CYBER SECURITY CEH COURSE

What is cyber Security?

Security Matters related to online communication are called Cyber Security.

What are Security Matters?

- Fixing Security
- Breaking Security
- Checking Security

What are the General Terminologies in Cyber Security?

1. **Exploit:** An action that causes unexpected behavior which an attacker can use to perform harmful activities.
2. **Vulnerability:** A security weakness that can be exploited. It is the main risk, while minor risks can be ignored depending on their impact.
3. **Asset:** Anything that needs protection from exploitation.
4. **Risk:** The damage caused by exploiting a vulnerability.
5. **Threat:** A constant Danger to an asset. It can be a person, object or an event.
6. **Bug:** An error, fault or flaw in a computer program that may cause unexpected behavior.
7. **Bug Bounty:** Finding bugs in the code. People who excel in this field usually have a programming background.
8. **InfoSec:** Short for Information security.
9. **Penetration Testing:** The professional name for hacking. It means testing and reporting security loopholes.
10. **Vulnerability Testing:** Finding Security loopholes.
11. **Zero Day Vulnerability:** A vulnerability unknown to professionals and only exploited by hackers. If reported but no fix is released it is called a zero day attack.
    - If a patch is released but the user has not installed it, it is **not** considered a Zero-Day

What are the two main building blocks?

Vulnerability and Exploit are the two main building blocks.
If a Vulnerability is found it shows how it can be exploited.

Key Concept:

Only a Dead Machine is a Secured Machine. Everything made by man can never be 100% perfect.

Three major classifications of Cyber Security

1. **Ethical Hacking / Penetration Testing:**
   - ➢ Authorized hacking to identify and fix security loopholes.
2. **Hacking Investigation / Forensics:**
   - ➢ Investigation of Cyber Crimes and recovery of digital evidence
3. **Defense / Counter Measure:**
   - ➢ Protecting systems by preventing, detecting and responding to attacks.

What is Hacking?

Unauthorized access of any digital systems is called hacking.

What is the difference between Ethical and Unethical Hacker?

Ethical Hacker	**Unethical Hacker**
A hacker whose skills do not cause harm to IT assets is called an Ethical Hacker.	A hacker whose skills cause harm to IT assets is called an Unethical Hacker.

- Cyber laws exist to keep hackers within ethical boundaries.

Types of Hackers

1. **Black Hat:** Malicious hackers who break into systems illegally for profit or harm.
2. **White Hat:** Ethical hackers who legally test systems to improve security.
3. **Gray Hat:** Hackers who sometimes break the law but without malicious intent, often to expose flaws.
4. **Suicide Hacker:** A hacker who risks their career or freedom by hacking, knowing they will be caught.

5. **Cyber Terrorist:** Hackers who create fear and disruption online, targeting people or governments.
6. **State Sponsored Hackers:** Hackers employed by governments to steal secrets or attack other nations.
7. **Hacktivist:** Hackers who target government or corporate systems as a form of protest.
8. **Script Kiddies:** Unskilled hackers who use pre-made tools or scripts developed by real hackers.
9. **Hacker Team:** A group of hackers working together on attacks or projects.
10. **Insiders:** People within an organization who misuse their access to cause harm.
11. **Industrial Spies:** Hackers who steal trade secrets and business information for competitive advantage.

From My Weakest link to My Strongest Asset

Technical Skills:

1. **High Technical Knowledge of how to perform/launch sophisticated attacks.**

   Reason: I am still building my foundation (terminologies basics of DoS/DDoS, SQL injection etc) sophisticated attacks require solid networking + OS + scripting, and that's where I'm not confident.

2. **Don't Learn anything but you must know everything.**

   Reason: This Jack of all trades hacker instinct being able to pull from broad knowledge instantly isn't my strong suit yet. I sometimes jump between topics (OOP → web dev → Oracle → Hacking) without locking them down. This shows that I haven't developed the know everything instinct.

3. **In Depth Knowledge of networking concepts, technologies, and related hardware.**

Reason: I have touched networking concepts (IP, routing, protocols), but haven't dived deep. For Penetration testing this is crucial. I would say that I am aware but not comfortable.

4. **In depth Knowledge of major operating systems (Windows, Unix, Linux, Macintosh)**

   Reason: I recently installed Kali Linux in VMware and tinkered with Bios Settings. That shows I am getting exposure to Linux/Windows internals, but still in learning mode. Not completely weak, but not mastery either.

5. **The Knowledge of security areas and related issues.**

   Reason: I have been studying ethical vs unethical hacking, types of attacks, FUD, RAT, phishing, etc. This theoretical side is improving.

