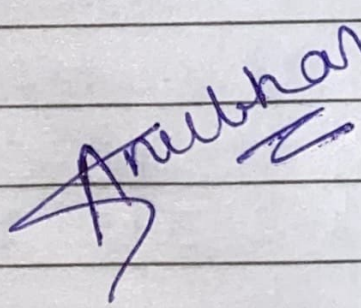
Date:
P. No:

Name : Anubhav Singh
Class : MCA 9th Sem.
Subject : N/w & information security
Subject code : IC-903
Roll no : IC-2K16-54
Institute : IIPS, DAVV, Indore



Q.1. What is the difference between authentication, integrity, confidentiality & non-repudiation.

Ans. Authentication:- It is the mechanism to identify the user or system or the entity. It ensures the identification of the person trying to access the information. The authentication is mostly secured by using user name & password. The authorized person whose identity is pre-registered can prove their identity & can access the sensitive info.

Integrity:- It gives the assurance that the information received is ocect & accurate. If the content of the message is changed after the sender sends it but before reaching its intended receiver. Then, it is said that the integrity of the message is lost.

Confidentiality :- The degree of confidentiality determines the secrecy of the information. The principle specify that only the sender & receiver will be able to access the information shared between them. Confidentiality comprise if any unauthanticate person is able to access a message.

Non-repudiation :- It is a mechanism that prevents the denial of message content send through a network. In some cases the sender sends the message & later denies it. But the non-repudiation doesn't allow the sender to refuse the receiver.

Q.2. Explain side channel attack & its types.

Ans. Side channel attack rely on measuring techniques & frequencies of your computer to establish pattern that can extract private info. from your machine. These monitors check your power uses & electromagnetic emmissions during cryptographic operations. Due to low cost & simplicity of these attacks, multiple side channels techniques can be used.

Types of side channel attacks:

1. cache attack :- Monitor uses cache (attack) access in shared physical system. commonly found in virtualized environment or a type of cloud service.

ii. Power & current attack :- These attack are based on analyzing the power consumption of the unit while it performs the encryption operation. The source of power consumption are : dynamic power, leakage current, short circuit & others.

iii. Time or delay attack :- The attacks are based on meaning the time & it takes for a unit to perform operation. The source of time & delay is executed time required to complete an operation.

iv. Electromagnet emission attack :- Based on leaked electromagnetic radiation, which can directly provide plain text & other information. The source of EM emission is acceleration of charges in antenna. Near field EM waves donate the electric & magnetic field.

Date:
P. No: 05

v. Optical attacks:- Secrate & sensitive data can be read by visual recording using a high resolution camera, or other devices that have such capabilities.

vi. Acoustic attack: Exploit sound produced during a compilation.

Q-3 What is intrusion detection system Explain its categories and operating models in details.

Ans- Intrution detection system:- It is a software that automates the intrution detection process. The primary responsibility of an IDS is to detect unwanted & malicious activity.

Why to use IDS: They have been promoted as cost effective way to block malicious traffic to detect and contain worm and virus threats to serve as a n/w monitoring requirements, and to act as a network senitizing agent.

Categories of IDS:-

1. Network Intrusion detection system:- NIDS are placed at a strategic point or point within the n/w to

monitor traffic to and from all devices on the monitor n/w. It performs an analysis of passing traffic on the ether subnet and matches the traffic that is passed on the subnet to the library of known attacks. Once an attack is identified, or abnormal behaviour is sensed, the alert can be sent to the admin. NIDS can be combined with other technologies to increase deduction & prediction rates.

2. Host intrusion detection system:
On individual host or devices on the n/w HIDS monitor the unbounded & outbonded packets from the devices only & it will alert the user or admin if suspicious activity is detected. It takes a snapshot of existing system likes & matches it to the previous

snapshot. If the critical system files were modified or detected, an alert is sent to admin to investigating. An HIPS can be seen on mission critical machine, which are not expected to change this configuration.

