Penetration Testing Resources	
1	**#### Penetration Testing Resources**
2	* [Metasploit Unleashed](http://www.offensive-security.com/metasploit-unleashed/) - Free Offensive Security metasploit course
3	* [PTES](http://www.pentest-standard.org/) - Penetration Testing Execution Standard
4	* [OWASP](https://www.owasp.org/index.php/Main_Page) - Open Web Application Security Project
5	**#### Exploit development**
6	* [Shellcode Tutorial](http://www.vividmachines.com/shellcode/shellcode.html) - Tutorial on how to write shellcode
7	* [Shellcode Examples](http://shell-storm.org/shellcode/) - Shellcodes database
8	* [Exploit Writing Tutorials](https://www.corelan.be/index.php/2009/07/19/exploit-writing-tutorial-part-1-stack-based-overflows/) - Tutorials on how to develop exploits
9	* [GDB-peda](https://github.com/longld/peda) - Python Exploit Development Assistance for GDB
10	* [shellsploit](https://github.com/b3mb4m/shellsploit-framework) - New Generation Exploit Development Kit
11	**#### Social Engineering Resources**
12	* [Social Engineering Framework](http://www.social-engineer.org/framework/) - An information resource for social engineers
13	**#### Lock Picking Resources**
14	* [Schuyler Towne channel](http://www.youtube.com/user/SchuylerTowne/) - Lockpicking videos and security talks
15	* [/r/lockpicking](https://www.reddit.com/r/lockpicking) - Resources for learning lockpicking, equipment recommendations.
16	**#### Penetration Testing Distributions**
17	* [Kali](http://www.kali.org/) - A Linux distribution designed for digital forensics and penetration testing
18	* [BlackArch](http://www.blackarch.org/) - Arch Linux-based distribution for penetration testers and security researchers
19	* [NST](http://networksecuritytoolkit.org/) - Network Security Toolkit distribution
20	* [Pentoo](http://www.pentoo.ch/) - security-focused livecd based on Gentoo
21	* [BackBox](http://www.backbox.org/) - Ubuntu-based distribution for penetration tests and security assessments
22	**#### Basic Penetration Testing Tools**

23	* [Metasploit Framework](http://www.metasploit.com/) - World's most used penetration testing software
24	* [Burp Suite](http://portswigger.net/burp/) - An integrated platform for performing security testing of web applications
25	* [ExploitPack](http://exploitpack.com/) - Graphical tool for penetration testing with a bunch of exploits
26	* [BeeF](https://github.com/beefproject/beef) - The Browser Exploitation Framework Project
27	* [faraday](https://github.com/infobyte/faraday) - Collaborative Penetration Test and Vulnerability Management Platform
28	* [evilgrade](https://github.com/infobyte/evilgrade) - The update explotation framework
29	* [commix](https://github.com/stasinopoulos/commix) - Automated All-in-One OS Command Injection and Exploitation Tool
30	**#### Vulnerability Scanners**
31	* [Netsparker](https://www.netsparker.com/communityedition/) - Web Application Security Scanner
32	* [Nexpose](https://www.rapid7.com/products/nexpose/) - Vulnerability Management & Risk Management Software
33	* [Nessus](http://www.tenable.com/products/nessus) - Vulnerability, configuration, and compliance assessment
34	* [Nikto](https://cirt.net/nikto2) - Web application vulnerability scanner
35	* [OpenVAS](http://www.openvas.org/) - Open Source vulnerability scanner and manager
36	* [OWASP Zed Attack Proxy](https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project) - Penetration testing tool for web applications
37	* [Secapps](https://secapps.com/) - Integrated web application security testing environment
38	* [w3af](https://github.com/andresriancho/w3af) - Web application attack and audit framework
