Question Bank Unit 1

1. What is vulnerability in the Internet Crime.

A vulnerability is a weakness that can be exploited by cybercriminals to gain unauthorized access to a computer system. After exploiting a vulnerability, a cyberattack can run malicious code, install malware, and even steal sensitive data.

Vulnerabilities can be exploited by a variety of methods, including SQL injection, buffer overflows, cross-site scripting (XSS), and open-source exploit kits that look for known vulnerabilities and security weaknesses in web applications.

Many vulnerabilities impact popular software, placing the many customers using the software at a heightened risk of a data breach, or supply chain attack. Such zero-day exploits are registered by MITRE as a Common Vulnerability Exposure (CVE).

vulnerability Examples

There are several different types of vulnerabilities, determined by which infrastructure they're found on. Vulnerabilities can be classified into six broad categories:

1. Hardware

Any susceptibility to humidity, dust, soiling, natural disaster, poor encryption, or firmware vulnerability.

2. Software

Insufficient testing, lack of audit trail, design flaws, memory safety violations (buffer overflows, over-reads, dangling pointers), input validation errors (code injection, cross-site scripting (XSS), directory traversal, email injection, format string attacks, HTTP header injection, HTTP response splitting, SQL injection), privilege-confusion bugs (clickjacking, cross-site request forgery, FTP bounce attack), race conditions (symlink races, time-of-check-to-time-of-use bugs),

. Network

Unprotected communication lines, man-in-the-middle attacks, insecure network architecture, lack of authentication, default authentication, or other poor network security.

4. Personnel

Poor recruiting policy, lack of security awareness and training, poor adherence to security training, poor password management, or downloading malware via email attachments.

5. Physical site

Area subject to natural disaster, unreliable power source, or no keycard access.

6. Organizational

Improper internal controls, lack of audit, continuity plan, security, or incident response plan.

2. Explain passive attacks and active attacks with respect to cyber criminals?

There are two types of attacks that are related to security namely passive and active attacks. In an active attack, an attacker tries to modify the content of the messages. In a passive attack, an attacker observes the messages and copies them.

Passive Attacks

The first type of attack is passive attack. A passive attack can monitor, observe or build use of the system's data for sure functions. However, it doesn't have any impact on the system resources, and also, the data can stay unchanged. The victim is difficult to note passive attacks as this sort of attack is conducted in secret. Passive attack aims to achieve data or scan open ports and vulnerabilities of the network.

An **eavesdropping attack** is taken into account as a kind of passive attack. An eavesdropping attack is to steal data transmitted among two devices that area unit connected to the net. Traffic analysis is enclosed in eavesdropping. An eavesdropping attack happens once the attackers insert a software package within the network path to capture future study network traffic. The attackers have to be compelled to get into the

network path between the end point and the UC system to capture the network traffic. If their area unit additional network methods and also the network methods area unit longer, it'll be more comfortable for the offender to insert a software package within the network path.

3. The **release of messages** is additionally another kind of passive attack. The attackers install a package to the device by using virus or malware to watch the device's activities like a conversation of messages, emails, or any transferred files that contain personal information and knowledge. The attackers will use the data to compromise the device or network.
4. Some other attacks that have emerged thanks to the exponential interconnection of insecure devices like IoT infrastructure include those that square measure protocol-specific, likewise as wireless device networks-based
5. For example, in associate IoT-based, mostly sensible-home systems, the communication protocol used is also RPL (Routing protocol for low-power and lossy networks). This protocol is employed thanks to its compatibility with resource-constrained IoT devices that cannot use ancient protocols.

Active Attacks

6. An active attack could be a network exploit during which the attackers will modify or alter the content and impact the system resource. It'll cause damages to the victims. The attackers can perform passive attacks to gather info before they begin playacting a vigorous attack. The attackers attempt to disrupt and forced the lock of the system. The victims can get informed concerning the active attack. This sort of attack can threaten their integrity and accessibility. A vigorous attack is tougher to perform compared to a passive attack.
7. **Denial-of-Service** attacks (DoS) are one in each of the samples of active attack. A denial-of-Service attack happens once the attackers take action to close up a tool or network. This may cause the first user to be unable to access the actual device or network. The attackers can flood the target device or network with traffic till it's not responding or flaming. The services that are affected are emails, websites, or on-line banking accounts. Dos attacks may be performed merely from any location.
8. As mentioned on top of, DoS attack includes flooding or flaming the device and network. Buffer overflow attack is one in every of the common DoS attacks. This sort of flooding attack sends a lot and a lot of traffic to the network that exceeds the limit that a buffer will handle. Then, it'll lead to a flaming of the system. What is more, **ICMP flood**, called ping flood, is additionally a kind of flooding attack. The assaulter can send spoofed packets and flood them with ICMP echo requests. The network is forced to reply to all or any claims. This may cause the device not to be accessible to traditional traffic.
9. Moreover, **SYN flood** is additionally a kind of flooding attack. The attackers can keep generating SYN packets to all or any of the ports of the server. Faux

informatics addresses are usually used. The server that is unaware of the attack can then reply to the SYN-ACK packets. The server can fail to access the shoppers and therefore crash. Applied math approaches may be prone to develop attack detection techniques for attacks like SYN flood. One such technique is projected by authors wherever they need projecting SYN flood attack detection theme supported Bayes calculator for unintended mobile networks.

10. **Trojan horse attacks** are another example of network attack, the most ordinary sort of that is backdoor trojan. A backdoor trojan permits the attackers that don't have the authority to realize access to the pc system, network, or code application. As an example, the attackers may hide some malware in an exceedingly explicit link. Once the users click the link, a backdoor is going to be downloaded within the device. Then, the attackers can have basic access to the device. Apart from that, a rootkit is additionally another example of a trojan attack. A rootkit is usually won't to get hidden privileged access to a system. It'll give root access to the attackers. The attackers can manage the system; however, the users won't get informed of it. They will amend any settings of the pc, access any files or photos, and monitor the users' activities. A number of the favored rootkit examples are Lane Davis and Steven Dake, NTRootKit, philosopher Zeus, Stuxnet, and Flame. Flame a malware that's established within the year 2012 that is intended to attack Windows OS. It will perform some options like recording audio, screenshotting, and observance network traffic.
11. Moreover, a **replay attack** is one in every one of the samples of active attack. The attackers can snoop on a specific user before they begin playacting a replay attack. Then, they're going to send to the victim Associate in Nursing the same message from Associate in Nursing authorized user, and the message is appropriately encrypted. Replay attacks enable the assaulter to possess access to the information and knowledge keep within the compromised device. They can also gain money profit as they're able to duplicate the group action of the victim. This as a result of the attackers can listen to the frames of this session, mistreatment constant info to perform the attack while not limiting the number of times. There's another attack referred to as a cut-and-paste attack that is comparable to a replay attack. In a cut-and-paste attack, the assaulter can mix different ciphertext elements and send them to the victim. The assaulter can then get the data they require and use them to compromise the system.

3.what is the difference between Threat,vulnerability, and Risk?

The **Threat**, **Vulnerability**, and **Risk** these terms are interrelated but not the same. In this article, we are going to discuss the difference between them and how they are related to each other.

Threat

A cyber threat is a malicious act that seeks to steal or damage data or discompose the digital network or system. Threats can also be defined as the possibility of a successful cyber attack to get access to the sensitive data of a system unethically. Examples of threats include **computer viruses**, **Denial of Service (DoS) attacks**, **data breaches**, and even sometimes **dishonest employees**.

Types of Threat

Threats could be of three types, which are as follows:

1. **Intentional-** Malware, phishing, and accessing someone's account illegally, etc. are examples of intentional threats.
2. **Unintentional-** Unintentional threats are considered human errors, for example, forgetting to update the firewall or the anti-virus could make the system more vulnerable.
3. **Natural-** Natural disasters can also damage the data, they are known as natural threats.

Vulnerability:

In cybersecurity, a vulnerability is a flaw in a system's design, security procedures, internal controls, etc., that can be exploited by cybercriminals. In some very rare cases, cyber vulnerabilities are created as a result of cyberattacks, not because of network misconfigurations. Even it can be caused if any employee anyhow downloads a virus or a social engineering attack.

Types of Vulnerability

Vulnerabilities could be of many types, based on different criteria, some of them are:

- **Network-** Network vulnerability is caused when there are some flaws in the network's hardware or software.
- **Operating system-** When an operating system designer designs an operating system with a policy that grants every program/user to have full access to the computer, it allows viruses and malware to make changes on behalf of the administrator.
- **Human-** Users' negligence can cause vulnerabilities in the system.
- **Process-** Specific process control can also cause vulnerabilities in the system.

Risk:

Cyber risk is a potential consequence of the loss or damage of assets or data caused by a cyber threat. Risk can never be completely removed, but it can be

managed to a level that satisfies an organization's tolerance for risk. So, our target is not to have a risk-free system, but to keep the risk as low as possible. Cyber risks can be defined with this simple formula- **Risk = Threat + Vulnerability**. Cyber risks are generally determined by examining the threat actor and type of vulnerabilities that the system has.

Types of Risks

There are two types of cyber risks, which are as follows:

1. External- External cyber risks are those which come from outside an organization, such as cyberattacks, phishing, ransomware, DDoS attacks, etc.
2. Internal- Internal cyber risks come from insiders. These insiders could have malicious intent or are just not be properly trained.

Difference Between Threat, Vulnerability, and Risk

	Threat	Vulnerability	Risks
1.	Take advantage of vulnerabilities in the system and have the potential to steal and damage data.	Known as the weakness in hardware, software, or designs, which might allow cyber threats to happen.	The potential for loss or destruction of data is caused by cyber threats.
2.	Generally, can't be controlled.	Can be controlled.	Can be controlled.
3.	It may or may not be intentional.	Generally, unintentional.	Always intentional.
4.	Can be blocked by managing the vulnerabilities.	Vulnerability management is a process of identifying the problems, then categorizing them, prioritizing them, and resolving the vulnerabilities in that order.	Reducing data transfers, downloading files from reliable sources, updating the software regularly, hiring a professional cybersecurity team to monitor data, developing an incident management plan, etc. help to lower down the possibility of cyber risks.

	Threat	Vulnerability	Risks
5.	Can be detected by anti-virus software and threat detection logs.	Can be detected by penetration testing hardware and many vulnerability scanners.	Can be detected by identifying mysterious emails, suspicious pop-ups, observing unusual password activities, a slower than normal network, etc.

4.What is Cybercrime? Explain different types of Cybercrimes in detail.

Cybercrime refers to criminal conduct committed with the aid of a computer or other electronic equipment connected to the internet. Individuals or small groups of people with little technical knowledge and highly organized worldwide criminal groups with relatively talented developers and specialists can engage in cybercrime.

here are several types of cybercrimes; the most common ones are email frauds, social media frauds, banking frauds, ransomware attacks, cyber espionage, identity theft, clickjacking, spyware, etc. Let us now see how these crimes are executed.

Malware

Malware is a broad phrase that encompasses a wide range of cyberattacks such as Trojans, viruses, and worms. Malware can simply be described as code written to steal data or destroy things on a computer.

How malware causes harm can assist us to classify the type of virus that we are dealing with. So, let us talk about it!

- **Viruses:** Viruses, like their biological namesakes, attach themselves to clean files and infect other clean files. Viruses can spread uncontrollably, causing

damage to the core functionality as well as deleting and corrupting files. Viruses usually appear as executable files downloaded from the internet.

- **Trojan:** This type of malware masquerades as legitimate software that can be hacked. It prefers to function invisibly and creates security backdoors that allow other viruses to enter the system.
- **Worms:** Worms use the network's interface to infect a whole network of devices, either locally or via the internet. Worms infect more machines with each successive infected machine.

Phishing

Phishing frequently poses as a request for information from a reputable third party. Phishing emails invite users to click on a link and enter their personal information.

In recent years, phishing emails have become much more complex, making it impossible for some users to distinguish between a real request for information and a fraudulent one. Phishing emails are sometimes lumped in with spam, but they are far more dangerous than a simple advertisement.

There are five steps to phishing:

- **Preparation:** The phisher must pick a business to target and figure out how to obtain the email addresses of that business' customers.
- **Setup:** Once the phisher has decided which entity to mimic and who the victims will be, the setup process can begin. The phisher constructs and distributes communications and collects data.
- **Carry out the attack:** This is a process that most people are familiar with. The phisher sends a fake message that appears to come from a well-known source.

- **Phishing ding data:** The phisher keeps track of the information that victims submit to websites or pop-up windows.
- **Identity theft and fraud:** The phisher uses the collected information to make unlawful transactions or perform other forms of fraud; up to a quarter of the victims never fully recover.

Enroll in our Cyber Security courses to be a master in this domain!

DDoS Attack

As the name suggests, a denial-of-service (DoS) attack focuses on disrupting network service. Attackers transmit a large amount of data traffic via the network until it becomes overloaded and stops working. A DoS attack can be carried out in a variety of ways, but the most common is a distributed denial-of-service (DDoS) attack. It involves the attacker sending traffic or data, by utilizing several machines, that will overload the system.

