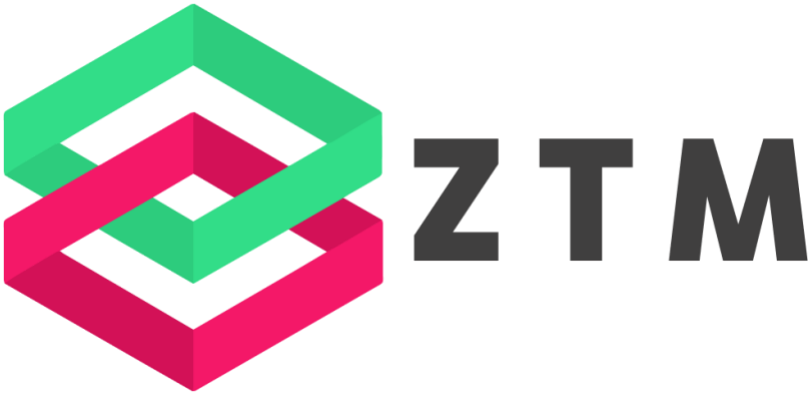

CYBERSECURITY CHEAT SHEET

ALEKSA TAMBURKOVSKI

V1.01

HEEELLLOOOOO!

I'm Andrei Neagoie, Founder and Lead Instructor of the Zero To Mastery Academy.

After working as a Senior Software Developer over the years, I now dedicate 100% of my time to teaching others valuable software development skills, help them break into the tech industry, and advance their careers.

In only a few years, **over 750,000 students** around the world have taken Zero To Mastery courses and many of them are now working at top tier companies like Apple, Google, Amazon, Tesla, IBM, Facebook, and Shopify, just to name a few.

This cheat sheet, created by our Cybersecurity & Ethical Hacking instructor (Aleksa Tamburkovski) provides you with the key Cybersecurity terms, tools, and information that you need to know and remember.

If you want to not only learn Cybersecurity but also get the exact steps to build your own projects and get hired as a Cybersecurity Engineer or Ethical Hacker, then check out our Career Paths.

Happy Learning!
Andrei

Founder & Lead Instructor, Zero To Mastery
Andrei Neagoie

Cybersecurity Cheatsheet

Terms & Definitions

Asset

Assets are anything that a cyber security strategy should protect. It can be both physical and digital assets ranging from physical computer machines to softwares and data that needs to be protected

Access Control (AC)

The selective restriction of access to Users on a certain platform, application, or software.

Authentication

Process of proving an individual is who they claim they are. Authentication can be completed by providing several factors for authentication such as: usernames, passwords, 2fa (two factor authentication) codes.

Antivirus

A software used for detecting and removing a malicious software from the machine that the antivirus is installed on. The detection methods used can vary from signature detection (which makes it important to keep antivirus software always up to date to newer methods such as AI or pattern recognition of malware which some antiviruses have.

Backup

A copy of data stored in a safe environment which can be used to restore the data in case the original one gets compromised/deleted. Usually backup is stored on a different/separate physical device. If there are not multiple backups, losing the backup data would result in ultimate data loss (considering original data was also deleted/compromised).

Bug

An error/mistake in software code which can (not necessary) lead to a vulnerability being present.

BYOD (Bring Your Own Device)

A common term usually found in a company's security policy which determines whether the employees can bring their own device to work.

Botnet

A collection of computers which have been infected by a malicious software in order to run commands given to them by the attacker from the Command and Control Centre.

Blue Team

A team of experts with a goal to defend and protect an organization from Cyber Attacks. They are constantly analyzing organizations security and implementing new measures to improve its defences.

Black Hat

A hacker who violates computer security for their own personal profit. The hacking done by a black hat hacker is in many cases with malicious intent and in all cases without permission.

Critical Infrastructure

Physical or virtual assets that are important/vital to the organization. Usually cyber security strategies will be based around these types of assets.

Cyber Attack

An attempt to compromise the protected system. Goals of Cyber Attacks depend on the attackers mindset and can range from simple information gathering to damaging the critical infrastructure and data.

Cryptography

Mathematical processes performed on data to provide the confidentiality, authentication and integrity. The goal of Cryptography is to protect the information and communication so that only those who the information is intended to can process it and read it.

CVE (Common Vulnerabilities and Exposures)

A database of publicly disclosed information security issues. A CVE number uniquely identifies one vulnerability from the list.

Data Breach

Unwanted disclosure or access to confidential information.

Data Theft

Act of intentionally stealing data. Data theft can happen through physical theft or through data leakage.

DDOS (Distributed Denial of Service)

An attack during which the access of a certain system is blocked usually due to purposely ran flooding attacks and connection resource demand.

Digital Certificate

Proving the identity through a third party entity which is set to be the certificate authority.

Digital Forensics

Digital forensics (sometimes known as digital forensic science) is a branch of forensic science encompassing the recovery, investigation, examination and analysis of material found in digital devices, often in relation to mobile devices and computer crime.

DLP

Also known as Data Loss Prevention is a collection of security strategies used to prevent the occurrence of data loss and data leakage.

Encoding

Converting cleartext into ciphertext (seemingly random form of data).

Encryption Key

Encryption Key is a random string of bits created for scrambling and unscrambling data. They are designed with intention to be unpredictable and unique.

Firewall

A tool used for security which can be both a hardware and a software tool, used for filtering traffic. A firewall is controlled by a set of rules which determine which traffic will be let through and which traffic will be blocked. There are different types of firewalls such as Host based or Network Based firewalls.

Honeypot

A purposefully vulnerable system used for trapping Black Hat Hackers. It is a false system made as a decoy for the hacker to fall for. It is used to trick the attacker into exploiting the honeypot which can alert security experts of a potential threat being present.

