Physical Penetration Test

Chris Danyluk, Nick Regan, Jacob Shapiro and Dan MacCarthy

School of Computer Science & Mathematics, Marist College

CMPT 479N - Cybersecurity Capping Project

Professor DeCusatis

December 9th, 2022

Table of Contents

I. ABSTRACT

For this paper, we attempted to discover a new method to teach cybersecurity analysts about physical penetration testing. We started by taking an assessment of our knowledge and then completing 11 challenges, before retaking the same assessment again. The result of the second assessment was a large increase in the number of questions correct. In theory, this method could work to teach people about physical penetration testing, but the low sample size prevents any conclusions from being made.

II. INTRODUCTION

How do you appropriately teach someone physical penetration testing? Anyone learning would gain minimal experience until they were out in the field as a penetration tester, but by then it's too late. Our project sought to resolve this by developing an educational model to assist with training new workers. We started off with an assessment of what we knew about penetration testing, shortly followed by eleven challenges designed to test our cybersecurity knowledge and our critical thinking skills. After completing every challenge in our way, we took the same assessment we started the project off with to see how much we grew, as well as designing some Mind Maps about our project. With all of this, we were able to develop a gamification model of our project to help user retention of the information learned.

A. USER CASES

Before we started our project, we compiled a list of user stories to keep in mind as we progressed throughout each of the challenges. These user stories are as follows:

- As a worker, I want to learn more about what I can do to protect myself at work so that I am not at risk for an attack. This knowledge could help me to keep myself and my work secured, which may result in better job security.

- As a manager/CEO, I want to learn more about the vulnerabilities of my company so that I may protect my assets better. I do not want my company's assets and intellectual property to be leaked, so maintaining strong security is a must.
- As a penetration tester, I want to receive written consent before starting my work so that I may conduct a safe and ethical penetration test. Most of what I do as a penetration tester would be illegal, despite it being done in the name of security. As such, receiving written consent from my employer means that I may perform an ethical penetration test so long as I remain inside the scope of the given permissions.
- As a penetration tester, I want to be able to ethically impersonate a person so that I may get better results and to understand how the company would fare in a real attack. However, certain limits must be employed as this could easily become unethical should a new user try to gain access outside the scope of the job. Additionally, a person's job security could be negatively affected should I impersonate them too easily or too well.
- As a penetration tester, I want to report any and all information learned during a penetration test so that I can help my employer bolster their defenses. It is my job to learn as much as possible about the vulnerabilities of a company so that I may give advice on how to mitigate those vulnerabilities.

Following these user stories before beginning any penetration test is a must as it helps define the goals of a penetration test as well as keep us ethical. Penetration testers must employ a strong basis of ethics to ensure that our work does not shift from an ethical penetration test to an actual attack.

B. CREDIT

As we worked, we recorded what each of us did to help maintain credibility, but kept our jobs loose to allow for anyone to work on any particular task. For the purpose of the project, we are all penetration testers, but we are a team first and foremost. As such, we all must be working well together and understand each other's work just as well as our own so that we may accomplish our tasks efficiently. We have compiled a brief summary of what each of our main tasks were during the project, as well as who performed each one.

- Chris Danyluk identified the first building which began our penetration test as well as the camera system that was deployed at the penetration test site. He helped locate our infiltration point into the penetration test site, as well as the pretexts that would be applied there to remain undercover. Once inside, he identified what an ESPKey is and how to effectively utilize one. Additionally, he demonstrated how a ProxMark works by utilizing one and how a ProxMark and ESPKey can work in tandem. Lastly, he helped identify some RFID cards used throughout the penetration test and various lockpicks that could be used to gain access to the server room. For this paper, he worked on the challenges 1, 3, 7, 8, and 11, as well as the introduction, before/after assessment, and the conclusion.
- Nick Regan discovered the vulnerability used to enter that car that helped us locate the penetration test site. He helped locate where the penetration test site was as well as information related to the location such as the security office location. He identified one of the entry mechanisms to gain access to the building and subsequently bypassed that system. Once inside, he provided information on the elevator system used to traverse through the building. He demonstrated

intensive knowledge on safes and how to break into the one we discovered during our penetration test. Finally, he helped identify various RFID card frequencies. For this paper, he worked on challenges 2 and 6, as well as the mind maps.

- Dan MacCarthy identified the tools needed to unlock the car we used to locate the penetration test site. He also led the team in locating the penetration test site.Once inside, he discovered what type of elevator was being used as well as how we could utilize various keys to access the fire service mode for that elevator. While we were waiting to gain full access to the elevator, he discovered a set of keys. With this set of keys, he managed to identify them and work out the bitting code from a glance before creating a copy using the blank key set in our penetration test kit. Finally, he helped identify some of the RFID cards we came across as well as a tool to bypass the lock into the server room. For this paper, he worked on challenges 9 and 10, as well as editing/reviewing this paper.
- Jacob Shapiro identified various CVEs related to breaking into cars, which we utilized to break into the car that helped us locate the penetration test site. He helped locate where the penetration test site was located as well as information relating to it such as the security office location. He helped locate our infiltration point as well as the pretexts to be used to maintain our undercover status. He identified the lock used to enter the interior of the building as well as how to crack the code or bypass it with a Lishi tool. He demonstrated immense knowledge on RFID cards and how to clone them with just an Arduino in case we needed to bypass the RFID locks on the inside. Finally, once inside, he identified various UDTs and how we could potentially use one to enter the server room. For this

paper, he worked on challenges 4 and 5, as well as the entirety of the final presentation.

The reason this was skewed towards one member writing most of this paper is because that particular member had the most time to dedicate to the final paper in the group as well as being able to write at nearly double the speed of every other group member (I did this on my own volition). For some of the provided tasks, one member from our team dealt with it alone before informing the rest of us about how they dealt with it. For others, however, we worked together as a team so that we may approach the problem from all angles and have a more thorough plan for tackling each challenge.

III. CHALLENGES

A. CHALLENGE 1

Starting off our challenges, we were given a very limited amount of information. Included in our information was a list of companies that interact with our target and a picture of one of them. In order for us to gain any useful information about our target, we first needed to take a look at this photo and discover what business this was; if we could figure out what

business this was, then we could figure out more about our target from them.

Fig. 1, Picture of business that receives regular shipments from our target, as well as a sign in the center of the photo.

In the middle of the picture we can see a street sign that when zoomed in on reads: “Bartow, City of Oaks and Azaleas.” After discovering this we started googling that city name along with its slogan, and we discovered that this particular city was located in Polk County, Florida. Continuing on with using the signs to our advantage, we saw the sign on the right side of the picture. Even though the sign itself is cut off, the part we could read said “Sara Fl.” Furthermore, the building itself was covered in flower decals. If we use that to assume that the cut off sign stood for flowers, we started googling Sara’s Flowers, limiting our search to the town of Polk County that we had previously discovered. Once we had found this building we went into google street view and compared the flower shop, the building we were told to look into, and the signs we had looked at to the picture we were given. When we were certain that everything matched up and we had found the correct street, we were able to use google maps to see that the building in question was the Florida Department of Citrus

(https://www.floridacitrus.org/). Once we identified the building name we could start doing research to find out more information. We were able to see their website, phone number, and hours of operation.

Once we found the building and were able to go in person, we found a company car in the parking lot. Peering inside the vehicle, we found some mail laying on the seat. Doing a reverse image search of the car we were able to come to the conclusion that this particular car is a 2020 Honda Breeze, a car almost exclusively sold in China, however, basically an equivalent to the Honda CRV.

Fig. 2, A 2020 Honda Breeze found in the parking lot.

Now that we know the type of car we can look in the CVE database to see if there are any known vulnerabilities that we can exploit. Looking into CVE-2021-46145 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-46145) and CVE-2022-27254 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27254) [1] we discovered that these types of cars use a repeating radio frequency on their key fobs every time the car is unlocked, making them vulnerable to a replay attack or a Rolling PWN attack. A Rolling PWN attack is

when a bad actor intercepts code sent from a car owner's keyfob and then utilizes that code to gain access to the vehicle [2]. Investigating further, we discovered that most, if not all, Honda cars suffer from this vulnerability. Even if that was not the case, some of the information provided to us beforehand stated that this particular car has not been updated to protect against old security flaws, so this approach should work regardless. However, we did not have an SDR on us and the owner of the vehicle was not around for us to intercept the radio frequency upon the key fob's activation. Instead, we pulled out our Flipper Zero, a small device designed to act like a cybersecurity swiss army knife that can interact with tons of devices in the real world [3]. With our flipper zero, we popped open the locks and gained access to the vehicle. Using the address on the package, we were able to truly begin our penetration test.

Now, while these vulnerabilities are not from the target themselves, they are from a business within their supply chain. Vulnerabilities from within the supply chain, in some cases, can be just as bad as vulnerabilities from the target because the target is to assume that the people they work with are legitimate and secure. We could identify two vulnerabilities taking place. The first of which is the repeating radio frequency that enabled us to utilize a rolling pwn attack. As we mentioned before, this vulnerability would most likely have been patched out on an updated vehicle, but as this is not an updated vehicle, we can exploit this. The best way to mitigate this threat would be to simply get all new company cars. While this may seem like a very expensive solution, the fact that these cars are not being updated at all means that they are likely vulnerable to a host of other vulnerabilities that we did not even exploit. Not employing this solution would also mean that any future vulnerabilities that arise would not be fixed, meaning there is a chance that a far worse vulnerability would be revealed later that could be exploited against the company. Alternatively, if money can not be spared to upgrade all of the company cars, video

surveillance could be installed in the parking lot. Unless someone was actively watching the camera feeds at all hours of the day, every day, this would not act as a deterrent. Rather, this would allow for the company to pursue whoever broke into their property.

The second vulnerability we noticed was that a source of important information was left out in plain sight. This information was the reason we broke into the car to begin with. We likely would have ignored the car and continued on our way if we had determined it to be just a car with no additional use to us. In practice, there are several ways to protect against this vulnerability, but ultimately, all those ways boil down to two methods of dealing with the issue. The first is for employees to not leave important information out in the open and to instead lock anything of value inside a drawer or compartment. This should apply not just to cars, but to people in offices and even at home. By concealing important information and locking it away, one can prevent its theft and reduce their odds of a break-in. The second method should not be a replacement to the first, but rather an additive to further reduce risk of a break-in. This method is to tint the windows of the car. By tinting the windows of the car (or office, as this advice can be applied anywhere), one can prevent those from outside from seeing in, effectively concealing important information to the outside world. Of course, this does not help protect against those who are already inside, which is why it is a good idea to employ both methods to maximize mitigation of this vulnerability.

B. CHALLENGE 2

Continuing on with the challenges, we were asked to discover as much information as possible regarding the address on the package found in challenge one. To do so, we started off by google searching the address on the package, that being 165 Business Boulevard, Clear Brook,

VA 22624. The results of the search indicated that the address was linked to an Amazon fulfillment center in West Virginia.

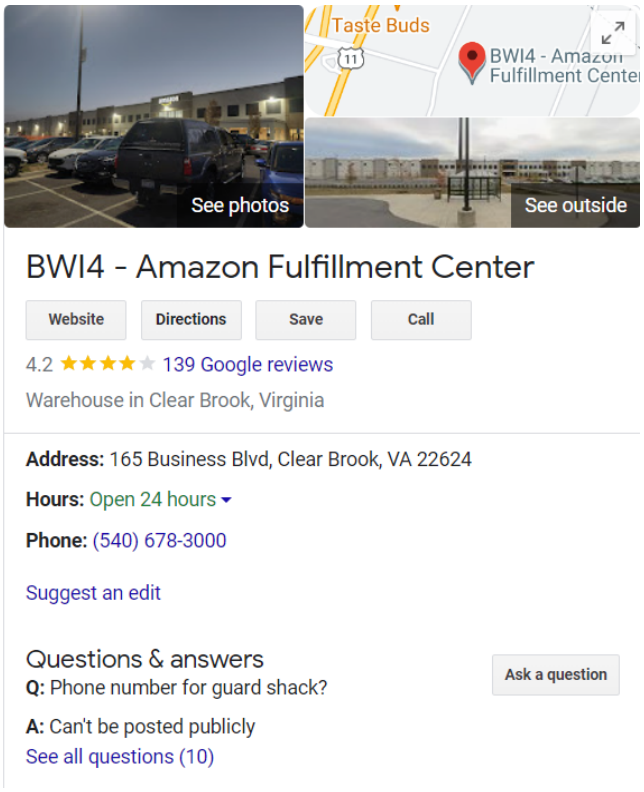

Fig. 3, Google search results of BW14 Amazon.

Aerial images were then taken of the facility using various satellite imaging tools such as google earth and apple maps. The facility appeared to be located on the edge of a small town and had some open fields to its East. Street view mode was then utilized to capture closer and more detailed pictures of the building to give us a better idea of what we were up against.

Fig. 4, Image of the amazon facility taken from the parking lot on the west side [4].

We were able to gather street view images of the North, West, and South sides of the building before encountering barriers with the street view range. Interior pictures of the fulfillment center were also gathered from different google map posts that employees uploaded

while on the job. These images included shots of storage areas, loading docks, and the security office (see additional Fig. 5).

Once we gathered all we could, we reported our findings to our client and were then asked to locate the entrance to the Amazon fulfillment center on Woodbine Road. Our client also requested that information regarding the security office entrance and the receiving dock driver's entrance be reported as well. We started off by prioritizing the Woodbine street entrance. It was determined that the fulfillment center had two main entrances, those being one for "All Trucks" and one for "Visitors and Associates." This was discovered from a sign present on Woodbine Road West of the facility.

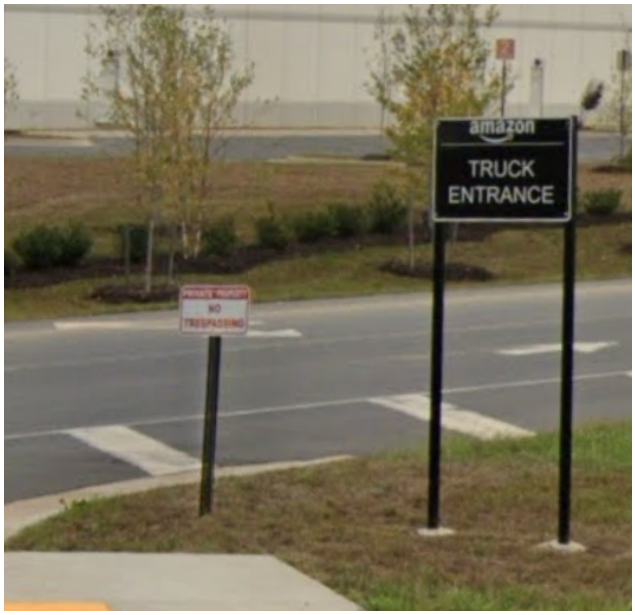

Fig. 6, An image taken on Google street view depicting the Amazon fulfillment center and a sign stating the address, "Visitors & Associates" and "All Trucks"

Fig. 7, An image taken on Google street view depicting a sign that states "Truck Entrance" as well as road markers pointing further down the road.