3. Protocol based IDS:- It comprises of a system or agent that would consistently resides the front end of a server controlling and interrupted the protocol b/w the user / devices & server.

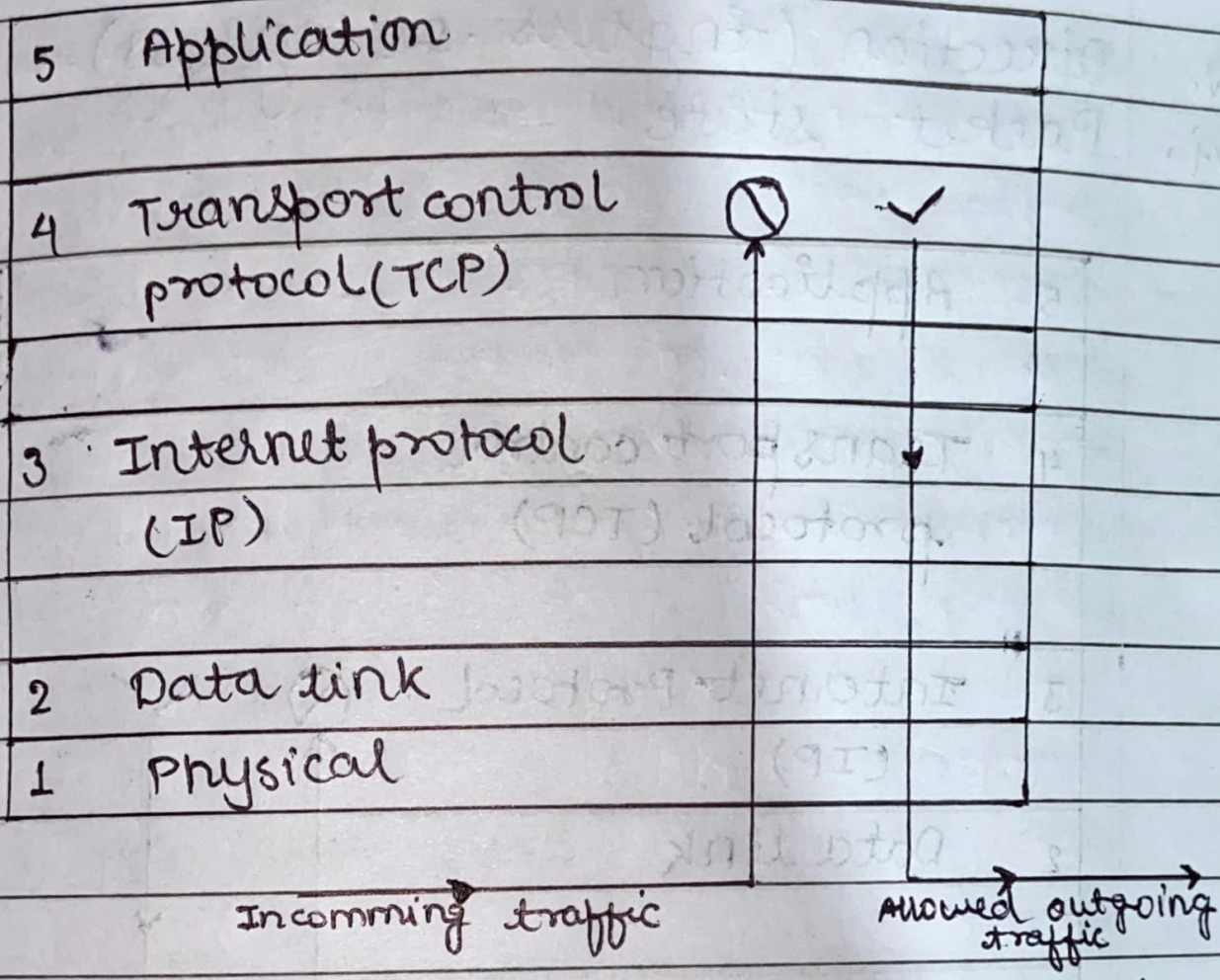
4. Application protocol based IDS: It is a system agent that gradually resides b/w a group of servers. It identifies the instructions by monitoring and interpreting the communication or an application specific protocols.