39	* [Wapiti](http://wapiti.sourceforge.net/) - Web application vulnerability scanner
40	* [WebReaver](http://www.webreaver.com/) - Web application vulnerability scanner for Mac OS X
41	* [DVCS Ripper](https://github.com/kost/dvcs-ripper) - Rip web accessible (distributed) version control systems: SVN/GIT/HG/BZR
42	* [arachni](https://github.com/Arachni/arachni) - Web Application Security Scanner Framework
43	**#### Network Tools**
44	* [nmap](http://nmap.org/) - Free Security Scanner For Network Exploration & Security Audits
45	* [pig](https://github.com/rafael-santiago/pig) - A Linux packet crafting tool

46	* [tcpdump/libpcap](http://www.tcpdump.org/) - A common packet analyzer that runs under the command line
47	* [Wireshark](http://www.wireshark.org/) - A network protocol analyzer for Unix and Windows
48	* [Network Tools](http://network-tools.com/) - Different network tools: ping, lookup, whois, etc
49	* [netsniff-ng](https://github.com/netsniff-ng/netsniff-ng) - A Swiss army knife for for network sniffing
50	* [Intercepter-NG](http://intercepter.nerf.ru/) - a multifunctional network toolkit
51	* [SPARTA](http://sparta.secforce.com/) - Network Infrastructure Penetration Testing Tool
52	* [DNSDumpster](https://dnsdumpster.com/) - Online DNS recond and search service
53	* [Mass Scan](https://github.com/robertdavidgraham/masscan) - TCP port scanner, spews SYN packets asynchronously, scanning entire Internet in under 5 minutes.
54	* [Zarp](https://github.com/hatRiot/zarp) - Zarp is a network attack tool centered around the exploitation of local networks
55	* [mitmproxy](https://github.com/mitmproxy/mitmproxy) - An interactive SSL-capable intercepting HTTP proxy for penetration testers and software developers
56	* [mallory](https://github.com/justmao945/mallory) - HTTP/HTTPS proxy over SSH
57	* [DET](https://github.com/sensepost/DET) - DET is a proof of concept to perform Data Exfiltration using either single or multiple channel(s) at the same time
58	* [pwnat](https://github.com/samyk/pwnat) - punches holes in firewalls and NATs
59	* [dsniff](https://www.monkey.org/~dugsong/dsniff/) - a collection of tools for network auditing and pentesting
60	* [tgcd](http://tgcd.sourceforge.net/) - a simple Unix network utility to extend the accessibility of TCP/IP based network services beyond firewalls
61	**#### Wireless Network Tools**
62	* [Aircrack-ng](http://www.aircrack-ng.org/) - a set of tools for auditing wireless network
63	* [Kismet](https://kismetwireless.net/) - Wireless network detector, sniffer, and IDS
64	* [Reaver](https://code.google.com/p/reaver-wps/) - Brute force attack against Wifi Protected Setup
65	* [Wifite](https://github.com/derv82/wifite) - Automated wireless attack tool
66	* [wifiphisher](https://github.com/sophron/wifiphisher) - Automated phishing attacks against Wi-Fi networks
67	**#### SSL Analysis Tools**

68	* [SSLyze](https://github.com/nabla-c0d3/sslyze) - SSL configuration scanner
69	* [sslstrip](http://www.thoughtcrime.org/software/sslstrip/) - a demonstration of the HTTPS stripping attacks
70	* [sslstrip2](https://github.com/LeonardoNve/sslstrip2) - SSLStrip version to defeat HSTS
71	#### **Web exploitation**
72	* [WPScan](http://wpscan.org/) - Black box WordPress vulnerability scanner
73	* [SQLmap](http://sqlmap.org/) - Automatic SQL injection and database takeover tool
74	* [weevely3](https://github.com/epinna/weevely3) - Weaponized web shell
75	* [Wappalyzer](https://wappalyzer.com/) - Wappalyzer uncovers the technologies used on websites
76	* [cms-explorer](https://code.google.com/archive/p/cms-explorer/) - CMS Explorer is designed to reveal the the specific modules, plugins, components and themes that various CMS driven web sites are running.
