Assignment :- 01

Que 1:- What is network and why it needs security Explain.

Ans :- Computer network is a group of computers and associated devices connected to each other in order to provide communication information sharing and resource sharing.

Need for securing a network :-
Every network needs security against attackers and hackers both.

1) To protect the secret information from unauthorised users.
2) To protect it from unwanted editing by unauthorised users.
3) To protect it from loss during journey
4) To protect from unwanted delay in transmission / route.
5) It should be protected from replicating and capturing viruses.
6) It needs a proper protection from worms and bombs.
7) There is a need of protection from Trojan horses as they are enough dangerous for your computer.

Red Wings
Page No.___ Date __/__/__20__

Ques: What are cyber ethics? Explain.

Ans: The term "cyber ethics" refers to a set of moral rules or a code of behaviour applied to the online environment. As a responsible netizen, you should observe these rules to help make cyberspace a safe place.

Some people may have lower standard ethics in cyberspace as they thought there is no law governing the virtual world and their anonymity will save them from being detected. Infact, these are all misconceptions. The law also governs the internet and you may attract legal liabilities if you perform the following activities:

- Posting obscene and indecent content on the internet.
- Obtaining property ~~and~~ or services online by deception.
- Spreading viruses or malicious codes; and
- gaining unauthorised access to computers, etc.

Red Wings
Page No.__ Date __/__/20__

Assignment :- 02

Ques:- Distinguish between public and private keys in an asymmetric-key cryptosystem.

Ans:-

	Private Key	Public Key
1.	Private key is used to both encrypt and decrypt the data and is shared between the sender and receiver of encrypted data.	The public key is only used to encrypt data and to decrypt the data, the private key is used and is shared.
2.	The private key mechanism is faster.	The public key mechanism is slower.
3.	The private key is kept secret.	The public key is free to use.
4.	The private keys mechanism is called symmetric being a single key between two parties.	The public key mechanism is called asymmetric being two keys for different purposes.
5.	The private key is to be shared between two parties.	The public key can be used anyone.
6.	Performance testing checks the reliability, scalability, and speed of the system.	Load testing checks the sustainability of the system.

Ques:- Distinguish between symmetric and asymmetric key cryptosystems.

Ans:-

	Symmetric Key	Asymmetric key.
1.	It only requires a single key for both encryption and decryption.	It requires two key one to encrypt and the other one to decrypt.
2.	The size of cipher text is same or smaller than the original plain text.	The size of cipher text is same or larger than the original plain text.
3.	The encryption process is very fast.	The encryption process is ~~very~~ slow.
4.	It is used when large amount of data is required to transfer.	It is used to transfer small amount of data.
5.	It only provides confidentiality.	It provides confidentiality, authencity and non-repudiation
6.	Ex:- 3DES, AES, DES and RC4.	Ex:- ECC, EI Gamal, DSA and RSA.

Assignment # 03

Que 1: What are fast and slow infectors?

Ans: A fast infector infects any file accessed, not just run. A slow infector only infects files as they are being created or modified. The term fast or slow when dealing with viruses pertains to how often and under what circumstances they spread the infection. Typically, a virus will load itself into memory when an infected program is run.

Que 2: Explain the following terms:

a) Dropper

A dropper is a program that has been designed or modified to "install" a virus onto the target system. The virus code is usually contained in a dropper in such a way that it won't be detected by virus scanners that normally detect that virus. While quite uncommon, a few droppers have been discovered. A dropper is effectively a trojan horse whose payload is installing a virus infection. A dropper which installs a virus only in memory is sometimes called an "injector".

b) Companion Virus

A companion virus is one that, instead of modifying an existing file, creates a new program which is executed instead of the intended program. On exit, the new program executes the original program so that things appear normal. On PCs this has usually been accomplished by creating an infected .COM file with the same as an existing EXE file. Integrity chucking antivirus software that only looks modifications in existing files will fail to detect such viruses

c) Activity monitoring programs:

Activity monitors are special software which are used as virus prevention tools. These programs try to prevent infection before it happens by looking for virus-like activity, such as attempts to write to another executable, reformat the disk, etc An alternative term for these softwares is BEHAVIOR BLOCK BLOCKER

Ex: SECURE and FluShot+ (PC), and Gate Keeper (Macintosh)

d) Virus Simulators

There are three different kinds of programs that are often called "virus simulators".

Page No.
Date

None of the three generate actual viruses.

The first kind demonstrate the audio and video effects of some real computer viruses.
The second kind are programs that simulate a virutual environment - a virutual computer, with virtual disks, virtual files and virtual viruses on them.
The third kind are programs that generate file containing scan strings used by some scanners to detect real viruses.

Page 1/6
Date

Assignment # 04

Qu 1: What are the advantages of firewalls?

Ans: 1. They can stop incoming requests to inherently insecure services by monitoring traffic, e.g. you can disallow rlogin, or RPC services as NFS.

2) They stop hackers and key loggers
3) They help block trojan horses.
4) They can control access to other services e.g.
   a) bar callers from certain IP address
   b) filter the service operations
   c) hide information.
5) They are more secure than securing each host due to:
   a) The complexity of the software on the host.
   b) The number of hosts that need to be secured.

Qu 2: What are the functions of firewalls?

Ans: 1. Monitoring and controlling bandwidth
2. Filtering of the internet.
3. SD-WAN and internet aggregation.
4. Using a sandbox.
5. Wireless controller built-in.
6. Packet inspection (Deep Packet Inspection)

Page No.
Date

Assignment: 05

Ques: Discuss various types of IDs in brief?

