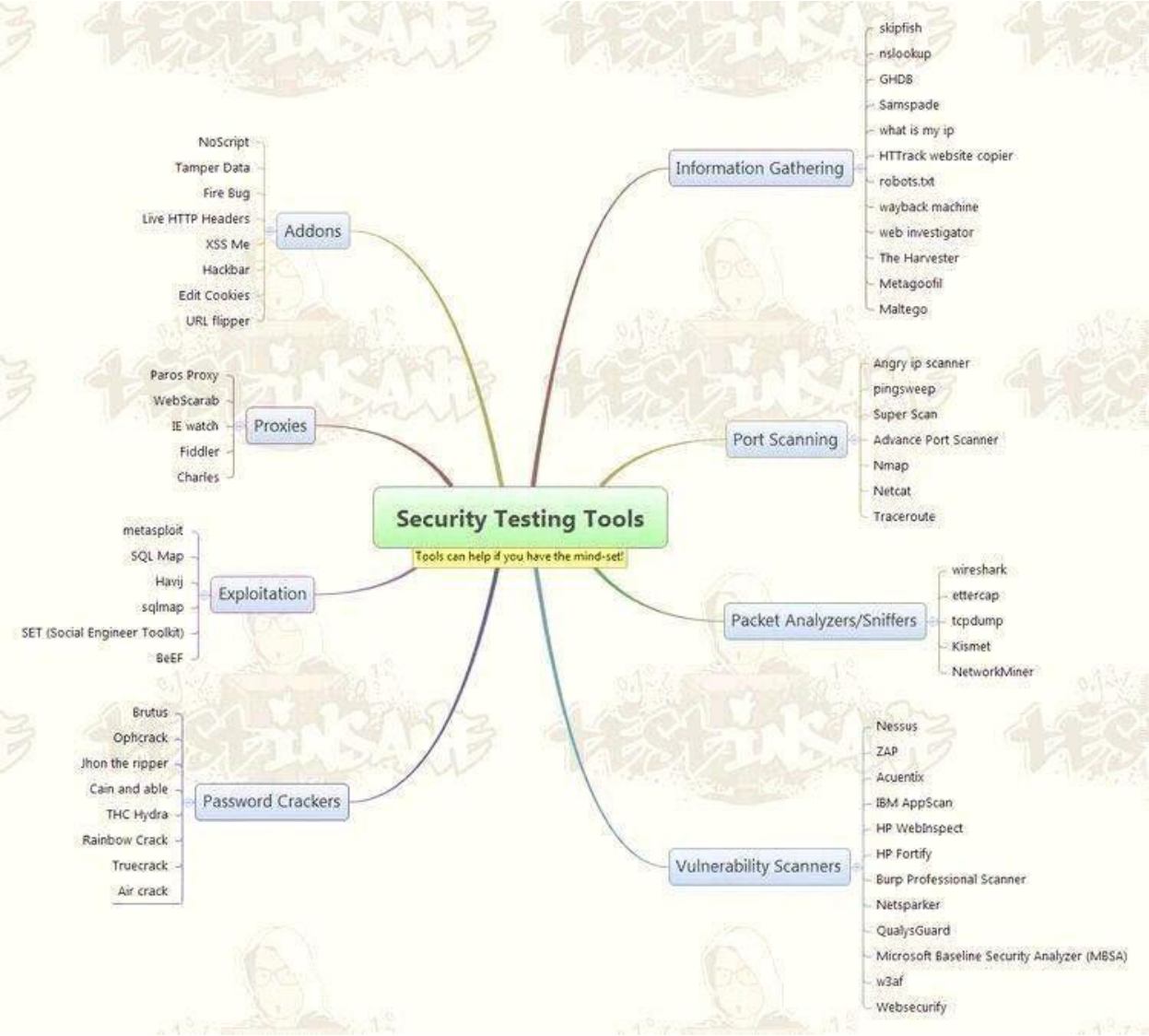
Security tools mind map



🔰**Best Temporary mailbox** (Updates)🔰

Ⓜ self-test for specific purposes, can be used for registration test use, or used to prevent other social workers.

— https://www.guerrillamail.com/en/
— https://10minutemail.com
— https://www.trash-mail.com/inbox/
— https://www.mailinator.com
— http://www.yopmail.com/en
— https://generator.email
— https://en.getairmail.com
— http://www.throwawaymail.com/en
— https://maildrop.cc

— https://owlymail.com/en
— https://www.moakt.com
— https://tempail.com
— http://www.yopmail.com
— https://temp-mail.org/en
— https://www.mohmal.com 👍 Best options
— http://od.obagg.com 👍 Best options
— http://onedrive.readmail.net 👍 Best options
— http://xkx.me 👍 Best options
— https://www.emailondeck.com
— https://smailpro.com
— https://anonbox.net
— https://M.kuku.lu

Few **tool for**:

- Port Forwarding Tester
- What is My IP Address
- Network Location Tools
- Visual Trace Rout Tools
- Phone Number Geolocator
- Reverse E-mail Lookup Tool
- Reverse IP Domain Check
- WHOIS Lookup Tools

https://www.yougetsignal.com/

DNS MAP
https://github.com/makefu/dnsmap/

Stanford Free Web Security Course
https://web.stanford.edu/class/cs253/

Top 10 web hacking techniques of 2019
https://portswigger.net/research/top-10-web-hacking-techniques-of-2019

Testing for WebSockets security vulnerabilities
https://portswigger.net/web-security/websockets

