INDEX

EXPERIMENT-1

AIM OF EXPERIMENT:

Introduction to Network Security.

1(a) What is network security:-

Ans- Network security is a set of technologies that protect the usability and integrity of a companyintrastructure by preventing the entry of proliferation with in a network of a wide variety potential threats.

1(b) Whynetwork security is essential?

Ans-Network security is essential because network security is critical because it prevents cyber criminal from gaining access to valuable data and sensitive information.

- When hachers get hold of such data they can cause a verify of problems including identify theft stolen assets and reputational harm.

1(c) what are the basic principle of network security?

Ans-Network security is essential because network security is critical because it prevents cyber criminal from gaining access to valuable data and sensitive information

- Depending upon the application and context there are 3 principle and one of these principle of might be more important than others.

i) Confidentiality:-

- The degree of confidentiality determine the secure of information. The principle specify that only the sender and receiver will be able to access the information shared between them.
- Confidentiality comprises if an authorized person is able to access a massage .

ii) Authentication:-

- Authentication is the mechanism to identify the user or system or the entity .
- It ensure the identify of the person drying to access the information .
- The authentication is mostly secured by using username and password .
- The authorized person whose identify and can access sensitive information.

iii) integrity:-

- Integrity gives the assurance that the information received is exact and accurate .
- If the content of the message is changed after the sender sends it but before reaching the intended receiver , then it is said that the integrity of the message is lost .

1(d) What are the types of network security available?

Ans – Types of network security:-

There are various types of network securities .

These securities are:- i) Access control :-It ensures that only a handful of authorized personnel must be able to work with the allowed amount of resources.

ii) Antivirus and Anti-malware software :-

It ensure that any malicious software dose not enter the data . The malicious software like viruses ,Trojans and worms is handled by the same.This ensure that not only the entry of the malwares protected but also that the system is well equipped to fight once it has entered.

iii) Cloud Security:-

Now a day , lot many organizations are joining handle with cloud technology where a large amount of important data is stored over the internet. This is very vulnerable to the malpractices that few unauthorized dealers might. Pertain this data must be protected and it should be ensured that this protection is not jeopardized by anything many business embrace saas application for providing some of their employees the allowance of accessing the data stored over the cloud. This type of security ensures creating gaps in the visibility of the data.

EXPERIMENT-2

AIM OF THE EXPERIMENT: -

Introduction to computer virus.

2(a) what is computer virus?

- Computer virus is a program.
- Sometimes it may help to secure our data or sometimes it harm our computer or data.
- Virus can be transmitted through a host.
- The host can be CD & different USB devices or internet.

2(b) what is virus types of virus?

I. Boot sector virus :
   - This virus is loaded when booting process is initiated.
   - Ex – Disk-killer

II. Program virus :
   - It infects during the execution of program this virus is loaded in the memory execution of files.
   - Ex – Cascade

III. Macro virus :
   - Infects the document gets transmitted from one file to another file.
   - Ex – word concept

IV. Multi positive virus :
   - This virus infects the boot record when system booted next time it will not allow to load.
   - Ex – flip

V. Polymorphic virus :
   - This virus is capable of encrypting code which are difficult to crack.
   - Ex – Cascade, virus.101

VI. Stealth virus :
   - This virus uses technique to occupy large space in device.
   - Ex –whale

2(c) what are various technique of virus detection?

- Program will not run.
- Computer takes a lot of time to boot.
- settings are done automatically.
- File and folder may not open.

2(d) what are various method of virus prevention?

- Load antivirus.

- Always scan the external devices before opening.
- Do not open unknown mails.

2(e) what is anti-virus?

- Antivirus is a kind of software used to prevent, scan, delete, viruses from a computer.
- Once installed most antivirus software runs automatically in the background to provide real time protection against virus attacks.

EXPERIMENT-3

AIM OF THE EXPERIMENT:-

Study of various Anti-virus softwares available in indian market.

3a) Quick Heal total security:

Quick Heal antivirus provide all round protection for your PC against digital threats and all other kinds of cyber threats it is tough on viruses, light on your PC.

Features:

- Ransomware Protection
- Virus protection
- safe Banking
- Anti-malware
- File vault
- anti-tracher

3b) 360 Total Security:

360 total security is powerful program that keeps your PC protected and optimized it includes many tools to improve your computer performance to help you free space or to protected your system . If you running a program you are not sure wheather it contains malware or not.

Feature:

- Virus scan
- Speed up manages
- Router manager
- Browser protection
- Sand Box
- Firewall

3c) MCAFEE Total protection:

Get continuous protection from phising viruses, hackers and ransomware. Your security also include alerts before connecting to risky websites.

Features:

- VPN
- Firewall

- Password manager
- Anti-Spam
- Home-Network analyzer

3d) NORTON 360 standard plan:

Norton anti-viruses is an anti-virus or anti-malware software product founded by peter Norton developed and distributed by gen digital since 1990 as a part of its Norton family of computer security products.It uses signatures and hecuristics of identity viruses.

Features:

- Anti-Spyware
- Secure VPN
- Safe CAM/ webcam protection
- Dark web monitoring.

3e) AVTRA:

AVTRA Operations Gmbtt is a German multinational computer security software company mainly known for their Avira free security anti-virus software. Avira was founded in 2006 but the antivirus application has been under active development since 1986 through its predecessor company +1+BEDV DatentechnikGmbtt.

