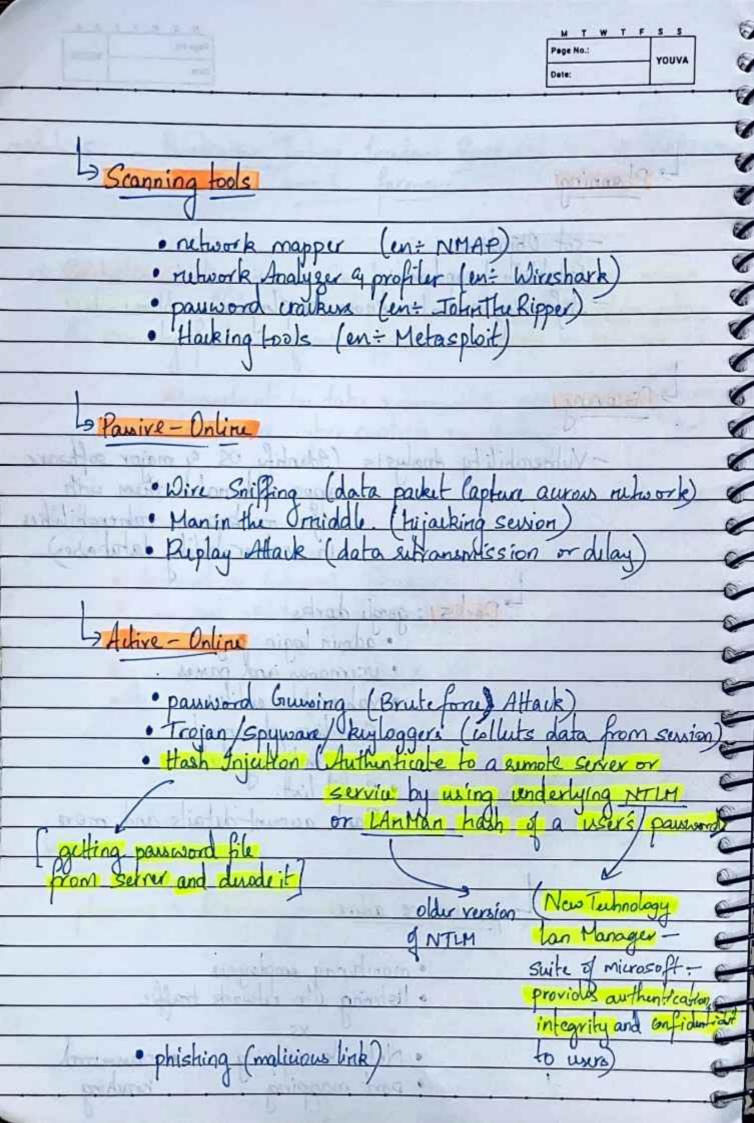
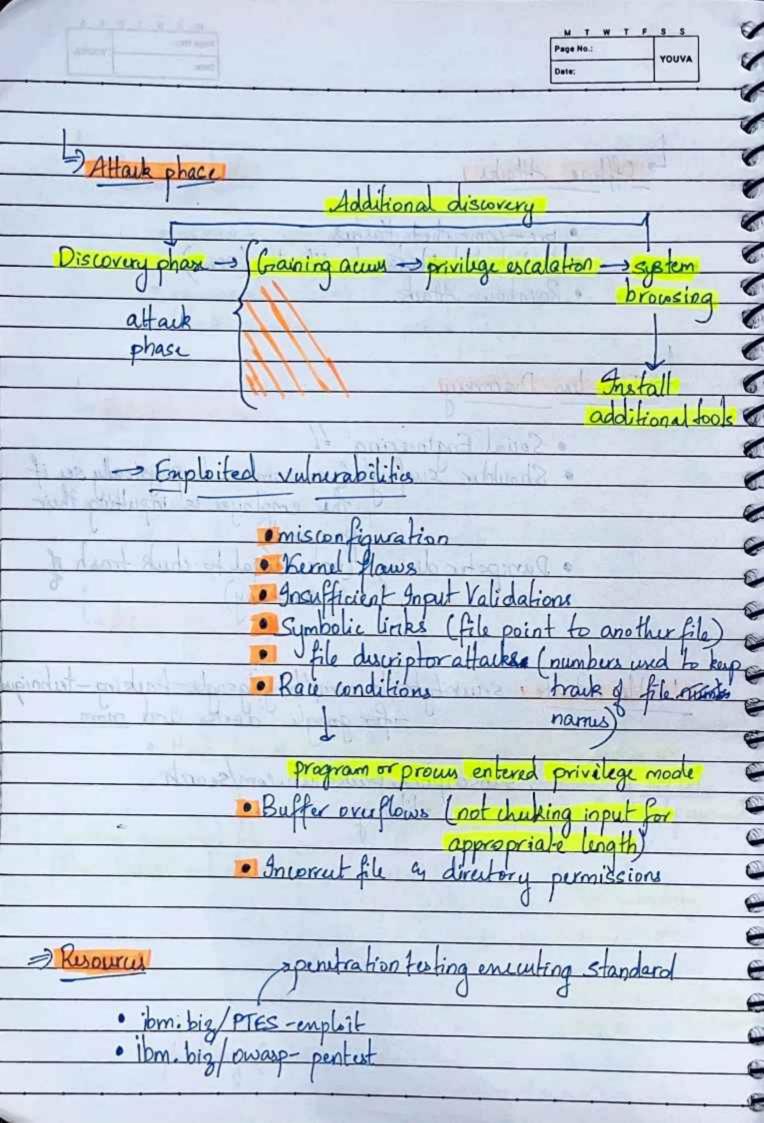


-	THE RESERVE AND ADDRESS OF THE PARTY OF THE	The second secon	r F S S
-		Page No.: Date:	AVUOY
-		10000	
-			
			100
	Planning	ter fallow	and T
1		V	
	-set Objutives	1 CO-19-1	
	- Establish boundaries	N mikam N	
	- Informing need-to-know employ	us	
	Parile (ent Melacobil)	midwell o	
		v	
	13 Discovery	1.0	
		analold - 25	- 01
P	- Vulnerability Analysis (9 dentify	os a mai	or software
P	apps and	match the	em with
-	CHARLES CHICAGO OF	known v	uherabilibes atabases)
1	(unlike a ansolumentis or dias)	ecability d	atabases)
-		4	
-	Dorks : google dorks	Seal A	41
-	· admin login	pagus	mille XX
	· Usernamus and		
	· ruberable ex		
	· Sensitive do		-
10	Most militare Prail list	agra)
1	Bank august	م ماناما م	V
10		- Altais a	
Tu	No.	ink has 15	T Po Political
Ta	pasive vs active	ANIAS DIVINI NO	The latest
Ta	- Usano Y nal Mila		
1	- Alezanda to the manifering ample	uta it	
1	• monitoring emplo	early tralle	
	VC VC		
-	· Network mapping	0 0	and the
-	· Network mapping		makim



