Assignment 1 question answer:

Types of Penetration Tests

- Network Penetration Test
- Web Application Penetration Test
- Client Side Penetration Testing
- Social Engineering Penetration Test
- Physical Penetration Test

Network Penetration Test: The main purpose is to identify the most exposed vulnerabilities and security weaknesses in the network infrastructure (servers, firewalls, switches, routers, printers, workstations, and more) of an organization before they can be exploited.

Network penetration tests should be performed to protect your business from common network-based attacks including:

- Database Attacks
- Man In The Middle (MITM) Attacks
- FTP/SMTP Based Attacks

Web Application Penetration Test:Web application penetration testing is used to discover vulnerabilities or security weaknesses in web-based applications. It uses different penetration techniques and attacks with aims to break into the web application itself.The typical scope for a web application penetration test includes web based applications, browsers, and their components such as ActiveX, Plugins, Silverlight, Scriptlets, and Applets.

- These types of tests are far more detailed and targeted and therefore are considered to be a more complex test. In order to complete a successful test, the endpoints of every web-based application that interacts with the user on a regular basis must be identified.

- This requires a fair amount of effort and time from planning to executing the test, and finally compiling a useful report.

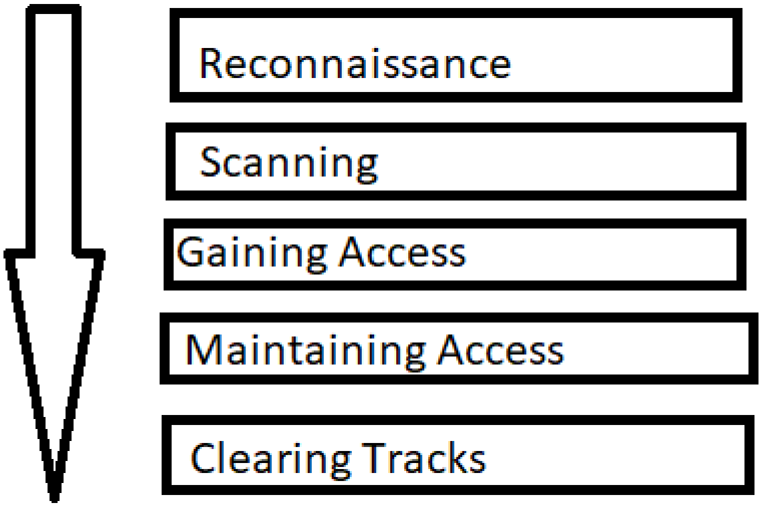
- The techniques of web application penetration testing are continuously evolving with time due to the increase in threats coming from web applications day by day.

Client Side Penetration Testing:

Client side penetration testing is used to discover vulnerabilities or security weaknesses in client side applications.These could be a program or applications such as Putty, email clients, web browsers (i.e. Chrome, Firefox, Safari, etc.), Macromedia Flash, and others. Programs like Adobe Photoshop and the Microsoft Office Suite are also subject to testing.

Social engineering penetration testing This type of penetration testing assesses how susceptible your staff is to exposing confidential information. Social engineering involves an attempt to gain the trust of an employee, usually by tricking them into sharing private data or performing an action that exposes data to a masked malicious actor. Phishing emails are a prime example of a social engineering ploy. A hacker may pose as a manager (using a very similar email address), and ask an employee to share a login or transfer money under urgency. White hat penetration testers may try to exploit your staff into sharing protected information to reveal the need for more in-depth employee security training and management

2 What are the phases in the penetration testing lifecycle?



Reconnaissance:

This is the first step of Hacking. It is also called as Foot printing and information gathering Phase. This is the preparatory phase where we collect as much information as possible about the target. We usually collect information about three groups,Network,Host, People involved.There are two types of Footprinting:

Active: Directly interacting with the target to gather information about the target. Eg Using Nmap tool to scan the target.

Passive: Trying to collect the information about the target without directly accessing the target. This involves collecting information from social media, public websites etc.

2. Scanning:

Three types of scanning are involved:

Port scanning: This phase involves scanning the target for the information like open ports, Live systems, various services running on the host.

Vulnerability Scanning: Checking the target for weaknesses or vulnerabilities which can be exploited. Usually done with help of automated tools.