Features:

- Virus scanner & cleaner
- Fast VPN
- System optimizer
- Identify protection

3f) Bitdefender Anti-virus plus:

Bitdefender is a Romanian cyber security technology company headquartered in Bucharest, Romania, with offices in the United States. Europe, Australia and middle East.

The company was founded in 2001 by current LED and main share holder, florin talpes.

Features:

- Device Optimizer
- Privacy firewall
- Parental control
- Protection against malware
- Protection for every OS(widows, Macros, Android+ios)

3g) Kaspersky Antivirus:

Kaspersky antivirus is a proprietary antivirus program developed by Kaspersky lab. It is designed to protect users from malware and is primarily designed for computer running Microsoft windows and macos, although a version for linux is available for business consumers.

Features:

- Functional encryption for safe payment transactions on PC and mac.
- Private browsing
- Ad & adult content blocker
- System Optimizer
- VPN

3h)Trend Micro:

Trend micro is an American Japanese multinational cyber security s/w company with global headquarters in Tokyo, Japan, Texas, United States, other regional Head quarters and R+D centre are located around East Asia, southeast Asia, Europe & North America.

Features:

- Security Risk protection
- Office scan firewall
- Web reputation

- Damage cleanup services
- Anti-spyware

3i)AVG:

AVG antivirus is a line of antivirus software developed by AVG technologies, a subsidiciary of Avast a part of Gen Digital. It is available for windows macos and Android.

Features:

- System performance scan
- Fake website protection
- Webcam protection
- Real-time protection
- Antitheft phone tracher

3j)AVAST:

AVAST Free antivirus s/w defect, blocks and removes all types of malware, viruses, spyware Trosans and more. You'll also get security for yours wi-fi network and real-time defence against phising attacks unsafe websites and other threats to your devices.

Features:

- Webcam protection
- Website protection
- Document protection
- Advanced firewall protection
- Information breach monitoring.
- AIM OF THE EXPERIMENT :-
- Installation of anti-virus software.
- STEP 1:
- If you brought anti-virus software on a CD or DVD from a store. You must first put the CD or DVD into your computer's disc drive. However ,you can also get the program setup in your USB drive on pen drive. When you install process, a window will open that guides you, and the installation process should start automatically.
- STEP 2:
- If you did not buy a CD or DVD and instead downloaded an antiviruses application from the internet you must now locate the downloaded file on your computer. If you downloaded the Zipfile for the program setup, you are required to unzip the file to access the installation files. Then, find the file that has a name like install exc, setup exc or a similar name, and double click on that file tom start the

- installation process of the antivirus program. When you install the program, through the install process, a window will open that guides you and the installation process should start automatically.
- STEP 3:
- Follow the steps for installing the antivirus program in the installation process window. The recommended options are provided by the install process, which helps the antivirus program to work properly. There is one exception that the install process recommends installing any helpful program for your computer or any toolbar for the internet browser. Whenever you are installing an antivirus program you need to decline the install of those other program or uncheck all boxes. Also, the anti-virus program does not require any additional software to install and successfully on the computer.

STEP 4:

- Close out the install window when you have completed the installation process of an anti-virus.
- STEP 5:
- If you installed the software with a CD or DVD remove it from the computer's disc drive.
- After following all the above steps, the anti-virus program will be installed successfully and ready to use. Restart your computer system. However it is not required. However if you restart he computer, any changes to the operating system will be applied appropriately.

EXPERIMENT-4

AIM OF THE EXPERIMENT :-

Installation of anti-virus software.

STEP 1:

If you brought anti-virus software on a CD or DVD from a store. You must first put the CD or DVD into your computer's disc drive. However, you can also get the program setup in your USB drive on pen drive. When you install process, a window will open that guides you, and the installation process should start automatically.

STEP 2:

If you did not buy a CD or DVD and instead downloaded an anti viruses application from the internet you must now locate the downloaded file on your computer. If you downloaded the Zip file for the program setup, you are required to unzip the file to access the installation files. Then, find the file that has a name like install exc

Setup exc or a similar name, and double click on that file tom start the installation process of the antivirus program. When you install the program, through the install process, a window will open that guides you and the installation process should start automatically.

STEP 3:

Follow the steps for installing the antivirus program in the installation process window. The recommended options are provided by the install process, which helps the antivirus program to work properly. There is one exception that the install process recommends installing any helpful program for your computer or any toolbar for the internet browser. Whenever you are installing an antivirus program you need to decline the

install of those other program or uncheck all boxes. Also, the anti-virus program does not require any additional software to install and successfully on the computer.

STEP 4:

Close out the install window when you have completed the installation process of an anti-virus.

STEP 5:

If you installed the software with a CD or DVD remove it from the computer's disc drive.

After following all the above steps, the anti-virus program will be installed successfully and ready to use. Restart your computer system. However it is not required. However if you restart he computer, any changes to the operating system will be applied appropriately.

EXPERIMENT-5

AIM OF THE EXPERIMENT:

Comparison of various Anti-virus software studied in experiment no.3 .

