- **GNU Bash** - ist eine sh-kompatible Shell, die nützliche Funktionen aus der Korn-Shell und der C-Shell enthält.
- **Zsh** - ist eine Shell für den interaktiven Einsatz, obwohl es auch eine leistungsstarke Skriptsprache ist.
- **tclsh** - ist eine sehr leistungsstarke plattformübergreifende Schale, die für eine Vielzahl von Anwendungen geeignet ist.
- **bash-it** - ist ein Framework für die Verwendung, Entwicklung und Wartung von Shell-Skripten und benutzerdefinierten Befehlen.
- **Oh My ZSH!** - ist das beste Framework für die Verwaltung Ihrer Zsh-Konfiguration.
- **Oh My Fish** - das Fishshell-Framework.
- **Starship** - die Inserat-Eingabeaufforderung in Rust.
- **powerlevel10k** - ist eine schnelle Neuimplementierung des Powerlevel9k ZSH-Themas.

▪ Shell-Plugins

- **z** - verfolgt den Ordner, den Sie am meisten verwenden, und ermöglicht es Ihnen, zu springen, ohne den gesamten Pfad eingeben zu müssen.
- **fzf** - ist ein allzweck-Befehlszeilen-Fuzzy-Finder.
- **zsh-autosuggestions** - Fischähnliche Autovorschläge für Zsh.
- **zsh-syntax-highlighting** - Fish-Shell wie Syntaxhervorhebung für Zsh.

▪ Manager

- **Midnight Commander** - ist ein visueller Dateimanager, lizenziert unter GNU General Public License.
- **Ranger** - ist ein VIM-inspirierter Dateimanager für die Konsole.
- **nnn** - ist ein winziger, blitzschneller, funktionsreicher Dateimanager.
- **Bildschirm** - ist ein Vollbild-Fenstermanager, der ein physisches Terminal vervielfacht.
- **tmux** - ist ein Terminal-Multiplexer, können Sie einfach zwischen mehreren Programmen in einem Terminal wechseln.
- **tmux-cssh** - ist ein Tool, um komfortable und einfach zu bedienende Funktionen, Clustering und Synchronisation von tmux-Sitzungen einzustellen.

▪ Texteditoren

- **vi** - ist einer der häufigsten Texteditoren auf Unix.
- **vim** - ist ein hochgradig konfigurierbarer Texteditor.
- **emacs** - ist ein erweiterbarer, anpassbarer, freier/libre Texteditor - und vieles mehr.
- **micro** - ist ein moderner und intuitiver terminalbasierter Texteditor.
- **neovim** - ist ein kostenloser Open Source, leistungsstarker, erweiterbarer und nutzbarer Code-Editor.
- **Spacemacs** - eine von der Community gesteuerte Emacs-Distribution.
- **spacevim** - eine community-gesteuerte Vim-Verteilung.

▪ Dateien und Verzeichnisse

- **fd** - ist eine einfache, schnelle und benutzerfreundliche Alternative zu finden.
- **ncdu** - ist ein einfach zu bedienender, schneller Festplattennutzungs-Analysator.

▪ Netzwerk

- **PuTTY** - ist ein SSH- und Telnet-Client, der ursprünglich von Simon Tatham entwickelt wurde.
- **Mosh** - ist ein SSH-Wrapper, der entwickelt wurde, um eine SSH-Sitzung über eine flüchtige Verbindung am Leben zu erhalten.
- **Eternal Terminal** - ermöglicht Mausscrolling und tmux Befehle innerhalb der SSH-Sitzung.
- **nmap** - ist ein kostenloses und Open Source (Lizenz) Dienstprogramm für Die Netzwerkermittlung und Sicherheitsüberwachung.
- **zmap** - ist ein schneller Einzelpaket-Netzwerkscanner, der für internetweite Netzwerkumfragen entwickelt wurde.
  - **-Masscan** - ist der schnellste Internet-Port-Scanner, spuckt SYN-Pakete asynchron aus.
- **pbscan** - ist ein schnellerer und effizienterer zustandsloser SYN-Scanner und Bannergreifer.
- **hping** - ist ein befehlszeilenorientierter TCP/IP-Paket-Assembler/Analyzer.
- **mtr** - ist ein Tool, das die Funktionalität der Programme "Traceroute" und "Ping" in einem einzigen Netzwerkdiagnosetool kombiniert.
- **mylg** - ist ein Open-Source-Dienstprogramm, das die Funktionen der verschiedenen Netzwerksonden in einem Diagnosetool vereint.
- **netcat** - ist ein Netzwerkdienstprogramm, das Daten über Netzwerkverbindungen hinweg liest und schreibt, indem es das TCP/IP-Protokoll verwendet.
- **tcpdump** - ist ein leistungsstarker Befehlszeilenpaketanalysator.
- **tshark** - ist ein Tool, mit dem wir den Netzwerkverkehr (wireshark cli) abladen und analysieren können.
- **Termshark** - ist eine einfache Terminal-Benutzeroberfläche für tshark.
- **ngrep** - ist wie GNU grep auf die Netzwerkschicht angewendet.
- **netsniff-ng** - ist ein Schweizer Taschenmesser für Ihr tägliches Linux-Netzwerk Sanitär, wenn Sie so wollen.
- **sockdump** - unix-Domänensocketverkehr absetzen.
- **Stenograph -** ist eine Paketerfassungslösung, die darauf abzielt, alle Pakete schnell auf die Festplatte zu spoolen.
- **tcpterm** - Visualisieren Sie Pakete in TUI.
- **bmon** - ist ein Überwachungs- und Debugging-Tool, um netzwerkbezogene Statistiken zu erfassen und visuell vorzubereiten.
- **iptraf-ng** - ist ein konsolenbasiertes Netzwerküberwachungsprogramm für Linux, das Informationen über IP-Datenverkehr anzeigt.
- **vnstat** - ist ein Netzwerk-Verkehrsmonitor für Linux und BSD.
- **iPerf3** - ist ein Werkzeug zur aktiven Messung der maximal erreichbaren Bandbreite in IP-Netzwerken.
- **ethr** - ist ein Network Performance Measurement Tool für TCP, UDP & HTTP.
- **Etherate** - ist ein Linux CLI-basiertes Ethernet- und MPLS-Verkehrstesttool.

- **Echoip** - ist ein IP-Adresssuchdienst.
- **Nemesis** - Paketmanipulation CLI-Tool; Handwerk und injizieren Pakete von mehreren Protokollen.
- **packetfu** - eine Bibliothek zur Paketmanipulation auf mittlerer Ebene für Ruby.
- **Scapy** - Paketmanipulationsbibliothek; schmieden, senden, dekodieren, Pakete einer Vielzahl von Protokollen erfassen.
- **impacket** - ist eine Sammlung von Python-Klassen für die Arbeit mit Netzwerkprotokollen.
- **ssh-audit** - ist ein Tool für die SSH-Serverüberwachung.
- **aria2** - ist ein leichtes Multiprotokoll- und Multi-Source-Befehlszeilen-Download-Dienstprogramm.
- **iptables-tracer** - beobachten Sie den Pfad von Paketen durch die iptables-Ketten.
- **-** ein hochgradig konfigurierbares Werkzeug, um gegen eine beliebige Anzahl von Hosts nach was auch immer Sie wollen.

▪ Netzwerk (DNS)

- **dnsdiag** - ist ein DNS-Diagnose- und Leistungsmesstool.
- **heftig** - ist ein DNS-Aufklärungstool, um nicht zusammenhängenden IP-Speicherplatz zu lokalisieren.
- **Subfinder** - ist ein Subdomain-Erkennungstool, das gültige Subdomains für Websites entdeckt.
- **sublist3r** - ist ein schnelles Subdomains-Enumerationstool für Penetrationstester.
- **anmasse** - ist ein Tool, das Subdomain-Namen durch Dasabkratzen von Datenquellen, Durchforsten von Webarchiven und mehr erhält.
- **namebench** - bietet personalisierte DNS-Serverempfehlungen basierend auf Ihrem Browserverlauf.
- **massdns** - ist ein leistungsstarker DNS-Stub-Resolver für Massensuch- und Aufklärungsflüge.
- **knock** - ist ein Tool, um Subdomains in einer Zieldomäne über eine Wortliste aufzulisten.
- **dnsperf** - DNS-Leistungstesttools.
- **dnscrypt-proxy 2** - ein flexibler DNS-Proxy mit Unterstützung für verschlüsselte DNS-Protokolle.
- **dnsdbq** - API-Client, der Zugriff auf passive DNS-Datenbanksysteme bietet (pDNS bei Farsight Security, CIRCL pDNS).
- **grimmig** - schnelle dns-Proxy, gebaut auf Black-Hole-Internet-Werbung und Malware-Server.

▪ Netzwerk (HTTP)

- **curl** - ist ein Befehlszeilentool und eine Bibliothek zum Übertragen von Daten mit URLs.
- **kurly** - ist eine Alternative zum weit verbreiteten Curl-Programm, geschrieben in Golang.
- **HTTPie** - ist ein benutzerfreundlicher HTTP-Client.
- **wuzz** - ist ein interaktives cli-Tool für die HTTP-Inspektion.
- **h2spec** - ist ein Konformitätstesttool für die HTTP/2-Implementierung.
- **h2t** - ist ein einfaches Tool, um Sysadmins zu helfen, ihre Websites zu härten.

◈ htrace.sh - ist ein einfaches Schweizer Taschenmesser für http/https Fehlerbehebung und Profilierung.
◈ httpstat - ist ein Werkzeug, das Curl-Statistiken in einer Art von Schönheit und Klarheit visualisiert.
◈ httplab - ist ein interaktiver Webserver.
◈ Lynx - ist ein Textbrowser für das World Wide Web.
◈ HeadlessBrowsers - eine Liste von (fast) allen kopflosen Webbrowsern.
◈ ab - ist ein Ein-Thread-Befehlszeilentool zur Messung der Leistung von HTTP-Webservern.
◈ Belagerung - ist ein http-Lasttest- und Benchmarking-Dienstprogramm.
◈ wrk - ist ein modernes HTTP-Benchmarking-Tool, das eine erhebliche Last erzeugen kann.
◈ wrk2 - ist eine konstante Durchsatz, korrekte Latenzaufnahme Variante von wrk.
◈ vegeta - ist eine konstante Durchsatz, korrekte Latenzaufnahme Variante von wrk.
◈ bombardier - ist ein schnelles plattformübergreifendes HTTP-Benchmarking-Tool, das in Go geschrieben wurde.
◈ gobench - http/https Load Testing and Benchmarking Tool.
◈ hey - HTTP-Lastgenerator, ApacheBench (ab) Ersatz, früher bekannt als rakyll/boom.
◈ Boom - ist ein Skript, mit dem Sie Ihre Web-App-Bereitstellung schnell verrauchen können.
◈ SlowHTTPTest - ist ein Tool, das einige Denial-of-Service-Angriffe auf Anwendungsebene simuliert, indem HTTP verlängert wird.
◈ gobuster - ist ein kostenloses und Open-Source-Verzeichnis/Datei & DNS-Busting-Tool in Go geschrieben.
◈ ssllabs-scan - Befehlszeilenreferenzimplementierungsclient für SSL Labs-APIs.
◈ http-observatory - Mozilla HTTP Observatory cli version.

▪ SSL

◈ openssl - ist ein robustes, kommerzielles und voll funktionsfähiges Toolkit für die TLS- und SSL-Protokolle.
◈ gnutls-cli - Client-Programm, um eine TLS-Verbindung zu einem anderen Computer einzurichten.
◈ sslyze - schnelle und leistungsstarke SSL/TLS-Server-Scan-Bibliothek.
◈ sslscan - testet SSL/TLS-fähige Dienste, um unterstützte Verschlüsselungssammlungen zu ermitteln.
◈ testssl.sh - TLS/SSL-Verschlüsselung überall auf jedem Port testen.
◈ Chiffrescan - eine sehr einfache Möglichkeit herauszufinden, welche SSL-Chiffresuites von einem Ziel unterstützt werden.
◈ spiped - ist ein Dienstprogramm zum Erstellen symmetrisch verschlüsselter und authentifizierter Pipes zwischen Socketadressen.
◈ Certbot - ist das Tool von EFF, um Zertifikate von Let es Encrypt zu erhalten und (optional) HTTPS auf Ihrem Server automatisch zu aktivieren.
◈ mkcert - einfaches Zero-Config-Tool, um lokal vertrauenswürdige Entwicklungszertifikate mit beliebigen Namen zu erstellen.
◈ - Tools zum Bootstrap-Zertifizierungsstellen, Zertifikatanforderungen und signierte Zertifikate.

◈ **Sublert** - ist ein Sicherheits- und Aufklärungstool, um neue Subdomains automatisch zu überwachen.
◈ **mkchain** - Open Source Tool, mit dem Sie eine gültige SSL-Zertifikatkette erstellen können.

