**Cyber Security Full Course – Edureka (Notes)**

**Cyber Threats**

* **Malware** – malicious software (viruses, worms, trojans, ransomware, etc.)
* **Phishing** – fraudulent emails/websites to steal credentials
* **Password Attacks** – brute force, dictionary attacks, credential stuffing
* **DDoS (Distributed Denial of Service)** – overwhelming a system with traffic
* **Man-in-the-Middle (MitM)** – intercepting and altering communications
* **Drive-by Downloads** – unintentional download of malicious code
* **Malvertising** – malicious ads that deliver malware
* **Rogue Software** – fake security software or tools

**Information is Beautiful**

Website that visualizes the history of the world’s biggest **data breaches**.

**CIA Triad – Core Cyber Security Goals**

Cyber security aims to protect against unauthorized:

1. **Modifications**
2. **Deletion**
3. **Access**

Known as the **CIA Triad**:

* **C**onfidentiality
* **I**ntegrity
* **A**vailability

**Key Concept: Vulnerability → Threat → Risk**

* **Vulnerability:** Weakness in a system.
* **Threat:** Potential exploit of a vulnerability.
* **Risk:** Impact when a threat successfully exploits a vulnerability.

**Early Days of Hacking**

The meaning of *hacker* has evolved over the last 50 years.

**Types of Hackers**

* **White Hat:** Ethical hackers; test systems legally.
* **Black Hat:** Malicious hackers for illegal gain.
* **Grey Hat:** In-between; may perform unauthorized activity, sometimes report vulnerabilities.

**Skills Necessary to Become a Hacker**

* **Computing Skills:** OS, programming, databases.
* **Networking Skills:** TCP/IP, protocols, firewalls.
* **Life Skills:** Problem-solving, persistence, communication.

**Types of Attacks**

* **Defacing:** Attack on a website to alter its visual appearance.
* **Buffer Overflow:** Occurs when a program writes data beyond buffer memory limits, potentially allowing code execution.
* **Denial of Service (DoS/DDoS):** Overwhelms a service/system;  
  Example: *Tribe Flood Network (TFN)* – an early DDoS tool.

**Penetration Testing**

Simulated attack to test security of a system/network. Goals:

* Assess weaknesses
* Understand risks
* Attempt exploitation to identify vulnerabilities  
  Then generate a **report** and suggest **fixes**.

**Footprinting**

Process of gathering information about a computer system/network.  
Tools and examples:

* **Wayback Machine:** History of websites
* **Netcraft:** Internet security services & website info
* **ARIN:** Regional Internet Registry (IP info)

**DNS – Domain Name System**

Converts domain names into IP addresses; makes URLs easier to remember.