End Term Solutions

Q1 [CO1]. Compare the functioning of Chinese wall model with the Bell La Padula model and Clark-Wilson Integrity Model. Identify scenarios in which each is better than the other two. Scenarios must be explained in details with all the technicalities.

Ans: The Chinese wall model, Bell-La Padula model, and Clark-Wilson Integrity Model are all models for computer security and information flow control. These models are designed to protect against unauthorized access to sensitive information and to ensure that information is only accessed and modified by authorized users. The Chinese wall model is a confidentiality model that is used to prevent conflicts of interest in financial institutions. It is based on the concept of a "Chinese wall" that separates different departments or units within an organization, so that information cannot be shared between them. This model is often used in the financial industry to prevent employees from using insider information for personal gain. The Bell-La Padula model, also known as the Basic Security Model, is a confidentiality model that is based on the concept of "security levels" and "security classes". This model classifies information into different security levels based on its sensitivity, and assigns users to different security classes based on their clearance level. The model then defines rules for how information can be accessed and shared between users of different security classes. For example, a user with a "top secret" clearance would be able to access information classified as "top secret", but not information classified as "secret" or "confidential". The Clark-Wilson Integrity Model is an integrity model that is based on the concept of "well-formed transactions". This model defines a set of rules for how information can be accessed and modified in a system, and enforces those rules through the use of "integrity verifiers". These verifiers are programs that ensure that transactions are performed in a way that is consistent with the rules of the system. This model is often used in financial and accounting systems to ensure the integrity of financial transactions. In summary, the Chinese wall model is a confidentiality model that is used to prevent conflicts of interest, the Bell-La Padula model is a confidentiality model that is based on security levels and classes, and the Clark-Wilson Integrity Model is an integrity model that is based on well-formed transactions. Each of these models has its own strengths and limitations, and is suitable for different types of systems and environments. [2 marks]

> One scenario where the Chinese wall model might be a better choice than the Bell-La Padula model is in a financial setting, where different groups or individuals within an organization need to access different types of sensitive financial information. In this scenario, the Chinese wall model, which is specifically designed to address the need to prevent conflicts of interest and protect against insider trading, might be a better choice than the Bell-La Padula model, which is more focused on protecting against unauthorized access to sensitive information. [1 mark]

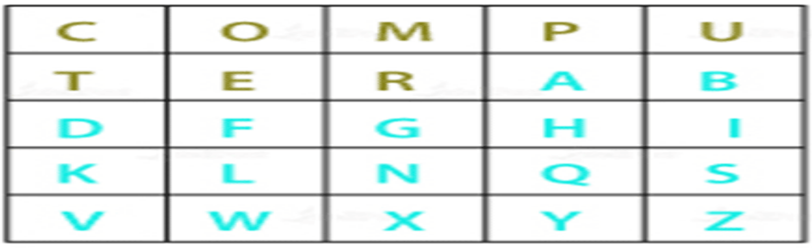
>One scenario where the Clark-Wilson integrity model might be a better choice than the Bell-La Padula model is in an organization that needs to maintain a high level of integrity and consistency in its data. In this scenario, the Clark-Wilson integrity model, which is specifically designed to enforce the integrity and consistency of data, might be a better choice than the Bell-La Padula model, which is more focused on protecting against unauthorized access to sensitive information. [1 mark]

> One scenario where the Clark-Wilson integrity model might be a better choice than the Bell-La Padula model is in an organization that needs to maintain a high level of integrity and consistency in its data. In this scenario, the Clark-Wilson integrity model, which is specifically designed to enforce the integrity and consistency of data, might be a better choice than the Bell-La Padula model, which is more focused on protecting against unauthorized access to sensitive information. [1 mark]

Q 2(a)[2.5 marks] a) Encrypt “communication” using key “computer” and Playfair Cipher Algorithm.

[Step by step marking, 0.5 marks for 1st step, 0.5 marks for 2nd Step, 1.5 marks for Step 3]

1. First, create a digraph from the plaintext by applying rule 2, which is CO MX MU NI CA TI ON.
2. Make a key matrix that is 5 by 5. (by rule 3). The significant element in our circumstance is COMPUTER.



