Focus area BUW3333

- Network Signature (definition)

* Set of characteristics used to define a type of network activity

- Categories of suspicious TCP/IP packets

* Bad header information
* Suspicious data payload
* Single-packet attacks
* Multiple-packet attacks

- Denial-of-service (DoS) attack under the Multiple-Packet Attacks

* ICMP flood
* UDP flood
* SYN flood

- Packet Sniffer

* Is a software or hardware that monitors traffic going into or out of a network device
* It captures information about each TCP/IP packet it detects
* Captures packets and studies them help in identifying the characteristics of what type of connection is underway and whether the transmission is legitimate or suspicious
* Example: wireshark

- Categories of suspicious traffic signatures

* Informational (traffic might not be malicious, eg ICMP echo request)
* Reconnaissance (attacker’s attempt to gain information about a network as a prelude to an attack, eg ping sweeps and port scans)
* Unauthorized access (Traffic caused by someone who has gained unauthorized access)
* Denial of service (traffic might be part of a more complex attack)

- Ping Sweeps

* To gain access to specific resources on an internal network, a hacker needs to determine the location of a host
* Known as ICMP sweep
* Used by attackers to determine the location of a host

- Common Vulnerabilities and Exposures (CVE)

* Is a dictionary that provides definitions for publicly disclosed cybersecurity vulnerabilities and exposures.
* To make it easier to share data across separate vulnerability capabilities (tools, databases, and services) with these definitions.

- terms in the context of cryptography

- requirements for secure use of symmetric encryption

- block cipher and a stream cipher

* Block cipher processes the input one block of elements at a time, producing an output block for each input block
* Stream cipher processes the input elements continuously, producing output one element at a time, as it goes along

- symmetric block ciphers

* The most commonly used symmetric encryption algorithms
* Processes the plaintext input in fixed-sized blocks and produces a block of ciphertext of equal size for each plaintext block
* The three most important symmetric block ciphers are Data Encryption Standard (DES), Advanced Encryption Standard (AES) and Triple DES (3DES)

- Message Authentication (definition)

- important aspects of message authentication

* To verify that the contents of the message have not been altered
* The source is authentic
* Verify a message’s timeliness and sequence relative to other messages flowing between two parties.

- the process of message authentication using a Message Authentication Code (MAC)