77	* [joomscan](https://www.owasp.org/index.php/Category:OWASP_Joomla_Vulnerability_Scanner_Project) - Joomla CMS scanner
78	* [WhatWeb](https://github.com/urbanadventurer/WhatWeb) - Website Fingerprinter
79	* [BlindElephant](http://blindelephant.sourceforge.net/) - Web Application Fingerprinter
80	#### **Hex Editors**
81	* [HexEdit.js](http://hexed.it/) - Browser-based hex editing
82	* [Hexinator](https://hexinator.com/) (commercial) - World's finest Hex Editor
83	#### **Crackers**
84	* [John the Ripper](http://www.openwall.com/john/) - Fast password cracker
85	* [Online MD5 cracker](http://www.md5crack.com/) - Online MD5 hash Cracker
86	* [Hashcat](http://hashcat.net/oclhashcat/) - The more fast hash cracker
87	#### **Windows Utils**
88	* [Sysinternals Suite](http://technet.microsoft.com/en-us/sysinternals/bb842062) - The Sysinternals Troubleshooting Utilities
89	* [Windows Credentials Editor](http://www.ampliasecurity.com/research/windows-credentials-editor/) - security tool to list logon sessions and add, change, list and delete associated credentials
90	* [mimikatz](http://blog.gentilkiwi.com/mimikatz) - Credentials extraction tool for Windows OS

91	* [PowerSploit](https://github.com/PowerShellMafia/PowerSploit) - A PowerShell Post-Exploitation Framework
92	* [Windows Exploit Suggester](https://github.com/GDSSecurity/Windows-Exploit-Suggester) - Detects potential missing patches on the target
93	* [Responder](https://github.com/SpiderLabs/Responder) - A LLMNR, NBT-NS and MDNS poisoner
94	* [Empire](https://github.com/PowerShellEmpire/Empire) - Empire is a pure PowerShell post-exploitation agent
95	**#### Linux Utils**
96	* [Linux Exploit Suggester](https://github.com/PenturaLabs/Linux_Exploit_Suggester) - Linux Exploit Suggester; based on operating system release number.
97	**#### DDoS Tools**
98	* [LOIC](https://github.com/NewEraCracker/LOIC/) - An open source network stress tool for Windows
99	* [JS LOIC](http://metacortexsecurity.com/tools/anon/LOIC/LOICv1.html) - JavaScript in-browser version of LOIC
100	* [T50](http://sourceforge.net/projects/t50/) - The more fast network stress tool
101	**#### Social Engineering Tools**
102	* [SET](https://github.com/trustedsec/social-engineer-toolkit) - The Social-Engineer Toolkit from TrustedSec
103	**#### OSInt Tools**
104	* [Maltego](http://www.paterva.com/web6/products/maltego.php) - Proprietary software for open source intelligence and forensics, from Paterva.
105	* [theHarvester](https://github.com/laramies/theHarvester) - E-mail, subdomain and people names harvester
106	* [creepy](https://github.com/ilektrojohn/creepy) - A geolocation OSINT tool
107	* [metagoofil](https://github.com/laramies/metagoofil) - Metadata harvester
108	* [Google Hacking Database](https://www.exploit-db.com/google-hacking-database/) - a database of Google dorks; can be used for recon
109	* [Shodan](https://www.shodan.io/) - Shodan is the world's first search engine for Internet-connected devices
110	* [recon-ng](https://bitbucket.org/LaNMaSteR53/recon-ng) - A full-featured Web Reconnaissance framework written in Python
111	**#### Anonymity Tools**
112	* [Tor](https://www.torproject.org/) - The free software for enabling onion routing online anonymity

113	* [I2P](https://geti2p.net) - The Invisible Internet Project
114	* [Nipe](https://github.com/HeitorG/nipe) - Script to redirect all traffic from the machine to the Tor network.
