Finals Notes

Additional Notes for Finals Exam

General

Terminology

E2E Encryption (E2E)

What is end-to-end encryption?

- Method of secure communication that prevents third parties from accessing data while it’s transferred from one end system or device to another
- Uses PKC (public key cryptography), to encrypt data on sender’s device, and only intended recipient can decrypt it
- Cannot be read or modified by ISP, application service provider, or other MITM
- Vulnerabilities:
  - Metadata
  - Endpoints
  - Intermediaries (not true end-to-end)

CII

- Essentially a system that is necessary for essential service
- Such that the incapacity of the system causes devastating damage

MITRE

- Aiming to solve problems for a safer world, through cybersecurity
- Has MITRE ATT&CK, which is a globally-accessible knowledge base of adversary tactics and techniques baed on real-world observations

- Used as a foundation for development of specific threat models and methodologies in various entities

SetUID

- OS libary function that sets the effective User ID of the calling process
- Can allow other users to make certain calls with the access rights/permissions of another user (User ID)

Bell-Lapadula

- System in designing file structure, for computer security
- Read-down, write-up
- Prevent users from accessing above their clearance
- Can only read downwards, cannot read upwards
- Can only write upwards, cannot write downwards

SOC

Security Operating Center

- Responsible for monitoring and managing an organisation’s security posture

Split into levels:

1. Triage: monitoring and identification
2. Investigation: analyzing and recommending
3. Threat Hunting: active defense, identify vulnerabilities

Crypto

Rainbow Tables

- Table of pre-computed strings and corresponding hashes
- Used to reverse-search hashes and find pre-images

General

- Security of MAC is on forgery, not collision
- Generally, you want 128 bits for a secure password

Network

ARP Poisoning

- ARP deals with the resolution of IP address to MAC address, so need to know both
- In the data link layer

HTTPS

- Requires verification of valid certificate
- If padlocked, then that means a certificate is valid
- However, address bar spoofing is still possible, and a malicious website can still have a valid certificate

Access Control

- `UID` is effective UID, `RUID` is real UID (based on the user calling the process)
- The `/etc/shadow` file contains the hashed and salted passwords of all users
- The superuser in Linux/UNIX environment can only have a UID of 0, but can have a username other than `root`