Network Mapping: Finding the topology of network, routers, firewalls servers if any, and host information and drawing a network diagram with the available information. This map may serve as a valuable piece of information throughout the haking process.

3**. Gaining Access:**

This phase is where an attacker breaks into the system/network using various tools or methods. After entering into a system, he has to increase his privilege to administrator level so he can install an application he needs or modify data or hide data.

4. Maintaining Access:

Hacker may just hack the system to show it was vulnerable or he can be so mischievous that he wants to maintain or persist the connection in the background without the knowledge of the user. This can be done using Trojans, Rootkits or other malicious files. The aim is to maintain the access to the target until he finishes the tasks he planned to accomplish in that target.

5. Analysis and Reporting

This is the result of a penetration test. As part of the last stage, the security team prepares a detailed report describing the entire penetration testing process. Some information or detail that should appear are:

- The seriousness of the risks emanating from the vulnerabilities discovered

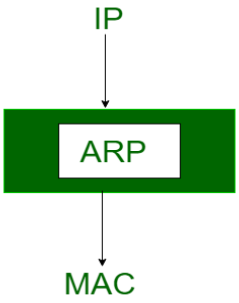
- The tools that can successfully penetrate the system
- Highlighting those points where security had been implemented correctly
- Those vulnerabilities that need to be corrected and how to prevent future attacks (remediation recommendations)

3)**Briefly explain about working of ARP and mention the 2 types of attacks involved in ARP with the help of a neat diagram.**

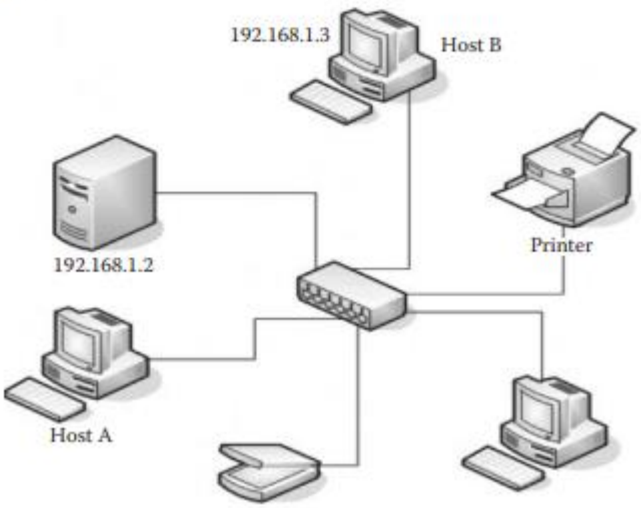
Ans)Address Resolution Protocol (ARP) is a communication protocol used to find the MAC (Media Access Control) address of a device from its IP address. This protocol is used when a device wants to communicate with another device on a Local Area Network or Ethernet.

- Most of the computer programs/applications use **logical address (IP address)** to send/receive messages, however, the actual communication happens over the **physical address (MAC address)** i.e from layer 2 of the OSI model.
- So our mission is to get the destination MAC address which helps in communicating with other devices.
- This is where ARP comes into the picture, its functionality is to translate IP address to physical addresses.

ARP finds the hardware address, also known as Media Access Control (MAC) address, of a host from its known IP address.



How ARP Works



So let’s imagine the scenario shown in the image, where on a switch-based network, “Host A” with an IP 192.168.1.2 would like to communicate with “Host B” with an IP 192.168.1.3. In order to communicate on a local area, Host A would need to have the MAC address of Host B. Host A will look inside its ARP cache and see if the entry for Host B’s IP address is present inside the ARP table. If it’s not present, Host A will send an ARP broadcast packet to every device on the network asking “Who has Host B’s IP address?” Once Host B receives the ARP request, it will send an ARP reply telling Host A “I am Host B and here is my MAC address.” The MAC address would be then saved inside the ARP table. An ARP cache contains a list of the IP and MAC addresses of every host we have communicated with.

