

CHAPTER-1

Network

A **network** consists of two or more computers that are linked in order to share resources (such as printers and CDs), exchange files, or allow electronic communications. The computers on a **network** may be linked through cables, telephone lines, radio waves, satellites, or infrared light beams. A computer network is a group of computers that use a set of common communication protocols over digital interconnections for the purpose of sharing resources located on or provided by the network nodes

What is Security

S-Sensible E-Efficient in work C-Claver U-Understanding R-Regular I-Intelligent T-Talent Y-Young

Security, in information technology (IT), is the defense of digital information and IT assets against internal and external, malicious and accidental threats.

What is network security

Network security is a broad term that covers a multitude of technologies, devices and processes. In its simplest term, it is a set of rules and configurations designed to protect the integrity, confidentiality and accessibility of computer networks and data using both software and hardware technologies. Every organization, industry or infrastructure, requires a degree of network security solutions in place to protect it from the ever-growing landscape of cyber threats in the wild today.

How does network security work?

There are many layers to consider when addressing network security across an organization. Attacks can happen at any layer in the network security layers model, so your network security hardware, software and policies must be designed to address each area.

Network security typically consists of three different controls: physical, technical and administrative

Here is a brief description of the different types of network security and how each control works.

1) Physical Network Security

Physical security controls are designed to prevent unauthorized personnel from gaining physical access to network components such as routers, cabling cupboards and so on. Controlled access, such as locks, biometric authentication and other devices, is essential in any organization.

2) Technical Network Security

Technical security controls protect data that is stored on the network or which is in transit across, into or out of the network. Protection is twofold; it needs to protect data and systems from unauthorized personnel, and it also needs to protect against malicious activities from employees.

3) Administrative Network Security

Administrative security controls consist of security policies and processes that control user behavior, including how users are authenticated, their level of access and also how IT staff members implement changes to the infrastructure.

Types of network security

1) Network Access Control

To ensure that potential attackers cannot infiltrate your network, comprehensive access control policies need to be in place for both users and devices. Network access control (NAC) can be set at the most granular level. For example, you could grant administrators full access to the network but deny access to specific confidential folders or prevent their personal devices from joining the network.

2) Antivirus and Antimalware Software

Antivirus and antimalware software protect an organization from a range of malicious software, including viruses, ransomware, worms and trojans. The best software not only scans files upon entry to the network but continuously scans and tracks files.

3) Firewall Protection

Firewalls, as their name suggests, act as a barrier between the untrusted external networks and your trusted internal network. Administrators typically configure a set of defined rules that blocks or permits traffic onto the network.

4) Virtual Private Networks

Virtual private networks (VPNs) create a connection to the network from another endpoint or site. For example, users working from home would typically connect to the organization's network over a VPN. Data between the two points is encrypted and the user would need to authenticate to allow communication between their device and the network.

5) Rename routers and **networks.**

6) Use strong passwords.

7) Keep everything updated.

8) Turn on encryption.

9) Turn off the WPS (Wi-Fi protected setup) setting.

CHAPTER - 2

VIRUS (Vital Information under siege)

A computer virus is a malicious software program loaded onto a user's computer without the user's knowledge and performs malicious actions.

How does a computer get a virus?

There are many ways a computer can become infected with a computer virus or other malware. When a virus is made, it's often distributed through shareware, pirated software, e-mail, P2P programs, or other programs where users share data. Once downloaded, copied, or otherwise acquired, if the infected program is executed, it can potentially affect anything that a computer can access.

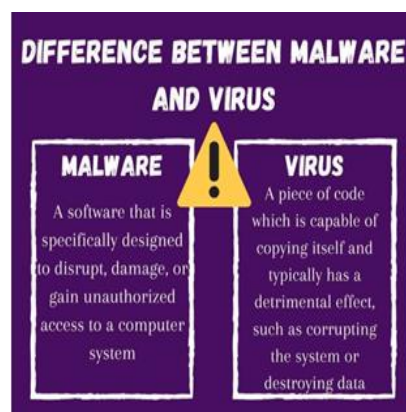
What can a virus do to a computer?

- Delete some or all files without consent.
- Cause various error messages in files or on programs.
- Changes volume label.
- Marks clusters as bad in the FAT .
- Create more than one partition.
- Causes cross linked files.
- Causes a "sector not found" error.
- Decrease the speed of the computer, causing the system to run slow or be low on resources.
- Create logical partitions or partitions decrease in size.
- Make directories appear as garbage.
- Cause hardware problems such as keyboard keys not working, printer issues, modem issues, etc
- Disable ports such as LPT or COM ports.
- Cause keyboard keys to be remapped.
- Alter the system time and date.
- Cause system to hang or freeze randomly.
- Cause activity on HDD or FDD randomly.
- Increase file size.
- Change file attributes.
- Increase or decrease memory size.
- Randomly change file or memory size.
- Extend boot times.
- Cause a computer to make strange noises, make music, clicking noises, or beeps.
- Display pictures randomly.
- Unusual or undocumented error messages.

Types of Computer Virus

- **Boot Sector Virus** – It is a type of virus that infects the boot sector of floppy disks or the Master Boot Record (MBR) of hard disks. The Boot sector comprises all the files which are required to start the Operating system of the computer. The virus either overwrites the existing program or copies itself to another part of the disk.
- **Direct Action Virus** – When a virus attaches itself directly to a .exe or .com file and enters the device while its execution is called a Direct Action Virus. If it gets installed in the memory, it keeps itself hidden. It is also known as Non-Resident Virus.

- **Resident Virus** – A virus which saves itself in the memory of the computer and then infects other files and programs when its originating program is no longer working. This virus can easily infect other files because it is hidden in the memory and is hard to be removed from the system.
- **Multipartite Virus** – A virus which can attack both, the boot sector and the executable files of an already infected computer is called a multipartite virus. If a multipartite virus attacks your system, you are at risk of cyber threat.
- **Overwrite Virus** – One of the most harmful viruses, the overwrite virus can completely remove the existing program and replace it with the malicious code by overwriting it. Gradually it can completely replace the host's programming code with the harmful code.
- **Polymorphic Virus** – Spread through spam and infected websites, the polymorphic virus are file infectors which are complex and are tough to detect. They create a modified or morphed version of the existing program and infect the system and retain the original code.
- **File Infector Virus** – As the name suggests, it first infects a single file and then later spreads itself to other executable files and programs. The main source of this virus are games and word processors.
- **Spacefiller Virus** – It is a rare type of virus which fills in the empty spaces of a file with viruses. It is known as cavity virus. It will neither affect the size of the file nor can be detected easily.
- **Macro Virus** – A virus written in the same macro language as used in the software program and infects the computer if a word processor file is opened. Mainly the source of such viruses is via emails.



CHAPTER – 3

What is an Anti-Virus?

Antivirus software is a **type** of program designed and developed to protect **computers** from malware like **viruses**, **computer** worms, spyware, botnets, rootkits, keyloggers etc.

That means it is a set of programs which can detect and remove all the harmful and malicious software from your device. This anti-virus software is designed in a manner that they can search through the files in a computer and determine the files which are heavy or mildly infected by a virus. There are many versions and **types of anti-virus** programs are present on the market.

Different name of antivirus software which is most commonly used:

- **Norton Antivirus**
- **QUICKHEAL**
- **Kaspersky Antivirus**
- **AVAST Antivirus**
- **McAfee Antivirus**

INSTALLATION OF ANTI VIRUS

How to install an antivirus program on a computer

Antivirus programs help prevent [viruses](#) and [spyware](#) from infecting a computer and therefore are one of the essential software programs each computer should have running at all times. There are thousands of viruses and spyware on the Internet, and any one of them can cause damage to personal files or the computer's [operating system](#).