Various types of Anti-virus software :-

(a) quick heal total security
(b) 360 total security
(c) MCAFEE total protection
(d) NORTON 360 standard plan
(e) AVTRA
(f) Bit defender Anti-virus plus
(g) Kaspersky
(h) Trend micro
(i) AVG
(j) AVAST

FUNCTION	(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)	(i)	(j)
1)Ransom ware protection	✔									
2) Virus scan/ protection	✔	✔			✔					
3) Secure VPN			✔	✔	✔		✔			
4) Dark web monitoring				✔						
5) System optimizer					✔					
6) Firewall protection		✔	✔			✔		✔		✔
7) Private browsing							✔			
8) Anti-software			✔	✔		✔		✔		
9) Damage-cleanup services								✔		
10) Web cam protection				✔					✔	✔
11) Antitheft phone tracker									✔	
12) Safe banking	✔						✔			
13) Browser protection		✔					✔			
14) Website protection									✔	✔
15) Information breach monitoring										✔

EXPERIMENT-6

AIM OF THE EXPERIMENT:-

Study about firewall.

(a)Introduction of firewall:

A firewall is a network security device, either. hardware or software-based ,which monitors all incoming and outgoing traffic. Based on a defined set of security rules it accepts ,rejects or drops that specific traffic.

(b)Importance of firewall:

(i)Monitoring network traffic.

(ii)Source or destination-based blocking of incoming Networking traffic.

(iii)Outgoing network traffic can be blocked based on the source or destination.

(iv)Block network traffic based on content.

(v)Report on network traffic and firewall activities.

(vi)Stops virus attacks and spyware.

(vii) Preventing hacks.

(viii) Promotes privacy.

(c)Basic working principle:

Allow internal users to access external www servers, but not allow external users to access our internal server.

(d) Functions of firewall.

i)Network threat prevention.

ii) Application and identity based control.

iii) Hybrid cloud support.

IV) Scalable performance.

v)Access validation.

vi) Network traffic management &control.

vii) Record report on events.

(e) Limitation of firewall:

i) Firewall cannot stop users from accessing malicious websites ,making it vulnerable to internet threats or attacks.

ii) It cannot protect against the transfer of virus infected files or software.

iii) It cannot prevent misuse of passwords.

iv) It cannot protect against non technical security risks , such as social Engineering.

v)It cannot protect if security rules are misconfigured.

vi)It cannot stop or prevent attackers with modems from dialing into or out of the internal network.

vii)It cannot secure the system which is already infected.

EXPERIMENT-7

AIM OF THE EXPERMENT-:

Study about various firewall delivary method?

(1)Hardware based firewall:

A hardware based firewall is an appliance that acts as a secure gateway bet device inside the network perimeter and those outside it.Because they are self –contained application ,hardware based firewalls don't consume processing power or other resources of the host device.

Sometimes it called network based firewall,these application are ideal for medium and large for medium and large organizations looking to protect many device, Hardware

based firewall require more knowledge to configure and manage then their host based counter parts .

(2)Software based firewall:

A software beased firewall or host firewall runs on a server or other device ,Host firewall software needs to be installed on each device requiring protection .As such software based firewall consume some of the host device cpu and ram resources .

Software based firewall provide individual device significant protection against viruses and other malicious content .They can discern different program running on the host,while filtering inbound and outbound traffic .this provid a finegranied level if control ,making it possible to enable communication do/from one program but prevent it to /form another .

(3)Cloud /hosted firewalls:

Managed security sevice providers (MSSPS) offer cloud based firewall .This hosted service can be configured to track both internal network activity and third party on demand environments .

Alos known as firewall as a service ,cloud based firewall can be entirely managed by an MSSP ,making it a good option for Aarge or highly distributed enterprises with gaps in security resources .cloud .based firewall can also be benefical to maller organization with limited staff and expertise.

EXPERIMENT-8

AIM OF THE EXPERIMENT:

Study about parameters of firewalls.

Parameter of Firewalls:-

I. Block by default :

Block all the traffic by default and explicitly enable only specific traffic to known services. You achieve this behavior by configuring the last rule in an access control list to deny all traffic. You can do this explicitly or explicitly, depending on the plat from.

II. Allow specific traffic:

The rules that you use to define network access should be as specific as possible. This strategy is the principle of least privilege.

A layer 4 firewall was the following parameter for an access rule:-

1. Source IP addresses (or range of IP addresses)
2. Destination IP addresses (or range of IP addresses)
3. Destination port (or range of ports)
4. Protocol of the traffic (TCP,ICMP,OR UDP)

a) Specify source IP address:

If the service should be accessible to everyone on the in internet, then the any source IP addresses.is the correct option. The Following is a list of common server management ports and database ports

Server management ports:

1. Linux ssh:port22
2. Windows RDP :port3389

Database ports:

1. SQL server:port1433
2. Oracle:port1521
3. My SQL:port2206

Be specific about who can reach these ports

b) Specify the destination IP address:

The destination IP address is the IP address of the server that runs the service to which you want to enable access. Always specify which server or servers are accessible configuring value of any could lead to a security breach.

c) Specify the destination port:

The destination port corresponds to the accessible service. This value of this field should never be any.

d) Examples of dangerous configuration:
   1. Permit if any allows all traffic from any source on any port to any destination. A good rule would be permitting tip any WEBSERMER1 http.
   2. Permit if any WEB-server1- allows all traffic from any source to web serve. A good rule would be permit if any WEB-SERVER1 http.
   3. Permit up tip any WEB-SERVER 3389-allows RDP access from any source to the Web server. A good rule would be –permit tip 12.34.56.78.3389 WEB-SERVER1 where 12.34.56.78 is the IP addresses of the administrators computer on the internet.
   4. Permit tip from any source to the database. A good rule would be-permit tip 23.45.67.89 DB-SERVER13306 (where 23.45.67.89 is the IP address of the host on the internet that needs access to the database).

