

(1/8) - FOUNDATEONS OF CYBERSELURITY MODULÉ - 1 :-=> Course 1 Overnieur: and core skills Systems Security Proffesional [CISSP] security domains, security frameworks and controls as well as a foundational security model called Confidentiality, Integrity and Availability [CIA] triad. - also will know about some common tools used by security analysts. . > Madate 1 Roadmap: - (all & avail) In this course, you will: · Perognize core skills and knowledge noded to become a security analyst. · Identify seavily attacks impact business operations · Identify & security domains · Define security framework and control Still Sats . · Communicating effectively. · Collaborating with other · Tolentifying throats rules & nulnerabilities · Problem - Solving.

	Page No:
	1-10/1
` ⇒.	Cybensecurity: 1-11
	The practice of ensuing confidentiality
	A A A A A A A A A A A A A A A A A A A
	Lucia inquithorised access of
Land of the second	LABOR WEST WASHINGTON
	D IT Of COUNTY -
2.21	Protock against included and
10.4014	Meals Hoon Significant
15 19	Maintains and invitores Laures
10	Reduces expenses.
Albalal	land has simpleful molecularity and
=	Campan John Wills.
n 3 - 1 m	Society Analyst Specialist
	· Generality Analyst/Specialist
Elaber 1	· Security Operations Contre (SOC) analyst
Sil sil	· I pornation security analyst.
HOME TO	I thought a gradual I shall e
=	Common cylorsecurity tourinologies:
	- Ulin you arried with ot
	Compliance:
abolinas	. It is the process of following internal
9	standards and external regulations to avoid
1.	Lives i & security breaches.
	Landagon Against
	Sowity frameworks:
Oan b	They are guidelines ared for
SEST PISS	building plans to help mitigate risks and
Total !	threats to date and prinage
	Wille Han contemplated o
133	Lacater & Adam daniel complete to To
	mitigate -> make something less something
	The state of the s

· Security Controls:

These are safegouards designed to reduce specific security risk. They are used with security frameworks to establish a strong security posture

· Security Posture:

It is an organization's ability to manage its defense of critical assets and data and react to change. A strong security posture leads to lower risk for the organization.

· Threat actos: (malicious attacker)

security risk. This risk can relate to computers, application, network and data.

· Internal threat:

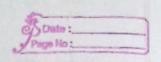
A threat or an attack from a current or former employee or even a trusted partners.

Notwork Socurity:

It is the practice of keeping an organizations returned infrastructure securie from unauthorized offers.

· Cloud Security:

stored in the cloud are properly configured or set up correctly and access to those arets is limited to authorized users.



Programming It is a process that can be used to create a specific set of instruction for a computer to execute tasks - Automation of repetitive tasks Crearching a list of malicious domains) - Romaning was traffic. - Alorting Suspictous activity. Transferrable Skills: · Communication · Time - Management · Callaboration (Growth mindset · Analysis · Dinerse Perspectures · Problem - Solving Technical Skills: · Programming languages y Pythes ESQL [Security Information and event Management] · Correntes Forensics · Intrusion Detection System [IDS] · Threat Landscape knowledge · Incident Response Comp TIA Security +: Certified course - check about it

Page No:

THE RESERVE TO STATE OF THE PARTY OF	The state of the s
7	Keep Organisations Secure:
	W Analytical thinking
	(ii) Collaboration
	(iii) Malmare prevention
	(w) Communication
	(v Understanding programming languages
	(V) Understanding programming languages (VI) Using SIEM
	O SURV C
ラ	TERMINOLOGIES: ALEN ALLEN STATES
	expected at authors show authorities of
(i)	Personally identifiable Information: [PII]
	Personally identificable Information: [PII] Any information: [PII]
	Tobal Canal
(11)	Sonitive PIT : [SPII]
	YPIP which contains sensitive information.
ÚM	
VVA	tion of a casatio and a
	Countries historical and Variation (i)
	Company of the Compan
	> CERTS 1 Computer Emogray Region Fee Tel
	I respond to compate reside actives
	Street respectables
	san design of chatte and x
	The doubter offer of the first
	the total and the terms of the
1	

4	
25	Ombo :
90	At .
2/14	go NG :