An individual may not recognize that their computer has been hijacked and is helping to the DoS attack in many cases. Disrupting services can have major ramifications for security and internet access; many large-scale DoS attacks have occurred in the past. Many instances of large-scale DoS attacks have been implemented as a single sign of protests toward governments.

5.What is Hacking? Explain types of Hackers.

A commonly used hacking definition is the act of compromising digital devices and networks through unauthorized access to an account or computer system. Hacking is not always a malicious act, but it is most commonly associated with illegal activity and data theft by cyber criminals.

Hacking refers to the misuse of devices like computers, smartphones, tablets, and networks to cause damage to or corrupt systems, gather information on users, steal data and documents, or disrupt data-related activity.

A traditional view of hackers is a lone rogue programmer who is highly skilled in coding and modifying computer software and hardware systems. But this narrow view does not cover the true technical nature of hacking. Hackers are increasingly growing in sophistication, using stealthy attack

methods designed to go completely unnoticed by cybersecurity software and IT teams. They are also highly skilled in creating attack vectors that trick users into opening malicious attachments or links and freely giving up their sensitive personal data.

As a result, modern-day hacking involves far more than just an angry kid in their bedroom. It is a multibillion-dollar industry with extremely sophisticated and successful techniques.

Types of Hacking/Hackers

There are typically four key drivers that lead to bad actors hacking websites or systems: (1) financial gain through the theft of credit card details or by defrauding financial services, (2) corporate espionage, (3) to gain notoriety or respect for their hacking talents, and (4) state-sponsored hacking that aims to steal business information and national intelligence. On top of that, there are politically motivated hackers—or hacktivists—who aim to raise public attention by leaking sensitive information, such as Anonymous, LulzSec, and WikiLeaks.

A few of the most common types of hackers that carry out these activities involve:

Black Hat Hackers

Black hat hackers are the "bad guys" of the hacking scene. They go out of their way to discover vulnerabilities in computer systems and software to exploit them for financial gain or for more malicious purposes, such as to gain reputation, carry out corporate espionage, or as part of a nation-state hacking campaign.

These individuals' actions can inflict serious damage on both computer users and the organizations they work for. They can steal sensitive personal information, compromise computer and financial systems, and alter or take down the functionality of websites and critical networks.

White Hat Hackers

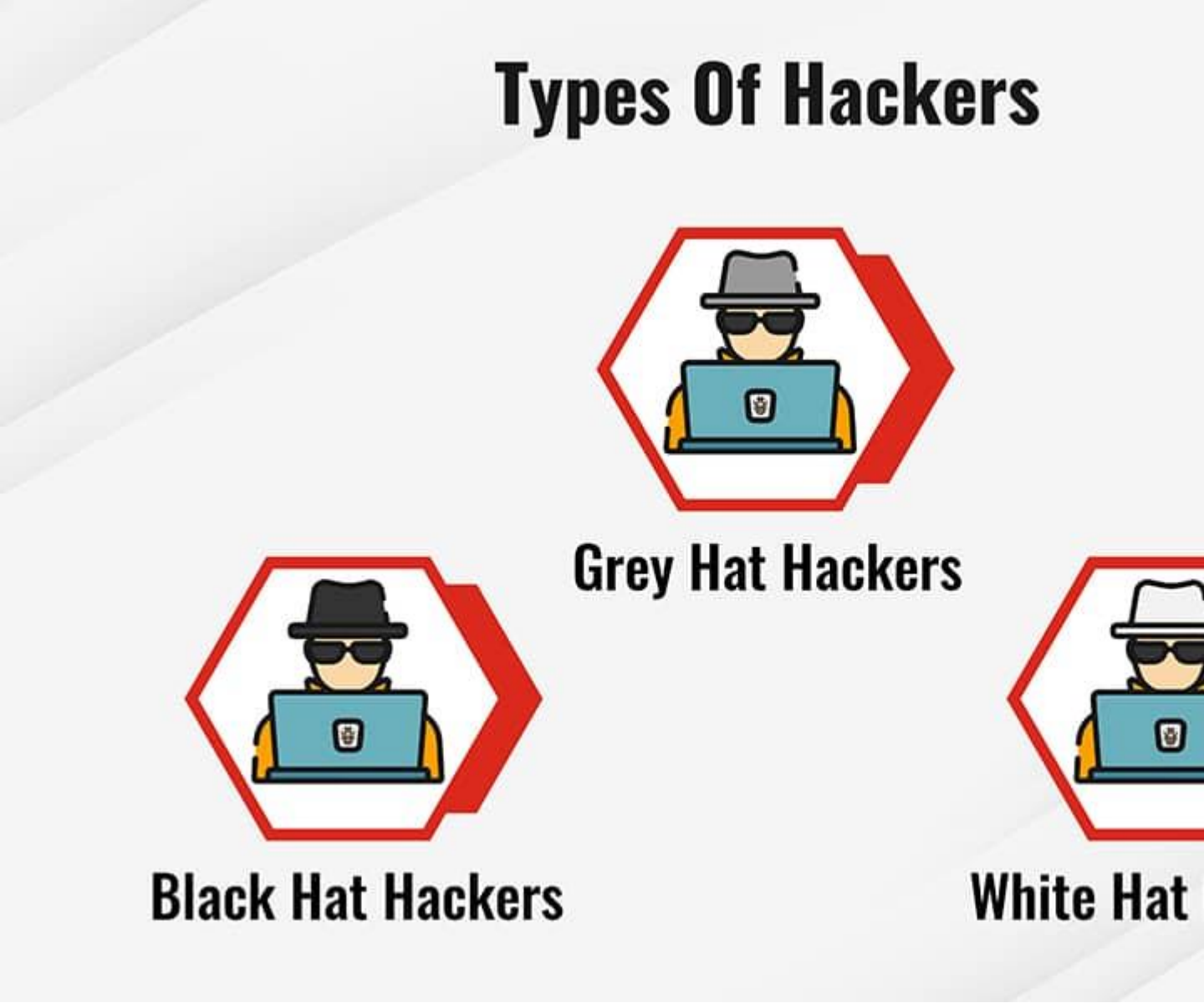
White hat hackers can be seen as the "good guys" who attempt to prevent the success of black hat hackers through proactive hacking. They use their technical skills to break into systems to assess and test the level of network security, also known as ethical hacking. This helps expose vulnerabilities in systems before black hat hackers can detect and exploit them.

The techniques white hat hackers use are similar to or even identical to those of black hat hackers, but these individuals are hired by organizations to test and discover potential holes in their security defenses.

Grey Hat Hackers

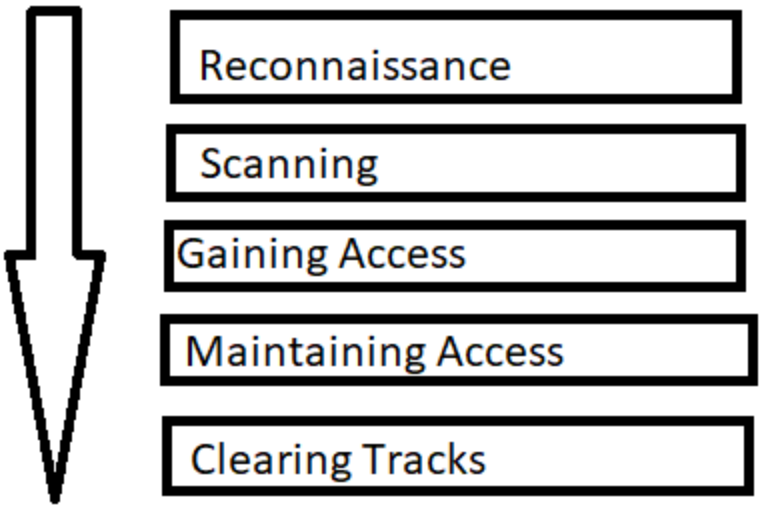
Grey hat hackers sit somewhere between the good and the bad guys. Unlike black hat hackers, they attempt to violate standards and principles but without intending to do harm or gain financially. Their actions are typically carried out for the common good. For example, they may exploit a vulnerability

to raise awareness that it exists, but unlike white hat hackers, they do so publicly. This alerts malicious actors to the existence of the vulnerability.



6.What are phases of hacking? Explain in detail.

5 phases in hacking



There is a term called **Vulnerability Assessment** which is quite similar to Penetration Testing. Vulnerability Assessment means reviewing services and systems for security issues. Many people use pen testing and vulnerability assessment interchangeably for each other but they are not the same. The penetration testing process is a step ahead of vulnerability assessment. Vulnerability Assessment only discovers flaws in the system but PT provides a way to remove those flaws as well.

1. Reconnaissance: This is the first phase where the Hacker tries to collect information about the target. It may include Identifying the Target, finding out the target's IP Address Range, Network, DNS records, etc. Let's assume that an attacker is about to hack a websites' contacts. He may do so by using a search engine like maltego, researching the target say a website (checking links, jobs, job titles, email, news, etc.), or a tool like HTTPTrack to download the entire website for later enumeration, the hacker is able to determine the following: Staff names, positions, and email addresses.

2. Scanning: This phase includes the usage of tools like dialers, port scanners, network mappers, sweepers, and vulnerability scanners to scan data. Hackers are now probably seeking any information that can help them perpetrate attacks such as computer names, IP addresses, and user accounts. Now that the hacker has some basic information, the hacker now moves to the next phase and begins to test the network for other avenues of attacks. The hacker decides to use a couple of methods for this end to help map the network (i.e. Kali Linux, Maltego and find an email to contact to see what email server is being used). The hacker looks for an automated email if possible or based on the information gathered he may decide to email HR with an inquiry about a job posting.

3. Gaining Access: In this phase, the hacker designs the blueprint of the network of the target with the help of data collected during Phase 1 and Phase 2. The hacker has finished enumerating and scanning the network and now decides that they have some options to gain access to the network. For example, say a hacker chooses a Phishing Attack. The hacker decides to play it safe and use a simple phishing attack to gain access. The hacker decides to infiltrate the IT department. They see that there have been some recent hires and they are likely not up to speed on the procedures yet. A phishing email will be sent using the CTO's actual email address using a program and sent out to the techs. The email contains a phishing website that will collect their login and passwords. Using any number of options (phone app, website email spoofing, Zmail, etc) the hacker sends an email asking the users to log in to a new Google portal with their credentials. They already have the Social Engineering Toolkit running and have sent an email with the server address to the users masking it with a bitly or tinyurl.

Other options include creating a reverse TCP/IP shell in a PDF using **Metasploit** (may be caught by spam filter). Looking at the event calendar they can set up an Evil Twin router and try to Man in the Middle attack users to gain access. A variant of Denial of Service attack, stack-based buffer overflows, and session hijacking may also prove to be great.

4. Maintaining Access: Once a hacker has gained access, they want to keep that access for future exploitation and attacks. Once the hacker owns the system, they can use it as a base to launch additional attacks.

In this case, the owned system is sometimes referred to as a zombie system**.** Now that the hacker has multiple e-mail accounts, the hacker begins to test the accounts on the domain. The hacker from this point creates a new administrator account for themselves based on the naming structure and tries and blends in. As a precaution, the hacker begins to look for and identify accounts that have not been used for a long time. The hacker assumes that these accounts are likely either forgotten or not used so they change the password and elevate privileges to an administrator as a secondary account in order to maintain access to the network. The hacker may also send out emails to other users with an exploited file such as a PDF with a reverse shell in order to extend their possible access. No overt exploitation or attacks will occur at this time. If there is no evidence of detection, a waiting game is played letting the victim think that nothing was disturbed. With access to an IT account, the hacker begins to make copies of all emails, appointments, contacts, instant messages and files to be sorted through and used later.

5. Clearing Tracks (so no one can reach them): Prior to the attack, the attacker would change their MAC address and run the attacking machine through at least one VPN to help cover their identity. They will not deliver a direct attack or any scanning technique that would be deemed "noisy".

Once access is gained and privileges have been escalated, the hacker seeks to

cover their tracks. This includes clearing out Sent emails, clearing server logs, temp files, etc. The hacker will also look for indications of the email provider alerting the user or possible unauthorized logins under their account.
Most of the time is spent on the Reconnaissance process. Time spend gets reduced in upcoming phases. The inverted triangle in the diagram represents a time to spend in subsequent phases that get reduced.

7. Define following terms: a. Vulnerability b. Threat c. Exploit d. Active attack e. Passive attack f. Cyberspace g. Cyber security

A. A vulnerability, in information technology (IT), is a flaw in code or design that creates a potential point of security compromise for an endpoint or network. Vulnerabilities create possible attack vectors, through which an intruder could run code or access a target system's memory. The means by which vulnerabilities are exploited are varied and include code injection and buffer overruns; they may be conducted through hacking scripts, applications and free hand coding. A zero-day exploit, for example, takes place as soon as a vulnerability becomes generally known.

B.

A cyber threat or cybersecurity threat is defined as a malicious act intended to steal or damage data or disrupt the digital wellbeing and stability of an enterprise. Cyber threats include a wide range of attacks ranging from data breaches, computer viruses, denial of service, and numerous other attack vectors. This article looks at the definition of cyber threats, types of cyber threats, and some common examples of threats. It also explores related concepts such as cyber threat intelligence and cyber threat hunting and shares the top five best practices for effective cyber threat hunting.