115	**#### Reverse Engineering Tools**
116	* [IDA Pro](https://www.hex-rays.com/products/ida/) - A Windows, Linux or Mac OS X hosted multi-processor disassembler and debugger
117	* [IDA Free](https://www.hex-rays.com/products/ida/support/download_freeware.shtml) - The freeware version of IDA v5.0
118	* [WDK/WinDbg](http://msdn.microsoft.com/en-us/windows/hardware/hh852365.aspx) - Windows Driver Kit and WinDbg
119	* [OllyDbg](http://www.ollydbg.de/) - An x86 debugger that emphasizes binary code analysis
120	* [Radare2](http://rada.re/r/index.html) - Opensource, crossplatform reverse engineering framework.
121	* [x64_dbg](http://x64dbg.com/) - An open-source x64/x32 debugger for windows.
122	* [Pyew](http://code.google.com/p/pyew/) - A Python tool for static malware analysis.
123	* [Bokken](https://inguma.eu/projects/bokken) - GUI for Pyew Radare2.
124	* [Immunity Debugger](http://debugger.immunityinc.com/) - A powerful new way to write exploits and analyze malware
125	* [Evan's Debugger](http://www.codef00.com/projects#debugger) - OllyDbg-like debugger for Linux
126	* [Medusa disassembler](https://github.com/wisk/medusa) - An open source interactive disassembler
127	* [plasma](https://github.com/joelpx/plasma) - Interactive disassembler for x86/ARM/MIPS. Generates indented pseudo-code with colored syntax code.
128	**#### CTF Tools**
129	* [Pwntools](https://github.com/Gallopsled/pwntools) - CTF framework for use in CTFs
130	**#### Penetration Testing Books**
131	* [The Art of Exploitation by Jon Erickson, 2008](http://www.nostarch.com/hacking2.htm)
132	* [Metasploit: The Penetration Tester's Guide by David Kennedy et al., 2011](http://www.nostarch.com/metasploit)
133	* [Penetration Testing: A Hands-On Introduction to Hacking by Georgia Weidman, 2014](http://www.nostarch.com/pentesting)
134	* [Rtfm: Red Team Field Manual by Ben Clark, 2014](http://www.amazon.com/Rtfm-Red-Team-Field-Manual/dp/1494295504/)
135	* [The Hacker Playbook by Peter Kim, 2014](http://www.amazon.com/The-Hacker-Playbook-Practical-Penetration/dp/1494932636/)

136	* [The Basics of Hacking and Penetration Testing by Patrick Engebretson, 2013](https://www.elsevier.com/books/the-basics-of-hacking-and-penetration-testing/engebretson/978-1-59749-655-1)
137	* [Professional Penetration Testing by Thomas Wilhelm, 2013](https://www.elsevier.com/books/professional-penetration-testing/wilhelm/978-1-59749-993-4)
138	* [Advanced Penetration Testing for Highly-Secured Environments by Lee Allen, 2012](http://www.packtpub.com/advanced-penetration-testing-for-highly-secured-environments/book)
139	* [Violent Python by TJ O'Connor, 2012](http://www.elsevier.com/books/violent-python/unknown/978-1-59749-957-6)
140	* [Fuzzing: Brute Force Vulnerability Discovery by Michael Sutton et al., 2007](http://www.fuzzing.org/)
141	* [Black Hat Python: Python Programming for Hackers and Pentesters by Justin Seitz, 2014](http://www.amazon.com/Black-Hat-Python-Programming-Pentesters/dp/1593275900)
142	* [Penetration Testing: Procedures & Methodologies by EC-Council, 2010](http://www.amazon.com/Penetration-Testing-Procedures-Methodologies-EC-Council/dp/1435483677)
143	* [Unauthorised Access: Physical Penetration Testing For IT Security Teams by Wil Allsopp, 2010](http://www.amazon.com/Unauthorised-Access-Physical-Penetration-Security-ebook/dp/B005DIAPKE)
144	* [Advanced Persistent Threat Hacking: The Art and Science of Hacking Any Organization by Tyler Wrightson, 2014](http://www.amazon.com/Advanced-Persistent-Threat-Hacking-Organization/dp/0071828362)