Windows grep Software to Search (and Replace) through Files and Folders on Your PC and Network
https://www.powergrep.com/

Reflected XSS on http://microsoft.com subdomains
https://medium.com/bugbountywriteup/reflected-xss-on-microsoft-com-subdomains-4bdfc2c716df

The Art of Hacking
https://github.com/The-Art-of-Hacking/h4cker/

Remote iPhone Exploitation
https://googleprojectzero.blogspot.com/2020/01/remote-iphone-exploitation-part-1.html
https://googleprojectzero.blogspot.com/2020/01/remote-iphone-exploitation-part-2.html
https://googleprojectzero.blogspot.com/2020/01/remote-iphone-exploitation-part-3.html

Mapping-Injection
https://github.com/antonioCoco/Mapping-Injection

Social Engineering Payloads
https://github.com/t3ntman/Social-Engineering-Payloads

Maryam : Open-source Intelligence (OSINT) Framework
https://github.com/saeeddhqan/Maryam

DarkScrape: OSINT Tool to find Media Links in Tor Sites
https://github.com/itsmehacker/DarkScrape

Rapid7_OSINT
All the tools you need to make your own mind up from the Open Data Sets
https://github.com/tg12/rapid7_OSINT

Sifter : A Osint, Recon & Vulnerability Scanner
https://kalilinuxtutorials.com/sifter/

🔰**Awesome OSINT Navigator**🔰
- Source: https://start.me/p/rxRbpo/ti

Application Security Wiki
https://appsecwiki.com

IoT Security Wiki
https://iotsecuritywiki.com

Zelos - A comprehensive binary emulation platform.
https://github.com/zeropointdynamics/zelos

Learn Authentication The Hard Way
Part I
https://www.andrew-best.com/posts/learn-auth-the-hard-way-part-one
Part II
https://www.andrew-best.com/posts/learn-auth-the-hard-way-part-two
Part III
https://www.andrew-best.com/posts/learn-auth-the-hard-way-part-three

Important tools solving CTF challenges.

++Networking
- Wireshark, tshark
- tcpdump
- netcat, telnet
- nmap

++ Forensics
- dd
- strings
- scalpel
- TrID
- binwalk
- foremost
- ExifTool
- Any hex editor
- DFF
- CAINE
- The Sleuth kit
- Volatility

++Crypto
- Cryptool
- hashpump
- Sage
- John the Ripper
- hashcat
- Online tools(web)
- Modules for python

++Stegano
- OpenStego
- OutGuess
- Steghide
- StegFS

- pngcheck
- Gimp
- Audacity
- Mp3Stego
- ffmpeg
- Own tools

++Reverse
- GDB
- IDA Pro
- Immunity Debugger
- OllyDbg
- Radare2
- nm
- objdump
- strace
- ILSPy(.NET)
- JD-GUI(Java)
- FFDec(Flash)
- dex2jar(Android)
- uncomplye2(Python)
- Any hex editor
- Exe unpackers
- Resource unpackers
- Compilers

500 gb of Programming languages tutorial collection ranges from
- C
- C++
- Citrix
- Go
- Java Android
- Javascript
- Linux
- Php
- Python
- Ruby
- And general Stuff

Link :
https://drive.google.com/drive/mobile/folders/0B6RiB8cVZQhmTDZvN0JadGtScGs/0ByWO0aO1eI_MN1BEd3VNRUZENkU?sort=13&direction=a

Best books for hacking!!

1.**Hacking: How to Hack Computers, Basic Security and Penetration Testing Ebook**

Download Link : https://drive.google.com/file/d/0B4CdA3JV_23OSW5BTVlNU1RlaW8/view

2.**Master the Kali Linux - From Noob to Expert Hacking - 8 Ebooks**
Download Link : http://www.mediafire.com/file/wv4sun24cwoow17/Kali+tutorial.rar

3.**Grey Hat Hacking - The Ethical Hacker's Handbook Ebook**
Download Link : https://drive.google.com/file/d/0Bw1xURlCeiXiQXphUzlLTV8xWmM/view

4.**Hacking The Art of Exploitation Ebook**
Download Link : http://www.mediafire.com/file/ht5dy5dwmf4h0j7/hacking-the-art-of-exploitation.pdf

5.**The Hacker's Underground Hand Book.**
Download Link : http://www.mediafire.com/file/kb94m3pa9zahrv9/The-Hackers-Underground-Handbook.pdf

Here are few links (Ebooks) that you guys might be interested.

1. **The Hacker Playbook : Practical Guide To Penetration Testing**
Link : http://www.allitebooks.com/the-hacker-playbook-practical-guide-to-penetration-testing/

2.**The Hacker Playbook 2: Practical Guide To Penetration Testing**
Link : http://www.allitebooks.com/the-hacker-playbook-2-practical-guide-to-penetration-testing/

3. **Android Hacker's Handbook**
Link : http://www.allitebooks.com/android-hackers-handbook/

4. **BackTrack 5 Wireless Penetration Testing Beginner's Guide**
Link : http://www.allitebooks.com/backtrack-5-wireless-penetration-testing-beginners-guide/

---

10 Best Penetration Testing Tools 2020

Metasploit, NMAP, Wireshark, Aircrack, Nessus, Social Engineering Toolkit, W3AF, Burp Suite, BeEF, SQLmap
https://cybersecuritynews.com/penetration-testing-tools/

