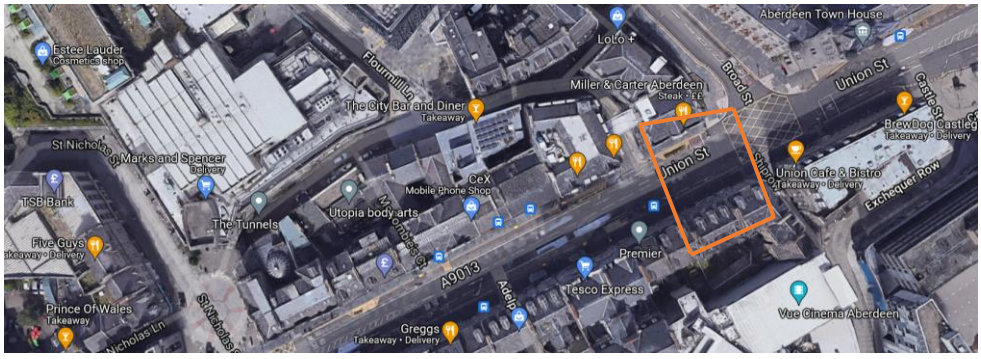
CM3109 Coursework Document **Rory Cameron 2002511**

The purpose of this report is to access and evaluate the security of a future Tuscan/Fusion bar opening in Aberdeen in 2022, Cantina Lorenzo (CL). As a freelance security consultant commissioned by CL, this report will decide on a potential bar/restaurant to be bought out by investors, which fits CL's basic selection criteria. As well as this, physical access points to the building will be assessed, to see if they can be exploited to provide access to the restaurants back offices, in the hopes of retrieving physical access to the restaurant's fileserver. 3 attack scenarios on how to retrieve this fileserver will be thoroughly walked through, with countermeasures on how to prevent these attacks given.

The building/business chosen to be bought and taken over by CL is The Esslemont Bar & Restaurant, located at 38 Union Street, Aberdeen, AB10 1BD **(1)**.

Figure 1: An Image of the front of The Esslemont Bar & Restaurant

Figure 2: A satellite view of 38 Union Street, Highlighted in Orange Square



Located at the eastern side of union street, it's in a key area for business due to many retail/hospitality businesses in proximity. This means people in this area will generally be looking to spend money, increasing the chances they find 38 union street and choose to dine there.

By using a wide range of OSNIT techniques such as company websites, google maps and social media. Information was found out about the building and the current restaurant that resides there. Full ethical and legal considerations were made when researching. Only information publicly available was obtained, with no use of invasive techniques or software. As well as this, nobody with any connections to the building/restaurant were asked for information or pressured into giving any information.

The Esslemont Bar & Restaurant is a mid to high range restaurant with the capacity to sit 112 people **(2).** They are open 11am – Midnight 7 days a week **(3**), with their busiest times being from 7pm-9pm, especially on Fridays and Saturdays **(3)**. Regarding uniform Instagram shows the waiters wear black shoes and trousers, with a white shirt with a black apron over it. Bar tenders wear the same thing, rather with a waistcoat instead of an apron **(4)**. While this information is regarding the current restaurants polices and may not fit Cantina Lorenzo's dress code, it may still be like this if the restaurant is bought and taken over.

By Using Google maps, physical access points to the building were discovered:

Figure 3: Front (Customer) Door

Figure 4: Northern back fire escape

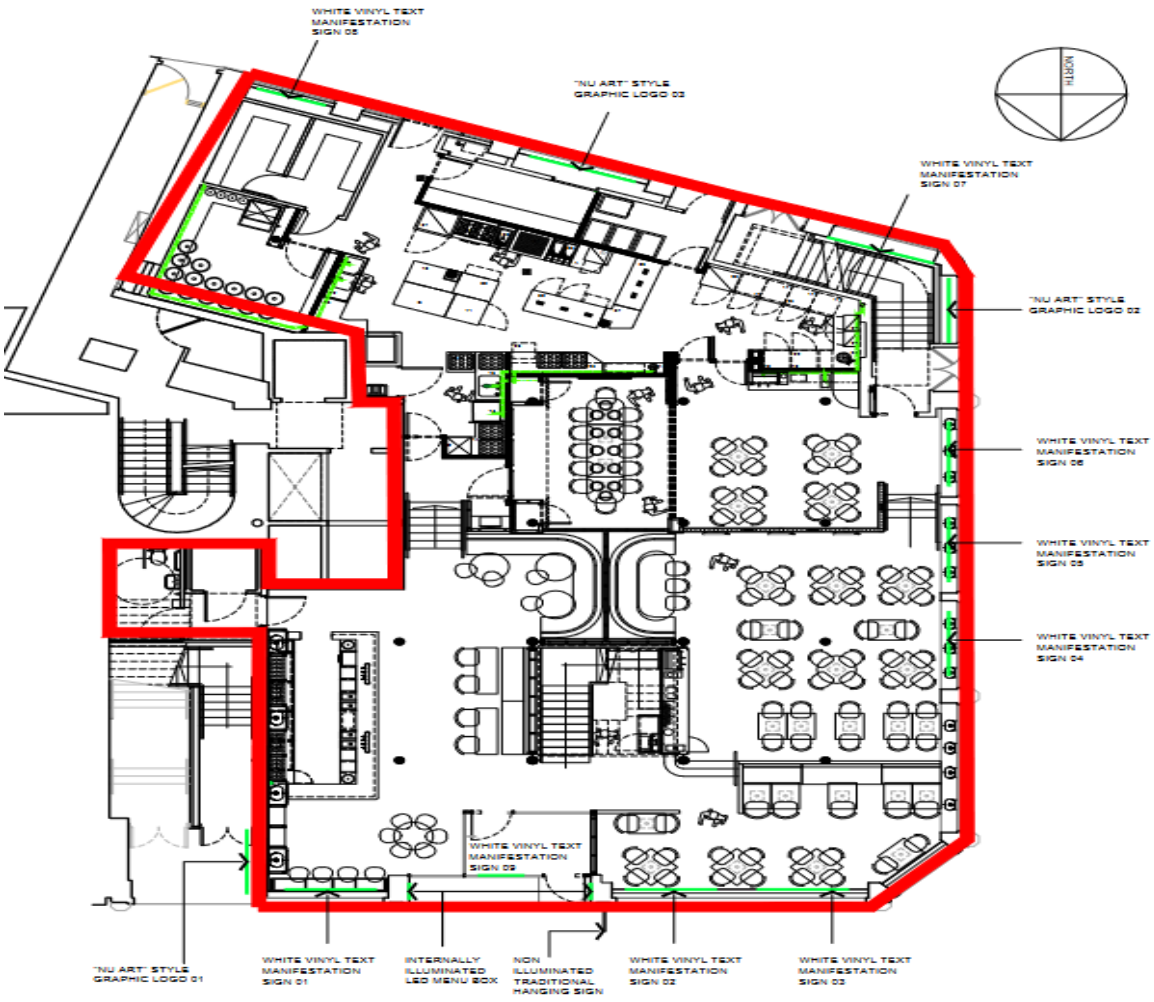
Figure 5: Eastern wall fire escape

Figure 6: Northern wall back door

We can see that two of these doors have a lock. It is unclear what type of lock is on the backfire escape, however we can see the lock on the back door. It is a CodeLocks 155 Mortice Latch, an entry level mechanical push lock for “light duty entry control” **(5)**.

Figure 7: CodeLocks 155, The type of lock on the back door

Figure 8: Floor plan of The Esslemont Bar and Restaurant



Accessing the Councils planning register, floor plans have been discovered. Several points can be made from studying these. The front entrance will constantly be watched by staff from the main front desk, located directly in front of entrance under the stairs, as well as from staff at the bar on the west side of the restaurant. Back offices are located at the end of the kitchen, this is where fileserver will be kept. To enter kitchen, a tester would either go through 2 staff doors from the customer side, or through one of the back doors outside, that lead directly to the kitchen. Finally, it appears that a blind spot exists within the building at the customer toilets, as it is behind and out of peripheral vision of bar, as well as front desk staff having obstructed vision due to tables when looking that way.

Attack Scenarios:

Scenario 1:

Overview:

This attack involves a tester having a normal dining experience within the restaurant, before heading to the toilets and switching into a waiter's uniform. The tester will enter the kitchen and walk through until at the back offices, where they will obtain access to the fileserver.

Vulnerabilities:

This attack is going to take advantage of the fact that on a weekend evening, the restaurant will be at its busiest, meaning staff members will be serving lots of customers, not having time to idle and notice an attack. This attack also takes advantage of the customer toilets that are out of view from any fixed member of staff, i.e., those at the bar or the front book in station.

Setup:

- Tester purchases et of clothes identical to waiter's uniform.
- Tester wear uniform under normal clothes.
- Tester books table for s Saturday between 7pm and 9pm.

