- ★ Featured
- Recommended for you
- Advanced Search
- Recruiters / Hiring Managers

SHORTCUTS Edit

- Account Takeover Prevention
- # BYOD
- Cequence Security
- Cybersecurity Career Track
- FIPS 140-2 Validation without Consultants
- RSA Conference
- Springboard
- # infosec career
- # mobile device management

MY PROFILE

Are you a Vendor? Click here

How to use Peerlyst
Secure Drop
FAQ
About
In the News
Contact us
Privacy Policy
Terms of Service
Careers

Join the discussion ›

Claus Cramon Houmann
Employee at Not Telling you Hackers

Dec 30, 2016 • updated Feb 20, 2019 • last reply Mar 25, 2019 • 66.1K views

Follow Sponsor this post

The complete list of Infosec related cheat sheets

I do not think I have collected them all yet, but here's what I have so far. Please suggest more.

Penetration testing and webapp cheat sheets:

- mobile application pentesting: https://www.peerlyst.com/posts/mobile-application-penetration-testing-cheat-sheet
- python for pentesting Python Penetration Testing Cheet Sheet
- web application penetration testing Web Application Penetration Testing Cheat Sheet
- pentesting https://github.com/jshaw87/Cheatsheets/blob/master/Cheatsheet_PenTesting.txt

- 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 CHEAT-SHEET (Nmap Scanning Types, Scanning Commands , NSE Scripts)
- 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://nmapcookbook.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/HarmJ0y/CheatSheets/blob/master/Beacon.pdf
- Java-Deserialization https://github.com/GrrrDog/Java-Deserialization-Cheat-Sheet
- Metasploit https://www.tunnelsup.com/metasploit-cheat-sheet/
- Another Metasploit: http://resources.infosecinstitute.com/metasploit-cheat-sheet/
- Powerupsql https://github.com/NetSPI/PowerUpSQL/wiki/PowerUpSQL-CheatSheet
- Scapy https://pen-testing.sans.org/blog/2016/04/05/scapy-cheat-sheet-from-sans-sec560#
- HTTP status codes http://suso.suso.org/docs/infosheets/HTTP_status_codes.gif HTTP
- 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 attack surface analysis
- XSS Filter Evasion XSS filter evasion
- REST Assessment REST assessment api security
- Web Application Security Testing web application testing
- Android Testing android security
- IOS Developer iOS internals
- Mobile Jailbreaking mobile jailbreaking
- Comprehensive sql injection https://sqlwiki.netspi.com/
- sql injection https://www.veracode.com/security/sql-injection
- SQL injection: https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
- 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 python
- OWASP Webapp checklist owasp 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

Join the discussion >

- Wireless Testing https://github.com/jshaw87/Cheatsheets/blob/master/Cheatsheet_WirelessTesting.txt wireless testing
- CEH Cheat Sheet Exercises CEH exercises
- Meterpreter Cheat Sheet meterpreter tips
- netcat netcat tips
- Nessus NMAP Commands Tenable Nessus NMAP commands
- NMap Mindmap Reference mindmap
- NMap Quick Reference Guide nmap
- Reconnaissance Reference Sheet reconnaissance
- Tripwire Common Security Exploit-Vuln Matrix
- Linux - Bourne Shell Quick Reference.pdf Bourne Shell
- Linux - Quick Reference Card.pdf linux
- Linux - Shell Cheat Sheet.pdf
- Linux - Shell Scrip Cheat Sheet.pdf
- Linux - tcpdump.pdf
- Penetration Testing - Penetration Testing Framework (vulnerabilityassessment.co.uk) penetration testing framework
- XML Vulnerabilities and Attacks cheatsheet
- Memory segmentation cheat sheet
- IP, DNS & Domain Enumeration Cheatsheet
- Local Linux Enumeration & Privilege Escalation
- hashcat Nice cheatsheet for Hashcat by Kent R. Ickler / BHIS https://www.blackhillsinfosec.com/hashcat-4-10-cheat-sheet-v-1-2018-1/ via Martin Boller
- BASH Shell https://goalkicker.com/BashBook/ thanks InfosecTDK
- Subdomains Enumeration Cheat Sheet subdomain enumeration
- SSH Cheat Sheet
- John The Ripper Hash Formats
- Informix SQL Injection Cheat Sheet
- MSSQL Injection Cheat Sheet
- Oracle SQL Injection Cheat Sheet
- MySQL SQL Injection Cheat Sheet
- Postgres SQL Injection Cheat Sheet
- DB2 SQL Injection Cheat Sheet
- Ingres SQL Injection Cheat Sheet
- Cheatsheet_SSLStrip.txt
- Cheatsheet_Solaris pentesting.txt
- Cheatsheet_BrowserAddon_Tools.txt
- Cheatsheet_UsefulCommands.txt
- Cheatsheet_VOIP.txt
- Cheatsheet_AIXBuild.txt
- Cheatsheet_AVBypass.txt
- Cheatsheet_ApacheSSL.txt
- Cheatsheet_AttackingMSSQL.txt
- Cheatsheet_BashScripting.txt

