

# **HND/HNC Applied Computing**

## **Unit ACCA4024 – Network & Cyber Security Essentials**

### **Assignment**

**Due Date – 16/05/22**

**Student Name:**

**Alaw Roberts**

**AR181160**

# **Content**

## **Introduction**

### **1.0 Vulnerabilities, threats, and attacks**

### **2.0 Techniques that the company could adopt to mitigate vulnerabilities**

### **3.0 Scanning Tools - Nmap and Packet analysis**

### **4.0 Scanning Tools Metasploit and SQL Injection**

### **5.0 Cryptography Protection Techniques / Data Security**

### **6.0 Strategy/Security Policies for ABC Car Rentals**

## **References**

## **Appendix**

## **Introduction**

In this report, I will give information about what are the risks ABC Car Rentals has. How these risks can be dramatically reduced with security measures and policies.

Currently, there are many possible vulnerabilities, threats, and attacks due to how ABC Car Rentals company's systems are being accessed from various personal devices and offices 24/7 including possible uses of unsecured Wi-Fi internet access from various locations by company staff.

There are increased potential risks if staff are using personal devices for work such as their mobile phones and tablets which most likely do not have any protection such as anti-malware or antivirus software on their devices

There are many types of external threats, software-driven threats, internal threats, physical threats, and possible causes of social engineering due to how they run their business.

This means they are wide open to cyber-attacks when they log into their company account or any other company business account. As they also use video conferencing facilities and Cloud storage to make their business more effective, these also pose security risk factors.

### **1.0 Vulnerabilities, threats, and attacks**

The types of cyber-attacks which can happen are active ones or passive threats.

The difference between an active and passive threat is that when an active one happens, an attack can mean that a system is changed/modified and therefore can mean system resources are compromised, affecting businesses' operations.

When a passive attack occurs, it is when an attacker attempts to learn and gain information about a system. For example, they are collecting security information so that they can learn how to attack the system later. They are trying to collect/intercept any information that is transmitted.

[1]

It's critical to make sure that the company's security is protected to the highest level possible to reduce or have no impact on the company if a security breach happens. Having a serious security breach can cause major problems and issues within their infrastructure. It can mean a loss of reputation, large financial loss and losing the trust of important customers/clients that the company has.

These are the reasons behind having a low-security level within the company's infrastructure.

As explained by Andrew Tsonchev problems that can arise are things such as if your company has issues with low security or staff who have not had any training to be aware of such things, staff need to be aware of how to be safer and more secure online. [2]

Often these examples are **external threats** from cyber-criminals which can be a large problem:

- **Weakened Security controls** -This is a problem because staff can work from anywhere without proper security measures. Using Home Wi-fi or possibly public Wi-fi if working out of the house in cafes etc.
- **Email scams are a large problem, scams using email have been increasing-** staff might not know what to look out for in emails. There are many phishing/scam emails which are often the way in for hackers.
- **Attacks on remote-working infrastructure-** Working from home, or anywhere means that a lot of existing layers of security will not be there for remote workers, therefore, having less protection.
- **Errors and Creative solutions-** many employees are being encouraged to find new ways of doing things and therefore might do something which is not the secure and authorised way to do so.

This is a type of **internal threat**:

- **Malicious insiders and malicious housemates-** data can be easily taken from personal devices using devices such as USB if these ports are not blocked. People coming into the home who may not be trustworthy, risk having devices stolen from within the home. [2]

Other things which could be causing risk factors are:

- Attacks over the Cloud.
  - The use of online software chosen by staff that might not be secure or could even be unlicensed without them knowing.
  - Understanding your employee's changes from static to non-static work.
- [2]

**Social engineering** is a major factor:

(p.94) ***"The term social Engineering means using deception to manipulate someone into revealing information or doing something such as clicking onto a link in an email that will eventually reveal information or install malware or the like"*** [3]

This could be used within the building when someone pretends to be from the business and takes advantage to collect information inside the company's building or it could be an untrustworthy employer secretly trying to gather information.

Another type is **physical threats** such as loss and theft of devices. It is very easy to forget and misplace your devices such as a phone, tablet, or laptop and therefore these devices are a big risk to a company's business if they are open to being accessed. To avoid this risk of a device being wide open to an attack if stolen there are things which can be done according to Wright, such as using multi-factor authentication (MFA) and having strong passwords making sure that they are different for all accounts created. Having different passwords for each device they own, especially corporate devices. [4]

***“In our recent survey of more than 200 IT decision makers, 56% said they felt personal device use has left them more vulnerable to a security breach.” Lucy Wright***

Data breaches are more common due to personal devices being used. As these devices are not part of a company's IT infrastructure because they are not protected by the same security level which protects the rest of the network. Organisations must invest in their network security to protect their organisational data. [4]

### **Software-driven threats-**

Having outdated software can mean more vulnerabilities are a part of a software. It's a weakness in the software itself. It means an opportunity for it to lead to a breach.

