

HNC Applied Computing

**Network and Cyber Security
Essentials
ACCA4024**

**‘Synthesise a Solution to a Potential
Real Life Problem’**

**Eve Bryan
178197**

7/4/2022

Word Count: 3,129

Table of Contents

o) Introduction.....	4
1) Vulnerabilities, Threats and Attacks.....	4
1.1) Vulnerabilities.....	4
1.2) Threats.....	4
1.3) Attacks.....	5
2) Recommended Techniques.....	6
2.1) Hardware Protection Techniques.....	6
2.2) Software Protection Techniques.....	7
2.3) Importance of Cryptography.....	7
3) Demonstration of Vulnerability Scanning Tools.....	8
3.1) Scanning with NMAP.....	8
3.2) Packet Analysis.....	8
4) Demonstration of Ethical Hacking Tools.....	8
4.1) Metasploit.....	8
4.2) SQL Injection.....	9
5) Importance of Cryptographic Methods.....	9
5.1) Cryptographic Principles.....	9
5.2) Cryptographic Methods.....	9
5.3) Applications of Cryptography.....	10

6) Updated Strategy	10
6.1) Legal Requirements and Impact of Security Breaches.....	10
6.2) Information Security.....	11
7) Recommended Policy Guidelines for ABC Car Rentals	11
7.1) Physical Security.....	11
7.2) Software Security.....	12
7.3) Hardware Security.....	12
7.4) System Security.....	12
7.5) User Security.....	13
8) Appendix	14
9) Bibliography	17

o) Introduction

In this report I will be discussing the possible vulnerabilities, threats and attacks ABC Car Rentals may be prone to, as well as recommending techniques to prevent such attacks. I will also demonstrate vulnerability scanning and ethical hacking tools, and emphasise the importance of cryptographic methods. And finally revising the existing strategy to update ABC Car Rentals IT Security policies.

1) Vulnerabilities, Threats and Attacks

1.1) Vulnerabilities

ABC Car Rentals are vulnerable to threats and attacks in many ways, for example they are connected online with their clients and site offices 24 hours a day. They also use video conferencing facilities, cloud storage and the latest technologies to communicate. This could lead to external threats such as viruses, malware and cyber criminal attacks. ABC Car Rentals existing policies allow staff members, clients and vendors to access their network from any location on any device. This could lead to an internal threat such as unintentional disclosure of confidential client data. Allowing access from external networks via personal devices leaves the company vulnerable to cyber attacks.

1.2) Threats

There are many different kinds of external threats which ABC car rentals could be susceptible to due to the vulnerabilities in their IT security and policies, such as being prone to attacks from cyber criminals or terrorists, which could lead to loss of control when it comes to accessing client data. The cyber criminals could access the system and damage data and software on the computer's operating system by infecting it with viruses. They could also access the system without causing any damage, this is usually caused by hackers who are just curious and want to know what your organisation is doing. "Companies may use hacking for the purpose of corporate espionage, finding out about their competitor's plans, products and finances. While governments may use it for political espionage, spying on their rival countries" [1]

There are also software driven threats which any business can fall victim to as these malicious files can disguise themselves as something completely innocent. These files can then either be downloaded through untrustworthy links, email attachments or when downloading software. These software threats include viruses which can slow down your device and copy your personal and sensitive data.

Worms use infected machines as a host and scan and infect the other computers, They cause harm to the network by consuming bandwidth. Trojan horses attack digital devices from inside and will attempt to destroy the computer by overheating or crashing it. Ransomware is a malicious program that infects a device and holds its data hostage, by encrypting it, then requiring a ransom payment before the victim will be given the decryption key, and can regain their control of their files or data. Spyware is installed without the consent of the user and gathers personal and sensitive information. Adware can be used to take the user to fraudulent websites. Rootkits and Backdoors were created to control a computer, in what is called a botnet, to send massive amounts of junk mail, a Rootkit is used to open a backdoor for hackers to get into the system.

“An internal threat refers to the risk of somebody from the inside of a company who could exploit a system in a way to cause damage or steal data. These kinds of threats are particularly troubling, as employees are expected to be trusted individuals that are granted extended privileges, which can easily be abused” [2]. As ABC Car Rentals does not have the appropriate digital and physical security in place, users could accidentally or on purpose override security controls, which could lead to data breaches. Unintentional disclosure or damage is where an employee could leave a company device open which could lead to confidential information being put into the public domain. Physical damage to equipment is a threat all companies should be aware of, these threats can include, theft of equipment and data or malicious damage caused either by an employee, user or a thief. There are also forces of nature which could destroy important data such as floods, fire or other natural disasters.