EXPERIMENT-9

AIM OF THE EXPERMENT-9

Study about various type of firewalls.

Types of network firewalls:-

(1) Packet filters:

It is a techniques used to control network access by monitoring outgoing and incoming packets and allowing them to pass or halt based on the source and destination internet protocol address , protocols and port. This firewall is also known as a static firewall.

(2) Stateful inspection firewalls:

It is also a type of packet filtering which is used to control how data packets move through a firewall. It is also called dynamic packet filtering .These firewalls can inspect that if the packet belongs to a particular session or not. It only permits communication if and only if the session is perfectly established between two end points else it will block the communication.

(3) Application layer firewalls:

These firewalls can examine application layer information like an HTTP request. It finds some suspicious application that can be responsible for harming our network or that is not safe for our network then it gets blocked right away.

(4) Next generation firewalls:

These firewalls are called intelligent firewalls. These firewalls can perform all the tasks that are performed by the other types of firewalls that we learned previously but on top of that it includes additional features like application awareness and control, integrated intrusion awareness and control, integrated intrusion prevention and cloud delivered threat intelligence.

(5) Circuit level gateways:

A circuit level gateway is firewall that provides user datagram protocol (UDP) and transmission control protocol (TCP) connection security and works between an open systems interconnection (OSI) network models transport and application layers such as the session layer

(6) Software firewall:

The software firewall is a type of computer software that runs on our computers. It protects our systems from any external attacks such as unauthorized access , malicious attacks etc. by notifying us about the danger that can occur if we open a particular mail or if we try to open a website that is not secure.

(7)Hardware firewall:

A hardware firewall is a physical appliance that is deployed to enforce a networking boundary pass through this firewall, which enables it to perform an inspection of both inbound and outbound network traffic and enforce access controls and other security policies.

(8)Cloud firewall:

These are software based cloud deployed network devices. This cloud based firewall protects a private network from any unwanted access. Unlike traditional firewalls, a cloud filterdata at the cloud level.

EXPERIMENT-10

AIM OF THE EXPERIMENT: -10

Study about firewall configuration.

(1) Secure the firewall:-

Securing a firewall is the vital firststep to ensure only authorized administration haveaccess to it.

This includes action such as:-

- Update with the latest firmware.
- Never putting firewalls into production without appropriate configuration in place.
- Deleting, disabling or renaming default accounts and changing default passwords.
- Never using user accounts must have limited privileges based on individual responsibilities.
- Use unique, secure passwords.
- Disabling the simple Network Management protocol (SNMP),which collects and organizes information about devices on IP networks, or configuring it for secure wage.
- Restricting outgoing and incoming network traffic for specific applications or the TCP.

(2)Establish firewall zones and on IP address structure

It is important to identify network assets and resources that must be protected. This includes creating a structure that groups corporate assets into zones based on similar functions and the level of risks.

A good example of this is servers such as email servers, Virtual Private Network (VPN)servers, and web servers placed in a dedicated zone that limits inbound internet traffic, often refer advised to as a demilitarized zone (DMZ).

A general rule is that the more zones created the more secure the network is.

(3)Configure access control lists (ACLs):-

ACLs enable organizations to determine which traffic is allowed to flow in and out of each zone. ACLs act as firewall rules, which organizations can apply to each firewall interface and sub interface.

ACLs must be made specific to the exact source and destination port numbers and IP addresses. Each ACL should have a “deny all” rule created at the end of it;

which enables organizations to filter out unapproved traffic. It is also advisable to disable firewall administration interfaces from public access to protect the configuration and disable unencrypted firewall management and protocols.

(4)Configure other firewall services and logging:-

Some firewalls can be configured to support other services, such as DHCP sever, intrusion prevention system (IPS), and Network Time Protocol (NTP) server. It is important to also disable the extra services that will not be used.

Further, firewalls must be configured to report to a logging service to comply with and fulfill payment card industry data security standard (PCI DSS) requirements.

(5) Test the firewall configuration:

With the configuration made, it is critical to test them to ensure that correct traffic is being blocked and that the firewall performs as intended. The configuration can be tested through techniques like penetration testing and vulnerability scanning. Remember to back up the configuration in a secure location incase of any failures during the testing process.

(6)Manage firewall continually:-

Firewall management & monitoring are critical to ensuring that the firewall continues to function as intended. This includes monitoring logs, performing vulnerability scans and regularly reviewing rules, it is also important to document processes and manage the configuration continually and diligently to ensure ongoing protection of the network.

EXPERIMENT-11

AIM OF THE EXPERIMENT:-

Study about the Cryptography.

(a)Introduction to Cryptography:-

Cryptography is the study and practice of technique for secure communication in the presence of third parties called adversaries.It deals with developing and analyzing

protocols that prevents malicious third parties from retrieving information being shared between two entities there by following the various aspects of information security.

(b)Plain text:-

Plain text is any text, text file or document containing only text in ordinary readable format.