***“Software programs currently contain an unacceptable number of vulnerabilities” (p. 25) [3]***

Through these gaps and weaknesses, hackers can often exploit these vulnerabilities. They do this by going internally through the software to gain unauthorised access. This is one reason why updating your software is critical to reducing the chances of a breach occurring.

Many organisations don't have anti-malware software or make sure that their software is corrected or updated frequently enough.

***“The top human vulnerability hackers exploit is the human propensity to trust” [3]***

***“Far too many invite hackers into their computers and networks by, for example, clicking on malicious attachments from unknown senders and succumbing to phishing.” (p.93) [3]***

When staff do not know enough about the risks of using old software and other risks such as phishing ***“phishing is the use of an electronic communication, most often email that masquerades as being from someone trustworthy to include the recipient to reveal information such as usernames and passwords” (p.93) [3]***

Other things to be aware of are if staff are deciding to use unsecured Wi-fi networks which means a much greater risk for attacks. A company's network is usually much more secure than a home network, especially a public network!

Not only this but as they are not a company device, employers can access whatever they like on the internet meaning that they are more prone to get malware or viruses as usually many websites would be blocked on a company's device protecting them.

### **Malicious Software/Malware**

There are multiple types of malicious malware. These can be viruses, worms, trojan horses, spyware, adware and more. These are used to exploit systems which can mean a security breach and systems being exploited. [5]

According to McKnight data security is very important within a company large or small. They can both be impacted if no efforts are made. Make sure that your company's data is as safe as possible using security methods. [6]

***“Data security is a company's protective measures put in place to keep unauthorised access out of their databases, websites and computers.” McKnight [6]***

These are many reasons you would want to avoid an attack on your company.

It makes sure that you are protecting your company's reputation. Ensuring the integrity of your business's data. It will avoid any major unnecessary expenditure for example due to losing customer data, and employee information in a breach. This may mean large amounts of financial loss especially if the company did not have policies and strong measures to avoid it.

## **2.0 Techniques that the company could adopt to mitigate vulnerabilities**

This company could use techniques to mitigate these types of threats, attacks, and vulnerabilities that also do not impact the business's productivity and performance to reduce these risks. Employees can do something to reduce the risk of having their devices targeted or hacked.

The company can make sure a written policy/guideline is in place:

- staff can then know that certain websites should not be used.
- Explanation of how important it is to be aware of email scams and phishing and not trust emails that look genuine, are not grammatically correct, have a strange email address, or have odd-looking attachments.
- The company could provide staff with a course or a document showing them how to spot phishing emails and scam emails. This could increase their awareness of many cyber risks.

### **Using Cryptographic protection techniques:**

Allowing the use of the safest types of software for doing video calls such as What's app due to its use of end-to-end encryption which secures data across its entire journey from the sender to the receiver.

This means the data is encrypted when sent and then decrypted when it has reached its destination. Therefore, at no point during this journey, the data cannot be seen or accessed. This also means that in the event of a data breach, any leaked conversations are still secured. [7]

There are several techniques and encryption methods. Data must be encrypted, and the company should use the best suitable method of encryption.

Employees who are working at home should be using a VPN (Virtual Private Network). By using an encrypted VPN, they will be hiding their internet traffic inside a regular network. This makes it increasingly hard for cybercriminals to know and see that important data is transmitted over the network. Have employees create strong passwords which are easy to remember.

[8]

### **Using hardware and software protection techniques such as:**

Having good hardware security is important to protect your computer's hardware against attacks which might be caused due to security vulnerabilities within the Operating system.

Software protection is also extremely important if not more than hardware as the types of software can vary much and the security of each different one can be very different.

Very often software is more prone to malicious attacks and security risks as it might not be updated frequently enough by the user and therefore become vulnerable to attacks. To help protect their systems, software should be updated regularly or even set to update automatically. [9]

### **3.0 Scanning Tools - Nmap and Packet analysis**

#### **Nmap**

Use scanning tools to find out how vulnerable the company has made itself. Testing out certain methods such as scanning with Nmap and using Wireshark to analyse traffic. This can allow the company to use these tools to be able to test the security of their systems to understand how easy or hard it is to attack their network infrastructure using such tools.