C	O	M	P	U
T	E	R	A	B
D	F	G	H	I
K	L	N	Q	S
V	W	X	Y	Z

3. We will now look through each key-matrix pair individually to find the corresponding encipher.

- The first digraph is CO. The two are displayed together in a row. The CO and OM are encrypted using Rule 4(i).
- The second digraph is MX. Both of them are visible in the same column. The MX and RM are encrypted using Rule 4(ii).
- The third digraph is MU. The two are displayed together in a row. MU is encrypted into the PC using Rule 4(i).
- The fourth digraph is NI. The pair is visible in several rows and columns. NI is encrypted into SG using Rule 4(iii).
- The sixth digraph is CA. The pair is visible in several rows and columns. Rule 4(iii) states are used by CA to encrypt data.
- Therefore, the plaintext COMMUNICATION is encrypted using OMRMPCSGPTBDML.

2b)[2.5 marks] Differentiate between Transposition and Substitute Cipher. [2 marks for Difference, 0.5 marks for example]
Ans:

Difference between Substitution Cipher Technique and Transposition Cipher Technique:

S.NO	Substitution Cipher Technique	Transposition Cipher Technique
1.	In substitution Cipher Technique, plain text characters are replaced with other characters, numbers and symbols.	In transposition Cipher Technique, plain text characters are rearranged with respect to the position.
2.	Substitution Cipher's forms are: Mono alphabetic substitution cipher and poly alphabetic substitution cipher.	Transposition Cipher's forms are: Key-less transposition cipher and keyed transposition cipher.
3.	In substitution Cipher Technique, character's identity is changed while its position remains unchanged.	While in transposition Cipher Technique, The position of the character is changed but character's identity is not changed.
4.	In substitution Cipher Technique, The letter with low frequency can detect plain text.	While in transposition Cipher Technique, The Keys which are nearer to correct key can disclose plain text.
5.	The example of substitution Cipher is Caesar Cipher.	The example of transposition Cipher is Rail Fence Cipher.

Q 3 Alice can read and write to the file x, can read the file y and can execute the file z. Bob can read x, can read and write to y and cannot access z.

(a) Write an access control matrix for this situation.
(b) Write a set of access control lists (ACLs) for this situation, explaining which list is associated with which file.
(c) Write a set of capability lists for this situation, explaining what each list is associated with.
[5 marks]
Ans a) [2 marks]

	File x	File y	File z
Alice	{read,write}	{read}	{execute}
Bob	{read}	{read,write}	{}

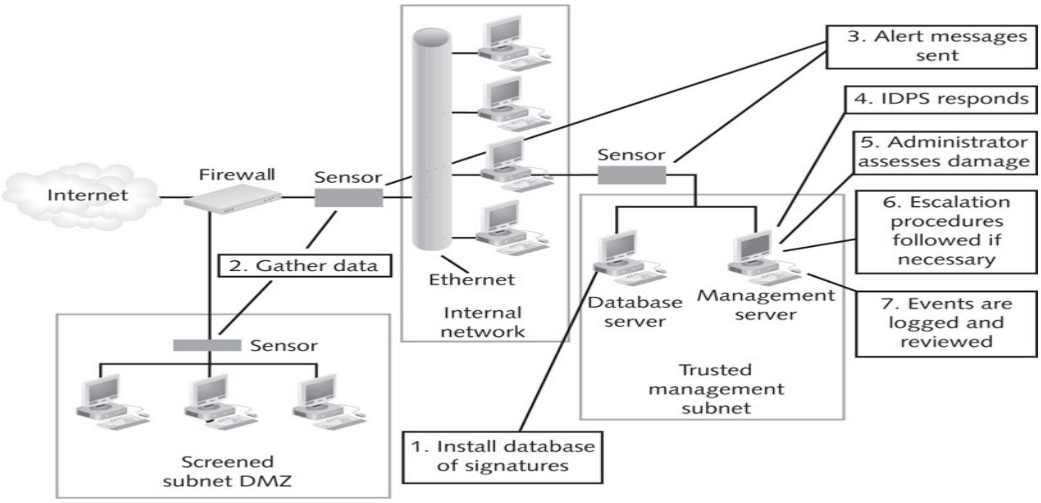
b) [1.5 marks]
ACL(File x)= Alice: {read,write}, Bob:{read}
ACL(File y)= Alice: {read},Bob: {read,write}
ACL(File z)=Alice:{execute}, Bob:{}

