sbilly / awesome-security

Watch 263 | Star 2,830 | Fork 529

<> Code | Issues 1 | Pull requests 1 | Projects 0 | Insights

A collection of awesome software, libraries, documents, books, resources and cools stuffs about security.

security awesome-list

212 commits | 1 branch | 0 releases | 48 contributors | MIT

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

sbilly Merge pull request #95 from kai5263499/master … Latest commit 807bc52 2 days ago

LICENSE	Initial commit	4 years ago

README.md	Add awesome container security link to other security awesome lists	2 days ago
contributing.md	Add a file. From https://github.com/sindresorhus/awesome	3 years ago

README.md

Awesome Security

A collection of awesome software, libraries, documents, books, resources and cool stuff about security.

Inspired by awesome-php, awesome-python.

Thanks to all contributors, you're awesome and wouldn't be possible without you! The goal is to build a categorized community-driven collection of very well-known resources.

Network

Scanning / Pentesting

- OpenVAS - OpenVAS is a framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution.
- Metasploit Framework - A tool for developing and executing exploit code against a remote target machine. Other important sub-projects include the Opcode Database, shellcode archive and related research.
- Kali - Kali Linux is a Debian-derived Linux distribution designed for digital forensics and penetration testing. Kali Linux is preinstalled with numerous penetration-testing programs, including nmap (a port scanner), Wireshark (a packet analyzer), John the Ripper (a password cracker), and Aircrack-ng (a software suite for penetration-testing wireless LANs).
- pig - A Linux packet crafting tool.
- scapy - Scapy: the python-based interactive packet manipulation program & library.
- Pompem - Pompem is an open source tool, which is designed to automate the search for exploits in major databases. Developed in Python, has a system of advanced search, thus facilitating the work of pentesters and ethical hackers. In its current version, performs searches in databases: Exploit-db, 1337day, Packetstorm Security...
- Nmap - Nmap is a free and open source utility for network discovery and security auditing.

- Amass - Amass performs DNS subdomain enumeration by scraping the largest number of disparate data sources, recursive brute forcing, crawling of web archives, permuting and altering names, reverse DNS sweeping and other techniques.

Monitoring / Logging

- justniffer - Justniffer is a network protocol analyzer that captures network traffic and produces logs in a customized way, can emulate Apache web server log files, track response times and extract all "intercepted" files from the HTTP traffic.
- httpry - httpry is a specialized packet sniffer designed for displaying and logging HTTP traffic. It is not intended to perform analysis itself, but to capture, parse, and log the traffic for later analysis. It can be run in real-time displaying the traffic as it is parsed, or as a daemon process that logs to an output file. It is written to be as lightweight and flexible as possible, so that it can be easily adaptable to different applications.
- ngrep - ngrep strives to provide most of GNU grep's common features, applying them to the network layer. ngrep is a pcap-aware tool that will allow you to specify extended regular or hexadecimal expressions to match against data payloads of packets. It currently recognizes IPv4/6, TCP, UDP, ICMPv4/6, IGMP and Raw across Ethernet, PPP, SLIP, FDDI, Token Ring and null interfaces, and understands BPF filter logic in the same fashion as more common packet sniffing tools, such as tcpdump and snoop.
- passivedns - A tool to collect DNS records passively to aid Incident handling, Network Security Monitoring (NSM) and general digital forensics. PassiveDNS sniffs traffic from an interface or reads a pcap-file and outputs the DNS-server answers to a log file. PassiveDNS can cache/aggregate duplicate DNS answers in-memory, limiting the amount of data in the logfile without loosing the essens in the DNS answer.
- sagan - Sagan uses a 'Snort like' engine and rules to analyze logs (syslog/event log/snmptrap/netflow/etc).
- Node Security Platform - Similar feature set to Snyk, but free in most cases, and very cheap for others.
- ntopng - Ntopng is a network traffic probe that shows the network usage, similar to what the popular top Unix command does.
- Fibratus - Fibratus is a tool for exploration and tracing of the Windows kernel. It is able to capture the most of the Windows kernel activity - process/thread creation and termination, file system I/O, registry, network activity, DLL

loading/unloading and much more. Fibratus has a very simple CLI which encapsulates the machinery to start the kernel event stream collector, set kernel event filters or run the lightweight Python modules called filaments.