6. **A computer expert adept at technical domains.**

   Reason: I have been coding (Laravel, Javascript, OOP, DSA). That shows that I have already have a strong computer science base.

Non-Technical Skills:

1. **Awareness of local standards and laws.**

   Reason: I have never really searched up Pakistan's Cyber Crime laws or organizational compliance standards. So I think this is my weakest non-technical area.

2. **Commitment to Organization security Policies.**

   Reason: I have just started the course of penetration testing but not working in an org yet, I haven't had to practice aligning with real company policies.

3. **A strong work ethic and good communication skills**

   Reason: I am motivated but I admit I am struggling with consistency. Work ethic is improving but not fully stable I'd like to think that I have good communication skills.

4. **Ability to learn quickly and adapt new technologies**

   Reason: I pick up new tools/systems fast.

5. **Hackers Mindset.**

   Reason: I think once I start to understand some thing or I think about it I start getting curious on how to do things and I like experimenting with things as well

Difference between Hacker and Hacking

Hacking	**Hacker**
Hacking is a Process Done by the Hacker	Hacker is the person performing the process of Hacking
Hacking is an activity of exploiting Vulnerabilities	Hacker is an individual with the knowledge and skills to carry out that activity.

Types of Hacking:

1. **Black Box Testing:** Nothing is provided to the hacker the hacker is kept in dark.
   - External hackers are usually hired for Black Box Testing because they have no prior knowledge of the company's Infrastructure.
2. **White Box Testing:** Testers are given comprehensive details about everything.
   - Internal Hackers teams or developers usually perform white box testing because they already know the company's infrastructure.
3. **Gray Box Testing:** Testers are given some information.
   - Grey Box Testing balances realism and efficiency, It stimulates an attacker with partial insider Knowledge.

Choosing the Right Testing Approach

- A company cannot do Black Box Testing with its own internal team, because they already know the infrastructure.
- External Hackers cannot do White Box Testing because they lack internal knowledge.

- Therefore Black Box Testing Should be done by external hackers while White Box Testing can be done by internal hacker teams.

User of Hacker Skills in Different Fields

1. **ISP (Internet Service Providers):** Hackers help secure network infrastructure, prevent DDoS attacks, and maintain uptime.
2. **Banks:** Hackers protect online banking systems, ATMs, and payment gateways against fraud.
3. **Medical Field:** Hackers secure patient records, hospital management systems, and medical devices connected to networks.
4. **E-Commerce:** Securing websites, payment gateways, and user data.
5. **Government:** Protecting sensitive data, defense networks, and intelligence.
6. **Telecommunication:** Safeguarding mobile networks and preventing call/data interception.
7. **Corporate Sector:** Securing internal servers, trade secrets, and cloud systems.

PCI DSS

PCI DSS stands for *Payment Card Industry, Data Security Standard*. Many companies claim DSS compliance, but to be valid it should clearly mention whether it is **Certified** or **Compliant**.

- **Example:** On Daraz.pk, if you zoom in the footer, you will see PCI DSS with the word "Compliant."

Security Department Architecture

1. **Information Security Department**

   Information Security (IS) is one of the most important fields in security, similar to how IT is important in technology. Every type of concern related to protecting information, systems, and data falls under IS. The Information Security Department is responsible for designing, implementing, and maintaining organization-wide security policies, guidelines, standards, and procedures.

   - **Policies** are the overall rules and principles.
   - **Standards** are the best practices chosen from those policies.

- **Guidelines** help organizations achieve those standards.
- **Procedures** are the exact steps to follow for implementing policies and guidelines.

Major Fields of Information Security

1. Communication and Network Security
2. Asset Security
3. Software Development Security
4. Identity and Access Management
5. Cryptography
6. Security Architecture & Engineering
7. Security and Risk Management
8. Information System Auditing Process
9. Governance and Security Policy of IT
10. Cyber Security

1. Communication and Network Security:-

This field ensures the protection of data during transmission across networks. It covers secure communication channels, firewalls, intrusion detection systems, and VPNs.

- **Example:**
  When an application (e.g., WhatsApp) displays “end-to-end encryption,” it indicates that messages are encrypted such that only the sender and intended recipient can decrypt and read them; intermediaries (including the service provider) cannot intercept or decipher the content

2. Asset Security:-

This field deals with protecting an organization’s physical and digital assets such as servers, databases, devices, and sensitive information. It focuses on classification, handling, storage, and disposal of assets securely.