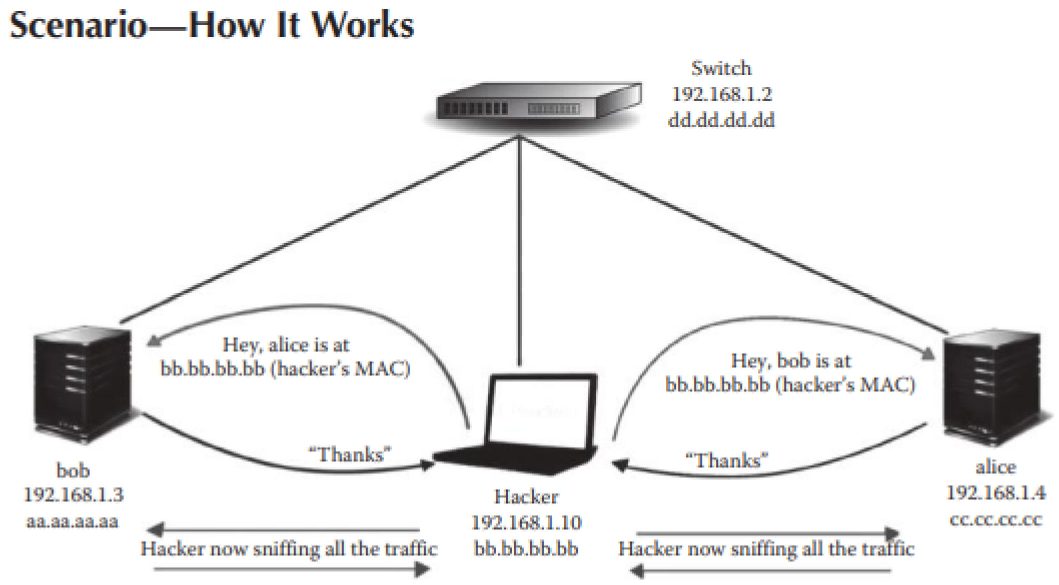
- **ARP Attacks:**
- There are two types of attack vectors that could be utilized with ARP:

  1. MAC flooding

  2. ARP poisoning or ARP spoofing

- **MAC** FloodingMAC Addresses are unique 48-bits hardware number of a computer, which is embedded into network card (known as Network Interface Card) during the time of manufacturing. MAC Address is also known as Physical Address of a network device..
- Flooding: Flooding is a non-adaptive routing technique following this simple method: when a data packet arrives at a router, it is sent to all the outgoing links except the one it has arrived on.
- a MAC flooding attack is to send a huge amount of ARP replies to a switch, thereby overloading the cam table of the switch.
- Once the switch overloads, it goes into hub mode, meaning that it will forward the traffic to every single computer on the network.

- All the attacker needs to do now is run a sniffer to capture all the traffic.
- This attack does not work on every switch; lots of newer switches have built-in protection against an attack.
- **ARP Poisoning**
- ARP poisoning is a very popular attack and can be used to get in the middle of a communication.
- This could be achieved by sending fake “ARP replies”. As discussed earlier, the ARP protocol would always trust that the reply is coming from the right device.
- Due to this flaw in its design, it can in no way verify that the ARP reply was sent from the correct device.
- The way it works is that the attacker would send a spoofed ARP reply to any computer on a network to make it believe that a certain IP is associated with a certain MAC address, thereby poisoning its ARP cache that keeps track of IP to MAC addresses.



Let’s take a look at the scenario presented in this image. The hacker sniffs all the traffic using the ARP spoofing attack. We have a switch with the IP 192.168.1.2. We have two hosts, namely, “bob” with the IP 192.168.1.3 and “alice” with the IP 192.168.1.4. The “hacker” computer is also located on the network with the IP 192.168.1.10. In order to launch an ARP spoofing attack, the attacker will send two spoofed ARP replies. The first reply will be sent to “alice” telling “bob” that “alice” is at the MAC address of the “hacker,” that is, “bb.bb.bb.bb”, so all the communication going from “bob” to “alice” will be forwarded to the hacker. Now, the hacker will send a spoofed ARP reply to “alice” as well telling that “bob” is located at the hacker’s MAC address, since he wants to sniff the traffic going from “alice” to “bob” as well. So through ARP spoofing, the hacker is now in the middle, sniffing traffic between the two hosts.