145	* [Bug Hunter's Diary by Tobias Klein, 2011](https://www.nostarch.com/bughunter)
146	**#### Hackers Handbook Series**
147	* [The Database Hacker's Handbook, David Litchfield et al., 2005](http://wiley.com/WileyCDA/WileyTitle/productCd-0764578014.html)
148	* [The Shellcoders Handbook by Chris Anley et al., 2007](http://wiley.com/WileyCDA/WileyTitle/productCd-047008023X.html)
149	* [The Mac Hacker's Handbook by Charlie Miller & Dino Dai Zovi, 2009](http://wiley.com/WileyCDA/WileyTitle/productCd-0470395362.html)
150	* [The Web Application Hackers Handbook by D. Stuttard, M. Pinto, 2011](http://wiley.com/WileyCDA/WileyTitle/productCd-1118026470.html)
151	* [iOS Hackers Handbook by Charlie Miller et al., 2012](http://wiley.com/WileyCDA/WileyTitle/productCd-1118204123.html)
152	* [Android Hackers Handbook by Joshua J. Drake et al., 2014](http://wiley.com/WileyCDA/WileyTitle/productCd-111860864X.html)
153	* [The Browser Hackers Handbook by Wade Alcorn et al., 2014](http://wiley.com/WileyCDA/WileyTitle/productCd-1118662091.html)
154	* [The Mobile Application Hackers Handbook by Dominic Chell et al., 2015](http://wiley.com/WileyCDA/WileyTitle/productCd-1118958500.html)
155	* [Car Hacker's Handbook by Craig Smith, 2016](https://www.nostarch.com/carhacking)

156	#### **Network Analysis Books**
157	* [Nmap Network Scanning by Gordon Fyodor Lyon, 2009](http://nmap.org/book/)
158	* [Practical Packet Analysis by Chris Sanders, 2011](http://www.nostarch.com/packet2.htm)
159	* [Wireshark Network Analysis by by Laura Chappell & Gerald Combs, 2012](http://www.wiresharkbook.com/)
160	* [Network Forensics: Tracking Hackers through Cyberspace by Sherri Davidoff & Jonathan Ham, 2012](http://www.amazon.com/Network-Forensics-Tracking-Hackers-Cyberspace-ebook/dp/B008CG8CYU/)
161	#### **Reverse Engineering Books**
162	* [Reverse Engineering for Beginners by Dennis Yurichev](http://beginners.re/)
163	* [Hacking the Xbox by Andrew Huang, 2003](https://www.nostarch.com/xbox.htm)
164	* [The IDA Pro Book by Chris Eagle, 2011](http://www.nostarch.com/idapro2.htm)
165	* [Practical Reverse Engineering by Bruce Dang et al., 2014](http://wiley.com/WileyCDA/WileyTitle/productCd-1118787315.html)
166	* [Gray Hat Hacking The Ethical Hacker's Handbook by Daniel Regalado et al., 2015](http://www.amazon.com/Hacking-Ethical-Hackers-Handbook-Edition/dp/0071832386)
167	#### **Malware Analysis Books**
168	* [Practical Malware Analysis by Michael Sikorski & Andrew Honig, 2012](http://www.nostarch.com/malware)
169	* [The Art of Memory Forensics by Michael Hale Ligh et al., 2014](http://wiley.com/WileyCDA/WileyTitle/productCd-1118825098.html)
170	* [Malware Analyst's Cookbook and DVD by Michael Hale Ligh et al., 2010](http://www.wiley.com/WileyCDA/WileyTitle/productCd-0470613033.html)
171	#### **Windows Books**
172	* [Windows Internals by Mark Russinovich et al., 2012](http://www.amazon.com/Windows-Internals-Part-Developer-Reference/dp/0735648735/)
173	#### **Social Engineering Books**
174	* [The Art of Deception by Kevin D. Mitnick & William L. Simon, 2002](http://wiley.com/WileyCDA/WileyTitle/productCd-0471237124.html)
175	* [The Art of Intrusion by Kevin D. Mitnick & William L. Simon, 2005](http://wiley.com/WileyCDA/WileyTitle/productCd-0764569597.html)
176	* [Ghost in the Wires by Kevin D. Mitnick & William L. Simon, 2011](http://www.hachettebookgroup.com/titles/kevin-mitnick/ghost-in-the-wires/9780316134477/)
