Task 1

15/01/2026

1)--
Cybersecurity , at its core is the practice of protecting systems,,neyworks,and programs from digital atacks.
These attcks usually aim to access,change or destroy sensitive information.

To achieve this level of protection, security professionals use a model called CIA triad.
Its like a checklist to evaluate how secure a system is.
CIA is short for
1.Confidentiality (privacy)
this means that the data is visible/accessible only to those authorized to see it, meaning keeping a secret 'secret'
eg :1. in a banking scenario, the banking app uses encryption ,meaning even if the wifi is tampered with, The attacker cant
see your payments or balance
2. in a social media setting, it could mean your profile is private so others can't view your hidden posts unless
you approve them

2.Integrity
here it ensure the above data has not been tampered with or altered by unauthorized people.
eg: 1. in banking , the amount sent lets take 10 rs , it ensures the amount doesnt magically change to 1000 or 10000
during the transfer
2. in social media, it could be like , preventing attacker from editing your posts, if a verfied is tampered
they could spread fake news
3.Availability
here we ensures that systems and data are up and running when authorized users need them
eg: 1. in a banking atmosphere, banks uses redadunat servers if a data center fails , so you can send money without a prob
2. to avoid something liek a server down error, company uses servers like cotent delivery networks during high traffic

2)--
There are different types of attackers
1-Script Kiddies (The Amateurs):Unskilled individuals or beginners who do not know how to write their own code, they use
pre-made scripts created by others to attacker

2-Insiders (The Internal Threat): They are cuurent or former employees,partners who has legit access to the organization's

system

3. Hacktivists (The Protestors): They are group of attckers views themselves as activits,they dont hack for money,
but to send messages. eg: groups like anonymous

4. Nation-State Actors (The Spies): Another group of attckers,who are skilled hacker groups directly funded and
trained by governments. They are often referred to as APTs (Advanced Persistent Threats).

3)--
Attack surface is where an attacker could exploit to enter data or extract data from a syatem.
1- from web applications, it is exposed to public to function so, attckers target input fields and others to inject
malicious code (sql injection,xss) to attempting to trick the application into revealing database
information or hijacking user sessions.
2. mobile apps, attack surface includes app and the device it runs on,hackers reverse engineer the app to
find hard coded api keys or exploit excessive permissions to gain access to user data
3.APIs, apis allow different software components to talk to eachother. because they are designed for machine-to-machine
commiication,they are sometimes less protected,making attckers easy to bypass front-end security or to scrape massive
amounts of data
4.networks, this includes the infrastructure that connects devices,such as wifi, routers ,and firewalls.Attackers scan networks for
open ports or unpatched devices, using them as a foothold to enter the system and move to more critical servers
5.cloud infrastructure, this is the rented computing power and storage.the primary risk here is misconfiguaration rather than straight forward attacking, meaning
setting sensitive records to public - allows anyone to download files with links

(4)--
OWASP Top 10 vulnerability
1. Broken Access Control Basically, users getting into places they shouldn't, like a standard user accessing the admin panel.
It’s like forgetting to chmod a sensitive file and letting anyone read or write to it.
2. Cryptographic Failures This is storing passwords in plain text or using weak encryption algorithms. If a hacker intercepts
the traffic, they see the raw data instead of a jumbled hash.
3. Injection When untrusted data is sent to an interpreter as part of a command or query, like SQL Injection. You put malicious
code in a login box, and the database executes it like it’s a real script.
4. Insecure Design These are flaws in the actual architecture or logic before you even start coding. You can't patch a bad blueprint;

the system was built to be insecure from the start.

5. Security Misconfiguration Leaving default settings on, verbose error messages, or open cloud buckets. It’s like installing a
fresh Linux distro and forgetting to configure firewalld or change the default root password.
6. Vulnerable and Outdated Components Using libraries or frameworks that already have known CVEs (Common Vulnerabilities and Exposures).
Your code might be clean, but if you import a vulnerable dependency, you're compromised.
7. Identification and Authentication Failures Weak login systems that allow credential stuffing or brute-force attacks. This happens when
you don't implement rate limiting or allow weak passwords like "password123".
8. Software and Data Integrity Failures Code or infrastructure that relies on plugins or updates from unverified sources. If the update
server is hacked, your "automatic update" just installed malware directly into the system.
9. Security Logging and Monitoring Failures Not recording critical events or ignoring alerts. If you don't have logs, you won't even know
you've been breached until it's too late to stop it.
10. Server-Side Request Forgery (SSRF) Tricking a server into making a request to an internal resource it shouldn't access. It’s like
making the web server scan the local network for you.

1)
Cybersecurity , at its core is the practice of protecting systems,,neyworks,and programs from digital atacks.
These attcks usually aim to access,change or destroy sensitive information.