11		
+	MODULE - 2:	1
	1 1134. 4. 1831 4 114.	-
	La Malinares	_
	La social Engineering	_
	La Divital Doe	_
panua	1. Somethe Dangard	_
V	M'S reagant (IV)	
₹	Virus	-
	The state of the s	=
	Computes Virus: Malicious code written to interpre units computes operations and cause damage to data and software.	_
	with computer operations and cause damage	1
talacha also	to data and software.	
	The state of the s	
=>	Malmare: Tarrall - reng miland	1
	desires or returner.	
	donires en retwerk.	
	The Parameter of the August of the Control of the C	ij
*	Two attacks in the past:	
	(1) Brain Virus (for pirated rottines) (1) Morris Worm (to find the total no. of	
-03	Brain-Vinda:	
7	CERTS: [Computes Emergency Rospions Town] Gresponds to computes society incidents	
La Preside	remands to computer society incidente	
	more responsibilities.	
樂	Two attacks in present and	
	Two attacks in present age: (i) The Loughetter attack (to steel logis (ii) Equipor breach y data bread in Equipor Iteading to tradit Grad	
	Ui) Equipor breach y date bread in Equipou	
	Theading to Credit and	
	uples .	
THE REAL PROPERTY.		

16	
CS Date:	7
Pege No:	-1
S Legano.	=)

ョ	Social Engineering:
	A manipulation technique that exploits human
	Social Engineering: A manipulation technique that exploits human error to gain primate information, access, or naturalles.
	Convince >> P.
	The same of the sa
	leads to more vulnerabilities
7	Phishina "
	The use of digital communication to trick people into revealing sensitive data or deploying malicious software.
	people into renealing sensitive data or denlowing
	malicious software.
	THE PERSON NAMED IN COLUMN TO A PARTY OF THE PERSON NAMED IN COLUMN TO A PARTY
	2000 has wallager whater white white
7	Common attacks and their effectiveness:
•	CSIRTS [Computer Society Incident Response Teams]
	PHISHTING: (types) (i) Business Email Compromise: [BEC]
	(i) Business Email Compromise: [BEC]
	private actor sends on and that
	seems to be legit which extracts credentials from the uses.
	(ii) Spear Phishing:
	specific uses. The original from a trusted source
-	CONTRACTOR AND
	(III) Whaling: (a John of Areas abishing)
1	targetting company executive
1	3 1
-	

-	
CAS Date:	
Page No:_	
2	

(1) Vishing:

The exploitation of electronic voice

communication to obline SPIT.

(V) Smishing:

Use of text messages to truck uses to

MALWARE: (types)

(i) Viruses:

4 Malicious code written to

interfere with computer operations and cause
damage to data & software.

Cthrough an attachnood or file download

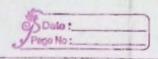
(i) Worns:

Approach itself across system on its own.

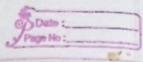
be downloaded by an user. Instead it ref replicates and spreads from an already injected comp.

(iii) Rensommare:

actors energypt an organisations data and domard payment to restou access



	(w) grymare:
	Malware that's used to gather and sell
	ifornation without consort.
*	Social Engineering:
ü)	Social media phishing: collects igto about target from social media and initiates altack.
	and initiates altack.
Ü	Watering halo attack:
	users.
(ii)	
LIAN I	USB boiling: - malware USB stick for an employee to find & instal
(w)	Physical Social engineering:
	impersonates an employee, customy, or vendos
	Physical Social engineering: impersonates an employee customer or vendor to olutain unauthorized access to a physical location
	the policies and musics who have the
7	Social Engineering Principles:
	SEA are effective bocause:
	· Authority · Intimidation
	· Consensus/3 ocial proof · Scarcity
	· Familiarity · Trust · Urgency



The eight CISSP security domains: 1) Security and Risk Management:
Defines security goals and objectives. risk mitigation, compliance, business continuity, and the law. 2) Asset Security:

Secures digital and physical assets.

It's also related to the storage maintenance. retention, and destruction of data old data 3) Security Architecture and Engineering: effective tools, system and processes are in 4) Communication and Network Security: Manage and secure physical notworks and wireless communications 5) Identity and Access Management: users follow established policies to control and manage physical assets, like office spaces and logical assets, such as notworks and applications.

6) Society assessment and testing:

Conducts security control torting, collects

and analyzes data, and also conducts security

audits to mointor for rusks, threats, and vulnerabilities

7) Socurity Operations:

Conducting investigations and implementations
preventine measures.

2) Software Doudepment Socurity:

Uses secure rading practices, which are a set of recommended guidelines that are used to create secure applications and services.

Determine the type of altack:

> Attack Types:

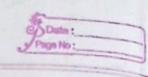
(i) Password attack:

It is an attempt to access passuard-secured devices, systems, retworks or data. Some forms of passward that youll leader in the cert program

· Brute Force

· Rainhour Table this attack comes under the communication and natural society domain.