System hacking full course:
Google drive link:
https://drive.google.com/drive/folders/18Jx6zVsZDzw3rSXLpkPocP44nMRpnYQH
A collection of inspiring lists, manuals, cheatsheets, blogs, hacks, one-liners, cli/web tools, and more.
https://github.com/trimstray/the-book-of-secret-knowledge

An Introduction to Buffer Overflow Vulnerability
https://medium.com/better-programming/an-introduction-to-buffer-overflow-vulnerability-760f23c21ebb

---

Awesome Malware Analysis
https://github.com/rshipp/awesome-malware-analysis

SANS Cyber Aces Online Tutorials
https://tutorials.cyberaces.org/tutorials.html

HQL Injection Exploitation in MySQL
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/hql-injection-exploitation-in-mysql/

Using WebRTC ICE Servers for Port Scanning in Chrome
https://medium.com/tenable-techblog/using-webrtc-ice-servers-for-port-scanning-in-chrome-ce17b19dd474

Source Code Analysis SQL Injection
http://ghostlulz.com/source-code-analysis-sql-injection/

Hacker High School PDF File:
01 Being a Hacker
02 Windows and Linux
03 Ports and Protocols
04 Services and Connections
05 System Identification
06 Malware
07 Attack Analysis
08 Forensics
09 Email Security
10 Web Security and Privacy
11 Passwords
12 Legalities
Link: https://drive.google.com/drive/folders/1F-uR5JHOlYM6tRcjJFnrdrRVMCk3hlQq

Hacking EBooks **Basic Hacking until Advance Hacking**

https://drive.google.com/drive/folders/1Tv_tLTeotyMcJz6mR0cOba1FaEnqaNbQ

Hacking-Security-Ebooks
Top 100 Hacking & Security E-Books (Free Download) - Powered by Yeahhub.com
https://github.com/yeahhub/Hacking-Security-Ebooks

Hacker Ebook
•Car Hacker Handbook
•The hacker playbook 1,2,3
•Grey hat Hacking
•Advanced Penetration testing
•Black hat python
•Defensive security
•Hacking-the art of exploitation
•Kali revealed
•Advanced pentesting by Cybrary
Many more go check it out

MORE THAN 100 HACKING EBOOK BEST COLLECTION
https://drive.google.com/drive/folders/17HQBvUleU9n8HuRIv8_Tm7geZsx_wa4W

Learn Ethical Hacking From Scratch [UPDATED]
Become an ethical hacker that can hack computer systems like black hat hackers and secure them like security experts.
Udemy Link 👇
https://www.udemy.com/learn-ethical-hacking-from-scratch/

Drive Link 👇
https://drive.google.com/drive/folders/1qhLjmXvzxxkhgZoXoGsXhNm8KjOrtGCT

Hacking wireless network:
Full course:
https://drive.google.com/drive/folders/1AEoreiuwP- nwNTtYPtsfySgiZmWVyom9

Metasploit course:
Google drive:
https://drive.google.com/drive/folders/1YLPpd9RhdbW3Icrfz4HM147C0y_IGPhE
Complete Kali Linux Tutorial, Complete Penetration Testing Training, Learn Hacking
Download : https://drive.google.com/drive/u/0/folders/1NFG4Li5Q7uulp7Hpn8t3ZkWvviGVg-fJ

#Computer_Forensics
Full course just for you :
https://drive.google.com/drive/folders/1luUwu4kyZ0YgBAPL_F5CZ6aDX6grETw0

🔰 **Udemy:- Learn Network Attacks and Security** 🔰
#udemy #network

This Video Tutorial Will Help You To Learn Different Types Of Network Attacks And Secure Yourself From It
https://drive.google.com/drive/u/0/mobile/folders/1PPv133qe42Tzhxu9BNitLM8lzTWylZxy

---

👍**CTF/Wargames**
https://overthewire.org/wargames
https://www.pentesterlab.com
http://www.itsecgames.com
https://exploit-exercises.com
https://www.enigmagroup.org
http://smashthestack.org
http://3564020356.org
https://www.hackthissite.org
http://www.hackertest.net
http://0x0539.net
https://vulnhub.com
https://ringzer0team.com
https://root-me.org
https://microcorruption.com
http://abctf.xyz
http://pwnable.kr
https://ctftime.org
https://www.vulnhub.com
https://w3challs.com/challenges/hacking
http://forensicscontest.com/puzzles
https://xss-game.appspot.com
http://pwnable.tw
https://io.netgarage.org
https://www.mavensecurity.com/resources/web-security-dojo

OWASP Wordpress Security Implementation Guideline

https://www.owasp.org/index.php/OWASP_Wordpress_Security_Implementation_Guideline

OWASP API Security Top 10
https://github.com/OWASP/API-Security/blob/develop/2019/en/dist/owasp-api-security-top-10.pdf

OWASP Firmware Security Testing Methodology
https://scriptingxss.gitbook.io/firmware-security-testing-methodology/

Introduction OWASP Nettacker
https://www.youtube.com/watch?v=rZfCFFewfiU&list=PLhaoFbw_ejdo-4nSeRKNH1pRhdfsn3CI7&index=46

OWASP AppSec California Video
https://www.youtube.com/channel/UCCLyDbVQ5Yls9WYgKcWVyFA

WARNING! All versions of #Microsoft Windows (7, 8.1, 10, Server 2008, 2012, 2016, 2019) operating systems contain 2 new font parsing library RCE vulnerabilities that are:
—CRITICAL
—UNPATCHED
—Under active ZERO-DAY attacks