The purpose of Nmap is used to scan IP addresses and ports which are in a network. It's also used to detect installed applications. It can be used by hackers that will try to exploit vulnerabilities in a system. They get access through uncontrolled/open ports of a system and then can use this information to gain further access. [10]

#### **Packet Analysis**

Wireshark is a tool that can be used as an analyser in a network protocol. It's usually used as a packet sniffer. It can do three things which are:

Packet capture: this means that it listens to a network connection. It collects a lot of traffic as much as thousands at a time which is also in real-time as it does it.

Filtering: Using filters, you can get any specific information that you need from it. It slices and dices real-time data by using filters.

Visualisation: It allows you to look at complete conversations, also network streams which means that you can collect information from the middle, and therefore it's a good packet sniffer. Using a tool that's able to look deep into the different parts of the network, discovering things which make it vulnerable. [11]

## **4.0 Scanning Tools Metasploit and SQL Injection**

### **Metasploit**

Metasploit could be a good tool for the company to use as you can understand how the system works and how easy it is to hack the company's systems using Metasploit software. By using another technique called an SQL injection using a virtualized environment, the company will be able to find out any potential weaknesses in its security.

Metasploit can allow you to do penetration testing. It allows you to find out how a person with intent can damage your network. As it's an open-source network framework, testing can be done via command line alterations or GUI according to Petters. It's a useful tool which is used to probe systematic vulnerabilities, on networks and servers. [12]

### **SQL Injection**

SQL injection techniques are used to gather information from a database. It is used by exploiting software vulnerabilities in web applications so that data can be stolen but not only this the data can be deleted or modified. Cybercriminals can gain access through administrative control by gaining access through the systems and then running these affected applications.

***“A SQLI is a type of attack by which cybercriminals exploit software vulnerabilities in web applications for the purpose of stealing, deleting, or modifying data, or gaining administrative control over the systems running the affected applications.”***  
[13]

It can be used by criminal hackers who enter malicious commands into web forms. They do this by entering through a search field, URL, or another example a login field. This is done on an unsecured website so that they can gain unauthorised access to important sensitive data. [13]

## **5.0 Cryptography Protection Techniques / Data Security**

According to Kearns because cyber-crimes are: ***“becoming increasingly common and more challenging to prevent due to the continuous and rapid advancement in technology”***

[14]

More businesses are using the cloud, and this is true for ABC Car Rentals’ work it can still mean that businesses are at risk of cybercrime and attacks due to being compromised using insecure networks, unwanted parties when sending data across a network in a cloud environment and therefore it is important to think about using cryptography in their security plans.

Reducing the risks of data being intercepted when transmitting data, files, and sensitive information over the internet.

***“Cryptography is converting plaintext data into an unreadable format through mathematical functions”*** [14]

Encryption is a way to make sure that your data is safe. Make sure that data is secured on the company’s systems and network. ***“encryption is a powerful data protection control that helps provide confidentiality and integrity of data”***. [15]

Cryptographic methods are key to securing the company’s data for example when using other tools such as messaging and video calling apps for conference meetings.

These methods should be implemented by ‘ABC Car Rentals’ as a more secure option for sending important data to staff and sharing important company secrets which you do not want to lose or let into the wrong hands. Losing this data could be detrimental to the company’s reputation and finance.

***“No matter which cybersecurity strategy or combination of strategies organizations pursue, when the rubber hits the road, protecting the data is the objective.”*** [15]

There are many types of encryptions. These are two of the most used and secure types:

### **AES encryption method-**

- Used in everyday business
- Very secure type
- Uses symmetric key encryption
- Works in many applications
- Most widely accepted

### **RSA encryption method-**

- Used for data being sent online
- Using a public key to encrypt the data
- The person on the receiving end will have the key to decrypt the sent messages.
- Not practical for large or numerous files. [16]

### **Importance of Data Security-**

There are many legal requirements for businesses to follow:

- The data protection act 1998 & 2018 GDPR  
[17]

Other Regulations which the business may need to look at:

- Computer misuse act 1990
- Copyright Designs and patents act 1988

Network and Information Security Regulations 2018 (NIS Regulations) This regulation deals with the security of information systems.

This should be a part of the business strategy to protect key IT systems and important information assets. This also means keeping systems/software up to date through upgrading continuously and testing making sure that the security of their systems keeps on developing and is current.

[18]

### **Information security-**

**There are 3 principles which the company should follow:**

#### **The CIA Triad**

1. Confidentiality- Having measures to prevent unauthorised access to information.
1. Integrity- Making sure data is accurate. That it has not been modified e.g., accidentally, or maliciously. Data is reliable.
2. Availability - The importance of having data protected. Having access to the software and that it's fully available to use when it is needed by staff etc.

