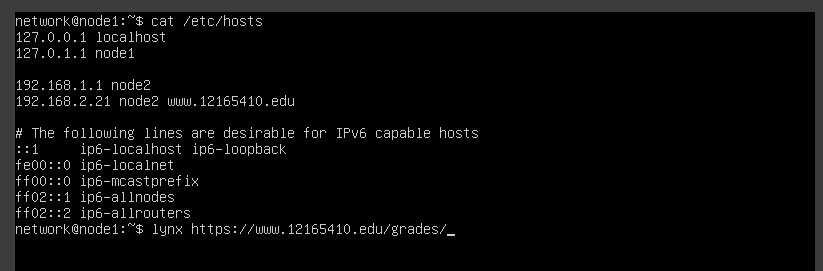
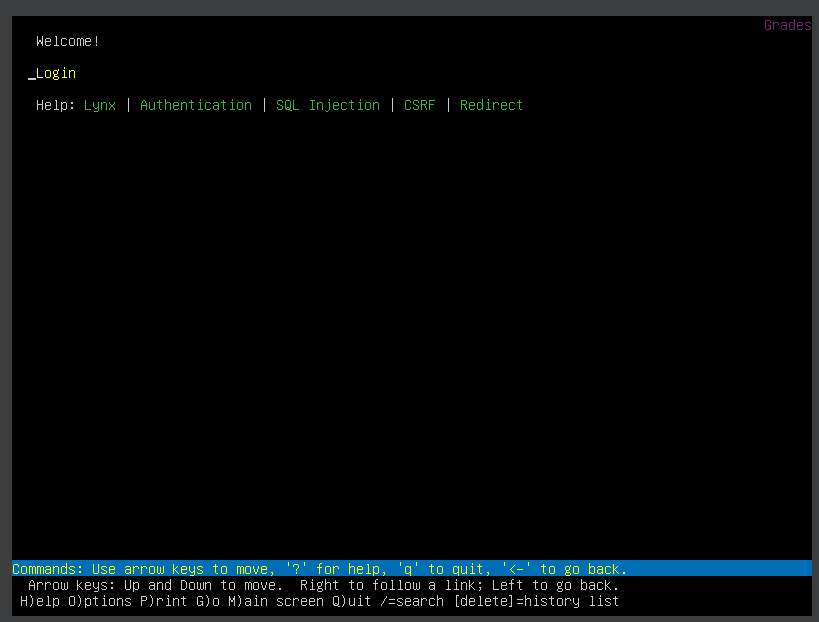
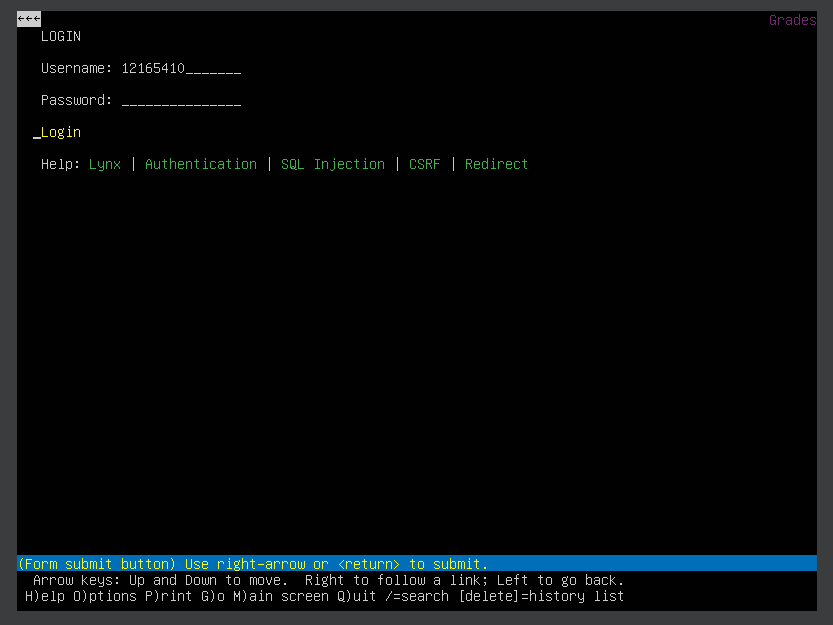
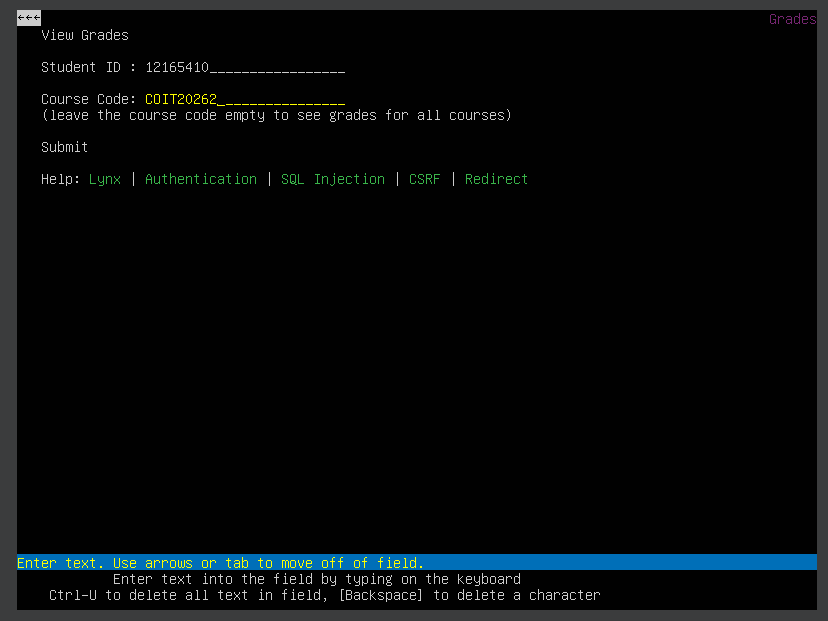
1. HTTPS and Certificates