Note : All new versions of Microsoft Windows now include [Windows Defender](#) to help protect your computer from viruses.

Install the antivirus program

To install an antivirus program on your computer, follow the steps below.

1. If you purchased the antivirus program from a retail store, insert the [CD](#) or [DVD](#) into the computer's disc drive. The installation process should start automatically, with a window opening to help guide you through the install process.
2. If you [downloaded](#) the antivirus program on the Internet, find the downloaded file on your computer. If the downloaded file is a zip file, [unzip](#) the file to extract and access the installation files. Look for a file named setup.exe, install.exe, or something similar, then [double-click](#) that file. The installation process should start, with a window opening to help guide you through the install process.
3. In the installation process window, follow the steps provided to install the antivirus program. The install process provides recommended options so the antivirus program will function properly, which in most cases can be accepted as is. The one exception is if the install process recommends to install any toolbars for Internet browsers or other helpful programs for your computer. If prompted to install other software with the antivirus program, uncheck all boxes or decline the install of those extra programs. No additional programs should

be needed for the antivirus program to install and run successfully on your computer.

4. When the install process is complete, close out of the install window.
5. If used, remove the CD or DVD from the computer's disc drive.

The antivirus program is now installed and ready to use. While it may not be required, we recommend [restarting](#) your computer so that any modified settings in the operating system can take effect correctly.

Update the antivirus program after installation

Out of the box, antivirus programs are not up-to-date and are missing the latest virus and spyware definitions. Without the latest definitions, the antivirus program will not know about the most recently created viruses and spyware, making your computer vulnerable to an infection.

After installing the antivirus program, we highly recommend you update it with the latest virus and spyware definitions. The updates allow the antivirus program to protect your computer from all viruses and spyware.

In many cases, the antivirus program automatically checks for and installs the latest updates. If prompted to do so, select Yes to update the antivirus program. If it does not prompt you to update immediately.

Enable automatic updates for the antivirus program

By default, most antivirus programs enable the automatic update feature. We strongly recommend automatic updates be enabled to keep the antivirus program up-to-date at all times.

To check if automatic updates are enabled in your antivirus program, follow the general steps below.

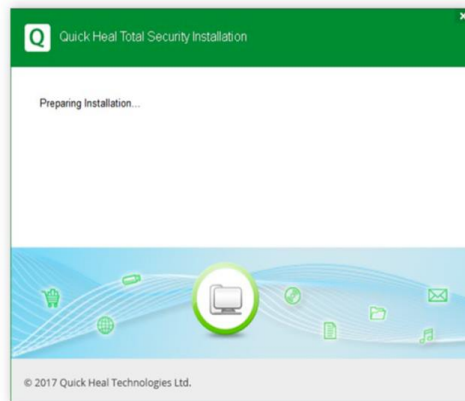
1. Open the antivirus program.
2. Look for a **Settings** or **Advanced Settings** button or link in the antivirus program window. If you do not see either option, look for an option like **Updates** or something similar.
3. In the Settings or Updates window, look for an option like **Automatically download and apply updates**. It may also refer to virus definitions instead of updates.
4. For the automatic updates option, check the box for that option, if not already checked.
5. Click the **Save** or **Apply** button to save the settings change.

Procedure to Install Quick Heal Total Security / Internet Security Antivirus from CD/DVD

Insert Quick Heal CD in the CD drive of your PC.

- The installer will autorun without any external action.

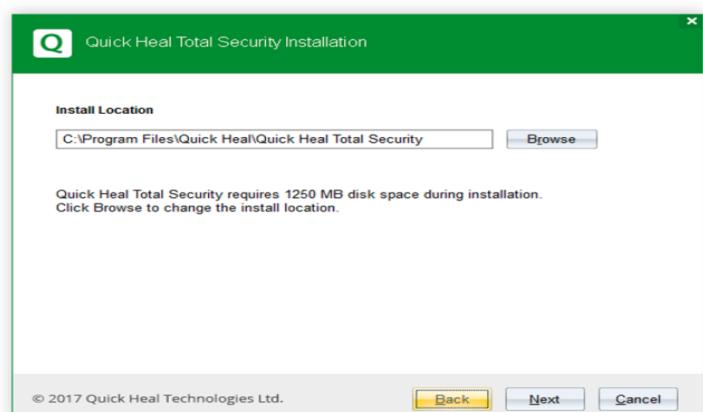
- Click on Install Quick Heal.



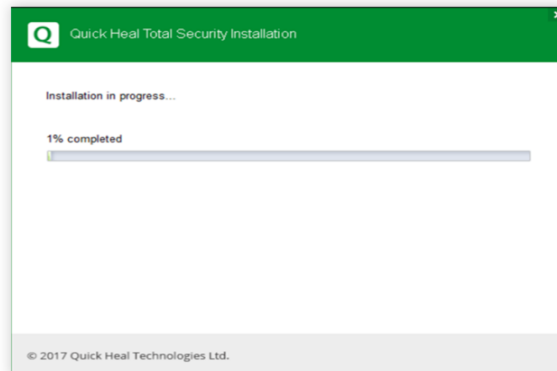
- Follow the steps in the setup wizard.
- Read the User and License and Agreement carefully and check the box that says 'I Agree'



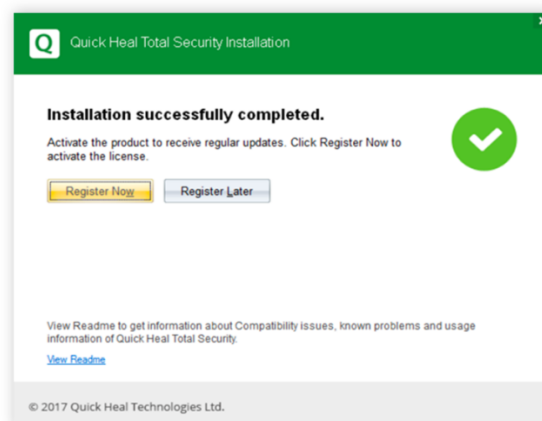
- Select the drive where the software is to be installed



- Let it install files in the selected drive, till it is 100% complete.



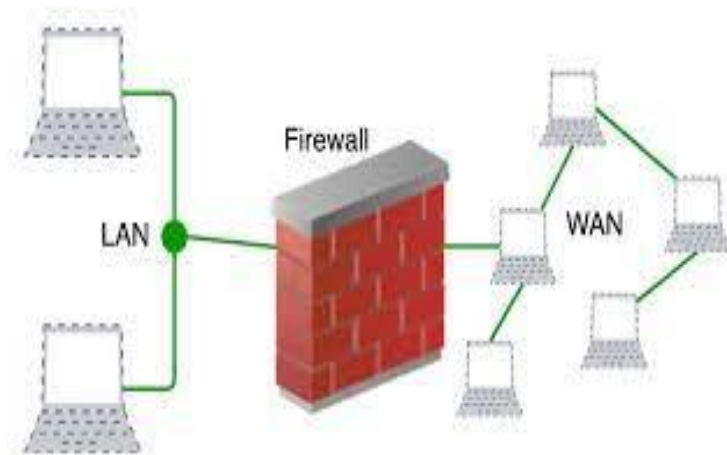
- Once completed, it will ask you to register the product. Click on 'Register Now'.



- you have the product key and the installation number with you.
- The product key can be found printed either on or inside the product packaging or will be provided when you [purchase Quick Heal AntivirusTotal Security/Internet security.](#)
- Fill the registration form and enter the product key received after buying the product.

CHAPTER - 4 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.**



What is a Firewall?

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

How does a Firewall work?

