Paul Collado

CSC-116-71

Homework 5

1. A Business Impact Analysis is an investigation and assessment of the impact that various attacks can have on the organization, and the 5 stages are:
   1. Threat attack identification and prioritization
   2. Business unit analysis
   3. Attack success scenario development
   4. Potential damage assessment
   5. Subordinate plan classification
2. An Incident Response plan addresses the identification, classification, response, and recovery from an incident, and the 4 phases are:
   1. Planning
   2. Detection
   3. Reaction
   4. Recovery
3. A Disaster Recovery plan addresses the preparation for and recovery from a disaster, whether natural or man-made, and the phases are:
   1. Priorities must be clearly established
   2. Roles and responsibilities must be clearly delineated
   3. Someone must initiate the alert roster and notify key personnel
   4. Someone must be tasked with the documentation of the disaster
   5. If and only if possible, attempts must be made to mitigate the impact of the disaster on the operations of the organization
4. Computer forensics is the process of collecting, analyzing, and preserving computer-related evidence, and the results are in the incident recovery process to determine how the incident occurred and what happened

Homework 6

1. A firewall in an information security program is similar to a building’s firewall in that prevents specific types of information from moving between the outside world(untrusted network) and the inside world(trusted network), and the 5 firewall category grouping are:
   1. Packet-filtering firewalls
   2. Application gateways
   3. Circuit gateways
   4. MAC layer firewalls
   5. Hybrids
2. NAT assigns nonrouting local address to the computer systems in the local area network and uses the single ISP-assigned address to communicate with the Internet, and they are used primarily to allow multiple internal users to share a single external Internet connection
3. The 4 common architectural implementations of firewalls are:
   1. Packet-filtering routers
   2. Screened host firewalls
   3. Dual-homed firewalls
   4. Screened subnet firewalls
4. A Virtual private network is a private and secure network connection between systems that uses the data communication capability of an unsecured and public network, one advantage of using VPN allows a user to turn the internet into a private network and send a receive date securely