IDS / IPS / Host IDS / Host IPS

- Snort - Snort is a free and open source network intrusion prevention system (NIPS) and network intrusion detection system (NIDS)created by Martin Roesch in 1998. Snort is now developed by Sourcefire, of which Roesch is the founder and CTO. In 2009, Snort entered InfoWorld's Open Source Hall of Fame as one of the "greatest [pieces of] open source software of all time".
- Bro - Bro is a powerful network analysis framework that is much different from the typical IDS you may know.
- OSSEC - Comprehensive Open Source HIDS. Not for the faint of heart. Takes a bit to get your head around how it works. Performs log analysis, file integrity checking, policy monitoring, rootkit detection, real-time alerting and active response. It runs on most operating systems, including Linux, MacOS, Solaris, HP-UX, AIX and Windows. Plenty of reasonable documentation. Sweet spot is medium to large deployments.
- Suricata - Suricata is a high performance Network IDS, IPS and Network Security Monitoring engine. Open Source and owned by a community run non-profit foundation, the Open Information Security Foundation (OISF). Suricata is developed by the OISF and its supporting vendors.
- Security Onion - Security Onion is a Linux distro for intrusion detection, network security monitoring, and log management. It's based on Ubuntu and contains Snort, Suricata, Bro, OSSEC, Sguil, Squert, Snorby, ELSA, Xplico, NetworkMiner, and many other security tools. The easy-to-use Setup wizard allows you to build an army of distributed sensors for your enterprise in minutes!
- sshwatch - IPS for SSH similar to DenyHosts written in Python. It also can gather information about attacker during the attack in a log.
- Stealth - File integrity checker that leaves virtually no sediment. Controller runs from another machine, which makes it hard for an attacker to know that the file system is being checked at defined pseudo random intervals over SSH. Highly recommended for small to medium deployments.

- AIEngine - AIEngine is a next generation interactive/programmable Python/Ruby/Java/Lua packet inspection engine with capabilities of learning without any human intervention, NIDS(Network Intrusion Detection System) functionality, DNS domain classification, network collector, network forensics and many others.
- Denyhosts - Thwart SSH dictionary based attacks and brute force attacks.
- Fail2Ban - Scans log files and takes action on IPs that show malicious behavior.
- SSHGuard - A software to protect services in addition to SSH, written in C
- Lynis - an open source security auditing tool for Linux/Unix.

Honey Pot / Honey Net

- awesome-honeypots - The canonical awesome honeypot list.
- HoneyPy - HoneyPy is a low to medium interaction honeypot. It is intended to be easy to: deploy, extend functionality with plugins, and apply custom configurations.
- Dionaea - Dionaea is meant to be a nepenthes successor, embedding python as scripting language, using libemu to detect shellcodes, supporting ipv6 and tls.
- Conpot - ICS/SCADA Honeypot. Conpot is a low interactive server side Industrial Control Systems honeypot designed to be easy to deploy, modify and extend. By providing a range of common industrial control protocols we created the basics to build your own system, capable to emulate complex infrastructures to convince an adversary that he just found a huge industrial complex. To improve the deceptive capabilities, we also provided the possibility to server a custom human machine interface to increase the honeypots attack surface. The response times of the services can be artificially delayed to mimic the behaviour of a system under constant load. Because we are providing complete stacks of the protocols, Conpot can be accessed with productive HMI's or extended with real hardware. Conpot is developed under the umbrella of the Honeynet Project and on the shoulders of a couple of very big giants.
- Amun - Amun Python-based low-interaction Honeypot.
- Glastopf - Glastopf is a Honeypot which emulates thousands of vulnerabilities to gather data from attacks targeting web applications. The principle behind it is very simple: Reply the correct response to the attacker exploiting the web application.