A Firewall analyses the network traffic and filters it so that the unsecured and suspicious networks cannot attack the system. The point where information is exchanged with an external network is called a port.

Firewall : Hardware or Software

This is very difficult to explain whether a firewall is a hardware or software. 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.

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.

History of Firewall

Firewalls have been the first and most reliable component of defense in network security for over 30 years. Firewalls first came into existence in the late 1980s. They were initially designed as packet filters. These packet filters were nothing but a setup of networks between computers. The primary function of these packet filtering firewalls was to check for packets or bytes transferred between different computers.

Functions of Firewall

The firewall works as a gatekeeper. It analyzes every attempt coming to gain access to our operating system and prevents traffic from unwanted or non-recognized sources. The firewall acts as a barrier or filter between the computer system and other

networks (i.e., the public Internet), we can consider it as a traffic controller. Therefore, a firewall's primary function is to secure our network and information by controlling network traffic, preventing unwanted incoming network traffic, and validating access by assessing network traffic for malicious things such as hackers and malware.

Generally, most operating systems (for example - Windows OS) and security software come with built-in firewall support. Therefore, it is a good idea to ensure that those options are turned on. Additionally, we can configure the security settings of the system to be automatically updated whenever available.

How is Firewall different from an Antivirus ?

A firewall is a security network designed to protect computer systems and networks from malicious attacks. Whereas, Antivirus is a software utility program designed to protect a system from internal attacks from viruses.

Difference between a Firewall and Anti-virus

Attributes	Firewall	Anti-virus
Definition	A firewall is defined as the system which analyzes and filters incoming or outgoing data packets based on pre-defined rules.	Anti-virus is defined as the special type of software that acts as a cyber-security mechanism. The primary function of Anti-virus is to monitor, detect, and remove any apprehensive or distrustful file or software from the device.
Structure	Firewalls can be hardware and software both. The router is an example of a physical firewall, and a simple firewall program on the system is an example of a software firewall.	Anti-virus can only be used as software. Anti-virus is a program that is installed on the device, just like the other programs.
Implementation	Because firewalls come in the form of hardware and software, a firewall can be implemented either way.	Because Anti-virus comes in the form of software, therefore, Anti-virus can be implemented only at the software level. There is no possibility of implementing Anti-virus at the hardware level.
Responsibility	A firewall is usually defined as a network controlling system. It means that firewalls are	Anti-viruses are primarily responsible for detecting and removing viruses from computer systems or other devices.

	primarily responsible for monitoring and filtering network traffic.	These viruses can be in the form of infected files or software.
Scalability	Because the firewall supports both types of implementations, hardware, and software, therefore, it is more scalable than anti-virus.	Anti-viruses are generally considered less-scalable than firewalls. This is because anti-virus can only be implemented at the software level. They don't support hardware-level implementation.
Threats	A firewall is mainly used to prevent network related attacks. It mainly includes external network threats? for example- Routing attacks and IP Spoofing.	Anti-virus is mainly used to scan, find, and remove viruses, malware, and Trojans, which can harm system files and software and share personal information (such as login credentials, credit card details, etc.) with hackers.

CHAPTER - 5

Types of Firewall

There are various types of Firewalls. Described below are each of them in detail for a better and simplistic understanding:

1. Packet Filtering Firewall

- One of the oldest types of Firewall
- This type of Firewall creates a checkpoint at the traffic router. Only the secure and verified IP address or networks are allowed for the further flow of data
- The data packets are not verified, i.e. the information or data is not opened at the Firewall stage
- They are easy to use and do not overload the device and do not affect its processing or functioning speed

2. Application level gateway Firewall

- It is also known as Proxy Firewall
- When the user connects with the destination server, it forms a connection with the application gateway
- The proxy then connects with the destination server and takes up the decision of forwarding the data packets
- It is a bit more secure in comparison to Packet Filtering Firewall
- Strong Memory and processors are required for using this Firewall

3. Circuit Level gateway Firewall

- This works as the Sessions layer of the OSI Model
- Using this, two Transmission Control Protocol (TCP) connections can be set up together
- It can easily let the flow of data packets continue without consuming major computer resources
- These Firewalls are not much efficient as they do not check the data packets and incase a data packet comprises malware, it will allow it to pass if the TCP connections are successfully done

4. Statefull Infection Firewall

- It is a combination of data packet inspection and TCP connection. Until both the fields are verified, the information cannot be approved
- They are less straining for the computer resources
- However, they are a bit slow in comparison to other Firewalls

5. Next-generation Firewall

- The recently launched Firewall systems are known as the Next-Gen Firewalls
- Under this, the data packets are also thoroughly checked before being passed on to the destination address
- These are still on the platform of improving and evolving and intend to use modern technology for automatic detection of errors and network safety

6. Software Firewall

- Any firewall which is installed in a local device or a cloud server is called a Software Firewall
- They can be the most beneficial in terms of restricting the number of networks being connected to a single device and control the in-flow and out-flow of data packets
- Software Firewall also time-consuming

7. Hardware Firewall

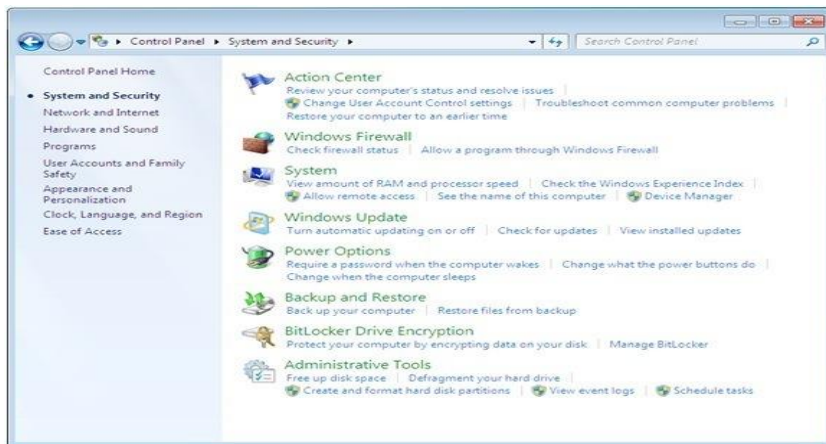
- They are also known as Physical-appliance based firewalls
- It ensures that the malicious data is stopped before it reaches the endpoint of the network at risk

How to set up the Windows 7 firewall to protect your computer against malicious activity.

Setup system and security setting

1. From the Start menu, click **Control Panel**, then click **System and Security**

2. Under Windows Firewall, select either **Check firewall status** to determine whether the firewall is turned on or off, or **Allow a program through Windows Firewall** to allow a blocked program through the firewall