C.An exploit (in its noun form) is a segment of code or a program that maliciously takes advantage of vulnerabilities or security flaws in software or hardware to infiltrate and initiate a denial-of-service (DoS) attack or install malware, such as spyware, ransomware, Trojan horses, worms, or viruses. So the exploit is not the malware itself but is used to deliver the malware. To exploit (in its verb form) is to successfully carry out such an attack.

D.ACTIVE ATTACK

An active attack, in computing security, is an attack characterized by the attacker attempting to break into the system. During an active attack, the intruder may introduce data into the system as well as potentially change data within the system.

E.PASSIVE ATTACK

A passive attack is a network attack in which a system is monitored and sometimes scanned for open ports and vulnerabilities. The purpose of a passive attack is to gain information A about the system being targeted; it does not involve any direct action on the target.

F.CYBERSPACE

Cyberspace refers to the virtual computer world, and more specifically, an electronic medium that is used to facilitate online communication. Cyberspace typically involves a large computer network made up of many worldwide computer subnetworks that employ TCP/IP protocol to aid in communication and data exchange activities.

g. Cyber security

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

- # Unit 2
- # 1. Explain Virus and Worms, Trojan Horses and Backdoors.
- Virus is a computer program or software that connect itself to another software or computer program to harm computer system. When the computer program runs attached with virus it perform some action such as deleting a file from the computer system. Virus can't be controlled by remote.
- Worms:
  Worms is also a computer program like virus but it does not modify the program. It replicate itself more and more to cause slow down the computer system. Worms can be controlled by remote.
- **Trojan Horse:**
  Trojan Horse does not replicate itself like virus and worms. It is a hidden piece of code which steal the important information of user. For example, Trojan horse software observe the e-mail ID and password while entering in web browser for logging.
- Backdoors:
- A backdoor is **a malware type that negates normal authentication procedures to access a system**. As a result, remote access is granted to resources within an application, such as databases and file servers, giving perpetrators the ability to remotely issue system commands and update malware.
-

2. Why Keyloggers are a threat? How cyber criminals use Keyloggers?

keylogger can pose a serious threat to users as they can intercept passwords and other confidential information entered through the keyboard. As a result, the cybercriminals can steal PIN codes, bank account numbers, passwords to emails and social networking account credentials. These credentials can later be used to steal the victim's money, identity and possibly extort information & money from close relatives.

How does it spread?

Keylogger spread in the same way as the other malicious software. The common methods of propagation of the malware are:

- When a user opens a malicious attachment received via email, text message, P2P networks or social networks;
- When a user visits a malicious website.

How to stay safe?

Following tips can help users protect themselves from keyloggers:

- Avoid visiting dangerous websites or downloading infected programs, videos and games;
- Be wary when opening attachments that come via unknown email P2P networks or text messages;
- Use on-screen virtual keyboard while entering crendentials on banking websites;
- Use Multi-factor authentication as an additional layer of protection. This prevent the attackers from accessing the accounts even if they have the login credentials;
- Use a comprehensive security solution.

How do cybercriminals use keyloggers?

Cybercriminals use keyloggers to steal credentials, bank login information, social media login information and personal information. From there, they can steal identities, money, or smear a person's online reputation.

Keyloggers are also used by law enforcement to track down cybercriminals and gain access to restricted accounts. In 2000-2002, the FBI used keyloggers to hack into Nicodemo Scarfo Jr's computer, obtaining evidence to convict the son of the famous mob boss and several associates.

In 2018, the website builder WordPress suffered a keylogging attack on at least 2,000 WordPress sites. The keylogger was installed via a crypto logging script, or in-browser crypto miner. The keylogger

allowed cybercriminals to gather credentials from thousands of websites and compromise information.

-

3. What is Virus and Warms?

Viruses and worms are malicious programs that self-replicate on computers or via computer networks without the user being aware; each subsequent copy of such malicious programs is also able to self-replicate.

Malicious programs which spread via networks or infect remote machines when commanded to do so by the “owner” (e.g. Backdoors) or programs that create multiple copies that are unable to self-replicate are not part of the Viruses and Worms subclass.

The main characteristic used to determine whether or not a program is classified as a separate behaviour within the Viruses and Worms subclass is how the program propagates (i.e. how the malicious program spreads copies of itself via local or network resources.)

Most known worms are spread as files sent as email attachments, via a link to a web or FTP resource, via a link sent in an ICQ or IRC message, via P2P file sharing networks etc.

Some worms spread as network packets; these directly penetrate the computer memory, and the worm code is then activated.

Worms use the following techniques to penetrate remote computers and launch copies of themselves: social engineering (for example, an email message suggesting the user opens an attached file), exploiting network configuration errors (such as copying to a fully accessible disk), and exploiting loopholes in operating system and application security.

Viruses can be divided in accordance with the method used to infect a computer:

- file viruses
- boot sector viruses
- macro viruses

- script viruses

Any program within this subclass can have additional Trojan functions.

It should also be noted that many worms use more than one method in order to spread copies via networks. The rules for classifying detected objects with multiple functions should be used to classify these types of worms.

This subclass of malicious programs includes the following behaviours:

- Email-Worm
- IM-Worm
- IRC-Worm
- Net-Worm
- P2P-Worm
- Virus
- Worm

4. How Buffer overflow attack works?

A buffer overflow attack takes place when an attacker manipulates the coding error to carry out malicious actions and compromise the affected system. The attacker alters the application's execution path and overwrites elements of its memory, which amends the program's execution path to damage existing files or expose data.

A buffer overflow attack typically involves violating programming languages and overwriting the bounds of the buffers they exist on. Most buffer overflows are caused by the combination of manipulating memory and mistaken assumptions around the composition or size of data.

A buffer overflow vulnerability will typically occur when code:

- Is reliant on external data to control its behavior
- Is dependent on data properties that are enforced beyond its immediate scope
- Is so complex that programmers are not able to predict its behavior accurately

Buffer Overflow Exploits

The buffer overflow exploit techniques a hacker uses depends on the architecture and operating system being used by their target. However, the extra data they issue to a program will likely contain malicious code that enables the attacker to trigger additional actions and send new instructions to the application.

For example, introducing additional code into a program could send it new instructions that give the attacker access to the organization's IT systems. In the event that an attacker knows a program's memory layout, they may be able to intentionally input data that cannot be stored by the buffer. This will enable them to overwrite memory locations that store executable code and replace it with malicious code that allows them to take control of the program.

Attackers use a buffer overflow to corrupt a web application's execution stack, execute arbitrary code, and take over a machine. Flaws in buffer overflows can exist in both application servers and web servers, especially web applications that use libraries like graphics libraries. Buffer overflows can also exist in custom web application codes. This is more likely because they are given less scrutiny by security teams but are less likely to be discovered by hackers and more difficult to exploit.

5.What is malware? Explain Types of malwares

Malware is a program designed to gain access to computer systems, normally for the benefit of some third party, without the user's permission. Malware includes computer viruses, worms, Trojan horses, ransomware, spyware and other malicious programs.

Types of Malware:

Viruses –

A Virus is a malicious executable code attached to another executable file. The virus spreads when an infected file is passed from system to system. Viruses can be harmless or they can modify or delete data. Opening a file can trigger a virus. Once a program virus is active, it will infect other programs on the computer.

Worms –

Worms replicate themselves on the system, attaching themselves to different files and looking for pathways between computers, such as computer network that shares common file storage areas. Worms usually slow down networks. A

virus needs a host program to run but worms can run by themselves. After a worm affects a host, it is able to spread very quickly over the network.

spyware –
Its purpose is to steal private information from a computer system for a third party. Spyware collects information and sends it to the hacker.

Trojan horse –
A Trojan horse is malware that carries out malicious operations under the appearance of a desired operation such as playing an online game. A Trojan horse varies from a virus because the Trojan binds itself to non-executable files, such as image files, audio files.

Logic Bombs –
A logic bomb is a malicious program that uses a trigger to activate the malicious code. The logic bomb remains non-functioning until that trigger event happens. Once triggered, a logic bomb implements a malicious code that causes harm to a computer. Cybersecurity specialists recently discovered logic bombs that attack and destroy the hardware components in a workstation or server including the cooling fans, hard drives, and power supplies. The logic bomb overdrives these devices until they overheat or fail.

ransomware –
Ransomware grasps a computer system or the data it contains until the victim makes a payment. Ransomware encrypts data in the computer with a key which is unknown to the user. The user has to pay a ransom (price) to the criminals to retrieve data. Once the amount is paid the victim can resume using his/her system.

Backdoors –
A backdoor bypasses the usual authentication used to access a system. The purpose of the backdoor is to grant the cyber criminals future access to the system even if the organization fixes the original vulnerability used to attack the system.

Rootkits –
A rootkit modifies the OS to make a backdoor. Attackers then use the backdoor to access the computer distantly. Most rootkits take advantage of software vulnerabilities to modify system files.

Keyloggers –
Keylogger records everything the user types on his/her computer system to

obtain passwords and other sensitive information and send them to the source of the keylogging program.

6Define following terms: a. Backdoors b. Spyware c. Proxy server d. Anonymizers e. Cyber defamation

A.backdoors

- A backdoor bypasses the usual authentication used to access a system. The purpose of the backdoor is to grant the cyber criminals future access to the system even if the organization fixes the original vulnerability used to attack the system.

B.Spyware

- Its purpose is to steal private information from a computer system for a third party. Spyware collects information and sends it to the hacker.

c. Proxy server

proxy server is a system or router that provides a gateway between users and the internet. Therefore, it helps prevent cyber attackers from entering a private network. It is a server, referred to as an "intermediary" because it goes between end-users and the web pages they visit online.

7.Write a short note on software piracy.

Software piracy has become a worldwide issue with China, the United States, and India being the top three offenders. The commercial value of pirated software is $19 billion in North America and Western Europe and has reached $27.3 billion in the rest of the world. According to the 2018 Global Software Survey, 37% of software installed on personal computers is unlicensed software.

Software piracy doesn't require a hacker or skilled coder. Any normal person with a computer can become a software pirate if they don't know about the software laws. With such a widespread impact, it's important to understand what software piracy is and the dangers it presents.

Software Piracy – Definition

Software piracy is the act of stealing software that is legally protected. This stealing includes copying, distributing, modifying or selling the software.

Copyright laws were originally put into place so that the people who develop software (programmers, writers, graphic artists, etc.) would get the proper credit and compensation for their work. When software piracy occurs, compensation is stolen from these copyright holders.

Software Piracy Regulation

Computer piracy is illegal and constitutes a federal crime. The monetary penalties for those who break this law can reach up to $150,000 per instance of copyright violation.

End-User License Agreement

The End-User License Agreement (EULA) is a license used for most software. It is a contract between the manufacturer and/or author and the end user. This agreement defines rules for software use and not every agreement is the same. One common rule in most EULAs prohibits users from sharing the software with others.

Types of Software Piracy

There are five main types of software piracy. This variety of pirating techniques explains how some individuals purposely pirate software while others may unknowingly be an accomplice.

Softlifting

Softlifting is when someone purchases one version of the software and downloads it onto multiple computers, even though the software license states it should only be downloaded once. This often occurs in business or school environments and is usually done to save money. Softlifting is the most common type of software piracy.

Client-server overuse

Client-server overuse is when too many people on a network use one main copy of the program at the same time. This often happens when businesses are on a local area network and download the software for all employees to use. This becomes a type of software piracy if the license doesn't entitle you to use it multiple times.

Hard disk loading

Hard disk loading is a type of commercial software piracy in which someone buys a legal version of the software and then reproduces, copies or installs it onto computer hard disks. The person then sells the product. This often happens at PC resale shops and buyers aren't always aware that the additional software they are buying is illegal.

Counterfeiting

Counterfeiting occurs when software programs are illegally duplicated and sold with the appearance of authenticity. Counterfeit software is usually sold at a discounted price in comparison to the legitimate software.

Online Piracy

Online piracy, also known as Internet piracy, is when illegal software is sold, shared or acquired by means of the Internet. This is usually done through a peer-to-peer (P2P) file-sharing system, which is usually found in the form of online auction sites and blogs.

Unit 3

1.What is Email spoofing? How it works and how it is dangerous for user?

- Email spoofing is a technique used in spam and phishing attacks to trick users into thinking a message came from a person or entity they either know or can trust. In spoofing attacks, the sender forges email headers so that client software displays the fraudulent sender address, which most users take at face value. Unless they inspect the header more closely, users see the forged sender in a message. If it's a name they recognize, they're more likely to trust it. So they'll click malicious links, open malware attachments, send sensitive data and even wire corporate funds.
- Email spoofing is possible due to the way email systems are designed. Outgoing messages are assigned a sender address by the client application; outgoing email servers have no way to tell whether the sender address is legitimate or spoofed.
- Recipient servers and antimalware software can help detect and filter spoofed messages. Unfortunately, not every email service has security protocols in place. Still, users can review email headers packaged with every message to determine whether the sender address is forged.

- ### A Brief History of Email Spoofing
- Because of the way email protocols work, email spoofing has been an issue since the 1970s. It started with spammers who used it to get around email filters. The issue became more common in the 1990s, then grew into a global cybersecurity issue in the 2000s.
- Security protocols were introduced in 2014 to help fight email spoofing and phishing. Because of these protocols, many spoofed email messages are now sent to user spamboxes or are rejected and never sent to the recipient's inboxes.

