UNIT-5 E-commerce and Cyber Security

5.1 Ethical Hacker

- It is also known as "white hats," ethical hackers are security experts that perform these security assessments. The proactive work they do helps to improve an organization's security position. It requires prior approval from the organization or owner of the IT asset for Ethical Hacking.
- Ethical hacking involves an authorized attempt to gain unauthorized access to a computer system, application, or data. Carrying out an ethical hack involves duplicating strategies and actions of malicious attackers. This practice helps to identify security vulnerabilities which can then be resolved before a malicious attacker has the opportunity to exploit them.

Ethical Hacking experts follow four key protocol concepts:

1. Stay legal

Obtain proper approval before accessing and performing a security assessment.

2. Define the scope

Determine the scope of the assessment so that the ethical hacker's work remains legal and within the organization's approved boundaries.

3. Report vulnerabilities

Notify the organization of all vulnerabilities discovered during the assessment. Provide remediation advice for resolving these vulnerabilities.

4. Respect data sensitivity

Depending on the data sensitivity, ethical hackers may have to agree to a non-disclosure agreement, in addition to other terms and conditions required by the assessed organization.

5.1.1 Roles and Responsibilities of Ethical Hacker

- **Role of Ethical Hacker**

In-depth Knowledge of Security:

Ethical hackers should be well versed with potential threats and vulnerabilities that can hack organizational systems. Ethical hackers are hired by organizations for their expertise skills and quick resolution to security vulnerabilities. They should be cyber security professionals having knowledge of the computer systems, network and security.

Think like Hackers:

The primary role of Ethical hackers is to attack the system like hackers, without adopting authorized methods. They are supposed to think like hackers who want to steal confidential data /information. Ethical hackers look for areas that are most likely to be attacked and the different ways in which attack can take place.

In-depth Knowledge of the Organization they intend to provide Service

Ethical hackers should be well versed with the services of the functional working of the organization they are associated with. It should have the knowledge about the information that is extremely safe and needs to be protected. Ethical hackers should be capable of finding the attack methods for accessing the sensitive content of the organization.

Ethical Hackers Responsibilities:

Hacking their own Systems: Ethical hackers hack their own systems to find potential threats and vulnerabilities. They are hired to find vulnerabilities of the system before they are discovered by hackers.

Diffuse the intent of Hackers: Ethical hackers are hired as a Precaution Step towards Hackers, who aim at breaching the security of computers. Vulnerabilities when detected early can be fixed and safe confidential information from being exposed to hackers who have malicious intentions.

Document their Findings: Ethical hackers must properly document all their findings and potential threats. The main part of the work they are hired by the organizations is proper reporting of bugs and vulnerabilities which are threat to the security.

Keeping the Confidential Information Safe: Ethical hackers must oblige to keep all their findings secure and never share them with others. Under any kind of situation they should never agree to share their findings and observations.

Sign Non-Disclosure Agreements: They must sign confidential agreements to keep the information they have about the organizations safe with them. This will prevent them to give -out confidential information and legal action will be taken against them if they indulge in any such acts.

Handle the loopholes in Security: Based on their observations, Ethical hackers should restore/ repair the security loopholes. This will prevent hackers from

5.1.2Benefits of Ethical Hacking

1. Improve Security Posture

One of the most important benefits of ethical hacking is that it can help organizations identify and address security vulnerabilities in their systems. Organizations can harden their defenses by testing their system against potential attacks and be better prepared to deal with real-world threats.

2. Reduce the Risk of Data Breaches

Data breaches are becoming increasingly common and can have devastating consequences for businesses. By identifying and addressing security vulnerabilities before they can be exploited, ethical hacking can help to reduce the risk of data breaches.

3. Improve Incident Response

In the event of a security incident, it is crucial to have an effective incident response plan in place. Ethical hacking can help organizations test and refine their incident response plans to better deal with actual incidents.

4. Enhance Security Awareness

Organizations that engage in ethical hacking often find that it helps to raise awareness of security issues among their employees. Employees can become more security-conscious and better equipped to deal with potential threats by testing their systems and identifying vulnerabilities.

