(1/8) - FOUNDATIONS OF CYBERSECURITY

↳ MODULE - 1 :-

⇒ Course | Overview :

↳ will learn primary job responsibilities and core skills.

↳ explore about Certified Information 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.

⇒ ~~Module~~ Course | Roadmap :- (all 8 avail)

► In this course, you will :-

- Define the field of security
- Recognize core skills and knowledge needed to become a security analyst.
- Identify security attacks impact business operations.
- Identify 8 security domains
- Define security framework and controls.

► Skill Sets :-

- Communicating effectively
- Collaborating with other
- Identifying threats, risks & vulneralilities.
- Problem - Solving

⇒ Cybersecurity :

The practice of ensuring confidentiality, integrity, and availability of information by protecting networks, devices, people and data from unauthorized access or criminal exploitation.

⇒ Benefits of Security :

- Protects against external and internal threat
- Meets regulatory compliance
- Maintains and improves business productivity
- Reduces expenses.

⇒ Common Job Titles :

- Security Analysts / Specialists
- Cybersecurity Analyst/Specialist
- Security Operations Centre (SOC) analyst
- Information security analyst.

⇒ Common cybersecurity terminologies :-

- Compliance:

It is the process of following internal standards and external regulations to avoid fines & security breaches.

- Security frameworks :

They are guidelines used for building plans to help mitigate risks and threats to data and privacy.

mitigate → make something less ~~serious~~ severe/serious

- Security Controls:

  These are safeguards 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 actor: (malicious attacker)

  It is any person or group who presents a 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 partner.

- Network Security:

  It is the practice of keeping an organizations network infrastructure secure from unauthorized access.

  ↳ devices ↳ data ↳ services ↳ systems

- Cloud Security:

  It is the process of ensuring that assets stored in the cloud are properly configured or set up correctly, and access to those assets 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 (searching a list of malicious domains)

  ↳ Reviewing web traffic.

  ↳ Alerting Suspicious activity.

⇒ Transferrable Skills :-

- Communication
- Collaboration
- Analysis
- Problem-Solving
- Time-Management
- Growth mindset
- Diverse Perspectives

⇒ Technical Skills:

- Programming languages } Python & SQL
- SIEM tools
  [Security Information and event Management]
- Computer Forensics
- Intrusion Detection System [IDS]
- Threat Landscape knowledge
- Incident Response

Study about this ⇒ CompTIA Security+ :

↳ Certified course

↳ check about it

⇒ **Keep Organisations Secure:**

(i) Analytical thinking
(ii) Collaboration
(iii) Malware prevention
(iv) Communication
(v) Understanding programming languages
(vi) Using SIEM

⇒ **TERMINOLOGIES:**

(i) Personally identifiable Information: [PII]

- Any info used to infer an individual's identity

(ii) Sensitive PII: [SPII]

↳ PII which contains sensitive information.

~~(iii)~~

↦ MODULE – 2 :

↳ Viruses
↳ Malwares
↳ Social Engineering
↳ Digital Age
↳ Security Domains

~~⇒ Virus~~

⇒ **Computer Virus :**
Malicious code written to interfere with computer operations and cause damage to data and software.

⇒ **Malware :**
Software designed ~~to~~ to harm devices or network.

* **Two attacks in the past :**
(i) Brain Virus (for pirated software)
(ii) Morris Worm (to find the total no. of internet users) ✓

~~(i) Brain Virus~~:
⇒ **CERTS** : [Computer Emergency Response Team]
↳ responds to computer security incidents
↳ more responsibilities.

* **Two attacks in present age :**
(i) The Loveletter attack (to steal login credential)
(ii) Equifax breach } data breach in Equifax
↳ leading to credit card upto

⇒ Social Engineering:

A manipulation technique that exploits human error to gain private information, access, or valuables.

$$\underbrace{\text{Convenience} >> \text{Privacy}}_{\text{leads to more vulnerabilities}}$$

⇒ Phishing:

The use of digital communications to trick people into revealing sensitive data or deploying malicious software.

⇒ Common attacks and their effectiveness :-

- CSIRTs [Computer Security Incident Response Teams]

* PHISHING: (types)

(i) Business Email Compromise: [BEC]

↳ A threat actor sends an email that seems to be legit which extracts credentials (or information) from the user.

(ii) Spear Phishing:

↳ A malicious email attack that targets a specific user. ↳ the email seems to originate from a trusted source.

(iii) Whaling: (a form of spear phishing)

↳ targetting company executive

(IV) Vishing :

↳ The explotation of electronic voice communication to obtain SPII.

(V) Smishing :

↳ Use of text messages to trick users to obtain SPII.