- ### How Email Spoofing Works and Examples
- The goal of email spoofing is to trick users into believing the email is from someone they know or can trust—in most cases, a colleague, vendor or brand. Exploiting that trust, the attacker asks the recipient to divulge information or take some other action.
- As an example of email spoofing, an attacker might create an email that looks like it comes from PayPal. The message tells the user that their account will be suspended if they don't click a link, authenticate into the site and change the account's password. If the user is successfully tricked and types in credentials, the attacker now has credentials to authenticate into the targeted user's PayPal account, potentially stealing money from the user.
- More complex attacks target financial employees and use social engineering and online reconnaissance to trick a targeted user into sending millions to an attacker's bank account.
- To the user, a spoofed email message looks legitimate, and many attackers will take elements from the official website to make the message more believable.

2. Define following terms: a. Salami attack b. Data diddling c. Email bombing

a.salami attack

A salami attack is a type of cybercrime that attackers typically use to commit financial crimes. Criminals steal money or resources from financial accounts on a system one at a time. This attack occurs when several minor attacks combine to form a powerful attack.

Data diddling

Data diddling is the act of extracting and changing the value of data without the knowledge of the owner is a crime. A data diddling (also called false data entry) simply means altering data before entering it or during entering to the computer system. Data diddling can also occur when data is altered just before it is processed by a computer system and this same data can be modified back after processing the fake data that was entered. This form of cybercrime usually occurs within the organization providing customer services i.e. electricity organization, medical organization, transport organization, etc. where customer bills, personal information or order of valuable and important records are manipulated.

Email bombing

Email bombing means sending a large number of emails to the victim's email id with the intention to crash the victim's email account or email server. The mail Bombing idea is usually conducted by Black Hat Hackers who send a large number of emails consciously in order to discontinue the usage of the targeted email addresses. There are several open-source computer hacking tools designed for email bombing, cybercriminals who use them can instruct any of these programs to continuously and repeatedly send a single email to a targeted victim's email address in order to overwhelm the email account through the email address and this may also cause an entire server to shut down.

3. What is forgery. List out all the documents which can be forged and explain it by an example.

Forgery is committed when: **a person signs in another's name with the intent to defraud**; a person alters the name, amount or payee's name with intent to defraud. Although a crime of forgery is committed, only the forged signature is considered invalid.

Simple Forgery: Simple forgery is just as it sounds. It is very basic and is done with very little effort. Someone will write something or sign a document with no attempt to follow a known sample of the handwriting or signature. The person will then try to pass off the handwriting or the signature as the original copy of someone else's original document.

Free Hand Simulation: Forgery that is a free hand simulation is just a little more advanced than a simple forgery. When a person attempts free hand simulation, they have a sample of the handwriting or signature to look at. A forger will then try to recreate the shapes and styling of handwriting and signatures.

Tracing: When a signature is copied by using tracing methods, a person will attempt to reproduce the most obvious or prominent features of a signature or handwritten text. Many times traced signatures and writing can be matched exactly to the original signature or text. By using various methods such as light tables I can compare text and find evidence of document forgery by tracing.

Electronic Manipulation: In the digital age we live in, document forgery through electronic manipulation is becoming more common. People will use programs such as Photoshop to copy and alter the text in digital documents and with digitally scanned documents. With electronic manipulation, the possibilities are endless for document forgery.

Signs of Forgery

Slow and methodical strokes are one of the most common signs of forgery. When people are writing in their own style with their own handwriting, the writing is done fast. You make mistakes when writing and don't always correct them. When a person is copying a style of writing or a signature, they usually do so in a slow and methodical way, trying to get everything

just right. Writing in this way create very even strokes with little to no mistakes seen in the way they write.

No variation in pen pressure is also one of the most common signs of forgery in a document. When you write, you write quickly. Because you are writing quickly with little thought to it, pen pressure will vary. You will notice hard and thick lines as well as light and thin lines in your text as you write. If someone tries to copy your writing or signature, they will form the characters more carefully, creating even lines with no variation in pen pressure.

An unnatural tremor can be an indicator of document forgery. Tremors can happen because someone was nervous when they were writing. When I compare original handwriting to forged handwriting, you can spot a difference when there is an unnatural tremor caused by stress, fear, a medical condition, or other factors.

Substituted pages are forgeries found in multi-page documents. A forger may take a page out and try to change text or signatures on the page and then replace the whole page in the document. Substituted pages can be revealed by looking at certain characteristics of the pages throughout the document. I can compare features such as paper thickness and the type of paper used.

5. Describe DOS and DDOS attack with suitable example.

1. DOS Attack is a denial of service attack, in this attack a computer sends a massive amount of traffic to a victim's computer and shuts it down. Dos attack is an online attack that is used to make the website unavailable for its users when done on a website. This attack makes the server of a website that is connected to the internet by sending a large number of traffic to it.

2. DDOS Attack means distributed denial of service in this attack dos attacks are done from many different locations using many systems.

Difference between DOS and DDOS attacks:

DOS	DDOS
DOS Stands for Denial of service attack.	DDOS Stands for Distributed Denial of service attack.
In Dos attack single system targets the victim system.	In DDoS multiple systems attacks the victims system..

DOS	DDOS
Victim PC is loaded from the packet of data sent from a single location.	Victim PC is loaded from the packet of data sent from Multiple location.
Dos attack is slower as compared to DDoS.	DDoS attack is faster than Dos Attack.
Can be blocked easily as only one system is used.	It is difficult to block this attack as multiple devices are sending packets and attacking from multiple locations.
In DOS Attack only single device is used with DOS Attack tools.	In DDoS attack,The volumeBots are used to attack at the same time.
DOS Attacks are Easy to trace.	DDOS Attacks are Difficult to trace.
Volume of traffic in the Dos attack is less as compared to DDos.	DDoS attacks allow the attacker to send massive volumes of traffic to the victim network.
Types of DOS Attacks are: 1. Buffer overflow attacks 2. Ping of Death or ICMP flood 3. Teardrop Attack 4. Flooding Attack	Types of DDOS Attacks are: 1. Volumetric Attacks 2. Fragmentation Attacks 3. Application Layer Attacks 4. Protocol Attack.

6.How can we prevent DDOS attack?

DDoS Protection Techniques

Reduce Attack Surface Area

One of the first techniques to mitigate DDoS attacks is to minimize the surface area that can be attacked thereby limiting the options for attackers and allowing you to build protections in a single place. We want to ensure that we do not expose our application or resources to ports, protocols or applications

from where they do not expect any communication. Thus, minimizing the possible points of attack and letting us concentrate our mitigation efforts. In some cases, you can do this by placing your computation resources behind Content Distribution Networks (CDNs) or Load Balancers and restricting direct Internet traffic to certain parts of your infrastructure like your database servers. In other cases, you can use firewalls or Access Control Lists (ACLs) to control what traffic reaches your applications.

Plan for Scale

The two key considerations for mitigating large scale volumetric DDoS attacks are bandwidth (or transit) capacity and server capacity to absorb and mitigate attacks.

Transit capacity. When architecting your applications, make sure your hosting provider provides ample redundant Internet connectivity that allows you to handle large volumes of traffic. Since the ultimate objective of DDoS attacks is to affect the availability of your resources/applications, you should locate them, not only close to your end users but also to large Internet exchanges which will give your users easy access to your application even during high volumes of traffic. Additionally, web applications can go a step further by employing Content Distribution Networks (CDNs) and smart DNS resolution services which provide an additional layer of network infrastructure for serving content and resolving DNS queries from locations that are often closer to your end users.

Server capacity. Most DDoS attacks are volumetric attacks that use up a lot of resources; it is, therefore, important that you can quickly scale up or down on your computation resources. You can either do this by running on larger computation resources or those with features like more extensive network interfaces or enhanced networking that support larger volumes. Additionally, it is also common to use load balancers to continually monitor and shift loads between resources to prevent overloading any one resource.

henever we detect elevated levels of traffic hitting a host, the very baseline is to be able only to accept as much traffic as our host can handle without

affecting availability. This concept is called rate limiting. More advanced protection techniques can go one step further and intelligently only accept traffic that is legitimate by analyzing the individual packets themselves. To do this, you need to understand the characteristics of good traffic that the target usually receives and be able to compare each packet against this baseline.

Deploy Firewalls for Sophisticated Application attacks

A good practice is to use a Web Application Firewall (WAF) against attacks, such as SQL injection or cross-site request forgery, that attempt to exploit a vulnerability in your application itself. Additionally, due to the unique nature of these attacks, you should be able to easily create customized mitigations against illegitimate requests which could have characteristics like disguising as good traffic or coming from bad IPs, unexpected geographies, etc. At times it might also be helpful in mitigating attacks as they happen to get experienced support to study traffic patterns and create customized protections.

7 What is SQL injection?

SQL Injection

SQL injection is a code injection technique that might destroy your database.

SQL injection is one of the most common web hacking techniques.

SQL injection is the placement of malicious code in SQL statements, via web page input.

SQL in Web Pages

SQL injection usually occurs when you ask a user for input, like their username/userid, and instead of a name/id, the user gives you an SQL statement that you will **unknowingly** run on your database.

Look at the following example which creates a `SELECT` statement by adding a variable (txtUserId) to a select string. The variable is fetched from user input (getRequestString):

Example

```
txtUserId = getRequestString("UserId");
txtSQL = "SELECT * FROM Users WHERE UserId = " + txtUserId;
```

8.What is botnet? Why is it required?

botnets have become one of the biggest threats to security systems today. Their growing popularity among cybercriminals comes from their ability to infiltrate almost any internet-connected device, from DVR players to corporate mainframes.

- Botnets are also becoming a larger part of cultural discussions around cyber security. Facebook's fake ad controversy and the Twitter bot fiasco during the 2016 presidential election worry many politicians and citizens about the disruptive potential of botnets. Recently published studies from MIT have concluded that social media bots and automated accounts play a major role in spreading fake news.
- The use of botnets to mine cryptocurrencies like Bitcoin is a growing business for cyber criminals. It's predicted the trend will continue, resulting in more computers infected with mining software and more digital wallets stolen.
- Aside from being tools for influencing elections and mining cryptocurrencies, botnets are also dangerous to corporations and consumers because they're used to deploy malware, initiate attacks on websites, steal personal information, and defraud advertisers.
- It's clear botnets are bad, but what are they exactly? And how can you protect your personal information and devices? Step one is understanding how bots work. Step two is taking preventative actions.

- **How Do Botnets Work?**
- To better understand how botnets function, consider that the name itself is a blending of the words "robot" and "network". In a broad sense, that's exactly what botnets are: a network of robots used to commit cyber crime. The cyber criminals controlling them are called botmasters or bot herders.
- **Size Matters**
- To build a botnet, botmasters need as many infected online devices or "bots" under their command as possible. The more bots connected, the bigger the botnet. The bigger the botnet, the bigger the impact. So size matters. The

criminal's ultimate goal is often financial gain, malware propagation, or just general disruption of the internet.

- Imagine the following: You've enlisted ten of your friends to call the Department of Motor Vehicles at the same time on the same day. Aside from the deafening sounds of ringing phones and the scurrying of State employees, not much else would happen. Now, imagine you wrangled 100 of your friends, to do the same thing. The simultaneous influx of such a large number of signals, pings, and requests would overload the DMV's phone system, likely shutting it down completely.
- Cybercriminals use botnets to create a similar disruption on the internet. They command their infected bot army to overload a website to the point that it stops functioning and/or access is denied. Such an attack is called a denial of service or DDoS.

Botnet Infections

- Botnets aren't typically created to compromise just one individual computer; they're designed to infect millions of devices. Bot herders often deploy botnets onto computers through a trojan horse virus. The strategy typically requires users to infect their own systems by opening email attachments, clicking on malicious pop up ads, or downloading dangerous software from a website. After infecting devices, botnets are then free to access and modify personal information, attack other computers, and commit other crimes.
- More complex botnets can even self-propagate, finding and infecting devices automatically. Such autonomous bots carry out seek-and-infect missions, constantly searching the web for vulnerable internet-connected devices lacking operating system updates or antivirus software.
- Botnets are difficult to detect. They use only small amounts of computing power to avoid disrupting normal device functions and alerting the user. More advanced botnets are even designed to update their behavior so as to thwart detection by cybersecurity software. Users are unaware they're connected device is being controlled by cyber criminals. What's worse, botnet design continues to evolve, making newer versions harder to find.
- Botnets take time to grow. Many will lay dormant within devices waiting for the botmaster to call them to action for a DDoS attack or for spam dissemination.

Vulnerable Devices

- Botnets can infect almost any device connected directly or wirelessly to the internet. PCs, laptops, mobile devices, DVR's, smartwatches, security cameras, and smart kitchen appliances can all fall within the web of a botnet.
- Although it seems absurd to think of a refrigerator or coffee maker becoming the unwitting participant in a cyber crime, it happens more often than most people realize. Often appliance manufacturers use unsecure passwords to guard entry into their devices, making them easy for autonomous bots scouring the internet to find and exploit.
- As the never-ending growth of the Internet of Things brings more devices online, cyber criminals have greater opportunities to grow their botnets, and with it, the level of impact.