No patch available, so all Windows users are highly recommended to immediately apply workarounds (mentioned in the article) to reduce the risk of getting hacked.
Details ➤ https://thehackernews.com/2020/03/windows-adobe-font-vulnerability.html

---

VulnSpy privides materials allowing anyone to gain practical hands-on experience with cyber security.
https://www.vulnspy.com/

🔰**Online tool: XSS'OR - Hack with JavaScript** 🔰
▪Link: http://xssor.io

Cross-site scripting (XSS) cheat sheet
https://portswigger.net/web-security/cross-site-scripting/cheat-sheet

Awesome GitHub Repos
1. Book of Secret Knowledge = https://lnkd.in/fWKCdi4
2. Awesome Hacking = https://lnkd.in/f7VPTEX
3. Awesome Bug Bounty = https://lnkd.in/fPrQiVD
4. Awesome Penetration Testing = https://lnkd.in/fAUZgu5
5. Awesome Web Hacking = https://lnkd.in/f5n2hSd
6. Awesome Hacking Resources = https://lnkd.in/fcJ6wFH

7. Awesome Pentest = https://lnkd.in/fNNSFeN
8. Awesome Red Teaming = https://lnkd.in/fGpievF
9. Awesome Web Security = https://lnkd.in/ffG73u2
10. Penetration Test Guide based on OWASP = https://lnkd.in/ffyBwzG
11. Pentest Compilation = https://lnkd.in/f5JwJTD
12. Infosec Reference = https://lnkd.in/fY6wNmX

Bashar Bachir Analysis
https://github.com/itsKindred/malware-analysis-writeups/blob/master/bashar-bachir-chain/bashar-bachir-analysis.pdf

Penetration Testing Tools Cheat Sheet
https://highon.coffee/blog/penetration-testing-tools-cheat-sheet/

Reverse Shell Cheat Sheet
https://highon.coffee/blog/reverse-shell-cheat-sheet/

Security-cheatsheets
A collection of useful cheatsheets for cheat that focuses on aiding security-type people with either security tools or popular UNIX programs.
https://github.com/andrewjkerr/security-cheatsheets

Pentesting Cheatsheet – root@Hausec
https://hausec.com/pentesting-cheatsheet/

"**Google Dorks List 2018** — Fresh Google Dorks 2018 For SQLi" by Waziristani Haxor
https://link.medium.com/3T1WmO5VJ2

The **Kostebek** is a reconnaissance tool which uses firms' trademark information to discover their domains.
https://github.com/esecuritylab/kostebek

iOS Application Injection
https://arjunbrar.com/post/ios-application-injection

Alert Alarm SMS exploit - English version
https://jyx.github.io/alert-alarm-exploit.html

Open-AudIT is an application to tell you exactly what is on your network, how it is configured and when it changes
https://www.open-audit.org/index.php
Inspire women to fall in love with programming
https://djangogirls.org

Reversing and exploiting books
https://github.com/hdbreaker/ExploitingBooks

CVE-2020-0796 | Windows #SMBv3 Client/Server Remote Code Execution Vulnerability
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0796
https://thehackernews.com/2020/03/patch-wormable-smb-vulnerability.html

Dirilis kerentanan cve-2020-0796. Anda bisa mendapatkan tambalan dengan pergi ke alamat di bawah ini dan menginstalnya di sistem Anda.

📥https: //portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0796

Anda harus melakukan yang berikut untuk mengunduh pembaruan keamanan.

1- Tekan tombol windows + R untuk membuka RUN dan masukkan perintah Winver untuk menampilkan versi OS.
2- Unduh dan instal pembaruan sesuai dengan versi Windows Anda.
3- Mulai ulang Windows Anda.

Anda dapat bertindak dalam dua cara untuk memastikan tambalan diinstal.

CM Menggunakan CMD
Salin dan jalankan perintah berikut dalam CMD.

Mfm qfe dapatkan Keterangan, Keterangan, HotFixID, InstalledOn | findstr / C: "KB4551762"

Powers Menggunakan PowerShell
Salin dan jalankan perintah berikut di PowerShell.
⚙ Get-HotFix -HFID KB4551762

---

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200005

Peringatan serius

كد Kerentanan eksekusi kode jauh di sistem operasi Windows SMBv3

Dalam tambalan keamanan Microsoft yang dirilis pada 10 Maret 2020, Microsoft menerapkan kesadaran kerentanan pada SMBv3 yang memungkinkan eksekusi kode jarak jauh dan distribusi seperti cacing pada sistem yang rentan.
Meskipun belum jelas kapan Microsoft akan berusaha untuk memperbaiki tambalan, perusahaan menginginkan penggunanya untuk menonaktifkan SMBv3 sebagai solusi dan

memblokir koneksi TCP port 2 pada firewall dan komputer pengguna.

Jalur pengaturan ItemProperty adalah sebagai berikut:

"HKLM: \ SYSTEM \ CurrentControlSet \ Services \ LanmanServer \ Parameters"

Dan nonaktifkan Compression -Type DWORD -Value 1 -Force section.

Microsoft juga memperingatkan bahwa menonaktifkan kompresi SMBv3 tidak mencegah eksploitasi kerentanan ini dan mengharuskan SMB sepenuhnya dinonaktifkan.