- Kippo - Kippo is a medium interaction SSH honeypot designed to log brute force attacks and, most importantly, the entire shell interaction performed by the attacker.
- Kojoney - Kojoney is a low level interaction honeypot that emulates an SSH server. The daemon is written in Python using the Twisted Conch libraries.
- HonSSH - HonSSH is a high-interaction Honey Pot solution. HonSSH will sit between an attacker and a honey pot, creating two separate SSH connections between them.
- Bifrozt - Bifrozt is a NAT device with a DHCP server that is usually deployed with one NIC connected directly to the Internet and one NIC connected to the internal network. What differentiates Bifrozt from other standard NAT devices is its ability to work as a transparent SSHv2 proxy between an attacker and your honeypot. If you deployed an SSH server on Bifrozt's internal network it would log all the interaction to a TTY file in plain text that could be viewed later and capture a copy of any files that were downloaded. You would not have to install any additional software, compile any kernel modules or use a specific version or type of operating system on the internal SSH server for this to work. It will limit outbound traffic to a set number of ports and will start to drop outbound packets on these ports when certain limits are exceeded.
- HoneyDrive - HoneyDrive is the premier honeypot Linux distro. It is a virtual appliance (OVA) with Xubuntu Desktop 12.04.4 LTS edition installed. It contains over 10 pre-installed and pre-configured honeypot software packages such as Kippo SSH honeypot, Dionaea and Amun malware honeypots, Honeyd low-interaction honeypot, Glastopf web honeypot and Wordpot, Conpot SCADA/ICS honeypot, Thug and PhoneyC honeyclients and more. Additionally it includes many useful pre-configured scripts and utilities to analyze, visualize and process the data it can capture, such as Kippo-Graph, Honeyd-Viz, DionaeaFR, an ELK stack and much more. Lastly, almost 90 well-known malware analysis, forensics and network monitoring related tools are also present in the distribution.
- Cuckoo Sandbox - Cuckoo Sandbox is an Open Source software for automating analysis of suspicious files. To do so it makes use of custom components that monitor the behavior of the malicious processes while running in an isolated environment.
- T-Pot Honeypot Distro - T-Pot is based on the network installer of Ubuntu Server 16/17.x LTS. The honeypot daemons as well as other support components being used have been containerized using docker. This allows us to run multiple honeypot daemons on the same network interface while maintaining a small footprint and constrain each honeypot within

its own environment. Installation over vanilla Ubuntu - T-Pot Autoinstall - This script will install T-Pot 16.04/17.10 on a fresh Ubuntu 16.04.x LTS (64bit). It is intended to be used on hosted servers, where an Ubuntu base image is given and there is no ability to install custom ISO images. Successfully tested on vanilla Ubuntu 16.04.3 in VMware.

Full Packet Capture / Forensic

- tcpflow - tcpflow is a program that captures data transmitted as part of TCP connections (flows), and stores the data in a way that is convenient for protocol analysis and debugging. Each TCP flow is stored in its own file. Thus, the typical TCP flow will be stored in two files, one for each direction. tcpflow can also process stored 'tcpdump' packet flows.
- Xplico - The goal of Xplico is extract from an internet traffic capture the applications data contained. For example, from a pcap file Xplico extracts each email (POP, IMAP, and SMTP protocols), all HTTP contents, each VoIP call (SIP), FTP, TFTP, and so on. Xplico isn’t a network protocol analyzer. Xplico is an open source Network Forensic Analysis Tool (NFAT).
- Moloch - Moloch is an open source, large scale IPv4 packet capturing (PCAP), indexing and database system. A simple web interface is provided for PCAP browsing, searching, and exporting. APIs are exposed that allow PCAP data and JSON-formatted session data to be downloaded directly. Simple security is implemented by using HTTPS and HTTP digest password support or by using apache in front. Moloch is not meant to replace IDS engines but instead work along side them to store and index all the network traffic in standard PCAP format, providing fast access. Moloch is built to be deployed across many systems and can scale to handle multiple gigabits/sec of traffic.
- OpenFPC - OpenFPC is a set of tools that combine to provide a lightweight full-packet network traffic recorder & buffering system. It's design goal is to allow non-expert users to deploy a distributed network traffic recorder on COTS hardware while integrating into existing alert and log management tools.
- Dshell - Dshell is a network forensic analysis framework. Enables rapid development of plugins to support the dissection of network packet captures.
- stenographer - Stenographer is a packet capture solution which aims to quickly spool all packets to disk, then provide simple, fast access to subsets of those packets.