▪ Sicherheit

◈ **SELinux** - bietet ein flexibles MANDATORY Access Control (MAC) System, das in den Linux-Kernel integriert ist.
◈ **AppArmor** - schützt das Betriebssystem und anwendungen proaktiv vor externen oder internen Bedrohungen.
◈ **grapheneX** - Automated System Hardening Framework.
◈ **DevSec Hardening Framework** - Security + DevOps: Automatic Server Hardening.

▪-Audit-Tools

◈ **ossec** - aktive Überwachung aller Aspekte der Systemaktivität mit Dateiintegritätsüberwachung.
◈ **auditd** - bietet eine Möglichkeit, sicherheitsrelevante Informationen auf Ihrem System nachzuverfolgen.
◈ **Tiger** - ist ein Sicherheitstool, das sowohl als Sicherheitsaudit als auch als Intrusion Detection System verwendet werden kann.
◈ **Lynis** - gefechtgeprüftes Sicherheitstool für Systeme mit Linux-, macOS- oder Unix-basiertem Betriebssystem.
◈ **LinEnum** - Skript-Lokale Linux-Enumeration & Privilege Escalation Checks.
◈ **Rkhunter** - Scanner-Tool für Linux-Systeme, das Hintertüren, Rootkits und lokale Exploits auf Ihren Systemen scannt.
◈ **PE-Sieb** - ist ein leichtes Werkzeug, das hilft, Malware auf dem System laufen zu erkennen.

▪ Systemdiagnose/Debugger

◈ **strace** - Diagnose, Debugging und Lehrbenutzerraum-Dienstprogramm für Linux.
◈ **DTrace** - ist ein Tool zur Leistungsanalyse und Fehlerbehebung.
◈ **ltrace** - ist ein Bibliotheksaufruf-Tracer, der verwendet wird, um Aufrufe von Programmen zu Bibliotheksfunktionen nachzuverfolgen.
◈ **ptrace-burrito** - ist ein freundlicher Wrapper um ptrace.
◈ **perf-tools** - Performance-Analyse-Tools basierend auf Linux perf_events (aka perf) und ftrace.
◈ **bpftrace** - High-Level-Tracing-Sprache für Linux eBPF.
◈ **sysdig** - Systemexplorations- und Fehlerbehebungstool mit erstklassiger Unterstützung für Container.
◈ **Valgrind** - ist ein Instrumentierungsrahmen für den Aufbau dynamischer Analysewerkzeuge.
◈ **gperftools** - leistungsstarke Multithread-Malloc()-Implementierung sowie einige Leistungsanalysetools.

◈ Blicke - plattformübergreifendes Systemüberwachungstool, das in Python geschrieben wurde.
◈ htop - interaktiver Textmodus-Prozessbetrachter für Unix-Systeme. Es zielt darauf ab, ein besseres "Top" zu sein.
◈ bashtop - Linux-Ressourcenmonitor in reinem Bash geschrieben.
◈ nmon - eine einzige ausführbare Datei für Leistungsüberwachung und Datenanalyse.
◈ oben - ASCII Leistungsmonitor. Enthält Statistiken für CPU, Arbeitsspeicher, Datenträger, Swap, Netzwerk und Prozesse.
◈ lsof - zeigt in seiner Ausgabe Informationen über Dateien an, die von Prozessen geöffnet werden.
◈ FlameGraph - Stack Trace Visualizer.
◈ lsofgraph - kleines Dienstprogramm, um die Unix-lsof-Ausgabe in ein Diagramm zu konvertieren, das DIE FIFO- und UNIX-Interprozesskommunikation anzeigt.
◈ rr - ist ein leichtes Werkzeug zum Aufzeichnen, Wiedergeben und Debuggen der Ausführung von Anwendungen.
◈ Performance Co-Pilot - ein Toolkit zur Systemleistungsanalyse.
◈ Hexyl - ein Befehlszeilen-Hex-Viewer.

▪ Log Analyzer

◈ Winkelschleifer - schneiden und würfeln Protokolldateien auf der Befehlszeile.
◈ lnav - Log-Datei-Navigator mit Suche und automatischer Aktualisierung.
◈ GoAccess - Echtzeit-Webprotokollanalysator und interaktiver Viewer, der in einem Terminal ausgeführt wird.
◈ ngxtop - Echtzeit-Metriken für nginx-Server.

▪ Datenbanken

◈ usql - universelle Befehlszeilenschnittstelle für SQL-Datenbanken.
◈ pgcli - postgres CLI mit Automatischer Vervollständigung und Syntaxhervorhebung.
◈ mycli - Terminalclient für MySQL mit automatischer Vervollständigung und Syntaxhervorhebung.
◈ litecli - SQLite CLI mit automatischer Vervollständigung und Syntaxhervorhebung.
◈ OSQuery - ist ein SQL-basiertes Betriebssysteminstrumentierungs-, Überwachungs- und Analyseframework.
◈ pgsync - synchronisieren Sie Daten aus einer Postgres-Datenbank mit einer anderen.
◈ iredis - ein Terminalclient für Redis mit automatischer Vervollständigung und Syntaxhervorhebung.

▪ TOR

◈ Nipe - Skript, um Tor Network zu Ihrem Standard-Gateway zu machen.
◈ Multitor - ein Tool, mit dem Sie mehrere TOR-Instanzen mit einem Lastenausgleich erstellen können.

▪ Messenger/IRC-Clients

- Irssi - ist ein kostenloser Open-Source-Terminal-basierter IRC-Client.
- WeeChat - ist ein extrem erweiterbarer und leichter IRC-Client.

▪ Sonstiges

- sysadmin-util - Tools für Linux/Unix sysadmins.
- incron - ist eine inode-basierte Dateisystembenachrichtigungstechnologie.
- lsyncd - synchronisiert lokale Verzeichnisse mit Remotezielen (Live Syncing Daemon).
- GRV - ist eine terminalbasierte Schnittstelle zum Anzeigen von Git-Repositorys.
- Tig - Text-Modus-Schnittstelle für Git.
- tldr - vereinfachte und gemeinschaftsgesteuerte Manpages.
- Archiver - erstellen und extrahieren Sie einfach .zip, .tar, .tar.gz, .tar.bz2, .tar.xz, .tar.lz4, .tar.sz und .rar.
- commander.js - minimaler CLI-Ersteller in JavaScript.
- gron - machen JSON greppable!
- Bett - binärer Editor in Go geschrieben.

GUI-Tools [TOC]

▪ Terminal-Emulatoren

- Guake - ist ein Dropdown-Terminal für die GNOME-Desktop-Umgebung.
- Terminator - basiert auf GNOME Terminal, nützliche Funktionen für Sysadmins und andere Benutzer.
- Kitty - ist ein GPU-basierter Terminal-Emulator, der reibungsloses Scrollen und Bilder unterstützt.

▪ Netzwerk

- Wireshark - ist der weltweit führende und weit verbreitete Netzwerkprotokollanalysator.
- Ettercap - ist ein umfassendes Netzwerk-Monitor-Tool.
- EtherApe - ist eine grafische Netzwerküberwachungslösung.
- Packet Sender - ist ein Netzwerkdienstprogramm für die Paketgenerierung und integrierte UDP/TCP/SSL-Clients und -Server.
- Ostinato - ist paketfertiger und Verkehrsgenerator.
- JMeter™ - Open Source Software zum Laden des Funktionsverhaltens und zur Leistungsmessung.
- -Locust - skalierbares Benutzerauslastungstesttool, das in Python geschrieben wurde.

▪ Browser

- TOR Browser - schützen Sie Ihre Privatsphäre und schützen Sie sich gegen Netzwerküberwachung und Verkehrsanalyse.

▪ Passwort-Manager

◈ KeePassXC - speichern Sie Ihre Passwörter sicher und geben Sie sie automatisch in Ihre täglichen Websites und Apps ein.
◈ Enpass - Passwort-Manager und sichere Brieftasche.

▪ Messenger/IRC-Clients

◈ HexChat - ist ein IRC-Client, der auf XChat basiert.
◈ Pidgin - ist ein einfach zu bedienender und kostenloser Chat-Client, der von Millionen von Menschen genutzt wird.

▪ Messengers (Ende-zu-Ende-Verschlüsselung)

◈ Signal - ist eine verschlüsselte Kommunikations-App.
◈ Wire - sichere Nachrichten, Dateifreigabe, Sprachanrufe und Videokonferenzen. Alle mit End-to-End-Verschlüsselung geschützt.
◈ TorChat - dezentraler anonymer Instant Messenger auf Tor Hidden Services.
◈ Matrix - ein offenes Netzwerk für sichere, dezentrale Echtzeitkommunikation.

▪ Texteditoren

◈ Sublime Text - ist ein leichter, plattformübergreifender Code-Editor, der für seine Geschwindigkeit und Benutzerfreundlichkeit bekannt ist.
◈ Visual Studio Code - ein Open-Source- und kostenloser Quellcode-Editor, der von Microsoft entwickelt wurde.
◈ Atom - ein hackbarer Texteditor für das 21. Jahrhundert.

Webtools [TOC]

▪ Browser

◈ SSL/TLS-Funktionen Ihres Browsers - testen Sie die SSL-Implementierung Ihres Browsers.
◈ Kann ich verwenden - bietet aktuelle Browser-Support-Tabellen für die Unterstützung von Front-End-Webtechnologien.
◈ Panopticlick 3.0 - ist Ihr Browser sicher gegen Tracking?
◈ Privacy Analyzer - sehen Sie, welche Daten von Ihrem Browser verfügbar gemacht werden.
◈ Web Browser Security - es geht um Web Browser Fingerprinting.
◈ Wie ist mein SSL? - Helfen Sie einem Webserver-Entwickler zu erfahren, wozu TLS-Clients in der realen Welt fähig sind.
◈ sslClientInfo - Clienttest (inkl. TLSv1.3-Informationen).

▪ SSL/Sicherheit

◈ SSLLabs Server Test - kostenloser Online-Dienst führt eine gründliche Analyse der Konfiguration eines beliebigen SSL-Webservers durch.

- SSLLabs Server Test (DEV) - kostenloser Online-Dienst führt eine gründliche Analyse der Konfiguration eines beliebigen SSL-Webservers durch.
- ImmuniWeb® SSLScan - testen SSL/TLS (PCI DSS, HIPAA und NIST).
- SSL-Prüfung - Scannen Sie Ihre Website nach nicht sicheren Inhalten.
- CryptCheck - testen Sie Ihre TLS-Serverkonfiguration (z.B. Chiffren).
- urlscan.io - Service zum Scannen und Analysieren von Websites.
- Berichts-URI - Überwachung von Sicherheitsrichtlinien wie CSP und HPKP.
- CSP Evaluator - ermöglicht Entwicklern und Sicherheitsexperten, zu überprüfen, ob eine Content Security Policy.
- Useless CSP - öffentliche Liste über CSP in einigen großen Playern (könnte sie ein bisschen mehr kümmern).
- Warum kein HTTPS? - Liste der 100 besten Websites der Welt von Alexa Rang nicht automatisch umleiten unsichere Anfragen.
- TLS Cipher Suite Search
- cipherli.st - starke Chiffren für Apache, Nginx, Lighttpd und mehr. *
- dhtool - öffentliche Diffie-Hellman Parameter Service/Tool.
- badssl.com - denkwürdige Website zum Testen von Clients gegen schlechte SSL-Konfigurationen.
- tlsfun.de - registriert für verschiedene Tests bezüglich des TLS/SSL-Protokolls.
- CAA Record Helper - Generieren Sie eine CAA-Richtlinie.
- Common CA Database - Repository mit Informationen über Zertifizierungsstellen und deren Stamm- und Zwischenzertifikate.
- CERTSTREAM - Echtzeit-Zertifikattransparenz-Protokollaktualisierungsstream.
- crt.sh - entdeckt Zertifikate, indem sie ständig alle öffentlich bekannten CT überwacht.
- Hardenize - Stellen Sie die Sicherheitsstandards bereit.
- Cipher Suite-Kompatibilität - Testen Sie die TLS-Verschlüsselungs-Suite-Kompatibilität.
- urlvoid - dieser Dienst hilft Ihnen, potenziell schädliche Websites zu erkennen.
- security.txt - ein vorgeschlagener Standard (Generator), der es Websites ermöglicht, Sicherheitsrichtlinien zu definieren.
- ssl-config-generator - helfen Sie, die Mozilla Server Side TLS-Konfigurationsrichtlinien zu befolgen.

▪ HTTP-Header & Web-Linters

- Security Headers - analysieren Sie die HTTP-Antwortheader (mit Bewertungssystem zu den Ergebnissen).
- Observatory von Mozilla - eine Reihe von Tools, um Ihre Website zu analysieren.
- webhint - ist ein Linting-Tool, das Ihnen bei der Zugänglichkeit, Geschwindigkeit, Sicherheit und mehr ihrer Website hilft.