4) Define sniffing. Explain in detail about the types of sniffing

- **Sniffers** are a type of networking tool that is able to inspect packets of data traveling through a network. Sniffers may either be special software created to capture data packets or a physical hardware device that is connected directly to a network. In the case of software sniffers, the sniffer must be installed on a computer that has access to the target network. Data packets captured by sniffers are usually legitimate communications from end users, however, there are times when a malicious actor may be lurking on the network. A hacker can utilize network sniffers to capture data that may potentially reveal usernames, passwords, and other sensitive information. By using sniffers, network engineers can see what type of data is picked up by a sniffer and then make any necessary changes to the network before a hacker can capture data

types of sniffing

- Active sniffing
- Passive sniffing
- **Active sniffing** involves launching an Address Resolution Protocol (ARP) spoofing or traffic-flooding attack against a switch in order to capture traffic.
- **In passive sniffing** ,the traffic is locked but it is not altered in any way.
- Passive sniffing allows listening only. It works with Hub devices.
- On a hub device, the traffic is sent to all the ports.
- In a network that uses hubs to connect systems, all hosts on the network can see the traffic.
- Therefore, an attacker can easily capture traffic going through.

Explain in detail among **the OSSTMM and the NIST, which methodology is the best**

- The Open Source Security Testing Methodology Manual, or OSSTMM, is a peer-reviewed methodology for security testing, maintained by the Institute for Security and Open Methodologies (ISECOM). The manual is updated every six months or so, to remain relevant to the current state of security testing.
- An open-source security testing methodology manual (OSSTMM) basically includes almost all the steps involved in a penetration test.
- The methodology employed for penetration test is concise yet it’s a cumbersome process which makes it difficult to implement it in our everyday life.
- The penetration testing process typically goes through five phases: Planning and reconnaissance, scanning, gaining system access, persistent access, and the final analysis/report.
- Test goals are defined in first phase
- Scanning tools are used to understand how target responds to intrusions
- Web application attacks are staged to uncover a target vulnerabilities

- APTs (Advanced Persistent Threats)are intimated to see if a vulnerability can be used to maintain access.
- Results are used to configure WAF (web application firewall) settings before testing is run again
- Reconnaissance:
- This is the first step of Hacking. It is also called as information gathering Phase. This is the preparatory phase where we collect as much information as possible about the target. We usually collect information about three groups,
- Network
- Host
- People involved
- There are two types of Foot printing:
- **Active:** Directly interacting with the target to gather information about the target. Eg Using Nmap tool to scan the target
- **Passive:** Trying to collect the information about the target without directly accessing the target. This involves collecting information from social media, public websites etc.

Scanning:

Three types of scanning are involved:

Port scanning: This phase involves scanning the target for the information like open ports, Live systems, various services running on the host.

Vulnerability Scanning: Checking the target for weaknesses or vulnerabilities which can be exploited. Usually done with help of automated tools.

Network Mapping: Finding the topology of network, routers, firewalls servers if any, and host information and drawing a network diagram with the available information. This map may serve as a valuable piece of information throughout the haking process.

3**. Gaining Access:**

This phase is where an attacker breaks into the system/network using various tools or methods. After entering into a system, he has to increase his privilege to administrator level so he can install an application he needs or modify data or hide data.