	A TOTAL STREET	M T.	WTFS	
	40	Date:	YOU	JVA
				4
	- Offline Attacks	43500	g skielija	6
	Character lengthish		1	18
	pre-computed Hashus	CARLES OF		
	· Distributed Network Attack	e (ONA)	0 10/21	21(1)
	· Rainbow Attack		10	
		1/1 1	010	
1.8	A CONTRACT TO SERVICE AND SERV	11 0	phas	
1	42 Test-lus Discovery			
1	300- Lancelle 10	-/		
70	· Social Engineering			
T	· Shoulder surfing (use so	mion top	ysically	suif
TO	1 The en	playee is	inputton	their .
10	Pauson		1	1
10	· Dumpster diving (not ill	igal to ch	uk tras	hop
10	a comp	any)	17.16	7
-	THE WATER ST TOLOG OF THE STATE	4		
	All the little of the little o	* /		
	Notable website securitytrails com/bla	g/google-	hacking	-technique
	-for google	docks	nd mon	œ
	haltete or Delawations privilege mode	, ,		
	: subscription. packthub.	Com/Search	2	
	"Hard directions Tuprary	21.0		
	The state of the s	λ		
0	The Sharp of the A of There is	19		
2				
0	broken to prime une contract or the land			
1	The Designation of the second	1	E THE	ible .
I.A.	The second second second	A Comment	1	Till I
-	A control of the later of the l	a. b. 1913		
1	-401 H. Comban Desiran -ox	our god o	*	



		ALCOHOL STATE OF THE STATE OF T	M T W 1 Page No.:	
		WHERE SHARE	Dete:	YOUVA
		(200)		
	3	> Reporting	vanish of	faction &
	3			
	4	- Enculive Summary (who, what	-when where	of testing)
		Barkground	contracts to	8 3
	5	overall posture	1 2.	
	1	Risk Ranking	feel the	tind up
	0	6 General findings	De 10 miles	
		Recommendations	0	
		Roadmap		
TI	3	high livel de	tail	
H	-8		plakens not	T 21 6=
1	-61	> Tuhnical Review (why and ho	w of testing)	
1	-	ALL GALL		0 1
+	0	· Introduction (person in	volved Contact	
+	>0	· Scope · Vumerability Assument	bearing to the	involved et
7	1	· Vulrerabilety Confirmal		
1	0	· Vulnerability Confirmation	00	
	(8	- Risk/Enposure	w	
1	-	A Control of the Cont	rg	
1	2	Was the Control - Among The	10	
100	2	The second secon	10-	
	ور	toolah Shara bar . 199 Alahan	0	
	2	> penetration Tools for pentuling	4	
Ļ	1	Declaration or annual annual	lis.	
4	2	- Kali Linun	7	
4	1	· map.org !! (for CEH)	
	1	• JTRipper	(@ ib	m. biz/ <tool-< th=""></tool-<>
	1	· wireshark	non	u>
	2	- HTP (- 1.) 1		
	1	- HTB (practice) - lamewalkth	rough.	
	-			

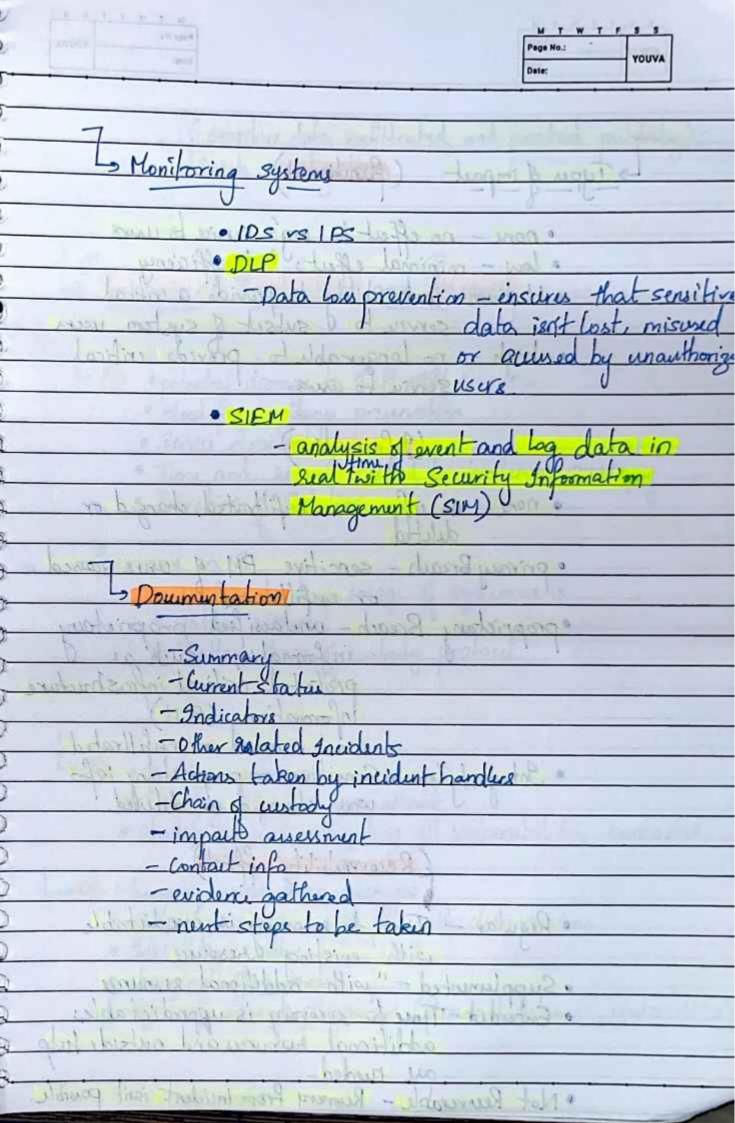
		M T W T F	,,
		Date:	YOUVA
		(W	
		_	
=> Incident Response		Torte	mare 6
	2 2	30	
Event: something not with ses	put to nom	nal behav	iour
of system or change	to normal be	naviour	6
O Comment	William Course		9
System or organization	gative impart	on the	
System or organization	Sont Instant	4	6
unc.	The Disputation Lot	9	0
At the Armit she	opalas.	4	
=> 1R Team models	-		
- Iram models	. 1	1 - 6	
Contral (Single suppor	c. Lan	STAMIN V	
• Coordinating	- Dor office		
· Coordinating	1 11 9		•
- Inmental	Lumeran da	10	ALL BLU
- wlationship with	other fearis	Vauas to	bokfor
	Flora La	1	
· management	troop Alder	0	
Information	Assirance		
O IT Support			The state of the s
· legal		011	
Public Aff	ains and med	ia Kulation	
Human Re	sources	soll Anda	HUNT E
Businus Co	ntinuity plann	ing	
thysical S	ecurity and f		anagement.
	D. Owa got	200	(
THOUSE COLUMN SITE	1. 1	ACCOUNT OF	
		1 117 705 8	
smeaso la chemicale		e wittelsor	
- LANGE AND THE PROPERTY OF THE PARTY OF THE	10-02- 1-01371037	1 1 1 m	

