

Cyber Security: Zero to Mastery

For more courses, resources and workshop, visit <https://zerotomastery.io>



Resources for the course:

1. Introduction To Cyber Security & History:

- Short History of Cyber Security - <https://cyber-security.degree/resources/history-of-cyber-security/>
- Cyber Security Roles - <https://www.geeksforgeeks.org/different-job-roles-in-cyber-security/>
- How to Approach the Cyber Security field - <https://cybersecurityguide.org/resources/cybersecurity-jobs/>

2. Cyber Security Basics & Theory & Goals:

- How Companies Get Hacked - <https://nanetech.com/2021/07/30/5-common-ways-businesses-get-hacked/>
- Cyber Security News - <https://cyware.com/cyber-security-news-articles>
- Red Team Vs Blue Team - <https://www.emagined.com/red-team-and-blue-team>

3) Understand Hackers - The Biggest Threat:

- White Hat, Black Hat, Gray Hat - <https://www.kaspersky.com/resource-center/definitions/hacker-hat-types>
- Biggest Data Breaches - <https://www.upguard.com/blog/biggest-data-breaches>
- How Does Typical Malware Work - <https://www.avast.com/c-malware>

4) Security Bugs & Vulnerabilities - Basics:

- Latest Cyber Security Vulnerability News - <https://portswigger.net/daily-swig/vulnerabilities>
- Vulnerability & Threats & Exploits - <https://www.rapid7.com/fundamentals/vulnerabilities-exploits-threats/>

- Zero To Mastery Ethical Hacking Course Covering Vulnerabilities - <https://zerotomastery.io/courses/learn-ethical-hacking/>

- Zero To Mastery Bug Bounty Course Covering Web Vulnerabilities - <https://zerotomastery.io/courses/learn-penetration-testing/>

- Buffer Overflow Introduction - https://owasp.org/www-community/vulnerabilities/Buffer_Overflow

- Hacking The Art Of Exploitation Book - <https://www.amazon.com/Hacking-Art-Exploitation-Jon-Erickson/dp/1593271441>

- Book for Python Hacking - <https://www.amazon.com/Black-Hat-Python-2nd-Programming/dp/1718501129>

5) Social Engineering Basics:

- Preventing Social Engineering Attacks - <https://www.stickmancyber.com/cybersecurity-blog/8-ways-organisations-prevent-social-engineering-attacks>

- Email Message Header Analyzer - <https://mha.azurewebsites.net>

6) Endpoint Protection Security:

- Brave Browser - <https://brave.com>

- Kali Linux OS For Penetration Testing - <https://www.kali.org>

- Read on XProtect For Mac - <https://www.howtogeek.com/217043/xprotect-explained-how-your-macs-built-in-anti-malware-works/>

- Ubuntu Disk Encryption - <https://ubuntu.com/core/docs/uc20/full-disk-encryption>

- KeePass Password Manager - <https://keepass.info>

- Bitdefender Antivirus - <https://www.bitdefender.com>

- Process Explorer - <https://docs.microsoft.com/en-us/sysinternals/downloads/process-explorer>

- Wireshark - <https://www.wireshark.org>

- Rootkit Hunter - <https://www.kali.org/tools/rkhunter/>

- IPTables Guide - <https://man7.org/linux/man-pages/man8/iptables.8.html>

- Article On OS Hardening - <https://www.trentonsystems.com/blog/system-hardening-overview>

- Qubes OS - <https://www.qubes-os.org>

7) Network Security:

- Types of Firewalls - <https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html>

- pfsense - <https://www.pfsense.org>
- Nmap Network Scanner - <https://nmap.org>
- Nmap Manual - <https://linux.die.net/man/1/nmap>
- Designing Secure Industrial Networks Steps - <https://www.isa.org/intech-home/2017/november-december/features/three-keys-designing-configuring-secure-networks>
- Routersploit - <https://github.com/threat9/routersploit>
- Wireless Security - <https://www.cisco.com/c/en/us/products/wireless/what-is-wi-fi-security.html>
- MITRE ATT&CK - <https://attack.mitre.org>

8) Anonymity & Privacy:

- Tor Browser - <https://www.torproject.org/download/>
- VPN vs Proxy - <https://nordvpn.com/blog/vpn-vs-proxy/>
- DuckDuckGo - <https://duckduckgo.com>
- Quick Guide to Anonymity - <https://www.security.org/vpn/anonymity/>