- In 2016, a large DDoS attack hit the internet infrastructure company Dyn. The attack used a botnet comprised of security cameras and DVRs. The DDoS disrupted internet service for large sections of the country, creating problems for many popular websites like Twitter and Amazon.

9. Explain botnet architecture

Botnet Architecture

Two distinct architectures characterize most botnets.

The “classic” botnet infrastructure is based on a client-server approach, which involves a Control and Command server that has centralized control over the bots. The C&C server sends automated commands throughout the botnet using a common communications protocol, usually IRC or HTTP. Using this type of communication, the botmaster can create dedicated channels between the bots and the C&C, as well as subgroup communications throughout the bot army. Botnets featuring client-server architecture are easier to set up, boast a well-known infrastructure with many guides and models to learn from, and allow the botmaster to directly communicate with all bots in a simple two-way session. On the other hand, this architecture is dependent on centralized C&C servers, which make the botnet easier to take down once discovered. Furthermore, the protocols used to form two-way communication create more traffic, making the exploitation of victim devices easier to detect.

A more modern approach to botnets completely retires the use of C&C servers, using a decentralized peer-to-peer (P2P) architecture instead. In this model, each bot serves as both client and server. This way, the bots are able to relay information between different devices in the network. While a botnet’s C&C server must possess a list of all the bots in its network, in a P2P model, each peer only possesses a list of its neighboring peers. Using this architecture, botnet traffic is harder to distinguish from legitimate traffic, the bots are harder to find, and the networks are harder to take down as there is no centralized power in the network.

Unit 4

1. What is digital forensic?

- Digital forensic science is a branch of forensic science that focuses on the recovery and investigation of material found in digital devices related to cybercrime. The term digital forensics was first used as a synonym for computer forensics. Since then, it has expanded to cover the investigation of any devices that can store digital data. Although the first computer crime was reported in 1978, followed by the Florida computers act, it wasn't until the 1990s that it became a recognized term. It was only in the early 21st century that national policies on digital forensics emerged.
- Digital forensics is the process of identifying, preserving, analyzing, and documenting digital evidence. This is done in order to present evidence in a court of law when required.

> - *"Digital forensics is the process of uncovering and interpreting electronic data. The goal of the process is to preserve any evidence in its most original form while performing a structured investigation by collecting, identifying, and validating the digital information to reconstruct past events.*

2. Explain phases of digital forensic.

Digital Forensics is defined as the process of preservation, identification, extraction, and documentation of computer evidence which can be used by the court of law. It is a science of finding evidence from digital media like a computer, mobile phone, server, or network. It provides the forensic team with the best techniques and tools to solve complicated digital-related cases.

Identification

It is the first step in the forensic process. The identification process mainly includes things like what evidence is present, where it is stored, and lastly, how it is stored (in which format).

Electronic storage media can be personal computers, Mobile phones, PDAs, etc.

Preservation

In this phase, data is isolated, secured, and preserved. It includes preventing people from using the digital device so that digital evidence is not tampered with.

Analysis

In this step, investigation agents reconstruct fragments of data and draw conclusions based on evidence found. However, it might take numerous iterations of examination to support a specific crime theory.

Documentation

In this process, a record of all the visible data must be created. It helps in recreating the crime scene and reviewing it. It Involves proper documentation of the crime scene along with photographing, sketching, and crime-scene mapping.

Presentation

In this last step, the process of summarization and explanation of conclusions is done.

However, it should be written in a layperson’s terms using abstracted terminologies. All abstracted terminologies should reference the specific details.

3.Explain the need of Digital Forensics.

digital forensics is the process of extracting and analyzing data contained within digital systems to find evidence that can help resolve cyberattacks, disputes, litigation, and criminal cases. Using methods of

electronic discovery, trained computer forensic analysts examine computers, cell phones, hard drives, networks, systems, and digital components for digital forensics investigative purposes.

Digital forensics is often a critical component of criminal cases, civil fraud cases, whistleblower complaints, internal investigations, and other matters that require analysis to understand when, how, and who used technology to perpetrate misdeeds.

Digital forensic investigations can unearth a great deal of information after cyberattacks, including:

- Identifying the cause and implications of cyberattacks
- Containing and remediating attacks
- Safeguarding digital evidence before it becomes obsolete
- Retracing hacker steps, and finding hacker tools
- Identifying whether data was accessed or exfiltrated
- Identifying the duration of unauthorized access to the network
- Geolocating the hacker logins and mapping them

When Can Digital Forensic Investigations Help?

Examples of common scenarios where digital forensics investigations might be needed include:

Accidental or deliberate company data disclosure

When corporate information is disclosed without permission, either by accident or by design.

Intellectual property theft

When an employee steals intellectual property from an employer and passes it to a competitor or uses it to set up a competing company.

Employee internet abuse or misuse

When an employee violates a computer policy, such as Internet use. If the systems in the office are used for any illegal activity, computer forensics can help determine when and how these illegalities happened.

Incident or breach investigations

When a cyberattack occurs, digital forensics can help identify exactly what happened and attempt to identify who or what was responsible, whether that's for prosecution or just internal knowledge.

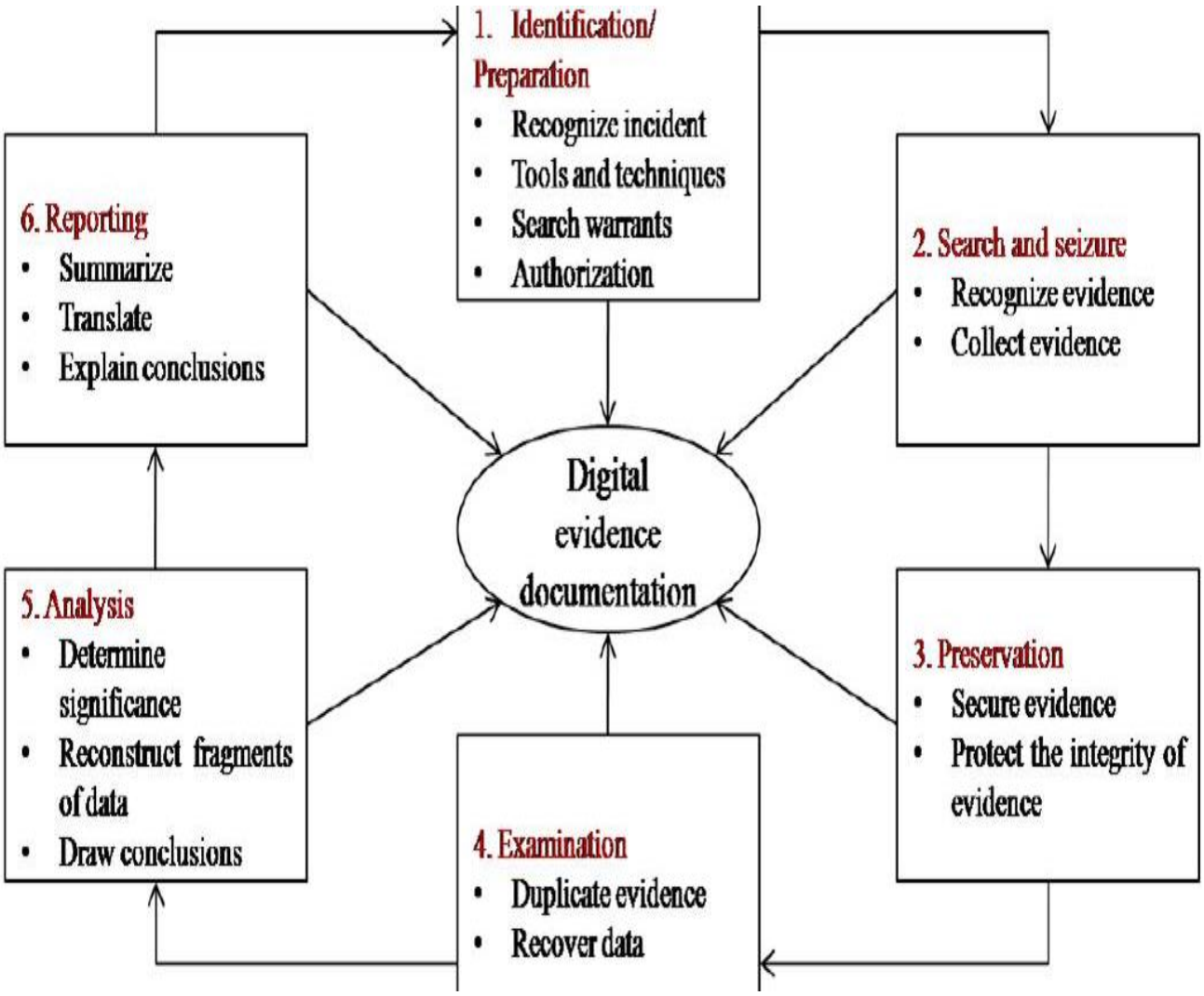
White-collar crimes

When insiders or scamsters commit financially motivated crimes, such as identity theft, Ponzi schemes, embezzlement, and other fraud schemes.

4.Explain digital forensic life cycle.

he digital forensics process is shown in the following figure. Forensic life cycle phases are:

1. Preparation and identification
2. Collection and recording
3. Storing and transporting
4. Examination/investigation
5. Analysis, interpretation, and attribution
6. Reporting
7. Testifying



1.Identifying the Evidence

In order to be processed and analysed, evidence must first be identified. It might be possible that the evidence may be overlooked and not identified at all. A sequence of events in a computer might include interactions between:

- Different files
- Files and file systems
- Processes and files
- Log files

In case of a network, the interactions can be between devices in the organization or across the globe (Internet). If the evidence is never identified as relevant, it may never be collected and processed.

2. Collecting and Recording Digital Evidence

Digital evidence can be collected from many sources. The obvious sources can be:

- Mobile phone
- Digital cameras
- Hard drives
- CDs
- USB memory devices

Non-obvious sources can be:

- Digital thermometer settings
- Black boxes inside automobiles
- RFID tags

Proper care should be taken while handling digital evidence as it can be changed easily. Once changed, the evidence cannot be analysed further. A cryptographic hash can be calculated for the evidence file and later checked if there were any changes made to the file or not. Sometimes important evidence might reside in the volatile memory. Gathering volatile data requires special technical skills.

3. Storing and Transporting Digital Evidence

Some guidelines for handling of digital evidence:

- Image computer-media using a write-blocking tool to ensure that no data is added to the suspect device

- Establish and maintain the chain of custody
- Document everything that has been done
- Only use tools and methods that have been tested and evaluated to validate their accuracy and reliability

Care should be taken that evidence does not go anywhere without properly being traced. Things that can go wrong in storage include:

- Decay over time (natural or unnatural)
- Environmental changes (direct or indirect)
- Fires
- Floods
- Loss of power to batteries and other media preserving mechanisms

Sometimes evidence must be transported from place to place either physically or through a network. Care should be taken that the evidence is not changed while in transit. Analysis is generally done on the copy of real evidence. If there is any dispute over the copy, the real can be produced in court.

4. Examining/Investigating Digital Evidence

Forensics specialist should ensure that he/she has proper legal authority to seize, copy and examine the data. As a general rule, one should not examine digital information unless one has the legal authority to do so. Forensic investigation performed on data at rest (hard disk) is called dead analysis.

Many current attacks leave no trace on the computer's hard drive. The attacker only exploits the information in the computer's main memory. Performing forensic investigation on main memory is called live analysis. Sometimes the decryption key might be available only in RAM. Turning off the system will erase the decryption key. The process of creating and exact duplicate of the original evidence is called imaging. Some tools which can create entire hard drive images are:

- DCFLdd
- Iximager
- Guymager

The original drive is moved to secure storage to prevent tampering. The imaging process is verified by using the SHA-1 or any other hashing algorithms.

5. Analysis, Interpretation and Attribution

In digital forensics, only a few sequences of events might produce evidence. But the possible number of sequences is very huge. The digital evidence must be analyzed to determine the type of information stored on it. Examples of forensics tools:

- Forensics Tool Kit (FTK)
- EnCase
- Scalpel (file carving tool)
- The Sleuth Kit (TSK)
- Autopsy

Forensic analysis includes the following activities:

- Manual review of data on the media
- Windows registry inspection
- Discovering and cracking passwords
- Performing keyword searches related to crime
- Extracting emails and images

Types of digital analysis:

- Media analysis
- Media management analysis
- File system analysis
- Application analysis
- Network analysis
- Image analysis
- Video analysis

6. Reporting

After the analysis is done, a report is generated. The report may be in oral form or in written form or both. The report contains all the details about the evidence in analysis, interpretation, and attribution steps. As a result of the findings in this phase, it should be possible to confirm or discard the allegations. Some of the general elements in the report are:

- Identity of the report agency
- Case identifier or submission number
- Case investigator
- Identity of the submitter
- Date of receipt
- Date of report
- Descriptive list of items submitted for examination
- Identity and signature of the examiner
- Brief description of steps taken during examination
- Results / conclusions

7. Testifying

This phase involves presentation and cross-examination of expert witnesses. An expert witness can testify in the form of:

- Testimony is based on sufficient facts or data
- Testimony is the product of reliable principles and methods
- Witness has applied principles and methods reliably to the facts of the case

Experts with inadequate knowledge are sometimes chastised by the court. Precautions to be taken when collecting digital evidence are:

- No action taken by law enforcement agencies or their agents should change the evidence
- When a person to access the original data held on a computer, the person must be competent to do so
- An audit trial or other record of all processes applied to digital evidence should be created and preserved
- The person in-charge of the investigation has overall responsibility for ensuring that the law and these are adhered to

5.What are cyber laws? Why we need it?