- **Example:**
  If a company has a hard drive that contains sensitive data and the drive gets old, destroying it or securely wiping it is part of asset security.

3. Software Development Security:-

This field ensures that security is integrated into every phase of the software development lifecycle (SDLC). It focuses on secure coding practices, code reviews, vulnerability testing, and preventing threats such as SQL injection or cross-site scripting. A domain within this is Bug Bounty, where developers and ethical hackers find and report vulnerabilities in applications.

4. **Identity and Access Management (IAM):-**
   IAM ensures that the right individuals have the right access to the right resources at the right time. It involves authentication (verifying identity) and authorization (granting role-based privileges).
   - ➢ **Example:**
     In a NADRA office, a receptionist may only have access to limited citizen data, while a senior officer can access the complete database.
5. **Cryptography:-**
   Cryptography is one of the oldest fields in Information Security. It is the science of converting plain text into cipher text (encryption) and then back into plain text (decryption). It ensures confidentiality, integrity, and authentication of data.
6. **Security Architecture and Engineering:-**
   This field focuses on designing and implementing frameworks to ensure security. An Information Security Architect must have knowledge of all domains and experience across multiple fields.
   - ➢ **Top Hierarchy:**
     i. **Architect:** Manages the overall security structure.
     ii. **Consultant:** Provides advice and recommendations
     iii. **Engineer:** Implements solutions such as firewalls, intrusion detection, and encryption.

7. **Security and Risk Management:-**
   This is one of the most important aspects of Information Security. *Risk* means the possibility of loss or damage. Risk management involves evaluating assets and threats, applying risk treatment, and reducing risks. Any risk left after treatment is called Residual Risk.
   - ➢ **Asset Evaluation:-**
     This is the process of identifying and valuing the assets of an organization, such as data, servers, applications, employees, or reputation. The value is based on how critical the asset is to the

organization’s operations. For example, a bank’s customer database is a highly valuable asset.

- **Threat Evaluation:-**
  This is the process of identifying possible sources of harm to assets. Threats can be internal (like a careless employee) or external (like a hacker, malware, or natural disaster). Evaluating threats helps organizations prepare defenses and prioritize security measures.

8. Information System Auditing Process:-

Auditing means reviewing and evaluating IT systems to ensure they follow established standards and policies. If companies follow standards and regularly perform audits, they can label themselves as Certified or Compliant. Auditing is not limited to Cyber Security or Information Security—it can cover financial, operational, and compliance areas as well.

ISO 27001

- ISO 27001 is an international standard consisting of best practices for Information Security Management Systems (ISMS). It has two main certification tracks:

- **Implementer –** Professionals who set up and implement ISO 27001 in organizations.
- **Auditor** – Professionals who evaluate whether organizations comply with ISO 27001.
- In Pakistan, government bodies may have local auditors, but for international recognition, certification is often validated by global institutions like the IMF or other international accreditation bodies.

ISO 27001 Experience Levels

- **Foundation Level** – Implementer or Auditor with less than 3 years of experience.
- **Implementer/Auditor** – With 3 to 5 years of experience.
- **Lead Implementer/Auditor** – With 5 to 12 years of experience.
- **Senior Lead Implementer/Auditor** – With more than 12 years of experience

ISO 27002

- ISO 27002 provides best practices and guidelines specifically for managers working within Information Security Management Systems (ISMS).

9. Governance and Security Policies of IT:-

Governance and Security Policies define who creates policies, how they are implemented, and how compliance is monitored. The quality of policies depends heavily on the knowledge and expertise of the policymakers. If unqualified people are in charge, the policies will be ineffective and harmful for the organization.

- **Examples:**
  - i. If the head of an IT department does not have proper IT knowledge, then the policies they create will not be effective.
  - ii. It's similar to giving the responsibility of preparing a household budget to someone who has no knowledge of accounts or money management — they won't be able to calculate an accurate budget.

Classification: Practical vs Documentation Fields

Documentation Fields	**Practical Fields**
1. Governance and Security Policies of IT	1. Communication and Network Security
2. Security and Risk Management	2. Software Development Security
3. Information System Auditing Process	3. Identity and Access Management
4. Security Architecture and Engineering	4. Cryptography
5. Asset Security (Somewhat)	5. Cyber Security

Notes on Departments

- Not every company with an IS department works on all 10 domains.
- If a company only works on one domain, the department is named after that domain instead of "IS Department."
- If a company focuses on documentation domains, that department is often referred to as GRC (Governance, Risk, and Compliance).