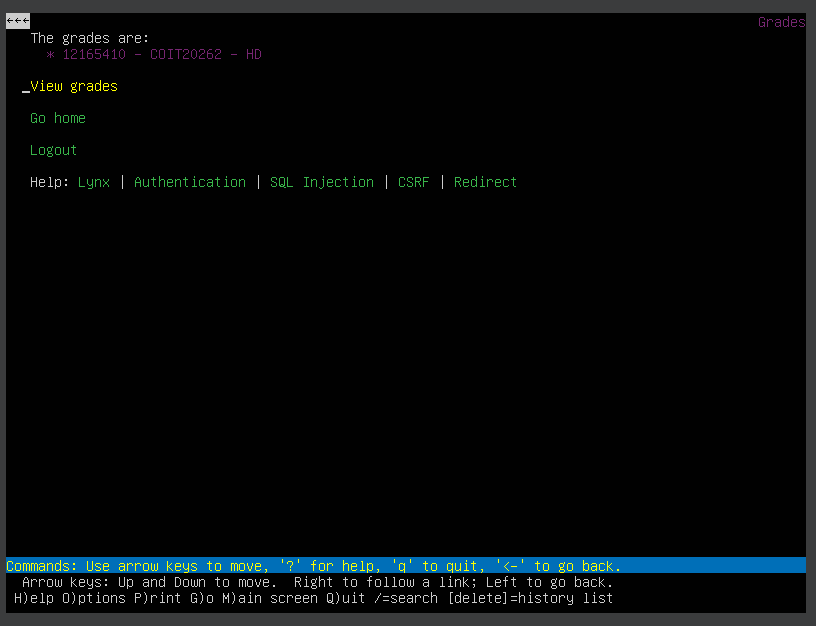
Part (a)