c)[1.5 marks]
CList(Alice)= File x:{read,write}, File y:{read}, File z:{execute}
CLIst(Bob)=File x:{read}. File y:{read,write}, File z={}

Q 4 [CO4: 4 Marks] Demonstrate step by step the examination of the Intrusion Detection Systems in securing an organization's IT infrastructure. **[Listing only steps – 1 Mark, Listing and Complete description of steps – 3 Marks; listing, description and diagram – 4 Marks]**

Examining Intrusion Detection Step by Step, the steps are

i. Installing the IDPS database
ii. Gathering data
iii. Sending alert messages
iv. The IDPS responds
v. The administrator assesses damage
vi. Following escalation procedures
vii. Logging and reviewing events


3. Alert messages sent
4. IDPS responds
5. Administrator assesses damage
6. Escalation procedures followed if necessary
7. Events are logged and reviewed
Internet
Firewall
Sensor
Sensor
Sensor
2. Gather data
Ethernet
Internal network
Database server
Management server
Trusted management subnet
Screened subnet DMZ
1. Install database of signatures

© Cengage Learning 2014

Step 1: Installing the IDPS Database

IDPS uses the database to compare traffic detected by sensors
Anomaly-based systems
Requires compiling a network baseline by observing network traffic (over a week)
Signature-based IDPS
Can use database immediately
You can add your own custom rule base

Step 2: Gathering Data

Network sensors gather data by reading packets
Sensors need to be positioned where they can capture all packets
- Sensors on individual hosts capture information that enters and leaves the host
- Sensors on network segments read packets as they pass throughout the segment

Sensors on network segments cannot capture all packets
- If traffic levels become too heavy

Step 3: Sending Alert Messages

IDPS detection software compares captured packets with information in its database
IDPS sends alert messages
- If captured packets match an attack signature or
- Deviates from normal network behavior

Step 4: The IDPS Responds

Command console receives alert messages
- Notifies the administrator

IDPS response actions:
- Alarm - Send an alarm message
- Drop – Packet is dropped
- Reset – IDPS stops and restarts network traffic
- Code analysis – Prevents malicious code from running
- File system monitoring – Prevent files from being modified
- Network traffic filtering – act as firewall
- Network traffic analysis – stop incoming traffic

Step 5: The Administrator Assesses Damage

Administrator monitors alerts
- Determines whether countermeasures are needed

Administrator need to fine-tune the database
- The goal is avoiding false negatives