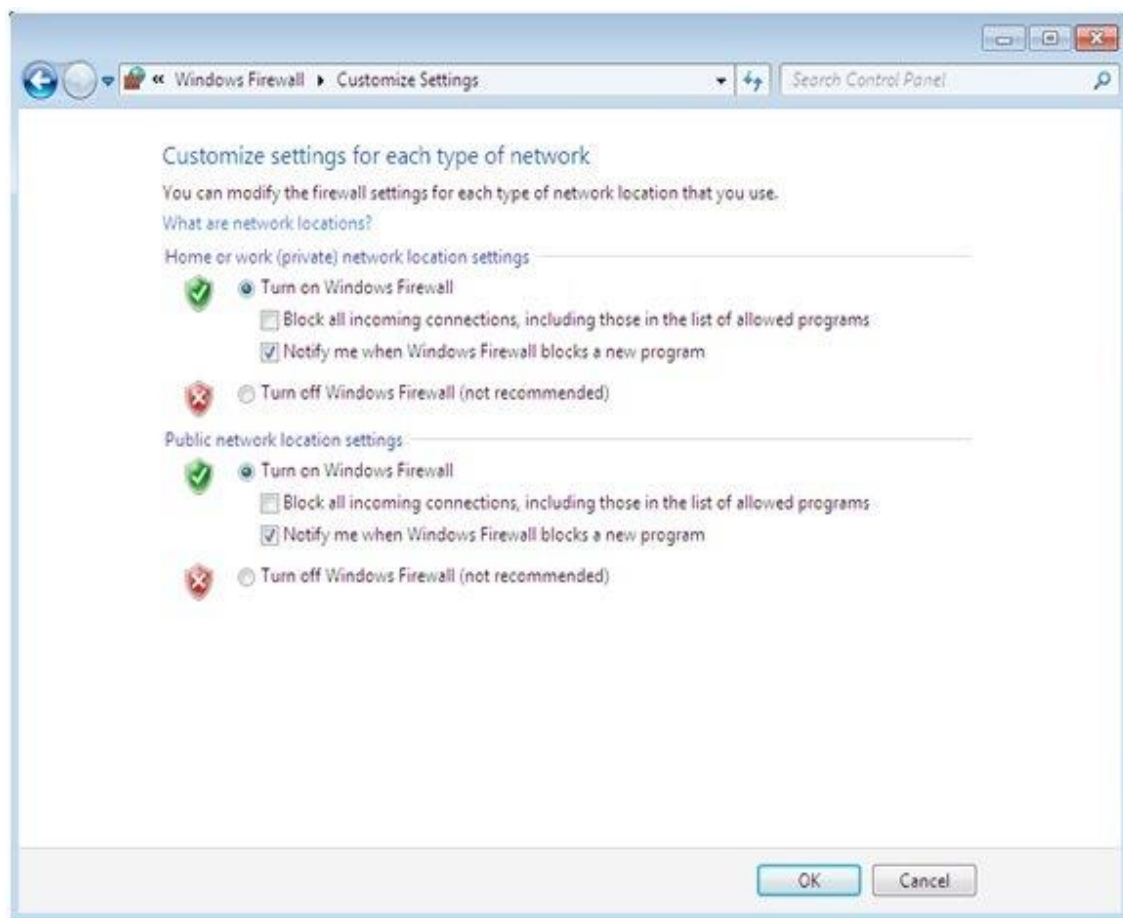


1. Click **Turn Windows Firewall on or off** from the left side menu
2. Configure the settings for your home/work (private) or public network
3. Click **OK** to save your changes



1. Turn on Windows Firewall for each network location you use - **Home or work (private)** or **Public**
 - Click **What are network locations?** for more information on network types
 - Domain network locations are controlled by your network administrator and can't be selected or changed
2. Select **Turn on Windows Firewall** under the applicable network location type (in image below, both locations are selected)
3. Select **Notify me when Windows Firewall blocks a new program** for each network type, if the box is not already checked

Click **OK** to save your changes



Turn on Windows Defender

Complete the following steps to turn on Windows Defender on your device.

1. Select the **Start** menu.
2. In the search bar, type **group policy**. Then select **Edit group policy** from the listed results. The Local Group Policy Editor will open.
3. Select **Computer Configuration > Administrative Templates > Windows Components > Windows Defender Antivirus**.
4. Scroll to the bottom of the list and select **Turn off Windows Defender Antivirus**.
5. Select **Disabled** or **Not configured**. It might feel counter-intuitive to select these options because the names suggest that you're turning Windows Defender off. Don't worry, these options actually ensure that it's turned on.
6. Select **Apply > OK**.

CHAPTER-6

Data Encryption and Decryption

Encryption is the process of translating plain text data ([plaintext](#)) into something that appears to be random and meaningless ([ciphertext](#)). Decryption is the process of converting ciphertext back to plaintext.

Before, we understand Encryption vs. Decryption let's first understand-

What is Cryptography?

Cryptography is used to secure and protect data during communication. It is helpful to prevent unauthorized person or group of users from accessing any confidential data. Encryption and decryption are the two essential functionalities of cryptography.

A message sent over the network is transformed into an unrecognizable encrypted message known as data encryption. At the receiving end, the received message is converted to its original form known as decryption.

What is meant By Encryption?

Encryption is a process which transforms the original information into an unrecognizable form. This new form of the message is entirely different from the original message. That's why a hacker is not able to read the data as senders use an encryption algorithm. Encryption is usually done using key algorithms.



What is meant by Decryption?

Decryption is a process of converting encoded/encrypted data in a form that is readable and understood by a human or a computer. This method is performed by un-encrypting the text manually or by using keys used to encrypt the original data.



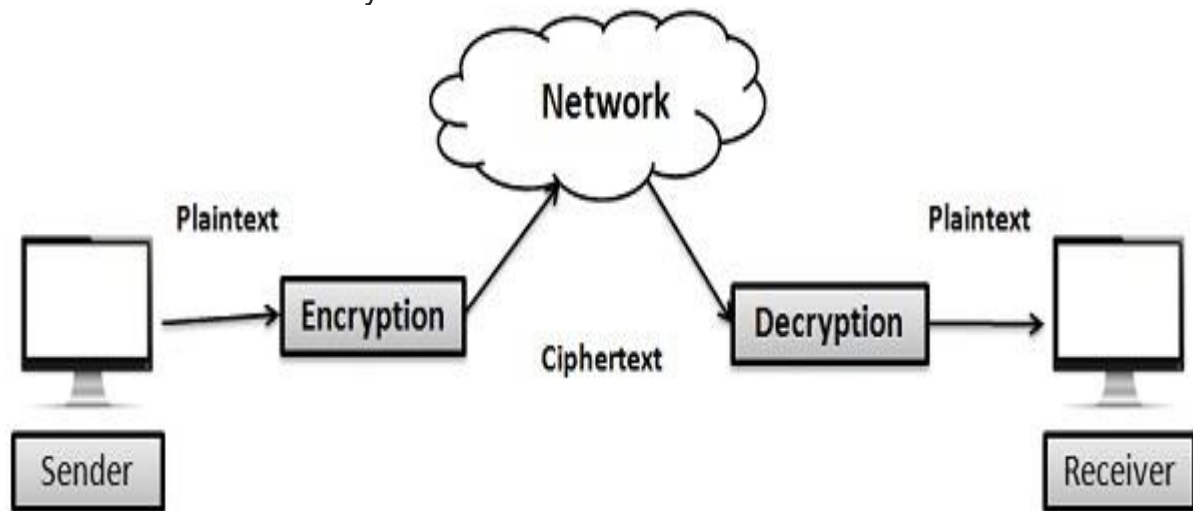
KEY DIFFERENCE

- Encryption is a process of converting normal data into an unreadable form whereas Decryption is a method of converting the unreadable / coded data into its original form.
- Encryption is done by the person who is sending the data to the destination, but the decryption is done at the person who is receiving the data.
- The same algorithm with the same key is used for both the encryption-decryption processes.

Why use Encryption and Decryption?

Here, are important reasons for using encryption:

- Helps you to protect your confidential data such as passwords and login id
- Provides confidentiality of private information
- Helps you to ensure that the document or file has not been altered
- Encryption process also prevents plagiarism and protects IP
- Helpful for network communication (like the internet) and where a hacker can easily access unencrypted data.
- It is an essential method as it helps you to securely protect data that you don't want anyone else to have access.