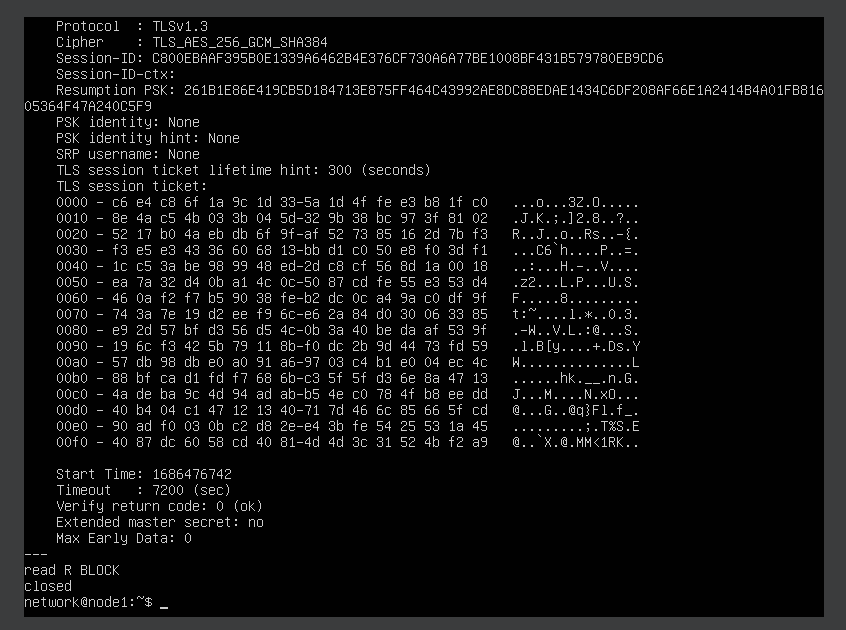






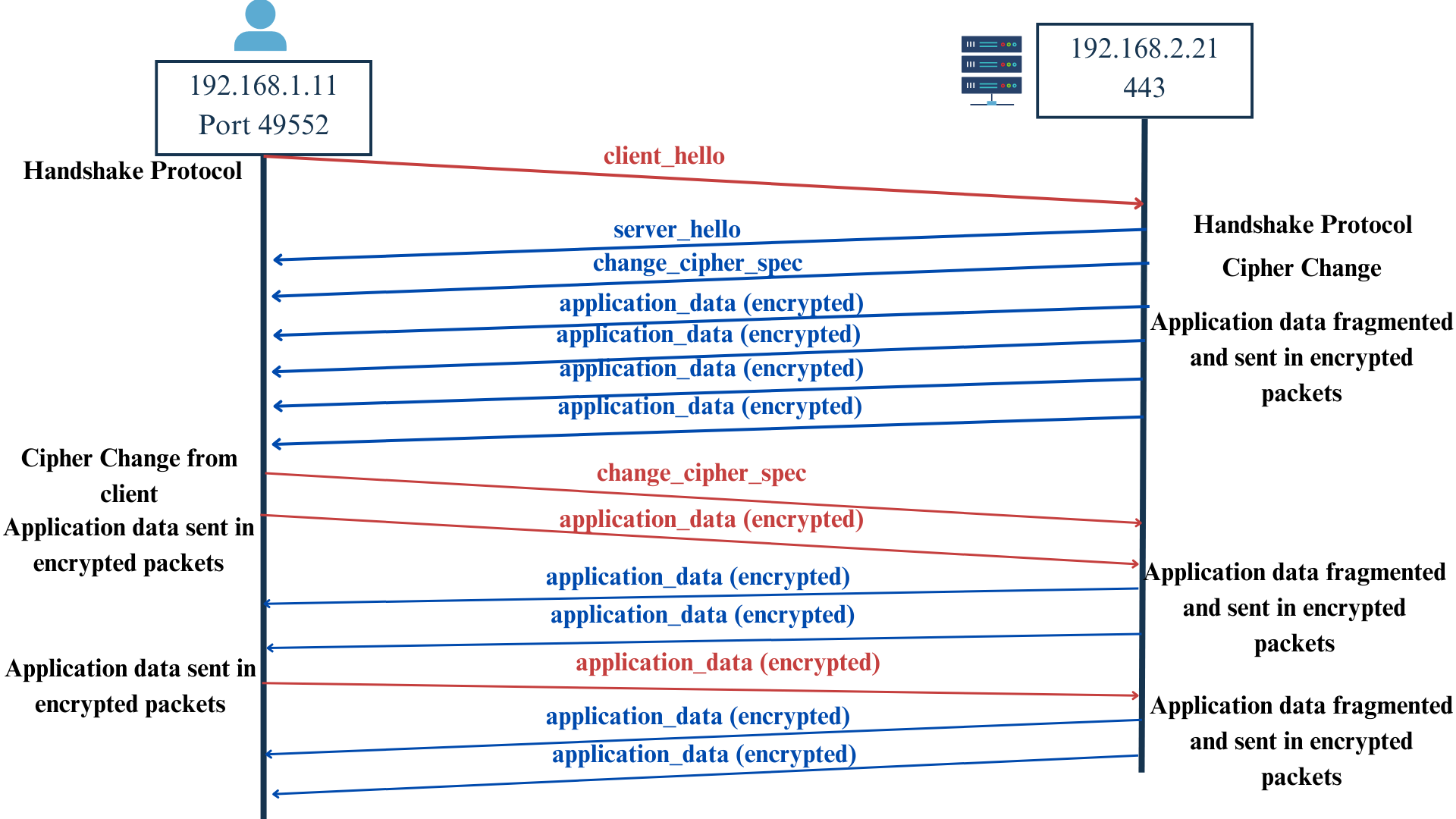






Part (b)

Submitted with the report.

Part (c)

