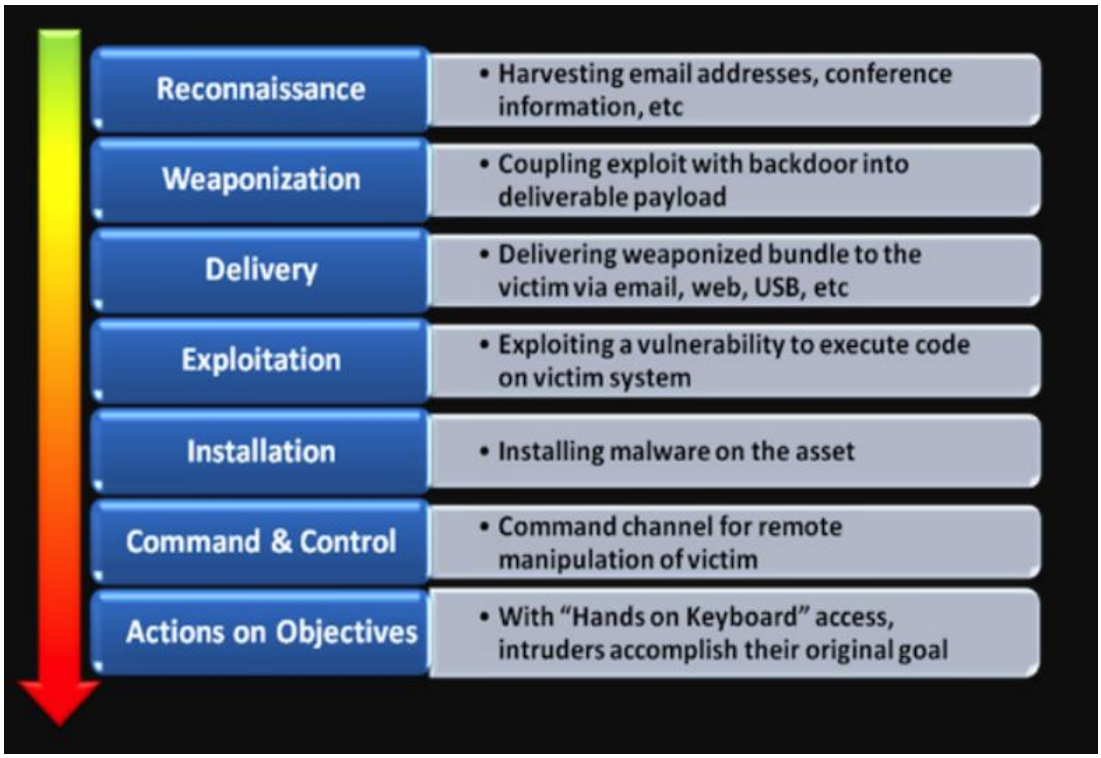
UNIT 1

1. What is Ethical Hacking and explain different Phases of Ethical Hacking.

Ethical hacking involves an authorized attempt to gain unauthorized access to a computer system, application, or data. Carrying out an ethical hack involves duplicating strategies and actions of malicious attackers. This practice helps to identify security vulnerabilities which can then be resolved before a malicious attacker has the opportunity to exploit them.

Phases Involved in Ethical Hacking:



1.Reconnaissance

- Generally,known as Information Gathering
- It is s a set of processes and techniques (Footprinting, Scanning & Enumeration) used to covertly discover and collect information about a target system
-

- Some Information includes-

✓ Domain Name
✓ IP Address
✓ Employee Information
✓ Phone Number
✓ Email Address

2.Weaponization

- This step happens at the attacker side
- Coupling exploit with backdoor into deliverable payload
- Here attackers have finished their research into your organization's vulnerabilities and have selected their targets. In this step, they are working out how best to get inside the network. This might be through a virus or malware tailored to exploit known vulnerabilities

3.Delivery

- The three most prevalent delivery vectors for weaponized payloads by attackers were observed to be email attachments, websites, and removable media such as a USB stick
- This step involves transmitting the weapon to the target

4.Exploitation

- In this step, the malware starts the action. The program code of the malware is triggered to exploit the target's vulnerability/vulnerabilities
- Often, exploitation targets an *application* or *operating system* vulnerability, but it could also more simply exploit the *users* themselves or leverage an operating system *feature that auto-executes code*

5.Installation

- Once the exploitation of the system has been successful, the malware code will install itself onto the targeted information system
- Here malware also installs an access point for the intruder / attacker. This access point is also known as the backdoor

6.Command & Control

- In this phase the attacker puts in place their *management and communication* code onto to the target network
- This software allows the attacker to fully manage the code in the environment and allows the attacker to move deeper into the network, exfiltrate data and conduct destruction or denial of service operations