Researchers discovered a new ransomware strain dubbed Pxj that encrypts users' files appends ".pxj" extension to the encrypted files. The new ransomware strain was discovered by IBM's X-Force Incident Response team, and the ransomware malware is all known as "XVFXGW". PXJ Ransomware The PXJ Ransomware code appears to be a new one, it doesn't share […]
The post New PXJ Ransomware Delete's Backup Copies and Disable's User Ability to Recover any Files (https://gbhackers.com/new-pxj-ransomware/) appeared first on GBHackers On Security (https://gbhackers.com/).

Here's how CISOs should prepare for Coronavirus-related cyber threats ➤
https://thehackernews.com/2020/03/coronavirus-cybersecurity-ciso.html

Memhunter is an Automated Memory Resident Malware Detection tool for the hunting of memory resident malware at scale, improving the threat hunter analysis process and remediation times.

It's a self contained binary that can be deployed and managed at scale, does not use memory dumps and relies purely on memory inspection to do its work. It also does not require any complex infrastructure to deploy.
The tool was designed as a replacement of memory forensic volatility plugins such as malfind and hollowfind.
Read the rest of Memhunter – Automated Memory Resident Malware Detection now! Only available at Darknet. (https://www.darknet.org.uk/2020/03/memhunter-automated-memory-resident-malware-detection/)

Reverse engineering focusing on x64 Windows.
https://github.com/0xZ0F/Z0FCourse_ReverseEngineering

Reverse Engineering for Beginners
https://www.begin.re

Reverse Engineering Resource Collection. 3000+ open source tools, ~600 blog post
https://github.com/alphaSeclab/awesome-reverse-engineering/blob/master/Readme_en.md

Awesome A curated list of awesome reversing resources
https://github.com/wtsxDev/reverse-engineering

Interactive guide to Buffer Overflow exploitation
https://nagarrosecurity.com/blog/interactive-buffer-overflow-exploitation

Linux Forensic - Everything related to Linux Forensics
https://github.com/ashemery/LinuxForensics

Automated Detection of Web Application Firewall
https://github.com/EnableSecurity/wafw00f

Script to Bypass SSL/Certificate Pinning in Android
https://github.com/51j0/Android-CertKiller

GraphQLmap is a scripting engine to interact with a graphql endpoint for pentesting purposes.
https://github.com/swisskyrepo/GraphQLmap

eGain Web API Email Header Injection
https://medium.com/maverislabs/cve-2019-17123-cbc946c99f8

EXIST is a web application for aggregating and analyzing cyber threat intelligence.
https://github.com/nict-csl/exist

🔰**Reverse TCP shell with Powershell**
https://github.com/ZHacker13/ReverseTCPShell

Toolkit to detect and keep track on Blind XSS, XXE & SSRF
https://github.com/SpiderMate/B-XSSRF

Network Infrastructure Penetration Testing Tool
https://github.com/SECFORCE/sparta

Drone pentesting framework console 😱🙈
https://github.com/dhondta/dronesploit

Wordlists for creating statistically likely username lists for use in password attacks and security testing

- http://weakpass.com
- http://hashes.org
- http://github.com/danielmiessler/SecLists
- http://github.com/berzerk0/Probable-Wordlists
- http://github.com/insidetrust/statistically-likely-usernames

Security Engineering — Third Edition
https://www.cl.cam.ac.uk/~rja14/book.html

Andorid Malware Adventures
https://www.linkedin.com/posts/kursatoguzhanakinci_deepsec-andorid-malware-adventures-activity-6608615164038131712-1Yrf

Developer Tools to Increase Your Productivity
medium.com/better-programming/developer-tools-to-increase-your-productivity-6f4ec0c96dd9

Android App Reverse Engineering 101
https://maddiestone.github.io/AndroidAppRE/

Android Pentest Suite
https://github.com/tiennguyen1510/Android-Pentest-Suite

HeapViewer
An IDA Pro plugin to examine the heap, focused on exploit development.
https://github.com/danigargu/heap-viewer
http://telegram.org/blog/ton-gram-notice
https://relayto.com/relayto/telegram-open-network-ton-ico-whitepaper-6kf4rycn/pdf

How to create an OS from scratch
https://github.com/cfenollosa/os-tutorial

BurpSuite

https://github.com/alphaSeclab/awesome-burp-suite/blob/master/Readme_en.md

OnionScan is a free and open source tool for investigating the Dark Web. For all the amazing technological innovations in the anonymity and privacy space, there is always a constant threat that has no effective technological patch - human error. [OnionScan]
https://github.com/s-rah/onionscan

Sudomy is a subdomain enumeration tool, created using a bash script, to analyze domains and collect subdomains in fast and comprehensive way . Report output in HTML or CSV format

https://github.com/Screetsec/Sudomy

Tmux Cheat Sheet & Quick Reference
https://tmuxcheatsheet.com

Tactical tmux: The 10 Most Important Commands
https://danielmiessler.com/study/tmux

Moloch is an open source, large scale, full packet capturing, indexing, and database system.
http://molo.ch

Awesome Competitive Programming
https://github.com/lnishan/awesome-competitive-programming

DevOps vs. Site Reliability Engineering (SRE)
https://youtu.be/V-B3XDaSadg

The Mobile Hacking CheatSheet
https://github.com/randorisec/MobileHackingCheatSheet

Awesome Mobile Security
https://github.com/vaib25vicky/awesome-mobile-security

Introduction to Android Hacking
https://www.hackerone.com/blog/androidhackingmonth-intro-to-android-hacking

