Name = Rajat Nigre
Roll No = 63, Sub = CSS

SARASWATI Education Society's
SARASWATI College of Engineering

PAGE NO. :
DATE :

Assignment - 2

Q.1) Discuss Various attack on Digital Signature?

→ There are three possible attack on digital signature.

(i) Choosen message attack = In theis attack, Some how make Alice sign on or more message for her. Eve now has a chosen-message pair. Eve later creates another message, with the content she wants & forges Alice's signature on it. This is similar to the choosen plaintext attack We discussed for encipherment.

(ii) Known-message Attack = In this, Eve has access to one or more message signature pair. In other word, She has to access to some document previously signed by Alice. Even tries to create another message & forges Alice's signature on it. this is similar to known-plaintext attack We discussed for encipherment.

(iii) Key-only Attack = In this attack, Eve has access only to the public information released by Alice. To forge a message, Eve need to create Alice's signature to convince Bob that the message is comming from Alice.

SARASWATI Education Society's
SARASWATI College of Engineering

PAGE NO. :
DATE :

Q.2) A & B decide to use Diffie Hellman algorithm to share a key. They chose p = 23 & g = 5 as the public parameters. Their secret key are 6 and 15 respectively. Compute the secret key that they share.

→ Step 1 = A & B have public key, P=23 and g = 5 respectively.

Step 2 = A have private key a = 6 & B have private key b = 15

Step 3 = A & B compute public value:

for A =-

$x = (5^6 \bmod 23) = 8$

for B =-

$y = (5^{15} \bmod 23) = 19$

Step 4 = A & B exchange public values, So A receive public key y = 19 & B receive public key x = 8.

Step 5 = A & B compute Symmetric key for A:

$K_a = y^a \bmod p = (19^6 \bmod 23) = 2$

for B

$K_b = y^b \bmod p = (8^{15} \bmod 23) = 2$

Step 6 = 2 is the shared key.

SARASWATI Education Society's
SARASWATI College of Engineering

PAGE NO. :
DATE :

Q.3) Write short note TCP/IP Vulnerabilites (layer wise).

→ TCP stand for Transmission Control protocal, deals with ensuring that it data packet are delivered in a reliable manner from one computer to another computer.

The TCP/IP suite is compaised of protocal at four layers.

- Application Layer = HTTP, FTP, SMTP, & SNMP.
- Transport Layer = Include TCP & UDP
- Network Layer = Include IP & internet control message protocal.
- Physical layer = Include ethernet & address resolution protocal.

(1) Packet Sniffing =

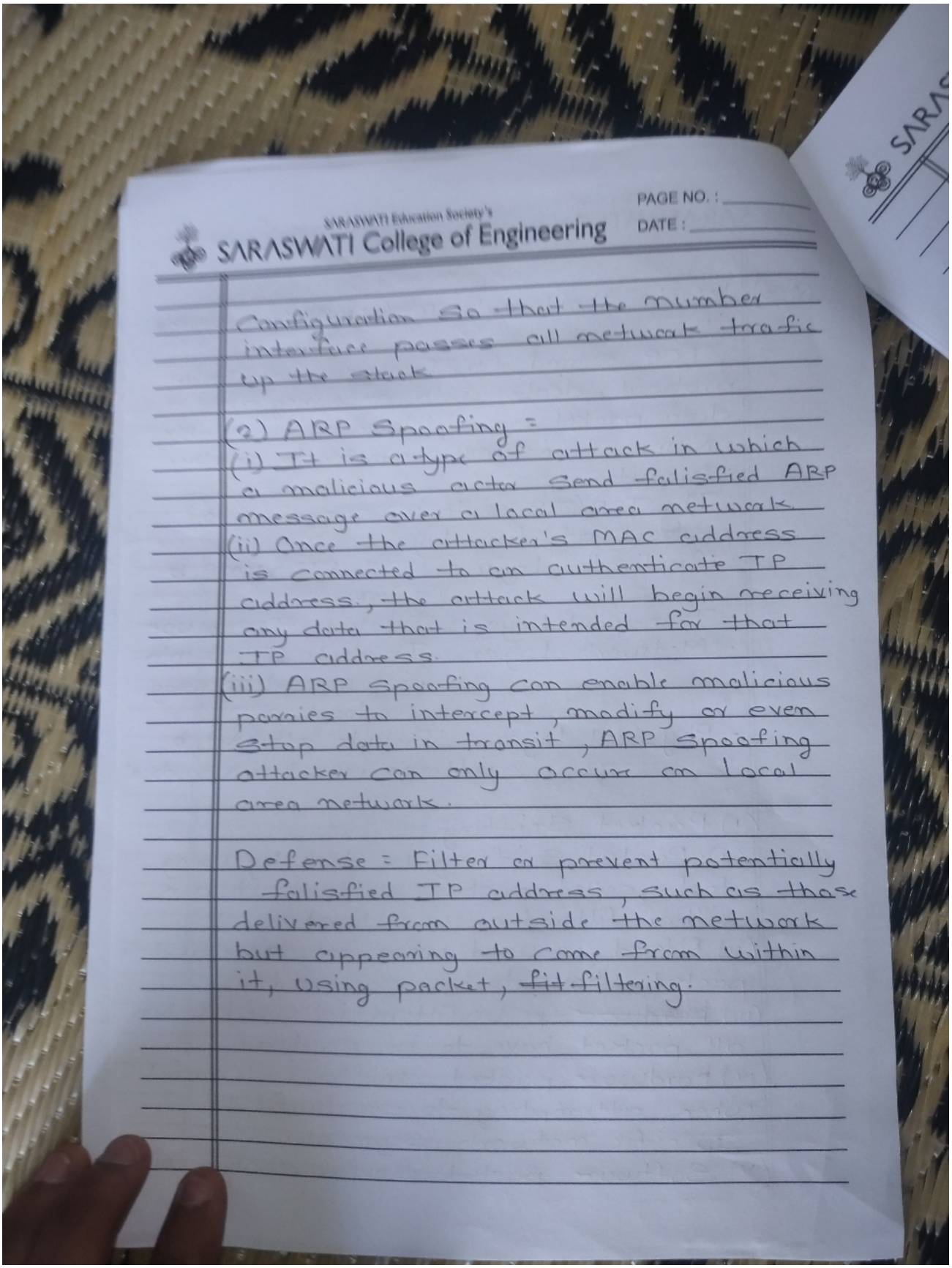
(i) Packet Sniffing is done by using tools called packet sniffer. It can either filtered or unfiltered.