▪ DNS

- ViewDNS - eine Quelle für kostenlose DNS-bezogene Tools und Informationen.
- DNSLookup - ist ein erweitertes DNS-Suchtool.
- DNSlytics - Online-DNS-Untersuchungstool.

- **DNS Spy** - überwachen, validieren und überprüfen Sie Ihre DNS-Konfigurationen.
- **Zonemaster** - hilft Ihnen, zu steuern, wie Ihr DNS funktioniert.
- **Leaf DNS** - umfassender DNS-Tester.
- **Subdomains online suchen** - Finden Sie Subdomains für den Durchdringungstest für die Sicherheitsbewertung.
- **DNSdumpster** - dns recon & research, find & lookup dns records.
- **DNS-Tabelle online** - Suche nach DNS-Einträgen nach Domäne, IP, CIDR, ISP.
- **inDNS** - DNS- und Mailserver-Integritätsprüfung.
- **DNS Bajaj** - überprüfen Sie die Delegierung Ihrer Domain.
- **BuddyDNS Delegation LAB** - Überprüfen, verfolgen und visualisieren Sie die Delegierung Ihrer Domain.
- **dnssec-debugger** - DS- oder DNSKEY-Eintragsvalidator.
- **PTRarchive.com** - diese Website ist für die Aufbewahrung historischer Reverse-DNS-Einträge verantwortlich.
- **xip.io** - Platzhalter-DNS für alle.
- **dnslookup (ceipam)** - einer der besten DNS-Propagationsprüfer (und nicht nur).
- **What es My DNS** - DNS-Verbreitungsüberprüfungstool.
- **DNSGrep** - schnell es nach großen DNS-Datasets suchen.

▪ Mail

- **smtp-tls-checker** - überprüfen Sie eine E-Mail-Domäne auf SMTP TLS-Unterstützung.
- **MX Toolbox** - alle Ihre MX-Eintrag, DNS, Blacklist und SMTP-Diagnose in einem integrierten Tool.
- **Secure Email** - komplette E-Mail-Testtools für E-Mail-Techniker.
- **Blacklistalert** - überprüft, ob Ihre Domain auf einer Echtzeit-Spam-Blacklist steht.
- **MultiRBL** - vollständige IP-Prüfung zum Senden von Mailservern.
- **DKIM SPF & Spam Assassin Validator** - überprüft die E-Mail-Authentifizierung und bewertet Nachrichten mit Spam Assassin.

▪ Encoder/Decoder und Regex-Tests

- **URL Encode/Decode** - Tool von oben, um eine Textzeichenfolge zu codieren oder zu dekodieren.
- **Uncoder** - der Online-Übersetzer für Suchanfragen zu Protokolldaten.
- **Regex101** - Online-Regex-Tester und Debugger: PHP, PCRE, Python, Golang und JavaScript.
- **RegExr** - Online-Tool zum Lernen, Erstellen und Testen von regulären Ausdrücken (RegEx / RegExp).
- **RegEx Testing** - Online-Regex-Testtool.
- **RegEx Pal** - Online-Regex-Testtool + andere Tools.
- **The Cyber Swiss Army Knife** - eine Web-App für Verschlüsselung, Codierung, Komprimierung und Datenanalyse.

▪ Net-Tools

◈ Netcraft - detaillierter Bericht über die Website, der Ihnen hilft, fundierte Entscheidungen über ihre Integrität zu treffen. *

◈ RIPE NCC Atlas - eine globale, offene, verteilte Internet-Messplattform.

◈ Robtex - verwendet verschiedene Quellen, um öffentliche Informationen über IP-Nummern, Domain-Namen, Host-Namen, Routen usw. zu sammeln.

◈ Security Trails - APIs für Sicherheitsunternehmen, Forscher und Teams.

◈ Online Curl - Curl-Test, analysieren HTTP Response Headers.

◈ Online-Tools für Entwickler - HTTP-API-Tools, Tester, Encoder, Konverter, Formatters und andere Tools.

◈ Ping.eu - Online-Ping, Traceroute, DNS-Suche, WHOIS und andere.

◈ Network-Tools - Netzwerktools für Webmaster, IT-Techniker & Geeks.

◈ BGPview - Suchen Sie nach einem beliebigen ASN-, IP-, Präfix- oder Ressourcennamen.

◈ Ist BGP noch sicher? - Überprüfen Sie die BGP-Sicherheit (RPKI) von ISPs und anderen wichtigen Internet-Playern.

◈ Riseup - bietet Online-Kommunikationstools für Menschen und Gruppen, die an befreienden sozialen Veränderungen arbeiten.

◈ VirusTotal - analysieren Sie verdächtige Dateien und URLs, um Arten von Malware zu erkennen.

▪ Datenschutz

◈ privacytools.io - bietet Wissen und Tools, um Ihre Privatsphäre vor globaler Massenüberwachung zu schützen.

◈ DNS Privacy Test Servers - DNS Privacy Recursive Servers List (mit einer "No Logging"-Richtlinie).

▪ Code Parser/Spielplätze

◈ ShellCheck - findet Fehler in Ihren Shell-Skripten.

◈ erklärthell - erhalten Sie interaktive Hilfetexte für Shell-Befehle.

◈ jsbin - live pastebin für HTML, CSS & JavaScript und mehr.

◈ - Online-Code-Editor für die Webanwendungsentwicklung. Unterstützt React, Vue, Angular, CxJS, Dojo, etc.

◈ PHP Sandbox - testen Sie Ihren PHP-Code mit diesem Codetester.

◈ Repl.it - eine sofortige IDE, um alles an einem Ort zu lernen, zu erstellen, zusammenzuarbeiten und zu hosten.

◈ vclFiddle - ist ein Online-Tool zum Experimentieren mit der Varnish Cache VCL.

▪ Leistung

◈ GTmetrix - analysieren Sie die Geschwindigkeit Ihrer Website und machen Sie es schneller.

◈ Sucuri-Lastzeittester - testen Sie hier die Leistung Ihrer Websites aus der ganzen Welt.

◈ Pingdom Tools - analysieren Sie die Geschwindigkeit Ihrer Website auf der ganzen Welt.

◈ PingMe.io - führen Sie Website-Latenztests in mehreren geografischen Regionen aus.

◈ PageSpeed Insights - analysieren Sie die Geschwindigkeit Ihrer Website und machen Sie

es schneller.

◈ **web.dev** - hilft Entwicklern wie Ihnen, die modernen Funktionen des Webs zu lernen und auf Ihre eigenen Websites und Apps anzuwenden.

◈ **Lighthouse** - automatisierte Swätprüfung, Leistungsmetriken und Best Practices für das Web.

▪ Massenscanner (Suchmaschinen)

◈ **Censys** - Plattform, die Informationssicherheitsexperten dabei unterstützt, Geräte zu erkennen, zu überwachen und zu analysieren.

◈ **Shodan** - die weltweit erste Suchmaschine für mit dem Internet verbundene Geräte.

◈ **Shodan 2000** - nutzen Sie Shodan für den Arbeitsalltag? Dieses Tool sucht nach zufällig generierten Daten aus Shodan.

◈ **GreyNoise** - Massenscanner wie Shodan und Censys.

◈ **ZoomEye** - Suchmaschine für Dener, mit der der Benutzer bestimmte Netzwerkkomponenten finden kann.

◈ **Netograph** - Werkzeuge, um tiefe Struktur des Webs zu überwachen und zu verstehen.

◈ **FOFA** - ist eine Cyberspace-Suchmaschine.

◈ **onyphe** - ist eine Suchmaschine für Open-Source- und Cyber-Bedrohungs-Intelligence-Daten gesammelt.

◈ **IntelligenceX** - ist eine Suchmaschine und Datenarchiv.

◈ **binaryedge** - es scannt den gesamten Internet-Raum und erstellen Echtzeit-Bedrohung Intelligenz Streams und Berichte.

◈ **wigle** - ist ein submissionbasierter Katalog von drahtlosen Netzwerken. Alle Netzwerke. Gefunden von jedermann.

◈ **PublicWWW** - finden Sie alle alphanumerischen Ausschnitte, Signaturen oder Schlüsselwörter in den Webseiten HTML, JS und CSS-Code.

◈ **IntelTechniques** - dieses Repository enthält Hunderte von Online-Suchdienstprogrammen.

◈ **Jäger** - können Sie E-Mail-Adressen in Sekunden schnelle und verbinden mit den Personen, die für Ihr Unternehmen wichtig sind.

◈ **GhostProject?** - Suche nach voller E-Mail-Adresse oder Benutzername.

◈ **Datenschutzverletzungen** - war meine E-Mail von Datenschutzverletzungen betroffen?

◈ **We Leak Info** - die weltweit schnellste und größte Suchmaschine für Datenverstöße.

◈ **Pulsedive** - Scann von bösartigen URLs, IPs und Domänen, einschließlich Portscans und Webanfragen.

◈ **Buckets von Grayhatwarfar** - Datenbank mit öffentlicher Suche nach Open Amazon S3 Buckets und deren Inhalt.

◈ **Vigilante.pw** - das durchbrochene Datenbankverzeichnis.

◈ **mit** - finden Sie heraus, mit welchen Websites websites gebaut werden.

◈ **NerdyData** - durchsuchen Sie den Quellcode des Webs nach Technologien, über Millionen von Websites.

◈ **den offenen FTP-Index** von Mamont - wenn ein Ziel über eine offene FTP-Site mit zugänglichen Inhalten verfügt, wird es hier aufgelistet.

◈ **OSINT Framework** - konzentrierte sich auf das Sammeln von Informationen aus kostenlosen Tools oder Ressourcen.

◈ **maltiverse** - ist ein Service, der sich an Cybersicherheitsanalysten für die erweiterte Analyse von Kompromissindikatoren orientiert.
◈ **Leaked Source** - ist eine Zusammenarbeit von Online-Daten in Form einer Suche.
◈ **We Leak Info** - um Alltagsmenschen zu helfen, ihr Online-Leben zu sichern, um zu vermeiden, gehackt zu werden.
◈ **pipl** - ist der Ort, um die Person hinter der E-Mail-Adresse, sozialen Benutzernamen oder Telefonnummer zu finden.
◈ **abuse.ch** - wird von einem zufälligen Schweizer Kerl, der Malware für Non-Profit kämpft, betrieben.
◈ **malc0de** - Malware-Suchmaschine.
◈ **Cybercrime Tracker** - überwacht und verfolgt verschiedene Malware-Familien, die verwendet werden, um Cyber-Verbrechen zu begehen.
◈ **shhgit** - finden Sie GitHub Geheimnisse in Echtzeit.
◈ **◈-Suchcode** - und hilft Ihnen, Beispiele für Funktionen, APIs und Bibliotheken in der Praxis zu finden.
◈ **Insecam** - das weltweit größte Verzeichnis von Online-Überwachungskameras.
◈ **Index-of** - enthält tolle Dinge wie: Sicherheit, Hacking, Reverse Engineering, Kryptographie, Programmierung usw.
◈ **Rapid7 Labs Open Data** - ist eine große Anzahl von Datensätzen von Project Sonar.

▪ Generatoren

◈ **diesepersondoesnotexist** - erzeugen gefälschte Gesichter mit einem Klick - endlose Möglichkeiten.
◈ **AI generierte Fotos** - 100.000 AI generierte Gesichter.
◈ **fakeface** - gefälschte Gesichter Browser.
◈ **Intigriti Redirector** - öffnen Umleitung / SSRF Nutzlast Generator.

▪ Kennwörter

◈ **bin ich pwned?** - Überprüfen Sie, ob Sie ein Konto haben, das bei einer Datenschutzverletzung kompromittiert wurde.
◈ **dehashed** - ist eine gehackte Datenbank-Suchmaschine.
◈ **Leaked Source** - ist eine Zusammenarbeit von Online-Daten in Form einer Suche.

▪ CVE/Exploits-Datenbanken

◈ **CVE Mitre** - Liste der öffentlich bekannten Cybersicherheits-Schwachstellen.
◈ **CVE-Details** - Erweiterte Datenbank für CVE-Sicherheitslücken.
◈ **Exploit DB** - CVE-konformes Archiv von öffentlichen Exploits und entsprechender anfälliger Software.
◈ **0day.today** - Exploits Markt bietet Ihnen die Möglichkeit, Zero-Day-Exploits zu kaufen und auch 0day Exploits zu verkaufen.
◈ **sploitus** - die Exploit-und Tools-Datenbank.
◈ **cxsecurity** - kostenlose Verwundbarkeitsdatenbank.
◈ **Vulncode-DB** - ist eine Datenbank für Schwachstellen und den entsprechenden

Quellcode, falls verfügbar.
- **cveapi** - kostenlose API für CVE-Daten.