Line between acceptable and unacceptable network use is not always clear

Step 6: Following Escalation Procedures

Escalation procedures

Set of actions to be followed if the IDPS detects a true positive

Should be spelled out in company's security policy

Incident levels

Level One

Might be managed quickly

Level Two

Represents a more serious threat

Level Three

Represents the highest degree of threat

Step 7: Logging and Reviewing the Event

IDPS events are stored in log files

May also be sent to a database file

Administrator should review logs

To determine patterns of misuse

Administrator can spot a gradual attack

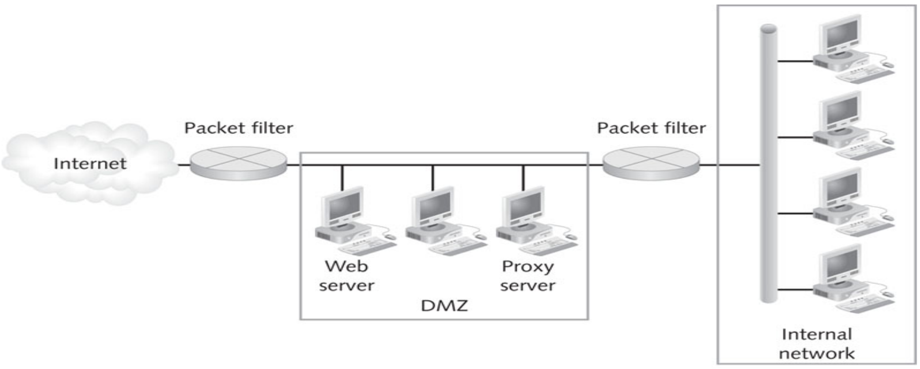
IDPS should also provide accountability

Ability to track an attempted attack or intrusion back to the responsible party

Some systems have built-in tracing features

Q 5 [CO4: 2+2=4 Marks] Write short note on the following

a. **Role of DMZ and how it helps Firewalls, in network security.** **[Diagram with relevant explanation presented below – 2 Marks]**



© Cengage Learning 2014

In computer security, a DMZ network (sometimes referred to as a "demilitarized zone") functions as a sub network containing an organization's exposed, outward-facing services. It acts as the exposed point to an untrusted network, commonly the internet.

The goal of a DMZ is to add an extra layer of security to an organization's local area network. A protected and monitored network node that faces outside the internal network can access what is exposed in the DMZ, while the rest of the organization's network is safe behind a firewall.

When implemented properly, a DMZ network gives organizations extra protection in detecting and mitigating security breaches before they reach the internal network, where valuable assets are stored.

There are numerous ways to construct a network with a DMZ. The two major methods are a single firewall (sometimes called a three-legged model), or dual firewalls. Each of these systems can be expanded to create complex architectures built to satisfy network requirements:

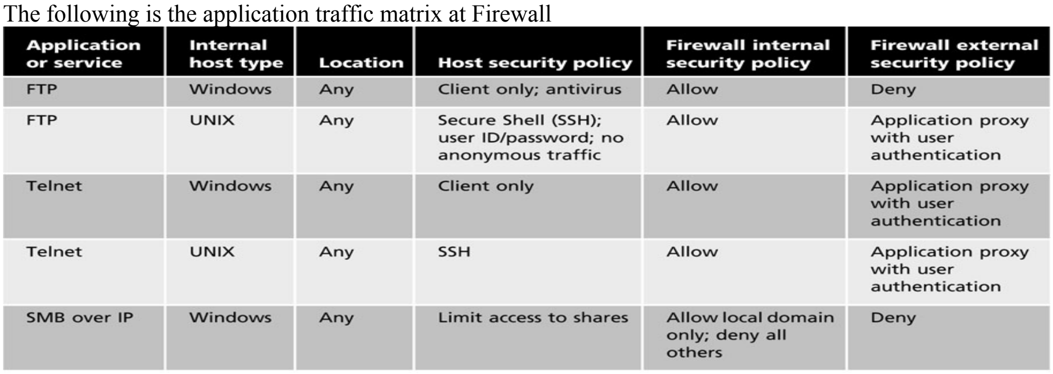
Single firewall: A modest approach to network architecture involves using a single firewall, with a minimum of 3 network interfaces. The DMZ will be placed Inside of this firewall. The tier of operations is as follows: the external network device makes the connection from the ISP, the internal network is connected by the second device, and connections within the DMZ are handled by the third network device.

Dual firewall: The more secure approach is to use two firewalls to create a DMZ. The first firewall (referred to as the "frontend" firewall) is configured to only allow traffic destined for the DMZ. The second firewall (referred to as the "backend" firewall) is only responsible for the traffic that travels from the DMZ to the internal network. An effective way of further increasing protection is to use firewalls built by separate vendors, because they are less likely to have the same security vulnerabilities. While more effective, this scheme can be more costly to implement across a large network.

b. Guidelines for firewall rule base and Firewall policy for application traffic.