To achieve this level of protection, security professionals use a model called CIA triad.
Its like a checklist to evaluate how secure a system is.
CIA is short for
1.Confidentiality (privacy)
this means that the data is visible/accessible only to those authorized to see it, meaning keeping a secret 'secret'
eg :1. in a banking scenario, the banking app uses encryption ,meaning even if the wifi is tampered with, The attacker cant
see your payments or balance
2. in a social media setting, it could mean your profile is private so others can't view your hidden posts unless
you approve them

2.Integrity
here it ensure the above data has not been tampered with or altered by unauthorized people.
eg: 1. in banking , the amount sent lets take 10 rs , it ensures the amount doesnt magically change to 1000 or 10000
during the transfer

2. in social media, it could be like , preventing attacker from editing your posts, if a verfied is tampered
they could spread fake news
3.Availability
here we ensures that systems and data are up and running when authorized users need them
eg: 1. in a banking atmosphere, banks uses redadunat servers if a data center fails , so you can send money without a prob
2. to avoid something liek a server down error, company uses servers like cotent delivery networks during high traffic

2)
There are different types of attackers
1-Script Kiddies (The Amateurs):Unskilled individuals or beginners who do not know how to write their own code, they use
pre-made scripts created by others to attacker

2-Insiders (The Internal Threat): They are cuurent or former employees,partners who has legit access to the organization's
system

3. Hacktivists (The Protestors): They are group of attckers views themselves as activits,they dont hack for money,
but to send messages. eg: groups like anonymous

4. Nation-State Actors (The Spies): Another group of attckers,who are skilled hacker groups directly funded and
trained by governments. They are often referred to as APTs (Advanced Persistent Threats).

3)
Attack surface is where an attacker could exploit to enter data or extract data from a syatem.
1- from web applications, it is exposed to public to function so, attckers target input fields and others to inject
malicious code (sql injection,xss) to attempting to trick the application into revealing database
information or hijacking user sessions.
2. mobile apps, attack surface includes app and the device it runs on,hackers reverse engineer the app to
find hard coded api keys or exploit excessive permissions to gain access to user data
3.APIs, apis allow different software components to talk to eachother. because they are designed for machine-to-machine
commiication,they are sometimes less protected,making attckers easy to bypass front-end security or to scrape massive
amounts of data

4.networks, this includes the infrastructure that connects devices,such as wifi, routers ,and firewalls.Attackers scan networks for
open ports or unpatched devices, using them as a foothold to enter the system and move to more critical servers
5.cloud infrastructure, this is the rented computing power and storage.the primary risk here is misconfiguaration rather than straight forward attacking, meaning
setting sensitive records to public - allows anyone to download files with links

(4)
OWASP Top 10 vulnerability
1. Broken Access Control Basically, users getting into places they shouldn't, like a standard user accessing the admin panel.
It’s like forgetting to chmod a sensitive file and letting anyone read or write to it.
2. Cryptographic Failures This is storing passwords in plain text or using weak encryption algorithms. If a hacker intercepts
the traffic, they see the raw data instead of a jumbled hash.
3. Injection When untrusted data is sent to an interpreter as part of a command or query, like SQL Injection. You put malicious
code in a login box, and the database executes it like it’s a real script.
4. Insecure Design These are flaws in the actual architecture or logic before you even start coding. You can't patch a bad blueprint;
the system was built to be insecure from the start.
5. Security Misconfiguration Leaving default settings on, verbose error messages, or open cloud buckets. It’s like installing a
fresh Linux distro and forgetting to configure firewalld or change the default root password.
6. Vulnerable and Outdated Components Using libraries or frameworks that already have known CVEs (Common Vulnerabilities and Exposures).
Your code might be clean, but if you import a vulnerable dependency, you're compromised.
7. Identification and Authentication Failures Weak login systems that allow credential stuffing or brute-force attacks. This happens when
you don't implement rate limiting or allow weak passwords like "password123".
8. Software and Data Integrity Failures Code or infrastructure that relies on plugins or updates from unverified sources. If the update
server is hacked, your "automatic update" just installed malware directly into the system.
9. Security Logging and Monitoring Failures Not recording critical events or ignoring alerts. If you don't have logs, you won't even know
you've been breached until it's too late to stop it.
10. Server-Side Request Forgery (SSRF) Tricking a server into making a request to an internal resource it shouldn't access. It’s like
making the web server scan the local network for you.

5)--
1. Email (Gmail/Outlook) This is the primary vector for Social Engineering and Payload Delivery; the "human" is the vulnerability here.
Attackers bypass filters to land a phishing link or a weaponized PDF directly in the inbox, waiting for a user execution event.

2. WhatsApp/Signal The Endpoint (your phone) is the attack surface here, not the network traffic (since it's E2EE). If malware gets
root/accessibility permissions on the device, it can scrape the screen or dump the local database, completely bypassing the encryption.
3. Banking Apps The main target is the API layer; attackers try to intercept and tamper with the JSON requests between the app and the
server. On the client side, they are vulnerable to Overlay Attacks, where malware detects the banking app opening and draws a fake login window on top of it.

6)--
User input triggers a client-side event, where the frontend validates the raw data and serializes it into a JSON payload sent via an encrypted HTTPS
request. The backend server intercepts this traffic, authenticates the session (checking headers/tokens), and routes the clean data through the
business logic layer. Finally, the application executes an SQL transaction or ORM method to commit the state change permanently to the
database storage.

7)--
At the Client level, attackers bypass frontend validation or execute XSS to hijack the session before data even leaves the browser.
In Transit, they perform Man-in-the-Middle attacks to sniff or tamper with the payload if the TLS encryption is weak. Finally,
at the Server and Database layers, they exploit logic flaws to escalate privileges or use SQL Injection to dump the backend storage.