Join the discussion ›

- Cheatsheet_DomainAdminExploitation.
- Cheatsheet_ExploitDev.txt
- Cheatsheet_GDB.txt
- Cheatsheet_GPG.txt
- Cheatsheet_HTTPBasicAuth.txt
- Cheatsheet_IKEScan.txt
- Cheatsheet_LinuxPrivilegeEsc.txt
- Cheatsheet_LocalSamDump.txt
- Cheatsheet_MSFPostExploitation.txt
- Cheatsheet_Metasploit.pdf
- Cheatsheet_MetasploitPayloads.txt
- Cheatsheet_MobileAppTesting.txt
- Cheatsheet_Networking.txt
- Cheatsheet_OWASPCheckList.txt
- Cheatsheet_Oracle.txt
- Cheatsheet_PenTesting.txt
- Cheatsheet_Pyinstaller.txt
- Cheatsheet_Python.pdf
- Cheatsheet_Remediations.txt
- Cheatsheet_SMBCapture.txt
- Cheatsheet_SMBEnumeration.txt
- Cheatsheet_SMTPOpenRelay.txt
- Cheatsheet_SQLInjection.txt
- Cheatsheet_Vlans.txt
- Cheatsheet_VulnVerify.txt
- Cheatsheet_Windows.txt
- Cheatsheet_WindowsCommandLine.pd
- Cheatsheet_WirelessTesting.txt
- Cheatsheet_XSS.txt
- Cheatsheet_scp.txt
- METASPLOIT.txt

Password cracking cheat sheets

- password cracking: https://www.unix-ninja.com/p/A_cheat-sheet_for_password_crackers
- Nice cheatsheet for Hashcat by Kent R. Ickler / BHIS https://www.blackhillsinfosec.com/hashcat-4-10-cheat-sheet-v-1-2018-1/

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

Join the discussion ›

- https://github.com/Invoke-IR/ForensicPosters forensics posters
- Regex / PCRE https://github.com/niklongstone/regular-expression-cheat-sheet
- Memory segmentation cheat sheet
- Volatility Memory Forensics Cheat Sheet - Sans Forensics
- Volatility Cheat Sheet - The Volatility Foundation
- Known command-lines of fileless malicious executions.

CISO, blue team, Sysadmin and webadmin cheat sheets

- Antivirus Event Analysis Cheat Sheet Version 1.2
- TLS Cheatsheet by Sean Wright
- Windows Logging ATT&CK matrix
- Windows logging Sysmon LOG-MD cheat
- Windows Advanced Logging Cheat Sheet
- 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
- AWS Cheat sheet https://posts.specterops.io/amazon-web-services-cheatsheet-59871854de8c
- Google compute cheat sheet https://posts.specterops.io/clouds-google-compute-cheatsheet-c063316d0c2b
- Microsoft azure cheat sheet https://posts.specterops.io/microsoft-azure-cheatsheet-d75223ddab65
- The windows logging Cheat Sheet https://www.malwarearchaeology.com/s/Windows-Logging-Cheat-Sheet_ver_Oct_2016.pdf
- The Windows Splunk Logging Cheat Sheet Splunk logging
- The Windows File Auditing Logging Cheat Sheet file auditing logging
- The Windows Registry Auditing Logging Cheat Sheet registry auditing logging
- The Windows PowerShell Logging Cheat Sheet powershell logging
- Curl HTTP https://bagder.github.io/curl-cheat-sheet/http-sheet.html
- Virtual Patching 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 linux security
- IP Tables iptables
- TCPDump tcpdump
- Wireshark Filters wireshark filters
- IP Access Lists

Join the discussion >

- Networking - Border Gateway Protocol.pdf BGP border gateway protocol
- 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
- IT Project Cheatsheet Collection
- The illustrated TLS 1.3 connection
- Known command-lines of fileless malicious executions.
- 5 Ways to Make Django Admin Safer
- AV Analysis Cheat Sheet

Threat hunting

- Windows Advanced Logging Cheat Sheet
- **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
- ELK-Hunting/ELK-cheatsheet.md

Privacy:

Join the discussion ›

Malware analysis and reverse engineering:

- Malware analysis: https://github.com/hslatman/cheatsheets/blob/master/sheets/cheat%20sheet%20reverse%20v5.png
- ADB: https://github.com/maldroid/adb_cheatsheet
- 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/idacheatsheet.html
- Regex https://github.com/niklongstone/regular-expression-cheat-sheet
- windbg Windbg-Cheat-Sheet
- Memory segmentation cheat sheet
- Unpacking for dummies

Text editors

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

---

Developers/Builders

- Angular and the OWASP top 10
- 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

- 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
- C - Cheat Sheets
- LAMP Cheat Sheet Collection
- Version Control Cheat Sheets List
- Open Source EN
- TDD tools for JavaScript
- Cursive
- Web Accessibility Collection
- Comp. Sci. GCSE (AQA 8520)

Join the discussion ›

- 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

Link aggregations:

- Link aggregation for pentest and blue team

----

windows ▶ malware ▶ learning ▶ linux ▶ blue team ▶ password ▶ HTTPS ▶ HTTP ▶ testing ▶ forensics ▶ python ▶ logging ▶ manual ▶ show more

Upvote 143 Share 13 Comment 100 Invite to discuss Bookmark

Support the community by sponsoring this post and promote your product! Sponsor this post

Join the discussion ›

InfosecTDK • Mar 25, 2019

as per Eric Geek Pen Testing Cheatsheets

Upvote Reply

Chiheb Chebbi • Mar 11, 2019

Ghidra cheatsheet https://ghidra-sre.org/CheatSheet.html

Upvote Reply

Older comments

More from author

Crowdsourcing: GDPR: A list of news sites that block your access if no cookies accepted

Claus Cramon Houmann

Related reading

A Collection of Awesome Penetration Testing Resources by Nick Raienko

Dawid Balut

Featured reading

A consumer endpoint security guide for laypeople

Kim Crawley

Explore more ›

Company contributions

7 Programming Languages to Learn for a Career in Cybersecurity

Springboard

Join the discussion ›