A collection of awesome penetration testing resources

Online Resources

Penetration Testing Resources

- Metasploit Unleashed - Free Offensive Security metasploit course
- PTES - Penetration Testing Execution Standard
- OWASP - Open Web Application Security Project

Exploit development

- Shellcode Tutorial - Tutorial on how to write shellcode
- Shellcode Examples - Shellcodes database
- Exploit Writing Tutorials - Tutorials on how to develop exploits
- GDB-peda - Python Exploit Development Assistance for GDB
- shellsploit - New Generation Exploit Development Kit

Social Engineering Resources

- Social Engineering Framework - An information resource for social engineers

Lock Picking Resources

- Schuyler Towne channel - Lockpicking videos and security talks
- /r/lockpicking - Resources for learning lockpicking, equipment

recommendations.

Tools

Penetration Testing Distributions

- Kali - A Linux distribution designed for digital forensics and penetration testing
- BlackArch - Arch Linux-based distribution for penetration testers and security researchers
- NST - Network Security Toolkit distribution
- Pentoo - security-focused livecd based on Gentoo
- BackBox - Ubuntu-based distribution for penetration tests and security assessments
- Parrot - A distribution similar to Kali, with multiple architecture

Basic Penetration Testing Tools

- Metasploit Framework - World's most used penetration testing software
- Burp Suite - An integrated platform for performing security testing of web applications
- ExploitPack - Graphical tool for penetration testing with a bunch of exploits
- BeeF - The Browser Exploitation Framework Project
- faraday - Collaborative Penetration Test and Vulnerability Management Platform
- evilgrade - The update explotation framework
- commix - Automated All-in-One OS Command Injection and Exploitation Tool
- routersploit - Automated penetration testing software for router

Docker for Penetration Testing

- `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 pull citizenstig/nowasp` - OWASP Mutillidae II Web Pen-Test Practice Application

Vulnerability Scanners

- Netsparker - Web Application Security Scanner
- Nexpose - Vulnerability Management & Risk Management Software
- Nessus - Vulnerability, configuration, and compliance assessment
- Nikto - Web application vulnerability scanner
- OpenVAS - Open Source vulnerability scanner and manager
- OWASP Zed Attack Proxy - Penetration testing tool for web applications
- Secapps - Integrated web application security testing

environment

- w3af - Web application attack and audit framework
- Wapiti - Web application vulnerability scanner
- WebReaver - Web application vulnerability scanner for Mac OS X
- DVCS Ripper - Rip web accessible (distributed) version control systems: SVN/GIT/HG/BZR
- arachni - Web Application Security Scanner Framework

Network Tools

- nmap - Free Security Scanner For Network Exploration & Security Audits
- pig - A Linux packet crafting tool
- tcpdump/libpcap - A common packet analyzer that runs under the command line
- Wireshark - A network protocol analyzer for Unix and Windows
- Network Tools - Different network tools: ping, lookup, whois, etc
- netsniff-ng - A Swiss army knife for for network sniffing
- Intercepter-NG - a multifunctional network toolkit
- SPARTA - Network Infrastructure Penetration Testing Tool
- DNSDumpster - Online DNS recond and search service
- Mass Scan - TCP port scanner, spews SYN packets asynchronously, scanning entire Internet in under 5 minutes.
- Zarp - Zarp is a network attack tool centered around the exploitation of local networks
- mitmproxy - An interactive SSL-capable intercepting HTTP proxy for penetration testers and software developers
- mallory - HTTP/HTTPS proxy over SSH
- DET - DET is a proof of concept to perform Data Exfiltration using either single or multiple channel(s) at the same time
- pwnat - punches holes in firewalls and NATs
- dsniff - a collection of tools for network auditing and pentesting
- tgcd - a simple Unix network utility to extend the accessibility of TCP/IP based network services beyond firewalls

- smbmap - a handy SMB enumeration tool
- scapy - a python-based interactive packet manipulation program & library

Wireless Network Tools

- Aircrack-ng - a set of tools for auditing wireless network
- Kismet - Wireless network detector, sniffer, and IDS
- Reaver - Brute force attack against Wifi Protected Setup
- Wifite - Automated wireless attack tool
- wifiphisher - Automated phishing attacks against Wi-Fi networks