▪ Mobile Apps-Scanner

- **ImmuniWeb® Mobile App Scanner** - Testen Sie die Sicherheit und den Datenschutz mobiler Apps (iOS & Android).
- **Quixxi** - kostenloser Mobile App Vulnerability Scanner für Android & iOS.
- **Ostorlab** - analysiert mobile Anwendungen, um Schwachstellen und potenzielle Schwachstellen zu identifizieren.

▪ Private Suchmaschinen

- **Startseite** - die weltweit privatesuchste Suchmaschine.
- **searX** - eine datenschutzrespektierende, hackbare Metasuchmaschine.
- **Darksearch** - die erste echte Dark Web Suchmaschine.
- **Qwant** - die Suchmaschine, die Ihre Privatsphäre respektiert.

▪ Secure Webmail-Anbieter

- **CounterMail** - ist ein sicherer und einfach zu bedienender Online-E-Mail-Dienst, der für maximale Sicherheit und Privatsphäre ausgelegt ist.
- **Mail2Tor** - ist ein Tor Hidden Service, der es jedem ermöglicht, E-Mails anonym zu senden und zu empfangen.
- **Tutanota** - ist der weltweit sicherste E-Mail-Service und erstaunlich einfach zu bedienen.
- **Protonmail** - ist der weltweit größte sichere E-Mail-Dienst, der von CERN- und MIT-Wissenschaftlern entwickelt wurde.
- **Startmail** - private & verschlüsselte E-Mail leicht gemacht.

▪ Crypto

- **Keybase** - es ist Open Source und wird von Public-Key-Kryptographie angetrieben.

▪ PGP-Schlüsselserver

- **SKS OpenPGP Key Server** - Services für die von OpenPGP verwendeten SKS-Schlüsselserver.

Systeme/Dienste [TOC]

▪ Betriebssysteme

- **Slackware** - die "Unix-ähnliche" Linux-Distribution.
- **OpenBSD** - multi-platform 4.4BSD-basiertes UNIX-ähnliches Betriebssystem.
- **HardenedBSD** - HardenedBSD zielt darauf ab, innovative Exploit-Minderungs- und Sicherheitslösungen zu implementieren.
- **Kali Linux** - Linux-Distribution für Penetration Testing, Ethical Hacking und

Netzwerksicherheitsbewertungen.

- **Parrot Security OS** - Cyber Security GNU/Linux-Umgebung.
- **Backbox Linux** - Penetrationstest und Sicherheitsbewertung orientierte Ubuntu-basierte Linux-Distribution.
- **BlackArch** - ist eine Arch Linux-basierte Penetrationtesting-Distribution für Penetrationstester und Sicherheitsforscher.
- **Pentoo** - ist eine sicherheitsorientierte Livecd, die auf Gentoo basiert.
- **Security Onion** - Linux-Distribution für Intrusion Detection, Enterprise Security Monitoring und Log Management.
- **Tails** - ist ein Live-System, das darauf abzielt, Ihre Privatsphäre und Anonymität zu bewahren.
- **vedetta** - OpenBSD Router Boilerplate.

▪ HTTP(s) Dienste

- **Varnish Cache** - HTTP-Beschleuniger für inhaltslastige dynamische Websites.
- **Nginx** - Open Source Web und Reverse Proxy Server, der Apache ähnlich ist, aber sehr geringes Gewicht.
- **OpenResty** - ist eine dynamische Web-Plattform, die auf NGINX und LuaJIT basiert.
- **Tengine** - eine Distribution von Nginx mit einigen erweiterten Funktionen.
- **Caddy Server** - ist ein Open-Source-, HTTP/2-fähiger Webserver mit HTTPS standardmäßig.
- **HAProxy** - der zuverlässige, leistungsstarke TCP/HTTP Load Balancer.

▪ DNS-Dienste

- **Unbound** - Validieren, Rekursive und Zwischenspeichern von DNS-Resolver (mit TLS).
- **Knot Resolver** - Zwischenspeichern der vollständigen Resolverimplementierung, einschließlich einer Resolverbibliothek und eines Daemons.
- **PowerDNS** - ist ein Open Source autoritativer DNS-Server, der in C++ geschrieben und unter der GPL lizenziert ist.

▪ andere Dienstleistungen

- **3proxy** - winziger kostenloser Proxy-Server.

▪ Sicherheit/Härtung

- **Emerald Onion** - ist eine 501(c)(3) Non-Profit-Organisation und Transit-Internet-Service-Provider (ISP) mit Sitz in Seattle.
- **Pi-Loch** - das Pi-Loch® ist ein DNS-Senkloch, das Ihre Geräte vor unerwünschten Inhalten schützt.
- **Maltrail** - bösartiges Verkehrserkennungssystem.
- **security_monkey** – überwacht AWS-, GCP-, OpenStack- und GitHub-Organisationen auf Assets und deren Änderungen im Laufe der Zeit.
- **-,** sichere und schnelle MicroVMs für serverloses Computing.

◈ **streisand** - richtet einen neuen Server ein, auf dem Sie WireGuard, OpenSSH, OpenVPN, Shadowsocks und mehr ausführen.

Netzwerke [TOC]

▪ Tools

◈ **CapAnalysis** - Web Visual Tool zur Analyse großer Mengen erfassten Netzwerkverkehrs (PCAP-Analysator).
◈ **Netbox** - IP-Adressverwaltung (IPAM) und Data Center Infrastructure Management (DCIM) Tool.

▪ Labs

◈ **NRE Labs** - lernen Sie dabei Automatisierung. Gerade jetzt, genau hier, in Ihrem Browser.

▪ Sonstiges

◈ **LBNL Network Research Group** - Homepage der Network Research Group (NRG); Tools, Vorträge, Papiere und mehr.

Container/Orchestrierung [TOC]

▪ CLI-Tools

◈ **gvisor** - Container-Laufzeit-Sandbox.
◈ **ctop** - Top-like-Schnittstelle für Container-Metriken.
◈ **docker-bench-security** - ist ein Skript, das dutzende gängige Best Practices für die Bereitstellung von Docker überprüft.

▪ Webtools

◈ **Moby** - ein kollaboratives Projekt für das Container-Ökosystem, um Container-basiertes System zu montieren.
◈ **Traefik** - Open Source Reverse Proxy/Load Balancer bietet eine einfachere Integration mit Docker und Let es encrypt.
◈ **kong** - Das Cloud-Native API Gateway.
◈ **Rancher** - komplette Container-Management-Plattform.
◈ **Portainer** - macht das Docker-Management einfach.
◈ **nginx-proxy** - automatisierter nginx-Proxy für Docker-Container mit docker-gen.

▪ Handbücher/Tutorials/Best Practices

◈ **docker-cheat-sheet** - ein kurzes Referenz-Spickzettel auf Docker.
◈ **awesome-docker** - eine kuratierte Liste von Docker-Ressourcen und -Projekten.
◈ **docker_practice** - lernen und verstehen Docker-Technologien, mit echter DevOps-Praxis!

◈ Labs - ist eine Sammlung von Tutorials zum Erlernen der Verwendung von Docker mit verschiedenen Tools.
◈ dockerfiles - verschiedene Dockerfiles, die ich auf dem Desktop und auf Servern verwende.
◈ kubernetes-the-hard-way - bootstrap Kubernetes den harten Weg auf Google Cloud Platform. Keine Skripte.
◈ kubernetes-the-easy-way - bootstrap Kubernetes die einfache Art und Weise auf Google Cloud Platform. Keine Skripte.
◈ Cheatsheet-kubernetes-A4 - Kubernetes CheatSheets in A4.
◈ k8s-security - kubernetes Sicherheitshinweise und Best Practices.
◈ kubernetes-production-best-practices - Checklisten mit Best Practices für produktionsbereite Kubernetes.
◈ kubernetes-production-best-practices - kubernetes security - Best Practice Guide.
◈ kubernetes-failure-stories - ist eine Zusammenstellung von öffentlichen Misserfolgs-/Horrorgeschichten im Zusammenhang mit Kubernetes.

Manuals/Howtos/Tutorials [TOC]

▪ Shell/Command-Zeile

◈ pure-bash-bible - ist eine Sammlung reiner Bash-Alternativen zu externen Prozessen.
◈ pure-sh-bibel - ist eine Sammlung reiner POSIX sh Alternativen zu externen Prozessen.
◈ ◈-Bash-Guide - ist ein Leitfaden, um Bash zu lernen.
◈ Bash-Handbuch - für diejenigen, die Bash lernen wollen.
◈ The Bash Hackers Wiki - halten Sie Dokumentation jeglicher Art über GNU Bash.
◈ Shell & Utilities - beschreibt die Befehle und Dienstprogramme, die von POSIX-konformen Systemen für Anwendungsprogramme angeboten werden.
◈ die-Kunst-der-Befehlszeile - beherrschen Sie die Befehlszeile auf einer Seite.
◈ Shell Style Guide - ein Shell-Style Guide für Von Google-basierte Open-Source-Projekte.

▪ Texteditoren

◈ Vim Cheat Sheet - große mehrsprachige vim Anleitung.

▪ Python

◈ Awesome Python - eine kuratierte Liste von fantastischen Python-Frameworks, Bibliotheken, Software und Ressourcen.
◈ Python-Cheatsheet - umfassendes Python-Cheatsheet.
◈ pythoncheatsheet.org - Grundreferenz für Anfänger und Fortgeschrittene.

▪ Sed & Awk & Sonstiges

◈ F'Awk ja! - erweiterte Sed- und Awk-Nutzung (Parsing für Pentesters 3).

▪ *nix & Netzwerk

◈ nixCraft - Linux- und Unix-Tutorials für neue und erfahrene Sysadmin.
◈ TecMint - der ideale Linux-Blog für Sysadmins & Geeks.
◈ Omnisecu - kostenlose Networking-, Systemadministrations- und Sicherheits-Tutorials.
◈ Linux-Cheat - Linux-Tutorials und Cheatsheets. Minimale Beispiele. Meistens Benutzerland-CLI-Dienstprogramme.
◈ Unix Toolbox - Sammlung von Unix/Linux/BSD-Befehlen und -Aufgaben, die für IT-Arbeiten oder fortgeschrittene Benutzer nützlich sind.
◈ Linux Kernel Teaching - ist eine Sammlung von Vorträgen und Labs Linux-Kernel-Themen.
◈ htop erklärt - Erklärung von allem, was Sie in htop/top auf Linux sehen können.
◈ Linux Guide and Hints - Tutorials zur Systemadministration in Fedora und CentOS.
◈ strace-little-book - ein kleines Buch, das strace vorstellt.
◈ linux-tracing-workshop - Beispiele und praktische Labore für Linux-Tracing-Tools-Workshops.
◈ http2-erklärt - ein detailliertes Dokument, das HTTP/2 erklärt und dokumentiert.
◈ http3-erklärt - ein Dokument, das die HTTP/3- und QUIC-Protokolle beschreibt.
◈ HTTP/2 in Action - eine hervorragende Einführung in den neuen HTTP/2-Standard.
◈ Wir programmieren einen TCP/IP-Stack - tolle Dinge, um Netzwerk- und Systemprogrammierung auf einer tieferen Ebene zu lernen.
◈ Nginx Admin es Handbook - beschreibt, wie Sie NGINX Leistung, Sicherheit und andere wichtige Dinge verbessern können.
◈ nginxconfig.io - NGINX Config Generator auf Steroiden.
◈ openssh-Richtlinie - ist es, operative Teams bei der Konfiguration von OpenSSH-Server und -Client zu unterstützen.
◈ SSH Handshake Explained - ist eine relativ kurze Beschreibung des SSH-Handshakes.
◈ die Knowledgebase von ISC - Sie finden einige allgemeine Informationen zu BIND 9, ISC DHCP und Kea DHCP.
◈ PacketLife.net - ein Ort, um Notizen während des Studiums für CiscoccNP-Zertifizierung zu erfassen.

▪ Microsoft

◈ AD-Attack-Defense - angriff und verteidigt aktives Verzeichnis mit modernen Post-Exploitation-Gegner-Handelsaktivitäten.

▪ Großanlagen

◈ Der System Design Primer - erfahren Sie, wie Sie große Systeme entwerfen.
◈ Awesome Scalability - Best Practices beim Erstellen von High Skalierbarkeit, hoher Verfügbarkeit, hoher Stabilität und mehr.
◈ Web Architecture 101 - die grundlegenden Architekturkonzepte.

▪ Systemhärtung

◈ CIS Benchmarks - sind sichere Konfigurationseinstellungen für über 100 Technologien, die als kostenloser PDF-Download zur Verfügung stehen.
◈ Security Harden CentOS 7 - dies führt Sie durch die Schritte, die erforderlich sind, um

CentOS zu schützen.

- **CentOS 7 Server Hardening Guide** - tolle Anleitung zum Härten von CentOS; vertraut mit OpenSCAP.
- **awesome-security-hardening** - ist eine Sammlung von Sicherheits-Härte-Anleitungen, Tools und anderen Ressourcen.
- **Der Practical Linux Hardening Guide** - bietet einen Überblick über die Härtung von GNU/Linux-Systemen.