[19]

## **6.0 Strategy/Security Policies for ABC Car Rentals**

This company should have suitable security measures in place. The company should have an updated and clear written policy. Having a strategy should mitigate all its current flaws within the company's security. These policies would need to be updated often.

A policy will make the company dramatically more secure from cyber-criminal attacks. Having relevant security policies in the company will help employees have a better understanding of the importance of maintaining data security, hardware security, and software applications inside the organisation. With all the current risks involved within 'ABC Car Rentals' business organisation. A plan/strategy is critical.

A policy would allow staff to understand the importance of following them as not doing so can mean a security breach while better securing clients' data.

### **Written Policy:**

- 1. Network access-** a policy explaining how they should be using home/personal devices stating what internet access is allowed e.g., should not be used using public Wi-Fi unless they have security measures such as anti-malware and VPN. Explaining other procedures such as device passwords, wireless network usage and firewalls and more.
- 2. Emails-** Having a guideline which explains how the use of emails can potentially create a cyber security breach due to phishing emails, scam emails which might contain attachments which include viruses and more.
- 3. Passwords-** A guideline which explains the importance of having strong passwords which cannot be guessed easily and following these standards consistently, therefore, reducing the chances of accounts being hacked.
- 4. Confidential Data-** A policy which defines what information the company considers to be sensitive data. An explanation of how this data should be used and handled by staff.
- 5. Physical Device security-** A policy which gives clear instruction on how devices are being used and transported with care. Reducing the chances of lost or stolen devices.

- 6. Incident Response-** A document explaining what should be done. A step-by-step approach that everyone in the business organisation can follow. This would allow the business to know what to do in the event of a breach. Keeping them alert to tell any other relevant parties, therefore, reducing the impact on their data integrity and network so that they can return to business as quickly as possible to also reduce time lost which is money lost.
- 7. Acceptable use-** a policy which explains clearly and states what resources under the IT department can be permitted to be used by who and what staff can use.

Even with strong policies, it's not enough. This would be a large step for a company such as 'ABC Car Rentals'. These policies should come with other practical forms of learning.

***"As such, any new IT policy should be accompanied by rigorous training initiatives to make sure everyone within the organisation - from the highest-ranking members to the frontline staff - know and understand these principles from back to front."***

**V.C**

[20]

Policies should be side by side with having good quality training for all staff.

This would give greater understanding for the staff, making sure that everyone in the organisation understands all the above and can consistently follow these guidelines/procedures.

These policies will need to be updated regularly to make sure that they continue to be relevant as technology enhances and changes and therefore staff should be reminded to re-read them often.

Knowing the risks involved means that the company is less likely to have a weakness in its network security.

Having these policies means that 'ABC Car Rentals' would be able to manage themselves and their staff and have appropriate security measures that are followed correctly.

As explained here by SecurityScorecard I agree with them that:

***"Employees tend to be the weakest link in an organization's security posture, often clicking on malicious links and attachments unintentionally, sharing passwords, or neglecting to encrypt sensitive files."*** [21]

This also tells me that having these policies will be beneficial and extremely important and I also agree with this statement by SecurityScorecard:

***“An effective way to educate employees on the importance of security is through a cybersecurity policy that explains each employee’s responsibilities for protecting systems and data within the organization.” [21]***

As explained in this report, being in a business environment these days is truly a minefield and we can see clearly that there are multiple things which need to be considered within an organisation to make sure that they have all the necessary security measures in place to stop potential cyber threats and attacks.