Other signs were also spotted stating that no weapons were allowed in the facility and that surveillance cameras were in use. We then went into google earth's street view and took several zoomed up images of the facility on its West side to determine that the "Visitors and Associates" entrance was the main entrance for Woodbine Road. Multiple security cameras were also seen in the zoomed up photos that would grab our attention later. Now it was time to focus our attention on the security office entrance and the dock driver's entrance. Several hours of examining all the possible google earth street view areas around the fulfillment center led us to conclude that the entrances we were searching for were located at the "All Truck" entrance. Unfortunately, this entrance was located on the East side of the building which was restricted from google earth street view. Luckily though, images of exactly what we needed were able to be obtained from various posts employees from the fulfillment center uploaded to google maps.

Next, it was time to assess the general security of the building. While examining exterior images of the fulfillment center, cameras were spotted scattered around the walls of the facility. A closer look at the cameras led us to determine that they were provided by a company called HIKVISION, a Chinese based surveillance company (https://us.hikvision.com/en). This information is significant because HIKVISION was added to the SDN list in 2021, meaning their assets are blocked and most U.S. people are prohibited from interacting with them [5], [6].

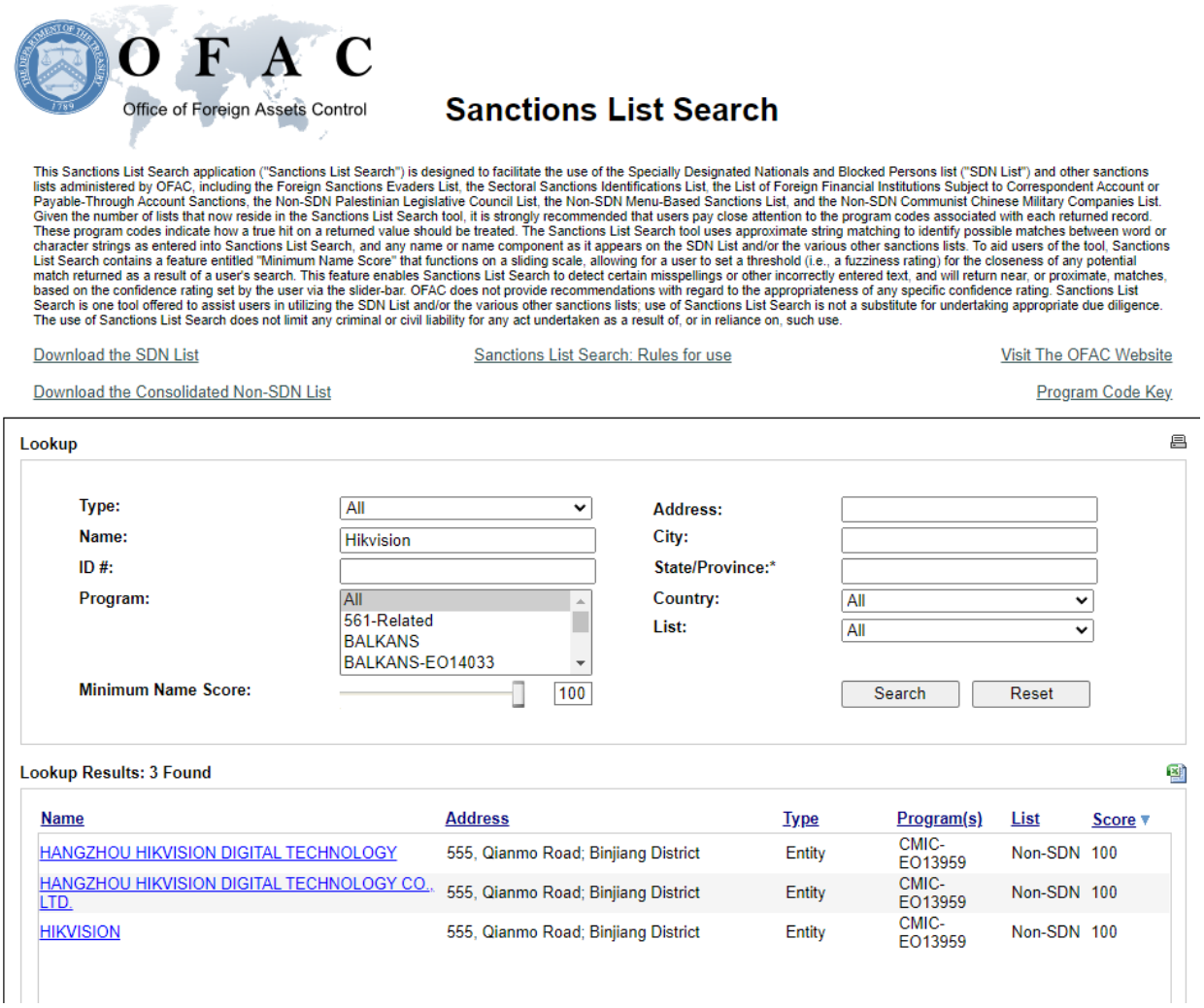

Fig. 8, A screenshot of the search results for Hikvision in the U.S. OFAC Sanctions List Search [5].

Additionally, as of November 25th, 2022, HIKVISION was banned from exporting goods to the U.S. and from being used in any U.S. organization unless proof is given that they will not "be used for public safety, security of government facilities, and other national security purposes [7], [8]". This means that even if the facility doesn't have to remove their HIKVISION cameras, there is a chance that any new CVE's that are reported for these cameras will not be patched. With the surveillance system identified, it was time to look at the security office.

Fig. 9, An image of the security office in the Amazon fulfillment center [9].

Further examination of the security office images led us to conclude that the door leading into the office operated using magnetic locks. To gain access to the office, workers and authorized personnel would utilize what appeared to be an RFID scanner. A secondary means of authorization was also visible, that being a mechanical lock. Based on the placement of the hinges on the door, it was also safely assumed that the door opened outwards rather than in the office. We now had all the information necessary to derive a plan to enter the fulfillment center.

The first part to any penetration test, whether that be for a physical location or a digital solution, is always reconnaissance. With this knowledge, it's reasonable to conclude that available information is a vulnerability. It's this vulnerability that allowed us to gain a good understanding of the layout of our target and the ability to plan a means of entry. In the case of the Amazon Fulfillment center, the main vulnerability causing information that we will focus on mitigating are internal images. More specifically, any images or pictures taken from within the building that depict the layout of a room.

The first approach to mitigating the risk of bad actors gaining information on the interior of a facility is to see what information is available. By conducting a google search on a facility, an organization can see what's available online for bad actors to use. Once aware of the information unauthorized personnel can collect, an organization can adjust their security measures to counter possible vulnerabilities to available information.

An organization can also mitigate the risk of excess information being available to the public by implementing policies that prevent workers from taking pictures within a facility. All the interior images gathered of the Amazon fulfillment center were all taken from workers. Even though the workers had no malicious intent with the pictures, they can still cause vulnerabilities to come to light. The principle of transitive trust applies here. If an individual is trusted with information, everyone that person knows is also trusted with the information due to the possibility of the individual telling others what they know. Therefore, to ensure as little vulnerability inducing information is available, it's recommended that a policy restricting employees from taking pictures within the faculty be implemented right away.

C. CHALLENGE 3

Once we had performed a sufficient amount of reconnaissance, we decided to come up with a few entry plans for making it into the facility. Utilizing google maps, we searched the surroundings of the facility thoroughly in order to locate the best approach for entering. After some deliberation, we developed two possible entry methods. The first entry method involves a canal running parallel to the train tracks on the east side of the building.

Fig. 10, Image of the canal running parallel of the facility on the east side.

If there was a pipeline runoff into the canal, we would enter through there as it would involve minimal human interaction. In order to make sure we don't get caught on the approach, our apparel would be a black sweatshirt and we would approach the facility around midday for two reasons: when the shift changes our sudden appearance will be less jarring, and many shipments will be coming in and out during that time meaning it will be a high traffic area.

If the first entry method was unavailable, we had a back up entry method, which is via an Amazon delivery truck. This is an Amazon fulfillment center, so naturally there would be multiple amazon trucks entering and exiting the premises, several times a day. We would access the truck via a truckstop or from the treeline by the southernmost fence. In order to remain unnoticed, we decided that the best way to enter with an Amazon truck would be to cling to the bottom of it using specialized tools. Similarly to the previous method, we would approach from

around midday, however our outfit would instead consist of an all black outfit with an alternate outfit underneath.

Once we enter the property, we would remove our approach apparel and put on an outfit similar to the workers uniform. Thanks to some of the pictures we found of the inside, we know that workers typically wear a standardized outfit. This outfit consists of a bright green safety vest, underclothing such as a black long sleeved shirt, jeans, and regular sneakers. In our bag we would include a hard hat and a lanyard with a fake id to further the uniform.

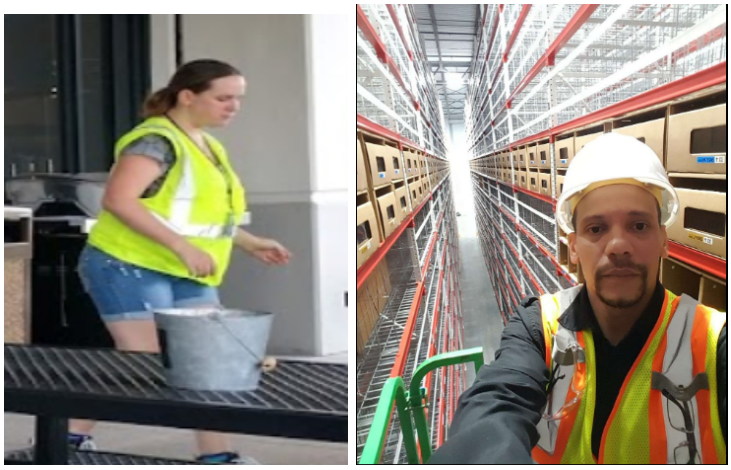

Fig. 11, An image depicting a worker wearing a standard uniform consisting of a vest, jeans, and some form of undershirt [4].

Fig. 12, An image depicting a worker wearing a standard uniform consisting of a vest, hard hat, and some form of long-sleeved undershirt [9].

Blending in with the workers could be difficult depending on the situation, but that is all a matter of charisma and following a few pretexts. Firstly, we would all try to make light talk with our co-workers while pretending to work. Next, we could all have differing types of earbuds that would allow us to remain in contact with each other, but we could easily pass it off as

listening to music while working. Lastly, we would learn some common phrases used in this particular work environment in order to better hold a conversation or even start one to keep off suspicion.

As we explored while maintaining our disguises, we took a few photos of the loading dock area to gain some insight on possible ways to enter the building. After analyzing the photos at home, we located a mechanism used as a possible entry point into the facility.

Fig. 13, Telephone entry system from Linear.

This mechanism is a telephone entry system for a brand called Linear. The Linear telephone entry system operates as a means of authentication that grants workers access to the facility. The main functionality of the telephone system is to automate the authentication process.

In order to automate the authentication process, the telephone entry system grants access control to the workers within the facility. Some of the possible access controls are as follows: some amount of users have their extensions or numbers added in the terminal that users can call to be granted access, master codes that are provided to workers who frequently traverse using this system to allow for ease of access, and workers who don't have normal access to the area can use the panel to dial security and potentially be granted access after explaining their situation [10].

It is these exact same access controls that are the primary vulnerabilities in this system. The first attack vector we can try is using the default factory entry code for the telephone entry panel. Every Linear telephone entry system comes with a default code of 123456 that allows the user to gain access to configuration settings and authentication access [11]. In the event that the facility has removed the default passcode for the system, we can move on towards examining the mini lock above the display screen. After conducting a reverse image search of the panel, we determined that the model of the telephone system is an AE100. Upon searching for default keys to access the AE100, we were able to find replacement default keys on amazon for 17.99 (https://www.amazon.com/Linear-222343-ACP00959-Replacement-AE1000/dp/B00GPP1FVC). Once we gain access to the hardware within the panel, we can rewire the system to reset all of its settings, therefore allowing us to use the factory default code to get in. However, this is likely to draw attention and due to us approaching from midday as part of our infiltration, there is likely a great deal of nearby foot traffic. This approach would arouse too much suspicion, so we could instead attempt to obtain one of the master codes. This could be done through social engineering once we are in the area. Social engineering is very circumstantial as its success relies completely on who we speak to and what we say. However, it may be slightly easier as all the security measures to prevent intrusions has made the facility overconfident; thus any workers in the area

would assume that we are authorized to be there. Finally, we could simply wait until a group of workers attempted to enter the building through the telephone entry pad and then tailgate them in.

There are a few noticeable vulnerabilities during this part of our penetration testing. Humans are generally empathetic creatures, which means it is almost criminally easy to manipulate them. As such, the most pressing issue we found with our approach is how we could use social engineering. Due to workers assuming anyone on grounds has a right to be there, our disguises and pretexts don't need to be too in-depth in order to appropriately blend in. Additionally, it is possible that we could bypass the Linear telephone entry system using social engineering. We could either speak with the nearby workers to try and gain a code, or take a big risk to call security to gain entry. In either case, we would gain access without using any tools. This threat can only really be stopped by employing regular social engineering training for all workers. Also, removing the idea that anyone in the facility has a right to be there because of the facility's overconfidence.

The second vulnerability we located was the use of outdated systems that we could exploit with minimal repercussions, simply because the system may never be updated again. This vulnerability matches with the Linear Access Telephone Entry system. As mentioned before, there are many ways we could bypass it. We could use the factory default code or the default key to bypass the system. This can be prevented by removing the factory default code and changing the lock on the system to a different lock. In extreme cases, the facility could just change the system to a more up-to-date system, such as an RFID reader.

The last vulnerability was mentioned in the previous challenge as well, but it also applies here: available information. The information available to us before we began our infiltration

allowed us to create our disguises and pretexts that let us blend in with the other workers. In this particular case, however, there are more ways to mitigate this vulnerability. Same as before, company policies could be added to prevent the posting of sensitive information online. Unlike before, the facility could add an identification system to make our disguises ineffective. Having some form of identification badge would alert any nearby workers to imposters as they would not have proper identification. Alternatively, having a supervisor or two in the area who knows everyone's face could be helpful here, as they would have been able to see that we were fakes before we infiltrated.