5. Build Trust With Customers

In today's security-conscious world, customers are increasingly concerned about the safety of their data. By demonstrating that you take security seriously and are proactive in addressing vulnerabilities, you can build trust with your customers and show that you are committed to protecting their data.

Other Advantages are as follow.

- Prevent harmful cyber attacks.
- Prevent penetration attacks of intruders.
- Find loopholes in the system and repair them with their expertise.
- Establish security and safety measures within the system.
- Prevent cyber terrorism and hacks from taking place.

5.1.3 Skills require to become Ethical hacker

Ethical hackers are professionals having immense tech-knowledge about security and safety of computer systems, operating systems, networking. They are required to have excellent hacking skills and prevent threats from harming the computer systems. Some of basic skills that must every hacker have included:

- Knowledge about Networking
- Expert in Scripting
- Good hands-on programming
- Exposure to multiple operating systems: Windows, Linux
- Knowledge of the backend database
- Experience with servers and search engines
- Well-versed with available tools in market

5.2 Penetration testing concepts

- Penetration testing is a type of security testing that is used to test the insecurity of an application. It is conducted to find the security risk which might be present in the system.
- If a system is not secured, then any attacker can disrupt or take authorized access to that system. Security risk is normally an accidental error that occurs while developing and implementing the software. For example, configuration errors, design errors, and software bugs, etc.
- Penetration testing normally evaluates a system's ability to protect its networks, applications, endpoints and users from external or internal threats. It also attempts to protect the security controls and ensures only authorized access.

  Penetration testing is essential because −
- It identifies a simulation environment i.e., how an intruder may attack the system through white hat attack.
- It helps to find weak areas where an intruder can attack to gain access to the computer's features and data.
- It supports to avoid black hat attack and protects the original data.
- It estimates the magnitude of the attack on potential business.
- It provides evidence to suggest, why it is important to increase investments in security aspect of technology

5.2.1 Phases of Ethical hacking

The Ethical hacking process has five phases. These are as follows:

1. Reconnaissance
2. Scanning
3. Access
4. Maintaining access

5. Clearing tracks

1. Reconnaissance

The reconnaissance phase is the first phase of the hacking process. This phase is also known as information gathering and footprinting**.** This phase is very time-consuming. In this phase, we observe and gather all the networks and servers that belong to an organization. We will learn everything about the organization like internet searching, social engineering, non-intrusive network scanning, etc. Depending upon the target, the Reconnaissance phase can last days, weeks or months. The main purpose of this phase is to learn about the potential target as much as possible. We normally collect information about three groups, which are as follows:

- People Involved
- Host
- Network

Footprinting is an ethical hacking technique used to gather as much data as possible about a specific targeted computer system, an infrastructure and networks to identify opportunities to penetrate them.

Footprinting is of two types:

1. **Active:** In the active reconnaissance, we directly interact with the target to get the information. To scan the target, we can use the Nmap tool. Nmap, the acronym for **Network Mapper**, is an open-source security auditing and network scanning software
2. **Passive:** In passive reconnaissance, we indirectly collect information about the target. We can get information about the target from public websites, social media, etc.

2. Scanning

After gathering all the target organization's information, the **exploitable vulnerabilities** are **scanned** by the hacker in the network. In this scan, the hacker will look for weaknesses like outdated applications, open services, open ports, and the equipment types used on the network.

The scanning is of three types:

Port scanning: In this phase, we scan the target to get information like live systems, open ports, various systems that are running on the host.

Vulnerability scanning: In this phase, we check the target for weaknesses that can be exploited. This scan can be done using automatic tools.

Network Mapping: In this, we draw a network diagram of available information by finding the routers, topology of the network, firewall servers, and host information. In the hacking process, this map may serve as an important piece of information.

3. Gaining access

In this phase, the hacker **gains access** to sensitive data using the previous phase's knowledge. The hackers use this data and the network to attack other targets. In this phase, the attackers have some control over other devices. An attacker can use various techniques like brute-forcing to gain access to the system.

4. Maintaining access

In this phase, to **maintain access** to devices, hackers have various options, like creating a backdoor.