		MTWT	F 3 5
	AVIIII4	Page No.:	YOUVA
-		Date:	
	15.4		
-	5 Common Attack Verbore	marke of a	ا المالية
7			
	Fortage 1 1 Page 11 1	John State of Drug	Ti de la companya de
	Attrition (Sustained or weakin defe	wa	1-1-
1	HAMITION (Sustained or	persis ton t after	aut do
1	weakin defe		
-	- Email	mark mosts M	0
	• Impersonation	Pulse 2 seren	41
	loss or theff of equipment		
10		1-11-1-11	Secretary.
	The state of the s	1 22	
	5) Incident Ruponse phase (NI	ST framework)	
		PARTITION OF THE PARTIT	
1.0		* 120 Pm	
-	Properation Detailion as 1	potainment =	- Post-
10		entainment =	- Post-
	Analysis	Eradication 4	
	Analysis		Post- Incident Activity
	Analysis	Eradication 4	
	Analysis	Eradication 4	17
	analysis day	Eradication 4	
	Note : Sans Equivalent	Eradication 4	Activity
	Note : Sans Equivalent - preparation	Ruovery	Activity
	Note : Sans Equivalent - preparation - identification	Eradication 4	Activity
	Note: Sans Equivalent - preparation - identification - Containment	Ruovery	Activity
	Note : Sans Equivalent - preparation - identification - Containment Eradication	Ruovery	Activity
	Note: Sans Equivalent - preparation - identification - Containment - Eradication - Recovery	Ruovery	Activity
	Note = Sans Equivalent - preparation - identification - (ontainment - Eradication - Recovery - lesson learned.	Ruovery .	Activity Activity
	Note: Sans Equivalent - preparation - identification - Containment - Eradication - Recovery	Ruovery .	Activity Activity
	Note = Sans Equivalent - preparation - identification - (ontainment - Eradication - Recovery - lesson learned.	Ruovery	Activity Activity
	Note: Sans Equivalent - preparation - identification - Containment - Eradication - Recovery - Lessons learned.	Ruovery	Activity Activity
	Note: Sans Equivalent - preparation - identification - (ontainment - Eradication - Recovery - lessons learned.	Ruovery	Activity Activity

	Date:	YOUVA	1
		10	-
	t ho	Ve C	1
> The best offence	ALDEN STORME		1
	A control		1
· Risk Accessment	A THOUGHT		1
Host Security	The Va		-
Metwork Security	part of prep		-
Malware Prevention	home Oc		_
· User aware run and training	bushle 18		_
- Annual of the	NO 300 100		-
			4
Preperation			-
2 Arquakimi			~
-Incident Ruponse Policy	more balance	(4)	~
• IR Team			
· Roles	1 straige con	- radaba	1
• Means, Tools, Russines (identifier Policy Testing (person suspensite Action	y and have con	Dromise Cal	
Policy Testing (person suspense)	te for terning pol	(y) -	
· Action	//	- 6	
	-//	-	-
	1 1 0 1	0 .	
Note: Documentationisto JR as an Air Ta	na is to Suba	Diving	
	admired and		
	INSIN CO		
> Defetion and Analysis	a timbi-	-	9
The state of the s	minted -	4	1
- Precursor: sign that an incident	dent may occur	y of	1
- Precursor: sign that an incide	observer log enh	ries of	+
sh	owing usage of v	ruln scanner)	+
-Indicator: sign that an incident	dust may hour	4	-
odured or may be	Maurica nous		
- sangu si may ve	The state of the s		
CAn	tivinus software o	derts	1

malwaye

intertion)



(functional) La Types of impact

- · none no effect to orgs service to usurs
- · low minimal effect; lost efficiency
- · Medium lost ability to provide a critical Service to Subset of System users
- · high no longerable to provide critical Service to users

(Information)

- · none no info was enfiltrated, changed or deleted
- · privary Breach sencitive PII of usus auscal
- proprietary Breach undassified proprietery information, such as protested critical infrastructure information (PCII) was accused or enfiltrated
 - · Integrity loss Sensitive or proprietary info was changed or deleted.

(Recoverability effort)

- · Kegular Time to survey is predictable with enisting resolute
- · Supplemented " with additional susource
- · Entended Time to secovery is uppredictable; additional suburus and outside tup are nuded.
- · Not Recoverable Rusnery from incident isn't possible.

	lu.	M T W T F S S
1		Pege No.: Dete: YOUVA
1		
1	-	Complete II - All II - II II II
-	-	(sensitive data enfiltrated and posted publicly);
-	-	Trainin invistigation.
-	-	
5		to note a manufacture of the contract of the c
1	10	Containment, Fradication and Recovery
-	13	containment, tradication and Recovery
-	7	Abeliana June 12
-	7	
-	7	· potential damage to theft said resources
		· Need for evidence preservation
		· Service Availability
		· Time and swards needed to implement strategy
		· Duration of Solution
/		- Property of the second secon
-		- Forensics in IR
	-	· eaphere backup image of system as-is
-		gather evidence
		follow chain of waterdy protocol
	(3)	A Sulfavora Albusta
		A Date and the contract of the
	هيا	(a) edeleties coolers
100	9	• disabling breached user account
	9	· identificance and it is it is the
	1	· identifying and mitigating all vulnerabilities emploited
	10	Burrery using clean backups
		· replacing compromised files with duan versions
6	-0	Installing patches plus with dean versions
	-	changing passwords
		· tightening disagree on 1 10 11
-	1	· tightening detwork parameter (Grewall rulesets, router ACLS)
-	G	The state of the s
		The Manufacture of the Country of th