(c)Cipher text:-

Cipher text is a series of randomwised letters or numbers which cannot be easily deciphered without the key.

(d)Substitution technique:-

The substitution technique involves replacing letters with other letters and symbols. In simple terms, the plaintext characterare substituted and additional substitute letters numerals and symbols are implemented in their place.

(e)Transposition Technique:-

In this transposition technique, the characters identities are kept the same, but their positions are a hered to produce the cipher text. A transposition cipher in cryptography is a types of encryption that scrambles the locations of characters without altering the characters themselves.

(f)Encryption:-

Data encryption is a computing process that converts plain text or human-readable data into cipher text that is accessible only lay authorized users with the right cryptographic key. Simply put encryption converts readable data into a form that only people with the right password can decode and view.

(g) Decryption:-

Decryption is the process of transforming data that has been rendered unreadable through encryption back to its unencryption form.

EXPERIMENT-12

AIM OF THE EXPERIMENT:-

Difference between substitution Technique and Transposition Technique.

Feauture	**Substitiution Technique**	**Transposition Technique**
Definition	It replaces the plainted characters with other numbers, characters and symbols.	It scrambles the characters position in the plain text.
Alternations	The characters identify is changed , while its position does not change.	The characters position is changed instead of its identity.
Forms	It utilizes the monoalphabetic, polyalphabetic substitution cipher, and play fair cipher.	It utilizes the keyed and keyless transpositional ciphers.
Detection	The low frequency letter may easily identify the plaintext.	The keys close to the right key lead to the discovery of the plaintext.
Examples	Cacscr ciphar	Rail fence ciphar

EXPERIMENT-13

AIM OF THE EXPERIMENT: -

Study about various types of Cryptography

(i)Symmetric key cryptography:

Symmetric key Cryptography is a type of cryptography in which the single common key is used by both sender and receiver for the purpose et encryption and decryption of message. This system is also called private or secret key cryptography and AES (Advanced encryption system) is the most widely uses symmetric key cryptography. Types: AES, DES, Triple DES, RCD, RCY, RCD, IDEA Blow fish, stream cipher, Block cipher etc. are the types of symmetric key cryptography.

(ii) Asymmetric key Cryptography:

Asymmetric key Cryptography is completely diff. and a more secure approach than symmetric key cryptography.In this system every user less two keys or a pair of

keys (Private keys & Public key) for encryption and decryption process. Private key is kept Private key as a secret than every user and public key is distributed over the network if anyone wants to send message to any user you can use public keys of the intended recipient.

TYPES:

RSA, DSA, RKS, Elliptic curve technique etc. Are the common types of asymmetric key cryptography.

(iii)Hash function:

A Hash function is cryptography algorithm that takes input of arbitrary length and gives the output in fixed length. The hash function is also considered as a mathematical equation that takes numeric input and produce the output that is called hash ore message digest. This system operates in one-way manner and doesn't require any key. Also, it is considered as the building blocks of modern cryptography.

The hash function works in a way that it operates on two blocks of fixed length binary data and then generate hash code.

Types:

Message Digest 5 (MD5), SHA(Secure Hash Algorithm), RIPEMD and whirlpool etc.

EXPERIMENT-14

AIM OF THE EXPRIMENT:-

Write a program in c to perform encryption using XOR key.

Code:

```
#include<io stream>
#include<string.h>
Using name space std;
Void XOR ciphers(char original string[])
{
        Char XOR key='T',
        Intlen=strlen (original String);
        For(i=0;i<len;i++)
                {
                        Original String [i] = original String[i]^XOR key;
                        Count<<origional String[i];
                }

}
Intmain()
{

        Char sample String[]="Hello!";
        Count<<"The String is:"<<Sample String<<end1;
        Count<<"Encrypted String:";
        XOR chipher (Sample String);
        Return 0;
}
```

OUTPUT:-

The String is :Hello!

Encrypted Sting :188;u

AIM OF THE EXPERMENT:-

Write a program in C to perform decryption using XOR key.

Code:

```
#include<iostream>
#include<string.h>
Using namespace std;
void encrypt Decrypt (char inpstring [])
{
        char XOR key='p';
        int ten=strlen (inpstring);
        for(int i=0;i<len;I++)
        {
                Inpstring [i]=inpstring[i]^XOR key;
                Printf("%C", inpstring[i]);
        }
}
Intmain()
{
Char sample string[]="GeeksforGeeks";
Printf ("Encrypted String:");
Printf("\n");
Printf("Decrypted string:");
Return 0;
}
```

OUTPUT:

Encrypted string:55;#6?"55;#

Decrypted string: GeeksforGeeks

EXPERIMENT-16(A)

AIM OF THE EXPERIMENT:-16(A)

Study about VPN.S

INTRODUCTION TO VPN:

VPN stands for virtual Private network. It provides inline privacy and anonymity by building private Network from a public building a private Network from a public internet connection. VPN masks yourinternet protocol address so your online actions are virtually untraceable. VPN creates a virtual tunnel to transfer to data

"A VPN creates an encrypted tunnel to protect your personal data and communications, hide your IP address and lot you safely use public networks. Moreover, the privacy and securing provided by VPIN are fare better the Wi-Fi hotspots

FEATURES OF VPN:

- VPN provides platefulserver location.
- It also provides anonymous DNS servers.
- VPNare generally cost-effective.
- VPN supportsrouter.
- The VPN is highly encrypted and secure Along with VPN we get sequence VPN Protocols.
- It provides safely against DNS Leak.