A backdoor refers to any method by which authorized and unauthorized users are able to get around normal security measures and gain high level user access (aka root access) on a computer system, network or software application.
A persistent attack on the network can be maintained by the hacker using the backdoor. Without fear of losing access to the device, the hacker can perform an attack on the device they have gained control of. The chances of a hacker being discovered when a backdoor is created. The backdoor leaves a larger footprint for the IDS (intrusion detection system). Using the backdoor, a hacker can access the system any time in the future.

5. Clearing Tracks

An ethical hacker will never want to leave a track about the activities while hacking. So all the files which are related to the attack, he has to remove it. The **clearing tracks** phase's main purpose is to remove all traces through which no one can find him.

5.2.2 Areas of penetration testing

Penetration testing is usually done in the following areas, such as:

- **Network Penetration Testing:** In this testing, the physical structure of a system needs to be tested to identify the vulnerability and risk, which ensures the security in a network. In the networking environment, the tester identities security flaws in the design, implementation, or operation of the respective company or organization's network. The devices tested by a tester can be computers, modems, or even remote access devices, etc.
- **Application Penetration Testing:** In this testing, the logical structure of the system needs to be tested. An attack simulation is designed to expose an application's security

controls' efficiency by identifying vulnerability and risk. The firewall and other monitoring systems are used to protect the security system. Still, sometimes, it needs to be focused on testing, especially when traffic is allowed to pass through the firewall.

- **The system's response or workflow:** Social engineering gathers information on human interaction to obtain information about an organization and its computers. It is beneficial to test the respective organization's ability to prevent unauthorized access to its information systems. Also, this test is exclusively designed for the workflow of the organization or company.

5.3 SQL Injection

5.3.1 Concepts of SQL Injection

- SQL injection is a set of SQL commands that are placed in a URL string or in data structures in order to retrieve a response that we want from the databases that are connected with the web applications. This type of attacks generally takes place on webpages developed using PHP or ASP.NET.
- Successful SQLi attacks allow attackers to modify database information, access sensitive data, execute admin tasks on the database, and recover files from the system. In some cases attackers can issue commands to the underlying database operating system.

An SQL injection attack can be done with the following intentions −

- To dump the whole database of a system,
- To modify the content of the databases, or
- To perform different queries those are not allowed by the application.
- This type of attack works when the applications don’t validate the inputs properly, before passing them to an SQL statement. Injections are normally placed put in address bars, search fields, or data fields.
- The easiest way to detect if a web application is vulnerable to an SQL injection attack is to use the " ‘ " character in a string and see if you get any error.

5.3.2 Types of SQL Injection

- **Union-based SQL Injection** – Union-based SQL Injection represents the most popular type of SQL injection and uses the UNION statement. The UNION statement represents the combination of two select statements to retrieve data from the database.
- **Error-Based SQL Injection** – this method can only be run against MS-SQL Servers. In this attack, the malicious user causes an application to show an error. Usually, you ask the database a question and it returns an error message which also contains the data they asked for.
- **Blind SQL Injection** – in this attack, no error messages are received from the database; We extract the data by submitting queries to the database. Blind SQL injections can be divided into boolean-based SQL Injection and time-based SQL Injection

SQL attacks can also be classified by the method they use to inject data:

- **SQL injection based on user input** – web applications accept inputs through forms, which pass a user's input to the database for processing. If the web application accepts these inputs without sanitizing them, an attacker can inject malicious SQL statements.
- **SQL injection based on cookies** – another approach to SQL injection is modifying cookies to "poison" database queries. Web applications often load cookies and use their data as part of database operations. A malicious user, or malware deployed on a user's device, could modify cookies, to inject SQL in an unexpected way.
- **SQL injection based on HTTP headers** – server variables such HTTP headers can also be used for SQL injection. If a web application accepts inputs from HTTP headers, fake headers containing arbitrary SQL can inject code into the database.
- **Second-order SQL injection** – these are possibly the most complex SQL injection attacks, because they may lie dormant for a long period of time. A second-order SQL injection attack delivers poisoned data, which might be considered not dangerous in one context, but is malicious in another context. Even if developers sanitize all application inputs, they could still be vulnerable to this type of attack. A second-order SQL Injection, is a vulnerability exploitable in two different steps:

1. Firstly, we STORE a particular user-supplied input value in the DB and

2. Secondly, we use the stored value to exploit a vulnerability in a vulnerable function in the source code which constructs the dynamic query of the web application

5.3.3 Case study of SQL Injection

- We have an application based on employee records. Any employee can view only their own records by entering a unique and private employee ID. We have a field like an Employee ID. And the employee enters the following in the input field:

  236893238 or 1=1

  It will translate to:

1. **SELECT** * **from** EMPLOYEE **where** EMPLOYEE_ID == 236893238 or 1=1

The SQL code above is valid and will return EMPLOYEE_ID row from the EMPLOYEE table. The 1=1 will return all records for which this holds true. All the employee data is compromised; now, the malicious user can also similarly delete the employee records.

Example:

2. SELECT * from Employee where (Username == "" or 1=1) AND (Password="" or 1=1).

Now the malicious user can use the '=' operator sensibly to retrieve private and secure user information. So instead of the query mentioned above, the following query, when exhausted, retrieve protected data, not intended to be shown to users.

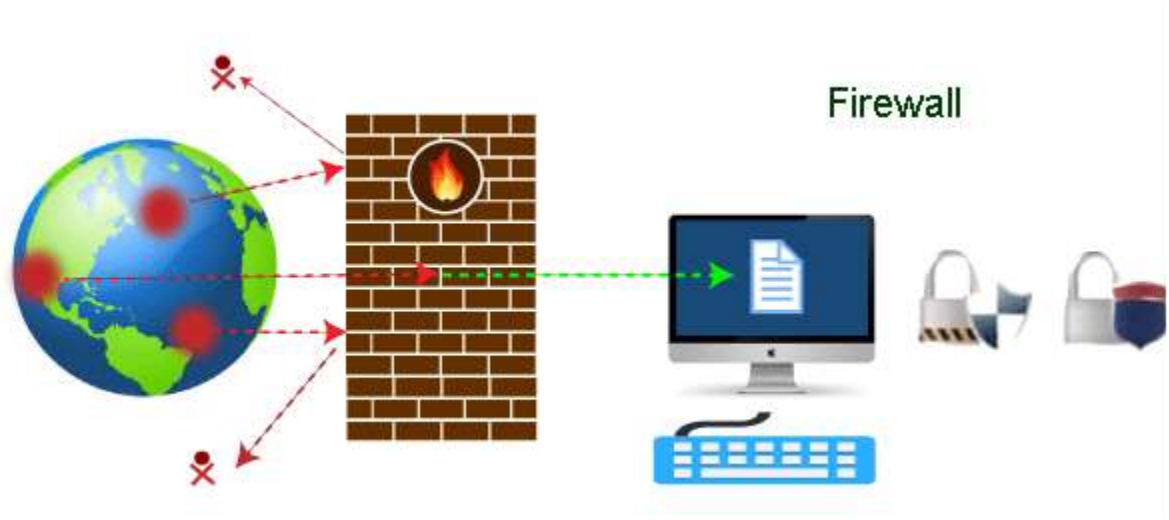
3. SELECT * from EMPLOYEE where (Employee_name =" " or 1=1) AND (Password=" " or 1=1)

5.4 Firewall

5.4.1 Concepts of Firewall

- Nowadays, it is a big challenge to protect our sensitive data from unwanted and unauthorized sources. There are various tools and devices that can provide different security levels and help keep our private data secure. One such tool is a 'firewall' that prevents unauthorized access and keeps our computers and data safe and secure.
- A firewall can be defined as a special type of network security device or a software program that monitors and filters incoming and outgoing network traffic based on a defined set of security rules. It acts as a barrier between internal private networks and external sources (such as the public Internet).
- The primary purpose of a firewall is to allow non-threatening traffic and prevent malicious or unwanted data traffic for protecting the computer from viruses and attacks.

A firewall is a cyber security tool that filters network traffic and helps users block malicious software from accessing the Internet in infected computers.



