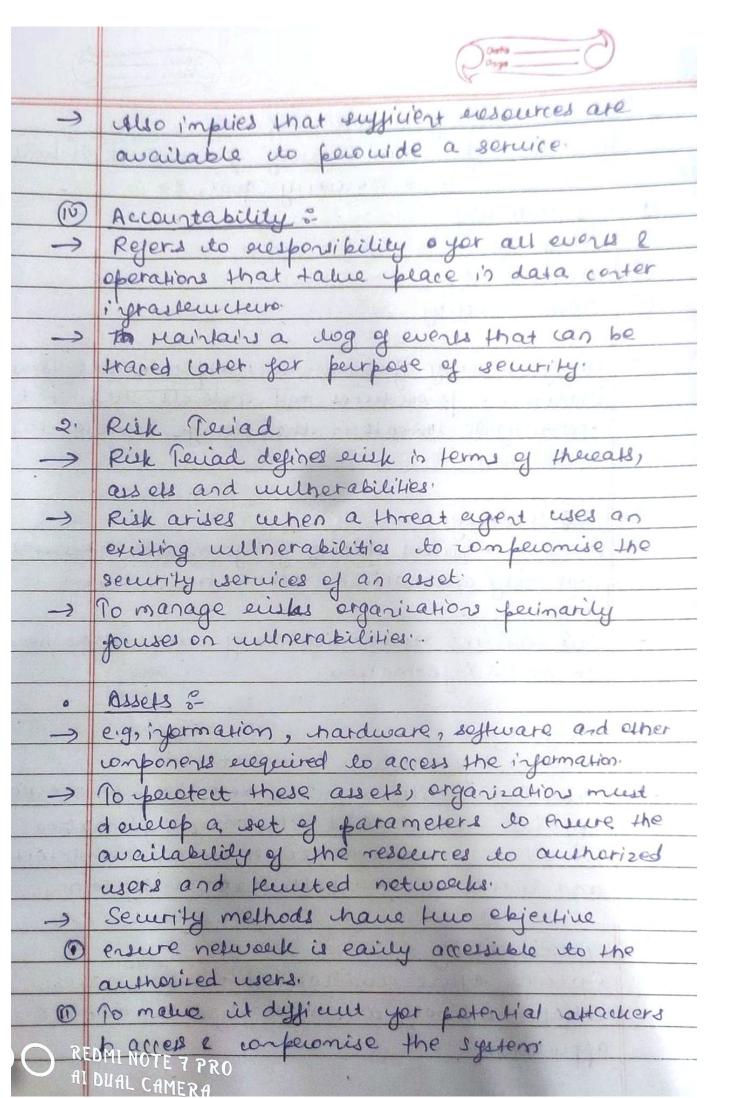
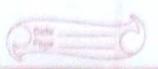
1.	Storage Sourity Framework
->	The basic information socurity guarnework is built
) - I	a achieve your wecurity goals 3-
0	Coyi derially
(1)	Thegenty
0	Availability
(10)	
•	Storage security gramework incorporates are useurity
	Mandards, perocedures and contects required
	clo mitigate threats in the storage tyraleucture
11/1/2	enuisonment.
	Control of the Contro
0	Confidentiality :-
->	Perouides required hiding of information & enurses
	that only authorized users have access to
	data.
7	this requires authortication of users who need
	to access information.
0	Integerity &
->	Ensures Typermation is unaltered.
->	Ensuring interity enquires detection & penetection
	against unautherized deletion of information
->	Perouides measures Luch as error detection
	and verrection yor both data & system.
	The state of the s
0	Availability &
->	theures othat authorized users have
	reliable & timely access do system, data &
	application.





The state of the s	
->	the security methods should becould adequate
	pereterior against unauthotized access, minuses of
	Premium colored and proper contra ", Marce Marce Colored
•	thream :
-	threats are peterial attacks, first
->	these attaces can be a time at passine
->	Active attacles :- include data modyication,
	alrial es service (Dos).
	They best threat to data integrity, availability
34.0	The a second ability
->	Passice attacks: are attemps to gain unauthorized
	access i'do the system.
	STORES TO LINE - TAKEN THE THOUSAND HAVE STRING TO A CONTROL OF THE STRING THE STRING TO STRING THE
	Vulnerability :-
->	the path that fewerdes access to Information
	are efter uninerable do peternial attaclu.
-)	Each of these path corrain various access paires
	which perouides different level of access to the
	storage resources
7	Implementing security contects at each acress
	points path is known as " Defence in Depth!"
->	Defence in Depth uses recommends using multiple
	security measures to I the eight of threats.
-)	Defence in Oepth is also known as "layered.
	applicant do servity", because there are
	muliple measures for security at different
	revels, defence in depth gives additional time to.
	detect & respond do an attack.
->	Attack surface 3 3- javors to consider whoo
	Allack rector 4 assessing the extent do
	work faisor Junion this an environment is vulnerable do security threats

	Ontra Dropa	
3.	Storage Security Domain .	
( sus	To identify the threats that apply do a storage	
	retwork, acress path to data storage can	
00	be categorized into s- security domains	
0	Application access	
(F)	Management access	
(10)	Backup, Replication and Archive	
0	Application acress Domain =	
->	included poly those application that	
Jakon Mil	includes only those applications that acress the data	
->	through file system er at doctabase interface.	
	considling user access to data :-	
	Acces contered services regulate user acces de date	
	mese sciences . Tallet les the throater of ileast	
	The second of th	
•	bers trucats affect data integerity and	
	any are a duly.	
•	Access vorteral mechanisms used in the application	
	accoss domain are user and host authorication	
1 (Line) 1	(technical vortecel) & authorization (administrating	
	confered.	
->	Zoning is a upsteral machanism on war as its	
	that segments the network into specific passes to be used you data drappic.	
	mes segment the network into specyc pains	
	to be used you data traffic.	
7	LUN masking determines which shotts can access	
	which storage denice.	
ALL MAN		