APPLICATION VPN:

- VPN can easily bypass geographic restrictions on websites. ore streaming audio and video.
- Using a VPN we can protect ourselves from shopping from up trustworthyWi-Fi hotspots.
- one can gain privacy online by hiding one's true Location
- One can protect themselves from being logged whiletormenting

WHAT DOES A VPN HIDE?

- User's Browsing History
- User IP address and location.
- User's device
- User's web activity- to preserveinternet -freedom.

ADVANTAGESOFVPN:

- It provides you Anonymity.
- It avoids the Geo-Restriction.
- It provides securityprotection fromcyber- attacks.
- It will prevent bandwidth in throttling.
-

- It will help you to improve gaming experience.
- It has capability to by-pass It has Pire wall.

DISADVANTAGES VPN:

- It can slow down the internet speed.
- It has privacy Issues.
- It might be connection droppings while you connected over VPN.
- It might have configuration difficulties.
- It has legality issues.
- AIM OF THE EXPERIMENT:-
- Study about types of VPN.
- i)Remote access VPN:-
- Remote access VPN permits a user to connect to a private network and access all its services and resources remotely.The connection between the user and the private network occurs through the internet and connection is secure and private.
- ii)Site to site VPN:-
- A Site to site VPN is also called as Router to Router VPN and is commonly used in the large companies.It's two types:-
- a)Internet based VPN:-
- When several offices of the same company are connected using site to site VPN type.It is called as internet based VPN.
- b)Extranet based VPN:-
- When companies use site to site VPN type to connect to the office of another company,It is called Extranet based VPN.
- iii)Cloud VPN:-
- A cloud VPN is a virtual private Network that allows users to securely connect to a cloud based infrastructure or service.
- iv)Mobile VPN:-
- Mobile VPN is a virtual private network that allows mobile user to securely connect to a private network,typically through a cellular network.
- v)SSL VPN:-SSL VPN(Secure Sockets Layer Virtual Private Network) is a type of VPN that uses the SSL protocol to secure the connection between the user and the VPN server.
- vi)PPTP VPN:-
- PPTP(Point to Point Tunneling protocol) is a type of VPN that uses a simple and fast method for implementing VPNs.
- vii)L2TP VPN:-

- L2TP(Layer 2 Tunneling Protocol)is a type of VPN that creates a secure connecting by encapsulating data packets being sent between two computers.L2TP is an extension of PPTP.
- viii)Open VPN:-
- Open VPN is an open-source software application that uses SSL and is highly configurable and secure.It creates a secure and encrypted connection between two computer by encapsulating the data packets being sent between them.

EXPERIMENT-16(B)

AIM OF THE EXPERIMENT:-

Study about types of VPN.

i)Remote access VPN:-

Remote access VPN permits a user to connect to a private network and access all its services and resources remotely.The connection between the user and the private network occurs through the internet and connection is secure and private.

ii)Site to site VPN:-

A Site to site VPN is also called as Router to Router VPN and is commonly used in the large companies.It's two types:-

a)Internet based VPN:-

When several offices of the same company are connected using site to site VPN type.It is called as internet based VPN.

b)Extranet based VPN:-

When companies use site to site VPN type to connect to the office of another company,It is called Extranet based VPN.

iii)Cloud VPN:-

A cloud VPN is a virtual private Network that allows users to securely connect to a cloud based infrastructure or service.

iv)Mobile VPN:-

Mobile VPN is a virtual private network that allows mobile user to securely connect to a private network,typically through a cellular network.

v)SSL VPN:-SSL VPN(Secure Sockets Layer Virtual Private Network) is a type of VPN that uses the SSL protocol to secure the connection between the user and the VPN server.

vi)PPTP VPN:-

PPTP(Point to Point Tunneling protocol) is a type of VPN that uses a simple and fast method for implementing VPNs.

vii)L2TP VPN:-

L2TP(Layer 2 Tunneling Protocol)is a type of VPN that creates a secure connecting by encapsulating data packets being sent between two computers.L2TP is an extension of PPTP.

viii)Open VPN:-

Open VPN is an open-source software application that uses SSL and is highly configurable and secure.It creates a secure and encrypted connection between two computer by encapsulating the data packets being sent between them.

EXPERIMENT-17A

AIM OF THE EXPERIMENT:-17A

Study about types of VPN protocol.

(1)Internet Protocol Security (IPSec):

Internet Protocol Security, Known as IPSec, is used to secure Internet communicate across an IP networks. IPSec secures Internet protocol communication by verifying the session and encrypt each data packet during the connection IPSec runs in 2 modes.

(I)Transport mode

(ii)Tunneling mode

(2)Layer 2 Tunneling Protocol; (L2TP):

L2TP or Layer 2 Tunneling Protocol is a tunneling protocol that is often combined with another VPN security protocol like IPSec to establish a highly secure VPN connection, L2TP generates a tunnel between two L2TP connection points and IPSec protocol encrypt the data and maintains secure communication between the tunnels.

(3)Point-to-Point Tunneling Protocol (PPTP):(PPTP) Protocol generates a tunnel and confines the data packet. Point-to-point protocol (PPP) is used to encrypt the data between the connections. PPTP is one of the most widely used VPN protocol and has been in use since the early release of windows. PPTP is also used on MAC and lines apart from windows.