- This is one of the most problematic questions whether a firewall is a hardware or software. As stated above, a firewall can be a network security device or a software program on a computer. This means that the firewall comes at both levels, i.e., hardware and software, though it's best to have both.
- Each format (a firewall implemented as hardware or software) has different functionality but the same purpose. A hardware firewall is a physical device that attaches between a computer network and a gateway. For example, a broadband router. On the other hand, a software firewall is a simple program installed on a computer that works through port numbers and other installed software.
- Apart from that, there are cloud-based firewalls. They are commonly referred to as FaaS (firewall as a service). A primary advantage of using cloud-based firewalls is that they can be managed centrally. Like hardware firewalls, cloud-based firewalls are best known for providing perimeter security.

5.4.2 Types of Firewall

Packet Filtering Firewall

A packet filtering firewall is a network security technique that regulates data flow to and from a network. It is a security mechanism that allows packets to move across networks while controlling their flow through the use of a set of rules, protocols, IP addresses, and ports.

Packet-filtering firewalls operate at the network layer (Layer 3) of the OSI model. Packet-filtering firewalls are very fast because there is not much logic going behind the decisions they make. They do not do any internal inspection of the traffic. Packet-filtering firewalls are

considered not to be very secure. This is because they will forward any traffic that is flowing on an approved port.

Packet filtering firewalls allow or deny network packets based on the following criteria:

- The source IP address is where the packet is being sent from.
- The packet's address is the destination IP address.
- Ports include source and destination ports

Proxy Firewall

A firewall proxy provides security by controlling the information going in and out of the network. Firewall proxy servers filter, cache, log, and control requests coming from a client to keep the network secure and free of intruders and viruses. Proxy firewall has its own IP (internet protocol) address so that internal network never makes a direct connection with outside internet. Since it monitors information at the application level, it is also known as application firewall.

How proxy firewall handles requests from the internal network :

1. The proxy firewall acts as intermediary between trusted internal network and outside internet.
2. If computers in internal network wish to make a connection with outside internet, they first communicate with the proxy.
3. Proxy then forwards data from internal network to the internet and sends data received from internet to internal network.
4. In this way the proxy firewall shields internal network from intruders in the outside internet and prevents direct connections between internal network and internet.

5.4.3 Working, Advantages and Importance of Firewall

- Working of Firewall

As mentioned previously, firewalls filter the network traffic within a private network. It analyses which traffic should be allowed or restricted based on a set of rules. Think of the firewall like a gatekeeper at your computer's entry point which only allows trusted sources, or IP addresses, to enter your network.

A firewall welcomes only those incoming traffic that has been configured to accept. It distinguishes between good and malicious traffic and either allows or blocks specific data packets on pre-established security rules.

These rules are based on several aspects indicated by the packet data, like their source, destination, content, and so on. They block traffic coming from suspicious sources to prevent cyberattacks.

For example, the image depicted below shows how a firewall allows good traffic to pass to the user's private network.

Fig: Firewall allowing Good Traffic

However, in the example below, the firewall blocks malicious traffic from entering the private network, thereby protecting the user's network from being susceptible to a cyberattack.

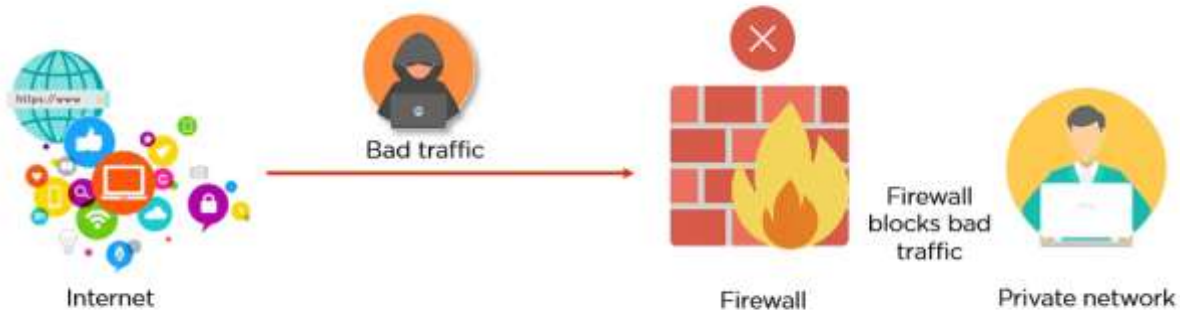


Fig: Firewall blocking Bad Traffic

This way, a firewall carries out quick assessments to detect malware and other suspicious activities.