Difference between Encryption and Decryption

Parameter	Encryption	Decryption
What is	It is a process of converting normal data into an unreadable form. It helps you to avoid any unauthorized access to data	It is a method of converting the unreadable/coded data into its original form.
Process	Whenever the data is sent between two separate machines, it is encrypted automatically using a secret key.	The receiver of the data automatically allows you to convert the data from the codes into its original form.
Location of Conversion	The person who is sending the data to the destination.	The receiver receives the data and converts it.
Example	An employee is sending essential documents to his/her manager.	The manager is receiving the essential documents from his/her employee.
Use of Algorithm	The same algorithm with the same key is used for the encryption-decryption process.	The only single algorithm is used for encryption and decryption with a pair of keys where each use for encryption and decryption.
Major function	Transforming humanly understandable messages into an incomprehensible and obscure form that can not be interpreted.	It is a conversion of an obscure message into an understandable form which is easy to understand by a human.

CHAPTER – 7

Program to Encrypt & Decrypt in C

What is Caesar Cipher Algorithm?

The Caesar Cipher algorithm is one of the oldest methods of password encryption and decryption system. It is popular by the following naming conventions:

- Caesar shift
- Caesar's cipher
- Shift cipher
- Caesar's code

This caesarc cipher encryption algorithm is a kind of substitution cipher wherein every character in the plain-text or the user input is replaced by another character which is defined with a fixed number of positions away from the existing character.

Caesar Cipher Encryption and Decryption Example

Input: ABCDEFGHIJ

Encrypted String: KLMNOPQRST

As you can find out from the encrypted string, we have moved every character's position by 10 towards the right. You can implement your own complex calculations as well.

However, this method cannot be implemented in real time systems for encrypting and decrypting strings as these are very easy to decode. In this method, every string character is replaced by a fixed value.

PROG -1

// Caesar Cipher Encryption and Decryption Program in C

```
#include<stdio.h>
#include<stdlib.h>
#include<string.h>
```

```
void decrypt(char arr[])
{
    int i;
    for(i = 0; i < strlen(arr); i++)
    {
        arr[i] = arr[i] + 10;
    }
}
```

```
void encrypt(char arr[])
{
    int i;
    for(i = 0; i < strlen(arr); i++)
    {
        arr[i] = arr[i] - 10;
    }
}
```

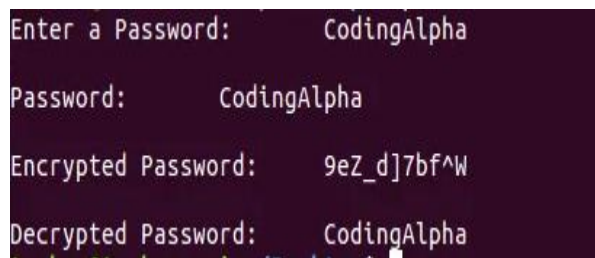
```
int main()
```

```

{
    char password[40];
    int ch;
    printf("Enter a Password:\t");
    scanf("%s", password);
    printf("\nPassword:\t%s\n",password);
    encrypt(password);
    printf("\nEncrypted Password:\t%s\n", password);
    decrypt(password);
    printf("\nDecrypted Password:\t%s\n", password);
    return 0;
}

```

OUTPUT of PROG-1



```

Enter a Password:      CodingAlpha
Password:      CodingAlpha
Encrypted Password:    9eZ_d]7bf^W
Decrypted Password:    CodingAlpha

```

PROG -2

//Simple C program to encrypt and decrypt a string

```
#include <stdio.h>
```

```
int main()
```

```

{
    int i, ch;
    char str[100];
    printf("\nPlease enter a string:\t");
    gets(str);
    do
    {
        printf("\nPlease choose following options:\n");
        printf("1 = Encrypt the string.\n");
        printf("2 = Decrypt the string.\n");
        printf("3 = exit ");
        scanf("%d", &ch);

        switch(ch)
        {
            case 1:
                for(i = 0; (i < 100 && str[i] != '\0'); i++)
                    str[i] = str[i] + 3; //the key for encryption is 3 that is added to ASCII value
                printf("\nEncrypted string: %s\n", str);
                break;
            case 2:
                for(i = 0; (i < 100 && str[i] != '\0'); i++)


```

```

        str[i] = str[i] - 3; //the key for encryption is 3 that is subtracted to ASCII value
        printf("\nDecrypted string: %s\n", str);
        break;
    default:
        printf("\nError\n");
    }
}while (ch<=2);
return 0;
}

```

OUTPUT of PROG-2

 DOSBox 0.74, Cpu speed: max 100% cycles, Frameskip 0, Program: TC

Please choose following options:

1. = Encrypt the string.
2. = Decrypt the string.
3. = exit

1

Encrypted string: kloor

Please choose following options:

1. = Encrypt the string.
2. = Decrypt the string.
3. = exit

2

Decrypted string: hello

Please choose following options:

1. = Encrypt the string.
2. = Decrypt the string.
3. = exit

3

Error

PROG -3

// WAP in c for Encryption

```
#include<stdio.h>
```

```
int main()
```

```
{
```

```
    char message[100], ch;
```

```
    int i, key;
```

```
    printf("Enter a message to encrypt: ");
```

```
    gets(message);
```

```
    printf("Enter key: ");
```

```
    scanf("%d", &key);
```

```
    for(i = 0; message[i] != '\0'; ++i)
```

```

{
    ch = message[i];
    if(ch >= 'a' && ch <= 'z')
    {
        ch = ch + key;
        if(ch > 'z')
        { ch = ch - 'z' + 'a' - 1; }
        message[i] = ch;
    }
    else if(ch >= 'A' && ch <= 'Z')
    {
        ch = ch + key;
        if(ch > 'Z')
        {
            ch = ch - 'Z' + 'A' - 1;
        }
        message[i] = ch;
    }
}
printf("Encrypted message: %s", message);
return 0;
}

```

OUTPUT of PROG-3

Enter a message to encrypt: axzd
Enter key: 4
Encrypted message: ebdh

PROG – 4

// WAP in c for Decryption

```
#include<stdio.h>
```

```

int main() {
    char message[100], ch;
    int i, key;
    printf("Enter a message to decrypt: ");
    gets(message);
    printf("Enter key: ");
    scanf("%d", &key);
    for(i = 0; message[i] != '\0'; ++i)
    {
        ch = message[i];
        if(ch >= 'a' && ch <= 'z')
        {
            ch = ch - key;
            if(ch < 'a')
            { ch = ch + 'z' - 'a' + 1; }
            message[i] = ch;
        }
        else if(ch >= 'A' && ch <= 'Z')

```

```

        {
            ch = ch - key;
            if(ch < 'A')
            { ch = ch + 'Z' - 'A' + 1; }
            message[i] = ch;
        }
    }
    printf("Decrypted message: %s", message);
    return 0;
}

```

OUTPUT of PROG - 4

Enter a message to decrypt: ebdh

Enter key: 4

Decrypted message: axzd

CHAPTER – 8

XOR key in C to Encrypt & Decrypt

Everything on a computer is stored as binary data, in the form of bytes (8 bits, or individual 1's or 0's)

Binary data can easily be "encrypted" with a "key" based on a little boolean operation called an xor, or exclusive or. XOR is a binary operator.