Sniffer

- wireshark - Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Wireshark is very similar to tcpdump, but has a graphical front-end, plus some integrated sorting and filtering options.
- netsniff-ng - netsniff-ng is a free Linux networking toolkit, a Swiss army knife for your daily Linux network plumbing if you will. Its gain of performance is reached by zero-copy mechanisms, so that on packet reception and transmission the kernel does not need to copy packets from kernel space to user space and vice versa.
- Live HTTP headers - Live HTTP headers is a free firefox addon to see your browser requests in real time. It shows the entire headers of the requests and can be used to find the security loopholes in implementations.

Security Information & Event Management

- Prelude - Prelude is a Universal "Security Information & Event Management" (SIEM) system. Prelude collects, normalizes, sorts, aggregates, correlates and reports all security-related events independently of the product brand or license giving rise to such events; Prelude is "agentless".
- OSSIM - OSSIM provides all of the features that a security professional needs from a SIEM offering – event collection, normalization, and correlation.
- FIR - Fast Incident Response, a cybersecurity incident management platform.

VPN

- OpenVPN - OpenVPN is an open source software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. It uses a custom security protocol that utilizes SSL/TLS for key exchange.

Fast Packet Processing

- DPDK - DPDK is a set of libraries and drivers for fast packet processing.
- PFQ - PFQ is a functional networking framework designed for the Linux operating system that allows efficient packets capture/transmission (10G and beyond), in-kernel functional processing and packets steering across sockets/end-points.
- PF_RING - PF_RING is a new type of network socket that dramatically improves the packet capture speed.
- PF_RING ZC (Zero Copy) - PF_RING ZC (Zero Copy) is a flexible packet processing framework that allows you to achieve 1/10 Gbit line rate packet processing (both RX and TX) at any packet size. It implements zero copy operations including patterns for inter-process and inter-VM (KVM) communications.
- PACKET_MMAP/TPACKET/AF_PACKET - It's fine to use PACKET_MMAP to improve the performance of the capture and transmission process in Linux.
- netmap - netmap is a framework for high speed packet I/O. Together with its companion VALE software switch, it is implemented as a single kernel module and available for FreeBSD, Linux and now also Windows.

Firewall

- pfSense - Firewall and Router FreeBSD distribution.
- OPNsense - is an open source, easy-to-use and easy-to-build FreeBSD based firewall and routing platform. OPNsense includes most of the features available in expensive commercial firewalls, and more in many cases. It brings the rich feature set of commercial offerings with the benefits of open and verifiable sources.
- fwknop - Protects ports via Single Packet Authorization in your firewall.

Anti-Spam

- SpamAssassin - A powerful and popular email spam filter employing a variety of detection technique.

Docker Images for Penetration Testing & Security

- `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 remnux/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 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-compose build && docker-compose up` - OWASP NodeGoat
- `docker pull citizenstig/nowasp` - OWASP Mutillidae II Web Pen-Test Practice Application

Endpoint

Anti-Virus / Anti-Malware

- Linux Malware Detect - A malware scanner for Linux designed around the threats faced in shared hosted environments.

Content Disarm & Reconstruct

- DocBleach - An open-source Content Disarm & Reconstruct software sanitizing Office, PDF and RTF Documents.

Configuration Management

- Rudder - Rudder is an easy to use, web-driven, role-based solution for IT Infrastructure Automation & Compliance. Automate common system administration tasks (installation, configuration); Enforce configuration over time (configuring once is good, ensuring that configuration is valid and automatically fixing it is better); Inventory of all managed nodes; Web interface to configure and manage nodes and their configuration; Compliance reporting, by configuration and/or by node.

Authentication

- google-authenticator - The Google Authenticator project includes implementations of one-time passcode generators for several mobile platforms, as well as a pluggable authentication module (PAM). One-time passcodes are generated using open standards developed by the Initiative for Open Authentication (OATH) (which is unrelated to OAuth). These implementations support the HMAC-Based One-time Password (HOTP) algorithm specified in RFC 4226 and the Time-based One-time Password (TOTP) algorithm specified in RFC 6238. Tutorials: How to set up two-factor authentication for SSH login on Linux

Mobile / Android / iOS

- android-security-awesome - A collection of android security related resources. A lot of work is happening in academia and industry on tools to perform dynamic analysis, static analysis and reverse engineering of android apps.
- SecMobi Wiki - A collection of mobile security resources which including articles, blogs, books, groups, projects, tools and conferences. *
- OWASP Mobile Security Testing Guide - A comprehensive manual for mobile app security testing and reverse engineering.
- OSX Security Awesome - A collection of OSX and iOS security resources

Forensics

- grr - GRR Rapid Response is an incident response framework focused on remote live forensics.