D. CHALLENGE 4

While we were analyzing our reconnaissance photos, we came across an additional lock on one of the interior doors. Bypassing this lock would get us inside, but we needed to understand the lock before we could effectively break it. To do so, we utilized OSINT to identify vital details pertaining to the lock both virtual and physical. The lock in question has two forms of entry: One being a ten digit keypad, the other a manual entry via key. Further analysis provided the information needed to identify the brand. The type of lock is the Trilogy DL2700. With this information, we were able to conduct further research providing valuable information on the number of digits required for valid input, which is a total of 5 digits. Ergo, the possible combinations with repetition is 10^5 which is equal to 100,000, since there are 10 numbers, with 5 potential positions. Learning this was rather intimidating. Utilizing brute forcing techniques are deemed impractical considering the timeframe in which we have to break the lock. Spending too much time will raise the eyebrows of those around, therefore, making our main objective to be as efficient as possible. Focusing our attention on research again, we came across factory

documentation for the Trilogy DL2700. Within the manual, we came across default access codes, which can be used once the lock has been exploited [12].

Now that the online research has been conducted, further inspection of the lock is needed to identify physical attributes that could prove to be beneficial. Looking at each button, we spotted 4 numbers with distinct features of bodily oils and erosion from repeated entries, as seen in fig. 14.

Fig. 14, A 10-digit keypad lock known as the Trilogy DL2700.

The deteriorated numbers 1,4,7,8,9 decreased the potential combination amount from 10^5 to 5!. An immense difference of 99,880, leaving a mere 120 remaining. Taking this a step further, we've come to realize how habitual human beings are. By utilizing the most common input pattern of passwords, we identified three passwords that had the highest probability of success: Input one being 1,4,7,8,9, Input two being 9,8,7,4,1, and Input three being 1,4,9,8,7. Of the three combinations, input three was the least probable. We based this input on how specific cultures read, more specifically, Arabic, Aramaic, Azeri, Dhivehi/Maldivian, Hebrew, Kurdish (Sorani), Persian/Farsi, and Urdu. All read from right to left, which gave us the idea of inputting the code top to bottom, right to left, as seen in fig 15.

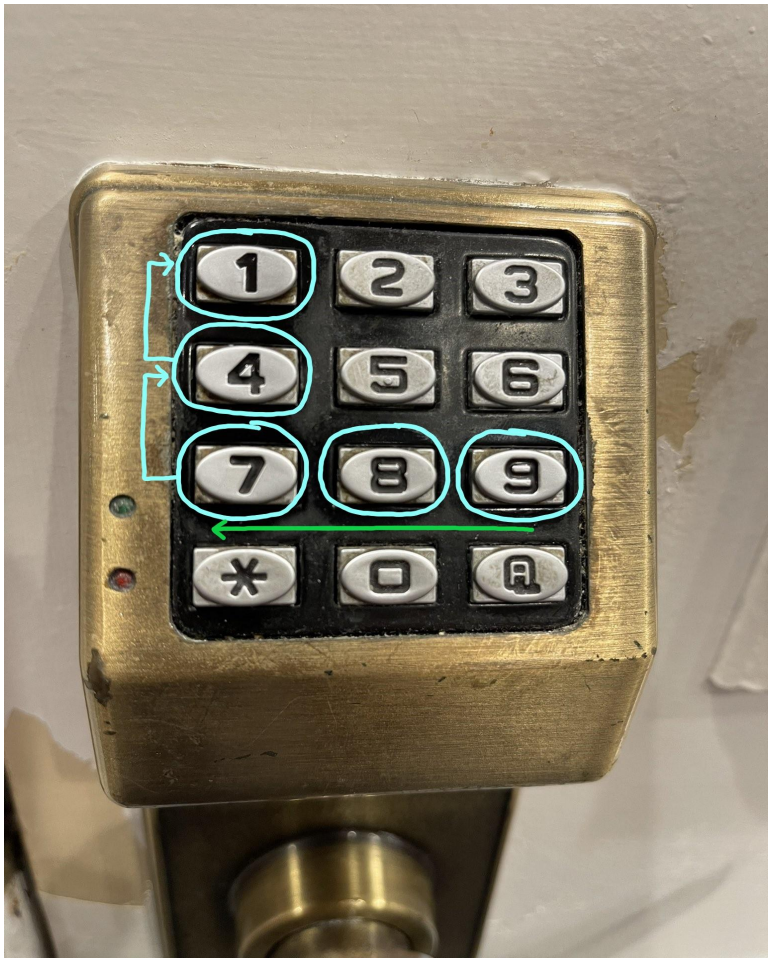

Fig. 15, A 10-digit keypad lock with one possible unlock combination

Although, due to the facility in question being from the United States, the likelihood of middleastern culture to interject with this is unlikely. The second most possible was the reverse of the most probable input method, reading top to bottom left to right. Flipping and turning the code upside down is a common theme as it provides a vastly different input, all while staying close to the traditional method. As mentioned, the most credible combination found was top to bottom right to left, as seen in figure 16.

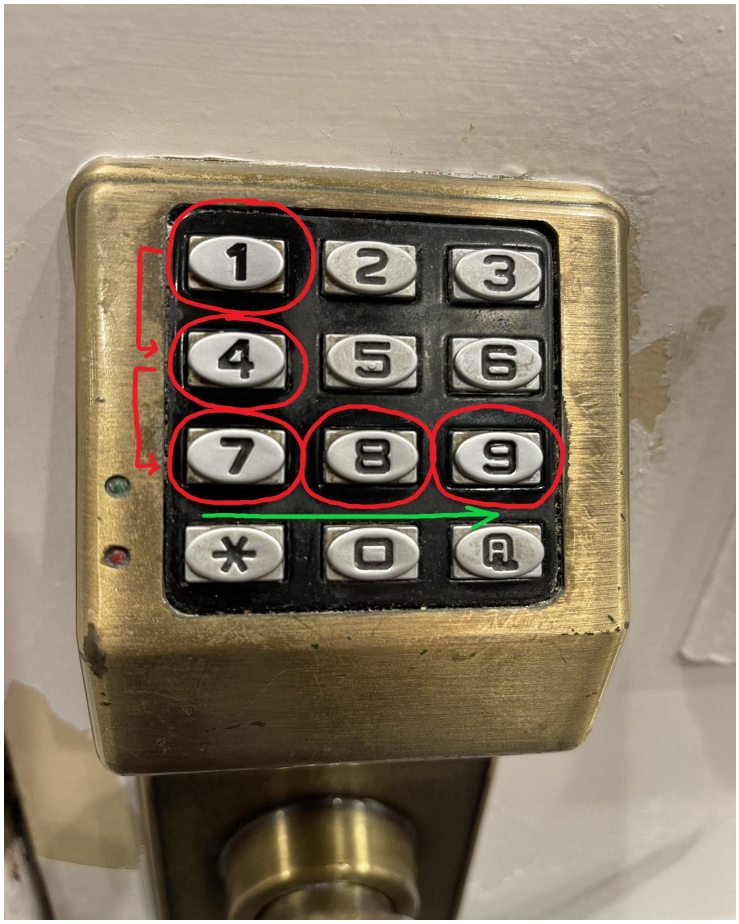

Fig. 16, A 10-digit keypad lock with another possible unlock combination

Reasoning for this is simple, this is a company founded and based in the United States. It's safe to assume that password inputs would fall under the same ideology as reading a book in the US. After inputting all three combinations, we found that input one was successful.

In the case we wanted to reset the lock to factory settings, we could have detached the backplate from the lock and removed the batteries. From there, holding down any numerical key for 10 seconds would drain the remaining charge from the device. After that, we would recconnect the batteries and within a three second window, hold the A button until 6 beeps emit from the device [12]. Now, the lock would be programmable for a new combination to be implemented. Considering the erosion on the existing keys, we decided this to be insignificant

for this scenario. If our attempt at penetrating the lock via keypad was unsuccessful, our client had us conduct research on a potential alternative method to gain access using manual key entry via a Lishi Tool.

In order to understand how to utilize this pen testing tool, we had to identify what exactly this device is. Lishi tools is a chinese locksmith tool company that provides a variety of locking picking tools. One example of a tool they provide is the Original Lishi Anti Glare 2-in-1 Pick & Decoder Padlock AM5 as seen in fig 17.

Fig. 17, Lishi Tool utilized to pick locks while measuring pin length [13]

This tool allows the user to pick a lock, while measuring the length of each pin in parallel. This provides insight into the pin sizes, potentially leading to creating a copy of the key. Utilizing the tool is relatively straight forward. Before inserting a Lishi Tool into the lock, make sure that the pick arm is down so it is not in the way when you insert it. Next, insert the tool into the lock and make sure all of the tool is inside of the keyhole. We would have to make note of where they want the tension, either clockwise or counterclockwise depending on how the lock opens. In our case, we would want the tension to be directed Counter-Clockwise. Starting from position one, apply downward force to the picking mechanism, if there is no click, move on to the next position. Repeat this for the remaining positions. Once we have reached the final position, the DL2700 has 6 pins so the 6th position, we would want to retrace back to the first

position and repeat step 3 until it's unlocked [14]. One aspect to keep in mind is this lock model utilizes a tumbler cylinder lock which can be tricky. Because of this, prior hands-on practice would be deemed necessary for maximum efficiency. Since this is theoretical, we could't directly apply this technique, but it would've worked.

Considering our success in exploiting the current lock, there are three major vulnerabilities with the current security measures in place. The keypad lock's password had clearly never been changed past the initial setup, so we were able to guess the digits used in the password. The solution to this issue is actually quite easy, all one has to do is cycling new passwords on the keypad regularly. By cycling passcodes frequently, it would become nearly impossible for us to tell what numbers were used more often than others. This is primarily a best practice, ensuring that all points of entry are secure, especially ones used as frequently as this.

The second vulnerability found is the input of the most commonly oriented passcodes. Randomness would also add a security layer to this system. The best possible route to take when inputting a new passcode is one that cannot be identified as or associated with a pattern. For example, rather than procuring a passcode similar to how books are read, implementing a combination such as 1,4,9,7,8 would've increased the amount of time taken to identify a possible password input exponentially in our pen test. This may not seem like a major difference, but swapping the last 3 positions tosses the needle even further in the haystack to do the notion of randomness, raising the probability of being caught.

The third and final vulnerability found within this lock system is the manual availability online. Having the ability to completely render the security system powerless due open source intelligence found on google is a daunting threat. We believe that withholding this information would mitigate the potential threat of resetting the entire locking system. Once you are on the

other side of the door, you obtain all the power when accessing the battery pack, figuratively and literally. Providing this documentation upon request from the lock owner should be the only way to obtain information pertaining to resetting the lock to factory settings. This ensures that once an attacker is inside, further exploitation of the system is mitigated.

E. CHALLENGE 5

Prior to getting inside the facility, our client provided intel indicating the utilization of RFID readers within the building. Prior research is vital to fully grasp how the interaction works, and possible roadblocks that may present themselves. To do so, our client provided an Arduino Uno and the RC522 RFID scanner to conduct hands-on practice learning how to read information from, copy said information, and write onto various RFID devices.

The RC522 has an operational voltage of 3.3v, which is critical when using the Arduino. Plugging the 3.3v pin into the 5v pin slot can short the device, causing the device irreversible damage. There are 6 other pins to make note of: GND, RST, SDA, MOSI, MISO, and SCK. Each have a corresponding pin slot which is provided in the program (https://github.com/miguelbalboa/rfid/blob/master/examples/RFID-Cloner/RFID-Cloner.ino) uploaded to the arduino, which will be explained in the future. The interaction between the RC522 and then RFID card/tag shown in fig. 18,

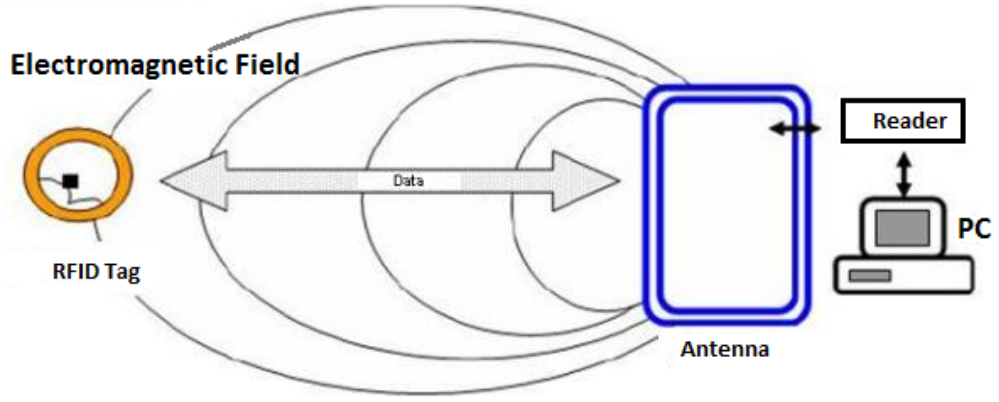

Fig. 18, Data interaction between RFID and Antenna [15]

RFID tags and keycards emit a 13.56Mhz which is read by the card reader or in our case, the RC522. In order for there to be a positive interaction, meaning data is transferred successfully, the frequency needs to be able to "activate" the ID. Think of it like the Diffie Hellman model interaction. The RFID tag is the private key and the Antenna gives out the public key. If your credentials meet that in which the antenna is looking for, it allows access. So in terms of a door, it opens the door.

The RFID tag has two main components: the antenna, for transmitting and receiving frequencies, and the RFID chip, which stores the UID and the remaining information on the card. In order to initiate this interaction, the Arduino IDE is needed to compile and upload code written in C#. This information gathered from the IDE is formatted in blocks of HEX, a total of 15 sectors. This can be seen by utilizing a GitHub repository made by miguelbalboa, which as mentioned previously allows RFID card contents to be read, copied, and written on other cards/tags. The program utilized is called RFID-Cloner. It is critical to note that none of the code used within this analysis belongs to this penetration testing group. The repository can be found online (https://github.com/miguelbalboa/rfid/tree/master/examples) [16], as well as in the appendix. Using the program is simple: plug in the pins to the corresponding pin slots, which are

provided within the program, verify, and compile. An example of the pin layout can be seen in fig. 19.