- Cyber law, also known as Internet Law or Cyber Law, is the part of the overall legal system thet is related to legal informatics and supervises the digital circulation of information, e-commerce, software and information security. It is associated with legal informatics and electronic elements, including information systems, computers, software, and hardware. It covers many areas, such as access to and usage of the Internet, encompassing various subtopics as well as freedom of expression, and online privacy.

- Cyber laws help to reduce or prevent people from cybercriminal activities on a large scale with the help of protecting information access from unauthorized people, freedom of speech related to the use of the Internet
- , privacy, communications, email, websites, intellectual property, hardware and software, such as data storage devices. As Internet traffic is increasing rapidly day by day, that has led to a higher percentage of legal issues worldwide. Because cyber laws are different according to the country and jurisdiction, restitution ranges from fines to imprisonment, and enforcement is challenging.
- Cyberlaw offers legal protections for people who are using the Internet as well as running an online business. It is most important for Internet users to know about the local area and cyber law of their country by which they could know what activities are legal or not on the network. Also, they can prevent ourselves from unauthorized activities.
- The Computer Fraud and Abuse Act was the first cyber law, called CFFA, that was enacted in 1986. This law was helpful in preventing unauthorized access to computers. And it also provided a description of the stages of punishment for breaking that law or performing any illegal activity.

• Why are cyber laws needed?

- There are many security issues with using the Internet and also available different malicious people who try to unauthorized access your computer system to perform potential fraud. Therefore, similarly, any law, cyber law is created to protect online organizations and people on the network from unauthorized access and malicious people. If someone does any illegal activity or breaks the cyber rule, it offers people or organizations to have that persons sentenced to punishment or take action against them.

6.Illustrate the aim and objective of Indian IT ACT 2000.

Information Technology Act, 2000

In 1996, the United Nations Commission on International Trade Law (UNCITRAL) adopted the model law on electronic commerce (e-commerce) to bring uniformity in the law in different countries.

Further, the General Assembly of the United Nations recommended that all countries must consider this model law before making changes to their own laws. India became the 12th country to enable cyber law after it passed the Information Technology Act, 2000.

While the first draft was created by the Ministry of Commerce, Government of India as the ECommerce Act, 1998, it was redrafted as the 'Information Technology Bill, 1999', and passed in May 2000.

Objectives of the Act

The Information Technology Act, 2000 provides legal recognition to the transaction done via electronic exchange of data and other electronic means of communication or electronic commerce transactions.

This also involves the use of alternatives to a paper-based method of communication and information storage to facilitate the electronic filing of documents with the Government agencies.

Further, this act amended the Indian Penal Code 1860, the Indian Evidence Act 1872, the Bankers' Books Evidence Act 1891, and

the Reserve Bank of India Act 1934. The objectives of the Act are as follows:

i. Grant legal recognition to all transactions done via electronic exchange of data or other electronic means of communication or e-commerce, in place of the earlier paper-based method of communication.

ii. Give legal recognition to digital signatures for the authentication of any information or matters requiring legal authentication

iii. Facilitate the electronic filing of documents with Government agencies and also departments

iv. Facilitate the electronic storage of data

v. Give legal sanction and also facilitate the electronic transfer of funds between banks and financial institutions

vi. Grant legal recognition to bankers under the Evidence Act, 1891 and the Reserve Bank of India Act, 1934, for keeping the books of accounts in electronic form.

Unit:5

1. What is Packet Filter Vs Firewall?

Firewall

- A firewall is a computer connected to both a private (protected) network and a public (unprotected) network, which receives and resubmits specific kinds of network requests on behalf of network clients on either the private or public network.
- Firewalls involve proxies. A proxy acts as a middle-man in a network transaction.

- Rather than allowing a client to speak directly to a server, the proxy server receives the request from the client, and then resubmits the request, on behalf of the client, to the target server.
- Each protocol or type of network transaction typically requires its own proxy program, and an administrator enables or installs specific proxies to determine what kinds of services will be allowed between the two networks.
- Firewalls are not routers or address translators.
- The internal network uses private address space. Neither side of the firewall knows about the address space on the other side of the firewall, and does not know how to route data to the other side of the firewall.

Packet Filters

- A packet filter is a set of rules, applied to a stream of data packets, which is used to decide whether to permit or deny the forwarding of each packet.
- These rules are usually on a router or in the routing layer of a computer's network protocol stack.
- Using a packet filter, an administrator can dictate what types of packets are allowed into or out of a network or computer.
- Prevents the outside network from having knowledge of the address space on the protected network.
- However, aside from translating the addresses of the internal network, packets are forwarded as received through the unit, and no proxies are involved.
- Any good firewall will also employ packet filtering.
- This is done to protect the firewall itself from intrusion and to isolate intruders from the internal network.

2. Difference between Stateless Vs Stateful Firewalls.

- **Stateful** firewalls monitor all aspects of the traffic streams, their characteristics and communication channels. These firewalls can integrate encryption or tunnels, identify TCP connection stages, packet state and other key status updates.
- **Stateless** Protocols are the type of network protocols in which Client send request to the server and server response back according to current state.

It does not require the server to retain session information or a status about each communicating partner for multiple request.

- **Differences between Stateless and Stateful firewalls :**

	Stateless Packet Filtering Firewalls	Stateful Packet Filtering Firewalls
1.	The stateless firewalls are designed to protect networks based on static information such as source and destination.	Stateful firewalls filter packets based on the full context of the connection.
2.	It uses some predefined packet filtering rules, the packets are judged based on that, if it conforms to the predefined rules then it is considered to be "safe" and allowed to pass through. If the conditions are not met, the packet is considered to be "unidentified" or "malicious" and it will be blocked.	It uses the concept of a state table where it stores the state of legitimate connections. Stateless firewall filters are only based on header information in a packet but stateful firewall filter inspects everything inside data packets, the characteristics of the data, and its channels of communication.
3.	Less secure than stateless firewalls.	Stateful firewalls are more secure.
4.	Cheaper or cost-efficient.	Expensive as compared to stateless firewall
5.	Faster than Stateful packet filtering firewall.	Slower in speed when compared to Stateless firewall.
6.	For small businesses, a stateless firewall could be a better option, as they face fewer threats and also have a limited budget in hand.	For larger enterprises, a stateful firewall would be a smarter option, as they have larger outgoing traffic that needs monitoring and enough money to afford it. Stateful firewalls offer dynamic packet filtering, so they can provide a thick security layer to mitigate attacks.

- **Note:** A firewall can be either stateful or stateless but never both.

3. Discuss advantages and disadvantages of NAT.

It is a process that is used for converting a single IP address space into a global one. This works with a router or firewall that interconnects two networks. We can connect many network address translations into an intranet with the help of a single public address. This method is mainly introduced to prevent address space exhaustion.

Many organizations used to have NAT as they want to have multiple devices to use a single IP address. In networking systems, it doubles the security of its features and addresses translation. In some cases, it will be useful for us and in some they don't.

Benefits :

Some of the benefits are:

- It allows you to rescue the private IP address.
- It has got good security features that enhance the security of private networks by separating the internal network from the external network.
- It helps to conserve the IP address space. You can connect a large number of hosts using a small IP address to the global internet.

Advantages :

1. **Lowers the cost –**
   When any organization uses NAT with their private IP address, they don't need to buy a new IP address for all the computers they have in their organization. They can use the same IP address for multiple computers out there. This will help to reduce the cost of the organization.

2. **Conserving Address –**
   When you use NAT overload, it will allow you to preserve the IPv4 address space which will give access to all the privatization of intranets. Here, it can be done with the help of Intranet Privatization. In this process, they used to save all the addresses at the port level in multiple applications.

3. **Connection Flexibility –**
   NAT has multiple tools, load balancing tools, and backup tools. These tools will help to increase the overall reliability and flexibility of the network. It will happen when we establish any connection either in the public or any of their connections.

4. **Consistency in the Network –**
   It has a scheme called consistent network addressing. It has a proper address space assigned for the use of public IP addresses. This happens because when we enlarge the network, then more IP addresses will be required.

5. **Network Security –**
   In-Network Address Translation all your original source and destination sources will be hidden by them completely. Without the user's permission, so that the hosts inside them will not be reached by other hosts in the network. This proves that they have got additional security.

6. **Private Addressing –**
   They have a private IPv4 addressing system that is owned by them. So, if you move to another addressing system, they will still have their own addressing system. If the user changes the internet service provider, it will prevent the internal address changes in them.

Disadvantages :

1. **Issues in the Performance –**
   For example, if a guest makes a request to the remote server, it will first check and confirm whether the connection belongs to the NAT server or not. Also, some hosts used to perform security mechanisms for the number of requests that can be accepted. If the number exceeds, they cannot make any further requests. In real-time protocols, this will create performance degradation.

2. **Application Use –**
   Sometimes hosts inside the network might be unreachable. Because of this, some applications in the NAT will have compatibility issues. This will depend on end-to-end functionality which some networks will fail to supply them.

3. **Usage of Protocols –**
   The values inside the headers can be changed in NAT, some of the tunneling protocols such as IPsec will be very complicated to use. When you modify the values inside the headers, then integrity checks will occur, which will interfere and fail them.

4. **Service Use –**
   When you use NAT, services such as TCP or UDP will be required. These services will be affected while using which makes them unstable. Also, incoming packets will have some issues while they try to reach their destination. We can stop this issue by configuring them with the NAT router.

5. **Usage of Memory –**
   NAT will examine the data packets of the incoming and outgoing services. They will convert the data packets into local and global IP addresses as well. Inside the memory, the translation details will get stored. This in turn will consume lots of memory as well as processor.

6. **Troubleshooting Issues –**
   When you use NAT, the end-to-end traceability will be reduced. Also, the IP address will be constantly changed multiple times. This in turn will make troubleshooting more difficult. In some cases, it will be more impossible especially when you are in remote locations.

4. Explain in detail: Network Address Translation (NAT) with suitable diagram.

To access the Internet, one public IP address is needed, but we can use a private IP address in our private network. The idea of NAT is to allow multiple devices to access the Internet through a single public address. To achieve this, the translation of a private IP address to a public IP address is required. **Network Address Translation (NAT)** is a process in which one or more local IP address is translated into one or more Global IP address and vice versa in order to provide Internet access to the local hosts. Also, it does the translation of port numbers i.e. masks the port number of the host with another port number, in the packet that will be routed to the destination. It then makes the corresponding entries of IP address and port number in the NAT table. NAT generally operates on a router or firewall.

Network Address Translation (NAT) working –

Generally, the border router is configured for NAT i.e the router which has one interface in the local (inside) network and one interface in the global (outside) network. When a packet traverse outside the local (inside) network, then NAT converts that local (private) IP address to a global (public) IP address. When a packet enters the local network, the global (public) IP address is converted to a local (private) IP address.

If NAT runs out of addresses, i.e., no address is left in the pool configured then the packets will be dropped and an Internet Control Message Protocol (ICMP) host unreachable packet to the destination is sent.

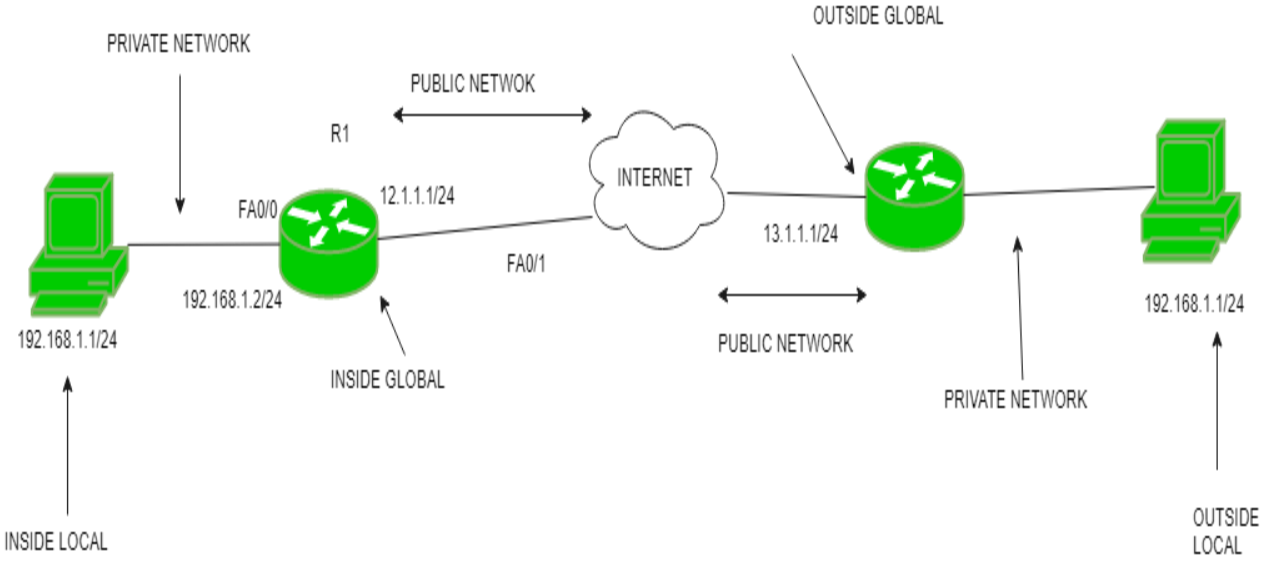
Why mask port numbers ?