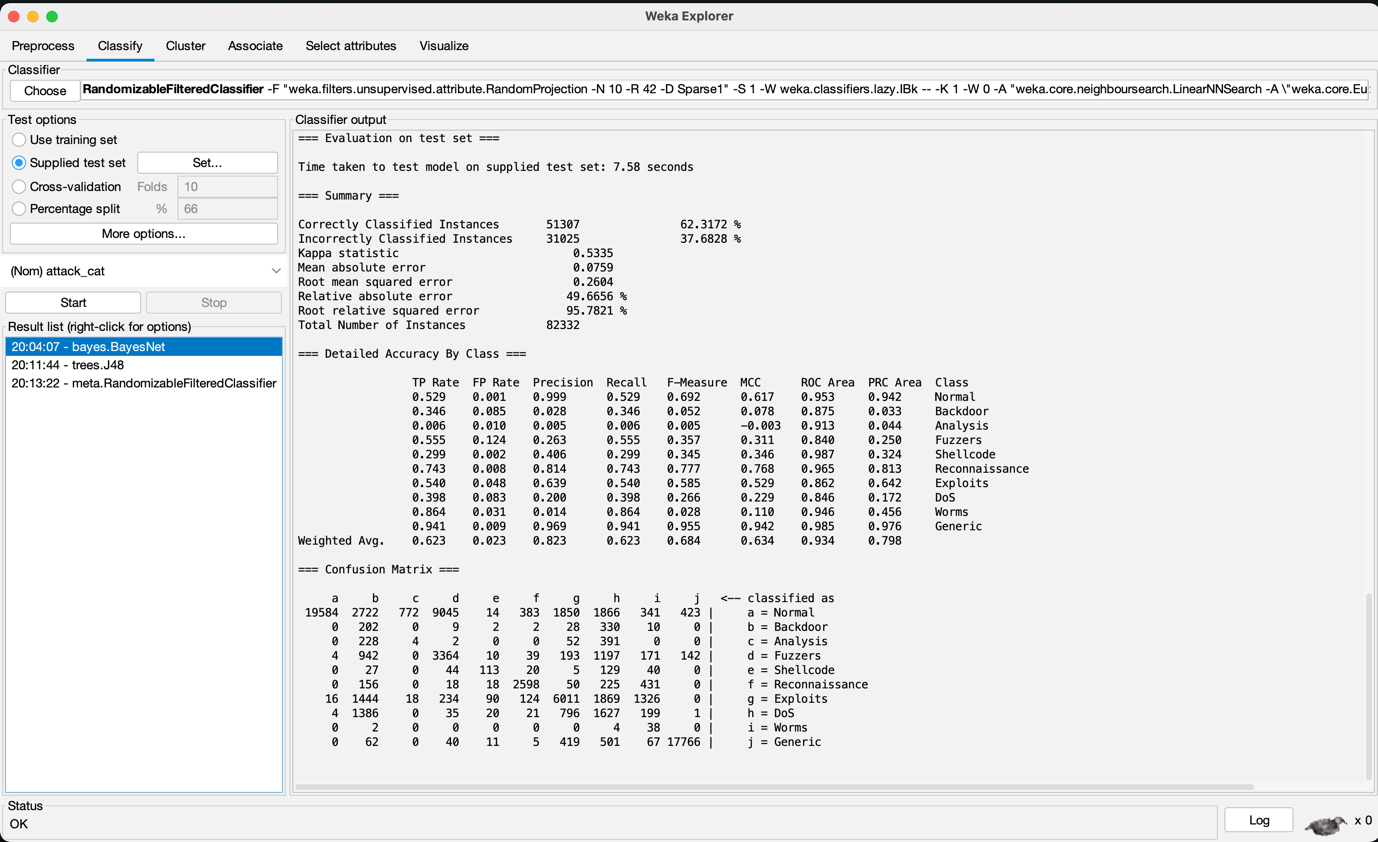
Part (d)

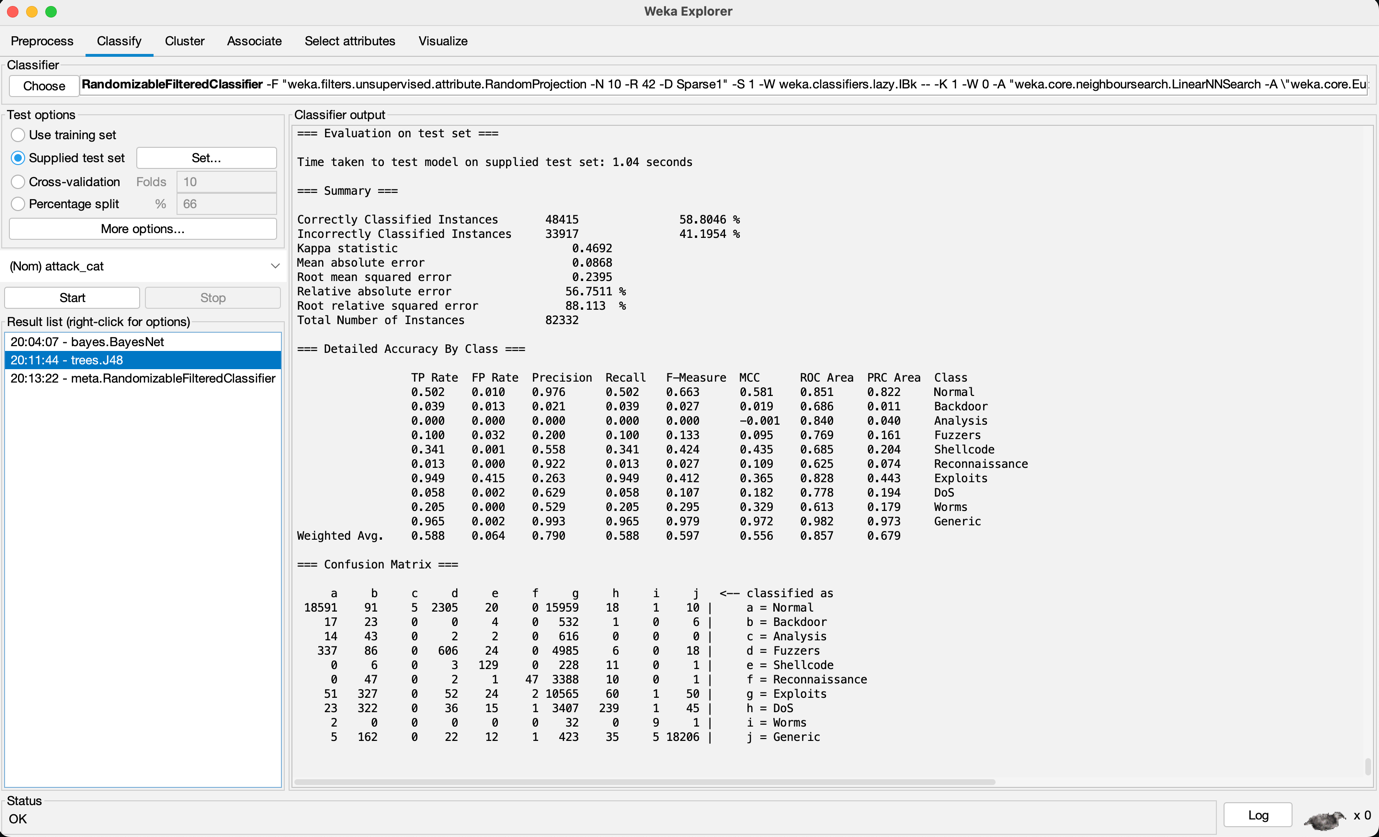
The CA keypair, or the central authority’s private key, is used to sign certificates for many other users in the domain. This means that if an attacker gains access to the CA’s private key, they may be able to sign certificates for all the users in the system and pretend to be other users for malicious reasons. They can also set attacks pretending to be those users. They can have access to all the users’ login credentials user, such as username and password, the personal grades of the students. With the login details, an attacker can have access to the student’s account.