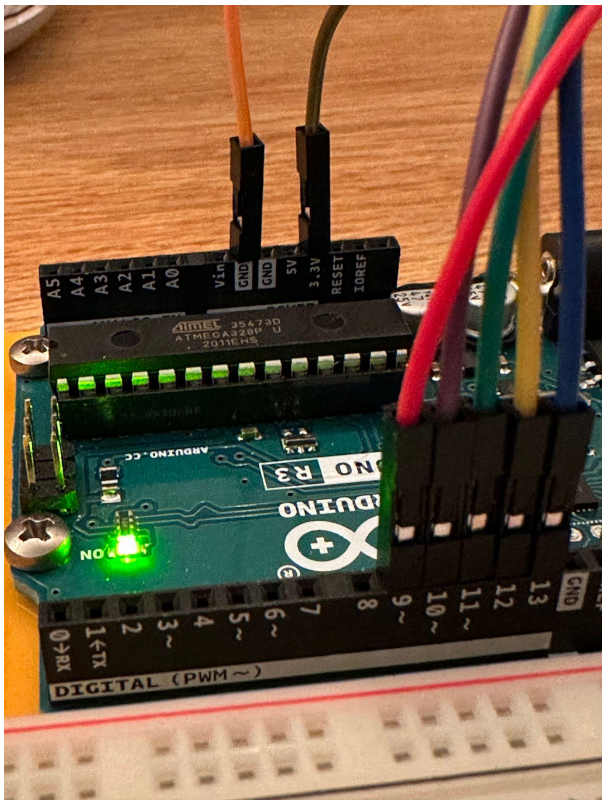

Fig. 19, Orienting pins for RC522 on the Arduino UNO

From there, open the serial monitor will present 3 options which we can choose which one to utilize:

1. Read Card
2. Write to Card
3. Copy the card

An example of utilizing the Read Card functionality is via a blue RFID tag given to us by our client. Looking at fig. 20 closely, we can identify all information given from the dumpinfo program.

```
Firmware Version: 0x88 = (clone)
Scan PICC to see UID, SAK, type, and data blocks...
Card UID: D9 A3 BE 20
Card SAK: 08
PICC type: MIFARE 1KB
Sector Block   0  1  2  3   4  5  6  7   8  9 10 11  12 13 14 15  AccessBits
  15     63   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
         62   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         61   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         60   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
  14     59   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
         58   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         57   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         56   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
  13     55   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
         54   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         53   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         52   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
  12     51   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
         50   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         49   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         48   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
  11     47   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
         46   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         45   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         44   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
  10     43   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
         42   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         41   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         40   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
   9     39   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
         38   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         37   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         36   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
   8     35   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
         34   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         33   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         32   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
   7     31   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
         30   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         29   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         28   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
   6     27   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
         26   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         25   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         24   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
   5     23   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
         22   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         21   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         20   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
   4     19   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
         18   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         17   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         16   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
   3     15   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
         14   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         13   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         12   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
   2     11   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
         10   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
          9   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
          8   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
   1      7   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
          6   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
          5   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
          4   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
   0      3   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
          2   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
          1   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
          0   D9 A3 BE 20  E4 08 04 00  62 63 64 65  66 67 68 69  [ 0 0 0 ]
```

Fig. 20, Blue RFID Tag Blank Hex Dump

There is a pattern between every single block, every 4th line is identical. The reason for this is due to the tag being blank. There is one minute difference, looking at line 0, that is where the information specific to this tag which holds the UID. This information is crucial due to

allowing an interaction with the reader. An analysis of the card is conducted and the reader identifies the UID and allows for further scanning if credentials are accepted within the company records/database(s). Tracing our steps back to the programs utilized for cloning, another is used for rewriting UIDs which is called ChangeUID. It is as simple as the previous, within the program, there is a section that allows you to change the UID of the target card as shown in figure 21. Once compiled, running the program rewrites the last line within the hex block, changing the UID.

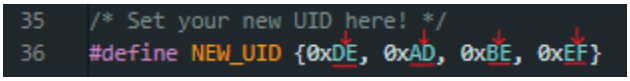

Fig. 21, Changing UID within Arduino IDE [16]

Let's apply this directly to our current objective, which is obtaining an employee ID in the target facility. Ideally, we would utilize social engineering to obtain the card from an employee and utilize the RFID-Cloner and ChangeUID program. Based on the swiftness of the process, we project to have the card in hand for less than 5 minutes. First, we read the card information, which will give us the UID. From there, taking our mock employee card and changing the UID from the default, to the newly obtained one. Next, scanning the employee card again via the Copy The Card program and then writing it to the new card. Finally, which will be the easiest portion of this manipulation, is returning the card to the rightful owner, by either coming up behind them saying you dropped this or mentioning they carelessly left it at their last location. This may sound too good to be true and that may be the case. Some keycards are encrypted, which can present a major issue due to the RC522s capabilities.

Our client also provided us with two hotel key cards to attempt a clone. The Sheraton keycard was partially encrypted while Hilton's was fully encrypted. Sheraton's keycard was

encrypted in the last 5 hex blocks, which contain the more sensitive information. The corresponding hex dump can be seen in figure 22.This gives insight on the amount of security this hotel invested in their keycards, which is noteworthy. As for the Hiltons, Small text on the bottom of the keycard is an indicator of where the card is originally from Aka, the maker of the card.

```
Card UID: 11 79 5E BF
Card SAK: 08
PICC type: MIFARE 1KB
Sector Block   0  1  2  3   4  5  6  7   8  9 10 11  12 13 14 15  AccessBits
  15     63   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
         62   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         61   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         60   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
  14     59   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
         58   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         57   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         56   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
  13     55   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
         54   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         53   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         52   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
  12     51   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
         50   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         49   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         48   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
  11     47   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
         46   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         45   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         44   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
  10     43   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
         42   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         41   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         40   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
   9     39   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
         38   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         37   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         36   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
   8     35   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
         34   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         33   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         32   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
   7     31   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
         30   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         29   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         28   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
   6     27   00 00 00 00  00 00 0F 00  FF 00 00 00  00 00 00 00  [ 0 1 1 ]
         26  MIFARE_Read() failed: A MIFARE PICC responded with NAK.
         25  MIFARE_Read() failed: Timeout in communication.
         24  MIFARE_Read() failed: Timeout in communication.
   5     23  PCD_Authenticate() failed: Timeout in communication.
   4     19  PCD_Authenticate() failed: Timeout in communication.
   3     15  PCD_Authenticate() failed: Timeout in communication.
   2     11  PCD_Authenticate() failed: Timeout in communication.
   1      7  PCD_Authenticate() failed: Timeout in communication.
   0      3  PCD_Authenticate() failed: Timeout in communication.
```

Fig. 22, Sheraton encrypted hex dump after sector 6

Hilton keycard has a fully-encrypted hex dump. Not a single block of hex was able to be seen when running read info, as seen in figure 23. The only information available was the UID, which is one important piece of the puzzle as mentioned previously. Using the RC522 has its limitations. That is where the tool studied in a previous challenge comes in, The Flipper Zero.

This can emulate scannable RFID cards, which could be applied to the two encrypted hotel keycards. The flipper zero can no longer be purchased commercially due to the magnitude of damage it can cause. In light of this, Customs have been seizing these devices to mitigate further exploitations. With encryption being an intimidating factor, there may need to be further research required regarding breaking encryption keys for keycards, or finding a tool that provides that.

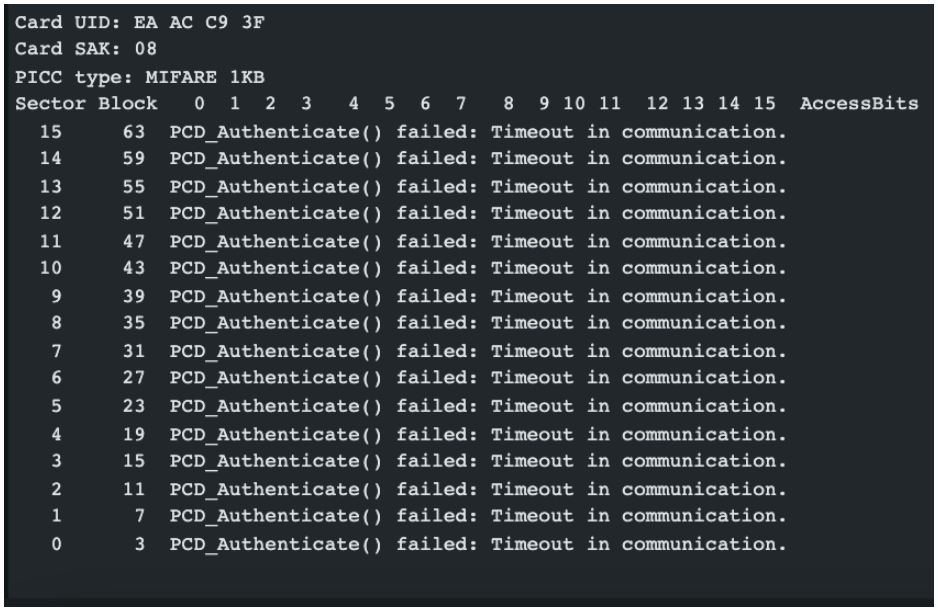

Fig. 23, Hilton key card full authentication failure

Identifying vulnerabilities for key card cloning can be difficult with the idea that the target RFID card may or may not be encrypted. In the case it is not, implementing an encryption key is vital to ensure sensitive information is not copied from an ID. Utilizing best practices similar to Hilton's keycards, would be most beneficial. Furthermore, implementing a 2FA or 3FA authentication system to mitigate potential cloning is favorable as well. Although expensive, this ensures that even if employee ID information is compromised, there still is a roadblock for perpetrators.

The next and final vulnerability found is the ability to obtain the ID via social engineering. Educating workers regarding tactics such as this would promote the overall security of the facility. Knowledge of potential attacks will prove to mitigate threats. Furthermore, storing the ID in a location on the body that is difficult to obtain may prove advantageous as well. Enforcing employees to wear clothing that has zippered pockets lessens the likelihood of the card being stolen. For an extra precaution, encasing it in an RFID shielding sleeve would eliminate the flipper zero method mentioned previously.

F. CHALLENGE 6

With the reconnaissance concluded and our skills fine tuned, we felt ready to attempt the penetration test of the facility. By using the plans discussed early from our reconnaissance, we managed to enter the building through the loading dock. Upon entry, we made our way to the lobby and located a posted corporate directory that allowed us to determine that our target, the data center, was located on the sixth floor. The directory also provided directions to a visitor center that was on the ground floor. With this knowledge, we proceeded through the lobby and made our way to the visitor center, where we decided to wait and assess the facility further.

The visitor center was chosen to be our first assessment point due to the nature of the area. People waiting within this area would arouse less suspicion because it's assumed that they are visitors meant to be there. The visit center also had open cubicles and a large waiting area that we were able to use to further assess the facility without gaining attention. After inspecting the area, we spotted an Otis elevator that could be used to access the upper floors. The elevator appeared to use an RFID scanner to authenticate users and had its button dial located in the cart. There were now a few different options we could use to bypass the elevator and gain access to the upper levels of the facility.

Our first bypass option involved utilizing the fire service mode. This mode is able to grant access to all floors within a building regardless of floor restrictions. Fire service mode was implemented into all modern elevators to give emergency response personnel the access needed to effectively respond to situations that required their attention. There are two phases associated with the fire service mode, those being phase one and phase two. Phase one fire service mode can be triggered by a smoke detector or key. This mode sounds an alarm and brings the elevator to a designated fire escape floor depending on its configuration. In order to shut off the phase one alarm, a key must be used in the phase one key hole located next to the door outside the elevator cart to reset it. To activate phase two, a key must be used in the phase two key hole located within the elevator cart to switch the mode from off to on. Once on, the operator will be able to bypass any elevator restrictions or authentication requirements needed to travel from floor to floor. To deactivate the mode, the phase two key is used to switch the dial from on to off [17]. For our purposes, the phase two fire service mode was the phase of interest.

Accessing the phase two fire service mode on an Otis elevator would require no more than a quick search on either amazon or ElevatorKeys.com (https://www.elevatorkeys.com/Otis-UTC-key) [18]. Since elevators are mass produced, most elevators will have a brand specific default access key for each of the service modes, meaning we'd likely be able to pick up the exact key needed for the elevator in the fulfillment center online. Unfortunately we didn't have the correct key on us and were unable to access the service mode key lock from within the cart without authorization to open the cart doors. Luckily though, we had another bypass option, that being the elevator's RFID scanner.

A quick glance at the RFID scanner allowed us to conclude that the lock management system was also secured within the elevator cart, preventing us from tampering with them.

Fortunately though, communication between RFID scanners and their management systems are not always encrypted. This left the door open for a man in the middle attack to occur where we could intercept the transmission of an authorized user ID and clone it for later use. Doing this would allow us to replay the copied user ID back to the scanner and trick it into granting us access to the elevator. To execute this attack, we'd need to utilize the capabilities of an ESPKey.

An ESPKey is a debugging tool and implantable logic analyzer that's designed to capture data from devices that use the Wiegand communication protocol. It can store a great deal of unique credential bitstreams, which can then be later replayed by connecting the device to a phone or a computer [19]. Essentially, it can intercept and record data that works with the Weigand protocol. It's standard for RFID scanners and systems to utilize the Wiegand protocol because of several desirable traits, so that's how we knew an ESPKey would work for this attack. We will discuss more about the Wiegand protocol in a later challenge.

After waiting a few minutes, the visitor center became less congested with people which left a small opening for us to execute the attack. We made our way to the RFID scanner and opened the wall unit using a flathead screwdriver. Upon opening the mount, we were greeted with a bundle of color coded wires. To install the ESPKey, the color coded wires had to be connected to the proper locations on the ESPKey's insulation displacement connectors. The insulation displacement connectors are connectors that allow the ESPKey to form connections with other devices through wires without stripping wire insulation [20].

We followed fig. 24, to install the ESPKey on the RFID Scanner. Essentially, the white data wire was connected to the 2nd connector from the top on the ESPKey. Next, the green wire was connected to the middle connector followed by the ground wire connecting to the connector under the green one. Lastly, the red cable was connected to the bottommost connector. Once the

ESPKey was installed, it was only a matter of waiting for an authorized worker to use the RFID scanner before we were able to proceed further in the facility.

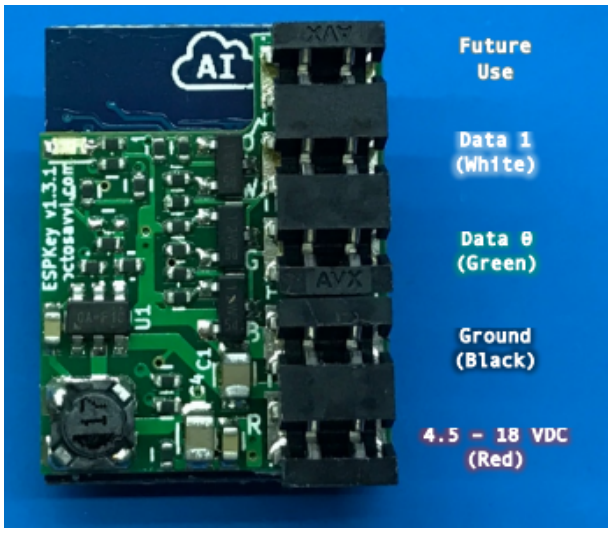

Fig. 24, ESPKey along with a readout of each insulation displacement connector on the right-hand side [20].

Upon getting this far in the penetration test, it's evident that traversing the fulfillment center was way easier than it should have been. Once we managed to enter the facility, we only had to focus on keeping a low profile, which gave us time to inspect potential roadblocks and plan ways to overcome them. This leads us to the first major vulnerability regarding security, that being unmonitored surveillance cameras.