Suppose, in a network, two hosts A and B are connected. Now, both of them request for the same destination, on the same port number, say 1000, on the host side, at the same time. If NAT does only translation of IP addresses, then when their packets will arrive at the NAT, both of their IP addresses would be masked by the public IP address of the network and sent to the destination. Destination will send replies to the public IP address of the router. Thus, on receiving a reply, it will be unclear to NAT as to which reply belongs to which host (because source port numbers for both A and B are the same). Hence, to

avoid such a problem, NAT masks the source port number as well and makes an entry in the NAT table.

NAT inside and outside addresses –

Inside refers to the addresses which must be translated. Outside refers to the addresses which are not in control of an organization. These are the network Addresses in which the translation of the addresses will be done.



- **Inside local address –** An IP address that is assigned to a host on the Inside (local) network. The address is probably not an IP address assigned by the service provider i.e., these are private IP addresses. This is the inside host seen from the inside network.

- **Inside global address –** IP address that represents one or more inside local IP addresses to the outside world. This is the inside host as seen from the outside network.

- **Outside local address –** This is the actual IP address of the destination host in the local network after translation.

- **Outside global address –** This is the outside host as seen from the outside network. It is the IP address of the outside destination host before translation.

Network Address Translation (NAT) Types –

There are 3 ways to configure NAT:

1. **Static NAT –** In this, a single unregistered (Private) IP address is mapped with a legally registered (Public) IP address i.e one-to-one mapping between local and global addresses. This is generally used for Web hosting. These

are not used in organizations as there are many devices that will need Internet access and to provide Internet access, a public IP address is needed.
Suppose, if there are 3000 devices that need access to the Internet, the organization has to buy 3000 public addresses that will be very costly.

2. **Dynamic NAT –** In this type of NAT, an unregistered IP address is translated into a registered (Public) IP address from a pool of public IP addresses. If the IP address of the pool is not free, then the packet will be dropped as only a fixed number of private IP addresses can be translated to public addresses.
   Suppose, if there is a pool of 2 public IP addresses then only 2 private IP addresses can be translated at a given time. If 3rd private IP address wants to access the Internet then the packet will be dropped therefore many private IP addresses are mapped to a pool of public IP addresses. NAT is used when the number of users who want to access the Internet is fixed. This is also very costly as the organization has to buy many global IP addresses to make a pool.

3. **Port Address Translation (PAT) –** This is also known as NAT overload. In this, many local (private) IP addresses can be translated to a single registered IP address. Port numbers are used to distinguish the traffic i.e., which traffic belongs to which IP address. This is most frequently used as it is cost-effective as thousands of users can be connected to the Internet by using only one real global (public) IP address.

Advantages of NAT –

- NAT conserves legally registered IP addresses.
- It provides privacy as the device's IP address, sending and receiving the traffic, will be hidden.
- Eliminates address renumbering when a network evolves.

Disadvantage of NAT –

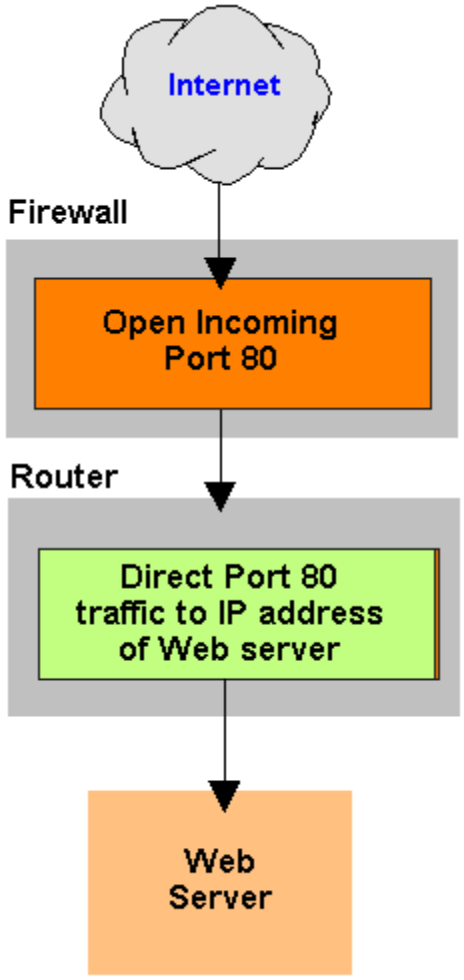
- Translation results in switching path delays.
- Certain applications will not function while NAT is enabled.

- Complicates tunneling protocols such as IPsec.
- Also, the router being a network layer device, should not tamper with port numbers(transport layer) but it has to do so because of NAT.

5.What is Port Forwarding?

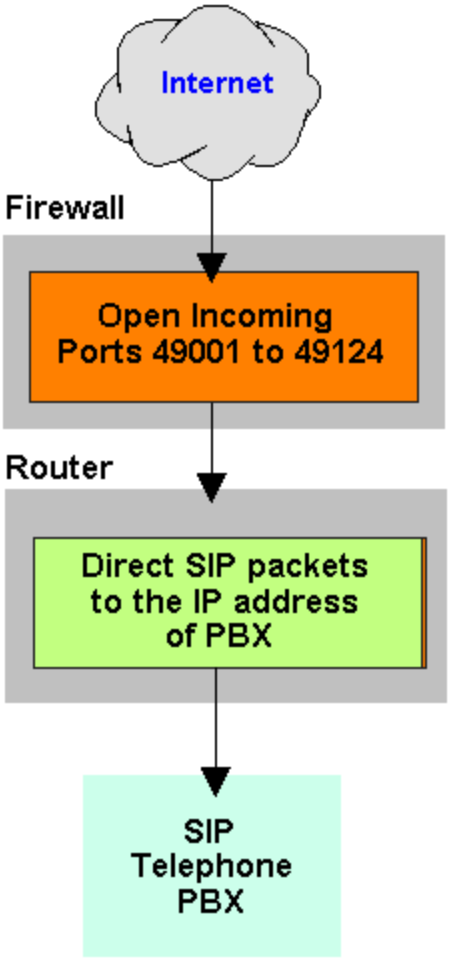
port forwarding is directing traffic from the outside world to the appropriate server inside a local TCP/IP network. Internet services are identified by a standard port number; for example, Web traffic uses port number 80. If the local network hosts a Web server that is accessible on the public Internet, the port forwarding panel in the router would be configured to direct Web/HTTP packets (port 80 traffic) to the IP address of the Web server in the local network (LAN). See TCP/IP port.

Ports are "opened" and "closed" in the firewall, which determines which types of traffic are allowed in or out. In a company, stand-alone commercial firewalls are used. In the home and small business, the firewall is built into the wireless router. For more details, see opening a port.
See firewall, wireless router and port triggering.



Forward Web Traffic

If a company hosts its own website, the router adds the IP address of the Web server to all

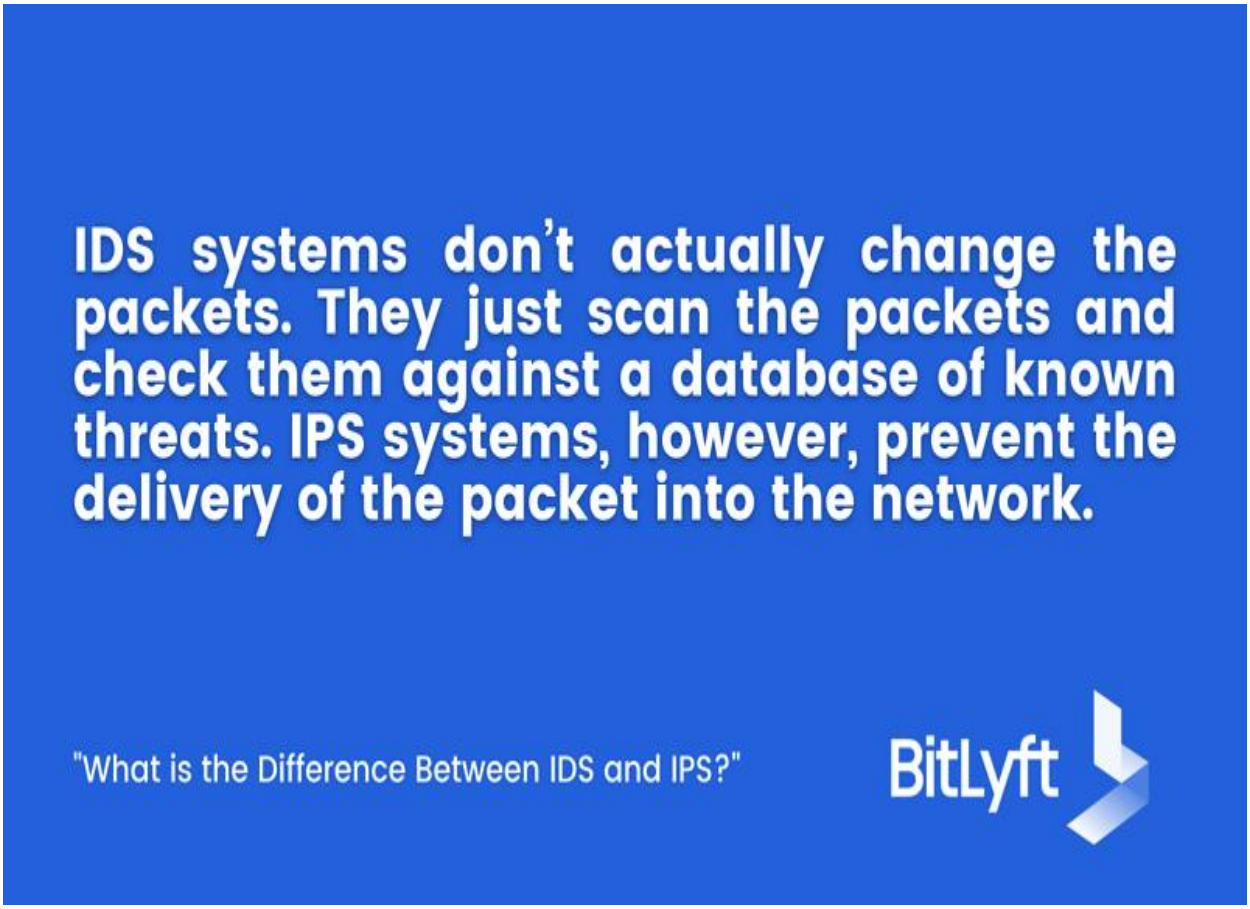


incoming port 80 packets (HTTP packets) from the Internet.

6.Brief Intrusion prevention system - snort? What is the difference between IPS and IDS?

In the ever changing field of cybersecurity, understanding industry terms and technologies is required. Two technologies included in this category are **Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).** IT professionals should know the difference between the two and how they operate. This knowledge is needed to keep your network secure from hackers.

IDS and IPS systems are two parts of network infrastructure that detect and prevent intrusions by hackers. Both systems compare network traffic and packets against a database of cyber threats. The systems then flag offending packets.



The primary difference between the two is that one monitors while the other controls. IDS systems don't actually change the packets. They just scan the packets and check them against a database of known threats. IPS systems, however, prevent the delivery of the packet into the network.

IDS and IPS definitions:

- **Intrusion Detection Systems (IDS):** IDS systems monitor and analyze network traffic for packets and other signs of network invasion. The system then flags known threats and hacking methods. IDS systems detect port scanners, malware, and other violations of system security policies.
- **Intrusion Prevention Systems (IPS):** IPS systems reside in the same area as a firewall, between the internal network and the outside internet. If the IDS system flags something as a threat, the IPS system denies the malicious traffic. If the traffic represents a known threat in the databases, the IPS will shut the threat out and not deliver any malicious packets.

Some manufacturers of IDS and IPS technologies merge the two into one solution. This solution is known as Unified Threat Management (UTM).

7.Explain intrusion detection systems in detail.

Intrusion Detection System (IDS) is a monitoring system that detects suspicious activities and generates alerts when they are detected. Based upon these alerts, a security operations center (SOC) analyst or incident responder can investigate the issue and take the appropriate actions to remediate the threat.

Classification of Intrusion Detection Systems

Intrusion detection systems are designed to be deployed in different environments. And like many cybersecurity solutions, an IDS can either be host-based or network-based.