4. Maintaining Access:

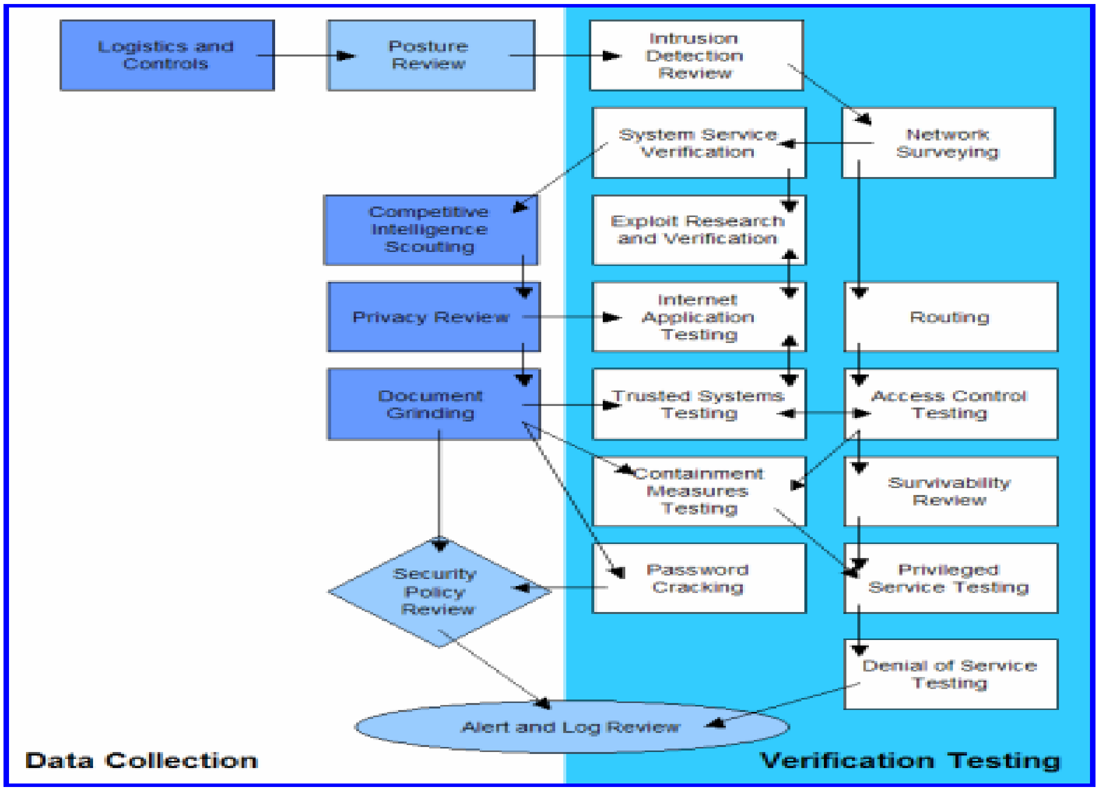
Hacker may just hack the system to show it was vulnerable or he can be so mischievous that he wants to maintain or persist the connection in the background without the knowledge of the user. This can be done using Trojans, Rootkits or other malicious files. The aim is to maintain the access to the target until he finishes the tasks he planned to accomplish in that target.

5. Analysis and Reporting

This is the result of a penetration test. As part of the last stage, the security team prepares a detailed report describing the entire penetration testing process. Some information or detail that should appear are:

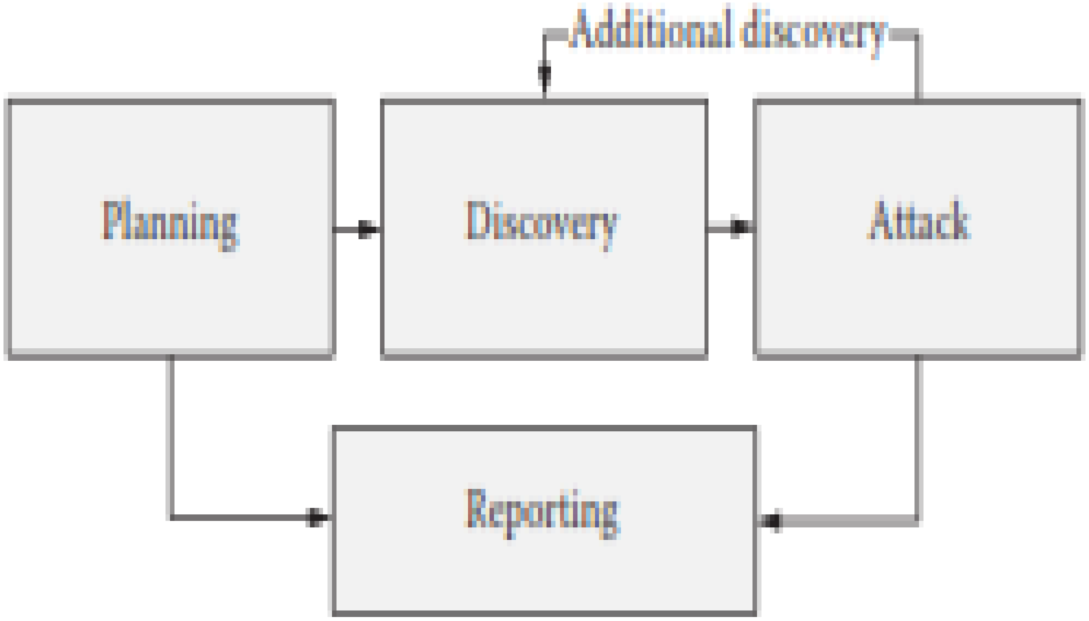
- The seriousness of the risks emanating from the vulnerabilities discovered
- The tools that can successfully penetrate the system
- Highlighting those points where security had been implemented correctly

