Penentration Testing:

- Ethical hacking needs consent of the party being hacked
- A penetration tester has authorisation from the “victim”, has good intent, does not misuse discovered vulnerabilites, and reports vulnerabilities to the client so they can be fixed.

Responsibilities of Ethical hackers:

- Conducting vulnerability assessment, identifying vulnerabilities, creating scripts and using those scripts to test the vulnerabilities and the organisations defence.
- Develop tools to help increase security
- Performing risk assessment for each enumerated vulnerability. This includes the assessing the possible risks in terms of potential loss of data, loss of reputation among customers and competition, losses incured in the form of penalties from law enforcment and security compliance authorities and the direct financial losses.
- Setup security policies to make it difficult for malicious actors to gain access to data or devices within the organisation.
- Train other staff for network security and brief them on how to keep themselves secure online. Administrative policies can be used to govern the actions of the employess. Such policies may include password policies etc.

Penetration Testing:

- Before starting the penetration test, an ethical hacker will conduct a vulnerability assessment which involves running a scanning tool to identify potential flaws or vulnerabilities in the organisations network. They will then proceed to the penetration test.
- Penetration testing is the part of ethical hacking that focuses on penetrating the information system using various attacks/exploits.
- A linux distribution, kali linux is used for pen testing. Kali linux comes with 600+ tools pre-installed and has advanced pen testing and security auditing features. It also includes tools for forensics and reverse engineering.

Phases of a Penetration Test:

- **Reconnaissance/ Information gathering phase**: The first and most important phase for a hacker or an ethical hacker. In this phase the tester will try to gather as much information as possible about their victim. This information allows them to decide what toolsets to use and how to attack the target. Information gathered during this phase may include ip addresses and network ip ranges in use by the organisation, domains and subdomains owned by the organistaion, network architectures and operating systems deployed, employees’ information for scoial engineering attacks, emails, phone numbers etc. During this stage, the tester will not ask if the information is useful. Anything and everything that can help validate and give information about target is obtained. This information later becomes the baseline for fine tuning attacks.

- **Scanning phase**: This phase makes use of the information obtained during the recon phase. The tester will identify live machines, scan for open ports, protocols and procedures, any processes that are running and identify any vulnerabilities within these processes and services. A live machine is needed because if a machine is not on the network, a remote attack will not be possible and a physical attack is needed. A tester will scan open ports(which are entry points for an intruder or a tester), probe the services running on those ports, identify service versions and conduct a vulnerability scan to identify any vulnerabilities in those services. Based on this information, they will develop/ craft their attack.
- **Gaining access phase**: The tester will attack the systems and try to gain access to victims' machines. The attack could be a social engineering campaign or a relevant exploit for an identified vulnerability or a password attack or a trojan which exploits flaws in the security setup and executes to check if access can be gained that way. All attacks carried out in this phase are temporary.
- **Maintaining access**: In this phase the tester has to ensure that there is a way back into the compromised systems/ machines. This might invlove installing a rootkit, a keylogger, traffic sniffers etc. to gain backdoor access to a machine.
- **Covering tracks**: All activities on a victims machine leave tracks/traces. For example a trojan will create files and directories, a virus will be destructive, a cracked password login creates a login entry in the log with a timestamp and the ip address which was used to log in, a script will leave logs etc. The goal of this phase(and the entire operation) is to avoid detection by deleting any traces of activity from the targets machine. This can include identifying where logs are stored and modifying or deleting them as necessary.

Types of Penetration Tests:

- **Black box test**: No information is given to the tester about the IT infrastructure of the organisation. The tester starts with phase 1. Such a pen test, tests the knowledge of the tester as well as the security implementations of the organisation to see if they can identify and detect the attack. This test provides a simulation of an actual attack by a malicious outside actor.
- **Grey box test**: The tester has some knowledge of the IT infrastructure of the organisation, like a regular emplyee in the organisation. The tester wont have administrator level knowledge but rather limited knowledge about the system and network. This test provides a simulation of an insider attack where a regular user tries to misuse their access, to try to gain confidential information or get access to unauthorised devices.
- **White box test**: The tester has full knowledge of the IT infrastructure of the organisation. This test provides a simulation of an insider attack by a user with complete knowledge of the infrastructure. This could be someone in an administrative position.

Areas of Penetration Testing:

- **Network services**: A tester finds vulnerabilities and weaknesses in the network infrastructure and checks if firewalls, switches, routers and other end network devices and interfaces are sufficiently configured to prevent attacks. Misconfiguration leaves

the devices and interfaces open to vulnerabilities which could be exploited to gain access to the network and devices.

- **Web app**: A web app is software deployed on a web server made available over an intranet or the internet. Vulnerabilities could be used to bypass authentication, gain access to the database of the web app and steal or leak info.
- **Client side apps**: While a web app is on the server, it's client-side users use a browser to interact with the web app. Browsers and operating systems have their own vulnerabilities. Identifying vulnerabilities on the client side, exploiting them and hacking the client or piggybacking on the clients connection are methods to gain access to the server.
- **Wireless networks**: A tester examines all the wireless devices used in an organisations offices. Since most wireless networks have phones, tablets, laptops and other devices connected, any device that has been compromised can be used to attack other devices on network.
- **Social engineering**: This involves tricking employees into revealing sensitive information knowingly or unknowingly via fake emails, websites etc. Social engineering attacks are successful because of the gulibility of humans. Human emotions can be toyed with and taken advantage of if caution is not excercised. An example of a social engineering attack is the infamous nigerian prince scam. The excitement of getting rich quick has leds hundreds of thousands of people to fall for such scams

Tools:

- Metasploit: A tool which has hundreds of built-in exploits which can be used to test for known vulnerabilities.
- Nmap: It scans for live devices, open ports, protocols and services.
- Beef: An application testing tool to find exploits within applications.
- Nessus vulnerability scanner: Network and host based scanner to identify vulnerabilities in the hosts.
- Wireshark: A network traffic sniffer. Allows capture and analysis network traffic/packets.
- Sqlmap: An automated tool used for sql injection attacks. A user only needs to identify what data can be gathered/manipulated through sql queries then predefine search parameters to get access to the database.
- John the ripper: A password cracking tool which can perform dictionary attacks(using lists to check if any items match a password) and brute force attacks(same as dictionary attacks but with every permutation and combination of the alphabet, numbers and chatacters to check if a password is crackable).

Many, many other tools exist. Some offer functionality similar to the ones above and others provide entirely different functionality.

Metasploit:

A framework of penetration testing that makes hacking simple. Tester identifies the vulnerability associated with an exploit and runs the exploit using metasploit.

- **Active exploit**: An active exploit, exploits a specific computer, runs until execution then exits. It uses brute force and exits when an error occurs.

- **Passive exploits**: Waits for incoming requests and exploits them as soon as they connect. Can be used in conjunction with malicious emails and web sites. Deploys a reverse connection payload on the victims machine. The machine initiates a connection back to the attacker which allows them to listen to traffic and exploit vulnerabilities.