▪ Sicherheit & Datenschutz

- **Hacking Artikel** - LRaj Kronleuchter Sicherheit & Hacking Blog.
- **AWS-Sicherheitstools** – machen Sie Ihre AWS-Cloud-Umgebung sicherer.
- **CyberSecurity-Inventar** von Rawsec - eine Bestandsaufnahme der Tools und Ressourcen zu CyberSecurity.
- **The Illustrated TLS Connection** - jedes Byte einer TLS-Verbindung erklärt und reproduziert.
- **SSL Research** – Best Practices für SSL- und TLS-Bereitstellung von SSL Labs.
- **SELinux-Spiel** - lernen SELinux durch tun. Lösen Sie Rätsel, zeigen Skillz.
- **Zertifikate und PKI** - alles, was Sie über Zertifikate und PKI wissen sollten, aber zu ängstlich sind.
- **The Art of Subdomain Enumeration** - eine Referenz für Subdomänenenumerationstechniken.
- **Beenden von Google** - der umfassende Leitfaden zum Beenden von Google.

▪ Web-Apps

- **OWASP** - weltweite gemeinnützige Wohltätigkeitsorganisation, die sich auf die Verbesserung der Sicherheit von Software konzentriert.
- **OWASP ASVS 3.0.1** - OWASP Application Security Verification Standard Project.
- **OWASP ASVS 3.0.1 Web App** - einfache Web-App, die Entwicklern hilft, die ASVS-Anforderungen zu verstehen.
- **OWASP ASVS 4.0** - ist eine Liste der Sicherheitsanforderungen oder Tests für Anwendungen.
- **OWASP Testing Guide v4** - enthält ein "Best Practice"-Penetrationstestframework.
- **OWASP Dev Guide** - dies ist die Entwicklungsversion des OWASP Developer Guide.
- **OWASP WSTG** - ist ein umfassender Open-Source-Leitfaden zum Testen der Sicherheit von Web-Apps.
- **OWASP API Security Project** - konzentriert sich speziell auf die zehn wichtigsten Sicherheitsanfälligkeiten in der API-Sicherheit.
- **Mozilla Web Security** - helfen Sie operativen Teams beim Erstellen sicherer Webanwendungen.
- **Security-Bulletins** - Security Bulletins, die sich auf Netflix Open Source beziehen.
- **API-Security-Checklist** - Sicherheitsgegenmaßnahmen beim Entwerfen, Testen und Freigeben Ihrer API.
- **CORS aktivieren** - aktivieren sie die ursprungsübergreifende Ressourcenfreigabe.
- **Application Security Wiki** - ist eine Initiative, um alle anwendungssicherheitsbezogenen

Ressourcen an einem Ort bereitzustellen.

- **Weird Proxys** - Reverse Proxy-bezogene Angriffe; es ist ein Ergebnis der Analyse von verschiedenen Reverse-Proxys, Cache-Proxys, etc.
- **Webshells** - große Serie über bösartige Nutzlasten.
- **Praktische Web-Cache-Vergiftung** - zeigen Sie, wie Sie Websites mit esoterischen Web-Funktionen kompromittieren.
- **Versteckte Verzeichnisse und Dateien** - als Quelle für vertrauliche Informationen über Webanwendung.
- **Explosive Blog** - großer Blog über cybersec und pentests.
- **Sicherheits-Cookies** - dieses Papier wird einen genauen Blick auf Cookie-Sicherheit nehmen.
- **APISecurityBestPractices** - helfen Sie, Geheimnisse (API-Schlüssel, DB-Anmeldeinformationen, Zertifikate) aus dem Quellcode herauszuhalten.

▪ All-in-One

- **LZone Cheat Sheets** - alle Cheat Sheets.
- **Dan es Cheat Sheets es** - massive Cheat Sheets Dokumentation.
- **Ricos Cheatsheets** - das ist eine bescheidene Sammlung von Cheatsheets.
- **DevDocs-API** - kombiniert mehrere API-Dokumentationen in einer schnellen, organisierten und durchsuchbaren Schnittstelle.
- **cheat.sh** - das einzige Spickzettel, das Sie brauchen.

▪ Sonstiges

- **CTF-Serie : Vulnerable Machines** - die folgenden Schritte könnten befolgt werden, um Schwachstellen und Exploits zu finden.
- **50M CTF Writeup** - 50 Millionen US-Dollar CTF von Hackerone - writeup.
- **ctf-tasks** - ein Archiv von Low-Level-CTF-Herausforderungen, die im Laufe der Jahre entwickelt wurden.
- Wie startet man die **RE/Malware-Analyse?** - Sammlung von einigen Hinweisen und nützlichen Links für Anfänger.
- **Das C10K-Problem** - es ist Zeit für Webserver, zehntausend Clients gleichzeitig zu behandeln, nicht wahr?
- **Wie 1500 Bytes zur MTU des Internets wurden** - tolle Geschichte über die Maximale Übertragungseinheit.
- **Profiler des armen Mannes** - Sampling-Tools wie dtrace es bieten nicht wirklich Methoden, um zu sehen, welche Programme blockieren.
- **HTTPS auf Stack Overflow** - dies ist die Geschichte einer langen Reise in Bezug auf die Implementierung von SSL.
- **Juliaes Zeichnungen** - einige Zeichnungen über Programmierung und Unix-Welt, zines über Systeme & Debugging-Tools.
- **Hash-Kollisionen** - dieses großartige Repository konzentriert sich auf die Hash-Kollisionsausnutzung.
- **sha256-animation** - Animation der SHA-256-Hashfunktion in Ihrem Terminal.
- **BGP Meets Cat** - nach 3072 Stunden Manipulation von BGP ist es Job Snijders gelungen,

eine Nyancat zu zeichnen.

- **bgp-battleships** - spielen Schlachtschiffe über BGP.
- **Was passiert, wenn...** - Sie geben google.com in Ihren Browser ein und drücken Sie die Eingabetaste?
- **how-web-funktioniert** - basierend auf dem 'Was passiert, wenn...' Repository.
- **HTTPS in der realen Welt** - tolles Tutorial erklären, wie HTTPS in der realen Welt funktioniert.
- **Gitlab und NFS-Fehler** - wie wir zwei Wochen damit verbrachten, einen NFS-Fehler im Linux-Kernel zu jagen.
- **Gitlab schmilzt -** postmortem auf dem Datenbankausfall vom 31. Januar 2017 mit den Lektionen, die wir gelernt haben.
- **How To Become A Hacker** - wenn Sie ein Hacker sein wollen, lesen Sie weiter.
- **Betriebskosten in** der CPU - eine Infografik, die helfen soll, die Kosten für bestimmte Vorgänge in CPU-Uhren zu schätzen.
- **Erstellen einer einfachen Datenbank** - Schreiben eines sqlite-Klons von Grund auf in C.
- **einfach-Computer** - große Ressource zu verstehen, wie Computer unter der Haube arbeiten.
- **Die Geschichte von "Habe ich gepfändet?"** - Arbeiten mit 154 Millionen Datensätzen in Azure Table Storage.
- **TOP500 Supercomputer** - zeigt die 500 leistungsstärksten kommerziell erhältlichen Computersysteme, die uns bekannt sind.
- **Wie man einen 8-GPU-Passwort-Cracker baut** - jede "schwarze Magie" oder stundenlange Frustration wie Desktop-Komponenten.
- **CERN Data Centre** - 3D-Visualisierungen der CERN-Computing-Umgebungen (und mehr).
- **Wie gefickt ist meine Datenbank** - bewerten, wie gefickt Ihre Datenbank ist mit dieser praktischen Website.
- **Linux Troubleshooting 101 , 2016 Edition** - alles ist ein DNS-Problem...
- **Five Whys** - Wissen Sie, was das Problem ist, aber Sie können es nicht lösen?
- **wiehttps.funktioniert** - wie HTTPS funktioniert ... in einem Comic!
- **howdns.works** - eine lustige und bunte Erklärung, wie DNS funktioniert.
- **POSTGRESQLCO. NF** - Ihre postgresql.conf Dokumentation und Empfehlungen.

Inspirierende Listen [TOC]

▪ SysOps/DevOps

- **Awesome Sysadmin** - erstaunlich tolle Open-Source-Sysadmin-Ressourcen.
- **Awesome Shell** - tolle Kommandozeilen-Frameworks, Toolkits, Guides und Gizmos.
- **Befehlszeilen-Textverarbeitung** - vom Suchen von Text zu Suchen und Ersetzen, von der Sortierung bis zur Verschönerung von Text und mehr.
- **Awesome Pcaptools** - Sammlung von Werkzeugen, die von anderen Forschern entwickelt wurden, um Netzwerkspuren zu verarbeiten.
- **awesome-ebpf** - eine kuratierte Liste von tollen Projekten im Zusammenhang mit eBPF.
- **Linux Network Performance** - erfahren Sie, wo einige der Netzwerksystemvariablen in den Linux/Kernel-Netzwerkfluss passen.

◈ **Awesome Postgres** - Liste der fantastischen PostgreSQL Software, Bibliotheken, Tools und Ressourcen.
◈ **Quick-SQL-Cheatsheet** - eine kurze Erinnerung an alle SQL-Abfragen und Beispiele für deren Verwendung.
◈ **Awesome-Selfhosted** - Liste der Netzwerkdienste und Webanwendungen freier Software, die lokal gehostet werden können.
◈ **Liste der Anwendungen** - riesige Sammlung von Anwendungen sortiert nach Kategorie, als Referenz für diejenigen, die nach Paketen suchen.
◈ **CS-Interview-Knowledge-Map** - erstellen Sie die beste Interviewkarte.
◈ **DevOps-Guide** - DevOps Guide von einfach bis fortgeschritten mit Interview-Fragen und Notizen.
◈ **FreeBSD Journal** - es ist eine große Liste von Zeitschriften über FreeBSD und andere wichtige Dinge.
◈ **devops-interview-questions** - enthält Interviewfragen zu verschiedenen DevOps und SRE-Themen.

▪ Entwickler

◈ **Web Developer Roadmap** - Roadmaps, Artikel und Ressourcen, die Ihnen helfen, Ihren Weg zu wählen, zu lernen und zu verbessern.
◈ **Front-End-Checkliste** - die perfekte Front-End Checkliste für moderne Webseiten und akribische Entwickler.
◈ **Front-End-Performance-Checkliste** - die einzige Front-End-Leistungscheckliste, die schneller läuft als die anderen.
◈ **Pythons magische Methoden** - was sind magische Methoden? Sie sind alles in objektorientierter Python.
◈ **wtfpython** - eine Sammlung überraschender Python-Schnipsel und weniger bekannter Features.
◈ **js-dev-reads** - eine Liste von Büchern und Artikeln, die der anspruchsvolle Webentwickler lesen kann.
◈ **Commit-Nachrichtenleitfaden** - ein Leitfaden, um die Bedeutung von Commit-Nachrichten zu verstehen.

▪ Sicherheit/Pentesting

◈ **Awesome Web Security** - eine kuratierte Liste von Web Security-Materialien und -Ressourcen.
◈ **awesome-cyber-skills** - eine kuratierte Liste von Hacking-Umgebungen, in denen Sie Ihre Cyber-Fähigkeiten trainieren können.
◈ **awesome-devsecops** - eine maßgebliche Liste von fantastischen devsecops Tools.
◈ **awesome-osint** - ist eine kuratierte Liste von erstaunlich genial OSINT.
◈ **awesome-threat-intelligence** - eine kuratierte Liste von Awesome Threat Intelligence-Ressourcen.
◈ **Red-Teaming-Toolkit** - eine Sammlung von Open-Source- und kommerziellen Tools, die bei roten Teamoperationen helfen.
◈ **awesome-burp-Extensions** - eine kuratierte Liste von erstaunlich tollen Burp Extensions.

- **Kostenlose Sicherheits-eBooks** - Liste einer kostenlosen Sicherheit und Hacking eBooks.
- **Hacking-Security-Ebooks** - Top 100 Hacking & Security E-Books.
- **Datenschutz** - kuratierte Liste der Datenschutz-RespektDienste und Software.
- **Reverse-Engineering** - Liste der fantastischen Reverse Engineering Ressourcen.
- **linux-re-101** - eine Sammlung von Ressourcen für Linux Reverse Engineering.
- **Reverseengineering-Leseliste** - eine Liste von Reverse Engineering-Artikeln, -Büchern und -Papieren.
- **Awesome-WAF** - eine kuratierte Liste von fantastischen Web-App Firewall (WAF) Sachen.
- **awesome-shodan-queries** - interessante, lustige und deprimierende Suchanfragen, um sie in shodan.io einzustecken.
- **RobotsDisallowed** - eine kuratierte Liste der häufigsten und interessantesten Robots.txt nicht zugelassenen Verzeichnisse.
- **HackingNeuralNetworks** - ist ein kleiner Kurs zur Ausnutzung und Verteidigung neuronaler Netzwerke.
- **Platzhalterzertifikate** - warum Sollten Sie wahrscheinlich kein Platzhalterzertifikat verwenden.
- **Verwenden Sie keine VPN-Dienste** - das macht jeder Drittanbieter".
- **awesome-yara** - eine kuratierte Liste von fantastischen YARA-Regeln, Tools und Menschen.
- **macOS-Security-and-Privacy-Guide** - Leitfaden zur Sicherung und Verbesserung der Privatsphäre auf macOS.
- **awesome-sec-talks** - ist eine gesammelte Liste von tollen Sicherheitsgesprächen.
- **Movies for Hackers** - Liste der Filme, die jeder Hacker & Cyberpunk sehen muss.