“Social engineering refers to the techniques used to deceive people into revealing private and confidential information”[3]. Examples of these attacks included blagging, where the criminal will invent a scenario in order to convince an employee they are someone else. It is used to gain information or access to restricted locations. There are also pharming and phishing attacks which are used to redirect the user to a fake site, deceive them into sharing sensitive information or get them to unknowingly install malware onto their device.

1.3) Attacks

Cyber attacks are assaults from cyber criminals who can target company data and breach the company's network. “If successful, cyber attacks can damage enterprises. They can cause valuable downtime, data loss or manipulation, and money loss through ransoms. Further, downtime can lead to major service interruptions and financial losses” [4]. An active cyber attack is when the hacker attempts to make changes to the target's data. An example of an active cyber attack

is a masquerade attack, where the attacker uses stolen login details to gain access to the system. Another is the man in the middle attack, where the criminal intercepts communication to spy or modify the travelling traffic. Passive cyber attacks are defined by an attacker simply monitoring your communications such as tracking your internet use, reading your emails or using a camera or microphone to spy on you.

A port scan attack is when the attacker finds their target by dispatching packets to ports on a host. Another example of a passive attack is an eavesdropping attack which “occurs when a hacker intercepts, deletes, or modifies data that is transmitted between two devices. Eavesdropping, also known as sniffing or snooping, relies on unsecured network communications to access data in transit between devices” [5]. The impact on a business after becoming victim to a cyber threat or attack can be huge. The consequences of this include operational impact on an organisation, which means the user does not trust the organisation's system, and if their confidence in the system is non-existent, the customer will not buy from your business. There is also a financial impact due to loss of service as well as damage to reputation. Legal consequences of data privacy breaches are serious and could lead to the business receiving a fine.

2) Recommended Techniques

2.1) Hardware Protection Techniques

In order for ABC Car Rentals to avoid these threats and attacks, there are certain hardware networking based protection techniques which can be used. It is important to have a hardware firewall, “A hardware firewall is a physical device responsible for filtering traffic coming to your website. This is achieved by placing a firewall between the uplink and the computer” [6]. This can prevent unauthorised access to a private network. Firewall filtering is used to control network access by monitoring the incoming and outgoing packets; any packets which do not obey the set rules are rejected.

“The Demilitarised Zone is an independent network that acts as a buffer zone between an external network and the internal network” [7]. It is important to protect the connection between the internet and LAN as this is where hackers will try to gain access. A Proxy server is simply a gateway for the user to access the internet, they prevent cyber attackers from entering private networks by mediating between the users and the online websites they visit. Intrusion detection systems are able to identify hacker activity that some anti malware software can miss. It does this by scanning and monitoring the network for suspicious activity.

2.2) Software Protection Techniques

Software protection techniques are just as important as hardware protection, a successful IT system must have at least some of the following policies in place. Antivirus software's primary purpose is to protect computers from viruses, and will also scan and remove any found viruses. Domain management "refers to the domain-wide management of the security aspects of a network. For example, you may use domain management to ensure that users only have certain access rights, and that only company-provided machines are able to connect to the network" [8]. This will help prevent any unauthorised devices connecting to the network as the user will have a domain account instead of individual user accounts.

Other software protection techniques include user authentication, this is where the log on procedure for staff would require a username and a password. When a client attempts to log in to the system they will log on to a domain rather than a local computer. To stop others from guessing a user's password it is important to ensure that all passwords are strong, at least 6 characters long and include special characters. Some operating systems such as Windows provide access controls that can be used to control which users have access to which files. "Every file and every folder in Windows has its own set of permissions. Permissions can be broken down into Access Control Lists with users and their corresponding rights" [9].

To protect the business against social engineering attacks it is important for staff to have an awareness of the risks and good cyber security training. The staff should know not to open emails or click links unless they are from a trusted sender and should also avoid highly tempting offers, "If it sounds too good to be true, the likelihood is that it is" [10]. It is also very important to have good physical security such as on the door to the office building, this is to stop tailgaters entering the building without permission. Staff should also be encouraged to question any person in the office they don't recognise.