After making our way to the loading dock and entering the fulfillment center, security should have been notified and sent to question our presence. Through proper surveillance monitoring, security would have seen us slip into the facility and could have sent a team to quickly apprehend us before we were able to cause any damage. The lack of this response indicates that the surveillance cameras are likely unmonitored and used for logging purposes only. Although a logging system is crucial and provides numerous benefits to an organization's

security, it does little to mitigate the damages of an active breach. To eliminate this vulnerability, we recommend establishing a twenty four hour video surveillance team that will actively monitor the cameras to ensure no breaches go undetected.

The next vulnerability that was noticed is the lack of security personnel at the loading dock. The success of an attack can all come down to the security of an entry point. If the entry points of a facility are fully guarded and secured then the chances of a physical breach occurring become far more unlikely by unauthorized individuals. With that in mind, it's imperative to ensure that the entry points of a facility are the most secure they can be. We recommend increasing the amount of guards stationed at all entry points. This is especially true for areas with lots of congestion such as the loading dock of the fulfillment center. A large number of guards stationed at the entry points would increase the likelihood of someone noticing an unfamiliar worker and questioning their presence in the area.

G. CHALLENGE 7

One quick resealing of an elevator panel later, we left the area to kill some time. Not knowing when anyone will use the elevator next, we decided to wait until nighttime when everyone had left to go home. While we were waiting, we noticed one of the janitors leave their keyring on a nearby table as he left the area, potentially to use the bathroom. We quickly took a photo and got to work on duplicating the keys, as it would likely be very important later on. For us to duplicate the keys using a photo, we first need to figure out what the bitting code of the keys are.

Fig. 25, A photo of three Kwikset keys on a keyring.

The bitting code on a key is a set of instructions for a locksmith to actually cut a key. However, if one knows the bitting code of a pre-made key, then they can easily duplicate it if they have the tools for it. The first step to figuring out what the bitting code of the keys in our picture are is to determine what type of keys they are. Looking at these keys we can identify them as Kwikset keys. Kwikset are the only type of keys that use a hexagonal shape as their key heads (as seen in fig. 26) and are also one of the most common types of keys. Some Kwikset keys have the 3 holes in the head, however not all of them do, such as with the case of the janitorial keys.

Fig. 26, A reference of each key type and their appearance [21].

It is also extremely common for Kwikset keys to use a 5-pin system, meaning each key would have 5 bitting codes to make the key unique. Looking at the keys in the picture we can see that there are 5 different pins in each key, further confirming that this is a Kwikset key. Now that we know what type of keys they are, we can get to work on discovering their bitting codes. There are special tools used to capture the bitting codes of different types of keys that could be used in this situation to help us make sure we get the codes correct. In this case we could use a key gauge to quickly confirm the bitting codes if we had enough time with the keys. Each different

kind of key has a different measurement for their pins, so we would need to be sure we had the right kind of key. If we had the actual set of keys, we could run each of the pins through this gauge, like the one in fig. 27, to gain an exact bitting code for all of the keys. However, we wouldn't want to get caught during this process, so our methods of finding the bitting codes have decreased dramatically.

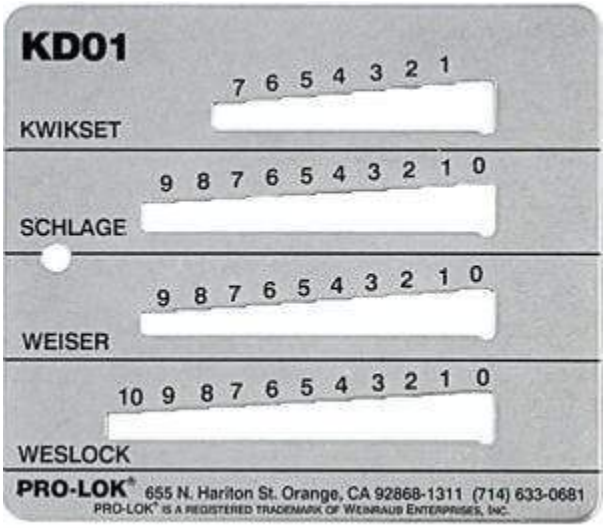

Fig. 27, A key gauge for Kwikset, Schlage, Weiser, and Weslock keys [22].

There are fortunately other ways to discover the bitting code of a key. For us, there are two possible methods we could utilize while in the field. The first is through any document processing application like Microsoft Word or Google Docs. With the help of a key decoder found on github (https://github.com/deviantollam/Key-and-Pin-Decoding) [23], we can upload a photo of a key gauge and our pictures of the key ring to the document. Next, we can set the photo of the key gauge to overlay on all other text, so it looks like the key gauge is on top of our picture. Once the key gauge is over our picture, we can scale and rotate the image such that the black bars on the top and bottom of the key gauge line up with the top and bottom of the key

blade. After we have properly aligned the key gauge over our picture, we simply need to read the code [24].

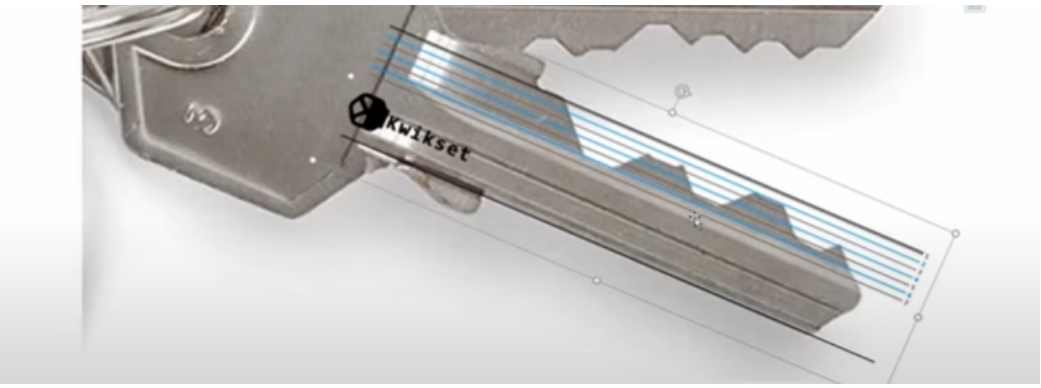

Fig. 28, The online Kwikset key decoder overlayed on the bottom most key [24].

To properly read the code, we read the key gauge numbers on each flat part of the key from the head of the key blade all the way to the tip. Now, if we were to use this method, we can see that the bitting codes of our keys are (top to bottom): 4-3-4-2-4, 3-2-5-4-3, and 6-3-5-2-5 [24].

This is one possible method to determine the bitting codes of the keys we took a photo of, and it was also not the method we used. The method we used was to simply eyeball it based on the scale of the photo and the key gauge we had. When using a key gauge, one simply has to place the key pin they want measured inside the gauge facing up and then slide the key down until it can no longer move any further [25]. If trained, this can become an indispensable tool for any penetration tester to have in their toolset. However, it is also significantly more prone to error, which can be costly for both time and resources if a mistake is made. After analyzing the photo in depth, we felt confident in saying that the bitting codes were as follows (top to bottom): 3-2-4-1-4, 2-1-5-3-2, and 6-2-5-1-5.

Fig. 29, A set of three Kwikset keys with numbers indicating the estimated bitting codes of each key.

Clearly there is a discrepancy between the eyeballed bitting codes and the bitting codes found in the previous method. In our case, this is fine as our key bitting code was consistently a lower number. This means that our key would be higher than the actual key, and we could later file the key down to the correct size if we needed to.

During this series of events, we noticed only one vulnerability that needed to be addressed. It was the workers' lack of following best practices. The janitor left the key ring alone as he left the area. They may have believed that they wouldn't be gone that long and thought it would be ok to leave the keyring with the rest of their gear, but that was not the case. All we needed to copy the keys was a picture of them, one that would have been significantly harder to

get had the janitor kept them on their person and out of sight. The best way to mitigate this risk is to use the same method to protect against social engineering, which is frequent training to make sure employees are following best practices.

H. CHALLENGE 8

After duplicating the key, we decided to check in on our ESPKey to see if it has captured any credentials. Upon connecting our device with the ESPKey local wifi, we discovered that a handful of people have used the elevator since installing the ESPKey. After selecting one of the captured credentials at random, we replayed it from our phone to open the door. Realizing that the captured credentials could be useful later on, we decided to clone it. For us to clone this ID card, we need the decimal value of the binary ID string. Once we obtain the binary code from our ESPKey, we can convert the code into decimal in one of two ways. The first way is to use an online binary to decimal converter such as (https://www.rapidtables.com/convert/number/base-converter.html). While this is incredibly handy, the second method can be far faster for people who are good at math. The second method is to just calculate it manually, and it's actually fairly easy to do if one understands the core concepts. The first thing to understand is that binary is base 2, which means it utilizes two numbers: 0 and 1. The same goes for decimal which is base 10, which is numbers 0 through 9. Upon looking at the binary ID string we captured, we can see that the string is **00000110011110001001100000**.

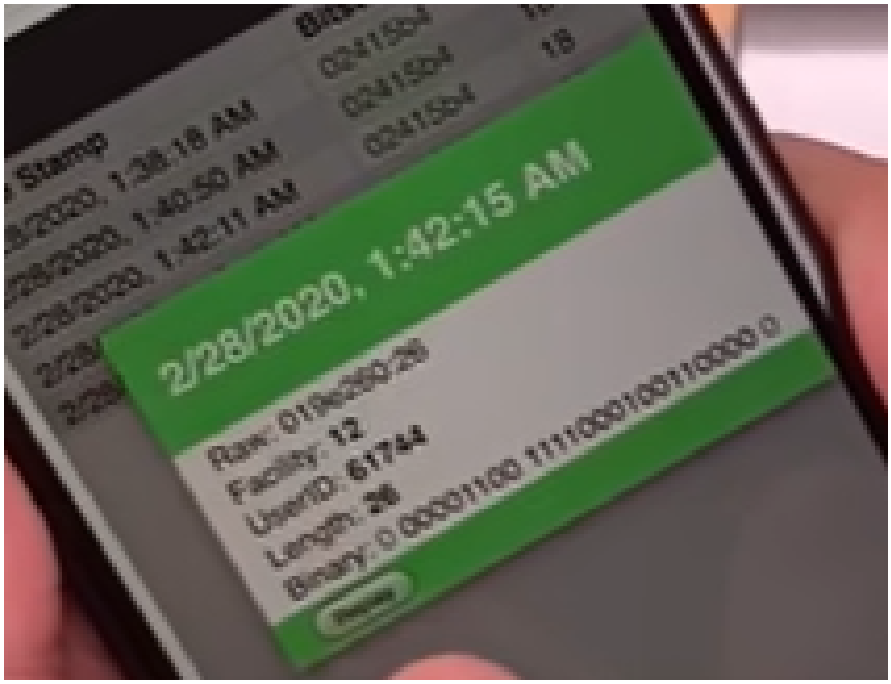

Fig. 30, Readout from the ESPKey of a randomly chosen set of credentials.

Next, to convert any base into another base, we must first convert it to base 10. Fortunately that is the base we are attempting to convert it to so we have no additional steps after applying the formula. The formula is $\Sigma(digit * base^{position})$. To explain the formula in English, it is the sum of each digit multiplied by its base to the power of its position. This means the binary string in decimal would look like $0 * 2^{25} + 0 * 2^{24} + \ldots + 0 * 2^{0} = 1696352$.

Once we arrived on the sixth floor, we were free to explore to our hearts content. As we wandered the hall unimpeded, we learned two things. One, this area was the IT department, which meant the server room was likely on this floor. Two, there were a great deal of badge readers identical to the one we just attacked, preventing us from entering most areas. For our best attempt at breaking into any of these rooms, we need to use the credentials from our ESPKey on our Proxmark. A Proxmark is a tool that can clone RFID cards very quickly based on proper given information. It can also broadcast RFID card info so it is unnecessary to clone a card for

every card found, however it can only store the most recent card info [26], [27]. Looking at the information we received on the ESPKey, we can determine a number of useful info for cloning the key. The first of which is the length. The length of 26 designates this key card to be a 26-bit card, the standard length and the only format that the Weigand protocol runs on (This format is also known as H10301) [28], [29]. The next piece of info we can obtain is the facility code. On the ESPKey, the facility code is 12, you can also calculate that by turning the first 8 bits of the binary code (after the parity bit) to decimal, which is 12 in our case. Last up is the card number. The card number is actually the User ID on the ESPKey readout, which is 61744. You can also calculate this number by taking the 16 bits after the facility code in the binary string and converting them to decimal [28].

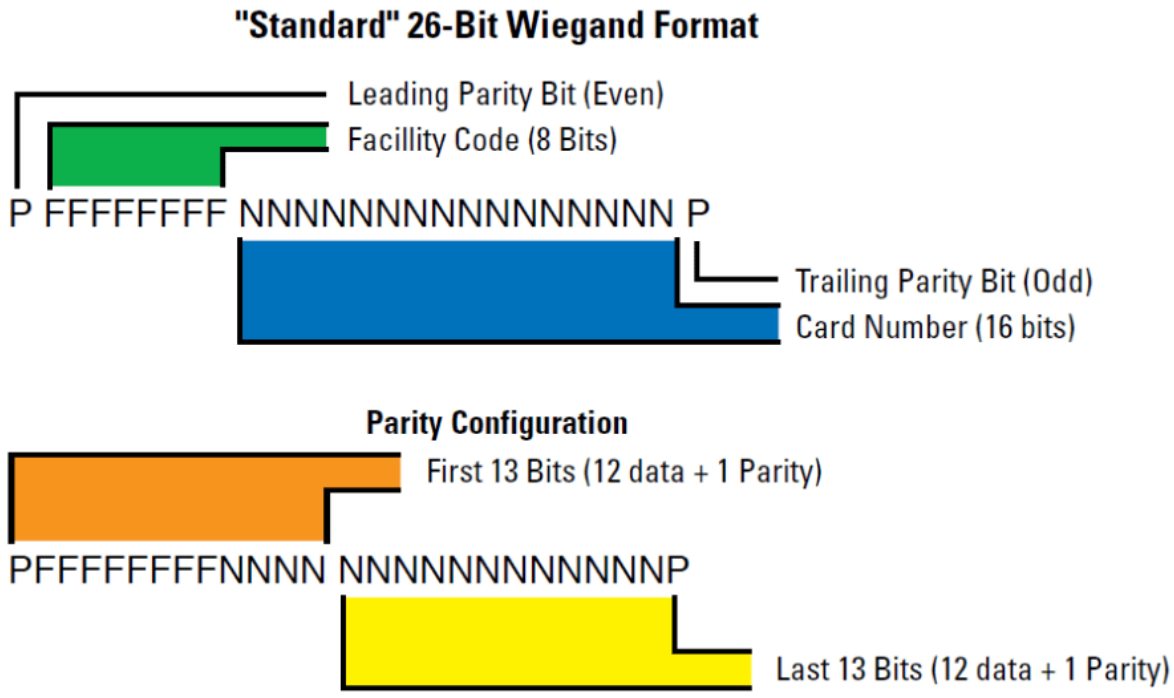

Fig. 31, Diagram of the 26-Bit Wiegand Format and its parity bit configuration [28], [30], [31].