Common port security risks & test
#port
DNS (53) UDP
SMTP (25) TCP
SNMP (161) UDP
SSH (22) TCP
FTP (21) TCP
Telnet (23) TCP
TFTP (69) UDP
RPC (111) TCP / UDP
NTP (123) UDP
Mssql (1433) TCP
Oracle (1521) TCP
RDP (3389) TCP
SIP (5060)
https://securityonline.info/common-port-security-risks-test-methods/

Red Teaming Toolkit Collection

https://github.com/infosecn1nja/Red-Teaming-Toolkit

Red-Teaming-Toolkit
A collection of open source and commercial tools that aid in red team operations.
https://github.com/infosecn1nja/Red-Teaming-Toolkit

Red Teaming Toolkit Collection
https://0xsp.com/offensive/red-teaming-toolkit-collection

Blue Team Cybersecurity Training
https://blueteam.academy/

RedGhost
Linux post exploitation framework designed to assist red teams in gaining persistence, reconnaissance and leaving no trace.
https://github.com/d4rk007/RedGhost

DEEPWARE SCANNER
https://www.deepware.ai

EC2 Security Strategy
https://asecure.cloud/g/strategy_ec2_security/

Flan Scan is a lightweight network vulnerability scanner. With Flan Scan you can easily find open ports on your network, identify services and their version, and get a list of relevant CVEs affecting your network.
A pretty sweet vulnerability scanner
https://github.com/cloudflare/flan

Social Scanner API Documentation
Find a given username instantly across 20 social networks with links to each profile in JSON!
https://rapidapi.com/dmchale.dev/api/social-scanner

SSRF_Vulnerable_Lab
EE | SSRF Vulnerable LAB | https://github.com/incredibleindishell/

hundreds of ethical hacking & penetration testing & red team & cyber security & computer science resources.
https://github.com/blaCCkHatHacEEkr/PENTESTING-BIBLE

Online operating system tester (Test a new operating system)
http://distrotest.net

Android Application Security Series
https://manifestsecurity.com/android-application-security/?fbclid=IwAR05NAISuICZTcXa4iBLRWFHIUFSJYA5iziY_-h4LIXxkW8DBYcnnVVdArE
Android Pentesting/Bug Hunting 101
-set-up Burp
-bruteforce OTP
-ADB leaks
-IDOR vulnerability
-list of static & dynamic vulnerabilities you should always check
https://link.medium.com/Ohrs3M1eFY

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing framework capable of performing static, dynamic and malware analysis. It can be used for effective and fast security analysis of Android, iOS and Windows mobile applications and support both binaries (APK, IPA & APPX) and zipped source code.
Project Link :
https://github.com/MobSF/Mobile-Security-Framework-MobSF

Galileo - Web Application Audit Framework
#pentest
Galileo is an open source penetration testing tool for web application, which helps developers and penetration testers identify and exploit vulnerabilities in their web applications.
https://github.com/m4ll0k/Galileo

How to Find out if you are under a DDoS Attack?
https://gbhackers.com/find-under-ddos-attack/

PENETRATION TESTING PRACTICE LAB - VULNERABLE APPS / SYSTEMS
https://www.amanhardikar.com/mindmaps/Practice.html

Penetration Testing Reference Bank - OSCP / PTP & PTX Cheatsheet
https://github.com/OlivierLaflamme/Cheatsheet-God

Penetration Testing Tools Cheat Sheet
https://highon.coffee/blog/penetration-testing-tools-cheat-sheet/

OSCP All Tools are Here
https://github.com/anandkumar11u/OSCP-60days

INE - OSCP Security Technology Course
https://drive.google.com/drive/folders/1b5irX384k4irnchVV4QSeWoupHxW6GP6

M0nkeyShell:

How to prepare for OSCP complete guide
Below are 5 skills which you have to improve before registering for OSCP
> Learn basic of Computer Network, Web application, and Linux
> Learn Bash and Python scripting
> Enumeration is key in OSCP lab, I repeat Enumeration is key in OSCP Lab and in real world too
> Download vulnerable VM machines from vulnhub
> Buffer Overflow (BOF) exploitation

Below are the free reference before registration of OSCP
> https://www.cybrary.it/course/ethical-hacking/
> https://www.cybrary.it/course/web-application-pen-testing/
> https://www.cybrary.it/course/advanced-penetration-testing/
> https://www.offensive-security.com/metasploit-unleashed/
> https://www.cybrary.it/course/python/

Below are the reference for Buffer overflow and exploit developmet for OSCP
> http://www.fuzzysecurity.com/tutorials/expDev/1.html
> https://www.corelan.be/index.php/2009/07/19/exploit-writing-tutorial-part-1-stack-based-overflows/

For Bash Scripting
> http://www.tldp.org/LDP/Bash-Beginners-Guide/html/

Privilege Escalation:
> http://www.greyhathacker.net/?p=738
> http://www.fuzzysecurity.com/tutorials/16.html
> https://github.com/GDSSecurity/Windows-Exploit-Suggester
> http://pwnwiki.io/#!privesc/windows/index.md
> https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/
> https://github.com/rebootuser/LinEnum
> https://www.youtube.com/watch?v=PC_iMqiuIRQ
> https://www.adampalmer.me/iodigitalsec/2013/08/13/mysql-root-to-system-root-with-udf-for-windows-and-linux/

Port redirection/tunneling
> https://chamibuddhika.wordpress.com/2012/03/21/ssh-tunnelling-explained/
> http://www.abatchy.com/search/label/Networking