2.3) Importance of Cryptography

Cryptography is the method of scrambling data up into unintelligible nonsense, transmitting it to an authorised user and then reverting the code back into plain English. "Cryptography protects the confidentiality of information, confidentiality is a key priority when it comes to cryptography. It means that only people with the right permission can access the information transmitted and that this information is protected from unauthorised access at all stages of its lifecycle" [11]. Therefore using cryptography to send confidential information to colleagues or clients would be extremely useful as there would be no leak of data.

3) Demonstration of Vulnerability Scanning Tools

3.1) Scanning with NMAP

As shown in the appendix I have completed multiple virtualized environments to demonstrate to ABC Car Rentals the purpose of these specific vulnerability scanning tools, NMAP and Wireshark. The first tool used was NMAP, which is an open-source network and security scanning software. NMAP is used to find the real security of a system. To test the system an ethical hacker would be hired by the company to use NMAP to find vulnerabilities in the system and determine if unauthorised access can be gained.

3.2) Packet Analysis

The second software is Wireshark, it is the most frequently used open source protocol analyzer. The main purpose of wireshark is to capture, monitor and analyse any traffic which can then be used to locate problems and their root cause as well as find malicious files. “Wireshark is often compared to a flashlight – a handy tool that lets you see what you're doing more clearly” [12] . It is also used for network troubleshooting, finding out if there are any issues within the network. Wireshark is able to analyse data through a live connection and is able to capture all sorts of traffic from different locations. Wireshark is used by businesses all over the world in order to gain a better insight into the true security of their systems and networks.

4) Demonstration of Ethical Hacking Tools

4.1) Metasploit

As can be seen in the images in the appendix I completed multiple virtualized environments in order to demonstrate to ABC Car Rentals the purpose of ethical hacking tools. Tools such as Metasploit, which is a penetration testing framework that consists of a few different tools which test network security. This allows businesses to employ ethical hackers to use metasploit on their system in order to demonstrate potential security vulnerabilities. It is an open source tool that is free and safe to download and use, it “makes hacking simple. It's an essential tool for many attackers and defenders” [13]. As the business is then aware of the issues that need to be addressed, they are able to fix them, this then makes it harder for real hackers to penetrate their network and system.

4.2) SQL Injection

SQL injection is a security vulnerability scanner which allows the attacker to tamper with the queries an application makes to a database. It can allow the attacker to see data that is not normally available for retrieval, this data can include those belonging to users such as customers or staff. In most cases attackers are able to delete or modify this data which causes constant changes to the behaviour and content of the application. Hackers are also able to perform malicious SQL statements.

5) Importance of Cryptographic Methods

As ABC Car Rentals communicate with their customers and colleagues through video conferencing and online technology such as emailing, they are at risk of private information being intercepted and leaked into the public domain. Cryptographic methods can be important and highly useful when trying to send confidential information between parties. It is an enhanced security technique to stop hackers and other unauthorised third parties from reading and stealing your private messages. Cryptography can reassure clients that their private and sensitive information would remain confidential, as this method reduces the chance of fraud. "Today's enemies are data thieves working to steal your data for profit. If they cannot steal your data and profit from it, they will look elsewhere. Encrypted data represents an insurmountable challenge from which they cannot profit" [14].

5.1) Cryptographic Principles

The cryptography procedure is quite simple. The sender begins by encrypting the message, encryption can either be symmetric or asymmetric. The encrypted message is then sent via the network to the intended recipient. However, before the recipient is able to open and decrypt the message they require authentication, this ensures the receiver that the message actually originated from the sender, and not from a hacker. It is also highly important to ensure that there is no loss of integrity of the messages being sent and encrypted. This means that the message should not have changed in any way during the encryption, transmission and decryption process. Non-repudiation, which is a cryptographic method, also prevents a sender or receiver from making the claim of not receiving or sending a message.

5.2) Cryptographic Methods

Shift ciphers are a cryptographic method, the concept is to simply replace each letter of the alphabet with another letter, it will shift by a fixed number between 0 and 25. This method was used by Julius Caesar to hide messages from his enemies. There are also block ciphers and stream ciphers, which are methods of converting

plaintext to ciphertext, the “main difference between a Block cipher and a Stream cipher is that a block cipher converts the plain text into cipher text by taking plain text’s block at a time” [15].