- Volatility - Python based memory extraction and analysis framework.
- mig - MIG is a platform to perform investigative surgery on remote endpoints. It enables investigators to obtain information from large numbers of systems in parallel, thus accelerating investigation of incidents and day-to-day operations security.
- ir-rescue - *ir-rescue* is a Windows Batch script and a Unix Bash script to comprehensively collect host forensic data during incident response.
- Logdissect - CLI utility and Python API for analyzing log files and other data.

Threat Intelligence

- abuse.ch - ZeuS Tracker / SpyEye Tracker / Palevo Tracker / Feodo Tracker tracks Command&Control servers (hosts) around the world and provides you a domain- and an IP-blocklist.
- Emerging Threats - Open Source - Emerging Threats began 10 years ago as an open source community for collecting Suricata and SNORT® rules, firewall rules, and other IDS rulesets. The open source community still plays an active role in Internet security, with more than 200,000 active users downloading the ruleset daily. The ETOpen Ruleset is open to any user or organization, as long as you follow some basic guidelines. Our ETOpen Ruleset is available for download any time.
- PhishTank - PhishTank is a collaborative clearing house for data and information about phishing on the Internet. Also, PhishTank provides an open API for developers and researchers to integrate anti-phishing data into their applications at no charge.
- SBL / XBL / PBL / DBL / DROP / ROKSO - The Spamhaus Project is an international nonprofit organization whose mission is to track the Internet's spam operations and sources, to provide dependable realtime anti-spam protection for Internet networks, to work with Law Enforcement Agencies to identify and pursue spam and malware gangs worldwide, and to lobby governments for effective anti-spam legislation.
- Internet Storm Center - The ISC was created in 2001 following the successful detection, analysis, and widespread warning of the Li0n worm. Today, the ISC provides a free analysis and warning service to thousands of Internet users

and organizations, and is actively working with Internet Service Providers to fight back against the most malicious attackers.

- AutoShun - AutoShun is a Snort plugin that allows you to send your Snort IDS logs to a centralized server that will correlate attacks from your sensor logs with other snort sensors, honeypots, and mail filters from around the world.
- DNS-BH - The DNS-BH project creates and maintains a listing of domains that are known to be used to propagate malware and spyware. This project creates the Bind and Windows zone files required to serve fake replies to localhost for any requests to these, thus preventing many spyware installs and reporting.
- AlienVault Open Threat Exchange - AlienVault Open Threat Exchange (OTX), to help you secure your networks from data loss, service disruption and system compromise caused by malicious IP addresses.
- Tor Bulk Exit List - CollecTor, your friendly data-collecting service in the Tor network. CollecTor fetches data from various nodes and services in the public Tor network and makes it available to the world. If you're doing research on the Tor network, or if you're developing an application that uses Tor network data, this is your place to start. TOR Node List / DNS Blacklists / Tor Node List
- leakedin.com - The primary purpose of leakedin.com is to make visitors aware about the risks of loosing data. This blog just compiles samples of data lost or disclosed on sites like pastebin.com.
- FireEye OpenIOCs - FireEye Publicly Shared Indicators of Compromise (IOCs)
- OpenVAS NVT Feed - The public feed of Network Vulnerability Tests (NVTs). It contains more than 35,000 NVTs (as of April 2014), growing on a daily basis. This feed is configured as the default for OpenVAS.
- Project Honey Pot - Project Honey Pot is the first and only distributed system for identifying spammers and the spambots they use to scrape addresses from your website. Using the Project Honey Pot system you can install addresses that are custom-tagged to the time and IP address of a visitor to your site. If one of these addresses begins receiving email we not only can tell that the messages are spam, but also the exact moment when the address was harvested and the IP address that gathered it.
- virustotal - VirusTotal, a subsidiary of Google, is a free online service that analyzes files and URLs enabling the identification of viruses, worms, trojans and other kinds of malicious content detected by antivirus engines and website

scanners. At the same time, it may be used as a means to detect false positives, i.e. innocuous resources detected as malicious by one or more scanners.