Firewall policy: addition to security policy that describes how firewalls should handle application traffic.
Risk assessment provides a list of applications and associated threats and vulnerabilities
General steps to create a firewall policy
Identify network applications that are needed
Determine methods for securing application traffic
Must balance security, user requirements, and cost
Consider all firewalls in your network
Develop a traffic matrix for each location

The following is the application traffic matrix at Firewall



Application or service	Internal host type	Location	Host security policy	Firewall internal security policy	Firewall external security policy
FTP	Windows	Any	Client only; antivirus	Allow	Deny
FTP	UNIX	Any	Secure Shell (SSH); user ID/password; no anonymous traffic	Allow	Application proxy with user authentication
Telnet	Windows	Any	Client only	Allow	Application proxy with user authentication
Telnet	UNIX	Any	SSH	Allow	Application proxy with user authentication
SMB over IP	Windows	Any	Limit access to shares	Allow local domain only; deny all others	Deny

Firewalls enable you to control access to your computer or network
By controlling access to particular applications
Options for defining rules
Allow traffic
Block traffic
Ask or prompt – user is prompted when application attempts to access the Internet
Keep list of rules as short as possible
About 30 rules (no more than 50 rules)
Shorter the rule base, faster the firewall will perform
Firewalls process rules in a particular order
Usually rules are numbered sequentially and displayed in a grid
Most important rules should be at the top of the list
Make the last rule a cleanup rule
Handles any other packets that have not been covered in preceding rul

Q 6. [CO4: 2+2+1+2 = 7 Marks] An organization planned to implement NAT at along with the Firewall to share the internet. In this connection, as a security engineer provide the solutions for following

a) Suggest suitable firewall settings for this case with advantages among distributed and centralized firewall.

A distributed firewall is a host-resident security software application, which protects the network as a whole against unwanted intrusion. Distributed firewalls have a standard set of capabilities:

Centralized Management: Though distributed firewalls don't exist in just one place, they do typically offer the ability to configure and "push out" consistent security policies. They also allow for centralized reporting, which makes it practical to update and consistently apply firewall policies.

Fine-Grained Access Control: Distributed Firewalls allow for fine grained access control, which standard firewalls cannot readily accommodate without greatly increasing their complexity and processing requirements.

Policies: The ability to set "security policies" to allow and deny access depending on determined criteria. This is basic functionality that underlies all firewalls. Distributed firewalls usually also have features that guarantee the integrity of the policy during transfer.

Pull and Push Distribution: Distributed firewalls typically support both "pull" and "push" methods of distribution – the former involving pinging the central management server to check whether it's up and active, then requesting its policies, and the latter ensuring that the hosts always have their updated policies at all times.

<u>Distributed firewall vs. centralized</u>

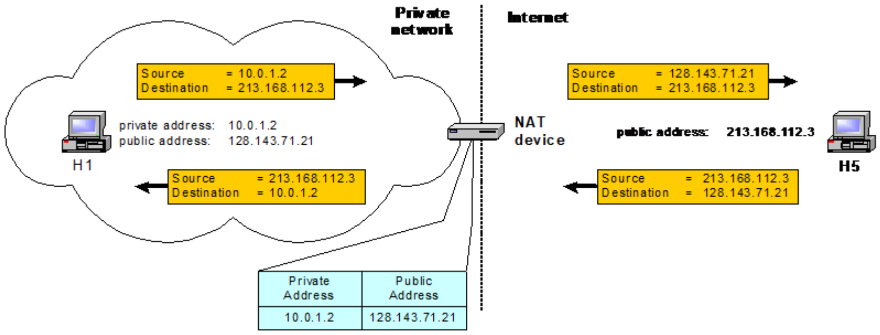
Advantage: Can filter traffic between internal hosts on the local network. For example, prevent ssh connections from certain internal hosts, avoiding possible attacks if they are compromised.

Disadvantage: Cannot protect against external flooding of an internal network – in a DoS attack, the links between local hosts will be flooded, whereas this could be prevented by throttling incoming traffic at a gateway firewall.

b) What is the main security benefit of NAT and why is it useful to combine NAT with a firewall, instead of using separate NAT and firewall devices?

NAT hides the addresses of devices behind the NAT device and prevents attacks that use knowledge of internal network addresses behind the NAT device. Some firewall policies, such as allowing traffic to high-numbered ports only if there was a matching outgoing request, require port numbers and internal addresses. This is easier to determine the firewall also knows the NAT translation table.