## References

- [1] shobha1617, "GeeksforGeeks," 24 December 2021. [Online]. Available: <https://www.geeksforgeeks.org/active-and-passive-attacks-in-information-security/>. [Accessed 5 May 2022].
- [2] A. Tsonchev, "Five security risks companies face as workers go remote," Dark Trace , 19 March 2020. [Online]. Available: <https://www.darktrace.com/en/blog/five-security-risks-companies-face-as-workers-go-remote/>. [Accessed 20 March 2022].
- [3] R. H. Sloan and R. Warner, "Human Vulnerabilities," in *Why don't we defend better?*, Boca Raton, CRC Press, 2019, pp. 25, 93-94.
- [4] L. Wright, "The BYOD effect: the security risks of using personal devices for work," CORE, [Online]. Available: <https://www.core.co.uk/blog/byod-effect-security-risks-personal-devices-work>. [Accessed 20 March 2022].
- [5] W. Stallings, "2.1 Systemic Encryption Principles," in *Network Security essentials: applications and standards*, Global Edition, Pearson Education, 2017, pp. 46-47.
- [6] L. Mcknight, "The Importance of Data Security for Your Company," 7 October 2020. [Online]. Available: <https://industrytoday.com/the-importance-of-data-security-for-your-company/>. [Accessed 15 March 2022].
- [7] I. Belcic and C. Corrigan, "AVG," 19 November 2021. [Online]. Available: <https://www.avg.com/en/signal/secure-message-apps>. [Accessed 4 May 2022].
- [8] R. Nations, "Important Encryption Techniques to Implement for Your Business," Record Nations Articles, No date. [Online]. Available: <https://www.recordnations.com/articles/encryption-techniques/>. [Accessed 9th May 2022].
- [9] Madhurihammad, "Difference between Hardware Security and Software Security," GeeksforGeeks, 5th March 2021. [Online]. Available: <https://www.geeksforgeeks.org/difference-between-hardware-security-and-software-security/?ref=gcse>. [Accessed 13th May 2022].
- [10] M. Shivanandhan, "What is Nmap and How to Use it – A Tutorial for the Greatest Scanning Tool of All Time," freeCodeCamp, 2 October 2020. [Online]. Available: <https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/>. [Accessed 9th May 2022].
- [11] ComopTia, "What Is Wireshark and How Is It Used?," ComopTia, No date. [Online]. Available: <https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it>. [Accessed 9th May 2022].
- [12] J. Peters, "What is Metasploit? The Beginner's Guide," Varonis, 29th March 2020. [Online]. Available: <https://www.varonis.com/blog/what-is-metasploit>. [Accessed 9th May 2022].
- [13] Malwarebytes, "SQL injection," Malwarebytes, No date. [Online]. Available: <https://www.malwarebytes.com/sql-injection>. [Accessed 6th May 2022].
- [14] L. Kearns, "The Importance of Corporate Cryptography," SecureCentrix, 2nd March 2022. [Online]. Available: <https://securicentrix.com/the-importance-of-corporate-cryptography/>. [Accessed 10th April 2022].
- [15] T. Rains, "Encryption and Key management," in *Cybersecurity Threats, Malware Trends, and Strategies*, United Kingdom , Packt Publishing, 2020, pp. 389-390.
- [16] L. Knerl, "What Are the Different Types of Encryption?," HP, 3rd August 2019. [Online]. Available: <https://www.hp.com/us-en/shop/tech-takes/what-are-different-types-of-encryption>. [Accessed 6th May 2022].
- [17] Seers, "Legal Requirements for Storing Business Information," Seers, No date . [Online]. Available: <https://seersco.com/articles/tag/legal-requirements-for-storing-business-information/>. [Accessed 13th May 2022].

- [18] T. John and P. F. Paul, "Cybersecurity and the legal UK landscape," White & Case , 1st May 2019. [Online]. Available: <https://www.whitecase.com/publications/alert/cybersecurity-and-uk-legal-landscape>. [Accessed 12th May 2022].
- [19] Imperva, "Information Security: The Ultimate Guide," Imperva, No date. [Online]. Available: <https://www.imperva.com/learn/data-security/information-security-infosec/>. [Accessed 12th May 2022].
- [20] V. College, "What should my organisation's IT policy include?," Virtual College, 15th March 2022. [Online]. Available: <https://www.virtual-college.co.uk/resources/what-should-my-it-policy-include>. [Accessed 9th May 2022].
- [21] SecurityScorecard, "6 Examples of Essential Cybersecurity Policies for Businesses," SecurityScorecard, 11th August 2021. [Online]. Available: <https://securityscorecard.com/blog/cybersecurity-policy-examples>. [Accessed 5th May 2022].

## Appendix

### Scanning with Nmap

Using Nmap here, reading through the learning materials to gather the information to be able to answer the questions. Information was gathered from the learning materials, online research and also using the Nmap tool.

The screenshot shows a Kali Linux desktop environment. On the left is a sidebar with icons for Trash, File System, Home, burpsuite, and Lab Files. The main window is a terminal titled 'AR181160@kali:~' displaying the Nmap help text. On the right is a 'Scanning with NMAP' challenge interface with a sidebar containing 'Network Details', 'Learning Outcomes', 'Learning Materials', and 'Challenges'. The 'Challenges' section is active, showing 'Flag 1' with the question 'Which IP Protocol does not have any error-checking?' and the answer 'UDP' submitted, marked as 'Correct'. 'Flag 2' has the question 'Of the 65,535 ports, what port is the last of the "assigned" ports?' and the answer '65535' submitted, also marked as 'Correct'.

