Cyber Security Assignment 2

1. What do you understand by Assume Breach in Zero Trust?

"Assume Breach" is a core principle in the Zero Trust security model, meaning that organizations should always assume their systems are compromised. Unlike traditional security models that rely on a secure perimeter, Zero Trust assumes that threats exist both inside and outside the network.

Key aspects include:

- Continuous Verification: Always authenticate users and devices before granting access.
- Least Privilege Access: Users get only the necessary access to perform their tasks.
- Micro-Segmentation: Dividing networks to prevent attackers from moving freely.
- Real-time Monitoring: Detecting and responding to threats quickly.

By following this approach, organizations can enhance security and minimize cyber threats.

2. Why is Identity and Access Management Important?

Identity and Access Management (IAM) is crucial for cybersecurity as it ensures that only authorized users have access to critical resources. It enhances security by reducing the risk of unauthorized access, data breaches, and cyberattacks.

Key reasons include:

- Enhancing Security: Ensuring only authorized users can access systems.
- Preventing Insider Threats: Restricting access to necessary resources only.
- Supporting Compliance: Meeting data protection regulations (e.g., GDPR, HIPAA).
- Reducing Attack Surface: Preventing cybercriminals from exploiting stolen credentials.
- Boosting Productivity: Automating authentication processes for users.

IAM plays a vital role in protecting sensitive data and ensuring organizations remain secure.