- Those vulnerabilities that need to be corrected and how to prevent future attacks (remediation recommendations

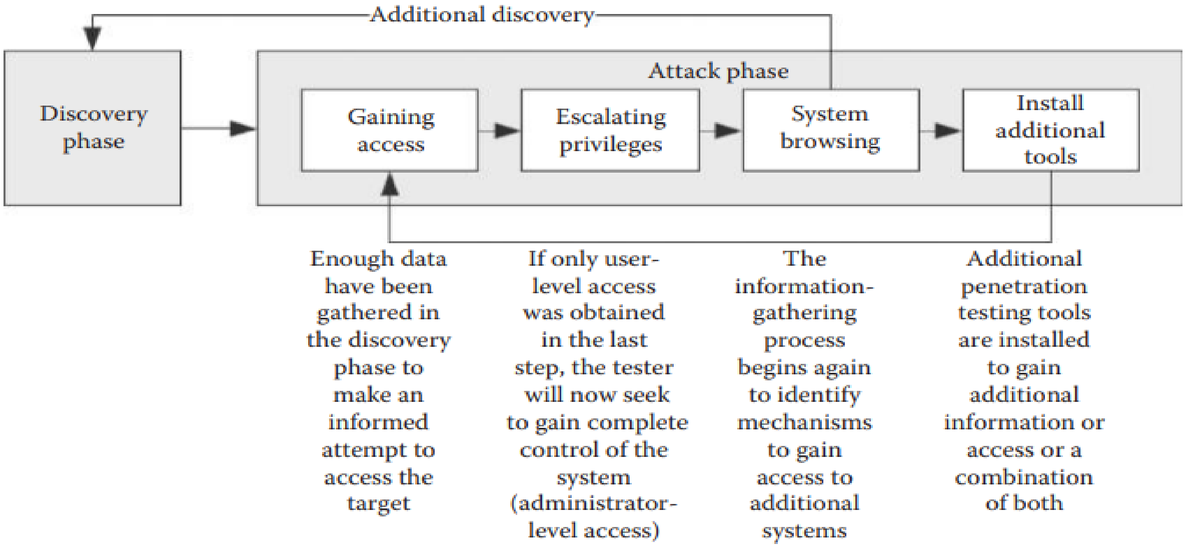


NIST

- NIST, on the other hand, is more comprehensive than OSSTMM, and it's something that you would be able to apply on a daily basis and in short engagements.
- The screenshot indicates the four steps of the methodology, namely, planning, discovery, attack, and reporting.
- The testing starts with the planning phase, where how the engagement is going to be performed is decided upon.
- This is followed by the discovery phase, which is divided into two parts—the first part includes information gathering, network scanning, service identification, and OS detection, and the second part involves vulnerability assessment.
- After the discovery phase comes the attack phase, which is the heart of every penetration test.
- If you are able to compromise a target and a new host is discovered, in case the system is connected with multiple interfaces, you would go back to step 2, that is, discovery, and repeat it until no targets are left.
- The indicating arrows in the block phase and the attack phase to the reporting phase indicate that you plan something and you report it—you attack a target and report the results.



- The organization also has a more detailed version of the chart discussed earlier, which actually explains more about the attack phase.
- It consists of things such as "gaining access," "escalating privileges," "system browsing," and "install additional tools."


Additional discovery
Discovery phase
Attack phase
Gaining access
Escalating privileges
System browsing
Install additional tools
Enough data have been gathered in the discovery phase to make an informed attempt to access the target
If only user-level access was obtained in the last step, the tester will now seek to gain complete control of the system (administrator-level access)
The information-gathering process begins again to identify mechanisms to gain access to additional systems
Additional penetration testing tools are installed to gain additional information or access or a combination of both

<u>Discuss in detail about OWASP and justify how we use OWASP for all "application penetration tests" we do here at the RHA InfoSEC</u>.