(4)SSL and TLS:-

SSL (Secure Sockets Layer) and TLS (Transport Layer Security) generate a VPN connection where the web browser acts as the client and user access is prohibited to specific applications instead of entire network. Online shopping websites commonly uses SSL and TLS protocol.

(5) Secure Shell (SSH):

Secure Shell or SSH generates the VPN tunnel through which the data transfer occurs and also ensures that tunnel is encrypted. SSH connections are generated by a SSH
client and data is transformed from a local port on to the remote server through the encrypted tunnel.

(6)SSTP (Secure Socket Tunneling Protocol):-

A VPN Protocol developed by Microsoft that uses SSL to secure the connection, but only available for window.

(7) IKEV2 (Internet Key Exchange Version 2):

A VPN Protocol that provides fast and secure connections, but not widely supported by VPN providers.

8) Open VPN: An open-secure VPN protocol that is highly configurable and secure,widely supported by VPN providers and considered one of the most secure VPN protocols.

(9) Wire Guard:

A relatively new and Lightweight VPN protocol that aims to be faster, simpler and more secure than existing VPN protocols.

EXPERIMENT-17B

AIM OF THE EXPERIMENT:-

Study about the difference between VPN and PROXY.

VPN	PROXY
(1) VPN ensures encryption, authentication and integrity protection.	(1) Proxy dose not ensure or provide any security.
(2) Protocols used in VPN are PTTP,L2TP etc.	(2)Protocols used in proxy are FTP, SMTP, STTP etc.
(3) VPN works on firewall.	(3)Proxy works on browser.
(4) VPN stands for virtual private Net-work. It simulate a private network.	(4)It does not simulate a private network over public network.
(5) VPN does not hide the IP address of client.	(5)Proxy used to anonymous network IP instead of actual IP address of client (means it hide the IP address of client)
(6) VPN creates tunnel between end user.	(6)But proxy does not create tunnel between end user.
(7) VPN of fears high amount of security.	(7)Proxy does not offer any type security.
(8) VPN provides seamless and stable connection.	(8)Proxy connection is highly unstable.
(9) VPN encrypt all of a user matter the website or app.	(9)Proxy servers only hide one website or app.
(10)VPN encrypt the traffic.	(10)Proxy does not encrypt traffic.

EXPERIMENT-18

AIM OF THE EXPERIMENT:18

Study about hacking.

(a)Introduction to Hacking:

A commonly used hacking definition is the act of compromising digital devices and network 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.

(b) History of Hacking:

Hacking first appeared as a term in the 1970s but became more popular through the next decade. An article in 1980 edition of psychology today ran the headline "The Hacker papers" in an exploration of computer wages addictive nature. Two years later, two movies, Tron and WarGames, were released, in which the lead characters set about hacking into computer systems, which introduced the concept of hacking to a wide audience and as a potential national security risk.

(c)Types of Hacking:

There are most commonly three types of Hacking.

I. Black Hat Hacker:

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 part of a nation-state hacking campaign.

II. 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 system 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.

III. Grey Hat Hackers:

Grey hat hackers sit somewhere between the good and 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 exist, but unlike white hat hackers , they do so publicly. This alerts malicious attackers to the existence of the vulnerability.

(d)Devices Vulnerable To Hacking:

i. Smart Devices:

Smart devices, such as smart phone, are lucrative targets for hackers. Android devices in particular, have a more open source and inconsistence software development process than Apple devices, which puts them at risk of data theft or corruption.

ii. Webcams:-

Webcams built into computers are a common hacking target, mainly because hacking them is a simple process. Hackers typically gain access to a computer using a remote access Trojan (RAT) in root kit malware, which also allows them to not only spy on users but also read their messages, see there browsing activity, take screenshots and hijack their webcam.

iii. Routers:-

Hacking routers enables an attacker to gain access to data sent and received across them and networks that accessed on them.

iv. Email:-

Email is one of the most common targets of cyber attackers. It is used to spread malware and ransomware and as traffic for phising attacks which enable attackers to target victims with malicious attachment or links.

v. Jail broken phones:-

Jail breaking a phone means removing restrictions imposed on its operating system to enable the user to install application or other software not available through its official appstore.

(e)Prevention from getting Hacked:-

(i) Software update.

(ii) Use unique passwords for different accounts.

(iii) Avoid clicking on ads.

(iv) Change the default username and password on your router and smart devices.

(f) Protect yourself against Hacking:-

- Download from first- party sources.
- Install antivirus software.
- Use a VPN.
- Do not login as admin by default.
- Use password manager.
- Use two factors Authentication.
- Brush up on Anti- phishing techniques.

(g) Ethical Hacking:-

Ethical Hacking refers to the actions carried out by white hat security hackers. It involves gaining access to the computer system and networks to test for potential vulnerabilities, and then fixing any identified weakness.

Using these technical skills for ethical hacking purposes is legal, provided the individual has written permission from the system or network owner protects the organizations privacy and reports all weakness they find to the organization and its vendors.

EXPERIMENT-19

AIM OF THE EXPERIMENT:

Study about Computer Network Security and penetration.

