**The Fundamentals of Cyber Security**



Photo by [Peter Conrad](https://unsplash.com/@pconrad?utm_source=medium&utm_medium=referral) on [Unsplash](https://unsplash.com/?utm_source=medium&utm_medium=referral" \t "_blank)

Once you know the basic blocks of Cybersecurity, you have to understand the fundamentals of Cybersecurity. What's the difference? Honestly, it is a matter of perspective. I consider basics to be the building blocks while the foundational layer to be on top of these bricks/blocks. This is where your brain is supposed to be like:

*“Wow! seems interesting, but at the same time it seems easy”*

In this story, we will provide an overview of foundational topics that will build your… foundation.

**1. Security Design**

This is more than just installing Antivirus and praying everything goes well.



Photo by [Bermix Studio](https://unsplash.com/@bermixstudio?utm_source=medium&utm_medium=referral" \t "_blank) on [Unsplash](https://unsplash.com/?utm_source=medium&utm_medium=referral" \t "_blank)

Well, if your praying is strong, you will be lucky. But what if the hacker is also praying, it then depends on who prays harder.

Imagine building a castle. Do you just put a moat around it and hope dragons don’t show up? I believe no. You build walls, drawbridges, archers, secret tunnels, basically layers upon layers.

This concept is called **Defense in Depth**(Trust me when I say that this is the soul of security design)

Key Concepts related to Security Design:

* **Defense in Depth**: Layers, if one fails, another layer. Two layers will slow the attacker, three will annoy them, four will make them give up (Budget constraints are an important aspect here though of how many layers you set up)
* **Least Privilege**: Nobody needs full keys to the castle except the king (or sysadmin or admin). Especially not DarKVoicE from the marketing department.
* **Zero Trust**: Trust no one, not even your own systems. Keep this motto “Verify, Verify Again. Then verify one more time.”
* **Security By Design**: If you build it secure from day one, you won’t cry when someone hacks you (or maybe you will, but its generally a good practice to always start any implementation, be it networks, applications, etc., to consider security from the beginning)

***Quick Quiz?***

Which of these is NOT a security design principle? (Don't Scroll Up, I am monitoring you) — reply in the comment section below

a. Defense in Depth

b. Least Privilege

c. Trust everyone blindly

d. Security by Design

**2. Networking: The Internet’s nerve system (and some people’s worst nightmare)**

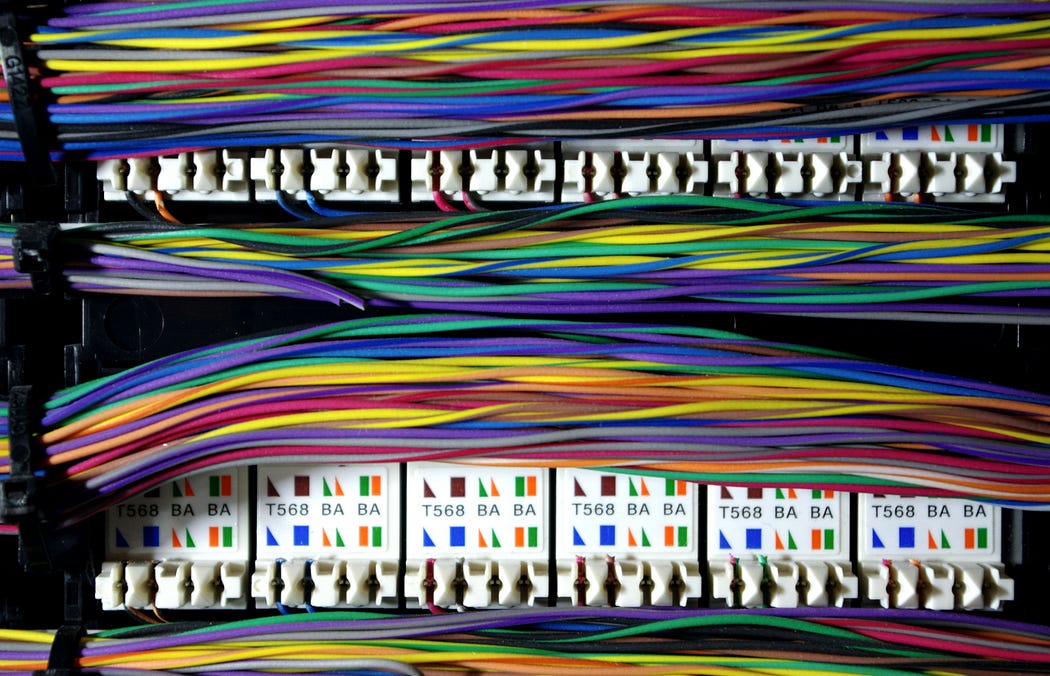


Photo by [Lee Lawson](https://unsplash.com/@lawsonlee?utm_source=medium&utm_medium=referral) on [Unsplash](https://unsplash.com/?utm_source=medium&utm_medium=referral" \t "_blank)

You think the internet is magic? Consider it as a lot of computers yelling and shouting at each other using protocols and ports.

If you don’t understand networking, you cannot grasp/map the cybersecurity concepts so easily.