▪ Sonstiges

- **Cheatography** - über 3.000 kostenlose Cheatsheets, Revisionshilfen und schnelle Referenzen.
- **awesome-static-analysis** - statische Analysetools für alle Programmiersprachen.
- **Informatik** - Weg zu einer kostenlosen Autodidaktenausbildung in Informatik.
- **Post-Mortems** - ist eine Sammlung von Postmortems (Konfigurationsfehler, Hardwarefehler und mehr).
- **build-your-own-x** - bauen Sie Ihre eigene (hier einfügen Technologie).
- **Project-Based-Tutorials-in-C** - ist eine kuratierte Liste von projektbasierten Tutorials in C.
- **The-Documentation-Compendium** - verschiedene README-Vorlagen & Tipps zum Verfassen hochwertiger Dokumentation.
- **awesome-python-anwendungen** - freie Software, die großartig funktioniert und auch open-source Python ist.
- **awesome-public-datasets** - eine themenzentrierte Liste von HQ-Open-Datasets.

Blogs/Podcasts/Videos [TOC]

▪ SysOps/DevOps

◈ **Varnish für PHP-Entwickler** - sehr interessante Präsentation von Varnish von Mattias Geniar.
◈ **Ein Netflix-Leitfaden für Microservices** - Josh Evans spricht über die chaotische und lebendige Welt der Microservices bei Netflix.

▪ Entwickler

◈ **Vergleichen von C mit Maschinensprache** - vergleichen Sie ein einfaches C-Programm mit dem kompilierten Maschinencode dieses Programms.

▪ Geeky Personen

◈ **Brendan Greggs Blog** - ist ein Branchenexperte für Computing-Performance und Cloud Computing.
◈ **Gynvael "GynDream" Coldwind** - ist IT-Sicherheitsingenieur bei Google.
◈ **Micha""lcamtuf" Zalewski** - White Hat Hacker, Computer-Sicherheitsexperte.
◈ **Mattias Geniar** - Entwickler, Sysadmin, Blogger, Podcaster und Public Speaker.
◈ **Nick Craver** - Softwareentwickler und Systemadministrator für Stack Exchange.
◈ **Scott Helme** - Sicherheitsforscher, internationaler Sprecher und Gründer von securityheaders.com und report-uri.com.
◈ **Brian Krebs** - The Washington Post und jetzt ein unabhängiger investigativer Journalist.
◈ **Bruce Schneier** - ist ein international bekannter Sicherheitstechnologe, genannt "Sicherheitsguru".
◈ **Chrissy Morgan** - Verfechterin des praktischen Lernens, nimmt Chrissy auch an Bug-Bounty-Programmen teil.
◈ **Andy Gill** - ist ein Hacker im Herzen, der als Senior Penetration Tester arbeitet.
◈ **Daniel Miessler** - Cybersicherheitsexperte und Autor.
◈ **Samy Kamkar** - ist ein US-amerikanischer Datenschutz- und Sicherheitsforscher, Computer-Hacker.
◈ **Javvad Malik** - ist Sicherheitsanwalt bei AlienVault, einem Blogger-Event-Sprecher und Branchenkommentator.
◈ **Graham Cluley** - Referent und unabhängiger Computersicherheitsanalytiker.
◈ **Kacper Szurek** - Detektionsingenieur bei ESET.
◈ **Troy Hunt** - Web-Sicherheitsexperte, bekannt für öffentliche Aufklärung und Öffentlichkeitsarbeit zu Sicherheitsthemen.
◈ **raymii.org** - sysadmin, spezialisiert auf den Aufbau von Cloud-Umgebungen mit hoher Verfügbarkeit.
◈ **Robert Penz** - IT-Sicherheitsexperte.

▪ Geeky Blogs

◈ **Linux Audit** - der Linux-Sicherheitsblog über Auditing, Härtung und Compliance von Michael Boelen.
◈ **Linux Security Expert** - Schulungen, Howtos, Checklisten, Sicherheitstools und mehr.
◈ **Die Grymoire** - Sammlung von nützlichen Beschwörungen für Zauberer, seien Sie Computer-Assistenten, Magier, oder was auch immer.

◈ **Secjuice** - ist die einzige gemeinnützige, unabhängige und freiwillige Publikation im Bereich der Informationssicherheit.

◈ **Entzifferung** - Sicherheitsnachrichten, die informieren und inspirieren.

▪ Geeky Vendor Blogs

◈ **Tenable Podcast** - Gespräche und Interviews im Zusammenhang mit Cyber-Exposition und vieles mehr.

◈ **Sophos** - Bedrohung News Room, geben Ihnen Nachrichten, Meinung, Beratung und Forschung zu Computer-Sicherheitsfragen.

◈ **Tripwire State of Security** - Blog mit den neuesten Nachrichten, Trends und Einblicken zu aktuellen Fragen der Informationssicherheit.

◈ **Malwarebytes Labs Blog** - Sicherheitsblog zielt darauf ab, Insider-News über Cybersicherheit zu bieten.

◈ **TrustedSec** - aktuelle Nachrichten und Trends zur Cybersicherheit.

◈ **PortSwigger Web Security Blog** - über Web-App-Sicherheitsvulns und Top-Tipps von unserem Team für Web-Sicherheit.

◈ **AT&T Cybersecurity Blog** - Neuigkeiten zu neu auftretenden Bedrohungen und praktische Ratschläge zur Vereinfachung der Bedrohungserkennung.

◈ **Thycotic** - wo CISOs und IT-Administratoren sich über Branchentrends, IT-Sicherheit, Datenschutzverletzungen und mehr informieren.

▪ Geeky Cybersecurity Podcasts

◈ **Risky Business** - ist ein wöchentlicher Podcast zur Informationssicherheit mit Neuigkeiten und ausführlichen Interviews.

◈ **Cyber, von Motherboard** - Geschichten, und konzentrieren Sie sich auf die Ideen über Cybersicherheit.

◈ **Tenable Podcast** - Gespräche und Interviews im Zusammenhang mit Cyber-Exposition, und vieles mehr.

◈ **Cybercrime Investigations** - Podcast von Geoff White über Cyberkriminalität.

◈ **Der viele Hut Club** - mit Geschichten aus einer vielzahl von Infosec Menschen (Whitehat, Greyhat und Blackhat).

◈ **Darknet Diaries** - wahre Geschichten von der dunklen Seite des Internets.

◈ **OSINTCurious Webcasts** - ist die investigative Neugier, die Menschen hilft, erfolgreich in OSINT.

◈ **Security Weekly** - die neuesten Informationen zur Informationssicherheit und Hacking-News.

▪ Geeky Cybersecurity Video Blogs

◈ **rev3rse Sicherheit** - offensive, binäre Ausnutzung, Web-Anwendungssicherheit, Verwundbarkeit, Härten, rotes Team, blaues Team.

◈ **LiveOverflow** - viel weiter fortgeschrittene Themen als das, was in der Regel in bezahlten Online-Kursen angeboten wird - aber kostenlos.

- **J4vv4D** - die wichtigen Informationen über unsere Internet-Sicherheit.
- **CyberTalks** - Vorträge, Interviews und Artikel über Cybersicherheit.

▪ Besten persönlichen Twitter-Konten

- **@blackroomsec** - ein White-Hat-Hacker/Pentester. Intergalaktischer Minensucher-Champion 1990.
- **@MarcoCiappelli** - Mitbegründer @ITSPmagazine, am Schnittpunkt von IT-Sicherheit und Gesellschaft.
- **@binitamshah** - Linux Evangelist. Malware. Kernel Dev. Security Enthusiast.
- **@joe_carson** - ein InfoSec Professional und Tech Geek.
- **@mikko** - CRO bei F-Secure, Reverse Engineer, TED Speaker, Supervillain.
- **@esrtweet** - oft als ESR bezeichnet, ist ein amerikanischer Softwareentwickler und Open-Source-Software-Befürworter.
- **@gynvael** - Sicherheitsforscher/Programmierer, @DragonSectorCTF Gründer/Spieler, technischer Streamer.
- **@x0rz** - Security Researcher & Cyber Observer.
- **@hasherezade** - Programmierer, Malware-Analyst. Autor von PEbear, PEsieve, libPeConv.
- **@TinkerSec** - Tüftler, Cypherpunk, Hacker.
- **@alisaesage** - unabhängiger Hacker und Forscher.
- **@SwiftOnSecurity** - Systemsicherheit, Arbeitssicherheit, sysadmin, Autor von decentsecurity.com.
- **@dakami** - Chefwissenschaftler bei White Ops, ist einer von nur sieben Personen mit der Befugnis, die DNS-Stammschlüssel wiederherzustellen.
- **@samykamkar** - ist ein berühmter "Grauhut" Hacker, Sicherheitsforscher, Schöpfer des MySpace "Samy" Wurm.
- **@securityweekly** - Gründer & CTO des Security Weekly Podcast-Netzwerks.
- **@jack_daniel** - @SecurityBSides Mitbegründer.
- **@thegrugq** - Sicherheitsforscher.
- **@matthew_d_green** - Kryptograph und Professor an der Johns Hopkins University.

▪ Besten kommerziellen Twitter-Konten

- **@haveibeenpwned** - überprüfen Sie, ob Sie ein Konto haben, das bei einer Datenschutzverletzung kompromittiert wurde.
- **@bugcrowd** - vertraut mehr der Fortune 500 als jede andere Crowdsourcing-Sicherheitsplattform.
- **@Malwarebytes** - vertrauenswürdigste Sicherheitsfirma. Unübertroffene Bedrohungssichtbarkeit.
- **@sansforensics** - der weltweit führende Anbieter von Digital Forensics and Incident Response.
- **@attcyber** - Die Edge-to-Edge-Technologien von AT&T Cybersecurity bieten Bedrohungsinformationen und vieles mehr.
- **@TheManyHatsClub** - ein informationssicherheitsorientierter Podcast und eine Gruppe von Personen aus allen Gesellschaftsschichten.

◈ **@hedgehogsec** - Hedgehog Cyber. Gibraltar und Manchesters Top-Boutique-Informationssicherheitsfirma.
◈ **@NCSC** - das National Cyber Security Centre. Helfen, das Vereinigte Königreich zum sichersten Ort zum Leben und Arbeiten online zu machen.
◈ **@Synacktiv** - IT-Sicherheitsexperten.

▪ **Ein Stück Geschichte**

◈ **How to Do Things bei ARL** - so konfigurieren Sie Modems, scannen Sie Bilder, zeichnen SIE CD-ROMs auf und andere nützliche Techniken. *

▪ **Sonstiges**

◈ **Diffie-Hellman Key Exchange (Kurzversion)** - wie Diffie-Hellman Key Exchange funktionierte.

Hacking/Penetration-Tests [TOC]

▪ **Pentesters Arsenal-Werkzeuge**

◈ **Sandcat Browser** - ein penetrationsorientierter Browser mit vielen erweiterten Funktionen, die bereits eingebaut sind.
◈ **Metasploit** - Tool und Framework für Pentesting-System, Web und viele mehr, enthält eine Menge eine bereit zu nutzen Exploit.
◈ **Burp Suite** - Tool zum Testen der Sicherheit von Webanwendungen, Abfangen von Proxys zum Wiedergeben, Einfügen, Scannen und Fuzz-HTTP-Anforderungen.
◈ **OWASP Zed-Angriffsproxy** - Abfangen des Proxys zum Wiedergeben, Einfügen, Scannen und Fuzz-HTTP-Anforderungen.
◈ **w3af** - ist ein Web Application Attack and Audit Framework.
◈ **Mitmproxy** - ein interaktiver TLS-fähiger ABfang-HTTP-Proxy für Penetrationstester und Softwareentwickler.
◈ **Nikto2** - Webserver-Scanner, der umfassende Tests an Webservern für mehrere Elemente durchführt.
◈ **sqlmap** - Tool, das den Prozess der Erkennung und Ausnutzung von SQL-Injektionsfehlern automatisiert.
◈ **Recon-ng** - ist ein voll funktionsfähiges Web Reconnaissance Framework, das in Python geschrieben wurde.
◈ **AutoRecon** - ist ein Netzwerk-Aufklärungstool, das automatisierte Aufzählungen von Diensten durchführt.
◈ **Faraday** - eine integrierte Multiuser Pentest-Umgebung.
◈ **Photon** - unglaublich schneller Crawler für OSINT entwickelt.
◈ **XSStrike** - modernste XSS-Erkennungssuite.
◈ **Sn1per** - automatisiertes Pentest-Framework für offensive Sicherheitsexperten.
◈ **vuls** - ist ein Agenten-weniger Schwachstellen-Scanner für Linux, FreeBSD und andere.
◈ **Tsunami** - ist ein Allzweck-Netzwerk-Sicherheitsscanner mit einem erweiterbaren Plugin-System.