(i) Acuretix :

Acretix is an automated web application security testing and ethical hacking tools. It is used to audit you web application by checking for vulnerabilities like SQL injection, cross site scripting and other exploitable vulnerabilities. It scans any website or web application that is accessible via web browser and uses the HTTP HTTPS protocol.

(ii) Nmap:

Nmap, short for network mapper, is a recornaissatool that is widely used by ethical hackeres to gethere information about target system.
features:

- Audit device security
- Detect open ports on remote houts
- Network mapping and enumeration
- Find vulnerabilities inside any new network.
- Launch massive DNS queries against domains and subdomains.

(iii) Metasploit:

Metasploit is an open-source pen testing freameworck written in Ruby.

Features:

- Eavade detection systems.
- run security vulnerability Scans.
- Execute remote attacks Enumerate networchs and host.

Supported platforms include:

- Mac os x
- Linux
- Windows

(iv) Wireshark: Wireshark is a free open-source software that slower you to analyse network traffic in real times.

Features :

- Saves analysis fore offline inspection
- packet browser

- powerful GUI

- Rich VOIT analysic
- Inspects and decompresses grip files
- Cexperts results to XML, postscript, CSV, one plaintext.

(v) Nikto: Nikto is another favourite well known as part of the Kali Kinum Distribution

features:

- Detects default installation files on any operating system.
- Detects out dated software applications.
- Integration with metasploit framework.
- Run cross-site scripting vulnerability tests.
- Execute dictionary based brute force attacks.
- Exports results in plain text, CSV or html files.

(vi) John the riper :-

John the riper is one of the most popular password crackers of all time.

Features:

- DES,MD5,Blowfish
- Kerberos AFS
- Hash (MLLAN), the system used in window NT/2000/XP/2003
- MD4, LDAP, my SQL (using third party modules).

(vii) Kismet:-

Kismet is one of the most used ethical hacking tools .it works network detector, packet sniffer and intrusion detection system for 802.11 wireless. LAN

The program runs under Linux , free BSD net BSD , open BSD , and Mac OSX. The client can also run on Microsoft windows.

(viii) SQL ninja:-

SQL ninja is another SQL vulnerability scanner bundled with kali Linux distribution.

Feature:

- Test database schema.
- Fingerprint remote database
- Brute force attacks with a word list.

- Direct shell & reverse shell

(ix) Wapiti:-

Wapiti is a free open source command line based vulnerability scanner written in python.

Feature:

- XSS attacks
- SQL injection
- X path injection
- XXE injection
- CRLF injection
- Server side request for query

(x) Canva:-

Canva is a great alternative to metasploit offering more than SDO exploit for testing remote networks.

Features:

- Takes a screenshots of remote system
- Downloads passwords
- Modifies files inside the system
- Escalates privileges to gain administrator access
- Remote network exploitation.

EXPERIMENT-20

AIM OF THE EXPERIMEN:

Study about digital signature.

Digital Signature:-

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message,software, or digital document.

I. Key Generation Algorithm :

Digital signature is electronic signature, which assure that the message was sent by a particular sender. While performing digital transaction authenticity and integrity should be assured,otherwise, the data can be altered or someone can also act as if he was the sender and expect a reply.

II. Signing Algorithms :

To create a digital signature signing algorithms like e-mail programs create a one way hash of the electronic data which is to be signed. The signing algorithm then encrypts the hash value using the private key (signature key). This encrypted has along with other information.

Like the hashing algorithm is the digital signature

This digital signature is appended with the data and sent to the verifier.

III. Signature Verification Algorithm :

Verifier receives digital signature along with the data. It uses verification algorithm to process on the digital signature and the public key & generates some value. I also apply the same hash function on the received data and generate a hash value. Then the hash value and the output of the verification algorithm are compared. It they both are equal, then the digital signature valid else it is invalid.

The step followed in creating digital signature:

IV. Message digest is computed by applying hash function on the message and then message digest is encrypted using private key of sender to from the digital signature.

V. Digital signature is then transmitted with the message.

VI. Receiver decrypts the digital signature using the public key of sender.

VII. The receiver can computer the message digest.

VIII. The message digests computed by receiver and the message digest need to be some for ensuring integrity.

Message digest is completed using one way hash function i.e. a hash function in which computation of hash value of a message is easy but computation of the message from hash value of the message is very difficult.

EXPERIMENT-21

AIM OF THE EXPERIMENT:-

Study about practical application of digital signature.

i.Legal document and contracts:

Digital signatures are legally binding .This make them ideal for any legal document that requires a signature authenticated by one or more parties and gurantees that the record has not been altered.

ii.Sales contracts:

Digital signing of contracts sales contracts authenticates the identity of the seller and the buyer and both parties can be sure that the signature are legally binding and that the terms

iii.Financial Documents:

Finance departments digitally sign invoices so customers can trust that the payment request is from the right seller, not from a bad actor trying to trick the buyer into sending payments to a fraudulent account.

iv. Health Data:

In the healthcare industry, privacy is paramount for both patient records and research data, digital signatures ensure that this confidential information was not modified when it was transmittied between the consenting parties.

v. shipping Document:

Helps manufactures avoid costly shipping errors by ensuring cargo manifests or bills of coding are always correct. However , physical papers are lambersome, not always easily accessible during transport, and can be lost . by digitally signing shipping documents. the sender and receipient can quickly access a file, checks that the signature is up to date and ensure that no tampering has no occurred.