SMVS
Page No.
Date : / /

Hands on Open Source

* Explain IPV4 and IPV6.

=> IPV4:

IPV4 stands for Internet Protocol Version 4 which is one of the core protocols of the Internet Protocol.

IPV4 Protocol enables device to communicate over a network.

IPV4 addresses are 32-bit numerical labels typically expressed in decimal formate.

IPV4 addresses are categorized into Five classes.

The IPV4 Header is 20 to 60 bytes long and contain Following detailes.

- Version: Specifies the IP version
- Header Length: Indicates the length of Header

Protocol: Specifies the Transport Layer Protocol.

Source Address: Identifiers the sender IP Address.

Destination Address: Identifiers the Receiver IP Address.

Version	IHL	TOS	Total Length
Identification		Flags	Fragment Offset
TTL	Protocol		Header checksum
Source Address			
Destination Address			
Options			
Data			

IPV4 supports Broadcasting, where a packet is sent from one host to all devices.

IPV4 has inherent security limitations as it was designed without robust security features.

IPV4 addresses can be classified as private or public address.

SMVS
Page No.
Date : / /

IPV4 has Address which is Unicast, Broadcast and Multicast

=> IPV6 :

IPV6 stands for Internet Protocol Version 6 which is the most recent version of the Internet protocol.

IPV6 is used to improve the limitation of IPV4.

IPV6 addresses are 128 bit which typically represented in Hexadecimal Format.

IPV6 provides a vastly larger address space than IPV4.

IPV6 supports three main types of Address : Unicast, Multicast and Anycast.

The IPV6 header is simpler than the IPV4 header which reducing processing overhead.

SMVS
Page No.
Date : / /

IPV6 Header has 128 bits and Also Includes Following:

- Version: Specifies the IP version
- Traffic class: Identifies the priority of the packet

Version	Traffic Class	Flow Label	
Payload Length		Next Header	Hop Limit
Source Address			
Destination Address			
Extension Headers :			

- Flow Label: Used For labeling packets
- Payload Length: Indicates the length of the payload

IPV6 supports stateless Address Autoconfiguration which enabling devices to automally configure their own IP address.

IPV6 Protocol provides encryption and authentication features.

SMVS
Page No.
Date : / /

* Two-Factor Authentication (2FA):

=> ~~Two~~ Two-Factor Authentication enhances security by requiring two different form of identication before ~~ga~~ granting access to an account or system.

There are main three primary factors of authentication:

1 Knowledge Factors:

This Factor includes the thing which are User Know mean Something You Known.

Credentials that the user must remember and provide to authenticate their identity.

2 Possession Factors:

This Factor includes the thing which are User has mean Something You Have.

This Factors ensure that only the legitimate user can access the system.

SMVS
Page No.
Date : / /

3 Inherence Factors:

This Factor includes the thing which user already have means Something You are

Biometric verification methods that rely on unique physical or behavioral traits of the user.

-> Advantages:

1 Increased Security: 2FA provides an additional layer of security beyond just a username and password.

2 Reduced Fraud and Identity Theft

3 Enhanced Trust

4 Mitigation of Password Weakness

5 User Awareness and Education

6 Protection Against Phishing

SMVS
Page No.
Date : / /

* MAC (Mandatory Access Control):

=> The MAC in cybersecurity is a security model used to regulates the access of users resources.

MAC enforces strict security rules and does not allow users to modify the permission.

Only a central administrator or the system defines and manage access policies.

Users cannot change access rules, they are strictly enforced by the system.

MAC is highly secure but can it can be rigid and more complex to manage compared to other access control models.

Each user and resource is assigned a security label, which consists of a classification level.

SMVS
Page No.
Date : / /

MAC uses specific policies such as Bell-LaPadula and Biba

Bell-LaPadula mainly focused on confidentiality and Biba is mainly focused on Integrity.

MAC can prevent unauthorized users from accessing sensitive information.

MAC helps enforce separation of duties by controling who can access or modify information.

MAC systems often have robust logging and monitoring capabilities which allowes organization to audit access to sensitive information.

Some MAC implementation support dynamic access controls that can change based on the context.

The rigidity of MAC can lead to challenges in usability and flexibility.

Date : / /

* Bridging :

=> Bridging in cybersecurity refers where different networks or segments are connected to faciliate communication while maintaing security control.

Network Bridging involves connecting two or more separate network to enables communication and data exchanges between them.

Bridging can introduce vulnerabilities, if not properly secured as it may allow unauthorized access to connected networks.

Bridged network can be monitored for suspicious activity using Intrusion Detection System.

A Bridging Firewall can inspect traffic parsing between two networks at the data link layer.

SMVS
Page No.
Date : / /

Bridging can be applied in Virtualized environments where Virtual LANs are used to separate networks.

Wireless Bridging can be used to extend the coverage of a wireless network by connecting two or more access points.

* RAID Protocol :

=> RAID Protocol stands for Redundant Array of Independent Disks which are focused on data redundancy, performance and reliability.

RAID Protocol help protect against data loss and ensure data integrity.

Different RAID levels provide varying balance of performance, redundancy and capacity.

RAID 0 : Data striping without Redundancy.

RAID 1 : Data Mirroring

RAID 5 : Data striping with Parity.

RAID 6 : Similar to RAID 5 but with double parity.

RAID 10 : Combination of RAID 1 and RAID 0.

RAID protocol increase data redundancy, ensuring that even if a hard drive fails, the data remains accessible.

RAID system can tolerate hardware failures, allowing continued operation without data loss.

RAID configurations often include checksums and parity information to verify data integrity.

This helps detect and correct errors, ensuring that the data remains accurate over time.

RAID is not a substitute for regular backups but is often

SMVS
Page No.
Date : / /

Used in conjunction with backup solution.

RAID can provide immediate recovery from hardware failures while backups are essential for recovering from data corruption.