* MALWARE : (types)

(i) Viruses :

↳ Malicious code written to interfere with computer operations and cause damage to data & software.
(through an attachment or file downloded)

(ii) Worms :

↳ Malware that can duplicate and spread itself across system on its own.
↳ the diff b/w Virus & Malware is that Worms needs not be downloded by an user. Instead it self-replicates and spreads from an already infected comp.

(iii) Ransomware :

A malicious attack where threat actors encrypt an organisation's data and demand payment to restore access.

(iv) Spyware:

Malware that's used to gather and sell information without consent.

↪ accesses devices.

* Social Engineering:

(i) Social media phishing:

→ collects info about target from social media and initiates attack.

(ii) Watering hole attack:

→ attacks a website frequently visited by a group of users.

(iii) USB baiting:-

→ malware USB stick for an employee to find & install

(iv) Physical social engineering:

→ impersonates an employee, customer, or vendor to obtain unauthorized access to a physical location

⇒ Social Engineering Principles:-

SEA are effective because:

- Authority
- Intimidation
- Consensus/Social 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:**
Optimizes data security by ensuring effective tools, system and processes are in place. → firewals

4) **Communication and Network Security:**
Manage and secure physical networks and wireless communications.

5) **Identity and Access Management:**
Keeps data secure, by ensuring users follow established policies to control and manage physical assets, like office spaces and logical assets, such as networks and applications.

6) <u>Security assessment and testing:-</u>

Conducts security control testing, collects and analyzes data, and also conducts security audits to monitor for risks, threats, and vulnerabilities

7) <u>Security Operations:</u>

Conducting investigations and implement~~ations~~ing preventive measures.

8) <u>Software Development Security:</u>

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

→ <u>Determine the type of attack:</u>

→ <u>Attack Types:</u>

(i) <u>Password attack:</u>

It is an attempt to access password-secured devices, systems, networks or data. Some forms of password that you'll learn in the cert progra are:

- Brute Force
- Rainbow Table

↳ this attack comes under the communication and network security domain.

Date :
Page No :

(ii) Social Engineering attack:-

Social engineering is a manipulation technique that exploits human error to gain private information, access or valuables

- Phishing
- Vishing
- Smishing
- Spear Phishing
- Whaling
- Social media phishing
- Business Email Compromise (BEC)
- USB baiting
- Water hole attack
- Physical social engg.

↳ 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 ~~employed~~ deployed.

- Malicious USB cable
- Malicious flash drive
- Card cloning and skimming

↳ this attack fall under asset security domain

~~⇒ Adversarial~~

(iv) Adversarial artificial intelligence:

It is a technique that manipulates artificial intelligence and machine learning technology to conduct attacks more efficiently

↳ this falls under both communication and network security and identity and access management domain

• .edu or .gov → websites are reliable source

↳ trusted & verified

(v) Supply-chain attack :

It targets systems, applications, hardware, and/or software to locate a vulnerability 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 chain. 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 limited to the security and risk management, security architecture and engg, and security operation domain.

(vi) Cryptographic attack :

It affects secure forms of communication between a sender and intended recipient.

Some cryptographic attacks are:

☆ (•) Birthday (•) Collision (•) Downgrade

↳ this attack falls under the communication and network security domain.

→ Understand attackers:

⇒ Threat Actor types:

(i) Advanced Persistent Threats: [APT]

- APTs have significant expertise accessing an organization's network without ~~authentication~~ authorization.
- APTs tend to research their targets in advance and can remain undetected for an extended period of time.
- Their intentions & motivations are to
  - * Damage critical infrastructure
  - * Gaining access to intellectual property.

(ii) Insider Threats:

Employees abusing their authorized access to obtain data that may harm an organization.

- Sabotage • Corruption • Espionage → spy
- Unauthorized data access or leaks.

(iii) Hacktivists:

They are threat actors that are driven by a political agenda.

- Demonstration
- Propaganda
- Social change campaigns
- Fame

⇒ Hacker types:

- A hacker is any person who uses computers to gain access to computer systems, networks, or data.

- There are threee main categories of hackers:

(i) Authorized hackers / Ethical hackers:
They follow a code of ethics and adhere to the law to conduct organizational risk evaluations. They are motivated to safeguard people and organizations from malicious threat actors

(ii) Semi-authorized hackers / Researchers:
They search for vulnerabilities but don't take advantage of the vulnerabilities they find.

(iii) Unauthorized hackers / Unethical hackers:
They are malicious threat actors who do not follow the law. Their goal is to collect and sell the confidential data for financial gain.

MODULE - 3 :-

Frameworks and Controls :

⇒ Security frameworks :

Guidelines used for building plans to help mitigate risks and threats to data and privacy.

↳ Protects 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 achieve security goals
(iii) Implementing ~~strong~~ strong security processes
(ix) Monitoring and communicating results

⇒ Security Controls :

Safeguards designed to reduce specific security risks foundational security model.