7.Actions on Objectives

- Once the attacker / intruder gains persistent access, they finally take action to fulfill their purpose, such as *encryption* for ransom, *data exfiltration* or even *data destruction*

2. Explain briefly about Information security and its elements.

To help protect your identity, it's important to take steps to help protect yourself and your personal information. These steps can include:

- **Use strong, secure passwords.** Use a complex and unique password for each of your online accounts.
- **Monitor your bank and other financial accounts.** Check your accounts on a regular basis for unfamiliar activity. And if the companies offer activity alerts via text or email, it may make sense for you to sign up for them.
- **Check your credit report.** Do so regularly to see if a thief has attempted to open a new credit card or another account in your name.
- **Take action as soon as possible.** If you see suspicious activity, contact the financial institution involved immediately. If your information was stolen in a data breach, let them know that, as well.
- **Secure your phone.** If your phone doesn't have a password, give it one. Although entering a password every time you use your phone is tedious, it provides a line of defense if your device is lost or stolen. Think about all the information a criminal could access with your unprotected phone.
- **Use only secure URLs.** Reputable sites begin with https://. The "s" is key. This is especially important when entering credit card or other personal information.
- **Implement high-quality security software.** Install and use a software suite that includes malware and virus protection — and always keep it updated.
- **Back up your files and ensure their safety.** Use secure online Data Backup solutions as backup for your PC in addition to its other security features.
- **Wipe your hard drive.** If you are recycling your old computer, make sure that you clear your hard drive prior to disposal. The same goes for your smartphones and tablets.
- **Avoid oversharing on social media.** Never post anything pertaining to sensitive information and adjust your settings to make your profiles private. While you're at it, hold off sharing vacation pics on social media while you're still on vacation. That tells everyone your house may be sitting empty, a perfect target for burglary.
- **Use an identity theft protection or credit monitoring service.** The mess caused by a stolen identity could take months or even years to fix. Given the recent number of data breaches, it's important to consider identity theft protection or a credit monitoring service.

3. What is Social Engineering and explain the Impact of Social Engineering Attack on an Organization.

Social engineering is the psychological manipulation of people into performing actions or divulging confidential information. Social engineering is a technique scammers use to manipulate people, for instance, employees at a company, to reveal sensitive and private information to them.

The Impact of Social Engineering Attack on an Organization.

- **Financial losses as a result of social engineering attacks**

  This is perhaps the one consequence of hacker attacks that everyone knows about – the amount of money the company loses directly as a result of a social engineering attack.

- **Loss of productivity as a result of a social engineering cyber attack**

  Any successful cyber attack causes a huge disruption of normal business operations. The IT team and several management-level employees need to postpone their other tasks in order to deal with the breach, all employees need to be updated about the hack and trained to prevent the same attack in the future, etc. All of this takes away time from the employee's duties and significantly lowers productivity.

- **The cost of recovering after a social engineering attack**

  Another common cost associated with spear-phishing attacks is the recovery cost, which represents the amount of money needed to hire an incident response team, purchase software that will prevent the same attack from occurring in the future and resolve the issue with the customers if their data was stolen during the attack.

- **Cyber-attacks cause business disruption**

  This consequence of social engineering is similar to the loss of productivity but it measures the impact of the hack on your customer satisfaction rates and your supply chain. Since a successful hacker attack disrupts your normal business operations, your business may experience downtime in product manufacturing, shipping or other operations

- **Social engineering hacks cause huge damage to your reputation**

  If you were a customer or a supplier of a company that experienced a significant cyber security breach, how likely would you be to trust this company again? Would you continue to do business with this company? Unfortunately, for many businesses and, the answer is 'no' – people don't want to put themselves and their information in danger so a lot of businesses lose a significant number of customers and suppliers after a security breach.

4. Who is a hacker and describe different categories of Hackers.

Hackers are well aware of the working within the computer and networking in organizations. The intention behind the hacking determines the type of hacker they are. Getting unauthorized access to systems or networks is illegal and termed as hacking. So, one might wonder what hackers do on getting access to the system, well they can use vulnerable points in the system to bring the system down or steal confidential data. There are different kinds of hackers

1. White Hat Hackers
2. Black Hat Hackers
3. Gray Hat Hackers
4. Script Kiddies
5. Green Hat Hackers
6. Blue Hat Hackers
7. Red Hat Hackers
8. State/Nation Sponsored Hackers
9. Hacktivist
10. Malicious insider or Whistleblower

1) White Hat Hackers

White hat hackers are computer professionals with expertise in cybersecurity. They are authorized or certified to hack the systems. These White Hat Hackers work for governments or organizations by getting into the system. They hack the system from the loopholes in the cybersecurity of the organization. This hacking is done to test the level of cybersecurity in their organization. By doing so, they identify the weak points and fix them to avoid attacks from external sources. White hat hackers work as per the rules and regulations set by the government. They are also known as ethical hackers.