177	* [No Tech Hacking by Johnny Long & Jack Wiles, 2008](http://www.elsevier.com/books/no-tech-hacking/mitnick/978-1-59749-215-7)

178	* [Social Engineering: The Art of Human Hacking by Christopher Hadnagy, 2010](http://wiley.com/WileyCDA/WileyTitle/productCd-0470639539.html)
179	* [Unmasking the Social Engineer: The Human Element of Security by Christopher Hadnagy, 2014](http://wiley.com/WileyCDA/WileyTitle/productCd-1118608577.html)
180	* [Social Engineering in IT Security: Tools, Tactics, and Techniques by Sharon Conheady, 2014](http://www.mhprofessional.com/product.php?isbn=0071818464)
181	**#### Lock Picking Books**
182	* [Practical Lock Picking by Deviant Ollam, 2012](https://www.elsevier.com/books/practical-lock-picking/ollam/978-1-59749-989-7)
183	* [Keys to the Kingdom by Deviant Ollam, 2012](https://www.elsevier.com/books/keys-to-the-kingdom/ollam/978-1-59749-983-5)
184	* [CIA Lock Picking Field Operative Training Manual](http://www.scribd.com/doc/7207/CIA-Lock-Picking-Field-Operative-Training-Manual)
185	* [Lock Picking: Detail Overkill by Solomon](https://www.dropbox.com/s/y39ix9u9qpqffct/Lockpicking%20Detail%20Overkill.pdf?dl=0)
186	* [Eddie the Wire books](https://www.dropbox.com/sh/k3z4dm4vyyojp3o/AAAIXQuwMmNuCch_StLPUYm-a?dl=0)
187	**### Vulnerability Databases**
188	* [NVD](http://nvd.nist.gov/) - US National Vulnerability Database
189	* [CERT](http://www.us-cert.gov/) - US Computer Emergency Readiness Team
190	* [OSVDB](http://osvdb.org/) - Open Sourced Vulnerability Database
191	* [Bugtraq](http://www.securityfocus.com/) - Symantec SecurityFocus
192	* [Exploit-DB](http://www.exploit-db.com/) - Offensive Security Exploit Database
193	* [Fulldisclosure](http://seclists.org/fulldisclosure/) - Full Disclosure Mailing List
194	* [MS Bulletin](https://technet.microsoft.com/security/bulletin/) - Microsoft Security Bulletin
195	* [MS Advisory](https://technet.microsoft.com/security/advisory/) - Microsoft Security Advisories
196	* [Inj3ct0r](http://1337day.com/) - Inj3ct0r Exploit Database
197	* [Packet Storm](http://packetstormsecurity.com/) - Packet Storm Global Security Resource
198	* [SecuriTeam](http://www.securiteam.com/) - Securiteam Vulnerability Information
199	* [CXSecurity](http://cxsecurity.com/) - CSSecurity Bugtraq List

200	* [Vulnerability Laboratory](http://www.vulnerability-lab.com/) - Vulnerability Research Laboratory
201	* [ZDI](http://www.zerodayinitiative.com/) - Zero Day Initiative
202	**### Security Courses**
203	* [Offensive Security Training](http://www.offensive-security.com/information-security-training/) - Training from BackTrack/Kali developers
204	* [SANS Security Training](http://www.sans.org/) - Computer Security Training & Certification
205	* [Open Security Training](http://opensecuritytraining.info/) - Training material for computer security classes
206	* [CTF Field Guide](https://trailofbits.github.io/ctf/) - everything you need to win your next CTF competition
207	* [Cybrary](https://www.cybrary.it/) - online IT and Cyber Security training platform
208	**### Information Security Conferences**
209	* [DEF CON](https://www.defcon.org/) - An annual hacker convention in Las Vegas
210	* [Black Hat](http://www.blackhat.com/) - An annual security conference in Las Vegas
211	* [BSides](http://www.securitybsides.com/) - A framework for organising and holding security conferences