⇒ ① CIA triad : [Confidentiality, Integrity & Availability]

(Only authorized users can access specific data)

(Data is authentic, correct, reliable)

(Data is accessible to those who have access to it)

- ~~Asset~~ :

⇒ ② NIST Cybersecurity Framework (CSF) :

A voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity 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 standards and external regulations.

- NIST: ⟶ Cybersecurity Framework (CSF)
  ⟶ Risk Management Framework (RMF)

  there are several other others controls, frameworks and compliance

⇒ The Federal Energy Regulatory Commission -
North American Electric Reliability Corporation:
[FERC - NERC]

- FERC-NERC is a regulation that work with electricity → works ~~in~~ with US and North America's power grid.
↓
must mitigate and report any potential threat/fi
↓
~~A~~ adheres to the Critical Infrastructure Protection
[CIP]

⇒ The Federal Risk and Authorization Management Program:-['FedRAMP]

- ~~It is~~ FedRAMP is a US federal govt. program that standardizes security asssesment, authorization, monitoring and handling of cloud services and product offerings.

⇒ Center for Internet Security: [CIS]

- CIS provides a set of controls that can be used to safeguard systems and networks against attacks.

⇒ General Data Protection Regulation : [GDPR]

- GDPR is European Union (E.U) general data regulation that protects the processing of E.U residents data and their right To privacy in and out of EU territory.

⇒ Payment Card Industry Data Security Standard:- [PCI DSS]

- PCI DSS is an international security standard that ensures ~~storing~~ security in storing, accepting, processing and transmitting credit card information to do so is a secure environment.

⇒ The Health Insurance Portability and Accountability Act:- [HIPAA]

- HIPAA is US federal law to protect patient health information. (prohibits patients info to be shared without their consent).

(1) Privacy (2) Security (3) Breach notification

if health info is exposed it leads to identity thefts and insurance frauds.

⇒ ~~ISO~~ International Organisation for Standardization [ISO]

- ISO is related to technology manufacturing and management across borders.
- It helps organization improve their processes and procedures for staff retention, planning, waste and services.

⇒ System and Organizations Controls : [SOC]

SOC type 1 , SOC type 2

- SOC1 and SOC2 are a series of reports that focus on an organizations uses across policies at different organization levels such as:
  - * Associate
  - * Supervisos
  - * Manages
  - * Executive
  - * Vendos
  - • Others
- They are used to assess an organization's financial compliance and levels of risk.

→ MODULE-4:

→ Important Cybersecurity tools:

- Log:

A record of events that occur within an organization's systems.

- SIEM tools: [Security Information and Event Management]

⊗ → An application that collects and analyses log data to monitor critical activities in an organization.

(i) Splunk
(ii) Chronicle } A Softwares

- Other key security tools:

(i) Playbooks:

A manual that provides detail about any operational action.

(ii) Network Protocol Analyzer :- (packet sniffer)

A tool designed to capture and analyze data traffic within a network.

① tcpdump ② Wireshark

⇒ Two types of Playbooks:

→ evidence

① Chain of Custody playbook: → what, who, where and why

• It is the process of documenting evidence possesion and control during an incident lifecycle.

② Protecting and Preserving evidence playbook:

• It is the process of properly working with fragile and volatile digital evidence.

→ Core Cybersecurity knowledge and skills:

- Programming:
  Used to create a specific set of instructions for a computer 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 repetetive and time consuming, and that require a high level of detail and accuracy.

- Web Vulnerability:
  It is a unique flaw in a web application that a threat actor could exploit by using malicious code or behavior, to allow unauthorized access, data theft, and malware deployment.

- **Antivirus Software:**

  - It is a software program used to prevent, detect, and eliminate malware and viruses. It is also called anti-malware.
  - Depending on the type of antivirus software it can scan the memory of a device to find patterns that indicate the presence of malware.

- **Intrusion Detection System: [IDS]**

  - It is an application that monitors system activity and alerts on possible intrusions.
  - The system scans and analyzes network packets → which carry small amounts of data through a network.

- **Encryption:**

  It is the process of converting data from a readable format to a cryptographically encoded format.

  Plaintext $\xrightarrow{\text{algorithm key}}$ Cipher text

  Encryption and Encoding not same

  Encryption ↓ decryption key is not publicly available

  Encoding → algorithm key publicly available

- **Penetration Testing: (Pen Testing)**

  It is the act of participating in a simulated attack that helps identify vulnerabilities in systems, networks, web applications, applications & processes.

Date :
Page No :

→ Check again in Coursera for a detailed info about creating one.

⇒ <u>Create a Cybersecurity Portfolio:</u>

* <u>Options for creating your Portfolio:</u>

(1) Documents folder
(2) Google Drive or Dropbox
(check it out) (3) Google Sites
(4) Git Repository

— x — x —