Now that we have both the facility code and the card number, we can input this information into our Proxmark to get the HID Prox ID. The HID Prox ID is actually the Tag ID

for a prox card. This Tag ID is the number required to clone a card with the Proxmark tool. It can be calculated from the Facility Code and the Card Code [26], [27]. While it is extremely uncommon, some cards do print the Facility code and Card Code on the card itself. If this was the case, all we would have to do is look at the card to receive the appropriate information for cloning it.

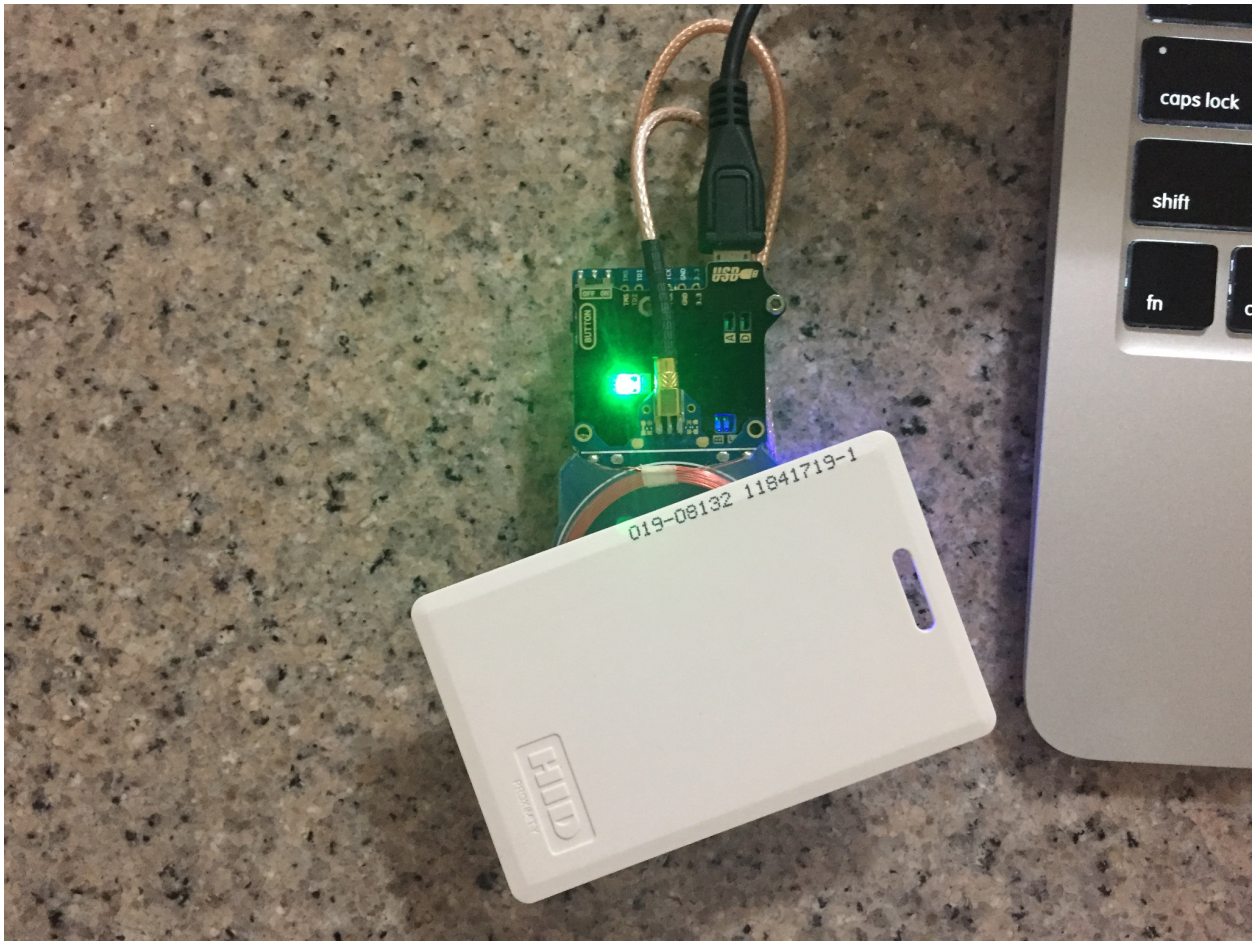

Fig. 32, An HID ProxCard with the Facility Code and Card Number printed on it resting on top of an older model Proxmark [27].

Now, in order to fully understand this system, it is worth noting what the Weigand protocol is. Wiegand refers to many different things, but the two most important things are the wire and protocol. Essentially, the wire has a special function that causes it to not break down

and could be used at a distance for sensors. The wires can be used at a distance for sensors because when they are brought near a magnetic field, the wires will switch polarity [20], [30], [31]. This is referred to as the Wiegand effect. Eventually, people discovered that the Wiegand effect can be measured and stored in binary form. A device designed to read in this data can then be used to scan the data against a database to discover if the cardholder is allowed access to wherever they are headed. Throughout all of this, the protocol itself is actually just the complete use of this wire technology in the real world. Everything from the wire to the cards and readers using the wires, it's essentially the "code" that is used alongside the physical devices for access control systems [20], [30], [31].

The primary vulnerability in this stage of our penetration test is the lack of security. As mentioned before, the lack of security in the building allowed us to move around freely on the sixth floor without worry. The solution to this would be to post more security guards, have them keep watch of various points-of-interest(POIs), and to have a security guard watching the camera feed. First, our main concern so far with this penetration test was not raising suspicion with other workers. By this point in the penetration test, we hadn't encountered any security so there was no need to keep a low profile once we made it to the sixth floor. Adding more security guards throughout the facility would prevent us from moving about as freely as well as making us conscious of what tools we used and where we used them. Second, having a security guard watch over various POIs or even just patrolling the area around POIs. If there was a security guard patrolling on the sixth floor, which was the IT department, it would have made exploring the area undetected significantly more difficult. Finally, the cameras used throughout the building were most likely used for the purpose of keeping logs after a break in occurs. It is highly unlikely that there are no cameras throughout the building, and we took no precautions to be seen by cameras

once we entered the facility grounds. There are likely cameras watching over the POIs, but given the fact that no alarms were raised when we began tampering with the elevator panel, no security guards were actively watching the camera feed. If there had been one, we likely would not have been able to install our ESPKey, let alone walk unimpeded through the IT department.

I. CHALLENGE 9

After we had successfully cloned the card we were able to roam around the interior of the floor. We were able to locate what looked to be an access point that led into the raised floor, so we tried to use the card we cloned. When the credentials on the card were declined we noticed that the card reader was different from the ones we had previously seen, meaning we needed to find a card with a higher level of access. As we were trying to find a new card that could grant us access we backtracked to an administrative office nearby, and used the key we copied from the janitor to gain entry. Unfortunately for us, whoever's office this is didn't leave anything out on their desk that we can use, however, we did notice a wall safe mounted nearby. This particular safe had an electronic lock, which narrowed down potential ways to open it.

Fig. 33, The front panel of a Saflok safe that we encountered in the administrative office.

To gain access to the safe, we first examined it to identify the brand. Once identified, we conducted a search to find the factory default passwords for the specific safe brand to see if the owner exercised good security practices. For Saflok, the factory default password is “lock” twice followed by 999999. If access is granted once using this code, the ability to change the safe passcodes would be an option for us [32]. If the passcode didn't work, we would try common passcodes such as 1234, 0000, 9876, to see if the user failed to choose a secure code. Saflok safes are also compatible with RFID chips. With this in mind, we also conducted a full sweep of the room to see if the RFID chip can be found. After that proved unfruitful, we inspected the safe to see how well it's been mounted on the wall. We looked for screws that could be undone or weakened. Once we found a way to unmount the safe, an exploit called the lock bounce method can be used. The lock bounce method works on the fact that safe locks aren’t securely held in place. The movement of the whole safe can shift the lock and cause the safe to be opened without the need of a passcode. Once the safe has been unmounted from the wall, we would pick up the safe and drop it to the ground while continuously pulling at the door. Once the safe hits the ground, the lock would temporarily shift in a manner that allows the door to be open for a split second. This process was repeated until the contents of the safe were accessible [33].

If the Saflok safe operated through a mechanical lock and was rated TL-15, we would have a challenge on our hands. This safe is very different in comparison to the one in question and can be seen in fig. 34**.** For a safe to be ranked TL-15, it would have to go through a penetration evaluation to test if the safe can withstand at least 15 minutes of break-in manipulation. The safe would also need to have 1 inch steel walls and a 1.5 inch steel door [34], [35].

Fig. 34, Blue TL-15 rated dial safe [36]

This evaluation is conducted by safe and lock pick professionals to ensure the safe is held at the highest standard. These professionals are also responsible for issuing the TRTL and TXTL ratings. Safes with the TRTL rating are able to withstand everything TL-15 safes can with the addition of resistance to oxy-fuel and gas cutting techniques. Depending on the issuer of the TRTL rating, safes with the rating may also be able to resist break-in manipulation for up to 30 minutes, in which they would be classified as a TRTL-30 safe [34]. A safe with this rating would definitely prove to be a headache gaining access to. At least explosives are still an option. That's where the TXTL rated safes come to ruin our day which can be seen in fig. 35. Safes with this rating are able to withstand explosives leaving them to be the most secure safes on the market [34].

Fig. 35 TXTL rated safe that has a digital keypad similar to one in question [37]

Looking at the vulnerabilities exploited in this challenge none of them are atrocious. The safe was very secure, and did not use an easily guessable password. The safe should have been mounted better so we could not have the opportunity to test the bounce method on it. Instead, you could change this safe out for a new, more durable one. If a better safe had been in place we would not have been able to get access through the bounce method. Another possible fix is to have security guards patrolling the area. If there was a security guard they would have heard us repeatedly dropping the safe on the floor and could have stopped us.

J. CHALLENGE 10

After we had successfully opened the safe we examined the contents of the safe to see if we could find anything that would be useful. Inside the safe we found a pack of blank RFID

cards, including one that has been separated from the pack. This card looked like it could work on the unique card reader to the server room. Also, the pack of cards has the code C-M110-PCG printed on the side of the box. Once we had the card we had to figure out what kind of RFID credentials could be on there. We decided to look up the code on the side of the card, and the result we got was that the card was a MiFare Classic 1K White PVC card.The credential list used on this card is pleasantly named “MiFare Classic.” The card was made by the company NXP, the memory size of the card is 1 KB, and its operating frequency is 13.56 MHz [38]. Based on this information, we know that this particular card is a high-frequency card, typically used in NFC cards and smart cards. This matches with what we know about MIFARE cards being used as special access cards, so we can assume that the purpose of this card is to get into the server room.

When it comes to RFID cards there are a few different variations. RFID cards emit radio singles containing information that can be picked up and read by other devices. The signals that are emitted can be sent via different frequencies that affect such as the strength of the signal and the distance the information can travel. There are three passive radio frequencies that RFID cards use to communicate data. Those are Low Frequency (LF), High Frequency (HF), and Ultra-High Frequency (UHF) [39]. Low Frequency radio waves cover frequencies of 30 KHz to 300 KHz (typical LF readers operate at 125KHz). Within these frequencies a handful of protocols are executed based on the ISO standards. The specific ISO standards that are followed are ISO 14223 and ISO/IEC 18000-2. LF cards and readers would mainly be used in access control and asset tracking. The typical range in which a device is able to read information emitted from LF cards is a few centimeters or inches from the source. High Frequency waves cover frequencies of 3MHz to 30 MHz (typical HF readers operate at 13.56 MHz). HF card waves have an increased data transmission time compared to LF cards but are more susceptible to radio interference.

Like LF, HF follows a set of ISO standards, those being ISO 15693 and ISO/IEC 14443. The HF radio waves are mainly used in NFC tags, proximity technology, and smart cards. Typical range for HF emitting cards is 3 feet from any direction of the HF source. Ultra-High Frequency waves consist of waves between 300MHz and 3GHz. Due to the large radio range it covers, a larger data transmission range is supported through UHF. The range UHF can transmit data is 40 feet from the source, however, this leaves it susceptible to the most radio interference compared to the LF and HF. UHF is mainly used in television signals and voice over radio communication [39].

K. CHALLENGE 11

As we returned to the server room, we discovered that the key card, unfortunately, did not work on the server room door. This is likely due to the card not yet being formatted with the proper credentials, but regardless, we need to get into this room. Looking at the door, we noticed that we could bypass the lock mechanism using an under the door tool (UDT), but that would trigger the proximity sensor on the door, thus setting off an alarm. Continuing past this point will put us on a timer, so we tried to find a faster way into the room. This led us to finding an American 1100 series padlock on the door, something that we could bypass faster than using a UDT.

Not having a key to get in will make accessing what is behind the lock difficult. Thankfully it is possible to bypass the American Lock 1100 series using a tool called the Peterson American Padlock Bypass Tool. The Peterson tool is a simple tool that can be slipped into the keyhole on an American Padlock and used to open it. All you need to do to open the lock is enter it in the keyhole and turn it, and all of a sudden you have unlocked the lock and successfully bypassed needing a key [40]. This tool is extremely easy to use and can be bought

online (https://www.thinkpeterson.com/american-padlock-bypass-tool/). For $24 we can keep this tool in our pen testing kit and easily be able to bypass any American series 1100 lock easily. Peterson also makes other tools such as the Peterson Mini Knife which can be used to open countless more locks including some master locks, sesame locks, and presto locks. These two tools can be used to easily bypass certain locks, fully eliminating the need to waste time lockpicking or set off an alarm using a UDT [41].

Of course, some people may not have this tool in their toolkit, which means they would have to break through this lock using just regular lockpicks. This is actually a fairly difficult lock to pick but is a great milestone for people who wish to test their talents. But first, any good lockpicker must pick their tools correctly to get the job done. For this type of lock (and almost every other kind), we only need two tools to break in: a sufficient pick and a tension wrench. The pick that would work best for this type of lock is a small hook because we need a pick that is best for applying pressure to a single pin at a time [42], [43]**.** This is primarily used for tumbler locks; a good small hook that would work for this lock is the Peterson short hook (also known as the Peterson Hook 1) because it is a standard lockpick that can break into almost all kinds of tumbler locks.

Fig. 36, A Peterson Hook 1 lockpick [42].

The tension wrench to best go along with this is the “Feather-Touch” wrench because it is good for constant tension and we would most likely be skilled enough in lock picks to make up

for the down-side [43]. Once we have these two tools, we can slowly pick this lock by starting at one end and slowly move through the pins. While applying an extremely light amount of tension from the Feather-Touch wrench, we want to slowly push each pin up until we hear a single click from the pin locking in place. Afterwards, we move onto the next pin [44], [45]. Unfortunately, as simple as this sounds, it is much harder in practice. Essentially, we do this repeatedly until we have pushed every pin into place and we have successfully picked the lock.