	M T W T F S S Page No.: Date: YOUVA
· high level testing, monitoring al	iployed.
J O winserde O	Letter ST
501.11	
Distinuident	n n 1 1
· lessons learned	Atronogiumna C
	1
- Utilizing data Collected (enviewing suspone - Evidence Retention	times, system imparted by
- Documentation	A Transfer of the Control of the Con
- Adaltin	L'insue o
	one wit .
=> Incident Rusponse Demo	training of
	At my solenous and IR
to content impact of our en april	
	1 8 GA-FLA
· Software Attacks	Cardinal
· Data enfi	
Information Sabotage	
· Theft of equipment	
lating long rest in many to mis making here	
L) Affack Vectors	the the
- capacita when the limit	in provide the
website wing hosting malicio	ent info for
Counter durius or cipps or including log info McAfu epoling Ordnunator	our hereork
mechanism including log info	from OS)
New generation figural	and the same by take
C TOTAL OF THE COUNTY	

1-1	1	Page No.: YOUVA
1	7	Date:
-		at he was not make the war interstight to
	-	La 1R prous
	-	
-	-	· preparation (contact shareholders, teams involved)
		· Detution & analysis
	10	· Containtment Fradication & Revovery
	1	· Post graident Activity
	10	the deal of the formand of the first of
	1	Cina belogar 199 has 1812 / affected and
	1	Jusing Bradar we see multiple information like
	1	Wind Philat Person of anylis and consult
1		Description
-	-	Log 10 + + + + + + + + + + + + + + + + +
4	-	offense type
-	-	offense Source
-	-	Magnifude mondant
4	10	Dertination 18
4		Dutination 18 - Indian - 1981
4		CENTRAL LOG Source States - 2381 .
4		V O I son to the latest of the
4	رفعيلا	flows
	عر	of most amount of dealer to the
-21	رور	- Clicking on any of the offenses, brings us to the summary page giving us different details, including Top 5 Source Its dust IPs, log sources.
		page giring us different details including Too 5
1	1	Source Its dust its log sources.
4	1	The state of the s
		- Main thing to notice is top 5 Annotations.
	الز	D. Mariell I. A. Commission of the Commission of
	1	-Going through the wents to get more details (DNS gueries, sisk meter, threat, etc.) To sheek it out, go to events, dick on Event/flow count
	1	Thisk miter, threat, etc.)
		10 their it out, go to events, dick on Event/flow count

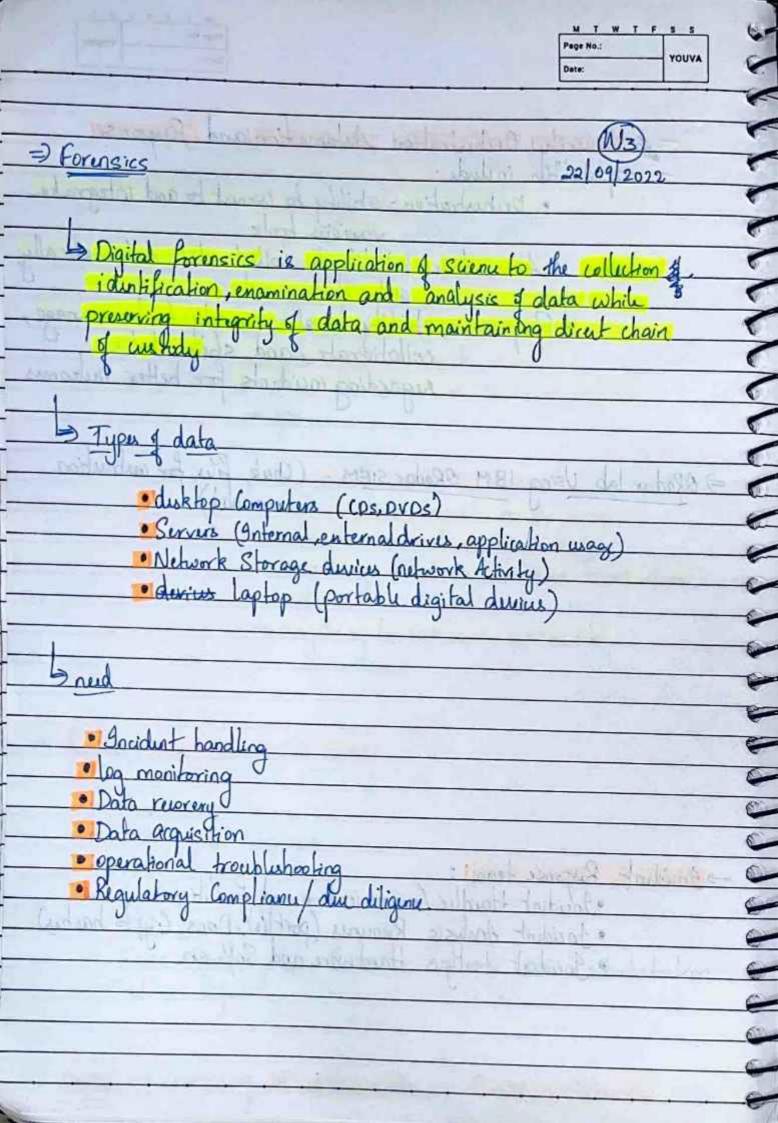
M	T	w	T	F	3	8
Page	No.:				YOUVA	
Date:					1	UVA

				M T W T F	3 5
				Date:	YOUVA
-Then	we note a	dent Repons	Cormation	to proved	to
step	2 of Inci	dent Repons	AND AND	na Ale	-
	V			A	-
-Jn a	n Snudent	Ruponse	orm, we	have:	1
Tage	- Jupe	on Source:	grudent:	DNS gury h	known
	Verus	ment: LAB	Okadar	9	Domet
		ame: LABPC		900	1
		ano: 192.16		Clarked one)	6
- 35	Webser	ver: No. (s	system is a	workefal	rion)
oue v	Public	IP: 8.8. K.8	(googlis	DNS Serve	5
			60.0	010	
	###+	+++++	####	###	
			Scare applied	0	-
	start 1	rewroting wi	nat time w	e found 1	he o
	Inform	nation	Un utilizado	COLUMN TO SERVICE STATE OF THE PERSON STATE OF	-
	n = 1309 -	weberdut to	Cornlini		-
	1002	www.ro	discov	(vied)	ing -
	• 1303 -	workstation	192.168.	4.6 LAB	P(02
imestamps ?		(found out)			nom
1		our workst	ation)	1	
	1307 -	Submit Hicke	it to retwo	rk team	to c
Summany		disable swift	port.	on outsid	- 0
2 0a	1309-	Kick off med	LU ENS F	Il sian	
	1915-	Reviewed McA	tee ENS	ill Scan su	
		Rusmound sy		A see Albertal	N- 0
	• 1500 -	Submit ticket	to have a	istam wine	201
January 2019	Lordon	and Short	Hara with	The state of the s	ind - o
			Anto Law		
	13 D PL	N N	100	1 2	6

