Jessica Braganza

BE Comp 2

F17112151

PAGE NO:

DATE:

ICS Assignment 3

1) Firewall architecture in detail?

Ans. 1) Firewall in computing, a firewall is a network security system that monitoring and controls the incoming and outgoing network traffic based on pre-determined security rules.

2) A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the internet that is assumed to not be secure or trusted.

3) Firewall categories : a) Host-based firewalls b) Network firewalls.

a) Host Firewall : A host firewall is a software application or suite of application installed on a singular computer. A personal host firewall is installed on.

b) Network firewall : A network firewall functions on the network level. This means that the firewall filters data as it travels from the Internet to the computer on the network.

4) Components of firewall architecture

i) Dual Homed Host Architecture

ii) Screened Host Architecture

iii) Screened Subnet Architecture

iv) Screening router.

5) Firewall logs Firewall in the process of filtering internet traffic, cell firewalls have some type of logging feature that documents how the firewall handled various types of traffic.

2) Trusted System Short Note.

Ans. 1) Another widely applicable requirement is protect data or resources on the basis of level of security as it is commonly found in the military where information is categorized as unclassified (U), confidential (C), secret (S), top secret (TS) or Higher.

2) Here subjects have varying rights of access to objects based on their classification. This is known as multilevel security. A system that can be proved to enforce this is referred to as a trusted system.

3) The general statement of the requirement for multilevel security is that a subject at a high level may not convey information to a subject at a lower or incompatible level unless the flow accurately reflect the will of an authorized user. This can be implementable level unless that flow accurately reflets. Using the bell model. in which a multi level secure system must enforce.

a) No read up: A subject can only read a object of less or equal security level - simple security property.

b) No write down: A subject can only write into a object of greater or equal security level * (star) property.

4) These 2 rules if properly enforced provide multilevel security. The model defined 4 access modes:

i) Read: The subject is allowed only read access to the object

ii) Append: The subject is allowed only write access to the object.

iii) Write: The subject is allowed both read and write access.

iv) Execute: The subject is allowed neither read and write access but may involve the object for execution.

3) What do you mean by cyber stalking? Explain in detail.

Ans. 1) Cyber stalking is defined as the repreated use of the Internet email or related digit electronic communication devices to annoy alarms or threaten a speific individual or group of individual.

2) Stories of criminal intimidation, harassment where ~~the~~ individuals use the internet as a tool to stalk another person.

3) Stalkers use victim information like mobile numbers,

address to impinge upon their normal life. some time cyber stalkers can learn what sort of things upset their victim and can learn and use this knowledge to harass their victim.

4) Stalkers target victims through chat rooms, email, facebook, etc.

5) Different forms of cyber security stalking: Threatening, emails, spam and online verbal abuse, inappropriate messages on message boards, computer virus, etc.

6) Effects of cyber stalking on a person

· nightmares · anxiety · fear for safety · shock and disbelief.

7) Section 66A of the IT Act deals with cyber stalking. A person who repeatedly sends emails can be booked under 66A.