2) Black Hat Hackers

Black hat hackers are also knowledgeable computer experts but with the wrong intention. They attack other systems to get access to systems where they do not have authorized entry. On gaining entry they might steal the data or destroy the system. The hacking practices used depends on the hacking individual's capacity and knowledge. As the intentions of the hacker make the hacker a criminal. The malicious action intent of the individual cannot be gauged either can the extent of the breach while hacking.

3) Gray Hat Hackers

The intention behind the hacking is considered while categorizing the hacker. The Gray hat hacker falls in between the black and white hat hackers. They are not certified, hackers. The hackers work with either good or bad intentions. The hacking might be for their gain. The intention behind hacking decides the type of hacker. If the intention is for personal gain then the hacker is considered to be a gray hat hacker.

4) Script Kiddies

It is a known fact that half knowledge is always dangerous. The Script Kiddies are amateurs in the field of hacking. They try to hack the system with scripts from other fellow hackers. They try to hack the systems, networks, or websites. The intention behind the hacking is just to get attention from their peers. Script Kiddies are juveniles who do not have complete knowledge of the hacking process.

5) Green Hat Hackers

Green hat hackers are learning the ropes of hacking. They are slightly different from the Script Kiddies due to their intention. The intent is to strive and learn to become full-fledged hackers. They are looking for opportunities to learn from experienced hackers.

6) Blue Hat Hackers

Blue Hat Hackers are similar to Script Kiddies. The intent to learn is missing. They use hacking as a weapon to gain popularity among their fellow beings. They use hacking to settle scores with their adversaries. Blue Hat Hackers are dangerous due to the intent behind the hacking rather than their knowledge.

7) Red Hat Hackers

Red Hat Hackers are synonymous with Eagle-Eyed Hackers. They are similar to white hackers. The red hat hackers intend to stop the attack of black hat hackers. The difference between red hat hackers and white hat hackers is in the process of hacking through intention remains the same. Red hat hackers are quite ruthless while dealing with black hat hackers or counteracting with malware. The red hat hackers continue to attack and may end up having to replace the entire system set up.

Above are 7 types of hackers broadly referred to in the cyber security world.

The three types of hackers listed below work in a different capacity.

8) State/Nation Sponsored Hackers

Government appoints hackers to gain information about other countries. These hackers are known as State/Nation sponsored hackers. They use their knowledge to gain confidential information from other countries to be well prepared for any upcoming danger to their country. The sensitive information aids to be on top of every situation but also to avoid upcoming danger. They report only to their governments.

9) Hacktivist

The hackers intend to hack government websites. They pose themselves as activists, so known as a hacktivist. Hacktivist can be an individual or a bunch of nameless hackers whose intent is to gain access to government websites and networks. The data gained from government files accessed are used for personal political or social gain.

10) Malicious insider or Whistleblower

An individual working in an organization can expose confidential information. The intent behind the exposure might be a personal grudge with the organization or the individual might have come across the illegal activities within the organization. The reason for expose defines the intent behind the exposure. These individuals are known as whistleblowers.

5. Define the term Malware and what are the different ways for malware to Enter a system.

"Malware" is short for "malicious software" - computer programs designed to infiltrate and damage computers without the user's consent. "Malware" is the general term covering all the different types of threats to your computer safety such as viruses, spyware, worms, trojans, rootkits and so on. Today many experts believe the amount of malicious software being released on the web might actually surpass the release of valid software.

Different types of malware

The term malware includes viruses, worms, Trojan Horses, rootkits, spyware, keyloggers and more. To get an overview of the difference between all these types of threats and the way they work, it makes sense to divide them into groups:

1. **Viruses and worms – the contagious threat**

Viruses and worms are defined by their behavior – malicious software designed to spread without the user's knowledge. A virus infects legitimate software and when this software is used by the computer owner it spreads the virus – so viruses need you to act before they can spread. Computer worms, on the other hand, spread without user action. Both viruses and worms can carry a so-called "payload" – malicious code designed to do damage.

2. **Trojans and Rootkits – the masked threat**

Trojans and rootkits are grouped together as they both seek to conceal attacks on computers. Trojan Horses are malignant pieces of software pretending to be benign applications. Users therefore download them thinking they will get a useful piece of software and instead end up with a malware infected computer. Rootkits are different. They are a masking technique for malware, but do not contain damaging software. Rootkit techniques were invented by virus writers to conceal malware, so it could go unnoticed by antivirus detection and removal programs. Today, antivirus products, like BullGuard Internet Security, strike back as they come with effective rootkit removal tools.

3. Spyware and keyloggers – the financial threat

Spyware and keyloggers are malware used in malicious attacks like identity theft, phishing and social engineering - threats designed to steal money from unknowing computer users, businesses and banks.