AND STATEMENT BOLLEGE ABOLANT



(ii) Social Enquiring attack:

Social engineering is a maripulation technique that explaits human error to gain prinate information, access or valuable · Philling · Vishing · Smushing

· Spear Phisting · Whating · Social modia phishing · Business Email Comprisming (BEC) · USB boiling

· Water hale attack · Physical Social engo

& this attack comes under security and risk management

(iii) Physical attack:

It is a security attack incident that affects not only digital but also physical environments where the incident is entryeddeplayed

· Malicious USB calle · Malicious flash druns

· and closing and skinning

4 this attack fall under asset security domain

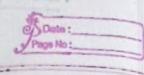
Adversion

Adversarial artificial intelligence:

It is a technique that maripulates artificial intelligence and martine learning technology to conduct attacks more efficiently

4 this falls under both communication and naturally and identity and accord management

· edu or · gon - welsites are roliable sauce - bruited & northere (v) Supply-chain attack: It targets systems, application, hardware, and/or software to locate a subscrability where malware can be deployed. Because every item sold undergoes a process that involves third parties, this means that the security breach can occur at any point in the supply chair. These attacks are costly because they can affect multiple organizations and individuals who work for them Supply- chain attacks can fall under several domains, including but not himited to the security and risk management, security architecture and engg, and security granation (VI) Cryptographic attack: Letures a sender and intended recipions. Some cryptographic altaces are: 图 () Birthday () Collision () Downgrade notruok security domais.



→ Understand attackers:

super shipping the Bratton to the

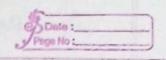
- => Threat Actor types:
- (i) Advanced Persistent Threats: [APT]
 - accessing an organization's naturale without authorization authorization.
 - · APTs land to research their targets in advance and can remais undetexted for an extended paried of time.

 Their interdions & motivation are to
 - * Danage critical intrastructure
 - a Graining accounts intellectual property
 - (ii) Insider Threats: Employees alusing their authorized access to obtain data that may have
 - Corruption Expianage
 Unautropyed data access or leaks.
 - (iii) Hacktivisti:

drives by a political agenda.

Demonstration

- · Propaganda · Social change campaigns



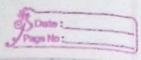
亨	Hac	Rer	ty	res:

- · A harber is any person who uses computers to gain access to computer systems, networks, or data.
- · There are three mais categories of hadrers:
 - (i) Authorized hackers / Ethical hackers:

 They follow a code of ethics and adhere to the law to conduct organizational risk evaluations. They are matinated to safeguard people and organizations from maticious threatailous
 - (ii) Seri-authorized hackers / Researchers:

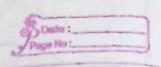
 They search for vulnerabilities but don't take advantage of the vulnerabilities they find.

They are malicious threat actors who do not follow the law. Their good is to collect and soll the confidential data for financial gais.



MODULE - 3: Francusks and Controls: Security framounts: Oruidelines used for building plans to help mitigate rusks and threats to data and prinary. Protoda PII - Securing financial info > Identifying security weaknesses > Managing organizational risks - Aligning security with business goals > Components of Security Frameworks: (i) Identifying and Documenting goals (ii) Setting guidelines to actions security goals (iii) Implementing strong security processes (ix) Monitoring and communicating results € Security Contrals: Sofeguardo dosigned to reduce specific security risks

	Journational security Date:
70	CIA triad: [Confidentiality, Integrity & Availability]
	Only authorized Data is authentic) Data is accessible specific data (correct, reliable) to those who have access to it
	NIST Cubattage of Estate 1
2	NIST Cyberrocurity Framework (CSF): A voluntary framework that consists of standards, guidelines, and best practices to manage cyberroccurity risk.
•	CIA triad is a model that helps inform how organizations consider risk when setting up systems and security policies.
•	Compliance is the process of adhering to internal standard and external regulations.
•	NIST: -> Cyberoscarity Francuscule (CSF) Risk Management Francuscule (RMF) there are several other other controls francuscules and compliance



The Federal Energy Regulatory Commission North American Electric Rehability Corporation:

[FERC - NERC]

EERC-NERC is a regulation that work with electricity - sworks in with US and North Arein is power grid.

must mitigate and report any potential troops

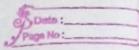
- => The Federal Risk and Authorization Management
 Program:-[Fed RAMP]
- program that standardizes society
 assessment, authorization, manitaring and
 handling of cloud services and product
 afferings
- => Center for Internet Security: [CIS]
- · CIS provides a set of controls that can be used to safeguard systems and retworks against attacks

- 7 General Data Protection Regulation: [GDPR]
 - · GIDPR is European Union (F. U) general data regulation that protects the processing of E. U residents data and their right to primary in and out of EU territory.
- => Payment Card Industry Data Socurity Standard:[PCI DSS]
- ensures storing security in storing accepting, processing and transmitting credit card information to do so is a secure ensurement.
- Accountability Act: [HIPAA]
- healts information. (probability patients into to be shown without their consent).