- IntelMQ - IntelMQ is a solution for CERTs for collecting and processing security feeds, pastebins, tweets using a message queue protocol. It's a community driven initiative called IHAP (Incident Handling Automation Project) which was conceptually designed by European CERTs during several InfoSec events. Its main goal is to give to incident responders an easy way to collect & process threat intelligence thus improving the incident handling processes of CERTs. ENSIA Homepage.
- CIFv2 - CIF is a cyber threat intelligence management system. CIF allows you to combine known malicious threat information from many sources and use that information for identification (incident response), detection (IDS) and mitigation (null route).
- CriticalStack - Free aggregated threat intel for the Bro network security monitoring platform.
- MISP - Open Source Threat Intelligence Platform - MISP threat sharing platform is a free and open source software helping information sharing of threat intelligence including cyber security indicators. A threat intelligence platform for gathering, sharing, storing and correlating Indicators of Compromise of targeted attacks, threat intelligence, financial fraud information, vulnerability information or even counter-terrorism information. The MISP project includes software, common libraries (taxonomies, threat-actors and various malware), an extensive data model to share new information using objects and default feeds.

Web

Organization

- OWASP - The Open Web Application Security Project (OWASP) is a 501(c)(3) worldwide not-for-profit charitable organization focused on improving the security of software.

Web Application Firewall

- ModSecurity - ModSecurity is a toolkit for real-time web application monitoring, logging, and access control.
- NAXSI - NAXSI is an open-source, high performance, low rules maintenance WAF for NGINX, NAXSI means Nginx Anti Xss & Sql Injection.
- sql_firewall SQL Firewall Extension for PostgreSQL
- ironbee - IronBee is an open source project to build a universal web application security sensor. IronBee as a framework for developing a system for securing web applications - a framework for building a web application firewall (WAF).

Scanning / Pentesting

- sqlmap - sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.
- ZAP - The Zed Attack Proxy (ZAP) is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications. It is designed to be used by people with a wide range of security experience and as such is ideal for developers and functional testers who are new to penetration testing. ZAP provides automated scanners as well as a set of tools that allow you to find security vulnerabilities manually.
- OWASP Testing Checklist v4 - List of some controls to test during a web vulnerability assessment. Markdown version may be found here.
- w3af - w3af is a Web Application Attack and Audit Framework. The project’s goal is to create a framework to help you secure your web applications by finding and exploiting all web application vulnerabilities.
- Recon-ng - Recon-ng is a full-featured Web Reconnaissance framework written in Python. Recon-ng has a look and feel similar to the Metasploit Framework.
- PTF - The Penetration Testers Framework (PTF) is a way for modular support for up-to-date tools.
- Infection Monkey - A semi automatic pen testing tool for mapping/pen-testing networks. Simulates a human attacker.

- ACSTIS - ACSTIS helps you to scan certain web applications for AngularJS Client-Side Template Injection (sometimes referred to as CSTI, sandbox escape or sandbox bypass). It supports scanning a single request but also crawling the entire web application for the AngularJS CSTI vulnerability.

Runtime Application Self-Protection

- Sqreen - Sqreen is a Runtime Application Self-Protection (RASP) solution for software teams. An in-app agent instruments and monitors the app. Suspicious user activities are reported and attacks are blocked at runtime without code modification or traffic redirection.

Development

- Secure by Design - Book that identifies design patterns and coding styles that make lots of security vulnerabilities less likely. (early access, published continuously, final release fall 2017)
- Securing DevOps - Book that explores how the techniques of DevOps and Security should be applied together to make cloud services safer. (early access, published continuously, final release January 2018)
- Understanding API Security - Free eBook sampler that gives some context for how API security works in the real world by showing how APIs are put together and how the OAuth protocol can be used to protect them.
- OAuth 2 in Action - Book that teaches you practical use and deployment of OAuth 2 from the perspectives of a client, an authorization server, and a resource server.

Usability

- Usable Security Course - Usable Security course at coursera. Quite good for those looking for how security and usability intersects.