This screenshot shows the same Kali Linux desktop environment. The terminal window displays the Nmap help text. The challenge interface on the right shows 'Flag 3' with the question 'What version of Open SSH is running on port 22?' and the answer '7.2p2' submitted, marked as 'Correct'. 'Flag 4' has the question 'What do you type at the start of your command to do something that "super users do"?' and the answer 'enter sudo' submitted, also marked as 'Correct'.

This screenshot shows a single challenge card for 'Flag 5' with 'Points: 15'. The question is 'How many algorithms does the SSH support?' and the answer '3' is submitted, marked as 'Correct'.

This screenshot shows two challenge cards. 'Flag 3' has the question 'Of the 65,535 ports, what port is the last of the "assigned" ports?' and the answer '1023' submitted, marked as 'Correct'. 'Flag 4' has the question 'What do you type at the start of your command to do something that "super users do"?' and the answer 'enter sudo' submitted, marked as 'Correct'.

## Packet analysis

Wireshark is a tool that can be used as an analyser in a network protocol. It's usually used as a packet sniffer. It can do three things which are:

Packet capture: this means that it listens to a network connection. It collects a lot of traffic as much as thousands at a time which is also in real-time as it does it.

Filtering: Using filters, you can get any specific information that you need from it. It slices and dices real-time data by using filters.

## Metasploit

**Flag 1 - How many packets were captured in this pcap? 7444**

The screenshot displays the Wireshark network protocol analyzer interface. The main pane shows a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The packet list includes TCP, ICMPv3, and ICMPv6 traffic. The packet details pane on the left shows the selected packet's structure, including Ethernet II, Internet Protocol Version 4, and ICMPv6. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII. On the right, the 'Packet Analysis' sidebar is visible, showing 'Flag 1' with the question 'How many packets were captured in this pcap?' and the answer '7444' entered in the input field. The 'Submit' button is highlighted in green, indicating a correct answer. Below this, 'Flag 2' and 'Flag 3' are also visible, each with a 'Submit' button and a 'Points' value.

| No.  | Time         | Source                 | Destination    | Protocol | Length | Info                                             |
|------|--------------|------------------------|----------------|----------|--------|--------------------------------------------------|
| 7439 | 54866119.524 | 192.168.131.129        | 149.174.28.143 | TCP      | 54     | 50125 → 80 [ACK] Seq=807 Ack=798 Win=63444 Len=0 |
| 7440 | 54866119.524 | 192.168.131.129        | 224.0.0.251    | TCP      | 54     | 50125 → 419 [CS] Seq=807 Win=63444 Len=0         |
| 7441 | 54866119.558 | 192.168.131.129        | 224.0.0.22     | ICMPv3   | 54     | Membership Report / Leave group 224.0.0.251      |
| 7442 | 54866119.558 | fe80::d9da:511d:d51... | ff02::16       | ICMPv6   | 90     | Multicast Listener Report Message v2             |
| 7443 | 54866119.636 | 192.168.131.129        | 224.0.0.22     | ICMPv3   | 54     | Membership Report / Leave group 224.0.0.251      |
| 7444 | 54866119.636 | fe80::d9da:511d:d51... | ff02::16       | ICMPv6   | 90     | Multicast Listener Report Message v2             |

Flag 1 Points: 5

How many packets were captured in this pcap?

7444 Submit

Correct

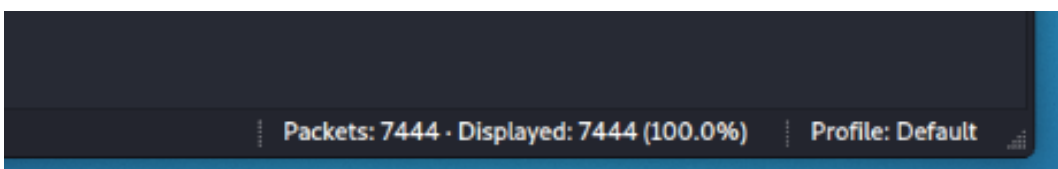
Flag 2 Points: 5

How many TCP Conversations were captured in this pcap?