The reason why we would utilize the bypass tool or the lockpicks over the UDT is because of what a UDT is. A UDT is a type of lock bypassing tool that allows the user to slip underneath a door and manipulates the handle from the inside to open. UDTs are made up of two parts; a steel rod that is roughly 3.5 feet long and metal cable that has a ring on the end of it for your finger, which can be seen in fig. 37. You slide the tool under the door and hook the end of the steel rod onto the door handle and then pull the steel cable to apply tension, which bends the rod. This causes the rod to flex and open the door handle [46]. This type of UDT is for a door with a round handle, not a door knob.

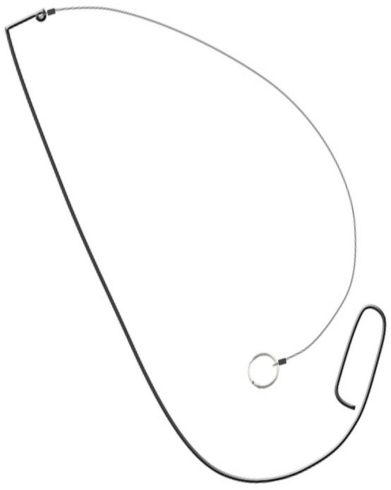

Fig. 37, Example of possible UDT utilized [46].

There are many different kinds of UDTs that can be useful for a penetration tester to bring on the job. Similar to the UDT stated above is the Silent Retractable Line UDT. This UDT is more of a modification to the one above, but it operates differently enough that some people may view them as different kinds of UDTs. The difference between this UDT and the previous one is that this one has a retractable line which makes it far easier to manage while in use (Not to mention more portable) [47]. While there are many different kinds of retractable line modifications for UDTs, this one is silent, allowing for a more covert entry than others. Another kind of UDT is known as the J Tool, which is used for thumb turned locks. This type of tool specializes in slipping through the gap in double doors and turning thumb turned deadbolts [48]. Alternatively, it can be used for security grates and grilles. A different tool that does something very similar is Sparrow's DDT (Double Door Tool) [49]. This tool makes use of the crash bars that allow people to exit doors locked by electromagnetic mechanisms. Once again, it slips through the gaps in the middle of the double doors and pushes up against the crash bars, disabling the electromagnetic lock and granting us entry [50]. Those are just a few of the many different kinds of UDTs.

Once we broke into the server room, we took a picture and left a smiley face sticker to prove that we were there. While we did end up tripping the alarm, we left before the security guard could reach the room. Had we been bad actors, that amount of time is more than enough for us to launch an attack on the servers by plugging in a USB filled with malware. Now, we can finally reflect on quite a few vulnerabilities that let us achieve our goal. Despite the fact that the key cards we discovered were not working, we managed to bypass the lock to the server room in about 2 seconds. There are a few different ways to solve this, but we believe that all of them should be implemented. Firstly, the lock on the door needs to be changed. The fact that we

managed to get into the room very quickly means that the lock really is not that good of a deterrent, the alarm is. A possible lock that could be implemented would be a two person door lock. Essentially, a lock that requires two distinct, valid key cards used at the same time to enter the room, instead of one key card held by one person and a padlock. Secondly, While having an alarm is good, the fact that we had enough time to do some damage before leaving means security was too far away to deal with a break-in. Had security been posted just outside the server room, we would have been unable to even get into the room, let alone have enough time to damage the servers should we have found a way past them. Continuing on with the lack of security, we would not have been able to approach the server room if there had been a tighter security system. This includes security guards patrolling important areas and making use of the camera feeds to prevent us from moving without being detected.

IV. MIND MAPS

Throughout the course of this penetration test, we documented our findings and organized the main points relating to each part of the test into an easy to read mind map. With this mind map, you'll be able to see all the major topics involving each of the steps taken to complete our penetration test of the Amazon fulfillment center.

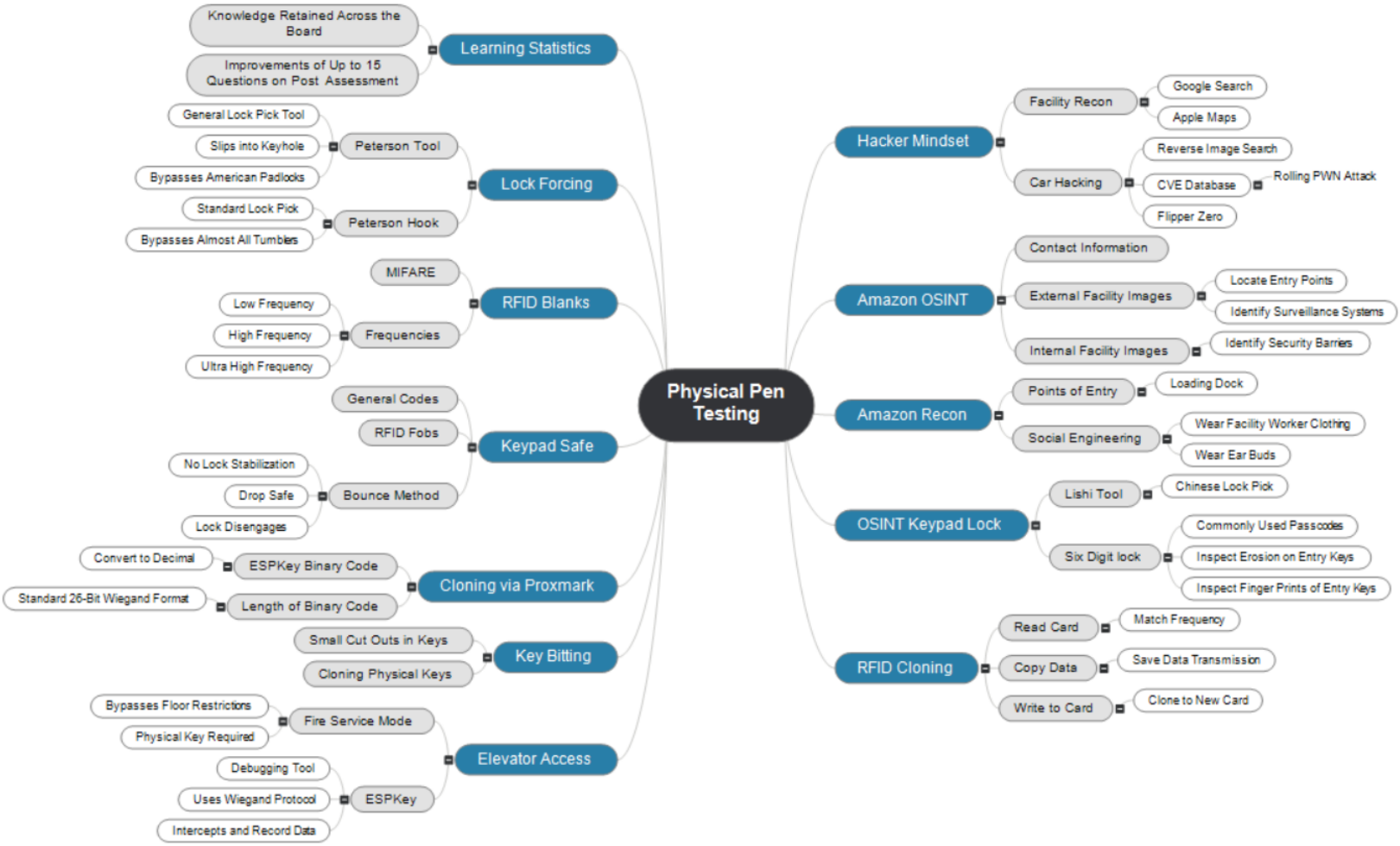

Fig. 38, A mind map showcasing the main topics of our entire project and what those topics covered.

V. ASSESSMENT COMPARISON

As stated before, our project's end goal was to see how much we could learn about physical penetration testing. Before we began our project, we took an assessment to determine how extensive our knowledge of penetration testing was. Each of the questions on the assessment was related to each of our challenges, whether it be about what a particular tool is or about how to perform ethical penetration testing. Once we had taken the assessment, we began the challenges without learning what our scores were. This was done so that we could not have

any advanced knowledge on whether anything we had felt confident about or guessed was correct. We took the exact same assessment once we had completed all of the challenges and compared our scores.

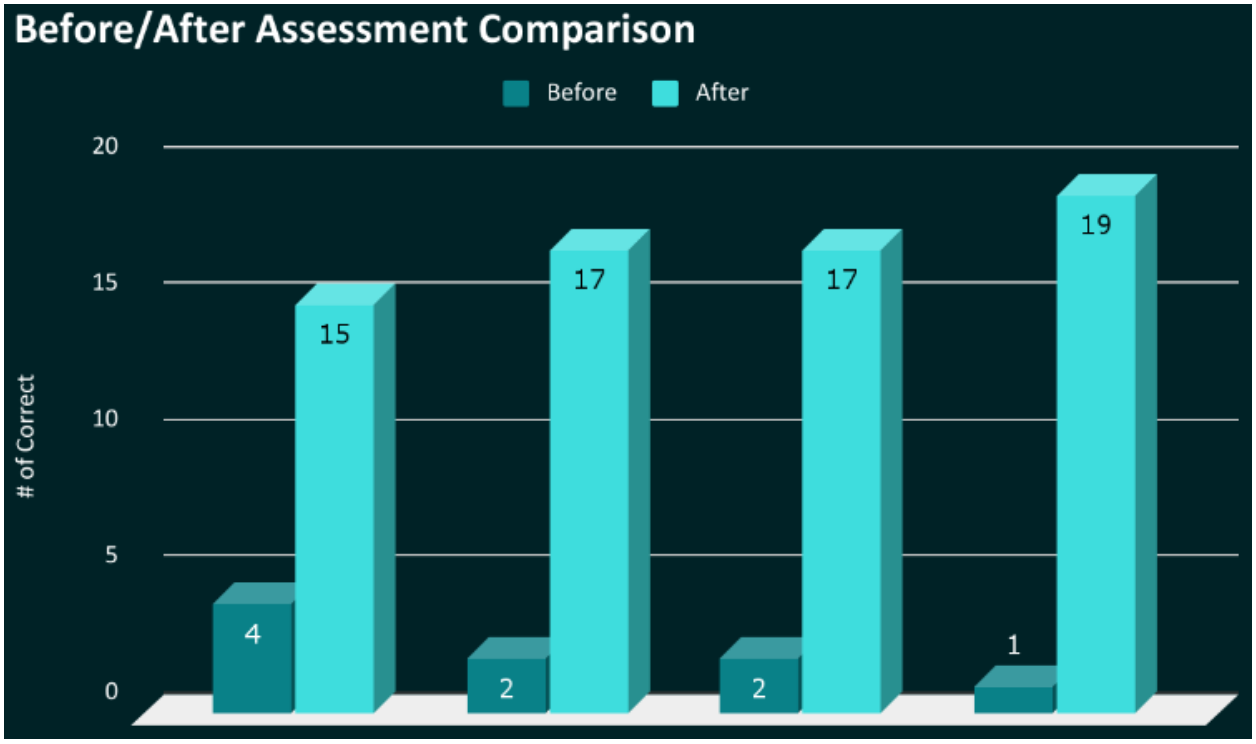

Fig. 39, Column chart comparison of the number of correct questions on the before and after assessments for each person.

In the before assessment, our highest score was 4 out of 20 questions correct while our lowest was a simple 1 out of 20. The average score was a 2.25 for the before assessment, but due to the fact that we cannot get partial credit on these questions, it rounds down to a 2 out of 20. On the other hand, the after assessment had a low of 15 out of 20 questions correct and a high of 19 out of 20 questions correct. Our average score was 17 out of 20, and as depicted by the graph, the most improvement was from the person who originally only got one question correct. The rate of increase for that person was, technically, 1800%. Moreover, our rate of increase for the group average was a 655% increase. For more information on the questions used in our

assessment, see Fig. 40 in the appendix for the questions and correct answers. While the sample size is far too low to state anything conclusively, it seems as though these challenges are capable of teaching people ethical physical penetration testing. It is, at the very least, worth looking into.

VI. CONCLUSION

With the conclusion of our physical penetration testing, our skills as ethical penetration testers has increased quite a fair amount. We began this journey with an assessment that we did horrible on and then told to complete a series of challenges. As we completed each challenge, our knowledge of the subject grew more and more. In order to not lose track of everything we learned, we decided to create a mind map so we could have all of the topics in an easy to read format. With this increased knowledge, we took the assessment again and scored significantly higher. This type of model can be used to increase knowledge on physical penetration testing.

VII. APPENDIX

Fig. 5,

https://www.google.com/maps/uv?pb=!1s0x89b5f98bfb6188bd%3A0x15732f1c10efd0a9!3m1!7e115!4shttps%3A%2F%2Flh5.googleusercontent.com%2Fp%2FAF1QipOiVvmQfZ55G5v5BAz0rhV5JakXKwW9x2pTE00a%3Dw213-h160-k-no!5samazon%20bwi4%20-%20Google%20Search!15sCgIgAQ&imagekey=!1e10!2sAF1QipOUxKwdcqyzFOWoY2iNX-fKXQGoCeFsMFBbiv6O&hl=en&sa=X&ved=2ahUKEwj8k5qD8JX6AhWzF1kFHfzqBVcQoip6BAhNEAM

Fig. 18,

https://www.semanticscholar.org/paper/Conceptual-Framework-of-Smart-Device-for-Smart-Home-Shukla-Singh/b4dde406011313cd4130130ad663770626a81a60

Fig. 21,

https://github.com/miguelbalboa/rfid/tree/master/examples/ChangeUID

Fig. 40,

Before/After Assessment for Physical Pen Testing Draft Answer Key

Q1. What is a Flipper Zero?

A Flipper Zero is a device that can be used to work with radio frequencies. It can be used to read and copy radio frequencies and can be used basically as a remote to control certain devices.

Q2. What is independent service mode on a standard elevator?

Independent service mode on an elevator makes the elevator ignore any calls to different floors and go directly to the floor requested from the inside. Independent service mode allows whoever is in the elevator to pause it in place on a given floor. Allowing things like large groups of people or large pieces of furniture/equipment to be moved without the worry of the doors being closed automatically and/or the elevator being called to another floor. To move the elevator to a different floor, the close door button needs to be held while pressing the desired floor.

Q3. What types of physical pen test information can be obtained from Google Street View?

Google street view can show you different entry points, cameras, types of doors and locks used, and more.

Q4. What is a ProxMark?

ProxMark is a tool that is used to clone RFID information and then broadcast or clone that same information onto a new card.

Q5. How many frequency bands are used for RFID readers?

RFID uses 3 different frequency bands: LF, HF, UHF.

Q6. What are the RFID bands used in commercial RFID readers?