 (1) Primary (2) Socurity (3) Breach notification

if health into is exposed it leads to identity thefts and visurance frounds.

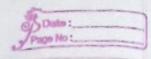
- > International Organisation for standardisation (30)
 - · ISO is related to technology manyfacturing and management across borders.
- and procedures for staff retention, planning, waste



	Page No:
⇒	System and Organizations Controls: [50]
diam.	SOC type 1, SOC type 2
as Mine	and a sories of moments
	SOCI and SOC2 are a sories of reports that jours on an organizations were access policies at different organizations levels such as:
	that Jours on an organization
37.5	access policies at different
	lands buch as:
da di	* Aprociate * Supervisos
	Maganes
Limite	* Froculine
	a venday
	• Oltros
•	They are used to assess an organization's
	They are used to assess an organization's Jinarcial compliance and levels of risk
1	
BOLLAGE T	the state of the s
	a manual nation bulgions to a select select stipon
	Latter of the Property of the Street and the Street
Total St	and who had become a fire add the of the
0 4	
	THE ADMINISTRATION OF THE PARTY
	A hundling heiffer has
ر بالعد الآل	
off at	Colombia de la Constantina del Constantina de la Constantina del Constantina de la C
The Mar	
om one	and a second sec
on one	The state of the second of the
The second second	and a second sec

Page No:

	Cy rapano:
H	MODULE-L:
p+	MODULE-4: Important Cybornewity tods:
•	
	A record of events that occur within an
	A record of events that occur within an organization's systems.
•	STEM tools: [Socurity Information and Front Management An application that collects and analyses log data to manitor critical activities in an organization.
(A) =	An application that collects and analyses log
	data to manitor critical activities in an organization.
	(i) Splink J Asollarus
	(i) Splunk J Asoftwares (ii) Chronicle
	Alm Turner Fact which distribute stores
•	Other key security tools:
	(i) Playbooks:
100	A manual that provides detail about any
	operational action.
	(ii) Notwork Protocol Analyzer: - (packet sniffer) A tool designed to capture and analyze data traffic within a network. Otopdump @Winestark
	A tool designed to capture and analyse
	data traffic uithis a naturale.
	" O topdump @ Wirestark
2	T to al Planbacks
-7	Two types of Playbooks:
0	
	. It is the process of documenting exidence
	Chain of Custody playbook: This the process of documenting exidence possession and control during an incident lifecycle.
2000	
(2)	Protecting and Preserving excidence playbook: It is the process of property working with fragile and udatile digital evidence.
	It is the process of property many
1886	frague and holable digital suidence.



Core Cyborsecurity knowledge and skills:

Programming:
Used to create a specific set

y instructions for a computes to execute tasks.

Linux:
An open source operating system.

• SQL:-[Structured Query Language]

A programming language used to

create, interact with, and request info

with a database.

· Database:
An organised collection of information of data

Python:
Used to perform tasks that are
repetitive and time consuming, and that
require a high level of detail and accuracy.

Web Yutnorality:

It is a unique flaw to a web
application that a threat actor could exploit
by using malicious code or behavior, to allow
unauthorized acress, data that, and malway
deployment.

alporithm pay publicly available

· Antirorus Softmare:

detect, and diminate malware and wruses It is also called arti-malware

it can scan the memory of a denire to find patterns that indicate the preserve of malware.

• Intrusion Detection System: [IDS]
• It is an application that manitars system activity and alorts on possible intrusions.

packets -> which carry small amounts of data through a naturark.

Encryption:

The process of converting data from a reputationally encoded Plaintent algoritha keys Cipher text

Encayption and Encoding not same

decryption ray is not publicly available

Penatration Testing: (Pen Testing) attack that holps identify valuerabilities in system, returbles, use applications, application, spraceus.

> Chak again in Courers for > Create a Cyberrocurity Portfolia: ox Options for wanting your Portfolia: (1) Documents Jelder (2) Groogle Drine or Dropbon (3) Groogle Sites (4) Grit Ropository