF site, users have to install open VPN and get credentials
Hacksplaining	a clickthrough security informational site, very good for beginners.
The cryptopals crypto challenges	A bunch of CTF challenges, all focused on cryptography.

Name	Description
The enigma group	web application security training, account based, video tutorials
Ringzer0 Team	an account based CTF site, hosting over 272 challenges
Hack The Box	Pen testing labs hosting over 39 vulnerable machines with two additional added every month
Over the wire	A CTF that's based on progressive levels for each lab, the users SSH in, no account required
Backdoor	pen testing labs that have a space for beginners, a practice arena and various competitions, account required
Vulnhub	site hosts a ton of different vulnerable Virtual Machine images, download and get hacking
Hack.me	lets you build/host/attack vulnerable web apps
Hack this site!	an oldy but goodie, account required, users start at low levels and progress in difficulty
Exploit exercises	hosts 5 vulnerable virtual machines for you to attack, no account required
PentesterLab	hosts a variety of exercises as well as various "bootcamps" focused on specific activities
SmashTheStack	hosts various challenges, similar to OverTheWire, users must SSH into the machines and progress in levels
PicoCTF	CTF hosted by Carnegie Mellon, occurs yearly, account required.
Shellter Labs	account based infosec labs, they aim at making these activities social
Pentest Practice	account based Pentest practice, free to sign up, but there's also a pay-as-you-go feature

Name	Description
Pentest.training	lots of various labs/VMS for you to try and hack, registry is optional.
pwnable.kr	Don't let the cartoon characters fool you, this is a serious CTF site that will teach you a lot, account required
pwnable.tw	hosts 27 challenges accompanied with writeups, account required
hackburger.ee	hosts a number of web hacking challenges, account required
http://noe.systems/	Korean challenge site, requires an account
Hacker Gateway	ctfs covering steganography, cryptography, and web challenges, account required
Solve Me	"yet another challenge", account required.
Challenge Land	Ctf site with a twist, no simple sign-up, you have to solve a challenge to even get that far!
Participating Challenge Sites	aims at creating a universal ranking for CTF participants
Hacker test	similar to "hackthissite", no account required.
Crackmes.de Archive (2011-2015)	a reverse engineering information Repo, started in 2003
ROP Emporium	Return Oriented Programming challenges
Google's XSS game	XSS challenges, and potentially a chance to get paid!

Reverse Engineering, Buffer Overflow and Exploit Development

Name	Description
Shell storm	Blog style collection with organized info about Rev. Engineering.
Buffer Overflow Exploitation Megaprimer for Linux	Collection of Linux Rev. Engineering videos
Reverse Engineering Malware 101	intro course created by Malware Unicorn, complete with material and two VM's
Reverse Engineering Malware 102	the sequel to RE101
Modern Binary Exploitation - CSCI 4968	RE challenges, you can download the files or download the VM created by RPISEC specifically for challenges, also links to their home page with tons of infosec lectures
Introductory Intel x86	63 days of OS class materials, 29 classes, 24 instructors, no account required
Binary hacking	35 "no bullshit" binary videos along with other info
Shellcode Injection	a blog entry from a grad student at SDS Labs
Reverse Engineering for Beginners	huge textbook, created by Dennis Yurichev, open-source
Exploit tutorials	a series of 9 exploit tutorials,also features a podcast
Exploit development	links to the forum's exploit dev posts, quality and post style will vary with each poster
f1AWS challenge	Through a series of levels you'll learn about common mistakes and gotchas when using Amazon Web Services (AWS).

Name	Description
Corelan tutorials	detailed tutorial, lots of good information about memory
Reverse engineering reading list	a github collection of RE tools and books
Reverse Engineering challenges	collection of challenges from the writer of RE for Beginners
Reverse Engineering for beginners (GitHub project)	github for the above
reversing.kr challenges	reverse engineering challenges varying in difficulty
Analysis and exploitation (unprivileged)	huge collection of RE information, organized by type.
A Course on Intermediate Level Linux Exploitation	as the title says, this course isn't for beginners
Lena's Reversing for Newbies (Complete)	listing of a lengthy resource by Lena, aimed at being a course
Megabeets journey into Radare2	one user's radare2 tutorials
Introduction to ARM Assembly Basics	tons of tutorials from infosec pro Azeria, follow her on twitter
Linux (x86) Exploit Development Series	blog post by sploitfun, has 3 different levels