1 xor 1 = 0

1 xor 0 = 1

0 xor 1 = 1

0 xor 0 = 0

A	B	A XOR B
T	T	F
T	F	T
F	T	T
F	F	F

Ex: $4^3 = 7$

In binary 0100
 ^ 0011

 0111

Ex: $2^3 = 1$

 0010
 ^ 0011

 0001

PROG - 5

```

#include<stdio.h>
#include<conio.h>
void main()
{
    int c = 2^3;
    int d = 4^3;
}

```

OUTPUT of PROG-5

1
7

```

clrscr();
printf("\n%d",c);
printf("\n%d",d);

}

```

BINARY CODE

```

0 – 0000
1 – 0001
2 – 0010
3 – 0011
4 – 0100
5 – 0101
6 – 0110
7 – 0111
8 – 1000
9 – 1001
A – 1010
B – 1011
C – 1100
D – 1101
E – 1110
F – 1111

```

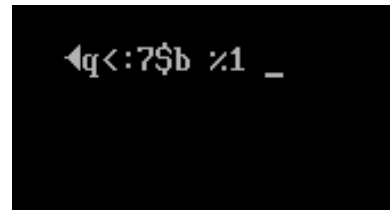
PROG - 6

```

#include <iostream.h>
int main()
{
    char string[11]="A nice cat";
    char key[11]="PQRSTABCDE";
    for(int x=0; x<10; x++)
    {
        string[x]=string[x]^key[x];
        cout<<string[x];
    }
    return 0;
}

```

OUTPUT of PROG-6



The program encrypts each character in the string using the ^ bit operator to exclusive-OR the string value with the key value for each character.

PROG - 7

```

#include<iostream.h>
#include<string.h>
using namespace std;
void XORChiper(char originalString[]) {
    char xorKey = 'T';
    int len = strlen(originalString);
    for (int i = 0; i < len; i++){
        originalString[i] = originalString[i] ^ xorKey;
        cout<<originalString[i];
    }
}
int main(){
    char sampleString[] = "Hello!";
    cout<<"The string is: "<<sampleString<<endl;
    cout<<"Encrypted String: ";
    XORChiper(sampleString);
    return 0;
}

```

Output

```

The string is: Hello!
Encrypted String: 188;u

```

PROG - 8

// C program to implement XOR - Encryption

```
#include<stdio.h>
```

```
#include<string.h>
```

```
void encryptDecrypt(char inpString[])
```

```
{
```

```
    // Define XOR key Any character value will work
```

```
    char xorKey = 'P';
```

```
    // calculate length of input string
```

```
    int len = strlen(inpString);
```

```
    // perform XOR operation of key with every character in string
```

```
    for (int i = 0; i < len; i++)
```

```
    {
```

```
        inpString[i] = inpString[i] ^ xorKey;
```

```
        printf("%c",inpString[i]);
```

```
    }
```

```
}
```

```
int main()
```

```
{
```

```
    char sampleString[] = "GeeksforGeeks";
```

```
    // Encrypt the string
```

```
    printf("Encrypted String: ");
```

```
    encryptDecrypt(sampleString);
```

```

printf("\n");

// Decrypt the string
printf("Decrypted String: ");
encryptDecrypt(sampleString);

return 0;
}

```

OUTPUT of PROG-8

Encrypted String: 55;#6?"55;#
 Decrypted String: GeeksforGeeks

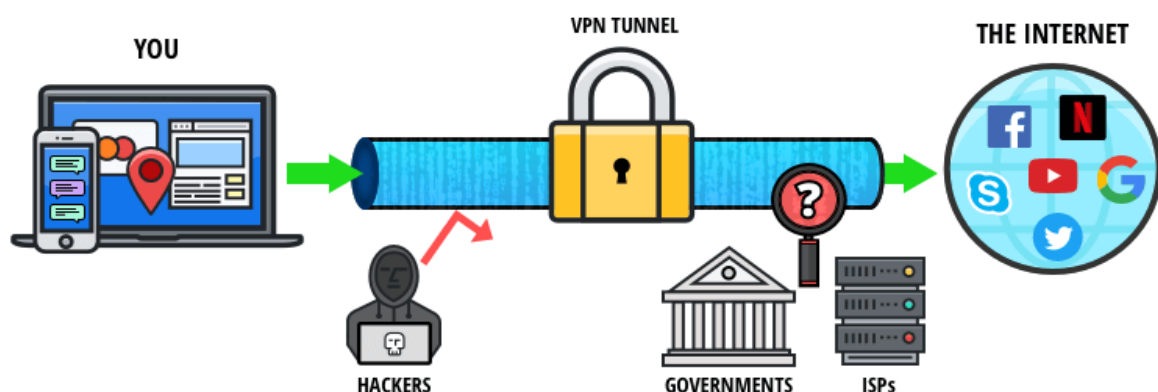
CHAPTER - 9

Virtual Private Network(VPN)

VPN stands for Virtual Private Network. It refers to a safe and encrypted network that allows you to use network resources in a remote manner. Using VPN, you can create a safe connection over a less secure network, e.g. internet. It is a secure network as it is completely isolated from rest of the internet. The government, businesses, military can use this network to use network resources securely.

How VPN Works

VPN works by creating a secure tunnel using powerful VPN protocols. It hides your IP address behind its own IP address that encrypts all your communication. Thus, your communication passes through a secure tunnel that allows you use network resources freely and secretly. This disguises your IP address when you use the internet, making its location invisible to everyone. A **VPN** connection is also secure against external attacks.



VPN protocols

There are several different VPN protocols that are used to create secure networks. Some of such protocols are given below;

- IP security (IPsec)

- Point to Point Tunneling Protocol (PPTP)
- Layer 2 Tunneling Protocol (L2TP)
- Secure Sockets Layer (SSL) and Transport Layer Security (TLS)

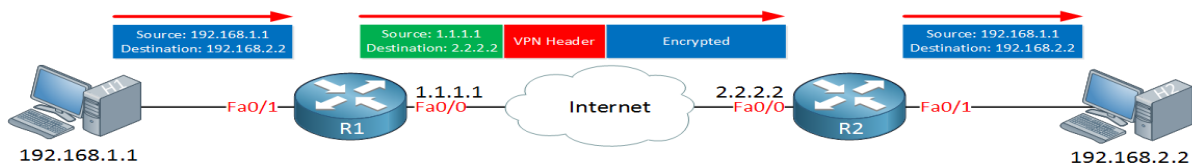
Types of VPN

- There are two common VPN types that we use:
 1. site-to-site VPN
 2. client-to-site VPN (remote access VPN)

1. Site-to-site VPN

With the site-to-site VPN, we have a network device at each site, between these two network devices we build a VPN tunnel. Each end of the VPN tunnel will encrypt the original IP packet, adds a VPN header, a new IP header and then forwards the encrypted packet to the other end of the tunnel.

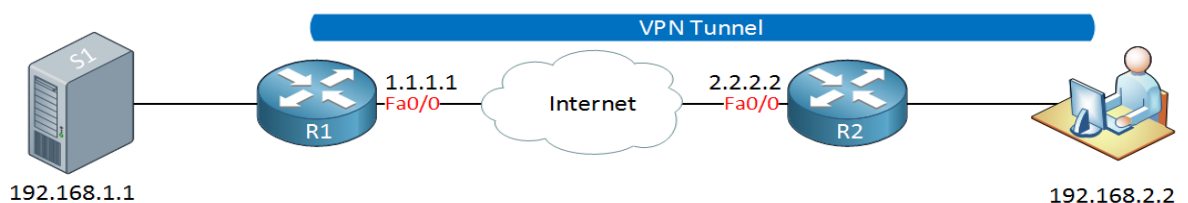
example of a VPN tunnel:



- H1 sends an IP packet with source 192.168.1.1 and destination 192.168.2.2.
- R1 encrypts the IP packet, adds a VPN header and creates a new IP header with its own public IP address as the source and 2.2.2.2 as the destination.
- R1 sends the new packet to R2.
- R2 receives the packet, checks if the packet really came from R1, decrypts it and forwards it to H2.
- H2 receives the original IP packet.