5. Hybrid IDS:- This is made by combination of two or more approaches of the IDS. In the hybrid detection system, last agent or system data are connected with NIW information to develop a complete view of the mobile wireless system. It is more effective as compare to other IDS.

Q.4. Explain in details about firewall processing modes & architecture.

Ans. The four main operations of firewall are as follows:

* Circuit level firewall (Data link layer):
Various frames are used for this type of firewall. It is the type provided whenever NAT & PAT technologies are used. When a protected computer starts a conversation with a remote computer, the traffic is intercepted by the circuit level firewalls which forwards the request. When the return traffic reaches the firewall, the internal table are checked to establish if it needs forwarding to a predicted computer or if it is a non request conversation.

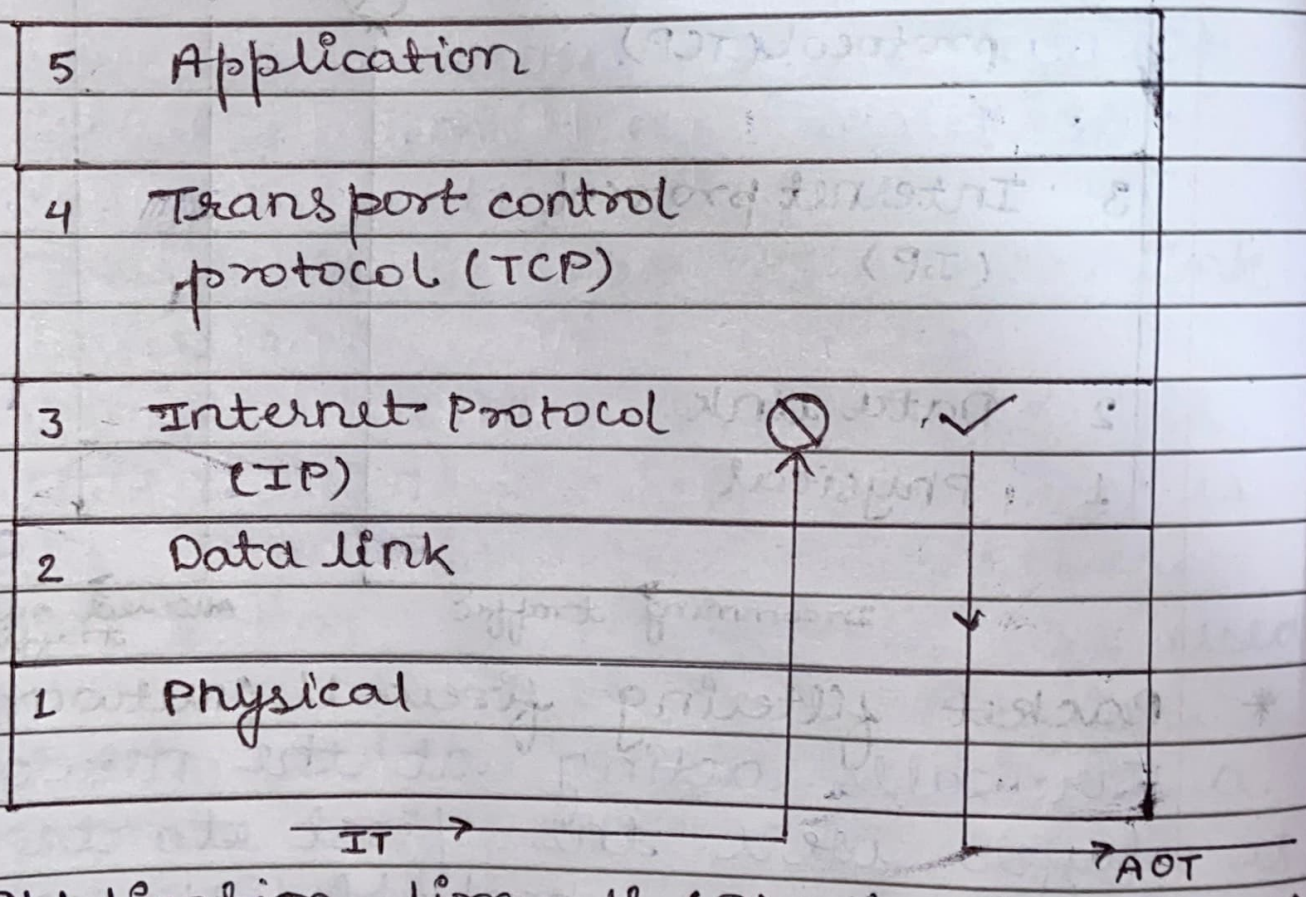


* Packet filtering firewall (Network layer)
Firewalls acting at the network layer were the first to be developed & are probably the most best understood by n/w admin. They work by examining each packet against set of defined rules which are as follows:-

i. Source & destination IP address.
ii. Source destination ports.
iii. Protocol at transport layer or N/w layer.
iv. Physical interface.

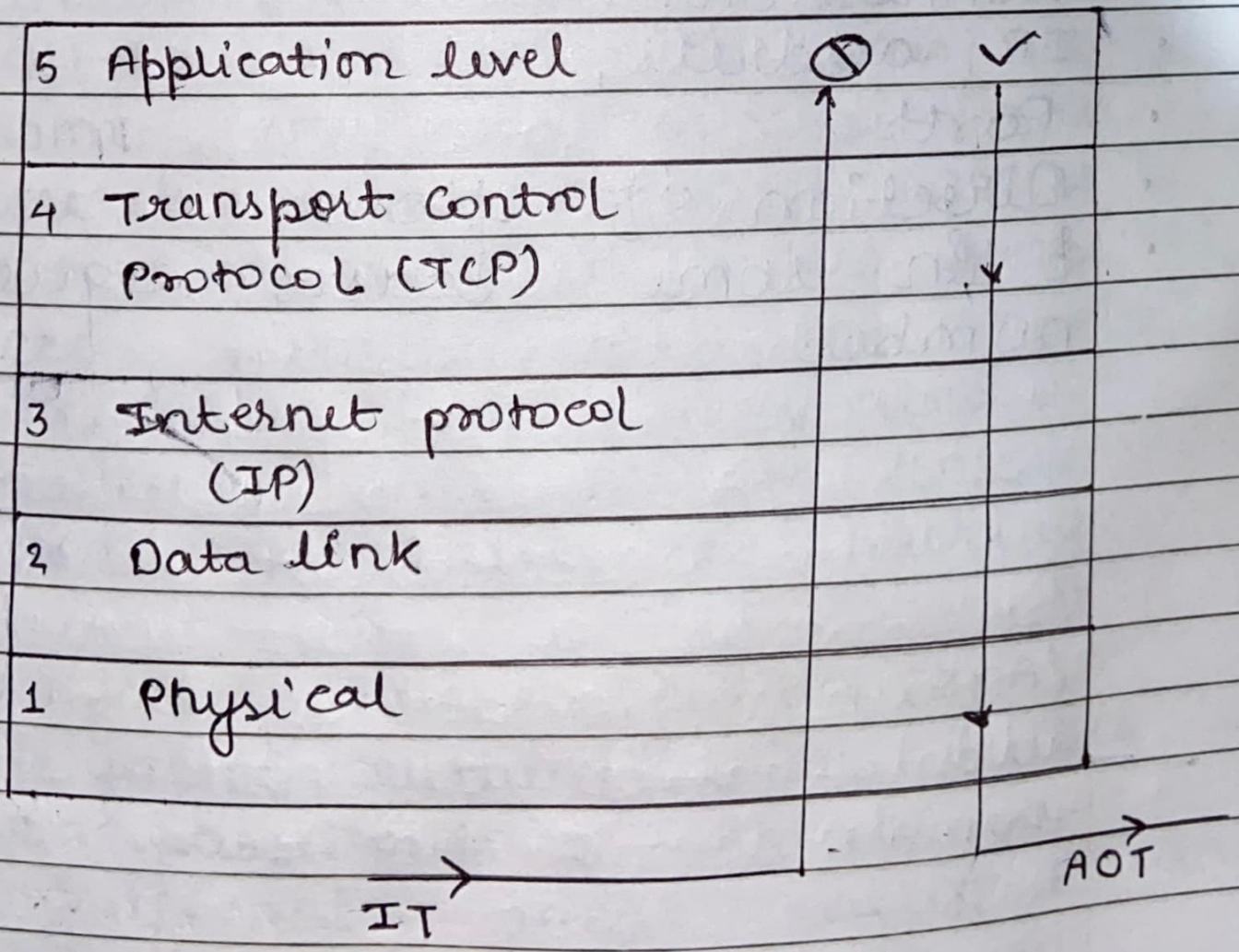
v. Direction (Engress or egress).