- **Host-Based IDS (HIDS):** A host-based IDS is deployed on a particular endpoint and designed to protect it against internal and external threats. Such an IDS may have the ability to monitor network traffic to and from the machine, observe running processes, and inspect the system's logs. A host-based IDS's visibility is limited to its host machine, decreasing the available context for decision-making, but has deep visibility into the host computer's internals.
- **Network-Based IDS (NIDS):** A network-based IDS solution is designed to monitor an entire protected network. It has visibility into all traffic flowing through the network and makes determinations based upon packet metadata

and contents. This wider viewpoint provides more context and the ability to detect widespread threats; however, these systems lack visibility into the internals of the endpoints that they protect.

Due to the different levels of visibility, deploying a HIDS or NIDS in isolation provides incomplete protection to an organization's system. A unified threat management solution, which integrates multiple technologies in one system, can provide more comprehensive security.

Detection Method of IDS Deployment

Beyond their deployment location, IDS solutions also differ in how they identify potential intrusions:

- **Signature Detection:** Signature-based IDS solutions use fingerprints of known threats to identify them. Once malware or other malicious content has been identified, a signature is generated and added to the list used by the IDS solution to test incoming content. This enables an IDS to achieve a high threat detection rate with no false positives because all alerts are generated based upon detection of known-malicious content. However, a signature-based IDS is limited to detecting known threats and is blind to zero-day vulnerabilities.
- **Anomaly Detection:** Anomaly-based IDS solutions build a model of the "normal" behavior of the protected system. All future behavior is compared to this model, and any anomalies are labeled as potential threats and generate alerts. While this approach can detect novel or zero-day threats, the difficulty of building an accurate model of "normal" behavior means that these systems must balance false positives (incorrect alerts) with false negatives (missed detections).
- **Hybrid Detection:** A hybrid IDS uses both signature-based and anomaly-based detection. This enables it to detect more potential attacks with a lower error rate than using either system in isolation.

IDS vs Firewalls

Intrusion Detection Systems and firewalls are both cybersecurity solutions that can be deployed to protect an endpoint or network. However, they differ significantly in their purposes.

An IDS is a passive monitoring device that detects potential threats and generates alerts, enabling security operations center (SOC) analysts or incident responders to investigate and respond to the potential incident. An IDS provides no actual protection to the endpoint or network. A firewall, on the other hand, is designed to act as a protective system. It performs analysis of the metadata of network packets and allows or blocks traffic based upon predefined rules. This creates a boundary over which certain types of traffic or protocols cannot pass.

Since a firewall is an active protective device, it is more like an Intrusion Prevention System (IPS) than an IDS. An IPS is like an IDS but actively blocks identified threats instead of simply raising an alert. This complements the functionality of a firewall, and many next-generation firewalls (NGFWs) have integrated IDS/IPS functionality. This enables them to both enforce the predefined filtering rules (firewalls) and detect and respond to more sophisticated cyber threats (IDS/IPS). Learn more about the IPS vs IDS debate here.

Selecting an IDS Solution

An IDS is a valuable component of any organization's cybersecurity deployment. A simple firewall provides the foundation for network security, but many advanced threats can slip past it. An IDS adds an additional line of defense, making it more difficult for an attacker to gain access to an organization's network undetected.

When selecting an IDS solution, it is important to carefully consider the deployment scenario. In some cases, an IDS may be the best choice for the job, while, in others, the integrated protection of an IPS may be a better option. Using a NGFW that has built-in IDS/IPS functionality provides an integrated solution, simplifying threat detection and security management.

Check Point has many years of experience in developing IDS and IPS systems that provide a high level of threat detection with very low error rates, enabling SOC analysts and incident responders to easily identify true threats. To see our NGFWs, with integrated IDS/IPS functionality, in action, request a demonstration or simply contact us with any questions. Furthermore, you're welcome to learn about preventing attacks on IoT networks and devices in this webinar.

8.What is VPN? List out security services VPN provides.

A **virtual private network**, better known as a VPN, gives you online privacy and anonymity by creating a private network from a public internet connection. VPNs mask your internet protocol (IP) address so your online actions are virtually untraceable. Most important, VPN services establish secure and encrypted connections to provide greater privacy than even a secured Wi-Fi hotspot.

A virtual private network is a key privacy tool that you should use when you're logging onto the internet from a public place such as a coffee shop, hotel lobby, or any other spot that offers access to free public Wi-Fi.

A VPN creates a type of tunnel that hides your online activity, including the links you click or the files you download, so that cybercriminals, businesses, government agencies, or other snoops can't see it.

VPN connection

A virtual private network connection allows you to access the internet through a remote server, hiding your actual location and browser history, and encrypting your data.

VPN privacy

This refers to the privacy that using a VPN provides. For instance, a VPN encrypts your data, disguises your location, and conceals your browsing history and the data you transmit via the internet.

VPN clients

A VPN client makes it easier for users to connect to a virtual private network. That's because it is the actual software that is installed on your computer, phone or tablet. The most common operating systems, such as Android, Windows, and iOS, already come with VPN client software pre-installed. However, many users choose to work with third-party VPN clients that offer different features and user interfaces.

VPN protocols

VPN protocols are similar to a set of instructions. VPN providers use these protocols to make sure that users are able to connect securely to a virtual private network. There are several VPN protocols available, all with their own strengths and weaknesses. OpenVPN is one of the more popular protocols. Users like OpenVPN because it is secure and works with most operating systems. The biggest downside of OpenVPN? It can offer slower connection speeds than other protocols.

VPN provider

Synonymous with VPN service, this is a service you sign up for that allows you to connect to a virtual private network by providing a temporary IP address that hides your actual address.

VPN server

VPN services allow you to connect to the internet through remote servers that they either own or have access to. This disguises your location.

VPN service

A service you sign up for that allows you to connect to a virtual private network by providing a temporary IP ddress that hides your actual address.

VPN tunnel

You might sometimes hear your virtual private network referred to as a VPN tunnel. This is just another name for the encrypted connection between your device — a laptop, phone, tablet or desktop computer — and the internet. You can create a VPN tunnel at home or on public Wi-Fi. Once you are using a VPN tunnel to connect to the internet, your ISP, private companies, or the government can no longer see the sites you are browsing or the links you are clicking. A VPN tunnel also hides your IP address. Instead of showing your real location, the sites you surf will only register the location of the VPN provider with which you are working.

9.Explain Linux firewall in detail.

Linux Firewall

Introduction to Linux Firewall

A firewall can be defined as a system of network security that controls and filters the traffic on the rule's predefined set. It is an intermediary system between the Internet and the device.

The kernel of Linux contains a subsystem, i.e., ***Netfilter.*** It is used for deciding or manipulating the network traffic fate headed through or into our server. All latest solutions of Linux firewall apply this system for a process which is known as ***"packet filtering".***

The packet filtering system process of the kernel will be of tiny use to many administrators without any userspace interface for managing it. It is the goal of iptables: if a packet reaches our server, it would be handed off for rejection, acceptance, or manipulation to the ***Netfilter subsystem*** based on various rules supplied to it through userspace by iptables.

Hence, iptables is all we require to handle our firewall if we are known to it. However, several frontends are present for simplifying the task.

> ***Note: If we already know about firewall working and only wish to know about the commands, then we can skip the firewall working and go to the tutorial's end.***

Some ***key points*** are mentioned below that we need to know about ***Linux firewall:***

- A firewall is a group of rules.
- When a packet of data moves out or into a protected space, then its contents (information about its target, protocol, and the origin it plans for using) are checked against the rules of the firewall to see if it must be permitted through.
- Besides, iptables is another tool of CLI to manage the rules of firewall on any Linux machine.
- Also, Firewalld is a tool to manage the rules of a firewall on any Linux machine.
- Linux firewall can also be described as a device that checks Network traffic (outbound/inbound connections) and establishes a decision to traffic out or pass the traffic.
- In this era, Network Security is derived from different kinds of Linux firewalls.
- In the traditional packet, firewall filtering deals with filtering and routing packets, where else NGFWs would work with some other functions (with OSI layers).

firewalld

firewalld can be defined as a way for protecting machines from outside from unwanted traffic. It enables all the users to manage network traffic (incoming) on host machines by specifying the firewall rules set. These rules can be used for sorting the traffic and either allow it or block through.

- ***firewalld*** applies the concepts of ***services and zones*** that simplify the management of traffic.
- ***Zones*** are a ***set of predefined rules.***
- Network sources and interfaces are assigned to the ***zone.***
- The traffic permitted depends on the network our computer is linked to and the level of security this network is elected.
- The ***firewall services*** can be defined as some predefined rules that enclose each essential setting to permit the traffic for a particular service and they use within the zone.
- Services use multiple ***addresses*** or ***ports*** for network communication.
- The ***filter communication*** of firewalls is based on the ***ports.***
- To permit network traffic for any service, its ports should be ***open.***
- ***firewalld*** can block every traffic on the ports that aren't set as open explicitly.

- By default, a few zones like ***trusted*** permit each traffic.
- ***firewalld*** could be used for separating networks into distinct ***zones*** based on the ***trust level*** that a user has determined for placing on the traffic and interfaces in that network.

Working of Linux Firewall

Most of the distributions of Linux ship with many tools of default firewall that could be used for configuring them. We will use ***"IPTables"*** (default tool) given in Linux to create a firewall. Iptables is used for setting up, inspecting, and maintaining the packet filter rules of IPv6 and IPv4 tables in a Linux kernel.

Important: Every command in this article requires the privileges of sudo.

Iptables Working

Network traffic is composed of **packets.** Data is divided into various small pieces (known as ***packets***), transferred over a network, put back altogether. Specifically, ***iptables*** recognizes the packets which are received and applies a group of rules for deciding what we can do to them.

Ipatables is a command-line interface application that permits an administrator for configuring particular rules that would enforce a Linux kernel to implement an action like drop, modify, or inspect network packets.

In a Linux device or machine, enabling the iptables will act as a ***router*** or/and ***Network Firewall.***

Distinct programs and modules of the kernel are used for distinct protocols such as IPtables applies on IPv4, arp tables on ARP, ip6tables on IPv6, and ebtables on Ethernet frames.

Later a project called ***Netfilter*** developed the Nftables for scalability and performance. It is a framework for the packet filtering process that does a similar job to Iptables.

Iptables is used for filtering packets according to:

1. **Tables:** These are files that can join the same operations. A table is composed of various ***chains.***

2. **Chains:** The chains are the rule's string. Ipatales finds an appropriate table if any packet is received, then executes it from the rule's chains until it searches for a match.
3. **Rules:** The rules are the statement that informs a system what needs to do with the packets. They can block a single packet type, or forward other types of packets. The result, in which a packet is transferred, is known as the ***target.***
4. **Targets:** The target is a determination of what needs to do with the packets. It is typically is for accepting it, rejecting it, or dropping it (which transfers the error back to a sender).

10.Explain Windows firewall in detail.

Windows Firewall is a Microsoft Windows application that filters information coming to your system from the Internet and blocking potentially harmful programs. The software blocks most programs from communicating through the firewall. Users simply add a program to the list of allowed programs to allow it to communicate through the firewall. When using a public network, Windows Firewall can also secure the system by blocking all unsolicited attempts to connect to your computer.

Known as Internet Connection Firewall (ICF) before the introduction of Windows XP Service Pack 2 in 2004, Windows Firewall is Windows' built-in security feature that guards against unauthorized network traffic on a user's computer. It helps protect a user's computer from intrusions and harmful attacks by controlling incoming and outgoing network traffic.

The native firewall acts as a barrier between the user's computer and the internet, monitoring all inbound and outbound connections that travel across users' network connections. This protects users against viruses, spyware, worms, Trojan horses, and other malicious software. A firewall can also be used to regulate or restrict access to certain internet services, such as online games or peer-to-peer file-sharing networks.

In addition to being integrated into Microsoft Windows XP Service Pack 2, previous versions of Microsoft operating systems also had Firewall installed by default.

WHAT PROTECTION DOES WINDOWS FIREWALL PROVIDE?

Windows firewall works with both IPv4 and IPv6 data packets at all levels of IP (Internet Protocol) networking (network address translation, IPsec, etc.).

For instance, an attacker may attempt to exploit TCP/IP stack vulnerabilities to establish their machines within a user network, from which they may collect data or launch attacks on the user's local area network using valid IP addresses. From there, a hacker may be able to capture and crack passwords and get control of the user's machine without the user being aware.

HOW DOES WINDOWS FIREWALL WORK?

Windows Firewall makes use of several features to help protect the user's computer from malicious attacks, including network isolation, which prevents malicious websites from taking over the user's browsing experience; traffic segregation, which protects the user's computer if it becomes a member of a botnet or becomes infected with a virus; and IPsec to encrypt Internet traffic.

Since Firewall executes all of these operations automatically, most users do not need to take any action. These features are enabled by default when the user installs Windows OS. While users can turn various features on and off, best practices call for all features to be enabled for maximum protection to protect computers from incoming threats. The firewall offers three distinct layers of protection: private, public, and domain.

- Private level means that all traffic will be blocked from both incoming and outgoing connections.
- At the public level, all connections from outside the user's local network will be blocked.
- Domain level is used if the users are on a network protected by an authentication server such as Active Directory and will block only incoming connections from outside of the local network unless authorized by the said authentication server. If a program requests access through any firewall other than the domain, it will prompt the user to either allow or deny access.