1: different types of hacking

White Hat Hackers

White Hat hackers are also known as Ethical Hackers. They never intent to harm a system, rather they try to find out weaknesses in a computer or a network system as a part of penetration testing and vulnerability assessments.

Ethical hacking is not illegal and it is one of the demanding jobs available in the IT industry. There are numerous companies that hire ethical hackers for penetration testing and vulnerability assessments.

Black Hat Hackers

Black Hat hackers, also known as crackers, are those who hack in order to gain unauthorized access to a system and harm its operations or steal sensitive information.

Black Hat hacking is always illegal because of its bad intent which includes stealing corporate data, violating privacy, damaging the system, blocking network communication, etc.

Grey Hat Hackers

Grey hat hackers are a blend of both black hat and white hat hackers. They act without malicious intent but for their fun, they exploit a security weakness in a computer system or network without the owner’s permission or knowledge.

Their intent is to bring the weakness to the attention of the owners and getting appreciation or a little bounty from the owners.

2: different types of attacks

1.1 Denial of Service

Denial of service attacks leverage a vulnerability to create a loss of service, often by crashing the vulnerable process. The Stress Testing category of the Kali Linux menu contains a number of tools for this purpose.

When many people hear the term "denial of service attack", they immediately think of resource consumption attacks that are sent out from multiple sources at once against a single target. These would be a distributed denial of services attack, or DDOS. These sorts of attacks are rarely part of a professional security assessment.

1.2. Memory Corruption

A memory corruption happens when a location within the memory space of a process is accidentally modified due to programming mistakes. Memory corruption bugs usually lead to unpredictable program behavior, however in many cases, these bugs allow process memory manipulation in such a way that the program execution flow can be controlled, allowing attacker-defined activity.

These attacks are typically referred to as buffer overflows, although this term is an over-simplification. The most common types of memory corruption are vastly different from one another and have their own tactics and techniques required for successful exploitation.

Stack Buffer Overflow: When a program writes more data to a buffer on the stack than there is space available for it, adjacent memory can be corrupted, often causing the program to crash.

Heap Corruption

1.3. Web Vulnerabilities

Due to the fact that modern web sites are no longer static pages, but instead dynamically generated for the user, the average website is quite complex. Web vulnerabilities take advantage of this complexity in an effort to attack either the back end page generation logic or the presentation to the visitor of the site.

These sorts of attacks are extremely common, as many organizations have reached the point where they have very few externally facing services. Two of the most prevalent web application attack types are SQL injection and cross-site scripting (XSS).

SQL injection: These attacks take advantage of improperly-programmed applications that do not properly sanitize user input, leading to the ability to extract information from the database or even the complete takeover of the server.

Cross-site scripting.

1.4. Password Attacks

Password attacks are attacks against the authentication system of a service. These attacks are often broken into online password attacks and offline password attacks, which you will find reflected in the Password Attacks menu category. In an online password attack, multiple passwords are attempted against a running system. In an offline password attack, the hashed or encrypted values of the passwords are obtained and the attacker attempts to obtain the clear text values. The protection against this sort of attack is the fact that it is computationally expensive to work through this process, limiting the number of attempts per second you can generate. However, workarounds for this do exist, such as using graphic processor units (GPUs) to accelerate the number of attempts that can be made. The kali-tools-gpu metapackage contains a number of tools that tap into this power.

Most commonly, password attacks target vendor-supplied default passwords. As these are well-known values, attackers will scan for these default accounts, hoping to get lucky. Other common attacks include custom dictionary attacks where a wordlist is created that has been tailored to the target environment and then an online password attack against common, default, or known accounts is conducted where each word is attempted in sequence.

In an assessment,

1.5. Client-Side Attacks

Most attacks are conducted against servers, but as services have become harder to attack, easier targets have been selected. Client-side attacks are a result of this, where an attacker will target the various applications installed on the workstation of an employee within a target organization. The Social Engineering Tools menu category has a number of excellent applications that can help conduct these types of attacks.

his sort of attack were commonly exploited by Flash, Acrobat Reader, and Java in the early 2000s. Currently HTML Application (HTA) is the popular method. In the above cases, attackers would try to solicit a target to visit a malicious web page. These pages would contain specialized code that would trigger either vulnerabilities in these client-side applications or trick the user, resulting in the ability to run malicious code on the targets system.

Client-side attacks are incredibly difficult to prevent, requiring a great deal of user education, constant application updates, and network controls to effectively mitigate the risk.

3: what is interface in java ?

An interface in Java is a blueprint of a class. It has static constants and abstract methods.The interface in Java is a mechanism to achieve abstraction. There can be only abstract methods in the Java interface, not method body. It is used to achieve abstraction and multiple inheritance in Java.

In other words, you can say that interfaces can have abstract methods and variables. It cannot have a method body.

4: what is the use of lambda expression in java?

Lambda expressions basically express instances of functional interfaces (An interface with single abstract method is called functional interface. An example is java.lang.Runnable). lambda expressions implement the only abstract function and therefore implement functional interfaces

lambda expressions are added in Java 8 and provide below functionalities.

Enable to treat functionality as a method argument, or code as data.

A function that can be created without belonging to any class.

A lambda expression can be passed around as if it was an object and executed on demand.

5:what is #progma in c ?

The #pragma in C is a directive that is provided by the C standard in order to provide extra required details to the C compiler. These extra details can be anything that was somehow not passed within the program or the code logic. These directives, known as pragma are prefixed by the STDC in the standard.