vi. Packet state.

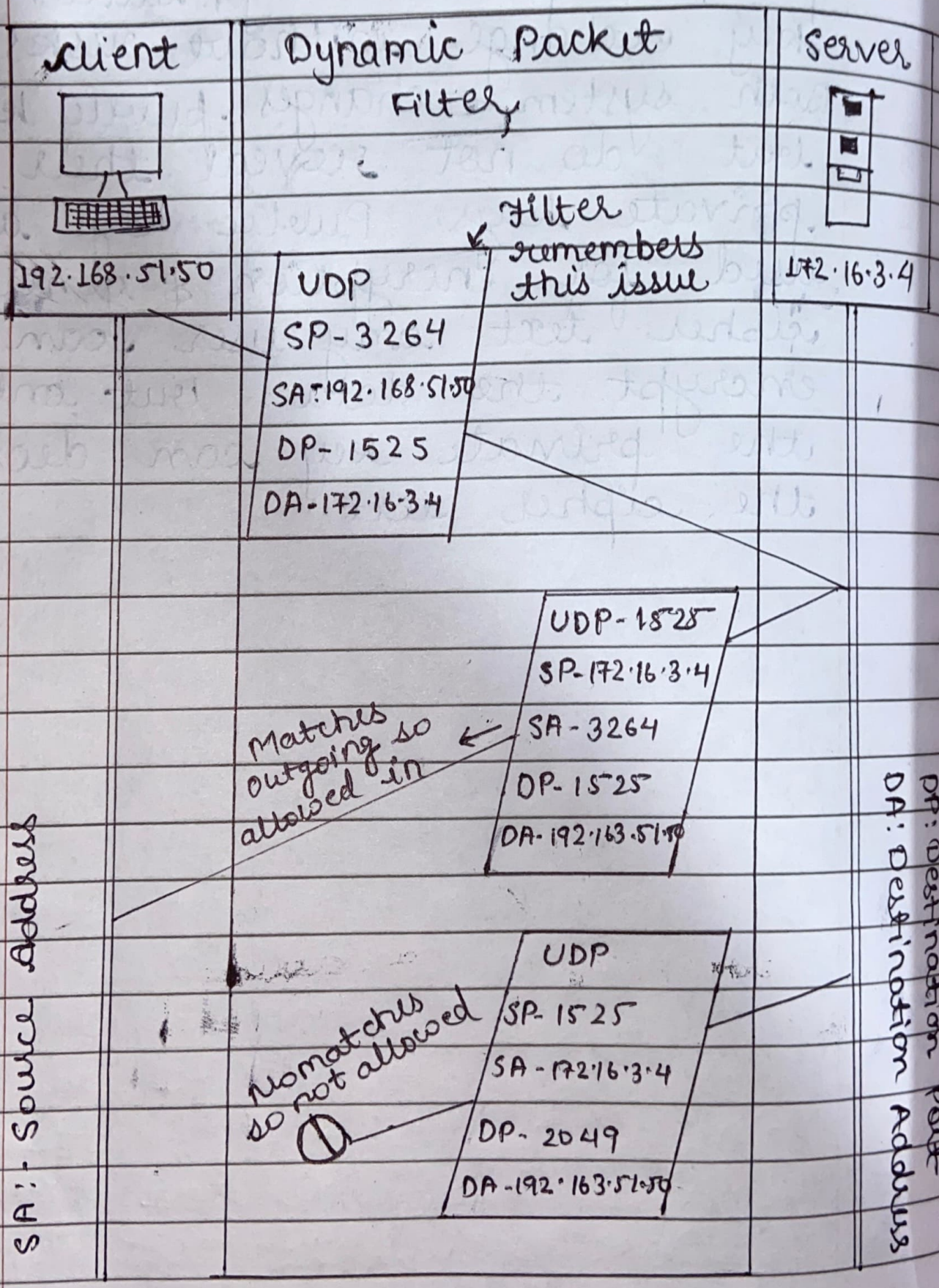


* Application firewall (Application layer): Firewall acting at appⁿ layer inspect a traffic at much higher level then traditional firewalls. They can be n/w devices placed at inline, proxy server to handel specific traffic or applications running on a server to filter traffic to a particular

program. Firewalls on the application level operate differently to those on the n/w layer because of how data is transmitted accross the n/w. Each chunk of data consist of two parts: 'the header' & 'the payload'. An app^n layer can inpect payload, header & packet together.



* Stateful multilayer firewall: It can identify conversation & track activity to deny new conversations connection from a hostile n/w, while permitting established connections to traverse the firewalls. This is achived through an internal table of attributes for each connections:
  - IP address,
  - Ports,
  - Direction of flow,
  - & in some cases sequence number.


Client
Dynamic Packet Filter
Server
192.168.51.50
172.16.3.4
Filter remembers this issue
UDP
SP-3264
SA:192.168.51.50
DP-1525
DA-172.16.3.4
UDP-1525
SP-172.16.3.4
SA-3264
DP-1525
DA-192.163.51.50
Matches outgoing so allowed in
UDP
SP-1525
SA-172.16.3.4
DP-2049
DA-192.163.51.50
No match this so not allowed
SP:- Source Port
SA:- Source Address
DP: Destination Port
DA: Destination Address

Q.5. Explain different authentication methods.

Ans. The different types of authentication methods are as follows:

1. Password authentication:
Anyone who uses internet is familiar with passwords. It is the most basic form of authentication. After a user enters his/her user name, they need to type in a secrete code to gain access to the n/w. If each user keeps this code private, the unauthorized access will be prevented. However, even secrete passwords are vulnerable to hacking.

11. 2-factor authentication (2FA):
2-factor authentication builds on passwords to create a significantly more robust security solution. It requires both a

password & possession of a specific physical object to gain access to a network - Something you know & something you have.

Eg:
ATM → PIN (4-digit) → OTP

iii. Token based authentication:
Some companies prefer not to rely on cell phones for their additional layer of authentication protection. They have instead turned into token authentication system. It uses a purpose built physical device for 2FA. This may be a dongel inserted in a computer USB port or a smart card containing a radio frequency identification or near-field communication chip.

iv. Biometric authentication:-
Biometric systems are cutting edge of computer authentication methods. They rely on user's physical characteristics to identify them. The most widely available biometric system used are finger prints, retinals, axiris scan, face scan, voice recognization. Since no two users can have same (exact) physical features.

Q.6. Explain Hacking & intrusion.