-	Abraga African	M T W T F S S
-		Date:
-	.0)	
-	- After doing all that, we can send to and allow them to process it and as	he information up
3	and allow them to process it and as	rehive it.
7	THE PERSON OF TH	THE RESERVE THE PERSON NAMED IN
7	- Now that the invertigation is done, we	don the incident
0	- Now that the investigation is done, we - Reason for closing - closed; testing - Note - copy paste the incident support	0
3	Note - copy paste the incident suppor	me form.
7	- If we see any false positives, en a	Inal I foral proc
8	Attack, it might just be an user u	orking with
7	sever to develop application using	an API
2	- So multiple 442 is expected (sew) for that system from workstation	on open closus
8	for that system from workstation	
-8-	- So we upse the Offense Stating.	Season: Non-gasive
-	- Note The rule threshold has bus	inward.
0	- lusers the amount of false positives	
(Notice State	
()	The state of the s	
	9 So to summarize IR prous	
-		
	Step 1 was preparation - know what to look for - know what assets we're - Events to brigger on - people to contact in case	Strong but the to
-	- know what to look for	
-	- know what assets we're	moniforing -
	- Even's to brigger on	1-19 Dect
	-people to contact in cas	e of incident
1	o step 2 may 2 lal 1 1) semile
0	= anthread and tralysis	d officiality
1	- revent exerts that him	101 to 10
-1	- gather information - remark events that brigger - determine if event is real	a alore
1		
1	of the automated and threat intelligence.	niaidras e. II es E

Page No.: YOUVA
Date:
· Step 3 was Containment, Eradication and recovery
- disconnect from network
- contact team for those network
eonnutions
- look for other threats
- look for areas that it might have
spread to
- get system back in state
- give direction to seimage System
- composition of the composition
to all the second that the second is the second to
· Step 4 was post invident Autivity
- after action report to be made
- include mistakes committed
- anything that could have been done
better
- anything to increase efficiency.
Automate St. Science Sci. S. S. S.
=) free and open source IR tools
1 - 10 - 10 - 10 - 10 - 10 - 10 - 10 -
- (yn+ 360
- GRR Rapid Ruponse
- Alien Vault
- Cyphon
- Sons Investigative forensics Toolkit (SIFT) Workstation
- Volatility - Sons Investigative forensics Toolkit (SIFT) Workstation - The Hive Project
J. 1752 of Sugar Str. Representation
5) SOAR -> combining 1R, automation and threat intelligence.
= 8

1	Page No.; Pute:
	- go Security Ochubration Automation and Ruppinse
	- ge Security Orchestration Automation and Ruponse
	· Orchestration: ability to connut to and integrate
	vourious toole
	- Automation - ability to collect data automatically
1	and extrict events:
1	· Response: ability to allow analysts to manage, collaborate, and share data
1	sigarding incidents for better outcomes
13	Augus aing militaries for perfer currons
	Para de de la constitución de la
1	=) ARadar lab Using IBM QRadar SIEM (Chak files for instruction
-	(savasas) surmanial)
-	(Raterial satisfaction application user)
-	Coloit Average agent 2 should be
-	The full between the pale of the stands
	The state of the s
	probability
1	Company to the company of the
1	Maria La Calle
	- gruident Rusponse team:
	· Incident Handler Communication and Pailter
	· Incident Analysis Resources (portlist Docs, Couple hashes)
1	Incident Analysis Resources (portlist Docs Crypto hashes) Incident Analysis Hardware and Software
1	A Company of the Comp
1	
-	
-	



Forensic Prous Collection Financination Analysis Reporting The property Computer at home office Alternate Sources of data Rushrake maniforing	A355		MTWT	133	
Collection Financination Analysis Reporting - more Types of data Finternally owned preparty Computer at home office Alternate Sources of data logs Kuystroke maniforing	-	aviety and a second sec	Page No.1	YOUVA	
Collection Financiation Analysis Reporting - more Types of data - more Types of data - faternally owned property - Computer at home office Alternate Sources of data - logs - keystroke manitoring	-		Dete:		
Collection Financiation Analysis Reporting - more Types of data - more Types of data - faternally owned property - Computer at home office Alternate Sources of data - logs - keystroke manitoring					
Collection Financiation Analysis Reporting - more Types of data - more Types of data - faternally owned property - Computer at home office Alternate Sources of data - logs - keystroke manitoring			S. Stabille 12	NATA.	
Collection Financiation Analysis Reporting - more Types of data - more Types of data - faternally owned property - Computer at home office Alternate Sources of data - logs - keystroke manitoring	0	=) Company D.	al al all	A 19	
Enamination Arralysis Reporting - more Types of data - more Types of data - faternally owned property - Computer at home office Alternate Sources of data - logs - Keystroke manitoring.	-	Forensic Prous Familian 24 pool 1	D O O	17.	
Enamination Arralysis Reporting - more Types of data - more Types of data - faternally owned property - Computer at home office Alternate Sources of data - logs - Keystroke manitoring.	-	· Collection	Testing Wall	(child	1
Analysis Reporting - more Types of data - more Types of data - faternally owned property - Computer at home office - Alternate Sources of data - logs - Keystroke manitoring.	7		n Parkey	In the same	
Reporting - more Types of data - computer at home office - Alternate Sources of data - logs - keystroke maniforing.	7			17	
- more Tupes of data Finternally owned property Computer at home office Alternate Sources of data logs Kuystroke manitoring.	7	Anawsis (3)	L. Marie San	0	
- more Types of data Fonternally owned property Computer at home office Alternate Sources of data logs Keystroke manitoring	3	· Reporting	orkanies Espen	DE L	
- more Types of data Fonternally owned property Computer at home office Alternate Sources of data logs Keystroke manitoring	~	O The state of the	Who had	4.430	
- more Tupes of data Fonternally owned property Computer at home office Alternate Sources of data logs Keystroke maniforing.	. 8	the standard pulled and the standard and a	STREET PROPERTY	0 100	
- more Tupes of data Fonternally owned property Computer at home office Alternate Sources of data logs Keystroke maniforing.	13	A STOREST TO THE REST OF THE R			
Enternally owned property Computer at home office Alternate Sources of data logs Keystroke monitoring.	7	50	mont ullari	SIE -	
Enternally owned property Computer at home office Alternate Sources of data logs Keystroke monitoring.	7		0		
Enternally owned property Computer at home office Alternate Sources of data logs Keystroke monitoring.	-	- more Types of data			
Computer at home office Alternate Sources of data logs Keystroke manitoring.		- 3 - 6			
Computer at home office Alternate Sources of data logs Keystroke manitoring.		Entrally amed accorde	Lawrence OC	Bar	F1.
logs Keystroke monitoring.	W)	Con Lat Later Property	. Grant stance	1 . 7	
logs Keystroke monitoring.	-	111 1 C office	A STATE OF	I Co	
190 A 180 A		Alterate Solves of data	SI I I I	HON -	
190 A 180 A	-	1098	although fill will	men'l -	
190 A 180 A	-	hustroke monitoring.			
-Steps to collect data	-				-10
- Stope to collet data		*10/F3/		1	4-
The state of the s	-	- Steps to willet data	ikal ilum 4	month to the	
parabound gloss tran a boothand Charlestoners to be come to being	2	franchine short top a houliant Charachers		- Will-	
Develop a plan to acquire the data Acquire data Verify integrity of data	2	Develop a plan to gravire the data	0	Terr	
Acquia data	1	· Acquia data	de Children Land		
Verify integriby of data	1	Verify into arity of data	mil and	-0	
2 The same	1	Il many band	Carried Head A	THE REAL PROPERTY.	
	-6				
C - Ol - O - O - O - O - O - O - O - O -	6	- Observe Chair 40 C 121	The state of the s		
IINOUVIE LINATA A L					
- Observe Chain of Contody		Tachana Spinal a	S HOUSE THE		
The state of the s			100000000000000000000000000000000000000		
	1	Kup log of every person who handled e	vidiou.		