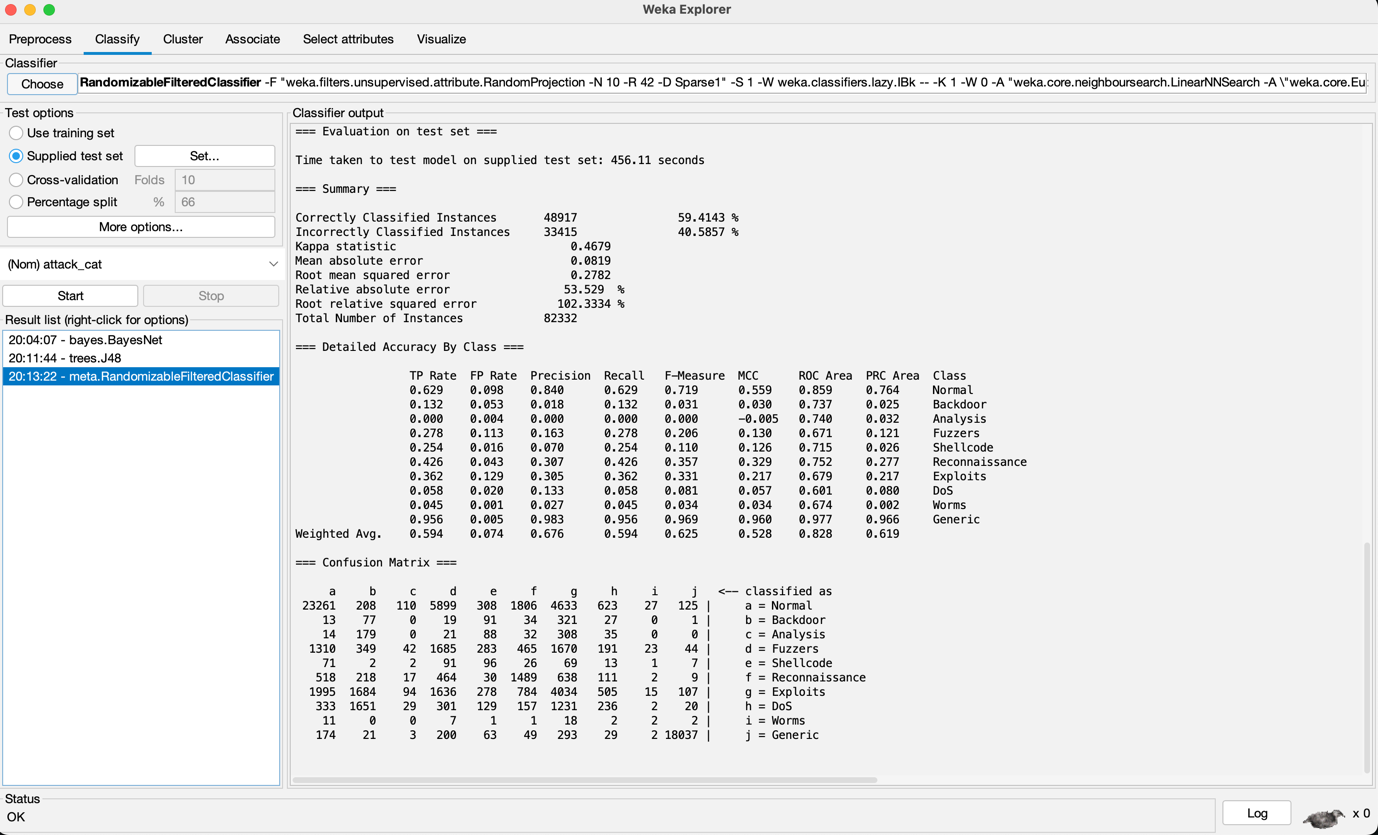
They may also be able to add, change, or delete a student’s grade as they can have access to users that have read, write, and execution authority. They could also add, changed details of, or delete a student or other users.