SSL Analysis Tools

- SSLyze - SSL configuration scanner
- sslstrip - a demonstration of the HTTPS stripping attacks
- sslstrip2 - SSLStrip version to defeat HSTS
- tls_prober - fingerprint a server's SSL/TLS implementation

Web exploitation

- WPScan - Black box WordPress vulnerability scanner
- SQLmap - Automatic SQL injection and database takeover tool
- weevely3 - Weaponized web shell
- Wappalyzer - Wappalyzer uncovers the technologies used on websites
- cms-explorer - CMS Explorer is designed to reveal the the specific modules, plugins, components and themes that various CMS driven web sites are running.
- joomscan - Joomla CMS scanner
- WhatWeb - Website Fingerprinter
- BlindElephant - Web Application Fingerprinter

Hex Editors

- HexEdit.js - Browser-based hex editing
- Hexinator (commercial) - World's finest Hex Editor

Crackers

- John the Ripper - Fast password cracker
- Online MD5 cracker - Online MD5 hash Cracker
- Hashcat - The more fast hash cracker

Windows Utils

- Sysinternals Suite - The Sysinternals Troubleshooting Utilities
- Windows Credentials Editor - security tool to list logon sessions and add, change, list and delete associated credentials
- mimikatz - Credentials extraction tool for Windows OS
- PowerSploit - A PowerShell Post-Exploitation Framework
- Windows Exploit Suggester - Detects potential missing patches on the target
- Responder - A LLMNR, NBT-NS and MDNS poisoner
- Empire - Empire is a pure PowerShell post-exploitation agent
- Fibratus - Tool for exploration and tracing of the Windows kernel

Linux Utils

- Linux Exploit Suggester - Linux Exploit Suggester; based on operating system release number.

DDoS Tools

- LOIC - An open source network stress tool for Windows
- JS LOIC - JavaScript in-browser version of LOIC
- T50 - The more fast network stress tool

Social Engineering Tools

- SET - The Social-Engineer Toolkit from TrustedSec

OSInt Tools

- Maltego - Proprietary software for open source intelligence and forensics, from Paterva.
- theHarvester - E-mail, subdomain and people names harvester
- creepy - A geolocation OSINT tool
- metagoofil - Metadata harvester
- Google Hacking Database - a database of Google dorks; can be used for recon
- Shodan - Shodan is the world's first search engine for Internet-connected devices
- recon-ng - A full-featured Web Reconnaissance framework written in Python
- github-dorks - CLI tool to scan github repos/organizations for potential sensitive information leak

Anonymity Tools

- Tor - The free software for enabling onion routing online anonymity
- I2P - The Invisible Internet Project
- Nipe - Script to redirect all traffic from the machine to the Tor network.

Reverse Engineering Tools

- IDA Pro - A Windows, Linux or Mac OS X hosted multi-processor disassembler and debugger
- IDA Free - The freeware version of IDA v5.0
- WDK/WinDbg - Windows Driver Kit and WinDbg
- OllyDbg - An x86 debugger that emphasizes binary code analysis
- Radare2 - Opensource, crossplatform reverse engineering framework.

- x64_dbg - An open-source x64/x32 debugger for windows.
- Pyew - A Python tool for static malware analysis.
- Bokken - GUI for Pyew Radare2.
- Immunity Debugger - A powerful new way to write exploits and analyze malware
- Evan's Debugger - OllyDbg-like debugger for Linux
- Medusa disassembler - An open source interactive disassembler
- plasma - Interactive disassembler for x86/ARM/MIPS. Generates indented pseudo-code with colored syntax code.

