Gupta Bhaskar Shashnarayan Arati
Infrastructure Security
Seat No:- 12273147
Bhaskar
11/01/2021

Q.3.

Ans:- There are many security threats and attacks that can damage the security of WLAN. Those attacks can be classified into logical attacks and physical attacks.

Logical attacks :-
Attacks on WEP is a security protocol based on the encryption algorithm called 'RC4', that aims to provide security to the WLAN to the security provided in the wired LAN. WEP has many drawback like the usage of small Initialization Vector(IV) and Short RC4 encryption Key as well as using XOR operation to cipher the key with plain text to generate cipher text.

There are various WEP is addressed are:-

i) MAC address spoofing:- MAC address are sent in the clear when communication between STAs and AP takes place. Since MAC address are sent in the clear, an attacker can obtain the MAC of authorized Stat on by sniffing airwaves using tools like ethereal.

Gupta Bhaskar Sheshnarayan Arati
Infrastructure Security
Seat No:- 12273147
Bhaskar
11/01/2021

ii) Denial of Service Attack:- (DoS)
DoS is a serious threats on both wired and wireless network. This attack aims to disable the availability of the network and the services it provides in WLANs.

iii) Man-in-Middle Attack:-
This is famous attack in both wired and wireless attacks. An illicit STA intercepts the communication between legitimate STAs and the AP.

Physical Attacks:-

i) Rogue Access Points:-
In normal situations, AP authenticates STAs to grant access to the WLAN. The AP server asked for authentication. Physical placement of APs the installation of APs is another security issue because placing APs inappropriately will expose it to physical attacks.

ii) AP's Coverage:- The main difference between WLANs and wired/fixed LANs is the WLANs relies on Radio frequency (RF) signals as a communication

Page no. 23.

Gupta Bhaskar Sheshnarayan Arati
Infrastructure Security
Seat No:- 12273147
Bhaskar
11/01/2021

The sign broadcast by the AP can propagate outside the perimeter of room or building. where an AP is placed. allowing users who are not physically in the building to gain access to the network.

Ans a. A firewall is an information security program is similar to a building's firewall in that it prevents specific types of information from moving between the outside world, known as the untrusted network (eg. the Internet), and the outside word known as trusted network.

Firewall categorization Methods:-
The FIVE processing modes are:

i) Packet filtering
ii) Application Gateways
iii) Circuit Gateways
iv) MAC layer firewals
v) Hybrids.

Packet Filtering:- If examine the header information of data packets that

Gupta Bhaskar Sheshnarayan Arati
Infrastructure Security
Seat No:- 12273147
Bhaskar
11/01/2021

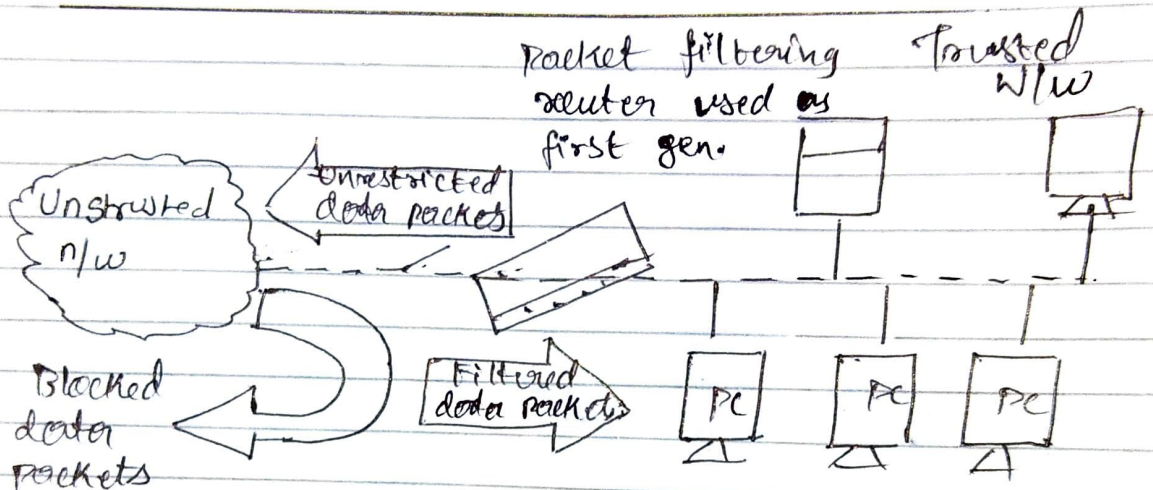

Fig. Packet Filtering Router

come into .a network . A packet filtering firewall installed .on a TCP/IP .based network typically .functions .at the Ip level .and determines whether .to drop a packet .or forward .to the next network connection.

The restrictions . most commonly implemented in packet filtering .firewalls are .based on combination .of following :-

Page No.
OS.

Gupta Bhaskar Sheshnarayan Arati
Infrastructure Security
Seat No:- 12273147
Bhaskar
11/01/2021

a) IP source and destination address
b) Direction
c) Transmission Control Protocol (TCP)

The Firewall Rule is as :-

Source Address	Destination Address	Services HTTP ; FTP SMTP	Action
172.16.x.x	10.10.x.x	Any	Deny
192.168.x.x	10.10.10.25	HTTP	Allow
192.168.0.1	10.10.10.10	FTP	Allow

Firewall Rule and Format