2. Client-to-site VPN

The client-to-site VPN is also called the remote user VPN. The user installs a VPN client on his/her computer, laptop, smartphone or tablet. The VPN tunnel is established between the user's device and the remote network device. Here's an example:



How to surf securely with a VPN

A VPN encrypts your surfing behavior, which can only be decoded with the help of a key. Only your computer and the VPN know this key, so your ISP cannot recognize where you are surfing. Different VPNs use different encryption processes, but generally function in three steps:

1. Once you are online, start your VPN. The VPN acts as a secure tunnel between you and the internet. Your ISP and other third parties cannot detect this tunnel.
2. Your device is now on the local network of the VPN, and your IP address can be changed to an IP address provided by the VPN server.
3. You can now surf the internet at will, as the VPN protects all your personal data.

Conclusion

In this lesson you have learned some of the basics of VPNs:

- VPNs can be used as an alternative to private WAN connections and offer a secure connection over an insecure medium, such as the Internet.
- VPNs offer features such as confidentiality, authentication, integrity and anti-replay.
- The two most common VPN types are site-to-site VPNs and client-to-site VPNs.
- Some common VPN protocols are:
 - IPSec: a framework that provides security on layer three of the OSI model.
 - PPTP: an old VPN protocol that uses PPP and GRE, insecure and should not be used anymore.
 - L2TP: a VPN protocol that tunnels layer two traffic, does not offer any encryption so should be used together with IPsec.
 - SSL VPN: uses SSL (HTTPS) to create a secure connection with the web browser.

CHAPTER - 10

Study of Hacking Tools

What is Hacking

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.

What is Hacker

A computer expert who does the act of hacking is called a "Hacker". Hackers are those who seek knowledge, to understand how systems operate, how they are designed, and then attempt to play with these systems.

Types of hackers

There are many different types of hackers, the most common of which are black, grey, and white hat hackers.

- ❖ Black hat hackers are the bad guys—the cyber criminals.
- ❖ White hat or ethical hackers are the good guys,
- ❖ Grey hat hackers are somewhere in the middle.

Other common hacker types include

- ❖ blue hat hackers, which are amateur hackers who carry out malicious acts like revenge attacks
- ❖ red hat hackers, who search for black hat hackers to prevent their attacks,
- ❖ green hat hackers, who want to learn about and observe hacking techniques on hacking forums.

❖ White Hat Hackers

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

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

❖ Black Hat Hackers

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

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

❖ Grey Hat Hackers

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

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

What is Ethical Hacking? How Legal is Ethical Hacking?

Ethical hacking refers to the actions carried out by white hat security hackers. It involves gaining access to computer systems and networks to test for potential vulnerabilities, and then fixing any identified weaknesses. Using these technical skills for ethical hacking purposes is legal, provided the individual has written permission from the system or network owner, protects the organization's privacy, and reports all weaknesses they find to the organization and its vendors.

Types of Hacking

We can segregate hacking into different categories, based on what is being hacked. Here is a set of examples –

- **Website Hacking** – Hacking a website means taking unauthorized control over a web server and its associated software such as databases and other interfaces.
- **Network Hacking** – Hacking a network means gathering information about a network by using tools like Telnet, NS lookup, Ping, Tracert, Netstat, etc. with the intent to harm the network system and hamper its operation.
- **Email Hacking** – It includes getting unauthorized access on an Email account and using it without taking the consent of its owner.
- **Ethical Hacking** – Ethical hacking involves finding weaknesses in a computer or network system for testing purpose and finally getting them fixed.
- **Password Hacking** – This is the process of recovering secret passwords from data that has been stored in or transmitted by a computer system.
- **Computer Hacking** – This is the process of stealing computer ID and password by applying hacking methods and getting unauthorized access to a computer system.

Advantages of Hacking

Hacking is quite useful in the following scenarios –

- To recover lost information, especially in case you lost your password.
- To perform penetration testing to strengthen computer and network security.
- To put adequate preventative measures in place to prevent security breaches.
- To have a computer system that prevents malicious hackers from gaining access.

Disadvantages of Hacking

Hacking is quite dangerous if it is done with harmful intent. It can cause –

- Massive security breach.
- Unauthorized system access on private information.
- Privacy violation.
- Hampering system operation.

- Denial of service attacks.
- Malicious attack on the system.

Purpose of Hacking

There could be various positive and negative intentions behind performing hacking activities.

- Just for fun
- Show-off
- Steal important information
- Damaging the system
- Hampering privacy
- Money extortion
- System security testing
- To break policy compliance

Different Hacking Tools used by Ethical Hackers

- **NMAP** : Nmap stands for Network Mapper. It is an open source tool that is used widely for network discovery and security auditing. Nmap was originally designed to scan large networks, but it can work equally well for single hosts. Network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.
- **Netsparker** : It is a dead accurate ethical hacking tool, that mimics a hacker's moves to identify vulnerabilities such as SQL Injection and Cross-site Scripting in web applications and web APIs. Netsparker uniquely verifies the identified vulnerabilities proving they are real and not false positives, so you do not need to waste hours manually verifying the identified vulnerabilities once a scan is finished. It is available as Windows software and online service.
- **Acunetix** : It is a fully automated ethical hacking tool that detects and reports on over 4500 web application vulnerabilities including all variants of SQL Injection and XSS. The Acunetix crawler fully supports HTML5 and JavaScript and Single-page applications, allowing auditing of complex, authenticated applications.
- **Metasploit**
- Metasploit is one of the most powerful exploit tools. It's a product of Rapid7 and most of its resources can be found at: www.metasploit.com. It comes in two versions – **commercial** and **free edition**. Metasploit can be used with command prompt or with Web UI.
- **Burp Suit**
- Burp Suite is a popular platform that is widely used for performing security testing of web applications. It has various tools that work in collaboration to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities. It is easy to use and provides the administrators full control to combine advanced manual techniques with automation for efficient testing.

Burp can be easily configured and it contains features to assist even the most experienced testers with their work.

- **Ettercap**
- Ettercap stands for Ethernet Capture. It is a network security tool for Man-in-the-Middle attacks. It features sniffing of live connections, content filtering on the fly and many other interesting tricks. Ettercap has inbuilt features for network and host analysis. It supports active and passive dissection of many protocols.
- You can run Ettercap on all the popular operating systems such as Windows, Linux, and Mac OS X.
- **LC4**
- LC4 was formerly known as **L0phtCrack**. It is a password auditing and recovery application. It is used to test password strength and sometimes to recover lost Microsoft Windows passwords, by using dictionary, brute-force, and hybrid attacks.
- LC4 recovers Windows user account passwords to streamline migration of users to another authentication system or to access accounts whose passwords are lost.

CHAPTER - 11

Study of Digital Signature

Introduction to Digital Signature

A digital signature is an electronic signature form used for authentication of the identity of the communicator or an authority signing the document. It ensures authenticity and originality of the content of the communication or the document. Digital Signatures remain unchanged throughout the communication or documentation, they are easily transportable and it cannot be imitated by anyone else. It also makes sure that the sender cannot deny the content sent via that signed document.

Understanding Digital Signature Certificate

Digital signature certificate can be better understood as the electronic alternative to physical or paper certificates such as driving license, PAN Card, passport, etc. Digital Certificates are proof of the identity of a person having a specified purpose. For example, a passport identifies a citizen's identity with relation to a nationality and that citizen is eligible to legally travel to any country on a grant of permission. Under these identity requirements, the digital certificate is used to electronically prove a citizen's identity and helps access to information or services via the internet or other electronic mediums or to sign documents digitally.

Need for a Digital Signature Certificate?

