Activity Guide 1 : Part 2

Ryan Coon

CST-407

Professor Ty Howard

December 10, 2023

|  |  |
| --- | --- |
| **Terms** | **Definition and Example** |
| **Three Types of Security Threats**  Vulnerability  Threat  Attack | **Vulnerability- a weakness in the system. An example of this would be a system not verifying user identity before allowing data access.**  **Threat- a set of circumstances that has the potential to cause loss or harm.**  **Attack- a human who exploits a vulnerability. Can also be launched by another system. An example would be DOS ing someones system causing it to shut down as they cannot handle the amount of messages it is receiving.** |
| **Four Types of Attacks**  I  I  M  F | Interception-Where an unauthorized individual gains access to confidential or private information.  Interruption- a network service is made degraded or unavailable for legitimate use.  Modification- tampering with the asset, or altering data.  Fabrication- creates illegitimate information, processes, communications or other data within a system. |
| **Three Pillars of Security**  C  I  A | Confidentiality – Involves efforts of an entire organization to make sure data is kept private. Access must be controlled to prevent unauthorized sharing of data whether it is intentional or accidental.  Integrity – Involves making sure the data you have is trustworthy and free of tampering. As long as your data is authentic, accurate, and reliable, integrity is maintained.  Availability – While it is necessary to keep data confidential with integrity maintained, it will be useless unless it is made available to the customers they serve. |
| **Six Types of Countermeasures**  1.  2.  3.  4.  5.  6. | Prevent it by blocking the attack or closing the vulnerability.  Deter to make the attack harder but not impossible.  Deflect to make another target more attractive.  Mitigate to make the impact less severe.  Detect as it happens or after the fact.  Recover from its effects. |
| **Three Aspects of Hacker Success**  M  O  M | Method- skills, knowledge, tools and other things with which to perpetrate the attack.  Opportunity- the time and access to execute an attack.  Motive- reason for wanting to attack. |