(ii) Fitered is used when only specific data packets have to be captured.

(iii) ~~hardware~~ p unfilterd is used when all packet have to be captured.

(iv) hardware packet sniffer is useful when attempting to see trafic of specific network segment.

(v) Software packet sniffer change this


SARASWATI Education Society's
SARASWATI College of Engineering
PAGE NO. :
DATE :

Configuration so that the number interface passes all network trafic up the stack.

(2) ARP Spoofing :
(i) It is a type of attack in which a malicious actor send falisfied ARP message over a local area network.
(ii) Once the attacker's MAC address is connected to an authenticate IP address, the attack will begin receiving any data that is intended for that IP address.
(iii) ARP Spoofing can enable malicious parties to intercept, modify or even stop data in transit, ARP Spoofing attacker can only occur on local area network.

Defense : Filter or prevent potentially falisfied IP address, such as those delivered from outside the network but appearing to come from within it, using packet, ~~fit~~ filtering.

SARASWATI Education Society's
SARASWATI College of Engineering

PAGE NO. :
DATE :

(3) Port Scanning

(i) Port Scanning is one of most popular technique attack use to discover service that they can exploited to break into system.

(ii) all the system that are connected to LAN on the internet via modem run service that listen to well know & not not - so well know ports.

(iii) In TCP three way handshake, the connecting client send the server a TCP synchronization packet, or SYN.

Defence : It is impossible to prevent an attack from scanning a network for ports. to detect & block unusual behaviour, use firewalls, which ports to stop or block.

(4) IP Spoofing

(i) It is one of the most frequency used spoofing attack method. In an IP address spoofing attack an attacker sends IP packet from false source address in order to disguise it self.

(ii) Denial of Service attack often use IP Spoofing to overload network & device with packets that appear to be from legitimate source.

SARASWATI Education Society's
SARASWATI College of Engineering

PAGE NO. :
DATE :

(iii) IP Spoofing is the action of masking a Computer IP address so that it look like it is authentic.

Defense : Use packet filtering, b Configure routers b firewalls to reject packet with spoofed address.

SARASWATI Education Society's
SARASWATI College of Engineering

PAGE NO. :
DATE :

Q.4) Write a short note on instruction detection system.

→ (i) An instruction detection software or device that monitors network traffic or for anomalous pattern.

(ii) These pattern indicate potentially supicious activity.

(iii) An IDS also monitors for violation of established network policy.

(iv) It can be divided into three different types.

(a) Masquerador = They are typically outsider from the trusted user & not authorized to use the Computer System. These intruder penetrate the system protection by way of of legitimate user account.

(b) Misfeasor = They are typically insider & legitimate user who accesses resource that they are not authroized to use.

(c) Clandestine user = They can be both insider & outsider. these type of intruders gain supervisory access to the system.

Types of IDS technologies.

(i) Network based
(ii) Wireless
(iii) Host based
(iv) Network behaviour Analysis.

SARASWATI Education Society's
SARASWATI College of Engineering

PAGE NO. :
DATE :

Q.5) Write a short note on Firewall & its type.

