the body of a data packet may contain sensitive information such as credit card numbers, dates of birth, or personal messages. The header contains the source and destination IP addresses for a data packet.

Passive packet sniffing - reading data in transit

Active – manipulate data in transit

Vpn tunnel

Encryption

Use https:// uses ssl-tls to encrypt data

IP spoofing – changes source ip of data packet

Replay , on path , smurf attack

**Smurf attack:** A network attack performed when an attacker sniffs an authorized user’s IP address and floods it with ICMP packets

Network Interface Card (NIC) is a piece of hardware that connects the device to a network. Only sends data packet if it has MAC Address to destination

pattern=".+@sampleCompany\.com" to be specific account email to allow

input.addEventListener("keydown", (e) => {  
 output.innerText = `You pressed the ${e.key} key`;  
}); keydown – takes any key pressed on the keyboard the assign it to e.

Submit for using onclick(submit) , keydown(enter) , method( requestSubmit() , submit()

Tenary operator : *variablename* = (*condition*) ?(if) *value1* : (else)*value2*

IPS monitors system activity for intrusive activity and takes action to stop the activity

IDS monitors system activity and alerts on possible intrusions.

Both are on the switch between Firewall and LAN

Cryptography can be applied to secure data that is processed and stored in a cloud environment.

Cryptographic erasure is a method of erasing the encryption key for the encrypted data

TPM is a computer chip that can securely store passwords, certificates, and encryption keys.

**Functions of OS**

Windows, macOS®, Linux, ChromeOS, Android, and iOS.

UEFI - Unified Extensible Firmware Interface

**bootloader** is a software program that boots the operating system

**Virtualization** is the process of using software to create virtual representations of various physical machines.

User Interface

Graphic user interface

Command line user interface

**Digital forensics** is the practice of collecting and analyzing data to determine what has happened after an attack.

Vulnerabilities, threats and risks

**risk** is anything that can impact the confidentiality, integrity, or availability of an asset.

**Likelihood x Impact = Risk**

SaaS refers to front-end applications that users access via a web browse

PaaS refers to back-end application development tools that clients can access online. Developers use these resources to write code and build, manage, and deploy their own apps

IaaS customers are given remote access to a range of back-end systems that are hosted by the cloud service provider.

**Compliance** is the process of adhering to internal standards and external regulations

Cyrptoraphy methods.

openssl aes-256-cbc -pbkdf2 -a -d -in Q1.encrypted -out Q1.recovered -k ettubrute

In this instance, the openssl command reverses the encryption of the file with a secure symmetric cipher, as indicated by AES-256-CBC. The -pbkdf2 option is used to add extra security to the key, and -a indicates the desired encoding for the output. The -d indicates decrypting, while -in specifies the input file and -out specifies the output file. The -k specifies the password, which in this example is ettubrute.

Types of SHA

1 , 224 , 256 , 384 , 512

SALT RANDOM STRING ADDED TO DATA BEFORE HASHING TO STRENGTHEN THE SECURITY

Sha256sum filename to generate sha of the file

Cmp file1hash file2has to see difference in hash