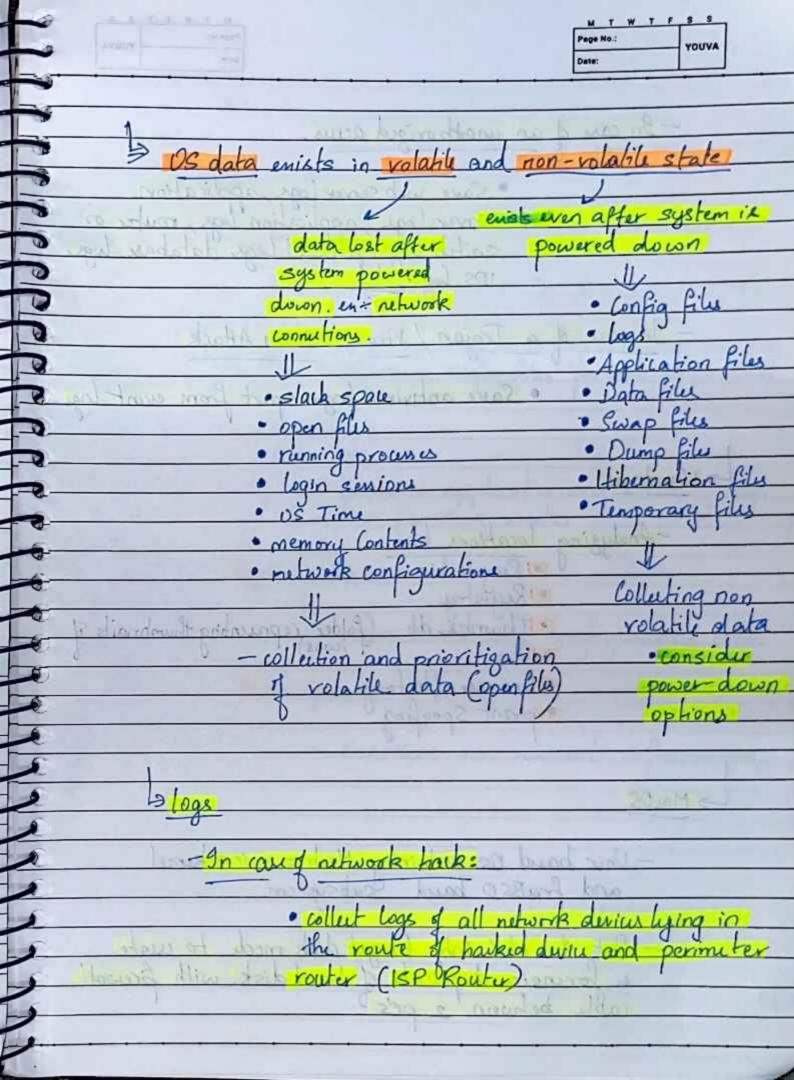
-

William William

	M T W T	FSS	0
	Date:	YOUVA	6
verify integrity of copy is original.			
vent dinterity of the	Dr str	216	100
grand gropy is original.	and the should	-	-
		10.5	
The state of the s	0.0(43.)	(D) b	0
	paranim	1	0
	at au o	A 6	0
-Bypansing Controls (OS and apps may have d	1	- 1.	-
-Con of John Cos and apps may have a	lata comprissio	n, encryphi	ACC
t 15	9		•
Taolsv			
- Basically enamining data		1 miles	
0		1	-0-
BY BY	a la grant d	Project ==	-
	0		-
13)	diam'rania		8
-include identifying people, place items and -Putting pieces of data -coordinated between multiple source of data	evento		
= Pulting pieces of data	1 111110		-
= condidated between multi-			-
munipu source of orata	18 crucial 16		
- michinan	Moreaus 10		
	D.		
L)A			000
Detail every test conducted methods and	A July 1	and the	0
Detail every test conducted sollings and	11 1	0.575	6
smult grant concerns y menous and	tools well a	nol	67
sexult and the second	a quille		-
and the second s	binote le		9
- Report Composition	NI SERVICE S		-
	2.7		
Forensic Acquisition & Enamination Findings & Report (Analysis) Conclusions.	ka Tina		-
Council Aca with 105	0 . /		_
Toreist Augustron 4 Enamination	treparation	Word -	
tindings 4 Keport (Andysis)	Д1		6
Condusions.	to be and to		6
the seques to page at the	Your In als to	ty.	
	11 11 11 11 11		