- OWASP stands **for Open Web Application Security Project.**
- The Open Web Application Security Project (OWASP) is a non-profit organization with a mission to make secure applications with free online educational content and community tools. Their mission is to make software security visible by providing all the tools, techniques, and mindsets to increase the application security of any software product.
- As you might have noticed, both the methodologies focused more on performing a network penetration test rather than something specifically built for testing web applications.
- The OWASP testing methodology is what we follow for all "application penetration tests".

- The OWASP testing guide basically contains almost everything that you would test a web application for.
- The methodology is comprehensive and is designed by some of the best web application security researchers.
- Under OWASP’s Broken Authentication category, it focuses on default or weak passwords. This has always been a major problem for all types of web applications. It is believed that weak passwords are still going to be a significant security vulnerability in 2021.
- Hackers have got their hands on advanced GPU technologies, which allows them to easily break weak passwords, even if the passwords use strong ciphers. They use brute-force attacks nowadays to break passwords.
- It is also found that administrators aren’t really vigilant about teaching users password best practices. Many enterprises are following the worst policies and systems for password selection. They only focus on uppercase and lowercase, special characters, and numbers, and not on password length itself.
- On the other hand, users are often forced to change their passwords frequently by the administrators, which causes them to use insecure passwords. All they do in the name of changing passwords is adding a predictable number or character at the end of the previous password.
- So, it is extremely important to follow good password habits in order to secure web applications in an organization.
- Injection
- Injection flaws are another great security vulnerability that might continue in 2021. They can lead to disastrous and undesirable results. Injection flaws may include file system injections, LDAP injections, SQL injections, and many more. Some of these flaws are so severe that they can even lead to remote code execution.
- Injection flaws happen when web applications take in users-supplied data in the form of a search or field query and pass it onto the server or backend database without a thorough input validation check.
- Thus, it becomes easy for the hackers to craft a string in an attempt to exploit the web application. The sad part is that without sufficient input sanitization, the query is executed on the server.
- Organizations need to use tried and tested remediation techniques like using a combination of output escaping, stored procedures, parameterized queries, and whitelists for server-side input validation.
- Another measure they can take is to use database controls like LIMIT for preventing mass disclosure in the event of a well-executed injection attack.

Explain in detail about the categories of penetration tests.

- The type of penetration testing normally depends on the scope and the organizational wants and requirements.
- types of Penetration Testing
- Following are the important types of Penetration testing −
- Black Box Penetration Testing
- White Box Penetration Testing
- Grey Box Penetration Testing

Black Box Penetration Testingin black box penetration testing, tester has no idea about the systems that he is going to test. He is interested to gather information about the target network or system. For example, in this testing, a tester only knows what should be the expected outcome and he does not know how the outcomes arrives. He does not examine any programming codes.

Advantages of Black Box Penetration Testing

It has the following advantages −

- Tester need not necessarily be an expert, as it does not demand specific language knowledge
- Tester verifies contradictions in the actual system and the specifications

- Test is generally conducted with the perspective of a user, not the designer

Disadvantages of Black Box Penetration Testing

Its disadvantages are −

- Particularly, these kinds of test cases are difficult to design.
- Possibly, it is not worth, incase designer has already conducted a test case.
- It does not conduct everything.

- **White Box Penetration Testing** this is a comprehensive testing, as tester has been provided with whole range of information about the systems and/or network such as Schema, Source code, OS details, IP address, etc.
- It is normally considered as a simulation of an attack by an internal source. It is also known as structural, glass box, clear box, and open box testing.

Advantages of White Box Penetration Testing

It carries the following advantages −

- It ensures that all independent paths of a module have been exercised.
- It ensures that all logical decisions have been verified along with their true and false value.
- It discovers the typographical errors and does syntax checking.
- It finds the design errors that may have occurred because of the difference between logical flow of the program and the actual execution.

Grey Box Penetration Testing

- In this type of testing, a tester usually provides partial or limited information about the internal details of the program of a system. It can be considered as an attack by an external hacker who had gained illegitimate access to an organization's network infrastructure documents

Advantages of Grey Box Penetration Testing

It has the following advantages −

- As the tester does not require the access of source code, it is non-intrusive and unbiased
- As there is clear difference between a developer and a tester, so there is least risk of personal conflict
- You don’t need to provide the internal information about the program functions and other operations
- .