1. Attack Detection from Real Intrusion Dataset

Part (a)







Part (b)

The two best classifiers were the BayesNet (BN) and meta RandomizableFilteredClassifier (RFC) as they produced the highest rate of correctly classified instances out of the three, with 62.31% and 59.41% respectively. While neither’s accuracy is particularly high, BN did have a higher accuracy percentage, with over 2000 more instances classified correctly than RFC.

The precision rate for BN was also higher for every class besides Worms and Generic, with the weighted average being significantly higher, meaning BN was able to detect more correct instances than not from the dataset.

The average recall rate was also higher in the BN classifier, with the classes Normal and Generic being the outliers. However, overall BN had a higher recall rate meaning it identified more instances out of the instances available.

The average F1 score for BN was higher, however, the individual class rates varied, with BN having a higher score in 6 and RFC having a higher one in 4. That said, BN still proves to be more reliable as it has had a higher instance rate of them all.

BN also had a much lesser FP rate, meaning there were fewer instances of it wrongly classifying instances to the wrong class, therefore, being more reliable that RFC. However, the instances for each class were divided with BN having a lower FP rate in 5 and RFC having a lower rate in the other 5. The FP rate difference however, favours for BN as RFC had a vastly higher FP rate in comparison.

Part (c)

BayesNet (BN) gave the best performance when compared among the other two, as not only did it correctly classify more than the others, but it was also more precise for each class for the most part, and had a higher recall rate, meaning that out of all the instances available for each class, it identified more. It also had a much smaller false positive rate overall, meaning it incorrectly classifying instances was lower, making it more reliable. The F1 score, which is a calculation that involves precision and recall rate was also higher for BN than the other two.

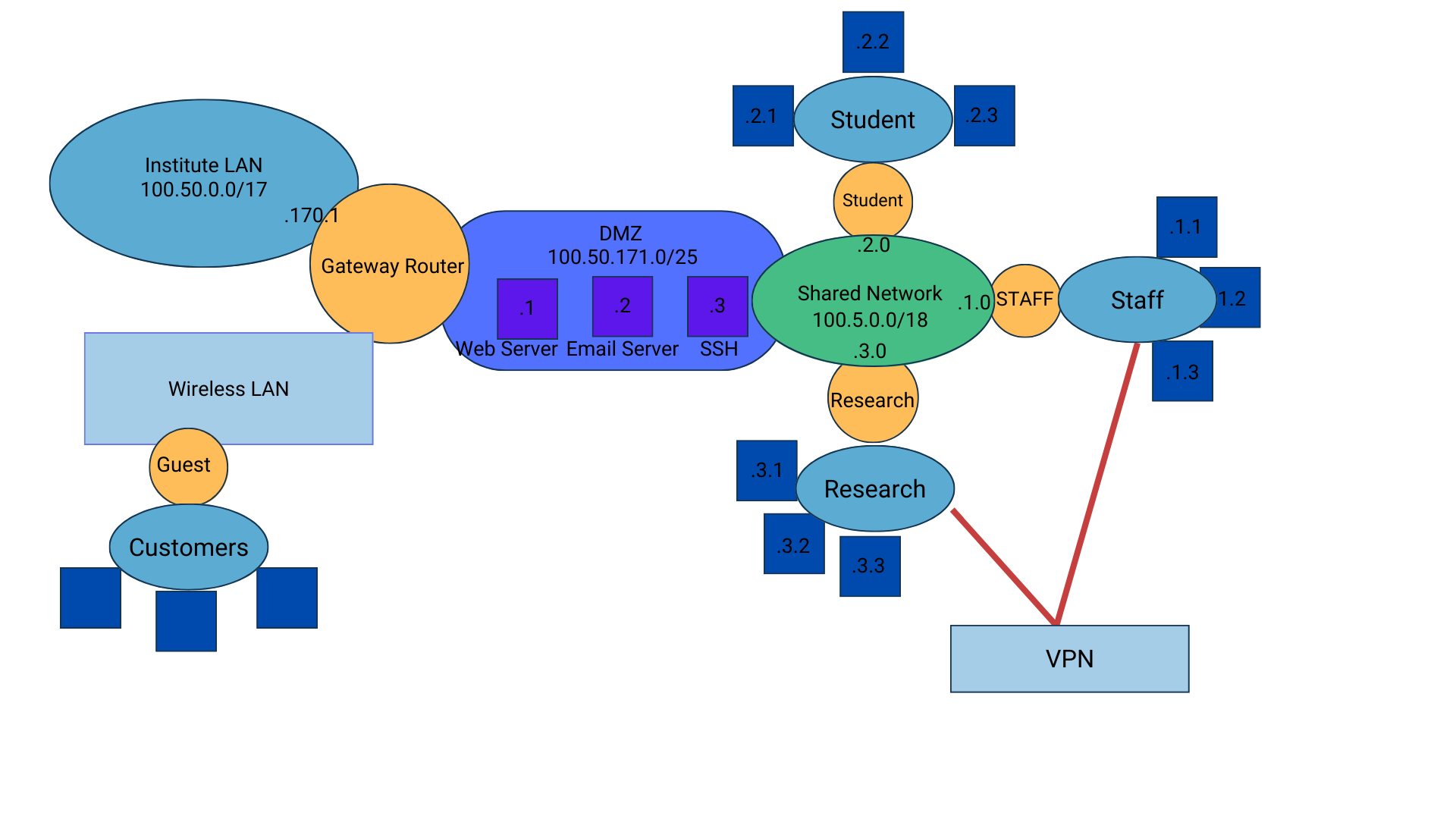
A few ways of improving the performance further can be adding more data, which can provide a more accurate result. This could also include adding more classes of attacks and segmenting the normal and generic classes into further distinct attack classes. It can also be important to check for any values and information that is missing in the instances and either filling them or removing them if filling is not an option. This can also provide a reliable result and fewer false positive and false negatives. Also, removing instances that don’t follow any of the classes should also be removed as they will either be a false positive or a false negative.

