Claus Cramon Houmann
Community Ma
Dec 30, 2016
• last reply A

Follow

Follow the author to get their posts on your wall. You can also follow tags, companies, and products.

Got It!

The comp fosec related cheat sheets

I do not think I have collected them all yet, but

Join the discussion ›

Penetration testing and webapp cheat sheets:

mobile application pentesting: https://www.peerlyst.com/posts/mobile-application-penetration-testing-cheat-sheet

Pentesting https://github.com/jshaw87/Cheat-sheets/blob/master/Cheatsheet_PenTesting.txt

XSS Vectors https://sql--injection.blogspot.lu/p/blog-page_80.html and cookie stealing

Penetration testing tools https://highon.coffee/blog/penetration-testing-tools-cheat-sheet/#port-scanning

Penetration testing & exploit development https://imgur.com/Mr9pvq9

Printer security testing http://hacking-printers.net/wiki/index.php/Printer_Security_Testing_Cheat_Sheet

Nmap (Printable, 2013): https://pen-testing.sans.org/blog/2013/10/08/nmap-cheat-sheet-1-0/

Nmap (Not printable, date unknown): https://hackertarget.com/nmap-cheatsheet-a-quick-reference-guide/

Nmap 5(older version, not printable): https://nmapcook-book.blogspot.lu/2010/02/nmap-cheat-sheet.html

Nmap 5 (older version, printable) http://www.cheat-sheets.org/saved-copy/Nmap5.cheatsheet.eng.v1.pdf

cobalt strike beacon https://github.com/Harm-J0y/CheatSheets/blob/master/Beacon.pdf

Java-Deserialization https://github.com/Grrr-Dog/Java-Deserialization-Cheat-Sheet

Metasploit https://www.tunnelsup.com/metas-ploit-cheat-sheet/

Another Metasploit: http://resources.infosecinsti-tute.com/metasploit-cheat-sheet/

Powerupsql https://github.com/NetSPI/PowerUp-SQL/wiki/PowerUpSQL-CheatSheet

Scapy https://pen-testing.san-s.org/blog/2016/04/05/scapy-cheat-sheet-from-sans-sec560#

HTTP Status codes http://suso.suso.org/docs/infosheets/HTTP_status_codes.gif

Beacon https://github.com/HarmJ0y/CheatSheets/blob/master/Beacon.pdf

Powershellempire https://github.com/HarmJ0y/CheatSheets/blob/master/Empire.pdf

Powersploit https://github.com/HarmJ0y/CheatSheets/blob/master/PowerSploit.pdf

PowerUp https://github.com/HarmJ0y/CheatSheets/blob/master/PowerUp.pdf

Powerview https://github.com/HarmJ0y/CheatSheets/blob/master/PowerView.pdf

Vim https://people.csail.mit.edu/vgod/vim/vim-cheat-sheet-en.pdf

Attack Surface Analysis

XSS Filter Evasion

REST Assessment

Web Application Security Testing

Android Testing

IOS Developer

Mobile Jailbreaking

sql injection https://www.veracode.com/security/sql-injection

MYSQL SQL injection http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet

Password cracking: https://www.unix-ninja.com/p/A_cheat-sheet_for_password_crackers

SSL manual testing: http://www.exploresecurity.com/wp-content/uploads/custom/SSL_manual_cheatsheet.html

Python

OWASP Webapp checklist

AIXBuild https://github.com/jshaw87/Cheatsheets/blob/master/Cheatsheet_AIXBuild.txt

AVBypass with Veil https://github.com/jshaw87/Cheatsheets/blob/master/Cheatsheet_AVBypass.txt

Bash Scripting https://github.com/jshaw87/Cheatsheets/blob/master/Cheatsheet_BashScripting.txt

IKEScan for aggresive mode

LinuxPrivilegeEsc

VOIP https://github.com/jshaw87/Cheat-sheets/blob/master/Cheatsheet_VOIP.txt

Wireless Testing https://github.-com/jshaw87/Cheatsheets/blob/master/Cheat-sheet_WirelessTesting.txt