There are low grade algorithms called ‘cryptographic primitive’ which help cryptographic designers create cryptography systems for security. Another method is one time pads, this technique uses a single key which has been pre-shared and is bigger than the message itself. This method could be used by ABC Car Rentals to send a message which is highly important and will never be sent again. Hash functions are used to convert data from one value to another, which makes it an ideal tool for cryptography. This technique could be used to “encrypt communication between web servers and browsers, and generate session ID’s for internet applications and data caching”[16].

5.3) Applications of Cryptography

Symmetric encryption is an encryption technique that uses a single private key, this means that it is faster and better for encrypting large amounts of data. Symmetric encryption requires key exchanges, as two parties need to have shared their private keys to be able to encrypt and decrypt their message. Whereas Asymmetric encryption is the most common as it is highly secure, this technique uses two keys, one private and one public. HTTPS protocol works on asymmetric encryption, it encrypts messages between two computers, and displays the data in a hypertext style. A digital certificate is used to ensure that the encrypted message has not been altered. They also confirm the details of the sender and receiver, this adds an extra layer of security. HTTPS protocol encrypts messages between two computers, and displays.

A Virtual Private Network (VPN) makes it possible for communication conducted over a network to be private. It does this through encrypting the transmitted data over the public network. Generic routing encapsulation is “a method of encapsulation of an IP packet in a GRE header which hides the original IP packet” [17]. Encryption of data on wi-fi networks is a technique which uses an algorithm to scramble a data signal between devices. This prevents unauthorised access from anyone who may want to read or intercept information sent via a wi-fi connection.

6) Updated Strategy

6.1) Legal Requirements and Impact of Security Breaches

The impact of a data breach on a business can be huge, The Data Protection Act of 1998 governs the processing and handling of data in Britain. This act protects

people from having their personal data mishandled or misused, it does this by establishing rights for the individuals and creates guidelines for the businesses to follow. This means the impact of a data breach can be big, legally. But data breaches can also affect business in other ways, customers and clients need to be able to trust that the information about them stored on your system is secure. If this trust is broken, and customers no longer have confidence, the business can fail. There is also a financial impact after a data breach due to loss of service and the cost of recovering the data.

“The Computer Misuse Act (CMA) was drafted in 1990 as the law governing the way that individuals can lawfully access data on a machine. Crucially, it criminalised any unauthorised access to data and the practice of making modifications to stored information without the permission of the owner”[18]. Consequences of breaking this law could be detrimental to the business. The legal consequences include a fine and possible prison time. Damage to the reputation of the company could also affect clients and their custom.

6.2) Information Security

Information security is a system that ensures data is securely kept and no unauthorised access or changes to the data are made. The data is protected when being sent to a location or machine, and when stored. The CIA triad is a set of core principles that every organisation should adopt. These principles are; Confidentiality, which refers to the efforts the organisation makes to keep data secure and private. Integrity, to ensure the data is authentic and reliable, and Availability which guarantees the user has reliable access to the data and applications they need.

7) Recommended Policy Guidelines for ABC Car Rentals

7.1) Physical Security

To ensure the safety of equipment, networks, software, hardware and staff members. And to stop any physical damage that could cause financial loss or damage to reputation, such as natural disasters, fire, floods and theft.

- Install an ID badging system for all authorised personnel
- Control all physical access to important places with security officers and digital locks such as keypads
- Monitor through the use of CCTV
- Staff must have training on social engineering techniques and know to question anyone they don't recognise
- There must be insurance for all hardware and physical equipment

7.2) Software Security

All software must be protected against malicious attacks and hackers to ensure the software is stable and works consistently under these potential risks.

- Monitor incoming and outgoing connections
- Install software to monitor network traffic
- Install anti-virus and virus detection software such as 'Avast Business Antivirus Pro'
- Create a firewall using software such as 'Sophos Firewall'
- Create a virtual private network (VPN)
- Manage the network domain to prevent any unauthorised devices connecting to the network
- User authentication must be in place for both staff and clients
- There must be access control methods such as user IDs and passwords

7.3) Hardware Security

There must be security in place to ensure the protection of physical devices. This is to protect them from things like unauthorised usage, data exfiltration and malware insertion.

- Install a hardware firewall such as 'Sophos XGS Series'
- Install a server based 'demilitarised zone'
- Install a 'proxy server' such as 'Bright Data'
- Download an Intrusion Detection System such as 'Ossec' which will work with any operating system

7.4) System Security

System security uses multiple types of tools to protect information and data from attacks by hackers and unauthorised access.