Submit

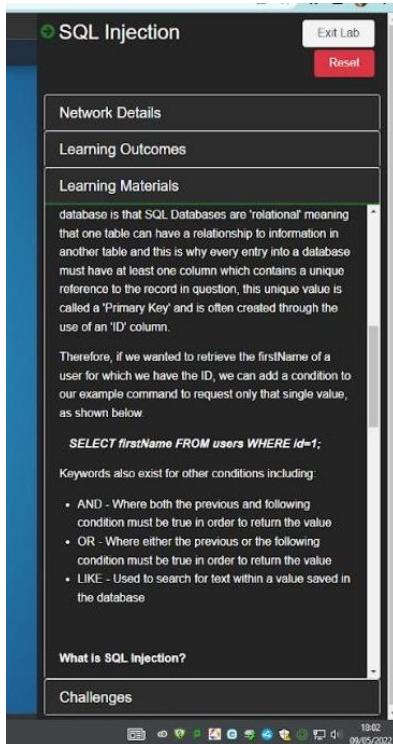
Incorrect

Flag 3 Points: 10



## SQL Injection

Most of the information to answer these SQL questions was in the learning materials. By looking closely I was able to find the answers.



The screenshot shows the 'SQL Injection' lab interface. The 'Learning Materials' section is expanded, displaying text about relational databases and a SQL query example. The query is: `SELECT firstName FROM users WHERE id=1;`. Below the query, it lists keywords for other conditions: AND, OR, and LIKE.

Network Details

Learning Outcomes

Learning Materials

database is that SQL Databases are 'relational' meaning that one table can have a relationship to information in another table and this is why every entry into a database must have at least one column which contains a unique reference to the record in question, this unique value is called a 'Primary Key' and is often created through the use of an 'ID' column.

Therefore, if we wanted to retrieve the firstName of a user for which we have the ID, we can add a condition to our example command to request only that single value, as shown below.

`SELECT firstName FROM users WHERE id=1;`

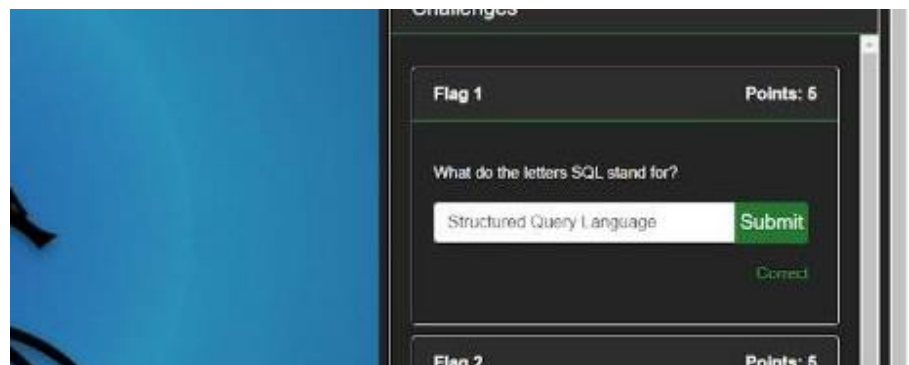
Keywords also exist for other conditions including:

- AND - Where both the previous and following condition must be true in order to return the value
- OR - Where either the previous or the following condition must be true in order to return the value
- LIKE - Used to search for text within a value saved in the database

What is SQL Injection?

Challenges

### Flag 1- What do the letters SQL stand for? Structured Query Language



The screenshot shows the 'Flag 1' challenge. The question is 'What do the letters SQL stand for?'. The answer 'Structured Query Language' is entered in the input field. The 'Submit' button is highlighted in green, and the status 'Correct' is shown below it.

Flag 1 Points: 5

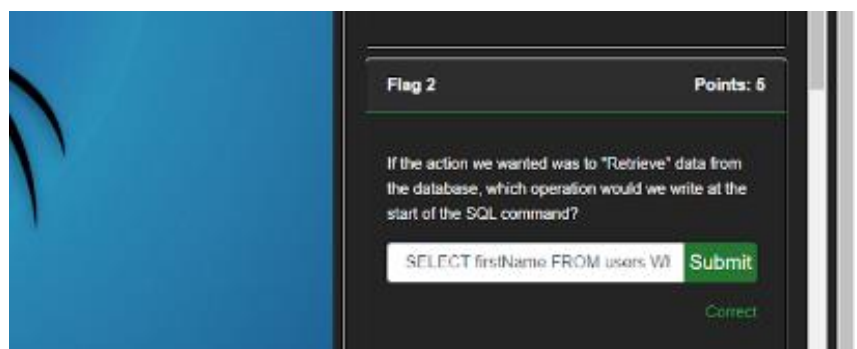
What do the letters SQL stand for?

Structured Query Language Submit

Correct

### Flag 2 – If the action we wanted was to 'Retrieve' data from the database, which operation would we write at the start of the SQL command.