- **aquatone** - ein Tool für Domain-Flyover.
- **BillCipher** - Informationserfassungstool für eine Website oder IP-Adresse.
- **WhatWaf** - Web Application Firewalls und Schutzsysteme erkennen und umgehen.
- **Corsy** - CORS-Fehlkonfigurationsscanner.
- **Waschbär** - ist ein leistungsstarkes offensives Sicherheitstool für Aufklärung und Schwachstellen-Scannen.
- **dirhunt** - finden Sie Webverzeichnisse ohne Bruteforce.
- **John The Ripper** - ist ein schneller Passwort-Cracker, derzeit für viele Geschmacksrichtungen von Unix, Windows und anderen verfügbar.
- **Hashcat** - das weltweit schnellste und fortschrittlichste Passwort-Wiederherstellungsprogramm.
- **p0f** - ist ein Tool, um die Spieler hinter jeder zufälligen TCP/IP-Kommunikation zu identifizieren.
- **ssh_scan** - ein Prototyp eines SSH-Konfigurations- und Richtlinienscanners.
- **LeakLooker** - finden Sie offene Datenbanken - powered by Binaryedge.io
- **exploitdb** - durchsuchbares Archiv aus der Exploit-Datenbank.
- **getsploit** - ist ein Befehlszeilendienstprogramm zum Suchen und Herunterladen von Exploits.
- **ctf-tools** - einige Setup-Skripte für Sicherheits-Recherche-Tools.
- **pwntools** - CTF Framework und nutzen Entwicklungsbibliothek.
- **Sicherheitstools** - Sammlung von kleinen Sicherheitstools, die hauptsächlich in Python erstellt wurden. CTFs, Pentests und so weiter.
- **pentestpackage** - ist ein Paket von Pentest-Skripten.
- **Python-Pentest-Tools** - Python-Tools für Penetrationstester.
- **fuzzdb** - Wörterbuch von Angriffsmustern und Primitiven für Black-Box-Anwendungsfehlerinjektion und Ressourcenermittlung.
- **AFL** - ist ein freier Software-Fuzzer, der von Google gepflegt wird.
- **AFL++** - ist AFL mit Community-Patches.
- **syzkaller** - ist ein unbeaufsichtigter, abdeckungsgesteuerter Kernel-Fuzzer.
- **pwndbg** - Nutzen Sie Entwicklung und Reverse Engineering mit GDB leicht gemacht.
- **GDB PEDA** - Python Exploit Entwicklungshilfe für GDB.
- **IDA** - Multiprozessor-Disassembler und Debugger nützlich für Reverse Engineering Malware.
- **radare2** - Framework für Reverse-Engineering und Analyse von Binärdateien.
- **Routersploit** - Nutzungsframework für eingebettete Geräte.
- **Ghidra** - ist ein Software Reverse Engineering (SRE) Framework.
- **Vulnreport** - Open-Source-Pentesting-Management- und Automatisierungsplattform von Salesforce Product Security.
- **Mentalist** - ist ein grafisches Werkzeug für die individuelle Wordlist-Generierung.
- **Bogenschießen** - Schwachstellenbewertung und -verwaltung hilft bei der Durchführung von Scans und der Verwaltung von Schwachstellen.
- **Osmedeus** - vollautomatisches offensives Sicherheitstool für Aufklärung und Schwachstellen-Scannen.
- **Rindfleisch** - das Browser-Exploitation-Framework-Projekt.
- **AutoSploit** - automatisierter Massenexploiter.

◈ SUDO_KILLER - ist ein Tool, um Fehlkonfigurationen und Schwachstellen von sudo-Regeln zu identifizieren und auszunutzen.
◈ yara - das Muster passend Schweizer Messer.
◈ Mimikatz - ein kleines Tool, um mit Windows-Sicherheit zu spielen.
◈ Sherlock - jagen Social-Media-Konten nach Benutzernamen über soziale Netzwerke.
◈ OWASP Threat Dragon - ist ein Tool, das verwendet wird, um Bedrohungsmodelldiagramme zu erstellen und mögliche Bedrohungen aufzuzeichnen.

▪ Pentests Lesezeichen Sammlung

◈ PTES - der Penetrationstest-Ausführungsstandard.
◈ Pentests MindMap - erstaunliche Mindmap mit anfälligen Apps und Systemen.
◈ WebApps Security Tests MindMap - unglaubliche Mindmap für WebApps-Sicherheitstests.
◈ Brute XSS - meistern Sie die Kunst des Cross Site Scripting.
◈ XSS-Spickzettel - enthält viele Vektoren, die Ihnen helfen können, WAFs und Filter zu umgehen.
◈ Offensive Security Bookmarks - Sammlung von Sicherheits-Lesezeichen, alle Dinge, die Autor benötigt, um OSCP zu übergeben.
◈ Awesome Pentest Cheat Sheets - Sammlung der Cheat-Blätter nützlich für Pentesting.
◈ Awesome Hacking von HackWithGithub - tolle Listen für Hacker, Pentester und Sicherheitsforscher.
◈ Awesome Hacking von carpedm20 - eine kuratierte Liste von awesome Hacking-Tutorials, Tools und Ressourcen.
◈ Awesome Hacking Resources - Sammlung von Hacking /Penetration Testing-Ressourcen, um Sie besser zu machen.
◈ Awesome Pentest - Sammlung von awesome Penetration Testing Ressourcen, Werkzeuge und andere glänzende Dinge.
◈ Awesome-Hacking-Tools - ist eine kuratierte Liste von tollen Hacking Tools.
◈ Hacking Cheat Sheet - Autor Hacking und Pentesting Notizen.
◈ Blackhat-arsenal-tools - offizielle Black Hat Arsenal Sicherheitstools Repository.
◈ Penetration Testing und WebApp Cheat Sheets - die vollständige Liste der Infosec-bezogenen Cheatsheets.
◈ Cyber Security Resources - umfasst Tausende von Cybersicherheitsreferenzen und -ressourcen.
◈ Pentest Bookmarks - es gibt eine Menge von Pentesting Blogs.
◈ Cheatsheet-God - Penetration Testing Reference Bank - OSCP/PTP & PTX Cheatsheet.
◈ ThreatHunter-Playbook - um die Entwicklung von Techniken und Hypothesen für Jagdkampagnen zu unterstützen.
◈ Beginner-Network-Pentesting - Hinweise für Anfänger Netzwerk Pentesting Kurs.
◈ OSCPRepo - ist eine Liste von Ressourcen, die Der Autor gesammelt haben, um sich auf das OSCP vorzubereiten.
◈ PayloadsAllTheThings - eine Liste nützlicher Nutzlasten und Umgehungsfunktionen für Web Application Security und Pentest/CTF.
◈ Nutzlasten - git alle Nutzlasten! Eine Sammlung von Webangriffsnutzlasten.

- **Befehl-Injektion-Nutzlast-Liste** - Befehl Injektion NutzlastListe.
- **AwesomeXSS** - ist eine Sammlung von Awesome XSS Ressourcen.
- **php-webshells** - gemeinsame php webshells.
- **Pentesting Tools Cheat Sheet** - eine schnelle Referenz-High-Level-Übersicht für typische Penetrationstests.
- **OWASP Cheat Sheet Series** - ist eine Sammlung von hochwertigen Informationen zu bestimmten Anwendungssicherheitsthemen.
- **OWASP-Abhängigkeitsprüfung** - ist eine Open-Source-Lösung, die oWASP Top 10 2013 Eintrag.
- **OWASP ProActive Controls** - OWASP Top 10 Proaktive Steuerelemente 2018.
- **PENTESTING-BIBLE** - Hacking & Penetration Testing & red team & cyber security & computer science resources.
- **pentest-wiki** - ist eine kostenlose Online-Sicherheits-Wissensbibliothek für Pentester/Forscher.
- **DEF CON Media Server** - tolle Sachen von DEFCON.
- **Awesome Malware Analysis** - eine kuratierte Liste von fantastischen Malware-Analyse-Tools und Ressourcen.
- **SQL Injection Cheat Sheet** - detaillierte technische Informationen über die vielen verschiedenen Varianten der SQL Injection.
- **Entersoft Knowledge Base** - tolle und detaillierte Referenz über Schwachstellen.
- **HTML5 Security Cheatsheet** - eine Sammlung von HTML5-bezogenen XSS-Angriffsvektoren.
- **XSS String Encoder** - zum Generieren von XSS-Code, um Ihre Eingabevalidierungsfilter mit XSS zu überprüfen.
- **gehen Bins** - Liste der Unix-Binärdateien, die von einem Angreifer ausgenutzt werden können, um lokale Sicherheitseinschränkungen zu umgehen.
- **Guifre Ruiz Notes** - Sammlung von Sicherheit, System, Netzwerk und Pentest Cheatsheets.
- **SSRF-Tipps** - eine Sammlung von SSRF-Tipps.
- **Shell-Sturm-Repo CTF** - großes Archiv von CTFs.
- **ctf** - CTF (Capture The Flag) Schreibaufe, Codeausschnitte, Notizen, Skripte.
- **My-CTF-Web-Challenges** - Sammlung von CTF Web Herausforderungen.
- **MSTG** - Das Mobile Security Testing Guide (MSTG) ist ein umfassendes Handbuch für Sicherheitstests für mobile Apps.
- **Internal-Pentest-Playbook** - Notizen zu den häufigsten Dingen für einen internen Netzwerk-Penetrationstest.
- **KeyHacks** - zeigt schnelle Möglichkeiten, wie API-Schlüssel, die von einem Bug-Bounty-Programm durchgesickert sind, überprüft werden können.
- **verbrieft/Forschung** - verschiedene Proof of Concepts der Sicherheitsforschung von Securitum durchgeführt.
- **Public-Pentesting-Reports** - ist eine Liste von öffentlichen Penetrationstestberichten, die von mehreren beratenden Sicherheitsgruppen veröffentlicht wurden.
- **awesome-bug-bounty** - ist eine umfassende kuratierte Liste der verfügbaren Bug Bounty.
- **bug-bounty-reference** - ist eine Liste von Bug-Bounty-Schreib-Ups.
- **Awesome-Bugbounty-Writeups** - ist eine kuratierte Liste von Bugbounty-Schreibungen.

- **Bug Bounty Writeups** - Liste der Bug Bounty-Schreibaufe (2012-2020).
- **hackso.me** - eine große Reise in die Sicherheit.

▪ Hintertüren/Exploits

- **PHP-Hintertüren** - eine Sammlung von PHP Hintertüren. Nur zu Bildungs- oder Testzwecken.

▪ Wordlisten und schwache Kennwörter

- **Weakpass** - für jede Art von Bruteforce finden Sie Wortlisten oder entfesseln die Macht von ihnen alle auf einmal!
- **Hashes.org** - ist ein kostenloser Online-Hash-Auflösungsdienst mit vielen unvergleichlichen Techniken.
- **SecLists** - Auflistung mehrerer Listentypen, die bei Sicherheitsbewertungen verwendet werden und an einem Ort gesammelt werden.
- **Wahrscheinlich-Wordlisten** - sortiert nach wahrscheinlicher Wahrscheinlichkeit, die ursprünglich für die Generierung und das Testen von Kennwörtern erstellt wurde.
- **Schädelsicherheitskennwörter** - Passwortwörterbücher und durchgesickerte Passwörter Repository.
- **Polnischen PREMIUM Wörterbuch** - offizielles Wörterbuch erstellt vom Team auf dem Forum bezpieka.org. * [1]
- **statistisch-wahrscheinlich-Benutzernamen** - Wortlisten für die Erstellung statistisch wahrscheinlicher Benutzernamenlisten für die Verwendung bei Passwortangriffen.

▪ Bounty-Plattformen

- **YesWeHack** - Bug Bounty Plattform mit infosec Jobs.
- **Openbugbounty** - ermöglicht jedem Sicherheitsforscher, der eine Schwachstelle auf jeder Website meldet.
- **Hackerone** - globale Hacker-Community, um die wichtigsten Sicherheitsprobleme anzusprechen.
- **bugcrowd** - Crowdsourcing-Cybersicherheit für das Unternehmen.
- **Crowdshield** - Crowdsourcing-Sicherheit & Bug-Bounty-Management.
- **Synack** - Crowdsourcing-Sicherheits- & Bug-Bounty-Programme, Crowd Security Intelligence-Plattform und vieles mehr.
- **Hacktrophy** - Bug Bounty Plattform.

