Pawel Derkacz

Security Engineering

Homework #1

Question 1)

- **LABEL**: ATTACK
- **L0**: Distributed Denial of Service (DDoS)
- **L1**: Keylogger
- **L2**: Man-in-the-Middle (MitM)
- **L3**: Burglary / Smuggling
- **L4**: Forgery
- **L5**: Assassination

Question 2)

- **L0**: Violates "Availability" by forcing the company to have slow to non-existent network communications.
- **L1**: Violates "Confidentiality", since the attacker has access to potentially private information.
- **L2**: Violates "Confidentiality" and possibly "Integrity", given that the attacker can gather information being sent between the HQ and the other building, and potentially modify the information being sent.
- **L3**: Violates "Confidentiality", since the attacker can steal private information that is being stored locally.
- **L4**: Violates "Integrity", since the attacker is taking data and creating a replica with false information on it.
- **L5**: Violates "Availability", given that the person assassinated held some kind of information unbeknownst to other people, and was going to deliver it.

Question 3)

- **L0**: Company would experience a lapse in productivity equivalent to the duration of a successful attack. Loss would be monetary in nature. **Low risk** for the fact that the attacker would need access to the LAN (and have multiple computers), and thus either need to break into the building or be an employee. **Medium risk** if the attacker was only trying to sever the company's connection to the outside world, since the attacker could do that from a secure location. This, however, does not create nearly as large commotion as the LAN DDoS would, and thus probably not worth the attacker's time.

- **L1**: Company could expect damage to reputation, along with damage to any corporate lead if the information logged contains corporate secrets. In all, monetary and reputational loss. **Medium to low risk**, since a lot of data could be logged, but unless the keylogger is installed a computer that belongs to a higher ranking employee, most of the data will be useless. A physical keylogger can only store so many characters (and thus might miss out on anything that IS of value), and a digital keylogger could be detected by software.
- **L2**: Exactly the same loss as described in **L1**, but with potentially higher reputational loss if that was the attacker's goal (the attacker would have to modify data accordingly). **High risk**, since the attacker could gather any information that is being communicated internally (either within the HQ or Network's building, unless two computers are used to get info in both) and potentially modify anything being sent, and thus being highly cost effective for the attacker.
- **L3**: Exactly the same loss as in **L1** (with no need of modification of what was stated). **Low risk** for burglary and **Medium** for smuggling, since a burglar would have to get past the fence or the guard, and still make sure to not be conspicuous inside the buildings. The burglar would also have to know where to go in order to get what they want to steal. This is much easier done by smugglers, since a smuggler would know the layout of the building and potentially know where to go in order to steal sensitive information.
- **L4**: Reputational loss, which may or may not lead to potential monetary loss, if customers turn away from the company due to the reputational loss. **Low risk** since the attacker would have to know exactly how the original document looks in order to create a convincing looking document to replace it. The forger is at least twice as likely to get caught than the smuggler, since the forger has to go back to the same place twice (once to get a picture of the document, and the second time to replace it).
- **L5**: Loss of an employee (victim), and potentially loss of more employees if they have the fear of also being killed. Also loss of information. **High risk** if and only if the information the victim holds is worth keeping forever secret versus the risk of being caught for the murder (which is also high).

Question 4)

- **L0**: Detection consists of being able see that the majority of incoming traffic is garbage. Prevention consists of filtering out these garbage requests if they follow a set pattern. Otherwise, prevention is not possible, but mitigation (of an outside attack) is, by means of having higher bandwidth and multiple servers.

- **L1**: Detection of a physical keylogger can be done by either seeing that a foreign object is connected between the computer port and keyboard cable, or by noticing a slight delay between striking a key to the keystroke being registered on the computer. Prevention can be done by visually inspecting the computer before use (every time). As for a digital keylogger, detection can be done through a process inspector (such as an antivirus program) and the program detecting that the process is recording keystrokes and writing them to a local file, or sending them over the internet. Prevention can be done by use of an antivirus program, along with needing a password to install any new program, and also potentially having someone monitor traffic, checking if suspicious data is being sent.
- **L2**: I am unsure how to detect MitM (over LAN), but prevention can be done by encrypting all information that is being sent on the LAN.
- **L3**: Detection can be done by visual means - if someone in the building is acting suspicious, they could be attempting to do something illegal (such as burglary/smuggling). Prevention can be done by posting video cameras at critical points across the building that record all activity (and having someone monitor that activity), and by potentially adding an extra layer of security (such as a door keypad) to any room that contains records of potential interest.
- **L4**: Detection and prevention are done by exactly the same means as stated in **L3**.
- **L5**: Detection is done visually, as in **L3**. Prevention can be done by having bulletproof windows (should the assassin be a shooter sniping from a distance) and by having an inspection station inside the building to check for weapons.