The LF band would be used for commercial use.

Q7. In physical pen testing, what is a UDT and how is it used?

A UDT is an Under the Door Tool. A UDT is usually a piece of metal with some string attached, and maybe some tape. It is used by slipping the tool under the door and catching it onto the doorknob on the other side. Once caught, pull the string down to turn the doorknob and open the door.

Q8. What is an ESPkey?

An ESPkey is a tool you can implant into certain places that can interact with any device using the Wiegand protocol. We mainly used it for stealing credentials.

Q9. What is an insulation displacement connector?

Insulation Displacement Connectors are used to connect different types of wires together.

Q10. What is key bitting?

Key bitting refers to the cut on the key on physical keys. Depending on the type of lock and key manufacturer there will be different codes. The lower the number the higher the cut, the higher the number the deeper the cut. Kwikset, the kind we worked with, scaled from 1-6 and used 5 codes per key.

Q11. What is a Lishi tool?

A Lishi tool comes from a Chinese locksmith tool company and can be used to pick certain kinds of locks. The one we used in our pen test allowed us to pick a padlock, while measuring the length of each pin so we can make a copy of the key in the future.

Q12. What is MiFare?

MiFare is a type of RFID credential card. These differ by using different kinds of MiFare, however the one we saw in our challenge was MiFare Classic.

Q13. What does a TL-15 rating on a safe mean?

TL-15 rating on a safe means that it can withstand at least 15 minutes of someone trying to break in.

Q14. How can an Arduino be used to pen test a smart card access system?

You can plug an Arduino into different smart card access systems and upload certain code to it to pen test the access system.

Q15. What is security hygiene?

Security Hygiene is practices performed on a regular basis by a company to ensure that their security measures are up to date and still properly working.

Q16. What is the definition of ethical pen testing?

When a third-party organization gets ***advance written consent*** for them to try and gain unauthorized access to a system with the goal of discovering ways to make said system more secure.

Q17. What is pretexting, and how does it relate to Occam's Razor?

Pretexting is a form of social engineering where an attacker can gain information about a certain topic through taking advantage of someone. It relates to Occam's Razor because through pretexting you can eliminate unnecessary information and get to useful information faster.

Q18. What is the Weigand protocol ?

The Weigand protocol is a way of wiring card readers to ensure that the card is read a specific way. It manipulates the behavior of magnetic fields based on how the card reader is wired.

Q19. How can a reverse image search be used in an ethical physical pen test?

Reverse image searching for certain photos will yield results that can either show us the origin of something we are looking for or even similar images that could be useful. If we had a photo of the inside of the Amazon warehouse we could maybe find more similar images that could be useful.

Q20. How can you mitigate a MITM attack against an RFID keypad reader?

The best approach is encrypting the data on the wire coming from the keypad.

VIII. WORKS CITED

[1] "CVE List." CVE - MITRE. https://cve.mitre.org/. (accessed Dec. 4th, 2022).

[2] "Rolling PWN Attack." Github. https://rollingpwn.github.io/rolling-pwn/. (accessed Dec. 4th, 2022).

[3] "Flipper Zero - Portable Multi-tool Device for Geeks." Flipper Zero. https://flipperzero.one/. (accessed Dec. 4th, 2022).

[4] "BWI4 - Amazon Fulfillment Center." Google Maps. https://www.google.com/maps/uv?pb=!1s0x89b5f98bfb6188bd%3A0x15732f1c10efd0a9!3m1!7e115!4shttps%3A%2F%2Flh5.googleusercontent.com%2Fp%2FAF1QipOiVvmQfZ55G5v5BAz0rhV5JakXKwW9x2pTE00a%3Dw213-h160-k-no!5samazon%20bwi4%20-%20Google%20Search!15sCgIgAQ&imagekey=!1e10!2sAF1QipOiVvmQfZ55G5v5BAz0rhV5JakXKwW9x2pTE00a&hl=en&sa=X&ved=2ahUKEwj8k5qD8JX6AhWzF1kFHfzqBVcQoip6BAhNEAM. (accessed Dec. 4th, 2022).

[5] "Sanctions List Search." OFAC Sanction Search. https://sanctionssearch.ofac.treas.gov/Details.aspx?id=30946. (accessed Dec. 4th, 2022).

[6] "Specially Designated Nationals And Blocked Persons List (SDN) Human Readable Lists." U.S. Department of the Treasury. https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists. (accessed Dec. 4th, 2022).

[7] FCC. 117th Congress, 2nd session (2022, Nov. 4). *DOC-389524A1, FCC Bans Equipment Authorizations For Chinese Telecommunications And Video Surveillance Equipment Deemed To Pose A Threat To National Security.* [Online] Available:

https://www.fcc.gov/document/fcc-bans-authorizations-devices-pose-national-security-threat

[8] C. Page. "US Government bans Huawei, ZTE and Hikvision tech over 'unacceptable' spying fears." Tech Crunch. https://techcrunch.com/2022/11/28/fcc-huawei-zte-hikvision-hytera-dahua-ban/. (accessed Dec. 4th, 2022).

[9] "Amazon Distribution Center - 281 Woodbine Rd, Clear Brook, VA, 22624." Businessyab. https://www.businessyab.com/explore/united_states/virginia/frederick_county/stonewall/clear_brook/woodbine_road/281/amazon-distribution-center.html. (accessed Dec. 4th, 2022).

[10] Linear, Carlsbad, CA, USA. *Telephone Entry System User Instructions*. Accessed: Dec. 4th, 2022. [Online]. Available: https://linear-solutions.com/wp-content/uploads/AE-100_user.pdf

[11] Linear, Carlsbad, CA, USA. *AE-100 Commercial Telephone Entry System Installation and Programming Instructions*. Accessed: Dec. 4th, 2022. [Online]. Available: https://linear-solutions.com/wp-content/uploads/AE-100.pdf

[12] Alarm Lock, Amityville, NY, USA. *Trilogy T2 Programming Instructions For DL2700 Mortise, Cylindrical & Exit Trim Locks.* Accessed: Dec. 4th, 2022. [Online]. Available: https://rapidlockanddoor.com/wp-content/uploads/2019/07/DL2700.pdf

[13] “Original Lishi Anti Glare 2-in-1 Pick & Decoder Padlock AM5.” Locksmith Keyless. https://www.locksmithkeyless.com/products/original-lishi-anti-glare-2-in-1-pick-decoder-padlock-am5-1?currency=USD&variant=40614917308585&utm_medium=cpc&utm_source=google&utm_campaign=Google%20Shopping&gclid=CjwKCAiAp7GcBhA0EiwA9U0mthxwlf1_zjwNkH-VXiahk8J3Rpb54CGu2dG0TSSZTq5LFMH5w4TU2RoCecEQAvD_BwE. (accessed Dec. 4th, 2022).

[14] “Using the Original LishiKW-1 2-in-1 Pick.” Original Lishi Tools. http://www.originallishi.com/using-the-original-lishi-kw-1-2-in-1-pick/. (accessed Dec. 4th, 2022).

[15] V. K. Shukla and B. Singh, "Conceptual Framework of Smart Device for Smart Home Management Based on RFID and IoT," 2019 Amity International Conference on Artificial Intelligence (AICAI), 2019, pp. 787-791, doi: 10.1109/AICAI.2019.8701301.

[16] miguelbalboa. “rfid.” Github. https://github.com/miguelbalboa/rfid/tree/master/examples. (accessed Dec. 5th, 2022).

[17] “Fire service mode (EFS).” Elevator Wiki | Fandom. https://elevation.fandom.com/wiki/Fire_service_mode_(EFS). (accessed Dec. 5th, 2022).

[18] “Otis UTC key.” ElevatorKeys. https://www.elevatorkeys.com/Otis-UTC-key (accessed Dec. 5th, 2022).

[19] “ESPKey Wiegand Interception Tool.” RedTeamTools. https://www.redteamtools.com/espkey. (accessed Dec. 5th, 2022).

[20] Octosavvi. *ESPKey Wiegand Interception Tool*, 1st edition. Accessed: Dec. 5th, 2022. [Online]. Available: https://www.redteamtools.com/content/ESPKey%20Tool%20Manual%20v1.0.0.pdf

[21] "Key Reference." Dave's Lock & Key - Bozeman. http://www.daveslockandkey.com/keyreference. (accessed Dec. 5th, 2022).

[22] "Key Gauge for Kwikset, Schlage, Weiser, Weslock." CLK Supplies. https://www.clksupplies.com/products/key-gauge-for-kwikset-schlage-weiser-weslock. (accessed Dec. 5th, 2022).

[23] deviantollam. "Key-and-Pin-Decoding." Github. https://github.com/deviantollam/Key-and-Pin-Decoding. (accessed Dec. 5th, 2022).

[24] TheNotSoCivilEngr. "[56] Decode Keys with Microsoft Word." Youtube. https://youtu.be/vxJ3Kovz-bo. (accessed Dec. 5th, 2022).

[25] HelpfulLockPicker. "[163] DIY: How To Decode A Key To A Lock By Sight In Minutes! (Basic DIY Locksmithing)." Youtube. https://youtu.be/AAkJzhfj_I8. (accessed Dec. 5th, 2022).

[26] Hacker Warehouse. "Cloning and Emulating RFID cards with Proxmark3." Youtube. https://youtu.be/W22juSqhJSA. (accessed Dec. 5th, 2022).

[27] K. Chung. "RFID Hacking with the Proxmark 3." Kevin Chung Blog. https://blog.kchung.co/rfid-hacking-with-the-proxmark-3/. (accessed Dec. 5th, 2022).

[28] B. Mehl. “How to Calculate Facility Code using Card Bit Calculators.” Getkisi. https://www.getkisi.com/blog/how-to-calculate-facility-code-using-card-bit-calculators. (accessed Dec. 5th, 2022).

[29] “26 Bit Card Format.” Open Options. https://www.ooaccess.com/kb/26-bit/. (accessed Dec 5th. 2022).

[30] A. Leavitt. “Everything You Need To Know About The Wiegand Protocol?” Safe and Sound Security. https://getsafeandsound.com/2018/09/wiegand-protocol/. (accessed Dec. 5th, 2022).

[31] “Wiegand Protocol, Reader, Card and Interface Explained.” Stebilex. https://stebilex.com/everything-you-need-to-know-about-wiegand-in-access-control/. (accessed Dec. 5th, 2022).

[32] LockPickingLawyer. “[603] Saflok Hotel Safe Override.” Youtube. https://youtu.be/De0D7otNxME. (accessed Dec. 5th, 2022).

[33] A. Dachis. “Crack Almost Any Electronic Safe with the Bounce Technique.” Lifehacker. https://lifehacker.com/crack-almost-any-electronic-safe-with-the-bounce-techni-5853610. (accessed Dec.5th, 2022).

[34] “Vault & Safe Classifications.” Vault and Safe. https://www.vaultandsafe.com/vault-safe-classifications/. (accessed Dec 5th. 2022).

[35] “What Do Gun Safe Ratings Mean? How Do You Choose a Gun Safe?” Liberty Safe. https://www.libertysafe.com/blogs/the-vault/gun-safe-ratings-explained. (accessed Dec. 5th, 2022).

[36] "Hollon PM-1814C TL-15 Burglary 2 Hour Fire Safe." Safe and Vault Store. https://www.safeandvaultstore.com/products/hollon-pm-1814c-tl-15-burglary-2-hour-fire-safe. (accessed Dec. 5th, 2022).

[37] "Mesa Safe Burglary & Fire Safe Cabinet, Digital Lock, 2 Hour Fire Rating, 22'W x 22'D x 40'H." Global Industrial. https://www.globalindustrial.com/p/burglary-file-safe-cabinet-2-hr-factory-fire-rating-digital-lock-22w-x-22d-x-40h?infoParam.campaignId=T9F&gclid=Cj0KCQiAyracBhDoARIsACGFcS5SEeGOiHkNP-iq6GbgoY9gz8QiQpaSZ3dLd-rJFSrBh03ugeah2-8aAks7EALw_wcB. (accessed Dec. 5th, 2022).

[38] "MIFARE® Classic 1K (MF1ICS50) White PVC Card." Universal Smart Cards. https://www.usmartcards.com/mifarer-classic-1k-mf1ics50-white-pvc-card.html. (accessed Dec. 5th, 2022).

[39] "Difference Between LF HF and UHF RFID." RFID Card. https://www.rfidcard.com/difference-between-lf-hf-and-uhf-rfid/#:~:text=The%20High-frequency%20band%20consists%20of%20frequencies%20from%203,a%20plethora%20of%20applications%20running%20on%20High-frequency%20applications. (accessed Dec. 5th, 2022).

[40] The Lock Picking Lebowski. "(24) American Lock 1100 padlock bypass addendum." Youtube. https://youtu.be/Y8WZsc0dUdw. (accessed Dec. 5th, 2022).

[41] "Peterson Knife Tool." LockpickWorld. https://www.lockpickworld.com/products/peterson-3-piece-mini-knife-bypass-tool-set. (accessed Dec. 5th, 2022).

[42] "Types of Lock Picks: The Overkill Guide." Art of LockPicking. https://www.art-of-lockpicking.com/types-of-lock-picks-guide/. (accessed Dec. 5th, 2022).

[43] "Lock Pick Types." ITS Tactical. https://www.itstactical.com/skillcom/lock-picking/lock-pick-types/. (accessed Dec. 5th, 2022).

[44] HelpfulLockPicker. "Red American Lock 1100 Series Picked with some Tips and Tricks Along The Way!" Youtube. https://youtu.be/ENjPw-oH2N8. (accessed Dec. 5th, 2022).

[45] allanvrc. "Any Tips for picking American lock 1100?" Reddit. https://www.reddit.com/r/lockpicking/comments/cetbrk/comment/eu5178b/?utm_source=share&utm_medium=web2x&context=3. (accessed Dec. 5th, 2022).

[46] "Under The Door Tool (UTDT)." Lock Pick Tools. https://lockpicktools.com/under-the-door-tool/. (accessed Dec. 5th, 2022).

[47] "Silent Retract Line for Under Door Tools." RedTeamTools. https://www.redteamtools.com/under-door-tool-silent-retract-line. (accessed Dec. 5th, 2022).

[48] "J Tool for Thumb Turn Locks." RedTeamTools. https://www.redteamtools.com/J-Tool-for-Thumb-Turn-Locks. (accessed Dec. 5th, 2022).

[49] "DDT (Double Door Tool)." Sparrows Lock Picks. https://www.sparrowslockpicks.com/products/ddt?pr_prod_strat=copurchase&pr_rec_id=fa051e378&pr_rec_pid=6802997117009&pr_ref_pid=6786831089745&pr_seq=uniform. (accessed Dec. 5th, 2022).

[50] BosnianBill. “(990) Sparrows Double Door Tool (DDT) Bypass.” Youtube. https://youtu.be/GLMyIvgG3zs. (accessed Dec. 5th, 2022).