CTF Tools

- Pwntools - CTF framework for use in CTFs

Books

Penetration Testing Books

- The Art of Exploitation by Jon Erickson, 2008
- Metasploit: The Penetration Tester's Guide by David Kennedy et al., 2011
- Penetration Testing: A Hands-On Introduction to Hacking by Georgia Weidman, 2014
- Rtfm: Red Team Field Manual by Ben Clark, 2014
- The Hacker Playbook by Peter Kim, 2014
- The Basics of Hacking and Penetration Testing by Patrick Engebretson, 2013
- Professional Penetration Testing by Thomas Wilhelm, 2013
- Advanced Penetration Testing for Highly-Secured Environments by Lee Allen, 2012
- Violent Python by TJ O'Connor, 2012
- Fuzzing: Brute Force Vulnerability Discovery by Michael Sutton et al., 2007
- Black Hat Python: Python Programming for Hackers and Pentesters by Justin Seitz, 2014

- Penetration Testing: Procedures & Methodologies by EC-Council, 2010
- Unauthorised Access: Physical Penetration Testing For IT Security Teams by Wil Allsopp, 2010
- Advanced Persistent Threat Hacking: The Art and Science of Hacking Any Organization by Tyler Wrightson, 2014
- Bug Hunter's Diary by Tobias Klein, 2011

Hackers Handbook Series

- The Database Hacker's Handbook, David Litchfield et al., 2005
- The Shellcoders Handbook by Chris Anley et al., 2007
- The Mac Hacker's Handbook by Charlie Miller & Dino Dai Zovi, 2009
- The Web Application Hackers Handbook by D. Stuttard, M. Pinto, 2011
- iOS Hackers Handbook by Charlie Miller et al., 2012
- Android Hackers Handbook by Joshua J. Drake et al., 2014
- The Browser Hackers Handbook by Wade Alcorn et al., 2014
- The Mobile Application Hackers Handbook by Dominic Chell et al., 2015
- Car Hacker's Handbook by Craig Smith, 2016

Network Analysis Books

- Nmap Network Scanning by Gordon Fyodor Lyon, 2009
- Practical Packet Analysis by Chris Sanders, 2011
- Wireshark Network Analysis by by Laura Chappell & Gerald Combs, 2012
- Network Forensics: Tracking Hackers through Cyberspace by Sherri Davidoff & Jonathan Ham, 2012

Reverse Engineering Books

- Reverse Engineering for Beginners by Dennis Yurichev

- Hacking the Xbox by Andrew Huang, 2003
- The IDA Pro Book by Chris Eagle, 2011
- Practical Reverse Engineering by Bruce Dang et al., 2014
- Gray Hat Hacking The Ethical Hacker's Handbook by Daniel Regalado et al., 2015

Malware Analysis Books

- Practical Malware Analysis by Michael Sikorski & Andrew Honig, 2012
- The Art of Memory Forensics by Michael Hale Ligh et al., 2014
- Malware Analyst's Cookbook and DVD by Michael Hale Ligh et al., 2010

Windows Books

- Windows Internals by Mark Russinovich et al., 2012

Social Engineering Books

- The Art of Deception by Kevin D. Mitnick & William L. Simon, 2002
- The Art of Intrusion by Kevin D. Mitnick & William L. Simon, 2005
- Ghost in the Wires by Kevin D. Mitnick & William L. Simon, 2011
- No Tech Hacking by Johnny Long & Jack Wiles, 2008
- Social Engineering: The Art of Human Hacking by Christopher Hadnagy, 2010
- Unmasking the Social Engineer: The Human Element of Security by Christopher Hadnagy, 2014
- Social Engineering in IT Security: Tools, Tactics, and Techniques by Sharon Conheady, 2014

Lock Picking Books

- Practical Lock Picking by Deviant Ollam, 2012

- Keys to the Kingdom by Deviant Ollam, 2012
- CIA Lock Picking Field Operative Training Manual
- Lock Picking: Detail Overkill by Solomon
- Eddie the Wire books

Vulnerability Databases

- NVD - US National Vulnerability Database
- CERT - US Computer Emergency Readiness Team
- OSVDB - Open Sourced Vulnerability Database
- Bugtraq - Symantec SecurityFocus
- Exploit-DB - Offensive Security Exploit Database
- Fulldisclosure - Full Disclosure Mailing List
- MS Bulletin - Microsoft Security Bulletin
- MS Advisory - Microsoft Security Advisories
- Inj3ct0r - Inj3ct0r Exploit Database
- Packet Storm - Packet Storm Global Security Resource
- SecuriTeam - Securiteam Vulnerability Information
- CXSecurity - CSSecurity Bugtraq List
- Vulnerability Laboratory - Vulnerability Research Laboratory
- ZDI - Zero Day Initiative

