
Physical Security LAB

LAB 3

Josiah Smythe

February 12, 2019

Dr. Lehrfeld -Information Security and Assurance

East Tennessee State University

1. Purpose

Preform an informal audit of the East Tennessee State University Millennium Centre with the intention to evaluate the amount of physical security thereof.

2. Materials

This security audit was completed by the four individuals, Aaron Barlow, Cory Moore, Garrett Landon and Josiah Smythe. This audit was completed in the ETSU Millennium Centre which is at the address 2001 Millennium Pl, Johnson City, TN 37604. This security analysis was completed on Wednesday February 6, 2018 beginning at 7:00 PM. A clipboard was used to hold a paper where all collected observations and record numerical values of security vulnerabilities were recorded.

3. Procedures and Results

This physical security audit was conducted in a methodical way by beginning at the walking overpass that connects the ETSU campus to the Millennium Centre. From this position the team began the by checking the physical security of the exterior of the building based on the number of exterior doors. This building has seventeen exterior doors, most of which are made of metal frames with glass panes. At the time of this evaluation the two doors on second floor facing the overpass and those on the first floor were unlocked. All the other doors were locked to entry from the outside, and enabled persons in the building to exit at will. The team discovered that a door on the back side of the building that had a faulty locking mechanism and the door was sometimes accessible even when locked. If shut firmly this door would lock, but if just let to shut on its own it may not lock.

After completing the exterior evaluation, the interior physical security was assessed beginning on the second floor. Upon entry it was noted that a security camera was mounted on the interior hallway facing the doorway nearest to the overpass. Above the same doorway there was an ADT motion sensor that was determined to be likely connected to the overhead security camera. On the second floor there were four open RJ-45 Ethernet wall and floor ports that were easily visible to an individual walking down the main hallway. All of the class rooms doors on the second floor were locked and secure, but the men's bathroom had a janitor closet that was unlocked. Inside there were several garden hoses and chemicals that were in store for cleaning. On the side of the building with offices there is an employee only area that was not clearly marked. The area was unlocked and upon entry the team discovered a sign on the wall stating employee's only. This area was not clearly marked and without it being securely locked down during the night it was a vulnerability to the security and safety of any items stored there. This area seemed to be a long-term storage area for event supplies like tables and chairs, a complete inventory was not made because upon discovery of the employee's only sign the team immediately evacuated the premises.

When the second-floor evaluation was complete the team began evaluating the first floor. It was discovered that in a stair well on the office side of the building there was an unlocked metal cabinet with about forty brand new printer ink cartridges. These printer cartridges were estimated to be of a value of near one thousand dollars. This stair well was right next to the door noted above that had a faulty locking mechanism and therefore this storage of printer cartridges was unsecure. An exposed printer was discovered on the first floor. The ability of using that open printer to access the previous information of any computer that had used that printer was brought to the attention of the team by Cory More. All of the class rooms on the first floor were locked except room number one hundred and thirty-seven B. This class room had near seventy-five open RJ-45 Ethernet ports mounted in on the tables. The teacher's computer

was unlocked and was accessible to anyone who attempted to open it. The podium cabinet was unlocked and inside was a collection of sound equipment and technology devices that were insecure. Upon exit of this room after the completion of the evacuation, all lights were turned off and everything was left exactly as it was upon entry. About thirty seconds after closing the door again to this class room an individual in a hoodie exited the room. Upon questioning the individual he disclosed that he was in the projector room, that was locked, and then he left the premises. The conversation interaction with this individual and the team was short and abrupt, stimulating the idea that he was not there working, but that he was hiding or sleeping in the projector room. There were also two additional cameras on the first floor monitoring the activity.

While evaluating this building a janitor was cleaning and a security guard was maintaining the interior security by walking the indoor area of the building. There are twenty-two doors on the interior of this building, and all were locked with the exception of the class room one hundred and thirty-seven B. Out the back of the building there was a box trailer stored in an open garage with no trailer hitch protection to stop theft.

4. Observations

This audit showed the various methods of physical security that have been employed in this building but also how this building has numerous serious vulnerabilities. Starting with the unknown individual that was in the projector room in room one hundred and thirty-seven B. This poses a serious security issue because this individual may lay low until late in the night and then make his move and steal or vandalize this building. The team decided that actions must be taken by the security team of the Millennium Centre and ETSU campus security in response to this discovery. Suggested steps would be to implement a careful search of each room before locking it down for the night, that would include all offices, closets and projector rooms.

Another aspect of this buildings security that was in danger was the vast number of RJ-45 Ethernet jacks that were exposed to the public. These ports could be used to infiltrate the network and access private data of any person connected to the network. The team did not attempt to connect to these Ethernet ports to avoid being suspicious, but these ports must either be removed, or a secure login connection software must be implemented to protect the network from individuals infiltrating or infecting the network through connecting to the open ports. This building also supports an open wireless network that is accessible to any person that enters the building, this poses a huge security vulnerability because all the data on that network is able to be sniffed by any hacker wanting to access it. This open network must be eliminated, and a solution would be to replicate the authentication system that has been implemented throughout the ETSU campus.

This audit brought to light show the importance of physical security for this building. It calls into question the efforts that are being made to maintain and secure this building as well as considering the results of those efforts. Performing an audit like this helps to stimulate a desire to consider the physical security of any building that is entered to consider the levels of security being implemented. It is thought careful analyses that evaluate how the building security is regulated and improvised that the physical security of any building is developed, and new technologies are implemented.
