Security Concepts
ivan notes 2022

Devices

- routers
  - -most routers support ACLs
    -ACLs define what traffic is allowed to and from where
- firewalls
  - stateful - keep track of the status of network connections
    -if a connection is allowed to a host, then it is allowed
    -server should not make the first move
- IDS
  - -monitor traffic for IoCs
    -fire alerts to notify security teams to investigate further and take action
- IPS
  - -like IDS, but can act directly to stop attacks as they happen
- OoB
  - IDS and IPS can both be 'inline' or 'out of band'
    -for best protection inline devices must be on every network segment
    -out of band devices have traffic forwarded to them from other network segments
- Proxies
  - -act as middle man to shield hosts
    -most common proxy is an HTTP proxy, used to filter unauthorized traffic
    -reverse proxies exist to shield the existence of multiple servers behind one proxy
- SIEM
  - Capable of ingesting and anlyzing data from multiple sources, can be configured with automated alerts - relies on synchronization to process time stamps on logs

TLS and SSL

- TLS
  - provides encryption for a variety of secure protocols

- SSL
  - -the predecessor for SSL, no longer secure
    -supports early forms of encryption that can be broken

Protocols

- SSH
  - encrypted, can tunnel there protocols, can perform complex file ops
    SCP - secure copy, simple file transfer
    SFTP - FTB tunneled via SSH
- FTP
  - used to transfer files, unencrypted
  - FTPS - FTP secure, not to be confused with SFTP, FTP with TLS encryption, support certificates
- VOIP
  - SIP
    - session initiation protocol - establishes connections between callers
  - RTP
    - Realtime transfer protocol - carries voice data between callers, unencrypted
  - SRTP
    - secure real time protocol - like RTP, but encrypted
- SNMP v3
  - v3 is encrypted

Architecture

- DMZ
  - designate a network segment that is accessible to the public, but does not access the rest of the network
- intranet
  - intra internal network
- extranet
  - private network accessible to authorized partners
- honey pot
  - attracts intruders to fake env

- minimize attack surface
  - least priv, open ports, which services, what permissions? reduce blast radius

Hashing

- one way, provides integrity
- data can be converted into a fixed length hash, unique to the data
- no mathematical process to reverse this, only way to is to figure out what is hashed is through trial and error

Cryptography

- Symmetric encryption
  - -one key is used to encrypt and decrypt data
    -this provides confidentiality
    -generally more efficient than asymmetric encryption
- Asymmetric encryption
  - everyone has 2 keys - public and private
    - public - known to everyone and directly associated with its owner
    - private - only known to its owner
  - public keys can encrypt data that can only be decrypted by its associated private key and vice cersa
  - generally slower than symmetric, often used to encrypt symmetric encryption keys when transferring them
  - can be used with hashing to digitally sign a message
    - hash of msg is computed > hash is encrypted with the senders private key > receiver decrypts hash with senders public key > if hash matches the message sent, then the message is authentic
- considerations
  - key strength is an assessment of how difficult a key or password would be to guess, indicated by length and complexity
  - strong vs weak encryption
    - Strong: PGP, AES
      Weak: WEP, DES

Virtualization

- -allows for rapid reconfig of entire networks
  -snapshots allow us to reset to known good state

- allows for sandboxing
  - observe what malware does without endangering any real assets
  - because malware is on a vm with no network access that we can destroy or reset to a clean snapshot with minimal effort

Malware

- keylogger
  - records keystrokes
- trojan horse
  - masquerades as a legit program
- worm
  - self propagate through networks
- virus
  - infects files in the hopes of being spread by users or host processes
- ransomware
  - holds data hostage

Attacks

- SQLi
  - placing db commands in input that will be read by the db
- XSS
  - embedding malicious code into innocent websites so victims who browse to the website will execute said code
- phishing
  - attempt to gain info or access by masquerading as a legit party
- DOS
  - denies access to systems or services, usually refers to actions by single attacker
  - syn flood: DOS attack that overwhelms victims through half open TCP connection
- DDOS
  - DOS attacks where large groups of hosts overwhelm victims with their combined bandwidth

- bots are infected hosts that participate in DDOS attacks without their owners consent

- ARP Poisoning
  - maliciously sending ARP requests to alter the ARP table of a host
  - allows attacker to redirect traffic destined for other machine
- Buffer Overflow
  - exploit that sends more data than a variable in a program can hold, allowing attackers to change the value of other memory locations

Vulnerabilities

- Default config
  - devices and services often come with a well known default password and other vulnerable configs
- Humans are the biggest vulnerability of any system
  - social engineering is effective, user training is the most effective countermeasure to this and other human issues
- improper input validation
  - not ensuring that user input will not lead to error or unexpected behavior in an app
  - use input validation to mitigate attacks, e.g. SQLi, XSS, etc