A digital signature certificate is a convenient way to authenticate an identity electronically with a high level of security for online transactions while safeguarding one's privacy of information shared via Digital Signature Certificate. These certificates are used to encrypt data in a way that only the desired recipient can have access to it. The digitally signed information also ensures that it remains unchanged throughout the process of digital transfer as well as verifying the identity of the sender of the message. **DSC is required bcoz** Physical documents are signed manually, similarly, electronic documents, for example e-forms are required to be signed digitally using a Digital Signature Certificate.

Purchasing a Digital Signature Certificate / Who issue DSC

Legally validated Signature Certificates can only be issued by the Controller of Certifying Authority (CCA), Government of India licensed Certifying Authority (CA) as per the requirement of an individual as well as organizational needs. A licensed Certifying Authority (CA) issues the digital signature. Certifying Authority (CA) means a person who has been granted a license to issue a digital signature certificate under Section 24 of the Indian IT-Act 2000.

Digital signatures are not to be confused with digital certificates. A digital certificate is an electronic document that contains the digital signature of the issuing CA. It binds together a public key with an identity and can be used to verify that a public key belongs to a particular person or entity

Applications of Digital Signature

- To send and receive encrypted emails, that are digitally signed and secured
- To carry out secure online transactions
- To identify participants of an online transaction
- To apply for tenders, e-filing with Registrar of Companies (MCA), e-filing of income tax returns and other relevant applications
- To sign and validate Word, Excel and PDF document formats

Classes & Types of Digital Signature Certificate

There are 3 types of Digital Signature Certificates, namely :- Class-1, Class-2 and Class-3.

Each has its own level of security and is meant for a particular category of professional and or sector of industry

Different Classes and Types of digital signatures

There are three different classes of digital signature certificates (DSCs):

- **Class 1. This** certificates shall be issued to individuals/private subscribers. It cannot be used for legal business documents as they are validated based only on an email ID and username. Class 1 signatures provide a basic level of security and are used in environments with a low risk of data compromise.
- **Class 2.** This certificates will be issued for both business personnel and private individuals use. It Often used for electronic filing ([e-filing](#)) of tax documents, including income tax returns and goods and services tax (GST) returns. Class

2 digital signatures authenticate a signer's identity against a pre-verified database. Class 2 digital signatures are used in environments where the risks and consequences of data compromise are moderate.

- **Class 3.** This certificate will be issued to individuals as well as organizations. The highest level of digital signatures, Class 3 signatures require a person or organization to present in front of a certifying authority to prove their identity before signing. Class 3 digital signatures are used for e-auctions, e-tendering, [e-ticketing](#), court filings and in other environments where threats to data or the consequences of a security failure are high.

Digital Signature is an USB type dongle which looks like a pendrive.

For class 2 requirement documents are

- PANCARD
- AADHAR CARD
- PHOTO
- EMAIL – ID
- MOBILE NO.



It is used for multipurpose like for Trademark, for GST, for Income Tax, for EPF, for TDS return, director kyc , for document signer, for pdf signer

For class 3 requirement documents are

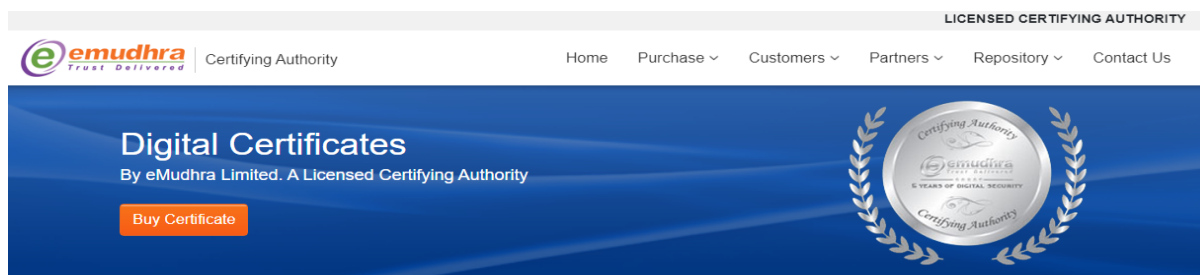
- PANCARD
- AADHAR CARD
- PHOTO
- EMAIL – ID
- MOBILE NO.
- BANK STATEMENT
- INCOME TAX RETURN
- OTHER DOCUMENTS

It is used for E-Tender, E-Ticketing , For Foreign Trade

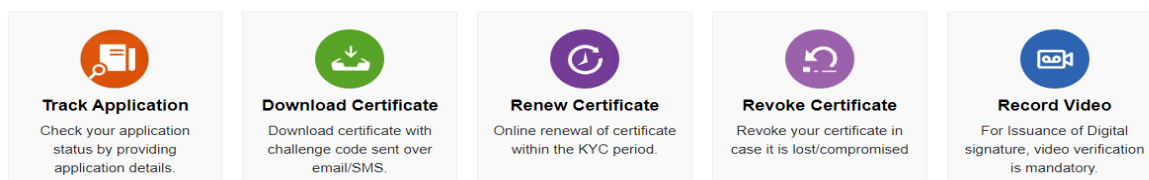
How to get a DSC.

The [s \(CCA\)](#) under the Ministry of Electronics & IT has authorised certain certifying authorities to issue digital signature certificates. You can find the full list of licensed certifying authorities on the [CCA website](#). For example :

Open the google -> open <https://www.e-mudhra.com/>



eMudhra Limited is a Certifying Authority licensed by Controller of Certifying Authorities, under Government of India. eMudhra operates under the guidelines set by Information Technology Act. With more than one million certificates issued, eMudhra caters to all kinds of subscribers who use Digital Certificates for Income Tax, MCA (ROC), Tenders, Foreign Trade, Banking, Railways and many other needs.



To fill in the Application form log in to the website of the Licence Certifying Authority.

Steps to apply for a Digital Signature Certificate

STEP 1: Log on and select your type of entity

Log on to the website of a Certifying Authority licensed to issue Digital Certificates in India. Having accessed the page, you will be guided to the Digital Certification Services' section. Now under the 'Digital Certification Services' section, click on the type of entity for which you want to obtain the DSC: 'individual or organization', etc. In case you are applying for an individual DSC, click on 'individual'. A new tab containing the DSC Registration Form will appear. Download the DSC Registration Form on your PC.

STEP 2: Fill the necessary details

Once you have downloaded the form, fill in all the necessary details as required in the form:

- Class of the DSC.
- Validity.
- Type: Only Sign or Sign & Encrypt.
- Applicant Name & Contact Details.
- Residential Address.
- GST Number & Identity Details of Proof Documents.
- Declaration.
- Document as proof of identity.
- Document as proof of address.
- Attestation Officer.
- Payment Details.

On filling up all the necessary details you must affix your recent photograph and put your signature under the declaration. Check thoroughly for completion of the form. Take a print of the completed form and preserve it.

STEP 3: Proof of identity and address

The supporting document provided as proof of identity and address must be attested by an attesting officer. Ensure the sign and seal of the attesting officer is visibly clear on the supporting proof documents.

STEP 4: Payment for DSC

A demand draft or cheque must be obtained towards payment for application of DSC in the name of the Local Registration Authority where you are going to submit your application for verification. You can find the details of the Local Registration Authority according to your city of residence by searching for a Certifying Authority licensed to issue Digital Certificates online.

STEP 5: Post the documents required

Enclose the following in an envelope:

- DSC Registration Form duly completed -Supporting document for Proof of Identity and proof of address attested by the attesting officer.
- Demand Draft/Cheque for payment.

Address the enclosed envelope to the Local Registration Authority (LRA) and post it to the designated address of the LRA for further processing.

On completion of the above-mentioned steps by filling in the DSC Form and providing necessary documents and payment, you have successfully completed the application process for your Digital Signature Certificate.