Execution:

- Tester will enter through the front entrance, acting as a normal customer there to dine, asking for a seat close to windows (able to get out seat more discreetly as not in vision of bar staff).
- Tester has forgettable conversation/experience with the staff, in the hopes that they do not stand out to anyone, or their face is remembered.
- Tester has normal dining experience and after paying, enters customer toilets, hiding face with mask and avoiding contact with staff.
- Inside toilets, Tester takes off normal clothes, so is now wearing waiter uniform
- Take lid off top of toilet and hide other clothes inside.
- Tester waits 5-10 minutes in toilet, so staff assume they have left restaurant.

- Tester walks out of toilets, turning left and going through 2 sets of staff doors to the kitchen, with the office and fileserver location being at the back.
- If the office door is locked, social engineer staff into unlocking door, example, asking member of staff to open the door for them due to them having spilled liquid on their hand. The tester could also say they are quickly trying to get an order out but need into the office so would want someone to open the door for them quickly when they get back, or tester could exclaim they have simply forgotten password.
- Inside office, tester retrieves fileserver.
- Tester confidently walks out of building either through already open back door or one that can obviously be opened, if not, walk out through the main customer door.

Countermeasures:

Countermeasures for this scenario would be to secure the unlocked staff doors. It would be suggested that an electronic key lock would be installed on these doors, as there easy to operate and don't require a key and would stop people from just walking in. CCTV could also overlook the door, to deter people from trying to gain access, as they risk being caught and identified.

Scenario 2:

Overview:

This attack involves a tester presenting themselves working for the ISP of the restaurant. They will attempt to gain access into the building during the morning before opening hours via the back entrance, before accessing the back offices and retrieving the fileserver.

Vulnerabilities:

This attack is going to exploit the back doors of the building to get into the restaurant. The lock is a CodeLocks 155 Mortice Latch, and with research, a video bypassing the locks has been found **(6)**. Restaurants require morning deliveries of fresh food every day meaning there is a high likelihood that a back door will be open to allow these deliveries to be made, which our penetration tester could exploit to gain access without having to bypass locks.

Setup:

- Tester goes near building in advance before attack, to login to the wifi to find out the name of their ISP.
- Tester purchases high vis jacket and creates fake ID badge belonging to ISP.
- Tester must watch and understand video of lock bypass method.
- Teste watches building for several days in the morning to determine food delivery times.

Execution:

- Tester arrives at time of morning food deliveries.
- If back door is left open to allow for deliveries, enter through door as intended.
- If back door is locked, head towards door with CodeLocks lock.
- While standing up to avoid suspicion, bypass lock by following video guide.
- Once door has opened, Tester will be in kitchen, Offices will be on the right.
- If staff speak to tester, explain they work for Internet Service Provider and are resolving a WI-FI issue. If staff accepts lie use social engineering to create a sense of urgency so access is needed to office. Tester should trick staff into thinking they were already in office but left to get tools and forgot password, making staff open office.
- If office is locked, bypass the lock using same method.
- In office, Tester pretends to genuinely be trying to resolve WI-FI issue.
- Tester walks out confidently with fileserver, staff already convinced tester is there for legitimate reasons and won't assume anything suspicious.

Countermeasures:

In terms of countermeasures, It would e recommended to change locks to more heavy duty, outdoor solution, the current locks installed are mainly meant for indoor purposes, that could easily be broken by someone with intent. Secondly, there does not appear to be any CTTV watching the doors, allowing attackers to have more confidence, installing CCTV would act as a deterrent to potential attackers.

Scenario 3:

Overview:

This attack involves a penetration tester purposely setting off a fire alarm, to make there way into the back offices unnoticed amongst the confusion and panic of people trying to find fire escapes to evacuate the building.

Vulnerabilities:

During a fire alarm, it would be a mutual assumption between everyone in the building that they all want to get out safely and not see harm to themselves or others, people will not be expecting anything malicious and will not question anything as they just want to get out. There will be panic and confusion initially, leading people to make questionable decisions, so a member of the public entering a staff only area would not seem strange, as they would appear to be trying to find a fire escape. In this scenario, the general public's safety is heavily exploited. Many modern buildings doors automatically open during fire alarms, which would allow easy access into staff areas. This attack would exploit the busy periods of the restaurant, as the more people panicking and being confused, means it would be easier to slip into staff areas.

Setup:

- Dine in restaurant in advance to locate fire alarms.
- Tester must watch and understand video on lock bypass method.
- Book table on a Saturday between 7pm and 9pm (busy period).