	Management Access Domain :-
->	Powerding management access through an external
	network of the potential you an our authorized
	heat or suritch les connect to that network.
->	In such circumstances, implementing appropriate
19%	security measures becovers certain types of
Contract of	remete communication yourn occuring.
->	Vering secure communication channel such as
August 1	Sewre sneu (SSH) et seure soulet layer (SSL)
	Control of the Control of the State of the S
	Backup, Repetitation and Archive 8-
-	aganization must esure that the disaster
	recovery (DR) site maintains the same level of
	security you the backed up data.
->	Peretecting Barbup, replication l'achine
11 1	ingrasteurchure requires addressing several
Mede	slattacles, DOS attacks e media theyt.
-	Such thereat expersents widetion of integerity.
	considertiality & availability.
	SAN security Architecture
gus 3	Sterage arthinetworking environments are a
	potential target yor onauthorized occess, they
	and misuse because of vartners & complexity
	y these environments.
->	security strangestrategies are based on the
101	"Defence i's Depthis concept.
->	this ensures that the jailure of one security.
	confered were net comperencise the cuses under:
	perestection.

-	-	10
0	Dafa	- [1]
1	Disgra	$\cdot \cup$
1		

		Com.
->	Security zones	Perotection Strategies
. 2	ne A Cauthorhication	· Reverite management
	management vosole]	LAN access to authorned
	A TOTAL PROPERTY AND A STATE OF	usots
		· implement tunelling for
		secure remote a well do the
	HARRIE LEGISLES AL BROWN	management LAN
		· use of two-factot
		authorstiation.
7000	B ( Firewall)	Block inapperoperate Heffic
	A CONTRACTOR OF THE STATE OF TH	by (a) firtering out address
		(b) screening yet
	The Section of the se	allowed pereforels:
	Salarature Assess	Fig. 18 fine and the second
zone (	( Access-Consered-Switch)	authenticate users of ro
302 3 T S		Sieutchos was using
		RADIUS, DH- CHAP & SOON
Zone D	( Most - 10-suntch)	Respected Faberic access
	A SHARM ON LAW TO THE	to de legitinate hous
A TEALLOW		by implementing a secure
X10		zoning method such as
		pert.
zone E	[ Switchtons to sweitch / switch	A Perotect Hayfic on
	to Reuter]	Faberic by wing E-Port
		authorication, encrypting
		the traffic in transit
×		The second second second
22:31		
~		

	6===9	Option	
2	one F( xoutance	9 mplement encryption	
	one F( pointance Extension)	yer in-yeight data	
70	ne h (switch to storago)	arrays on your san	
1980	storago)	arrays on your san	
5	Monitoring the storage	re Infrasteructure	
->	Monitoring is one of H	yor managing storage	
	that forms the basis	yor managing Horage	
	Tyrastauther sesse	ures,	
->	Perouides the perso	rmance & accessibility exakus	
	g various compone	2/8 1	
7	Helps to analyze	infrastructure resources.	
	of various eterage	infrastructure resources.	
		医侧侧侧 经保险证券	
*	Moritoring Paramet	ers ?-	
-	storage repeasement	ve components should be	
	movitored yer ?-		
	1 Accessibility		
	1 capacity		
	@ penjormance		
	@ Sewerly.		
0	Accessibility :-		
		ibility of how components or	
	sliw components involu	ves checking their availability	
	etatus by reviewin	g the alers generated by	
	Theon the uyton.		
->		ure might result in a	
	chain y availabile	ty alerts	



	Company of the second of the s
(1)	capacity 3
->	capacity mariforing ensures uninterrupted.
	data availability and scalability by
	percuring outages before they occur.
->	Inadequate capacity leads to degeraded
	perjamance.
->	Per ex: - y 801 g perts are utilized in a
	particular san yabric, this would indicate
	a now sunteh might be required in
	more arrays e servers are needs to be
	intalled on the same yabric
00	2-1-1-2-0
(11)	
->	Performance monitoring evaluates how
	officiently different storage l'yrasteurque
	components are performing.
->	also deals with utilization of resources
->	Performance measurement is a complex task
•	that involves various components on several
	interrelated parameters.
~	
(14)	
7	Helps to helk con or track unautherized
	configuration changes do storage intracteuraire
	resources de la
-	prysical security et a storage ingrateurchus
	The sales of the s
	badge readers, biometric scans er video
	cameras.

	6===0 Q===0
6	Storage Haneigemon Activities
7,	Authertication, Authorization & Kerberos in
-	PAS en wironment.
->	NAS is open to multiple explores, including
	urruses, unauthorized access & data tampering.
-	Permissions and ACLS (access voyered Valus) are
	deployed ever yorm the 1st level of beiotection
	ons eles elities by respecting accomplished
	and sharing.
V	
*	NAS File sharing: Authortication and
	authorization
	In a yile tharing environment, NAS devices we standard yile-sharing yelokulus NFS &
	use standard yille-sharing yelcholds NFSE
3	therefore, authentication & authorization are
	a the wife of supported on MAC down of the
	as in a UNIX et windows file sharing muiron
	O mea-
->	Authertication :
0	duthertication requires verifying the identity.
	of a network user and therefore inchesa.
	dogin tredential cookup on a network
	Syprimation system (NIS) server in a unix
	en wiron ment.
-4	Zinilarly, a windows went is authenticated.
	by a windows domain vortexouer that houses.
	the Active Disoctory.
	do validate network user vederties.
41	and the state of t