**SELECT firstName From users WHERE id=1**



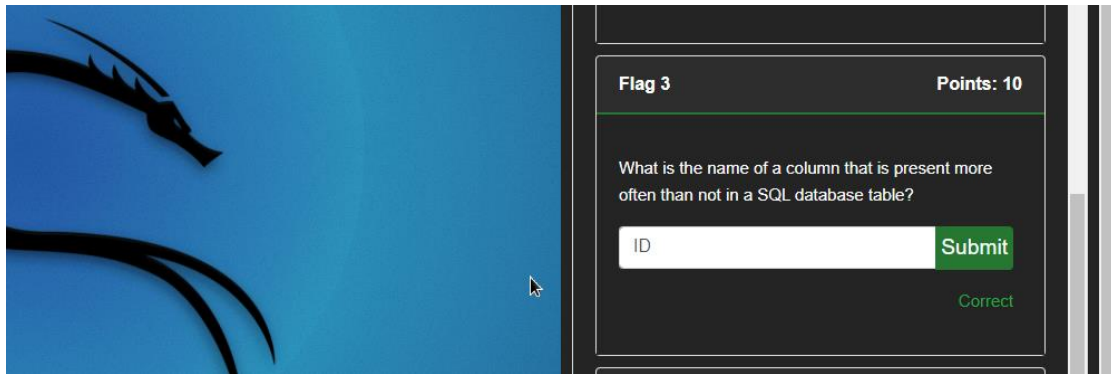
The screenshot shows the 'Flag 2' challenge. The question is 'If the action we wanted was to "Retrieve" data from the database, which operation would we write at the start of the SQL command?'. The answer 'SELECT firstName From users WHERE id=1' is entered in the input field. The 'Submit' button is highlighted in green, and the status 'Correct' is shown below it.

Flag 2 Points: 5

If the action we wanted was to "Retrieve" data from the database, which operation would we write at the start of the SQL command?

SELECT firstName From users WHERE id=1 Submit

Correct



The key difference between a spreadsheet and a SQL database is that SQL Databases are 'relational' meaning that one table can have a relationship to information in another table and this is why every entry into a database must have at least one column which contains a unique reference to the record in question, this unique value is called a 'Primary Key' and is often created through the use of an 'ID' column.

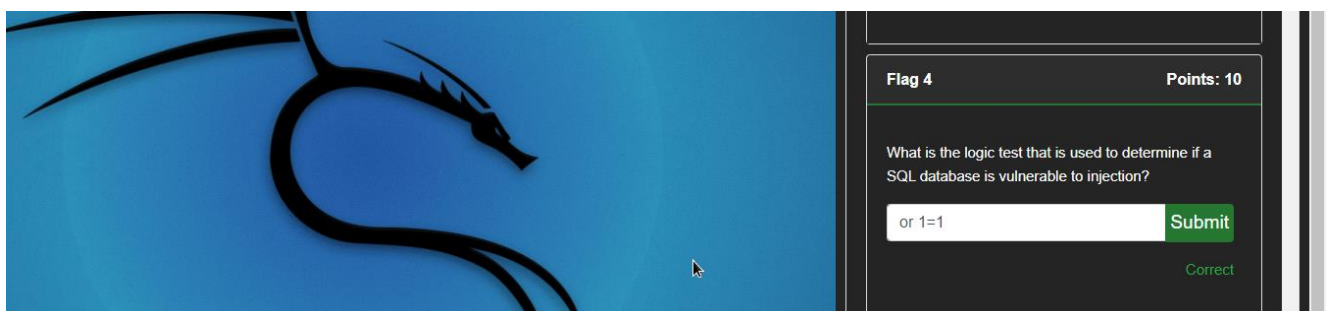
Therefore, if we wanted to retrieve the firstName of a user for which we have the ID, we can add a condition to our example command to request only that single value, as shown below.

```
SELECT firstName FROM users WHERE id=1;
```

**Flag 3- What is the name of column that is present more often than not SQL database table?**

**ID**

**Flag 4 - What is the logic test that is used to determine if a SQL database is vulnerable to injection? or 1=1**



**'OR '1'='1'**

Using the example from above, this would make the query executed on the database appear as below.

```
SELECT name FROM users WHERE id=' OR '1'='1';
```

As the equation 1=1 will always be true, this will then return all names from the database instead of the intended single name. It is important to not that the input starts with a single speachmark but does not end with one. This is because the application code will add the final one for us and we are using the first one to close the parameter that the application is expecting allowing us to add the OR condition to the query.