Practise Lab online & offline --- Most of this lab help you to understand different attack and (privilege escaltion very very important for OSCP)
> http://overthewire.org/wargames/bandit/
> https://www.explainshell.com/
> https://www.vulnhub.com/?q=kioptrix&sort=date-asc&type=vm
> https://www.vulnhub.com/entry/fristileaks-13,133/

> https://www.vulnhub.com/entry/brainpan-1,51/ (Buffer overflow vm)
> https://www.vulnhub.com/entry/mr-robot-1,151/
> https://www.vulnhub.com/entry/hacklab-vulnix,48/
> https://www.vulnhub.com/entry/vulnos-2,147/
> https://www.vulnhub.com/entry/sickos-12,144/
> https://www.vulnhub.com/entry/devrandom-scream,47/
> https://www.vulnhub.com/entry/skytower-1,96/
> https://github.com/rapid7/metasploitable3/wiki

Malware Analysis Training
https://github.com/OpenRCE/Malware-Analysis-Training

ckoo VM for Malware Analysis By binaryzone
Things you need:
1. The VM from here.
2. Username: user1 & Password: forensics
3. Add a Windows ISO to your Cuckoo VM
4. Submit a sample and get some results…
https://archive.org/download/CuckooVM

Fhex - A Fucking HexEditor
https://github.com/echo-devim/fhex

Zero Day Initiative
https://www.zerodayinitiative.com/advisories/ZDI-20-258/

Cross Site Scripting (XSS) Vulnerability Payload List
https://github.com/payloadbox/xss-payload-list

Awesome
https://github.com/sindresorhus/awesome

Awesome lists for hackers
https://github.com/Hack-with-Github/Awesome-Hacking

RAT And C&C Resources
https://github.com/alphaSeclab/awesome-rat

Collection of burpsuite plugins
https://github.com/Mr-xn/BurpSuite-collections

Malware Analysis & Reverse Engineering Course
https://class.malware.re

List of awesome reverse engineering resources
https://github.com/wtsxDev/reverse-engineering

Bypassing-Web-Application-Firewalls-And-XSS-Filters
https://github.com/frizb/Bypassing-Web-Application-Firewalls

[dos] Microsoft Windows 10 (1903/1909) - 'SMBGhost' SMB3.1.1 'SMB2_COMPRESSION_CAPABILITIES' Buffer Overflow (PoC)
https://www.exploit-db.com/exploits/48216

Adama
Searches For Threat Hunting and Security Analytics
https://github.com/randomuserid/Adama

Nord vpn acc
https://throwbin.io/LJWgn9c

Several sites for #Obfuscation or JavaScript code obscurity.
http://utf-8.jp/public/aaencode.html
http://utf-8.jp/public/jjencode.html
http://www.jsfuck.com

Learn Authentication The Hard Way
Part I
https://www.andrew-best.com/posts/learn-auth-the-hard-way-part-one
Part II
https://www.andrew-best.com/posts/learn-auth-the-hard-way-part-two
Part III
https://www.andrew-best.com/posts/learn-auth-the-hard-way-part-three

An Introduction to Buffer Overflow Vulnerability
https://medium.com/better-programming/an-introduction-to-buffer-overflow-vulnerability-760f23c21ebb

---

scanning wordpress - online
https://wpsec.com
https://scanurl.net/
http://www.scanwp.com/
https://quttera.com/
https://www.virustotal.com

C++ for Hackers
https://vimeo.com/384348826

Hacker Roadmap
https://github.com/sundowndev/hacker-roadmap

Hacker tools on Go (Golang)
https://github.com/dreddsa5dies/goHackTools

Movies about Hackers, Hacking, Computers and Technology
https://www.imdb.com/list/ls000393956/

Critical Security Flaw Found in WhatsApp Desktop Platform Allowing Cybercriminals Read From The File System Access
https://www.perimeterx.com/tech-blog/2020/whatsapp-fs-read-vuln-disclosure/

PASSWORD HASH LOOKUP/CRACKING ONLINE: #cracking
#pasword
hashkiller.co.uk/Cracker
cmd5.org
crack.sh
gpuhash.me
crackstation.net
onlinehashcrack.com
hash.help
passwordrecovery.io
cracker.offensive-security.com

11 Online Free Tools to Scan Website Security Vulnerabilities & Malware
#scanner
Tools Lists

1. https://www.scanmyserver.com/
2. http://sucuri.7eer.net/c/245992/212721/3713?u=https%3A%2F%2Fsitecheck.sucuri.net%2F
3. http://www.quttera.com/
4. https://www.acunetix.com/vulnerability-scanner/register-online-vulnerability-scanner/https://www.siteguarding.com/en/affiliate?partner_id=3662Acunetix
5. https://detectify.com/
6. https://www.siteguarding.com/en/affiliate?partner_id=3662
7. https://app.webinspector.com/UpGuard

8. https://www.netsparker.com/online-web-application-security-scanner/Observatory
9. https://app.upguard.com/webscan
10. https://observatory.mozilla.org/
11. https://www.tinfoilsecurity.com/

#Steganography - A list of useful tools and resources
https://0xrick.github.io/lists/stego/

Empat puluh situs bagus, beberapa di antaranya mungkin merupakan ide bisnis yang sukses

Kali ini kami ingin memperkenalkan 40 situs bagus kepada teman-teman. Beberapa di antaranya mungkin bermanfaat bagi Anda.