Privilege Escalation

Name	Description
Reach the root	discusses a process for linux privilege exploitation
Basic linux privilege escalation	basic linux exploitation, also covers Windows
Windows Privilege Escalation	collection of wiki pages covering Windows Privilege escalation
Privilege escalation for Windows and Linux	covers a couple different exploits for Windows and Linux
Windows Privilege Escalation Fundamentals	collection of great info/tutorials, option to contribute to the creator through patreon, creator is an OSCP
RootHelper	a tool that runs various enumeration scripts to check for privilege escalation
Windows exploits, mostly precompiled.	precompiled windows exploits, could be useful for reverse engineering too
Unix privesc checker	a script that checks for PE vulnerabilities on a system
Privilege escalation linux with live example	covers a couple common PE methods in linux
Windows privilege escalation checker	a list of topics that link to pentestlab.blog, all related to windows privilege escalation
Linux Privilege Escalation Scripts	a list of PE checking scripts, some may have already been covered
AutoLocalPrivilegeEscalation	automated scripts that downloads and compiles from exploitdb
Linux Privilege Escalation Check Script	a simple linux PE check script

Name	Description
Local Linux Enumeration & Privilege Escalation Cheatsheet	good resources that could be compiled into a script
4 Ways get linux privilege escalation	shows different examples of PE

Malware Analysis

Name	Description
Malware traffic analysis	list of traffic analysis exercises
Malware Analysis - CSCI 4976	another class from the folks at RPISEC, quality content

Network Scanning / Reconnaissance

Name	Description
Foot Printing with WhoIS/DNS records	a white paper from SANS
Google Dorks/Google Hacking	list of commands for google hacks, unleash the power of the world's biggest search engine

Vulnerable Web Application

Name	Description
OWASP Hackademic Challenges project	web hacking challenges

Name	Description
bWAPP	common buggy web app for hacking, great for beginners, lots of documentation
Damn Vulnerable Web Application (DVWA)	PHP/MySQL web app for testing skills and tools
WebGoat: A deliberately insecure Web Application	maintained by OWASP and designed to to teach web app security
OWASP Mutillidae II	another OWASP vulnerable app, lots of documentation.
OWASP Broken Web Applications Project	hosts a collection of broken web apps
Damn Small Vulnerable Web	written in less than 100 lines of code, this web app has tons of vulns, great for teaching
OWASP Juice Shop	covers the OWASP top 10 vulns
Google Gruyere	host of challenges on this cheesy web app

Vulnerable OS

Name	Description
Metasploitable2 (Linux)	vulnerable OS, great for practicing hacking
Metasploitable3 [Installation]	the third installation of this vulnerable OS
Vulnhub	collection of tons of different vulnerable OS and challenges

Name	Description
General Test Environment Guidance	white paper from the pros at rapid7

Linux Penetration Testing OS

Name	Description
BackBox	open source community project, promoting security in IT environments
BlackArch	Arch Linux based pentesting distro, compatible with Arch installs
Kali	the infamous pentesting distro from the folks at Offensive Security
LionSec Linux	pentesting OS based on Ubuntu
Parrot	Debian includes full portable lab for security, DFIR, and development
Bugtraq	advanced GNU Linux pen-testing technology
Android Tamer	Android Tamer is a Virtual / Live Platform for Android Security professionals.

Exploits

Name	Description
Exploit Database	database of a wide variety exploits, CVE compliant archive
CXsecurity	Indie cybersecurity info managed by 1 person
0day.today	Easy to navigate database of exploits

Name	Description
Snyk Vulnerability DB	detailed info and remediation guidance for known vulns, also allows you to test your code

Forums

Name	Description
Greysec	hacking and security forum
Hackforums	posting webstite for hacks/exploits/various discussion
0x00sec	hacker, malware, computer engineering, Reverse engineering
Antichat	russian based forum
EAST Exploit database	exploit DB for commercial exploits written for EAST Pentest Framework

Archived Security Conference Videos

Name	Description
InfoCon.org	hosts data from hundreds of cons
Irongeek	Website of Adrien Crenshaw, hosts a ton of info.

Online Communities

Name	Description
Hack+	link requires telegram to be used

Name	Description
MPGH	community of MultiPlayerGameHacking
Hacktoday	requires an account, covering all kinds of hacking topics

Online News Sources

Name	Description
Recent Hash Leaks	great place to lookup hashes
InfoSec	covers all the latest infosec topics
Threatpost	covers all the latest threats and breaches
Security Intell	covers all kinds of news, great intelligence resources
The Hacker News	features a daily stream of hack news, also has an app