Ans: Intrusion detection systems can be categorized in 3 different ways depending on the environment and type of intrusion to be detected. These three categories are:

- Network based ID systems.
- Host based ID systems.
- Misuse and anomaly detection systems.

- Network based ID systems

Network based intrusion detection systems (NIDS) are devices intelligently distributed within networks that passively inspect traffic traversing the devices on which they sit.

- Domain 7. Eric conrad.
- Local area network security.
- Embedded security.
- Guarding Against Network intrusions.

- Host based ID systems

A host based IDs (HIDS) is an intrusion detection system that is capable of monitoring and analyzing the internals of a computing systems as well as the network packets on its network interfaces

similar to the way a network based intrusion detection system (NIDS) operates. This was the first type of intrusion detection software to have been designed, with the originally target system being the mainframe computer where outside interaction was infrequent.

→ Misuse and Anomaly Detection System.
Misuse detection within network-based IDS involves checking for illegal types of network traffic
Detection of anomalous activity relies on the system knowing what is "regular" network traffic and this what isn't. Anomalous traffic to a host based IDS might be interactive accesses outside of normal office hours.

Que 2 (i) Explain Deployment of HIDS?
Ans (i) HIDS differ from NIDS in two ways. HIDS protects only the best host system on which it resides and its network card operates in nonpromiscuous mode. Nonpromiscuous mode of operation can be an advantage in some cases, because not all NICs are capable of promiscuous mode. In addition, promiscuous mode can be CPU intensive for a slow

host machine. HIDS can be run directly on the firewall as well, to help keep the firewall secure.

Another advantage of HIDS is the ability to tailor the ruleset to a specific need. For example, there is no need to interrogate multiple rules designed to detect DNS exploits on a host that is not running Domain Name Services. Consequently, the reduction in the number of pertinent rules enhances performance and reduces processor overhead.

Assignment # 06

Que 1:) Write notes on cyber security?

Ans:) Cyber security means protecting your computer, network, data and information from major cyber threats and attacks. It is the state of being protected from the unauthorized use of electronic data as well as damage to cyber assets. It is a critical issue for all business and defence systems. It includes security or protection from theft, damage and loss of hardware and software both. The cyber asset configuration management policy includes the purpose of securing both hardware and software assets along with information.

Que 2:) Explain the handling of cyber assets?

Ans:) Handling cyber assets means implementing successful cyber security or providing successful solution for cyber asset protection subscription. The NCCE at NIST provides most pressing cyber security problems with practical and standard based solutions using commercially available technologies. It collaborates with academic Industries and Government experts to build modular, open, end to end reference designs that are applicable.

Assignment 07

Q.1) Write short note on :-

a) VPN diagram

VPN is a mechanism of employing authentication integrity protection and encryption in order to transmit data on a public network in a secured way as to be a private network. It can connect distant networks of an organization. Thus it simulates a private network over a public network.

Virtual signifies that it depends on a virtual connection which are temporary and have no physical presence or significance.

b) Client configuration.

The client configuration is designed to allow the client to specify one or more endpoint each with its own name, address and contract, with each referencing the <binding> and <behaviour> elements in the client configuration to be used to configure that endpoint.

c) Exchanging keys

As VPN needs strong authentication and

Page No.
Date

provides security using encryption so there is always a need of exchange of encryption keys. As information encryption with public key can only be decrypted with private key while encryption with private key cannot be decrypted with public key.

Qu 2: What is the main aim of VPN?

Ans:)

- Encryption of your IP address: The primary job of a VPN is to hide your IP address from your ISP and other third parties.
- Encryption of protocols: A VPN should also prevent you from leaving traces. For
- Kill switch: If your VPN connection is suddenly interrupted, your secure will also be interrupted.
- Two-factor authentication: By using a variety of authentication methods, a strong VPN checks everyone who tries to log in.

Assignment 8

Q1. Write notes on:

a) Server disaster

A server disaster is more harmful as compared to network disaster because in server disaster the information loss is very common. Once your network is disaster resistant it does not mean that communication may not fail. If your server fails, though the network is operation but all its control along with data is lost. So server should not only be protected highly for disaster & but there should be proper plans to make is disaster resistant.

b) UPS

When your computer is working as server, the power is one of the most important factor. A good power source must protect your system from backup, brownout, power surges, spikes, noise, frequency variation, harmonic distortions etc. An uninterruptible power supply (UPS) provides all these protections to your system.

c) RAID

RAID is a disk management tool that comes with windows NT/2000/XP. It is a one stop, do it all utility for working with hard drives. It is very special type of drive organization technique with the help of drive signatures for implementing RAID the drives are configured as 'dynamic disks' that allow you to enlarge the partitions without deleting the partition or losing data.

Ques: What is clustering?

Ans: Clustering: It is the process of running the redundant servers by providing them support at operating system level. It provides fault tolerance and performance boosting. There are various types of cluster implementation but the most common among them are as follows:

a) Active/Passive cluster
b) Active/Active cluster

a) Active/Passive cluster: The active/passive cluster uses two server configuration i.e active server and passive server and is similar to redundant server. In this clustering all workstations are attached to external storage area or storage area network.

b) Active/Active clustering: In active/active clustering all workstation participate in processing the service requests. Every workstation has full access to shared storage space. The traffic load between workstation is balanced and for ~~what~~ that the cluster behaves as an intelligent unit.