The Ethical Hacking methodology

Firstly we will look into what is Red team and Blue Team.

- **Red Team** - The red team simulates real-world cyber attacks by ethically hacking systems and networks to identify vulnerabilities. They use tactics like penetration testing, phishing, and social engineering to bypass security controls and gain unauthorized access.

So, in short red teamers are the people who use offensive techniques like us to gain access to the system.

- **Blue Team** - The blue team is responsible for defending against cyber threats. They implement security measures, monitor systems, respond to incidents, and mitigate attacks. Their tasks include deploying firewalls, IDS/IPS, endpoint protection, and conducting security awareness training.

So, in laymen terms. Blue Team guys defend the organization assets and infrastructure while we try to attack it.

Then comes the Purple Team.

- **Purple Team** - The purple team facilitates collaboration between the red and blue teams. They analyze data from both teams, provide recommendations to improve security operations, and document best practices. Their goal is to enhance an organization's overall cybersecurity posture.

Types of Testing

There are primarily two types of testing - White box testing and Black Box Testing.

- **White Box Testing** - White box testing examines the internal structure, design, and implementation of software by analyzing code, data flows, and logic. It requires knowledge of programming languages and is typically performed by developers during unit and integration testing.
- **Black Box Testing** - Black box testing evaluates software functionality without knowledge of internal implementation details. It involves testing from the user's perspective by providing inputs and verifying expected outputs based on requirements. It is commonly used for higher-level testing like system and acceptance testing

Think of white box testing from a point of view of a developer where you have all access to the internal application source code. you are expected to find bugs in the code implementation itself.

While, the Black Box Testing emulates the testing approach from an external attacker point of view where you have no internal knowledge about the system.

Ethical Hacking Methodology

Now coming to the Ethical Hacking Methodology

The ethical hacking methodology refers to the structured approach and steps followed by ethical hackers to identify and test for vulnerabilities in an organization's computer systems and networks. In simple terms, it's the process ethical hackers use to legally and systematically attempt to hack into a system, just like a real attacker would, but with permission and good intentions.

So, before going further with the steps. I have stated here two things - permissions and intentions. Out of these two, permission is very very important. I mean, even if your intentions are good, you can still go to jail for hacking. So, that's why the permissions makes the absolute necessity here.

There is a thing called scope in penetration tests. Well, a scope is defined by the company you are trying to hack. If there are 10 computers in organization and you are only allowed to perform a penetration test on 5 of them. Then, you cannot go for the 6th one, even if your intentions are good. So, just remember to perform testing only on the assets which falls under the scope. Outside that, its a grey zone.

Now moving back to the methodology.

The Ethical Hacking Methodology consists of five distinct phases, each designed to methodically identify and exploit vulnerabilities while adhering to strict rules of engagement and legal guidelines.

There are 5 stages of ethical hacking. These are:

- **Reconnaissance** - This is the information gathering phase where the ethical hacker collects as much data as possible about the target system/network. This could include things like IP addresses, software/hardware details, employee information etc. It's like casing a house before attempting to break in.
- **Scanning** - Here the ethical hacker uses special tools and techniques to scan and map out the target's systems, applications, networks etc. to identify potential weaknesses or entry points. It's akin to checking all the doors and windows for potential vulnerabilities.
- **Gaining Access** - This is where the ethical hacker attempts to exploit the vulnerabilities found during scanning to actually gain unauthorized access into the target's systems, just like a real attacker would. Common methods include exploiting software bugs, social engineering tactics like phishing emails etc.
- **Maintaining Access** - Once inside, the ethical hacker tries to maintain that access and move laterally through the network, evading detection. This mimics how an attacker would try to persist and expand control.
- **Covering Tracks** - Finally, the ethical hacker aims to clear any logs or evidence that could reveal their activities, just as a real attacker would try to cover their tracks.

The key difference is that ethical hackers have permission, follow rules of engagement, and their sole purpose is to identify vulnerabilities so that they can be fixed - not to actually cause any damage or steal data. It's a legal way for organizations to proactively find and patch security holes before real attackers can exploit them.