Security Courses

- Offensive Security Training - Training from BackTrack/Kali developers
- SANS Security Training - Computer Security Training & Certification
- Open Security Training - Training material for computer security classes
- CTF Field Guide - everything you need to win your next CTF competition
- Cybrary - online IT and Cyber Security training platform

Information Security Conferences

- DEF CON - An annual hacker convention in Las Vegas
- Black Hat - An annual security conference in Las Vegas
- BSides - A framework for organising and holding security conferences
- CCC - An annual meeting of the international hacker scene in Germany
- DerbyCon - An annual hacker conference based in Louisville
- PhreakNIC - A technology conference held annually in middle Tennessee
- ShmooCon - An annual US east coast hacker convention
- CarolinaCon - An infosec conference, held annually in North Carolina
- HOPE - A conference series sponsored by the hacker magazine 2600
- SummerCon - One of the oldest hacker conventions, held during Summer
- Hack.lu - An annual conference held in Luxembourg
- HITB - Deep-knowledge security conference held in Malaysia and The Netherlands
- Troopers - Annual international IT Security event with workshops held in Heidelberg, Germany
- Hack3rCon - An annual US hacker conference
- ThotCon - An annual US hacker conference held in Chicago
- LayerOne - An annual US security conference held every spring in Los Angeles
- DeepSec - Security Conference in Vienna, Austria
- SkyDogCon - A technology conference in Nashville
- SECUINSIDE - Security Conference in Seoul
- DefCamp - Largest Security Conference in Eastern Europe, held anually in Bucharest, Romania
- AppSecUSA - An annual conference organised by OWASP
- BruCON - An annual security conference in Belgium
- Infosecurity Europe - Europe's number one information security event, held in London, UK

- Nullcon - An annual conference in Delhi and Goa, India
- RSA Conference USA - An annual security conference in San Francisco, California, USA
- Swiss Cyber Storm - An annual security conference in Lucerne, Switzerland
- Virus Bulletin Conference - An annual conference going to be held in Denver, USA for 2016
- Ekoparty - Largest Security Conference in Latin America, held annually in Buenos Aires, Argentina
- 44Con - Annual Security Conference held in London
- BalCCon - Balkan Computer Congress, annualy held in Novi Sad, Serbia
- FSec - FSec - Croatian Information Security Gathering in Varaždin, Croatia

Information Security Magazines

- 2600: The Hacker Quarterly - An American publication about technology and computer "underground"
- Phrack Magazine - By far the longest running hacker zine

Awesome Lists

- Kali Linux Tools - List of tools present in Kali Linux
- SecTools - Top 125 Network Security Tools
- C/C++ Programming - One of the main language for open source security tools
- .NET Programming - A software framework for Microsoft Windows platform development
- Shell Scripting - Command-line frameworks, toolkits, guides and gizmos
- Ruby Programming by @dreikanter - The de-facto language for writing exploits
- Ruby Programming by @markets - The de-facto language for writing exploits

- Ruby Programming by @Sdogruyol - The de-facto language for writing exploits
- JavaScript Programming - In-browser development and scripting
- Node.js Programming by @sindresorhus - JavaScript in command-line
- Node.js Programming by @vndmtrx - JavaScript in command-line
- Python tools for penetration testers - Lots of pentesting tools are written in Python
- Python Programming by @svaksha - General Python programming
- Python Programming by @vinta - General Python programming
- Android Security - A collection of android security related resources
- Awesome Awesomness - The List of the Lists
- AppSec - Resources for learning about application security
- CTFs - Capture The Flag frameworks, libraries, etc
- Hacking - Tutorials, tools, and resources
- Honeypots - Honeypots, tools, components, and more
- Infosec - Information security resources for pentesting, forensics, and more
- Malware Analysis - Tools and resources for analysts
- PCAP Tools - Tools for processing network traffic
- Security - Software, libraries, documents, and other resources
- Awesome List - A curated list of awesome lists
- SecLists - Collection of multiple types of lists used during security assessments
- Security Talks - A curated list of security conferences