10. Responsibility of Cyber Security Department:-

Ensure Protection of networks, systems and software from Cyber Attacks.

- **Core Functions (Hacking, Defense, Forensics):-**
  1. **Hacking (Ethical Hackers / Pen Testers)**
     - Find vulnerabilities and weaknesses.
  2. **Defense**
     - Build firewalls, IDS/IPS, security policies, and monitoring systems.
  3. **Forensics**
     - Investigate incidents after an attack.
     - Collect evidence and analyze what went wrong.

- **Real-World Practice: Cyber Drills:-**
  1. When hackers repeatedly find vulnerabilities and patch them (3–4 times), their workload decreases → their skills can start to deteriorate.
  2. That's why organizations conduct **Cyber Drills** (practice wars where teams compete against each other).
- **Cyber Security Teams (Color Teams):-**
  1. **Red Team (Attackers):-**
     - Ethical Hackers who try to break systems.
  2. **Blue Team (Defenders):-**
     - Security Staff Defending against Attacks.

iii. **Purple Team:-**
   - Work as a bridge between Red & Blue → knowledge sharing.

iv. **White Team:-**
   - Like a cricket umpire → Oversee drills, ensure fairness & no cheating.

v. **Yellow Team:-**
   - Builders of testing environments (mostly software developers & network professionals).

vi. **Orange Team:-**
   - Builders with attacker's perspective (Red-based builders).

vii. **Green Team:-**
   - Builders with defender's perspective (Blue-based builders).

- ❖ Finding new vulnerabilities is the primary job of Ethical Hackers / Penetration Testers.
- ❖ Cyber Security Department Focuses only on preventing **cyberattacks** (not responsible for physical asset damage).

Cyber Security Department

1. Focuses only on preventing **cyberattacks** (not responsible for physical asset damage).
2. Covers the protection of **network, systems, and software**.
3. Traditionally, does not provide **continuous monitoring**.

Security Operations Center (SOC)

- **Centralized unit** responsible for continuously monitoring and analyzing activities across an organization's information systems, including:
  - Networks
  - Servers
  - Endpoints
  - Databases

  - Applications
  - Websites
- **Differences from Cyber Security Department:**
  - SOC provides **24x7 monitoring**.
  - Attacks are detected **immediately** through SOC.
  - SOC is considered both a **department** and a **tool**.
- **Key Concepts in SOC:**
  - **Activity** and **Event** are the two primary elements being tracked.
  - Requires a dedicated **staff** for effective operation.
- **SOC Roles:**
  - **SOC Analyst Level 1** → Entry-level/junior role.
- **Tools:**
  - **Splunk** (widely used for SOC).

Life-cycle / Phases of Hacking:-

1. Foot-printing & Reconnaissance

- The information-gathering stage. The attacker tries to build a profile of the target: what systems exist, public IP ranges, domain names, employees, technologies in use, online footprints, etc. This can be done *passively* (just observing public info so the target doesn't notice) or *actively* (probing and interacting with the target, which is noisier). Reconnaissance sets the direction for everything that follows.

2. Scanning

- A more focused discovery step after reconnaissance. Scanning narrows down the list of potentially vulnerable hosts, services, open ports and software versions. Think of it as moving from a satellite map (reconnaissance) to walking the streets (scanning) to see specific doors and windows. Scanning can reveal entry points an attacker might try next.

3. Gaining Access

- This is when an attacker exploits a weakness (misconfiguration, unpatched software, weak credentials, social engineering, etc.) and achieves code execution, an authenticated session, or some level of control. In your phrase: the "successful attacks" phase — the hard goal attackers want to reach.

4. Maintain Access

- After initial compromise, the attacker tries to make their access persistent so they can return later without repeating the whole attack. This can be through backdoors, scheduled tasks, alternative accounts, or covert channels. From a defender's view the goal is to detect and remove these persistence mechanisms quickly.

5. Clearing Tracks

- The attacker attempts to hide what they did: delete or tamper with logs, alter timestamps, use anti-forensic techniques. Important reality: **you can't perfectly erase all traces.** Forensics, network logs, endpoint artifacts and external telemetry often retain evidence even when local logs are tampered with.

- ❖ Foot-printing, reconnaissance and scanning are all part of **information gathering**, with reconnaissance/foot-printing often being higher-level and scanning being more targeted. Reconnaissance = *who/what/where*; scanning = *how/which services/ports*.
- ❖ "Gaining access" = achieving a successful compromise.
- ❖ "Spoofing" is an impersonation technique (for example, falsifying an address or identity) used at different stages — often to evade detection or to trick systems/people.