212	* [CCC](http://events.ccc.de/congress/) - An annual meeting of the international hacker scene in Germany
213	* [DerbyCon](https://www.derbycon.com/) - An annual hacker conference based in Louisville
214	* [PhreakNIC](http://phreaknic.info/) - A technology conference held annually in middle Tennessee
215	* [ShmooCon](http://www.shmoocon.org/) - An annual US east coast hacker convention
216	* [CarolinaCon](http://www.carolinacon.org/) - An infosec conference, held annually in North Carolina
217	* [HOPE](http://hope.net/) - A conference series sponsored by the hacker magazine 2600
218	* [SummerCon](http://www.summercon.org/) - One of the oldest hacker conventions, held during Summer
219	* [Hack.lu](http://hack.lu/) - An annual conference held in Luxembourg
220	* [HITB](http://conference.hitb.org/) - Deep-knowledge security conference held in Malaysia and The Netherlands
221	* [Troopers](https://www.troopers.de) - Annual international IT Security event with workshops held in Heidelberg, Germany
222	* [Hack3rCon](http://hack3rcon.org/) - An annual US hacker conference

223	* [ThotCon](http://thotcon.org/) - An annual US hacker conference held in Chicago
224	* [LayerOne](http://www.layerone.org/) - An annual US security conference held every spring in Los Angeles
225	* [DeepSec](https://deepsec.net/) - Security Conference in Vienna, Austria
226	* [SkyDogCon](http://www.skydogcon.com/) - A technology conference in Nashville
227	* [SECUINSIDE](http://secuinside.com) - Security Conference in [Seoul](http://en.wikipedia.org/wiki/Seoul)
228	* [DefCamp](http://defcamp.ro) - Largest Security Conference in Eastern Europe, held anually in Bucharest, Romania
229	* [AppSecUSA](https://appsecusa.org/) - An annual conference organised by OWASP
230	* [BruCON](http://brucon.org) - An annual security conference in Belgium
231	* [Infosecurity Europe](http://www.infosecurityeurope.com/) - Europe's number one information security event, held in London, UK
232	* [Nullcon](http://nullcon.net/website/) - An annual conference in Delhi and Goa, India
233	* [RSA Conference USA](http://www.rsaconference.com/) - An annual security conference in San Francisco, California, USA
234	* [Swiss Cyber Storm](https://www.swisscyberstorm.com/) - An annual security conference in Lucerne, Switzerland
235	* [Virus Bulletin Conference](https://www.virusbtn.com/conference/index) - An annual conference going to be held in Denver, USA for 2016
236	* [Ekoparty](http://www.ekoparty.org) - Largest Security Conference in Latin America, held annually in Buenos Aires, Argentina
237	* [44Con](http://44con.com/) - Annual Security Conference held in London
238	**### Information Security Magazines**
239	* [2600: The Hacker Quarterly](http://www.2600.com/Magazine/DigitalEditions) - An American publication about technology and computer "underground"
240	* [Phrack Magazine](http://www.phrack.org/) - By far the longest running hacker zine
241	**### Awesome Lists**
242	* [Kali Linux Tools](http://tools.kali.org/tools-listing) - List of tools present in Kali Linux
243	* [SecTools](http://sectools.org/) - Top 125 Network Security Tools
244	* [C/C++ Programming](https://github.com/fffaraz/awesome-cpp) - One of the main language for open source security tools
245	* [.NET Programming](https://github.com/quozd/awesome-dotnet) - A software framework for Microsoft Windows platform development