Part (d)

The two attacks most detected lie under the class of “Normal” with 37,000 instances and “Generic” with 18,871 instances. These attacks fall under an umbrella of basic passive and active attacks such as releasing message contents, traffic analysis, masquerading attacks, replay attacks, and modification attacks. These attacks are not as specific as the others, therefore having a much larger number of instances, therefore, being general security attacks lumped into two classes.

1. Firewalls

Part (a)



Part (b)

1. FLUSH all: Assuming there were pervious rules, they are to be flushed to create new rules.
2. Enable SPI:
   1. Change the default policy to DROP, this is done to enhance security.
   2. ACCEPT packets that have an established or related TCP connection. This enables to create fewer rules.
3. Provide Gateway router ACCESS to the DMZ.
4. Provide Gateway router ACCESS to the Shared Network. Through the shared network, all the routers connected will also get access.
5. Provide Staff Router ACCESS to DMZ’s Web Server. Staff are allowed access.
6. Provide Student Router ACCESS to DMZ’s Web Server. Students are allowed access.
7. Provide Research Router ACCESS to DMZ’s Web Server. Researchers are allowed access.
8. Provide Staff Router ACCESS to DMZ’s Email Server. Staff are allowed access.
9. Provide Staff Router ACCESS to DMZ’s SSH Server. Staff are allowed access.
10. Provide Research Router ACCESS to DMZ’s SSH Server. Researchers are allowed access.
11. Provide Wireless LAN ACCESS to Gateway Router. Providing access will also provide access to Institution the Shared Network
12. Provide Wireless LAN ACCESS to Guest Router. Will provide access to customers through a different router.
13. Provide VPN ACCESS to Staff Router. Staff are allowed access.
14. Provide VPN ACCESS to Research Router. Researchers are allowed access.

As the packet filtering is via SPI, the default policy is to drop any packet unless it has access approval, therefore, only access rules are to be granted. This is done to enhance security. SPI also enables acceptance automatically with a previously established connection; therefore, the rules do not have to be written twice for connection from the other side.

Part (c)

Firstly, the whole table was flushed, so that there are no previous rules left for the new firewall system. While Virtnet didn’t have any prior firewall rules, there was nothing to flush. However, I demonstrated the process below.

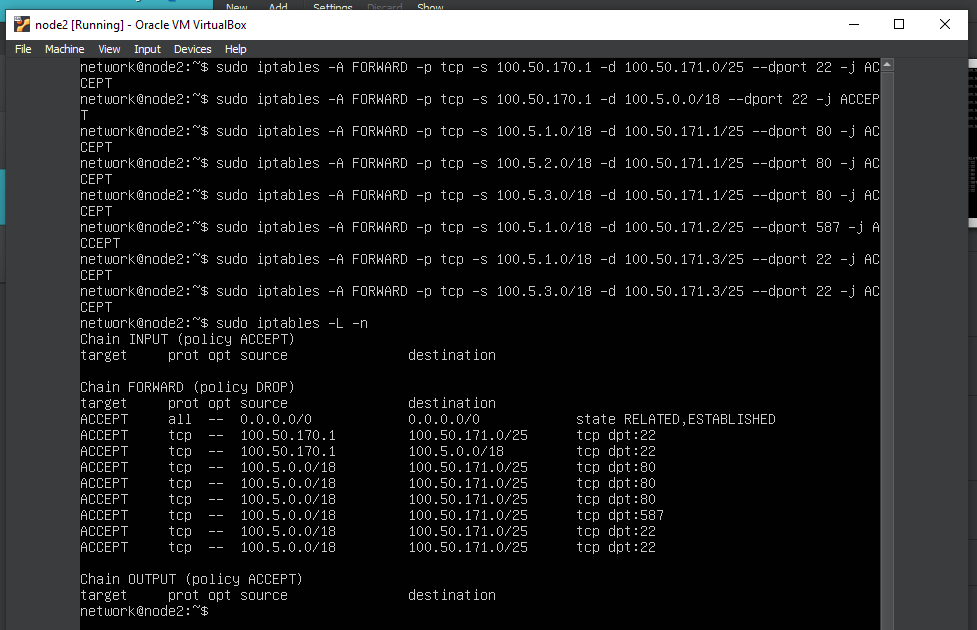
A screenshot of a computer

Description automatically generated

Secondly, SPI was established. This was done by changing the default policy to drop, and then creating the policy of established and related connections to have two-way communication. This can be seen below.



