coreb1t / awesome-pentest-cheat-sheets

Collection of the cheat sheets useful for pentesting

cheatsheet security-cheat-sheets pentest-cheat-sheets security pentest awesome penetration-testing

73 commits **1** branch **0** releases **3** contributors

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

coreb1t Added Empire, Powersploit, PowerUp Latest commit 9676c9e on Feb 21

.github	CONTRIBUTING.md	2 years ago

docs	PDF Wireshark Display Filters added	10 months ago
.travis.yml	travis.yml added	2 years ago
README.md	Added Empire, Powersploit, PowerUp	3 months ago

README.md

Awesome Pentest Cheat Sheets 

Collection of cheat sheets useful for pentesting

Contribution

Your contributions and suggestions are heartily welcome. Please check the Contributing Guidelines for more details.

Security Talks and Videos

- InfoCon - Hacking Conference Archive
- Curated list of Security Talks and Videos

General

- Docker Cheat Sheet
- Mobile App Pentest Cheat Sheet
- OSX Command Line Cheat Sheet

- PowerShell Cheat Sheet - SANS PowerShell Cheat Sheet from SEC560 Course (PDF version)
- Regexp Security Cheat Sheet
- Security Cheat Sheets - A collection of security cheat sheets
- Unix / Linux Cheat Sheet

Discovery

- Google Dorks - Google Dorks Hacking Database (Exploit-DB)
- Shodan - Shodan is a search engine for finding specific devices, and device types, that exist online

Exploitation

- Empire Cheat Sheet - Empire is a PowerShell and Python post-exploitation framework
- Exploit Development Cheat Sheet - @ovid's exploit development in one picture
- Java Deserialization Cheat Sheet - A cheat sheet for pentesters about Java Native Binary Deserialization vulnerabilities
- Local File Inclution (LFI) Cheat Sheet #1 - Arr0way's LFI Cheat Sheet
- Local File Inclution (LFI) Cheat Sheet #2 - Aptive's LFI Cheat Sheet
- Metasploit Unleashed - The ultimate guide to the Metasploit Framework
- Metasploit Cheat Sheet - A quick reference guide (PNG version)(PDF version)
- PowerSploit Cheat Sheet - PowerSploit is a powershell post-exploitation framework
- PowerView 2.0 Tricks
- PowerView 3.0 Tricks
- PHP htaccess Injection Cheat Sheet - htaccess Injection Cheat Sheet by PHP Secure Configuration Checker
- Reverse Shell Cheat Sheet #1 - Pentestmonkey Reverse Shell Cheat Sheet
- Reverse Shell Cheat Sheet #2 - Arr0way's Reverse Shell Cheat Sheet

- SQL Injection Cheat Sheet - Netsparker's SQL Injection Cheat Sheet
- SQLite3 Injection Cheat Sheet

Privilege Escalation

Linux Privilege Escalation

- Basic Linux Privilege Escalation - Linux Privilege Escalation by @g0tmi1k
- linux-exploit-suggester.sh - Linux privilege escalation auditing tool written in bash (updated)
- Linux_Exploit_Suggester.pl - Linux Exploit Suggester written in Perl (last update 3 years ago)
- Linux_Exploit_Suggester.pl v2 - Next-generation exploit suggester based on Linux_Exploit_Suggester (updated)
- Linux Soft Exploit Suggester - linux-soft-exploit-suggester finds exploits for all vulnerable software in a system helping with the privilege escalation. It focuses on software packages instead of Kernel vulnerabilities
- checksec.sh - bash script to check the properties of executables (like PIE, RELRO, PaX, Canaries, ASLR, Fortify Source)
- linuxprivchecker.py - This script is intended to be executed locally on a Linux box to enumerate basic system info and search for common privilege escalation vectors such as world writable files, misconfigurations, clear-text passwords and applicable exploits (@SecuritySift)
- LinEnum - This tool is great at running through a heap of things you should check on a Linux system in the post exploit process. This include file permissions, cron jobs if visible, weak credentials etc.(@Rebootuser)

Windows Privilege Escalation

- PowerUp - Excellent powershell script for checking of common Windows privilege escalation vectors. Written by harmj0y (direct link)
- PowerUp Cheat Sheet

- Windows Exploit Suggester - Tool for detection of missing security patches on the windows operating system and mapping with the public available exploits
- Sherlock - PowerShell script to quickly find missing software patches for local privilege escalation vulnerabilities
- Precompiled Windows Exploits - Collection of precompiled Windows exploits
- Metasploit Modules
  - post/multi/recon/local_exploit_suggester - suggests local meterpreter exploits that can be used
  - post/windows/gather/enum_patches - helps to identify any missing patches

Tools

- Nmap Cheat Sheet
- SQLmap Cheat Sheet
- SQLmap Tamper Scripts - SQLmal Tamper Scripts General/MSSQL/MySQL
- VIM Cheatsheet
- Wireshark Display Filters - Filters for the best sniffing tool

Tools Online

- XSS'OR Encoder/Decoder - Online Decoder/Encoder for testing purposes (@evilcos)
- WebGun - WebGun, XSS Payload Creator (@brutelogic)
- Hackvertor - Tool to convert various encodings and generate attack vectors (@garethheyes)
- JSFiddle - Test and share XSS payloads, Example PoC

Payloads

Genaral

- Fuzzdb - Dictionary of attack patterns and primitives for black-box application testing Polyglot Challenge with submitted solutions
- SecList - A collection of multiple types of lists used during security assessments. List types include usernames, passwords, URLs, sensitive data grep strings, fuzzing payloads, and many more

XSS

- XSS Polyglot Payloads #1 - Unleashing an Ultimate XSS Polyglot list by 0xsobky
- XSS Polyglot Payloads #2 - @filedescriptor's XSS
- Browser's-XSS-Filter-Bypass-Cheat-Sheet- Excellent List of working XSS bapasses running on the latest version of Chrome / Safari, IE 11 / Edge created by Masato Kinugawa

Write-Ups

- Bug Bounty Reference - huge list of bug bounty write-up that is categorized by the bug type (SQLi, XSS, IDOR, etc.)
- Write-Ups for CTF challenges
- Facebook Bug Bounties - Categorized Facebook Bug Bounties write-ups

Learning Platforms

Online

- Hack The Box :: Penetration Testing Labs
- OWASP Vulnerable Web Applications Directory Project (Online) - List of online available vulnerable applications for learning purposes

- Pentestit labs - Hands-on Pentesting Labs (OSCP style)
- Root-me.org - Hundreds of challenges are available to train yourself in different and not simulated environments
- Vulnhub.com - Vulnerable By Design VMs for practical 'hands-on' experience in digital security

Off-Line

- Damn Vulnerable Xebia Training Environment - Docker Container including several vurnerable web applications (DVWA,DVWServices, DVWSockets, WebGoat, Juiceshop, Railsgoat, django.NV, Buggy Bank, Mutilidae II and more)
- OWASP Vulnerable Web Applications Directory Project (Offline) - List of offline available vulnerable applications for learning purposes

Wireless Hacking

Tools

- wifite2 - Full authomated WiFi security testing script

Defence Topics

- Docker Security Cheat Sheet - The following tips should help you to secure a container based system (PDF version)
- Windows Domain Hardening - A curated list of awesome Security Hardening techniques for Windows

Programming

- JavaScript Cheat Sheet - Learn javascript in one picture (Online version) (PNG version)
- Python Cheat Sheet #1 - Learn python3 in one picture (PNG version)

- Python Cheat Sheet #2 - Learn python3 in one picture (Online version) (PNG version)
- Python Snippets Cheat Sheet - List of helpful re-usable code snippets in Python