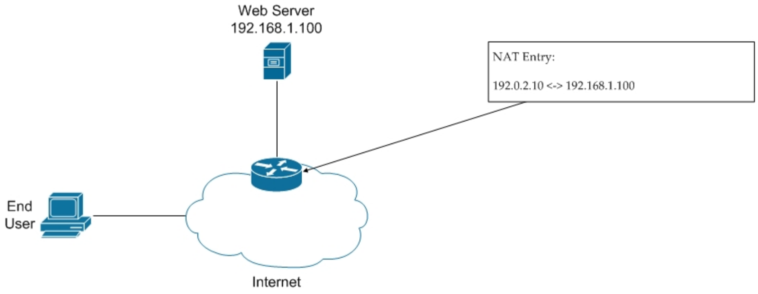
Pooling of IP addresses
Supporting migration between network service providers
IP masquerading
Load balancing of servers



c) How you implement the NAT at router and Gateway level.

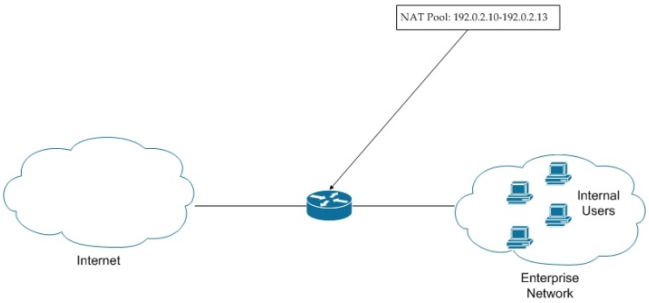
NAT takes several forms: Static NAT (SNAT), Dynamic NAT (DNAT), and Port Address Translation (PAT).

Static NAT
When using SNAT, a single internal (private) address is mapped to a single external (public) address. This type of implementation is most commonly used when a device inside a privately addressed network must be accessible directly from the Internet. Following Figure shows an example.



For this example, the router that connects the web server to the Internet is performing SNAT; specifically, it's translating from a public IP address (192.0.2.10) into a private IP address (192.168.1.100). If end users need to access this device, they use the public IP address. When the packet arrives at the web server's router, the public address is translated into the private address; this address is then used for all internal communications, whereas the public IP address is used for all external communications.

Dynamic NAT
DNAT provides the functionality of SNAT, but with a pool of addresses that are not device-specific. Following Figure shows an example.

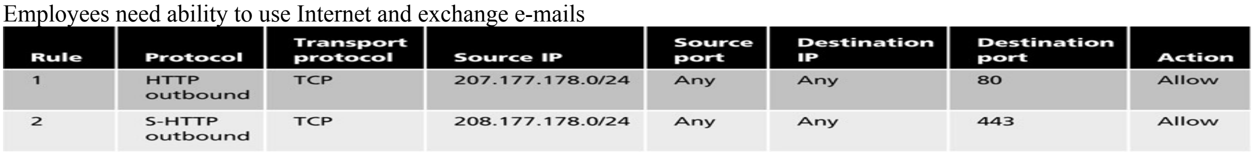


In this example, DNAT is configured on an Internet-connected router. This router is configured with a pool of public addresses that can be assigned to hosts that need to reach destinations on the Internet. The number of internal users that are allowed to use the Internet is restricted by the number of addresses that exist in the configured pool. In this example, if any of the four displayed users attempt a connection to the Internet, they succeed, because there are four different addresses in the pool. But if all addresses are in use, any other devices that attempt a connection will fail, because no more addresses are available in the pool.

In the similar way at Gateway at least two NIC cards must be configured for configuration mentioned above.

d) Write Firewall rules to control Internet services.