IDS (Intrusion Detection System)

An Intrusion Detection System (IDS) is a monitoring system that detects suspicious activities and generates alerts when they are detected.

IPS (Intrusion Prevention System)

A security tool used to constantly monitor the network for malicious activity and once discovering malicious activity, takes the action to block and prevent it.

Insider Threat

Potential that an employee or anyone that is considered to be internal personnel could pose a risk to the security of an organization.

Malware

Malicious software or Malware is code written with an intent to cause harm and violate the security of a system. There are many types of Malware: RATs, Keyloggers, Trojans, Rootkits, Backdoors, Adwares.

Packet Sniffing

Collecting/Capturing packets off of a data network communication.

Patch

An update used to repair the previously existing bug or flaw in the code/system. A patch can also be called implementing new features and capabilities.

Phishing

Phishing is considered to be a social engineering attack which tricks the target to give their confidential information such as usernames and passwords without knowing it. Phishing attacks are number one threat on the internet and in most cases they happen over email, phone number or social networks.

Penetration Testing

Security evaluation in which the pen-tester performs various checks and scans with various tools in order to discover a bug or vulnerability being present in the system. Once the pentest is done, the pen-tester submits a report to the organization revealing all the things he found during the Penetration Test.

Risk Management

IT risk management is the application of risk management methods to manage IT threats. IT risk management involves procedures, policies, and tools to identify and assess potential threats and vulnerabilities in IT infrastructure.

Red Team

A group of cybersecurity experts that perform offensive security exercises on the company to test its security. The goal of this is to act as an attacker and find out as many potential vulnerabilities which can compromise the system/assets of an organization.

Sandboxing

The act of isolating a system or an application in order to perform testing.

Social Engineering

Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. Social Engineering is used in one of the biggest threats on the internet: Phishing Attacks.

Spam

Unwanted messages usually received through email or text messages.

Two-Factor Authentication

Two-Factor Authentication (also known as 2FA) is an act of proving your identity in additional ways compared to just proving it with a password. Usually 2FA is done via additional code being sent to email or to the phone number linked to that account. 2FA can also be implemented with adding additional pins, smart cards or fingerprints.

VPN

Virtual Private Network is a communication link between systems which is encrypted in order to provide a more secure and private communication.

Vulnerability

Vulnerability Is a flaw in code or system that weakens the overall security of that system.

White Hat

A white hat hacker or ethical hacker is an individual who uses hacking skills to identify security vulnerabilities in hardware, software or networks.

Cybersecurity Reports

Reports are a necessary, and important, part of cybersecurity. Writing reports will differ depending on several factors such as the scope of your analysis, the organization structure, the important assets that need to be secured ... however there are some simple tips we can consider when writing any type of cyber security report:

1. **Key Findings**. The most important part of the report is what was actually discovered. Attention should be brought to the more severe/damaging vulnerabilities and these should be addressed first. After critical vulnerabilities are stated (if any were found) you can list less severe vulnerabilities or information disclosures that wouldn't have that hard of an impact.
2. **Proof of Concept**. Besides just listing the found vulnerabilities, it is also recommended to state how these vulnerabilities were found and to (if possible) provide a step by step guide on how anyone else could replicate/exploit these vulnerabilities or use them to their advantage.
3. **Simplicity**. It matters who the report is being written for. If you are doing a cyber security report or a penetration test report for a big company with blue team then your report can be written in technical details, however if the report is being written for an individual who is not familiar with security concept, terms and definitions, then it is important to keep it simple and to explain it to them in a way that they would understand. Usually letting them know what the dangers of discovered vulnerabilities are and pointing them in the right direction on how they can harden their security would be enough.
4. **Negative and Positive**. When writing the report it is a good idea to state both the negative and the positive findings. Prioritize the organizations weaknesses and state the findings related to security threats first but also mention their strengths.
5. **Confidentiality**. Your report is going to have sensitive information therefor it is necessary to not have it leaked, stolen or sent to the wrong person. It is also necessary that you perform a secure transfer of the report when providing it to the client. Having a cyber security report in the wrong hands could pose a security

threat to the organization. When confidentiality is of higher importance it is better to discuss the report contents in person compared to over email or phone.

6. **Scope**. In your report, you want to state the scope of the organization on which the report is focused on. Specify which systems, networks and applications were reviewed in the cyber security report.

Cybersecurity Tools

These are the key tools you should use for cybersecurity.

1. **Wireshark:** Wireshark is free and open source packet analyzer. Wireshark is the most often-used packet sniffer in the world.
2. **Tcpdump:** Tcpdump is a useful packet sniffing tool for networks. It helps in monitoring and logging TCP/IP traffic that is shared over a network. Tcpdump is preinstalled on most Linux systems and can be ran from terminal.
3. **Nessus:** Nessus is one of the best vulnerability assessment scanners out there. Nessus offers 3 different versions: Essentials, Professional and Expert.
4. **Metasploit** - Metasploit has an excellent collection of tools that are perfect for penetration testing. It is often used to meet a range of security objectives, such as discovering vulnerabilities of systems and networks, designing strategies to improve the company's Cyber Security defence.
5. **Burpsuite** - Burpsuite is used for performing security testing for web applications. It offers many functions from simple proxy functionality to different scanners, intruders to even more advance options such as spider, repeater, and decoder.
6. **Nmap** - Nmap (Network Mapper) is a free and open source tool used for network scanning and security Auditing. It offers many different options from running basic port scans to running more advance software versions and operating system scans. It can also be used as vulnerability scanner with the help of scripts.
7. **Aircrack-ng** - Aircrack-ng is a complete suite of tools to assess WiFi network security. Several things can be performed with aircrack from monitoring to attacking and cracking the password of the access point.