30	The second secon	
	SVINOY MATERIAL STATES	Page No.:
		Date: YOUVA
100	-Sans Anstitute best practice	(Bindings & Anglusis)
10	- Per practice	Grandy (may)
10	otake ss	M Madification Tim
	Bookmarekewidence via	forensic application of choice superting options within
	Use built in logainal	leoperting options within
	forencie tool	
17	highlight and aunorting	data item into . cov or . Int
	P.D.	- Colle Bad - Restour
1	olse digital audio repor	der vs handwritten notes when
170	pecusary	· outsid James -
2	Hab will and to be the date	
P	ount on audia totaled like of	* Charge like
-8	5 Data files	a linear trace than
-	not have an man; "xuismilate a month	1 Sections Day
-	- Windows - Unix	-macOs
-	FAT FAT -2	,3,4 • HFS+
-	• Reiser FS	· APES
	16 XFS	
-	32 TES	
-	· NITES · Btrfs	Maci : De la sant
-	Refs	Take I a
5	121 1 11	
6	- What not there	Translated and aloud
-	a Oald A Piles a sale of	(111 P) 11 1 (1 1 1.
1	valled flus for Killy	delited info pointing to file location
1	· Slark Cory : antice Elica	Maralia ikan ang d
1	file file	if it doen't mud that much
16	under it Spall and	The state of the s
	· Fru space: media le no	of allocated to
-	110	
1		

	M T W T	
	Date:	YOUVA
-MAC Data	line and	
Modification Time	della	
Acus Time	* Epons	
Crafted Time	10	
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	LI VIII	
Callaboration of the police of the special state of the s	Table 19	
- Colleting Backup	ASSA .	
· lugical Backup: copies files and di	cularia d	
Volume: dousn't ca	phure office	y data e
pruent on media	deluted B	iles or
residual data)	200 1	a e
: Rusoura Intensive	: can be	wo pn
20 ships - 12 stale-	live sys	tem ?
• Imaging: Generates bit-for-bit media (including free as	copy of o	riginal
media (including free ar	o slavi s	DAU)
: if widne or analysis	s ruded	it
chould be worked on the can't be used on live sy	is auphrat	4
econ pe usa on live sy	rem.	•
	STATE OF THE STATE	•
-Tools for Techniques	hat not the	1-
		. (
file viewed	· Colde	6
Uncompressing files		6
GUI for Data Stractures	aple v	-
Identifying known files	110 - 210	
String Searches and pattern matche		- 6
The state of the s	2 1001 5	



	Page No.:	YOUVA	
	Date:	10017	
- In case of an unashorized accus:		*	
The state of the s	July 200 5		
· Save web server logs, a	pplication		
Save web server logs, a Server logs, application Switch logs, firewall logs 1DS logs, etc.	logs, roul	wor	
switch logs, firewall logy	s databa	x logs	
IDS hogs , etc.		•	
DON BRIDE A PROBLEM COOK		(0 10
- In case of a Trojan / Virus / Worm A	Hack	(
- And the latter than GUID A. C.		(O R
· Save antivirus logs apart	from eve	nt loge.	
The second secon	V.		
Windows a some of a			
7.9		- 6	
		-	1
- Analyging locations like Recycle bin		-	-
Region		-	-
Registry Thumbs. db (folder ceprus	1. 10 1	111	-
Thumbs. db (folder ceprus	nting Thumbs	nails of	
prower Hickory			
print Speefing		•	-
		4	-
	THE EAST	6	فئيات
L> MacOS	and au	(فالما
	To a		المسلم
- Unix based us containing Mach z mil	crokunel	6	-
and fruksp band Subsystem.		6	
A CONTRACTOR OF THE PARTY OF TH		6	-
- Put the Mal into target disk mod a forensic duplicate of hard disk cable between 2 pc/s	e to way	e c	_
a forensic duplicate of hard disk	with fir	ewall a	
caple between 2 pc/s		-	3
			1-3

Aftern Contract and	Page No.:	YOUVA
	Date:	
Lo linua	polication.	16
-Analyze Location like:	sane -	
Port Bull as	N.A. IV	107
/etc [% System Root %	/System.32/	config
Control of the contro	CONTRACTOR OF THE PARTY OF	
- contains system con	igs direction	holding
- contains system con separate config files	foreach of	splication_
	the same of the sa	
/var/log		
		· L. I
- contains application - kept for 4-5 week	ara setter	ing ings.
of the stand wind water that the	and thinks	
/home/\$USER	Samuel .	F. H. Par
	of Dia long	
-usurdata and c	onfiguration	on info
	100	na A
etc/passed	o file steers	
All the same of th		
- contains user au	ount infor	mation.
Sharks		
Character of and state of the late		
the state of the s	-	
The second secon		
The second secon		