Malware Analysis refers to the process by which the purpose and functionality of the given malware samples are analyzed and determined. The culled-out information provides insights into developing an effective detection technique for the malicious codes. Additionally, it is an essential aspect for developing the efficient removal tools which can definitely perform malware removal on an infected system.

6. Jennifer decided that the licensing cost for a piece of video editing software was too expensive. Instead, she decided to download a keygen program to generate her own license key and install a pirated version of the editing software. After she runs the keygen, a license key is created, but her system performance becomes very sluggish, and her antimalware suite begins to display numerous alerts. Which type of malware might her computer be infected with and why?

Trojan is a malware that affected the Jennifer computer.

Trojan Horses are malignant pieces of software pretending to be benign applications. Users therefore download them thinking they will get a useful piece of software and instead end up with a malware infected computer. Trojan malware operates in much the same way, in that it sneaks into your system often disguised as a legitimate tool like an update or a Flash download then, once inside your system, it begins its attacks.

Once installed in the system, depending on its capabilities a Trojan can then potentially access and capture everything logins and passwords, keystrokes, screenshots, system information, banking details, and more -- and secretly send it all to the attackers. Sometimes a Trojan can even allow attackers to modify data or turn off anti-malware protection.

7.What is meant by zero day attack?

Zero Day Attack

If a hacker manages to exploit the vulnerability before software developers can find a fix, that exploit becomes known as a zero day attack.

Zero day vulnerabilities can take almost any form, because they can manifest as any type of broader software vulnerability. For example, they could take the form of missing data encryption, SQL injection, buffer overflows, missing authorizations, broken algorithms, URL redirects, bugs, or problems with password security.

This makes zero day vulnerabilities difficult to proactively find—which in some ways is good news, because it also means hackers will have a hard time finding them. But it also means it's difficult to guard against these vulnerabilities effectively.

How to Protect Against Zero Day Attacks?

It's difficult to protect yourself from the possibility of a zero day attack, since they can take many forms. Almost any type of security vulnerability could be exploited as a zero day if a patch is not produced in time. Additionally, many software developers intentionally try not to publicly reveal the vulnerability, the hopes that they can issue a patch before any hackers discover that the vulnerability is present.

There are a few strategies that can help you defend your business against zero day attacks:

- **Stay informed**
  Zero day exploits aren't always publicized, but occasionally, you'll hear about a vulnerability that could potentially be exploited. If you stay tuned to the news and you pay attention to releases from your software vendors, you may have time to put in security measures or respond to a threat before it gets exploited.

- **Keep your systems updated**
  Developers work constantly to keep their software updated and patched to prevent the possibility of exploitation. When a vulnerability is discovered, it's only a matter of time before they issue a patch. However, it's up to you and your team to make sure your software platforms are up to date at all times. The best approach here is to enable automatic updates, so your software is updated routinely, and without the need for manual intervention.

- **Employ additional security measures**
  Ensure that you are using security solutions that protect against zero day attack because these security measures may not be enough to fully protect you from a zero day attack

8. What is data breach?

A data breach is a security incident in which information is accessed without authorization. Data breaches can jeopardize businesses and consumers in a variety of ways. They are a costly expense that can damage lives and reputations and take time to repair.

It may seem like stories of massive data breaches pop up in the news frequently these days. But it shouldn't be all that surprising.

As technology progresses, more and more of our information has been moving to the digital world. As a result, cyber attacks have become increasingly common and costly.

Globally, the average total cost to a company of a data breach is $3.86 million, according to a study by the Ponemon Institute. This means that at $148 on average per stolen record, online crime is a real threat to anyone on the internet.

Corporations and businesses are extremely attractive targets to cybercriminals, simply due to the large amount of data that can be grabbed in one single action.

Why do data breaches occur?

Cybercrime is a profitable industry for attackers and continues to grow. Hackers seek personally identifiable information to steal money, compromise identities, or sell over the dark web. Data breaches can occur for a number of reasons, including accidentally, but targeted attacks are typically carried out in these four ways:

- **Exploiting system vulnerabilities.** Out-of-date software can create a hole that allows an attacker to sneak malware onto a computer and steal data.
- **Weak passwords.** Weak and insecure user passwords are easier for hackers to guess, especially if a password contains whole words or phrases. That's why experts advise against simple passwords, and in favor of unique, complex passwords.
- **Drive-by downloads.** You could unintentionally download a virus or malware by simply visiting a compromised web page. A drive-by download will typically take advantage of a browser, application, or operating system that is out of date or has a security flaw.
- **Targeted malware attacks.** Attackers use spam and phishing email tactics to try to trick the user into revealing user credentials, downloading malware attachments, or directing users to vulnerable websites. Email is a common way for malware to end up on your computer. Avoid opening any links or attachments in an email from an unfamiliar source. Doing so can infect your computer with malware. And keep in mind that an email can be made to look like it comes from a trusted source, even when it's not.