Ans. Intrusion :-

- Attempts to compromise the confidentiality, integrity, availability or to bypass the security mechanism of a computer system or networks.

- Intrusions have many causes such as malwares, attackers gaining. Unauthorized access to system from the internet, & authorized users of system from the internet, & authorized users of system what misuse their privilages or attempts to gain additional privilages for which they are not authorized.

- Although many intrusions are malicious in nature many other are not.

For eg:
A person might mistype the address of a computer & accidentally attempt to connect to a different system without authorization.

Hacking

Definition
Hacking is an attempt to exploit computer system or a private n/w inside a computer. It is the unauthorized access to or control over computer network security systems for some implicit purpose.

Description
What is a hacker? They are assumed to be intelligent & highly skilled in computers. In fact, breaking a computer system requires more intelligence & expertise than actually creating one. There are no hard and

fast rules whereas we can categorize hackers into neat compartments. In general, computer parlance, we call them white hat, black hat, gray hat. White hat professionals checks by hacking their own security system. To make it more hack proof. Black hat hackers hack to take control over system for personal gains. Gray hat contains curious people who have just about enough computer language skill to enable them to hack a system to locate potential loop holes in a n/w security system.

Q.7. What is Identity theft?

Ans. Identity theft occurs when someone uses your personal identifying info and pretends to be you in order to commit fraud or to gain other financial benefits. your personal identifying info could include your full name, home address, email-address, online login & passwords. social security number, driver's licence plates, passport number, or blank SIC number. Once, thieves access this information, they may use it to commit identity theft or sell it on the dark web.

There is how identity thieves might use our personal info for some major misconduct.

- Open new credit cards or other line to credit using your identity.

- Make unauthorized purchases using your existing credit card & debit cards.
- File a tax return using your social security number in order to claim your refund.
- Use your health insurance to get medical care.
- Pass an employment background check, or rent an apartment using your identity and financial standing.

Ways to identify thefts:

- Phishing
- Skimming
- Wifi - hacking
- Dumpster diving

Q.8. Explain in details about cyber crime?

Ans. Cyber crime or computer oriented crime, is a crime that involves a computer and a network. The computer may have been used in the commission of crime, or it maybe the target. Cybercrime may threaten a company, person or a nation's security and financial health.
There are many privacy concerns surrounding cyber crime when confidential information is intercepted or disclosed, lawfully or otherwise. Internationally, both governmental & non-state actors engage in cyber crimes, including espionage, financial theft and other cross border crimes. Cyber crimes crossing International borders & involving the actions

of at least one nation-state is sometimes reffered to as cyber warfare.

Types of cybercrime:

- Email & internet fraud.
- Identity fraud (identity theft).
- Theft of financial or card payment data.
- Cyberextortion (demanding money to prevent a threatened attack).
- Ransomware attacks (a type of cyberextortion).
- Cryptojacking (hackers mine crypto currency which they don't own).
- Crypto espionage (where hackers access govt. or company data).

Most cybercrimes falls under two main categories:

- Criminal activities that target.
- Criminal activity that uses computer to commit other crimes.

Example of cybercrimes:

- **Malware attack:**
A malware attack is where a computer system or network is infected with a computer virus or other type of malware. A computer compromised by malware could be used by cybercriminals for several purpose. These includes stealing confidential data using the compiler to carry out other criminal acts, or causing damage to data.

- **Phishing:**
A phishing campaign is when spam mails or other forms of communication are sent in mass, with the intension of tricking recipients into doing something that undermines their security or the security of

the organization they work for.

How to protect yourself against cybercrime:

- Keep s/w and OS updated: Keeping over s/w & OS upto date ensures that you benifit from the latest security patches to protect your computer.

- Use antivirus s/w & keep it updated: Using antivirus or a comprehensive internet solution like NPAV is a smart way to protect your system from attacks.