Web Services Rules
Employees need ability to use Internet and exchange e-mails



Rule	Protocol	Transport protocol	Source IP	Source port	Destination IP	Destination port	Action
1	HTTP outbound	TCP	207.177.178.0/24	Any	Any	80	Allow
2	S-HTTP outbound	TCP	208.177.178.0/24	Any	Any	443	Allow

DNS Resolution
Resolves fully qualified domain names (FQDNs) to their corresponding IP addresses
DNS uses UDP port 53 for name resolution
DNS uses TCP port 53 for zone transfers

E-mail Configuration
Setting up firewall rules that permit filtering e-mail is not simple
Variety of e-mail protocol that can be used:
POP3 and IMAP4 for inbound mail transport
SMTP for outbound mail transport
Lightweight Directory Access Protocol (LDAP) for looking up email addresses
HTTP for Web-based email service
Secure Sockets Layer (SSL) encryption should be used for additional security

FTP Transactions
Types of FTP transactions
Active FTP
If supported by some clients in your network, you cannot specify a port because the client can establish a connection with the FTP server at any port above 1023
Instead, specify the IP address of your FTP server
Passive FTP

ICMP Message Types
ICMPv4 and ICMPv6 function as housekeeping protocols for TCP/IP
Helps networks cope with communication problems
ICMPv4 packets have no authentication method
Attackers can use ICMP packets to attempt man-in-the-middle attacks
Firewall/packet filter must be able to determine whether an ICMP packet should be allowed to pass, based on message type

ICMP Message Types (cont’d)
ICMPv6 message types to pass through firewalls but never outside the organization:
Destination Unreachable (Type 1) – All codes
Packet Too Big (Type 2)
Time Exceeded (Type 3) – Code 0 only
Parameter Problem (Type 4) – Codes 1 and 2 only
Echo Request (Type 128)
Echo Response (Type 129)
Time Exceeded (Type 3) – Code 1

Parameter Problem (Type 4) – Code 0

Q7 [CO5]. Compare and contrast the advantages posed by copyrights, patents and trade secrets over each another. Explain scenarios in which the following holds true

- Using trade secrets better than using patents.
- Using copyrights better than using patents.
- Using patents better than using trade secrets.

Ans: Copyright, patent, and trade secret are all forms of intellectual property protection, but they each provide different types of protection and have their own unique advantages. Copyright is a form of protection that applies to original works of authorship, such as literary, dramatic, musical, and artistic works. The main advantage of copyright is that it provides automatic protection to the creator of a work as soon as it is fixed in a tangible form, such as being written down or recorded. This means that the creator does not need to register their work or take any other action in order for it to be protected. Patents, on the other hand, are a form of intellectual property protection that applies to new and useful inventions. The main advantage of a patent is that it gives the inventor the exclusive right to make, use, and sell their invention for a limited period of time. This can provide the inventor with a significant competitive advantage and can also serve as a deterrent to others who might want to copy their invention. Trade secrets, on the other hand, are a form of intellectual property protection that applies to information that is not generally known and that provides the owner with a competitive advantage. The main advantage of a trade secret is that it can provide protection for an indefinite period of time, as long as the information remains secret. This can provide a significant competitive advantage to the owner of the trade secret, as they can use the information to gain an edge over their competitors. Overall, the main advantage of copyrights is that they provide automatic protection to the creator of a work, the main advantage of patents is that they give the inventor the exclusive right to make, use, and sell their invention, and the main advantage of trade secrets is that they can provide protection for an indefinite period of time. [2 marks]

a) Patent protects new and useful invention whereas trade secret protects valuable and secret information. Patent gives the patent holder a right to exclude others from making, selling, using or importing the invention. Whereas the trade secret protects only from the misappropriation. Trade secrets are exclusive till whenever secret can be kept. Patents are protected till a time period. Example secret formula of soft drinks versus medicine formulas. [1 mark]

b) Unlike patents, which focus on an invention or something of function or utility, copyrights apply to works of authorship. With copyrights, the author gains the exclusive rights to creations for a fixed period like authorship of books, literary works, audio/video works. [1 mark]

c) If your invention can't be practiced without making it public, it may be better to patent it rather than rely on internal controls to keep it secret. Additionally, if your invention is susceptible to reverse-engineering, patenting it would likely be better since it safeguards against that. Like machine designs[1 mark]