Lastly, rules 3 to 10 are implemented, shown below, from connecting the gateway router to the DMZ network and Shared Network (shared network allows all hosts to access the router), and then the selected routers from the shared network getting access to DMZ’s web, email, and SSH servers.



Rules 11 and 12 regarding establishing WLAN connection to the gateway router and guest router remained impossible, as WLAN and Guest Router IP Addresses were not established. Same is the case with rules 13 and 14 where the VPN addresses weren’t established either.

1. Wireless security

Part (a)

The article presents the findings of a study done to highlight the threats that emerge from Wi-Fi connection, as over 75% of mobile internet usage is done through it. This study, performed mostly in China, is done by examining 19 million Wi-Fi access points (AP) and a crowd sourced security checking system called WiSC (Wi-Fi Security Checker) which runs on top of an Android application. The study uncovers the types of attacks, their prevalence, level of risk, and characterizes Wi-Fi threats, along with the motivation of the attackers and how to combat them, ending with guidelines for safety.

The major findings regarding prevalence uncovers around 4% of Wi-Fi APs had some sort of attacks detected. This finding strays from previous small-scale studies and understandings, that showed the highest detection rate being 1.5%. Most of these attacks were via ad injections, and technique where ads are discreetly shown to users on a webpage that was not authorized by the site owners. Interestingly, the study also found that they occurred more on secure APs. These ads were performed by what the article calls an “underground economy” that uses real ad requirements from advertisers and inserts their own ads through compromised APs, abusing the web analytics platform advertisers use. However, it is also uncovered that these platforms are able to create congestion by monetizing them and leveraging it to combat ad injection attacks. The study does understand it’s limitations, based on the n-value and location restrictions, but does manage to display insights that were previously unknown or misunderstood.

The idea of ads being shown without the knowledge of the site owners is a concept that intrigued me, as the different parties that are needed to be intercepted to display ads to install malware or other threats is one I had seen in life (before discovering ad-block software) but never understood how it could be possible. It also magnifies my understanding and reasoning for regular security testing.

Part (b)

This study dives into the concept of spectrum scarcity, which is the understanding that radio frequencies are a limited resource that should be managed with care. This concept has been challenging as it can often be a roadblock to achieving an enhanced quality of experience (QoE) for the newer generations of wireless connectivity, such as 5G and Wi-Fi 6. The scarcity becomes even more challenging as more devices than ever are connected to wireless networks, thanks to emerging technologies such as Internet of Things (IOT) smart home technologies. Therefore, there have been many partnerships to share the spectrum creating a “coexistence” to try and achieve the desired QoE. That said, this study implies that while achieving said QoE and the coexistence were of focus, the security vulnerabilities that arise from them were overlooked, and they are plentiful. Mainly, the complexity of authentication and authorization that in standalone networks are not an issue, but with shared networks can be a breeding ground for threats and attacks. These can result in exploits such as service blocking, rogue base-stations deployed, and eavesdropping attacks. The study encourages a new research opportunity and security framework design to address the challenges faced by coexistence networks.

Compared to the previous study which uncovered vulnerabilities about Wi-Fi attacks through ad injection, this uncovers the possibility of future attacks. It can be alarming knowing that the previous study, which was only a year older than this, showed the flaws in previous studies and how they vulnerabilities of general Wi-Fi are still not uncovered, this study is already showing that the rate wireless technology is improving only brings in more vulnerabilities and attacks.

Ramezanpour, K., Jagannath, J. and Jagannath, A. (2023) ‘Security and privacy vulnerabilities of 5G/6G and WIFI 6: Survey and research directions from a coexistence perspective’, Computer Networks, 221, p. 109515, accessed 2 June 2023. doi: 10.1016/j.comnet.2022.109515.

Part (c)

The studies provided insights into how, while convenient and mobile, wireless networks such as Wi-Fi can be a source of vulnerabilities and attacks. It also shows the limited understanding we currently have of these vulnerabilities and how the focus is shifted mostly on improving performance and QoS. While those are crucial, and maybe even essential in our internet-driven world, security analysis should also be given priority.

The first resource uncovering findings and metrics not known before is impactful and a sign that continuous dives into finding network security vulnerabilities should be implemented. It also encourages performing more studies with a wider reach location wise, eliminating the limitations found in this study.

The second resource introduced me to the concept of spectrum scarcity, which makes me understand the potential limitations of future wireless networking, and how actions such as the coexistence networks will need to be implemented to achieve more performance enhancements. That, along with our ever-growing demand of more devices and integration of wireless networks into every aspect of our lives will be a feat that is immensely challenging, and that is not even covering the exponential amount of security vulnerabilities that will be uncovered. This article provides a better glimpse of how the need for improved availability will impact security vulnerabilities and attacks. Therefore, the need and research for security analysts will increase too.