→ (i) Firewall is network security device that monitors incoming & outgoing network traffic & permits or blocks data packets based on a set of security rules.

(ii) Its purpose is to establish a ~~buffer~~ barrier between your internal network & incoming traffic from external source in order to block malicious traffic like virus & hackets.

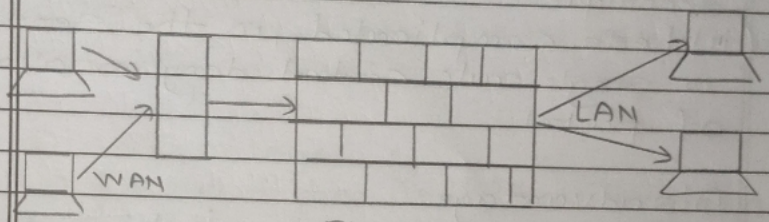
Working of Fire Walls:

(i) Firewall guard traffic at computers, entry point called ports, which is when information is exchanged with external device.

(ii) ex: " Source address 172.18.1.1 is allowed to reach destination 172.18.1.1 over port 22.

(iii) Think IP address a house & Port number as room within the house. only trusted people are allowed to enter house at all. then it's further filtered so that people within the house are only allow to access certain room depending on if they are owner, a child, or a guest. the owner is allowed into any

any room, while children & guest are allowed to certain room.



Firewall.

Type of firewalls =

(1) Packet filtering firewalls :-

i) Packt filtering as the basic and oldest type of firewall architecture, packet - filtering firewalls basically create a checkpoint as a traffic router or switch.

ii) It is newtwork security technique that is used to control data flow to and from a network.

iii) It is a security mechanism the allow the movement of packet across a network and controll their flow on the basic of set of rules, protocals, IP address & ports.

iv) The firewall can allow the fragment type packet after comparing the information with the ACL

SARASWATI Education Society's
SARASWATI College of Engineering

PAGE NO. :
DATE :

Advantage:
(i) Packet filters are faster than other technique.
(ii) Less complicated, in the sense that a single rule control deny or allow of packet.

Disadvantage:
(i) They are stateless, & hence not suitable for application layer protocal.
(ii) Complex firewall policies are different to implement using Filtering rules alone.

(2) Circuit level Firewalls:
(i) It is similar to packet filtering firwalls, but they operate at transport & session layer of the OSI model.
(ii) This can be stand-alone system or it can be the specialized function performed by an application level gatway for certain application.
(iii) It does not permit end-to-end TCP connection neither, the gateway sets two TCP connection.
(iv) The gateway can be configuted to support application level or proxy service an inbound connection & circuit-level outbound connection.

Advantage:
(i) They are more secured than Packet filter firewalls.
(ii) They maintain limited State information of the protocol.

Disadvantage
(i) Do not filter individual packets.

(3) Application layer Firewalls.:
(i) It also called Application level gateway firewall.
(ii) It is third generation firewall technology that evaluates network packet for valid data at the application layer before allowing a connection.
(iii) Application proxy is a program running on the firewall that emulate both ends of a network connection.
(iv) Each computer communicate with the other by passing all network traffic through the proxy program. the proxy program it evaluates the sent from the client & decides which to pass on & which to drop.

Advantage.
(i) They are capable of processing & manipulate packet data.
(ii) Can hide private system.

SARASWATI Education Society's
SARASWATI College of Engineering

PAGE NO. :
DATE :

Q.6 Explain Worms & Virues in detail also difference between them.

→ (i) A worm is a malicious software that reproduce it self and spread from one Computer to another Computer. it is similar to Computer Virus in self replacing, but it automatically executes it self.

(ii) Worms spread over a network and are capable of launching a cumbersome and destructive attack within a short period.

(iii) Worms are spread via software Vulnerabilities or phishig attack

Worm application / phases:

(i) Typical lifecycle of worm is similar as Computer Virus life cycle with the same ~~fo~~ stages: Dormant, Propogation, & execution.

(ii) fore worm, propogation proceeds through three phase in the initial phase, the number of increases exponentially.

(iii) After a time, infecting host waste some time attacking already infected hosts, which reduce the rate of infection.

(iv) During this middle phase, growth is approximately linear, but rate of infection is rapid.

SARASWATI Education Society's

SARASWATI College of Engineering

PAGE NO. :

DATE :

Worms	Virus.
(i) Worms is form of malware that replicates it self & can spread to different Computer via networks	(i) Virus malicious executable code attached to another executable file which will be harmful to the system.
(ii) Detection Complexity is medium.	(ii) Detection Complexity is high.
(iii) Damage caused usually medium.	(iii) Damage caused usually high.
(iv) User action not required.	(iv) User action required.
(v) human action not required.	(v) human action required.
(vi) Worms are executed via Weakness in system.	(vi) Virus are executed via executable files.
e.g = Stormworm, morris	e.g = Blaster, etc.