1. Situs Lynda adalah situs web tempat lebih dari 4 juta orang berlatih (Lynda.com sekarang adalah LinkedIn Learning).
2. Cari tau 101 Free Online Journal and Research Databases.
3. Situs Creative Life: Bawalah kreativitas Anda dengan kelas online gratis.
4. Situs Hackaday: Kembangkan keterampilan Anda dengan rekomendasi harian dari situs web ini.
5. Situs MindTools: Tempat untuk mempelajari keterampilan manajemen
6. Situs Codecademy: Di sekolah online ini Anda dapat belajar bekerja dengan Java, PHP, Python, dan banyak lagi.
7. Situs EdX: Situs web ini menawarkan banyak kursus online termasuk pemrograman.
8. Situs Platzi: Dapatkan pelatihan profesional dalam pemasaran, coding, pengembangan aplikasi dan desain dengan situs web ini.
9. Situs Big Think: Temukan artikel dan video tentang pemikir hebat di situs ini.
10. Situs kerajinan: Pelajari melalui tutorial menyenangkan oleh para ahli di bidang seni seperti memasak, merajut, menjahit, menghias kue dan banyak lagi.
11. Situs: Sumber lengkap kiat dan saran tentang topik apa pun yang mungkin Anda pikirkan.
12. Situs Lifehacker: Tips untuk kehidupan sehari-hari
13. Situs LitLovers: Pecinta sastra memiliki akses ke kursus online gratis di area ini.
14. Situs Udacity: Pelajari Pengodean Gratis di Kursus Online Gratis bersama Sebastian Tran.
15. Situs Zidbits: Tempat untuk mengakses artikel dan berita menarik dan fakta aneh
16. Situs TED Ed: Kumpulan tutorial berharga tentang berbagai topik
17. Situs Scitable: Jika Anda tertarik pada genetika, Anda dapat mempelajari tentang situs ini.
18. Situs ITunes U: Universitas ternama seperti Harvard dan Yale berbagi podcast di sini.
19. Situs Livemocha: Terhubung dengan 190 bahasa untuk mempelajari bahasa baru.
20. Situs MIT Open Courseware: Bergabunglah dengan Universitas MIT untuk mempelajari dasar-dasar pengkodean.
21. Situs WonderHowTo: Situs ini menawarkan video baru setiap hari untuk mempelajari cara melakukan berbagai hal.
22. Situs FutureLearn: Bergabung dengan tiga juta pengguna situs ini dan berpartisipasi dalam kursus tentang belajar dari kesehatan hingga sejarah.
23. Situs One Month: Pelajari keterampilan baru dalam sebulan.
24. Situs Khan Academy: Salah satu Platform Pendidikan Online Paling Populer dengan Tema Game
25. Situs Yousician: Bagaimana Anda belajar musik?
26. Situs Duolingo: Situs pembelajaran bahasa gratis
27. Situs Squareknot: Kreativitas juga bisa dipelajari.
28. Situs Web Highbrow: Layanan berlangganan yang mengirimi Anda tutorial lima menit setiap hari ke email Anda.
29. Situs Spreeder: Pelajari cara membaca di situs ini

30. Situs Memrise: Tingkatkan pengetahuan kosakata Anda.
31. Situs HTML5Rocks: Google profesional berbagi pembaruan terbaru, kiat sumber daya dan informasi terkait HTML5 lainnya dengan Anda.
32. Situs Daftar Artikel Wikipedia Daily: Dapatkan artikel Wikipedia di email Anda setiap hari.
33. Situs DataMonkey: Pelajari SQL dan Excel di situs ini.
34. Situs Saylor Academy: Belajar untuk mempresentasikan dan memberi kuliah dengan kursus online di situs ini.
35. Situs Cook Smarts: Pelajari memasak dasar dan profesional di situs ini.
36. Situs The Happiness: Belajar Menjadi Bahagia.
37. Situs: Kursus konten khusus dari fotografi hingga blogging
38. Situs Surface Languages: Jika Anda perlu belajar hanya beberapa kata dalam bahasa baru untuk perjalanan, jangan lewatkan situs ini.
39. Situs Academic Earth: Kursus akademik lanjutan tersedia dari 2009 hingga sekarang.
40. Situs Make: Pelajari cara melakukan hal-hal sederhana di rumah dan jadilah tukang reparasi Anda sendiri.

CompTIA Security+ Virtual Class.
ALL videos are in English.
Recorded Sessions:
Session 1: https://youtu.be/d_AU2g5dS6c
Session 2: https://youtu.be/6_LlVVlTQIY
Session 3: https://youtu.be/4BYsNI9kCbg
Session 4: https://youtu.be/mtINx1ROHDw
Session 5: https://youtu.be/yaSVeVZMEAQ
Session 6: https://youtu.be/4HpVH-h8xwI
Session 7: https://youtu.be/WSKZqHhRpuQ

Cybersecurity Analyst Internship Program.
CompTIA Pentest+ Virtual Class.
ALL videos are in Bahasa Indonesia.
Recorded Sessions:
Session 1: https://youtu.be/1Fm5lf0J4uQ
Session 2: https://youtu.be/QtO7ehcmS2Q
Session 3: https://youtu.be/ObwMe7gU_DQ
Session 4: https://youtu.be/ZeSpWx5jCMs
Session 5: https://youtu.be/GxGcHEI99tg

Docker for Web Apps Pentest:
https://youtu.be/zewCPGCoqhw