- Use strong passwords: Be sure to use strong passwords that people will not guess and do not record them anywhere

Date:
P. No: 28

- never open attachments in spam mails:

A classic way where computers get infected by malware attacks & other forms of cybercrimes is via email attachments in spam email.

Q.9. What is penetration testing?

Ans Penetration Testing

- A penetration test or pentest is a test evaluating the strength of all security controls on the computer system. Penetration test evaluate procedural & operational controls as well as technological control.

- A penetration test involves a team of security professionals who actively attempt to break into one's company's n/w by exploiting weakness & vulnerabilities in one's system

Method of penetration testing:-

- using social engineering hacking techniques to access system & related database.

- Sending of phishing emails to access critical accounts.

- Using unencrypted passwords shared in the n/w to access sensitive database.

- These attempts can be far more intrusive than a vulnerability scan and may cause a denial of service, increasing system utilization, which may reduce productivity & corrupt the machines.

Example tools for penetration testing:

- Kali linux :-
- Milasploit
- Wireshark
- Burpsuit
- Nessus
- Hydra, etc

Q.10 Explain control flow integrity?

Ans. CFI or Control flow integrity

- It is security policy.
- Execution must follow a path of a control flow graph.
- CFG can be pre compiled.
- Source code analysis.
- Binary analysis.
- Execution profiling.

Features:

- Protects against powerful adversary with full control over enter data memory.
- Widely applicable language neutral : requires binary only.
- Probably : correct & trustworthy formal semantics ; small verifier.

- Efficient
  0-45% in experiments, averages 16%.

CFI advisory model

CAN

- Overwrite any data memory at any time.
  Eg. Stack, heap, data segments.
- Overwrite register in current context.

CANNOT

- Execute data
  -NX takes care of that.
- Modify codes text segment usually read only.
- Write to %ip true in x86 overwrite registers other context kernel will restore rest.

CFI Summary:-

CFI ensures that control flow follows a path in CFG control flow graph.

- Accuracy of CFG determines level of inforcements.
- can build other security policies on top of CFI.

Q.11. Explain different security features available in UNIX.

Ans. UNIX security features:

* Each user has his own set of files
- Simple way to express who else can access.
- All users possesses run as that user.

* The system owns a set of files
- Root user is defined for system principal.
- Root can access anything.

* Users can invoke system services
- Need to switch to root user (set UID).

File permissions

- The permissions for the owner.
- The permissions for the group that may use this files.

- The permissions that apply to all the other accounts.

Each set may have none or more of the following permissions on the item.

- Read
- Write
- Execute

* Data Verification:
To create a checksum for a file, or to test a file against a checksum, use the SHA1 sum utility.

* Secure remote access with open SSH:
- Remote command line access.
- Remote command execution.
- Remote access to graphical s/w.
- File transfer.

Q.12. Write a short note on cryptography.

Cryptography :

- An encryption algorithm (E) is used to convert plaintext (P) into ciphertext (C) & viceversa. Most cryptographic systems incorporate random numbers algo. This random number generator (R) is seeded with a specific value. The seed & plain text generates the ciphertext. A key (k) may be used as the seed value. Hence,
  $E(K, P) = C, D, (K, C) = P$

- Without a key, the algorithm performs an encoding not an encryption. The same plaintext with always generate the same cipher text. An attacker knowing the algo. can readily decode the cipher text. Encryption algo use keys to vary

the cipher text; plain text, encryption with different keys generate different cipher text without knowing the correct key, an attacker can not decode the cipher text.

There are two types of primary keys:

- Symmetrical keys:
These are the keys which are same both for encryption & decryption. Risks are associated with the initial transfer of the key, but after the transfer, it can be used to safety encrypt data.

- Assymmetrical keys:
Uses one key to encrypt data & a different key to decrypt data. The key pairs, called

public & private key, allows key exchange without risks. Both system exchanges public keys but do not reveal their private keys. Public keys are used for encryption & generates cipher text any user can encrypt the data :- but only the private key can decrypt the cipher text.