Big Data

- data_hacking - Examples of using IPython, Pandas, and Scikit Learn to get the most out of your security data.
- hadoop-pcap - Hadoop library to read packet capture (PCAP) files.
- Workbench - A scalable python framework for security research and development teams.
- OpenSOC - OpenSOC integrates a variety of open source big data technologies in order to offer a centralized tool for security monitoring and analysis.
- Apache Metron (incubating) - Metron integrates a variety of open source big data technologies in order to offer a centralized tool for security monitoring and analysis.
- Apache Spot (incubating) - Apache Spot is open source software for leveraging insights from flow and packet analysis.
- binarypig - Scalable Binary Data Extraction in Hadoop. Malware Processing and Analytics over Pig, Exploration through Django, Twitter Bootstrap, and Elasticsearch.

DevOps

- Securing DevOps - A book on Security techniques for DevOps that reviews state of the art practices used in securing web applications and their infrastructure.

Operating Systems

Online resources

- Security related Operating Systems @ Rawsec - Complete list of security related operating systems
- Best Linux Penetration Testing Distributions @ CyberPunk - Description of main penetration testing distributions
- Security @ Distrowatch - Website dedicated to talking about, reviewing and keeping up to date with open source operating systems

Datastores

- blackbox - Safely store secrets in a VCS repo using GPG
- confidant - Stores secrets in AWS DynamoDB, encrypted at rest and integrates with IAM
- dotgpg - A tool for backing up and versioning your production secrets or shared passwords securely and easily.
- redoctober - Server for two-man rule style file encryption and decryption.
- aws-vault - Store AWS credentials in the OSX Keychain or an encrypted file
- credstash - Store secrets using AWS KMS and DynamoDB
- chamber - Store secrets using AWS KMS and SSM Parameter Store
- dotgpg A tool for backing up and versioning your production secrets or shared passwords securely and easily.
- Safe - A Vault CLI that makes reading from and writing to the Vault easier to do.
- Sops - An editor of encrypted files that supports YAML, JSON and BINARY formats and encrypts with AWS KMS and PGP.
- passbolt - The password manager your team was waiting for. Free, open source, extensible, based on OpenPGP.
- passpie - Multiplatform command-line password manager
- Vault - An encrypted datastore secure enough to hold environment and application secrets.

EBooks

- Holistic Info-Sec for Web Developers - Free and downloadable book series with very broad and deep coverage of what Web Developers and DevOps Engineers need to know in order to create robust, reliable, maintainable and secure software, networks and other, that are delivered continuously, on time, with no nasty surprises
- Docker Security - Quick Reference: For DevOps Engineers - A book on understanding the Docker security defaults, how to improve them (theory and practical), along with many tools and techniques.

Other Awesome Lists

Other Security Awesome Lists

- Android Security Awesome - A collection of android security related resources.
- Awesome CTF - A curated list of CTF frameworks, libraries, resources and software.
- Awesome Cyber Skills - A curated list of hacking environments where you can train your cyber skills legally and safely.
- Awesome Hacking - A curated list of awesome Hacking tutorials, tools and resources.
- Awesome Honeypots - An awesome list of honeypot resources.
- Awesome Malware Analysis - A curated list of awesome malware analysis tools and resources.
- Awesome PCAP Tools - A collection of tools developed by other researchers in the Computer Science area to process network traces.
- Awesome Pentest - A collection of awesome penetration testing resources, tools and other shiny things.
- Awesome Linux Containers - A curated list of awesome Linux Containers frameworks, libraries and software.
- Awesome Incident Response - A curated list of resources for incident response.
- Awesome Web Hacking - This list is for anyone wishing to learn about web application security but do not have a starting point.
- Awesome Threat Intelligence - A curated list of threat intelligence resources.
- Awesome Pentest Cheat Sheets - Collection of the cheat sheets useful for pentesting
- Awesome Industrial Control System Security - A curated list of resources related to Industrial Control System (ICS) security.
- Awesome YARA - A curated list of awesome YARA rules, tools, and people.
- Awesome Threat Detection and Hunting - A curated list of awesome threat detection and hunting resources.
- Awesome Container Security - A curated list of awesome resources related to container building and runtime security

Other Common Awesome Lists

Other amazingly awesome lists:

- awesome-awesomeness - awesome-* or *-awesome lists.
- lists - The definitive list of (awesome) lists curated on GitHub.
- Movies For Hacker - A curated list of movies every hacker & cyberpunk must watch.

Contributing

Your contributions are always welcome!