Execution:

- Tester enters, dining as normal.
- Locate fire alarm near customer toilets, as will be in blind spot to staff.
- Pull fire alarm, creating panic and evacuation between staff and customers.
- Whilst people are evacuating, make way through staff doors to kitchen.
- Kitchen staff should have evacuated out of back doors, so path to back office should be clear.
- If lock to office has been unlocked, either because it was automatic or because staff were in a rush, proceed to enter the office.
- If office is still locked, with nobody inside the building, tester has sufficient time to bypass the lock and enter the office.
- Steal the fileserver from the office.
- Leave via the kitchens back door and walk away from building.

Countermeasures:

A countermeasure for this type of attack would be to have Double-Knock file alarms installed in the building. These fire alarms will only go into full alarm mode when two devices from the same of different zones are activated at once. This means a lone attacker would not be able to create a full evacuation as it would be seen as a false alarm.

Considerations of attacks:

While all 3 of these attacks cannot technically be considered ethical and legal, some can be considered more than others. In scenario 1 dressing up as a waiter does not have many moral implications however talking to customers while impersonating an employee would be considered fraud. Scenario 2 is slightly less ethical, breaking the outdoor lock, which is considered breaking and entering. While nobody is physically harmed the impact it has on the owner having to invest in new locks is still damaging. Scenario 3 is the least ethical. It is a very serious offence to cause public stress, especially inciting immediate danger. This scenario may lead to physical harm to people, as well as potential mental issues such as trauma and PTSD. However, the attack is not as dangerous as actually starting a fire.

Conclusion:

Out of the 5 total vulnerabilities exploited throughout these attack scenarios, 3 vulnerabilities exploited were physical: Customer toilets blind spot, Back door fire escapes used for deliveries, as well as the weak type of locks on the back door. All these

vulnerabilities can be resolved, by implementing CCTV to act as crime deterrents, as well as installing more permanent, outdoor locking systems. Staff and the public were also exploited during this report. It is suggested the restaurant have some form of procedure for everyone entering staff areas, where key card access is required. CCTV could be used to track and check what staff are doing as well as who comes in and out. Vulnerabilities of building and restaurant are not severely exploitable compared to any other Aberdeen location, this building is also in a prime location for the hospitality business, for these reasons, it is recommended that CL choose 38 Union Street as their location for business.

Appendix:

(1) https://www.tripadvisor.co.uk/Restaurant_Review-g186487-d18723364-Reviews-The_Esslemont_Bar_Restaurant-Aberdeen_Aberdeenshire_Scotland.html
(2) https://www.theesslemont.co.uk/
(3) https://www.google.com/search?q=The+Esslemont+Bar+%26+Restaurant&source=lmns&bih=567&biw=1280&client=firefox-b-d&hl=en&sa=X&ved=2ahUKEwiR9e-iqunzAhVUhHMKHTO7A0IQ_AUoAHoECAEQAA
(4) https://www.instagram.com/the_esslemont/
(5) https://doorsolutionsdirect.co.uk/index.php?route=product/product&product_id=316&language=en&currency=GBP&gclid=CjwKCAjwwsmLBhACEiwANq-tXLoHK_z667qZjEJtWvaWGzCpa_3OkjqNHatXFePmfuIxJlYB-0-ODBoCo28QAvD_BwE
(6) https://www.youtube.com/watch?v=AGEn-T1Iyr4

Figure 1:
https://www.google.com/search?q=The+Esslemont+Bar+%26+Restaurant&client=firefox-b-d&sxsrf=AOaemvIJlSA5_XpumuWldGvGsr3rCBCtmg:1635294363657&source=lnms&tbm=isch&sa=X&ved=2ahUKEwiOi5idqunzAhVDUMAKHRFdC-sQ_AUoAnoECAEQBA&biw=1280&bih=567&dpr=1.5#imgrc=Sxd1JL37KburcM

Figure 2:

https://www.google.com/maps/@57.1474961,-2.0965054,148m/data=!3m1!1e3

Figure 3,4,5,6:

https://www.google.com/maps/@57.1474971,-2.0957099,3a,60y,335.29h,83.98t/data=!3m6!1e1!3m4!1s2lmEDFejCwVmybn5E6Prtw!2e0!7i13312!8i6656

Figure 7:
https://doorsolutionsdirect.co.uk/index.php?route=product/product&product_id=316&language=en&currency=GBP&gclid=CjwKCAjwwsmLBhACEiwANq-tXLoHK_z667qZjEJtWvaWGzCpa_3OkjqNHatXFePmfuIxJlYB-0-

Figure 8:https://publicaccess.aberdeencity.gov.uk/online-applications/applicationDetails.do?activeTab=documents&keyVal=PXB2QNBZJ6300

Word Count: 2170