▪ Web Training Apps (lokale Installation)

- **OWASP-VWAD** - umfassendes und gut gepflegtes Register aller bekannten anfälligen Webanwendungen.
- **DVWA** - PHP/MySQL-Webanwendung, die verdammt verwundbar ist.
- **metasploitable2** - anfällige Web-Anwendung unter Sicherheitsforschern.
- **metasploitable3** - ist eine VM, die von Grund auf mit einer großen Menge an Sicherheitslücken aufgebaut ist.

◈ DSVW - ist eine absichtlich anfällige Webanwendung, die in weniger als 100 Codezeilen geschrieben wurde.
◈ OWASP Mutillidae II - kostenlose, Open Source, absichtlich anfällige Web-Anwendung.
◈ OWASP Juice Shop Project - die fehlerfreiste anfällige Anwendung überhaupt.
◈ OWASP Node js Goat Project - OWASP Top 10 Sicherheitsrisiken gelten für Webanwendungen, die mit Node.js entwickelt wurden.
◈ juicy-ctf - führen Sie Capture the Flags and Security Trainings mit OWASP Juice Shop durch.
◈ SecurityShepherd - Web- und mobile Anwendungssicherheits-Schulungsplattform.
◈ Security Ninjas - Open-Source-Anwendungssicherheitstrainingsprogramm.
◈ Hackazon - eine moderne verwundbare Web-App.
◈ dvna - verdammt verwundbare NodeJS-Anwendung.
◈ django-DefectDojo - ist ein Open-Source-Tool zur Korrelation und Sicherheitsorchestrierung von Anwendungen.
◈ Google Gruyere - Web-Anwendung Exploits und Verteidigungen.
◈ Bodhi - ist ein Spielplatz, der sich darauf konzentriert, die Ausnutzung von clientseitigen Web-Schwachstellen zu erlernen.
◈ Websploit - Single vm lab mit dem Ziel, mehrere anfällige Applikationen in einer Umgebung zu kombinieren.
◈ vulhub - vorgefertigte Vulnerable Environments basierend auf docker-compose.
◈ CloudGoat 2 - das neue und verbesserte AWS-Bereitstellungstool "Vulnerable by Design".
◈ secDevLabs - ist ein Labor, um sichere Web-Entwicklung in einer praktischen Weise zu lernen.
◈ CORS-vulnerable-Lab - Testen Sie anfälligen Code und seinen Exploit-Code.
◈ RootTheBox - ein Spiel der Hacker (CTF Scoreboard & Game Manager).

▪ Labs (ethische Hacking-Plattformen/Trainings/CTFs)

◈ Offensive Security - echte leistungsbasierte Penetrationstests Seit über einem Jahrzehnt.
◈ Hack The Box - Online-Plattform, die Sie Ihre Penetration Sprossen Fähigkeiten zu testen.
◈ Hacking-Lab - Online ethisches Hacking, Computer-Netzwerk und Sicherheits-Herausforderungplattform.
◈ pwnable.kr - nicht-kommerzielle Wargame-Site, die verschiedene pwn Herausforderungen in Bezug auf System-Ausbeutung bietet.
◈ Pwnable.tw - ist eine Wargame-Website für Hacker, um ihre binären Exploit-Fähigkeiten zu testen und zu erweitern.
◈ picoCTF - ist ein kostenloses Computer-Sicherheitsspiel für Mittel- und Oberschüler.
◈ CTFlearn - ist eine Online-Plattform, die ethischen Hackern dabei helfen soll, ihr Wissen und ihre Fähigkeiten im Bereich Cybersicherheit zu erlernen und zu üben.
◈ ctftime - CTF-Archiv und einen Ort, an dem Sie weitere CTF-bezogene Informationen erhalten können.
◈ Silesia Security Lab - qualitativ hochwertige Sicherheitstestdienste.
◈ Praktische Pentest Labs - pentest lab, bringen Sie Ihre Hacking-Fähigkeiten auf die nächste Ebene.
◈ Root Me - die schnelle, einfache und erschwingliche Möglichkeit, Ihre Hacking-

Fähigkeiten zu trainieren.

- **rozwal.to** - eine großartige Plattform, um Ihre Pentesting-Fähigkeiten zu trainieren.
- **TryHackMe** - Das Erlernen von Cyber Security ist einfach.
- **-Hackxor** - ist ein realistisches Web-Anwendung Hacking-Spiel, entwickelt, um Spieler aller Fähigkeiten zu helfen, ihre Fähigkeiten zu entwickeln.
- **Hack Yourself First** - es ist voll von bösen App sec Löcher.
- **OverTheWire** - kann Ihnen helfen, Sicherheitskonzepte in Form von lustigen Spielen zu lernen und zu üben.
- **Wizard Labs** - ist ein Online-Penetration Testing Lab.
- **PentesterLab** - bietet anfällige Systeme, die zum Testen und Verstehen von Schwachstellen verwendet werden können.
- **RingZer0** - Tonnen von Herausforderungen entwickelt, um Ihre Hacking-Fähigkeiten zu testen und zu verbessern.
- **try2hack** - mehrere sicherheitsorientierte Herausforderungen für Ihre Unterhaltung.
- **Ubeeri** - vorkonfigurierte Laborumgebungen.
- **Pentestit** - emulieren IT-Infrastrukturen von echten Unternehmen für legale Stifttests und Verbesserung der Penetrationstests Fähigkeiten.
- **Microcorruption** - Umkehr Herausforderungen in der Web-Oberfläche getan.
- **Crackmes** - laden Sie Crackmeherunter herunter, um Ihre Reverse Engineering Fähigkeiten zu verbessern.
- **DomGoat** - DOM XSS Sicherheitslern- und Übungsplattform.
- **Stereotyped Challenges** - aktualisieren Sie Ihre Web-Hacking-Techniken noch heute!
- **Vulnhub** - ermöglicht es jedem, praktische "Hands-on"-Erfahrung in der digitalen Sicherheit zu sammeln.
- **W3Challs** - ist eine Penetrationstest-Trainingsplattform, die verschiedene Computer-Herausforderungen bietet.
- **RingZer0 CTF** - bietet Ihnen jede Menge Herausforderungen, die entwickelt wurden, um Ihre Hacking-Fähigkeiten zu testen und zu verbessern.
- **Hack.me** - eine Plattform, auf der Sie anfällige Web-Apps für Bildungs- und Forschungszwecke erstellen, hosten und teilen können.
- **HackThis!** - Entdecken Sie, wie Hacks, Dumps und Verunstumungen durchgeführt werden und sichern Sie Ihre Website gegen Hacker.
- **Enigma Group WebApp Training** - diese Herausforderungen decken die Exploits ab, die im OWASP Top 10 Projekt aufgeführt sind.
- **Reverse Engineering Herausforderungen** - Herausforderungen, Übungen, Probleme und Aufgaben - nach Ebene, Typ und mehr.
- **0x00sec** - die Heimat des Hackers - Malware, Reverse Engineering und Informatik.
- **We Chall** - es gibt viele verschiedene Herausforderungstypen.
- **Hacker Gateway** - ist der Ort für Hacker, die ihre Fähigkeiten testen wollen.
- **Hacker101** - ist eine kostenlose Klasse für Websicherheit.
- **contained.af** - ein dummes Spiel, um mehr über Container, Funktionen und Syscalls zu erfahren.
- **flAWS Herausforderung!** - eine Reihe von Levels, die Sie über häufige Fehler und Gotchas bei der Verwendung von AWS lernen.
- **CyberSec WTF** - bietet Web-Hacking-Herausforderungen, die von Kopfgeld-Schreibaufen

abgeleitet werden.

- **CTF Challenge** - CTF Web App Herausforderungen.
- **gCTF** - die meisten Herausforderungen, die im Google CTF 2017 verwendet werden.
- **Hack This Site** - ist ein kostenloser, sicherer und legaler Schulungsplatz für Hacker.
- **Attack & Defense** - ist ein browserbasiertes Cloud-Labor.
- **Cryptohack** - eine lustige Plattform zum Erlernen moderner Kryptographie.

▪ CTF-Plattformen

- **fbctf** - Plattform, um Capture the Flag Wettbewerbe auszurichten.
- **ctfscoreboard** - Anzeigetafel für Capture The Flag Wettbewerbe.

▪ Sonstige Ressourcen

- **Bugcrowd University** - Open-Source-Bildungsinhalte für die Forschergemeinschaft.
- **OSCPRepo** - eine Liste von Ressourcen und Skripten, die ich in Vorbereitung auf das OSCP gesammelt habe.
- **OWASP Top 10: Real-World Beispiele** - testen Sie Ihre Web-Apps mit realen Beispielen (zweiteilige Serie).
- **phrack.org** - eine tolle Sammlung von Artikeln von mehreren angesehenen Hackern und anderen Denker.
- **Practical-Ethical-Hacking-Resources** - Zusammenstellung von Ressourcen aus dem Udemy Course von TCM.

Ihr tägliches Wissen und Ihre Neuigkeiten [TOC]

▪ RSS-Reader

- **Feedly** - organisieren, lesen und teilen, was ihnen wichtig ist.
- **Inoreader** - ähnlich wie feedly mit einer Unterstützung zum Filtern, was Sie von rss abrufen.

▪ IRC-Kanäle

- **#hackerspaces** - Hackerspace IRC-Kanäle.

▪ Sicherheit

- **The Hacker News** - führende Nachrichtenquelle, die sich der Sensibilisierung für Sicherheitsexperten und Hacker widmet.
- **Neueste Hacking News** - bietet die neuesten Hacking-News, Exploits und Schwachstellen für ethische Hacker.
- **Security Newsletter** - Sicherheitsnachrichten als wöchentlicher Digest (E-Mail-Benachrichtigungen).
- **Google Online Security Blog** - die neuesten Nachrichten und Erkenntnisse von Google über Sicherheit und Sicherheit im Internet.

- **Qualys Blog** - Experten Netzwerk Sicherheit Beratung und Nachrichten.
- **DARKReading** - verbindet die Informationssicherheits-Community.
- **Darknet** - neueste Hacking-Tools, Hacker-News, Cybersicherheit Best Practices, ethische Hacking & Pen-Tests.
- **öffentlich Bekanntwerden** - Public Disclosure Watcher, der Sie über die kürzlich aufgedeckten Fehler auf dem Laufenden hält.
- **Reddit - Hacking** - ein Subreddit für Hacking und Hacker.
- **Packet Storm** - Informationssicherheitsdienste, Nachrichten, Dateien, Tools, Exploits, Ratschläge und Whitepaper.
- **Sekurak** - über Sicherheit, Penetrationstests, Schwachstellen und viele andere (PL/EN).
- **nf.sec** - grundlegende Aspekte und Mechanismen der Linux-Betriebssystemsicherheit (PL).

▪ Sonstiges/All-in-One

- **Changelog** - ist eine Gemeinschaft von Hackern; Nachrichten & Podcasts für Entwickler und Hacker.

Andere Cheat Sheets [TOC]

Erstellen Sie Ihre eigenen DNS-Server

- **Ungebundenes DNS-Tutorial** - ein validierender, rekursiver und zwischenspeichernder DNS-Server.
- **Knot Resolver auf Fedora** - wie man schnellere und sicherere DNS-Auflösung mit Knot Resolver auf Fedora bekommt.
- **DNS-over-HTTPS** - Tutorial zum Einrichten Ihres eigenen DNS-over-HTTPS (DoH)-Servers.
- **dns-over-https** - ein Cartoon-Intro zu DNS über HTTPS.
- **DNS-over-TLS** – nach Ihrem DoH-Server richten Sie Ihren DNS-over-TLS-Server (DoT) ein.
- **DNS-Server** - wie (und warum) führe ich meine eigenen DNS-Server aus.

Erstellen Sie Ihre eigene Zertifizierungsstelle

- **OpenSSL-Zertifizierungsstelle** - Erstellen Sie Ihre eigene Zertifizierungsstelle (Certificate Authority, CA) mit den OpenSSL-Befehlszeilentools.
- **step-ca-Zertifizierungsstelle** - erstellen Sie Ihre eigene Zertifizierungsstelle (Certificate Authority, CA) mit Open Source step-ca.

Erstellen Sie Ihr eigenes System/virtuelle Maschine

- **os-tutorial** - wie man ein Betriebssystem von Grund auf neu erstellt.
- **Schreiben Sie Ihre eigene virtuelle Maschine** - wie Sie Ihre eigene virtuelle Maschine (VM) schreiben.
- **x86 Bare Metal Beispiele** - Dutzende von minimalen Betriebssystemen, um x86 Systemprogrammierung zu lernen.
- **simple-computer** - die scott CPU aus "But How How It Know?" von J. Clark Scott.