There are different types of firewalls to read data packets at different network levels. Now, you will move on to the next section of this tutorial and understand the different types of firewalls.

- **Importance of Using a Firewall :**
  The following points listed below are the most relevant in explaining the importance of firewalls is as follows.

Feature-1 :
Monitoring Network Traffic –
Firewall security starts with effective monitoring of network traffic based on pre-established rules and filters to keep the systems protected. Monitoring of network traffic involves the following security measures.

1. **Source or destination-based blocking of incoming network traffic –**
   This is the most common feature of most firewalls, whereby the firewalls block the incoming traffic by looking into the source of the traffic.

2. **Outgoing network traffic can be blocked based on the source or destination –**
   Many firewalls can also filter data between your internal network and the Internet. You might, for example, want to keep employees from visiting inappropriate websites.

3. **Block network traffic based on content –**
   More modern firewalls can screen network traffic for inappropriate content and block traffic depending on that. A firewall that is integrated with a virus scanner, for example, can prevent virus-infected files from entering your network. Other firewalls work in tandem with e-mail services to filter out unwanted messages.

4. **Report on network traffic and firewall activities –**
   When filtering network traffic to and from the Internet, it's also crucial to know what your firewall is doing, who tried to break into your network, and who tried to view prohibited information on the Internet. A reporting mechanism of some sort is included in almost all firewalls.

Feature-2 :
Stops Virus Attacks and spyware –
With cyber thieves creating hundreds of thousands of new threats every day, including spyware, viruses, and other attacks like email bombs, denial of service, and malicious macros, it's critical that you put protections in place to keep your systems safe. The number of entry points criminals can exploit to get access to your systems grows as your systems become more complicated and strong. Spyware and malware programs designed to penetrate your networks, manage your devices, and steal your data are one of the most common ways unwelcome persons obtain access. Firewalls are a crucial line of defense against malicious software.

- **Advantages of Firewall**

1. Give Protection Against Harmful Elements

Firewalls are designed to protect the computer from viruses, malware, and other harmful codes. And if the computer has its firewall protection, the user can run the safe operations of their office task. Now it has become one of the essential tools for companies and individuals. Because it makes sure to prove a secure and efficient user experience while navigating the web pages. It also warns when users install any application and suggest relevant settings. Hence it is one of the valuable advantages of a firewall in a computer network.

2. Installation Process is Relatively Easy

If you are not a technical expert, then also you can install the firewalls on your computer. And for installing the firewalls, there is not any need for professional guidance. If you think you need some help in installing the firewalls. Then you can look for internet resources that are full of information. However, most modern operating systems like Windows 10, Windows 8, and 7 already have a pre-installed firewall. Although the hardware firewalls are a bit tricky to install, the user can need an expert.

3. Keep Analyzing Traffic

It is one of the crucial advantages of firewalls, as most threats happen through virtual traffic. Thus, if you have installed the firewalls in your device. In that case, it will keep running in the background and analyze all the traffic. Whatever the information passed into the device, all that runs through the firewalls. And if it finds any suspicious codes such as malware or virus, in that case, it automatically warns the user and stops that threat.

4. It Helps in Maintaining High-Level Privacy

A user expects complete privacy while going online, but they can suffer from this need with some unexpected scenarios. Hence, if they use the firewalls in that case, it will make sure to maintain their high-level privacy. And whenever they navigate the web pages, the firewall application will keep monitoring the viruses. Thus, it is also one of the significant benefits of firewalls that users can have. But they all need to have installed firewalls in their computer device.

5. Stop Attacks of Hackers

Some hackers conduct illegal activity by getting unauthorized access to the computers of people like us. Hence they keep looking for devices to hack and get access to sensitive data like credit card details. So they can harm you; moreover, they also spread harmful codes or viruses over the

internet. That can contact the computer and discover the data so the hacker can help hack the computer device. Thus, it is essential to have a firewall installed on your computer device.