CEH Cheat Sheet Exercises

Meterpreter Cheat Sheet

netcat

Nessus NMAP Commands

NMap Mindmap Reference

NMap Quick Reference Guide

Reconnaissance Reference Sheet

Tripwire Common Security Exploit-Vuln Matrix

Linux - Bourne Shell Quick Reference.pdf

Linux - Quick Reference Card.pdf

Linux - Shell Cheat Sheet.pdf

Linux - Shell Scrip Cheat Sheet.pdf

Linux - tcpdump.pdf

Penetration Testing - Penetration Testing Framework (vulnerabilityassessment.co.uk)

Password cracking cheat sheets

Password cracking: https://www.unix-ninja.com/p/A_cheat-sheet_for_password_crackers

---

Forensics cheat sheets

master boot record, guid partition table, NTFS volume boot record, Master file table record, standard information attribute, $Attribute list attribute, $file name attribute, and more forensics posters/cheat sheets: https://github.com/Invoke-IR/ForensicPosters

Mounting DD Images https://sift.readthedocs.io/en/latest/cheatsheet/

XP only - old https://www.sans.org/media/score/checklists/ID-Windows.pdf

https://www.sans.org/media/score/checklists/ID-Linux.pdf

https://github.com/Invoke-IR/ForensicPosters

Regex / PCRE https://github.com/niklongstone/regular-expression-cheat-sheet

---

CISO, blue team, Sysadmin and webadmin cheat sheets

CSP cheat sheet https://scotthelme.co.uk/csp-cheat-sheet/#require-sri-for (via Scott Helme)

HSTS Cheat Sheet HSTS
HPKP Cheat Sheet HPKP
HTTPS Cheat Sheet HTTPS
Performance Cheat Sheet HTTPS performance

HTTP Status codes http://suso.suso.org/docs/infosheets/HTTP_status_codes.gif

The windows logging Cheat Sheet https://www.malwarearchaeology.com/s/Windows-Logging-Cheat-Sheet_ver_Oct_2016.pdf

The Windows Splunk Logging Cheat Sheet

The Windows File Auditing Logging Cheat Sheet

The Windows Registry Auditing Logging Cheat Sheet

The Windows PowerShell Logging Cheat Sheet

Curl HTTP https://bagder.github.io/curl-cheat-sheet/http-sheet.html

Virtual Patching

Cloud Control Matrix (CCM) https://cloudsecurityalliance.org/group/cloud-controls-matrix/

Antivirus Event Analysis (what types of AV alerts should you worry about and why)

CiscoIOS https://github.com/jshaw87/Cheatsheets/blob/master/Cheatsheet_CiscoIOS.txt

GPG https://github.com/jshaw87/Cheatsheets/blob/master/Cheatsheet_GPG.txt

Regex / PCRE https://github.com/niklongstone/regular-expression-cheat-sheet

Security Onion http://chrissanders.org/2017/06/security-onion-cheat-sheet/

Linux Security Quick Reference Guide

IP Tables

TCPDump

Wireshark Filters

IP Access Lists

Common Ports

netcat

Linux Admin Quick Reference

Crontab Reference

Networking - Border Gateway Protocol.pdf

Networking - Cisco IOS IPv4 Access Lists.pdf

Networking - Cisco IOS Versions.pdf

Networking - Common TCP-UDP Ports.pdf

Networking - EIGRP (Enhanced Interior Gateway Routing Protocol).pdf

Networking - First Hop (Router) Redundancy.pdf

Networking - Frame Mode MPLS.pdf

Networking - IEEE 802.11 WirelessLAN.pdf

Networking - IEEE 802.1X Authentication.pdf

Networking - IPsec.pdf

Networking - IPv4 Multicast.pdf

Networking - IPv4_Subnetting.pdf

Networking - IPv6.pdf

Networking - IS-IS.pdf

Networking - NAT.pdf

Networking - OSPF.pdf

Networking - Physical Terminations.pdf

Networking - PPP.pdf

Networking - QoS.pdf

Networking - Spanning Tree.pdf

Networking - TCPIP.pdf

Networking - VLANs.pdf

Networking - Wireshark Display Filters.pdf

VMware - Reference Card.pdf

Threat hunting

Intrusion Discovery Cheat Sheet for Windows

Intrusion Discovery Cheat Sheet for Linux

https://www.sans.org/media/score/checklists/ID-Windows.pdf

https://www.sans.org/media/score/checklists/ID-Linux.pdf

Regex https://github.com/niklongstone/regular-expression-cheat-sheet

---

Malware analysis and reverse engineering:

Malware analysis: http://r00ted.-com/cheat%20sheet%20reverse%20v5.png

ADB: https://github.com/maldroid/adb_cheat-sheet

GDB vs windbg https://twitter.com/it4sec/status/828159963654668288/photo/1

REMNUX distro: https://zeltser.com/media/docs/remnux-malware-analysis-tips.pdf

IDAPro: https://securedorg.github.io/idacheat-sheet.html

Regex https://github.com/niklongstone/regular-expression-cheat-sheet

---

Text editors

VIM https://people.csail.mit.edu/vgod/vim/vim-cheat-sheet-en.pdf

---

Developers/Builders

- 3rd Party Javascript Management
- Access Control
- AJAX Security Cheat Sheet
- Authentication (ES)
- Bean Validation Cheat Sheet
- Choosing and Using Security Questions
- Clickjacking Defense
- C-Based Toolchain Hardening
- Credential Stuffing Prevention Cheat Sheet
- Cross-Site Request Forgery (CSRF) Prevention
- Cryptographic Storage
- Deserialization
- DOM based XSS Prevention
- Forgot Password
- HTML5 Security
- HTTP Strict Transport Security
- Injection Prevention Cheat Sheet
- Input Validation
- JAAS
- LDAP Injection Prevention
- Logging
- Mass Assignment Cheat Sheet
- .NET Security
- OWASP Top Ten
- Password Storage

- Pinning
- Query Parameterization
- Ruby on Rails
- REST Security
- Session Management
- SAML Security
- SQL Injection Prevention
- Transaction Authorization
- Transport Layer Protection
- Unvalidated Redirects and Forwards
- User Privacy Protection
- Web Service Security
- XSS (Cross Site Scripting) Prevention
- XML External Entity (XXE) Prevention Cheat Sheet
- Python
- Linux Commands Reference Card
- One page Linux Manual
- Unix Tool Box
- Treebeard's Unix Cheat Sheet
- Terminal Shortcuts
- More Terminal Shortcuts
- Useful Gnome/KDE shortcuts
- KDE Cheat Sheet
- Vi Cheat Sheet
- Concise Vim Cheat Sheet
- awk nawk and gawk cheat sheet
- Sed Stream Editor Cheat Sheet
- Screen Quick Reference
- Screen Terminal Emulator Cheat Sheet

- Vi/Vim Cheat Sheet
- Ubuntu Cheat Sheet
- Debian Cheat Sheet
- HTML - Markdown.pdf
- MAC - OSX Key Combo Reference Guide.pdf
- SQL - MySQL Commands.pdf

Owasp cheat-sheets still in draft/Beta stages:

- Application Security Architecture
- Business Logic Security
- Command Injection Defense Cheat Sheet
- PHP Security
- Regular Expression Security Cheatsheet
- Secure Coding
- Secure SDLC
- Threat Modeling
- Grails Secure Code Review
- IOS Application Security Testing
- Key Management
- Insecure Direct Object Reference Prevention
- Content Security Policy

Deep learning/AI/Machine learning

Keras deep learning

Numpy

Pandas

Pandas

SciPy

Matplotlib

Scikit

Neural Network Zoo

ggplot2

PySpark

Rstudio

Penetration test

mobile application | pentesting | XSS

exploit development | security testing

cobalt strike beacon | HTTP | sql injection

MYSQL | SQL | injection | SSL

manual show more

83 8 24

Michal Mike Dorosz and 12 others are sharing insights

Join the discussion...

pepepepe • July 18, 2017

Interesting list but https://www.sans.org/media/score/checklists/ID-Windows.pdf is quite old "Windows XP Pro / 2003 Server / Vista"

Some commands don't work on Win7

Upvote 1 Reply

1 reply

Michal Mike Dorosz • July 18, 2017

Hello Claus, thank you very much for great article! I can only imagine how long has it taken to complete the list ;)

Upvote 1 Reply

1 reply

View more comments