But what exactly do you need to know from the networking perspective:

* **TCP/IP and OSI Models**: Layer cakes for data. If you want to be a pro, paste these models in your heart (and brain). If you don’t want to be a pro, be the best googler (but only after you understand these concepts well).
* **Ports and Protocols**: HTTP (80), HTTPS (443), SSH (22), RDP (3389), and many others of course.
* **IP addressing and Subnetting**: Fancy math to separate neighborhoods on the internet.
* **Firewall Rules**: The bouncer at your *network*’s club. *No VIP? No Entry*

Tools to play with:

* **Wireshark**: Spy on your network traffic. Watch random 1000s of packets. Feel extremely confident but confused (I would then call you confidently confused… haha..(pretty lame))
* **Nmap:**Scan your networks (just your network please) like a digital stalker. See who’s home and what doors they left open.

***Quick Quiz?***

Test Yourself: What port does HTTPS use? kindly reply in the comments section.

a. 80

b. 443

c. 22

d. 3389

**3. Operating Systems (Trust me they are not your friends; you need to initiate first)**

Your OS (Operating System) is like a city, and cities have crime. If you don’t patch the potholes, criminals will use them.



Photo by [Claudio Schwarz](https://unsplash.com/@purzlbaum?utm_source=medium&utm_medium=referral) on [Unsplash](https://unsplash.com/?utm_source=medium&utm_medium=referral" \t "_blank)

OS Security Musts:

* **Accounts & Permissions**: Don’t run as admin/root except when absolutely necessary. (Please)
* **File Systems**: NTFS, ext4, APFS — different formats which are all vulnerable to lazy admins.
* **Patching**: Updates are annoying but vital.
* **Logs**: Every action leaves a trail. Sherlock homes will be proud, I think.

***Mini-Quiz***: Name one reason why running as admin/root all the time is a bad idea.

**4. Cryptography: When Math becomes Bodyguard**

If your data was a secret diary, cryptography is the lock on it, except that it’s cooler when mathematics are involved (and that nobody understands).



Photo by [Growtika](https://unsplash.com/@growtika?utm_source=medium&utm_medium=referral" \t "_blank) on [Unsplash](https://unsplash.com/?utm_source=medium&utm_medium=referral" \t "_blank)

Essentials:

* **Symmetric vs Asymmetric**: One key or two keys? AES (symmetric) vs RSA (asymmetric) [Google the difference, it’s simple]
* **Hashing**: Like digital fingerprints — one-way and unique, unless you use MD5 (please don’t, its insecure)
* **Digital Signatures**: The online “I swear this is me; I can do my own signature” stamp.
* **SSL/TLS**: The reason your browser shows a little padlock (check just before the URL https://medium…) and you trust buying those stocks online.

***Quick Quiz?***

What does SSL/TLS primarily provide?

a. Faster internet speeds

b. Encrypted communication

c. Antivirus protection

d. Better graphics

**5. Identity and Access Management (IAM): Who’s allowed in?**

Not everyone needs a VIP pass to your systems. IAM controls the guest list.



Photo by [Brett Jordan](https://unsplash.com/@brett_jordan?utm_source=medium&utm_medium=referral) on [Unsplash](https://unsplash.com/?utm_source=medium&utm_medium=referral" \t "_blank)

The Big Concepts:

* **Authentication**: Prove you are who you say you are (passwords, 2FA, Biometrics)
* **Authorization**: What you can actually do once authenticated (RBAC, ABAC) — like what files you can access.
* **SSO (Single Sign-On)**: One login to rule them all
* **Enforce Least Privilege**: Stop giving everyone admin access

**6. Threat Modelling: Think Like the Enemy**

Want to protect your castle? Imagine how it can be taken down in the first place.

Models to know:

* **STRIDE**: Spoofing, Tampering, Repudiation, Info Disclosure, Denial of Service, Elevation of Privilege. Sounds fancy, could look intimidating for some readers, but basically, what could possibly go wrong?
* **DREAD**: Damage, Reproducibility, Exploitability, Affected Users, Discoverability. How bad is it?
* **Attack Surface**: Every Point where you could get poked by an attacker

**7. Security Operations & Incident Response**

No system is perfect. When the inevitable happens…



Photo by [Boitumelo](https://unsplash.com/@writecodenow?utm_source=medium&utm_medium=referral) on [Unsplash](https://unsplash.com/?utm_source=medium&utm_medium=referral" \t "_blank)

* **SIEM**: Security Information and Event Management. Think of it as your 3 AM alarm screaming “Something is wrong”. SIEM’s typically collect logs from sources (servers, applications, etc.) and trigger if something goes wrong.
* **SOC**: The cyber first responders.
* **Incident Response Plans**: Know what to do before you Google “how to recover from ransomware”
* **Forensics**: Digital detective work after the mess/attack/incident

**8. Compliance & Governance: Because you have to**

Yes, you have to follow rules or get fined.



Photo by [Scott Graham](https://unsplash.com/@amstram?utm_source=medium&utm_medium=referral) on [Unsplash](https://unsplash.com/?utm_source=medium&utm_medium=referral" \t "_blank)

* **Frameworks**: NIST, ISO 27001, CIS Controls, the lengthy and boring but necessary guides.
* **Regulations**: GDPR, HIPAA, PCI-DSS, laws that will hunt and haunt you.
* **Policies**: Password rules, BYOD (Bring Your Own Device), Acceptable Use, basically your company’s way of saying “Do it or else”

Fundamentals aren’t flashy. No explosions or memes. But without them, you’re just fumbling in the dark with a butter knife.

*Tools change, hackers evolve, but fundamentals? They’re your survival manual in the chaos.*

***Bonus Brain Teasers:***

1. List two reasons why zero trust is better than “trust but verify”
2. Identify one potential risk of poor patch management
3. Describe how role-based access control improves security

**Enjoyed the read?**  
Smash the follow button, drop a comment, and share this with someone who still thinks “password” is a good password.