246	* [Shell Scripting](https://github.com/alebcay/awesome-shell) - Command-line frameworks, toolkits, guides and gizmos
247	* [Ruby Programming by @dreikanter](https://github.com/dreikanter/ruby-bookmarks) - The de-facto language for writing exploits
248	* [Ruby Programming by @markets](https://github.com/markets/awesome-ruby) - The de-facto language for writing exploits
249	* [Ruby Programming by @Sdogruyol](https://github.com/Sdogruyol/awesome-ruby) - The de-facto language for writing exploits
250	* [JavaScript Programming](https://github.com/sorrycc/awesome-javascript) - In-browser development and scripting
251	* [Node.js Programming by @sindresorhus](https://github.com/sindresorhus/awesome-nodejs) - JavaScript in command-line
252	* [Node.js Programming by @vndmtrx](https://github.com/vndmtrx/awesome-nodejs) - JavaScript in command-line
253	* [Python tools for penetration testers](https://github.com/dloss/python-pentest-tools) - Lots of pentesting tools are written in Python
254	* [Python Programming by @svaksha](https://github.com/svaksha/pythonidae) - General Python programming
255	* [Python Programming by @vinta](https://github.com/vinta/awesome-python) - General Python programming
256	* [Android Security](https://github.com/ashishb/android-security-awesome) - A collection of android security related resources
257	* [Awesome Awesomness](https://github.com/bayandin/awesome-awesomeness) - The List of the Lists
258	* [AppSec](https://github.com/paragonie/awesome-appsec) - Resources for learning about application security
259	* [CTFs](https://github.com/apsdehal/awesome-ctf) - Capture The Flag frameworks, libraries, etc
260	* [Hacking](https://github.com/carpedm20/awesome-hacking) - Tutorials, tools, and resources
261	* [Honeypots](https://github.com/paralax/awesome-honeypots) - Honeypots, tools, components, and more
262	* [Infosec](https://github.com/onlurking/awesome-infosec) - Information security resources for pentesting, forensics, and more
263	* [Malware Analysis](https://github.com/rshipp/awesome-malware-analysis) - Tools and resources for analysts
264	* [PCAP Tools](https://github.com/caesar0301/awesome-pcaptools) - Tools for processing network traffic
265	* [Security](https://github.com/sbilly/awesome-security) - Software, libraries, documents, and other resources
266	* [Awesome List](https://github.com/sindresorhus/awesome) - A curated list of awesome lists
267	* [SecLists](https://github.com/danielmiessler/SecLists) - Collection of multiple types of lists used during security assessments
268	* [Security Talks](https://github.com/PaulSec/awesome-sec-talks) - A curated list of security conferences

269	**### Security Blogs To Follow/Subscribe**
270	*[Web Application Security]]http://rootme.in/
271	Blackhills Information Security
272	Corelan
273	Gotham Digital
274	MWR
275	NCC Group
276	Netspi
277	Nettitude
278	NotSoSecure
279	Portcullis
280	PortSwigger
281	Rapid7
282	Secforce
283	SensePost
284	Tenable
285	TrustedSec
286	Trustwave
287	Bernardo Damele
288	Carnal0wnage
289	Christopher Truncer
290	CommonExploits
291	Cyberarms

292	Darknet
293	Darkoperator
294	Didier Stevens
295	DigiNinja
296	Enigma
297	g0tmi1k
298	harmj0y
299	Irongeek
300	Lab of a penetration tester
301	ObscureSecurity
302	Pentestacademy
303	Pentestgeek
304	Pentestlab
305	Pentestmonkey
306	Pentestn00b
307	phillips321
308	Room362
309	scriptjunkie
310	Skullsecurity
311	Cloud Security - http://threatresponse.cloud/
312	Curated list of aweosome things - http://awesomelists.top/