ò

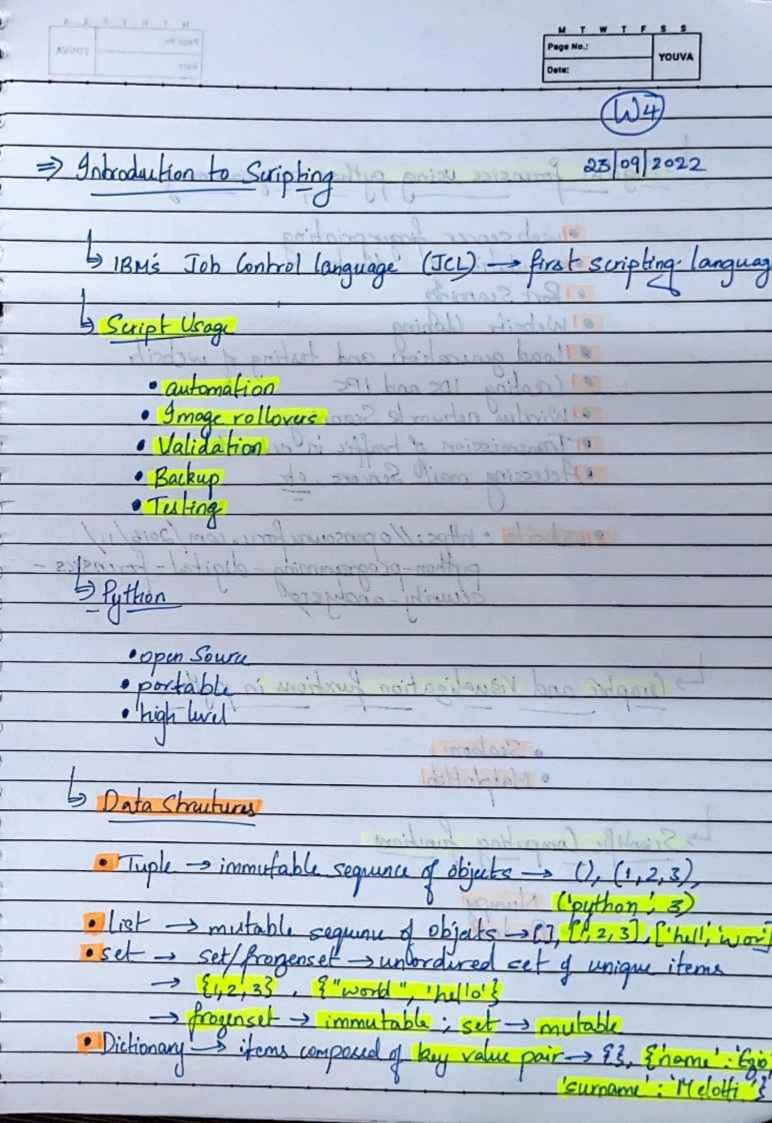
-

	Page No.1	YOUVA	6	
	Date:			
Application data	RUOI E			
- Apparation dates				
ocenfig sellings	(r)			
Au then tica from			0	-
logs the logs				
data			6	1
gunnom Hna files (Dorc links o	araphic)		1	-
App Architecture (local, client/so	ver per-to	DOLL)		-
		7		1
- I - Silver I - I				6
Type opplication				
THE PARTY OF THE PROPERTY OF THE PARTY OF TH		MA.		P
· Email Mary San All land				-
• Web Veage Chost-cookies, history, for a • Interactive Communications (group chat, etc.) • Data Concealment tools	ensifes; sever-	TS,18s,		
· Interactive Communications (group chat the) Type of righ	4)		-
· Data Concealment tools				-
· Security Applications	- Barbar	the at 1		
· Document Usage				6
· Document Verge · file sharing-	Y			
	101 : 1			15
protocol:	IKC-Dinterne	- Kulay		6
	Chart			-
				160
			9	2
The state of the s	handari -		-	9
The state of the s				1
			-	0
	E PROPERTY		-	(0)
The second secon		- 10	0	0
	-		4	9
			CONTRACTOR OF THE PARTY OF THE	

4			Page No.:	YOUVA	
4					_
*		-	11.152.16		
7	Day I I D I	a Digety La	1 21 2		
5	> Network Data	sa tel ulu, je	1000 P		
)	T-0/-0				
<u> </u>	>TCP/IP				
-		1 1	alli di		0
-	Application layer:	sends and	receives a	lata	For
		Particular as	ps, such	as Di	VC,
,		HTTP, SHT	<u> </u>	1.	
(parket) • Transport layer:	providus a	atten Con	neutro	<u>n</u>
7	Land of the state of	oriented or	connutio	n-lu	4
	The Character of the State of	servicus for	transport	ing	1
	Y (_u_bhxX,t_balling	application	ayur serv	ich b	etween
-		TCP/UDP	0 1		
(d	atagram) · Network layer (IP layer)	Routes	par	rels
-	V	ac	was not	works	
		IP-fund	amen tool	neh	ork
		other proto	for TCP/	IP.	
B		other proto	cols - 10	MP,	
10-		16MP	31330-19		
(fra	me) Hardware layer (Da	ta link layer	(): hand	ly	
	A STATE OF THE PARTY OF THE PAR	Co	mmunica	hone	on
	the state of the same of the	Physica	networ	R	
2.1		Compon	onts		
100	William American Committee and the committee of the commi	in + Etherne	t protou	1.	
		.4.	1		
	Sources of network data				
	· firewalls and Route	ers Come loc	even r	albit	(-)
	· packet Sniffers Gor	otocol And	years		/
	packet Sniffers & pro-	system	Jan		
	· Rimote Accus	0			

A Park to Silver and the second secon	M T W T	F 5 5		
	Date:	AVUOA		
			-	
			-	
· Network forensic Analysis Tools · Security wents management Software	and the second second			
· Security wents management Softw	ere	=	-	
0				
distribution of the second of	STE		0	II'
Data Value			16	
extendiation laws - sent and seem of also for			1	
IDS Software				
SEM Software				
NEAT Software (network forensic An	alusis bool	mon		
· firewalls, routers, promy servers, q	RAS			
THAT Servers (log each IP address)	alliannent-	- 1-		
avoción tod MAC addrew				
packet sniffers !!				
Network Monitoring	u alesa selvi			
ISP Records	o C.	A LA	_	
Thought we winder	203100	V CONC		
Avorded botomakend - 8"				
Attacker Identification				
Strain - Str			-	
Confact IP address owner			-	
Sand naharak har Place (sine 10) P	16.	110		
Send network traffic (ping 1P) (n Application Content (Data parket o	of recommo	ded for or	8	فر
of I parket c	Puld Conta	Un	-	
suk ISP Assistano attacker identity	(1/0)			
	1-	1 10	6	1
TISTING OF IT OPPORTUS FRENCH OF S	supicious a	(tivity)		1
	/	-		
State Shirty	Seur 10 1	V	0	I,
			9	10
The and haster from a work procedure	9	star to	-	1
asked Sailbur & produced Throughout	90		0	7
more distributed system	0/0		0	1
	The second secon			COLUMN TWO IS NOT THE OWNER.

Ī



	м	T	w	T	F	3 5
	Page	No.:				VOUVA
Ì	Date:		T			YOUVA

	M Page N	T W T F 3 S	
	Date:	YOUVA	-
			6
			*
190-11 P	1 0 1 0	Industra 6	-
Digital forensics using pyth	on programming	Makeryan, V	-
			-
owebserver finger po	oring	Swor in	6
Fort Scanning	Car Tarina, India	214(11.5	-
· Website Cloning		L.N.	-
load generation and	tasting 1 uch	a: L	-
(realing IDS and IPS	. Testing if went	8	-
Wireles network Scar	mino alles some		
Transmission of ballic	in achord		
Accessing mail Server	- ob	1 6	
	-	17.9	
· website: https://opens	oury fory com /2	016/01	
puthon-program	mmina = diaital.	Conners	-
sewihi-and	mming-eligital-	FOTOISICS	
) /	100	
	oen Sauge	N. C.	-6
Graphic and Visualization fur	retions in puthor	2 - 4	6
-10 -+	- 75	2000	6
Sealor			-
· Matplottib			0
	the transfer	STAP CO	0
Lo Scientific Computing functions	Martinglia		6
(= 1 - 0 V	Doubles e- 1	ordi Ve	0
(E. Tarbast Numpy			6
Pandas in the same	as idealine of	40/10	0
and without the landaute	+ Set/ Americal	-4508	0
February Whose	The state of the s		0
Morning 6- to sld from			63
med of the value cours - 52, There	6 6 7	Pikhen	6
His manual P. F.	4		
		-	-

Parant : It deep