- Data access metrics
- Create permissions to stratify access based on user needs
- Track database activity and monitor data access, to record and analyse data usage on the network to see who has accessed what and why
- Build a data log for audit, to use the database activity to reveal any data misuse or intrusion attempts
- Store data safely, have a robust backup strategy including multiple offsite and geographically separate copies
- Cryptography, use encryption techniques such as one time pads, asymmetric encryption for highly sensitive data and symmetric encryption for sending a large amount of data.

7.5) User Security

This will protect the organisation's customers and users from threats as they are using their personal devices.

- Users need to be educated on how to use data securely
- Delete unused data to prevent possible accidental data leaks
- Define data roles and responsibilities to improve clarity for employees and remove confusion

8) Appendix

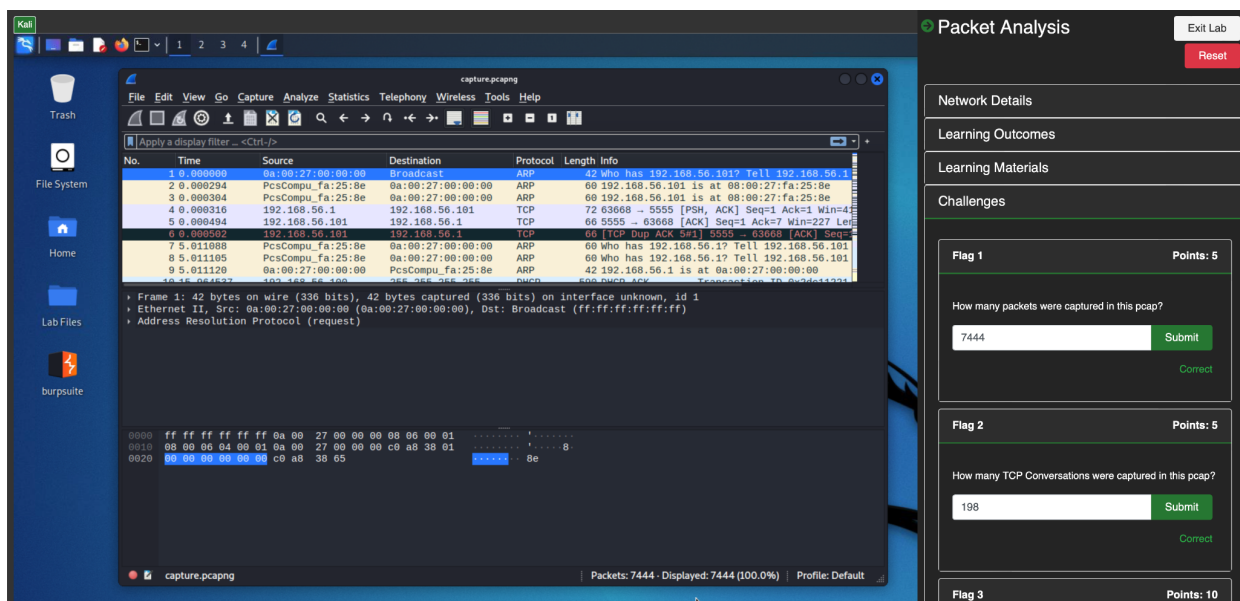
Scanning with NMAP (3.1)

The screenshot displays a virtualized environment with a Kali Linux desktop on the left and a NMAP scanning interface on the right. The terminal window shows the NMAP help text, including options like `--reason`, `--open`, `--packet-trace`, `--iflist`, `--append-output`, `--resume`, `--noninteractive`, `--stylesheet`, `--webxml`, `--no-stylesheet`, `MISC`, `EXAMPLES`, and `SEE THE MAN PAGE`. The NMAP interface on the right has a title bar "Scanning with NMAP" and buttons for "Exit Lab" and "Reset". It contains a "Network Details" section, "Learning Outcomes", "Learning Materials", and a "Challenges" section. The challenges are:

- Flag 1** (Points: 5): Which IP Protocol does not have any error-checking? Answer: UDP. Status: Correct.
- Flag 2** (Points: 5): Of the 65,535 ports, what port is the last of the "assigned" ports? Answer: 65535. Status: Correct.
- Flag 3** (Points: 10): What version of Open SSH is running on port 22? Answer: 7.2p2. Status: Correct.
- Flag 4** (Points: 15): What do you type at the start of your command to do

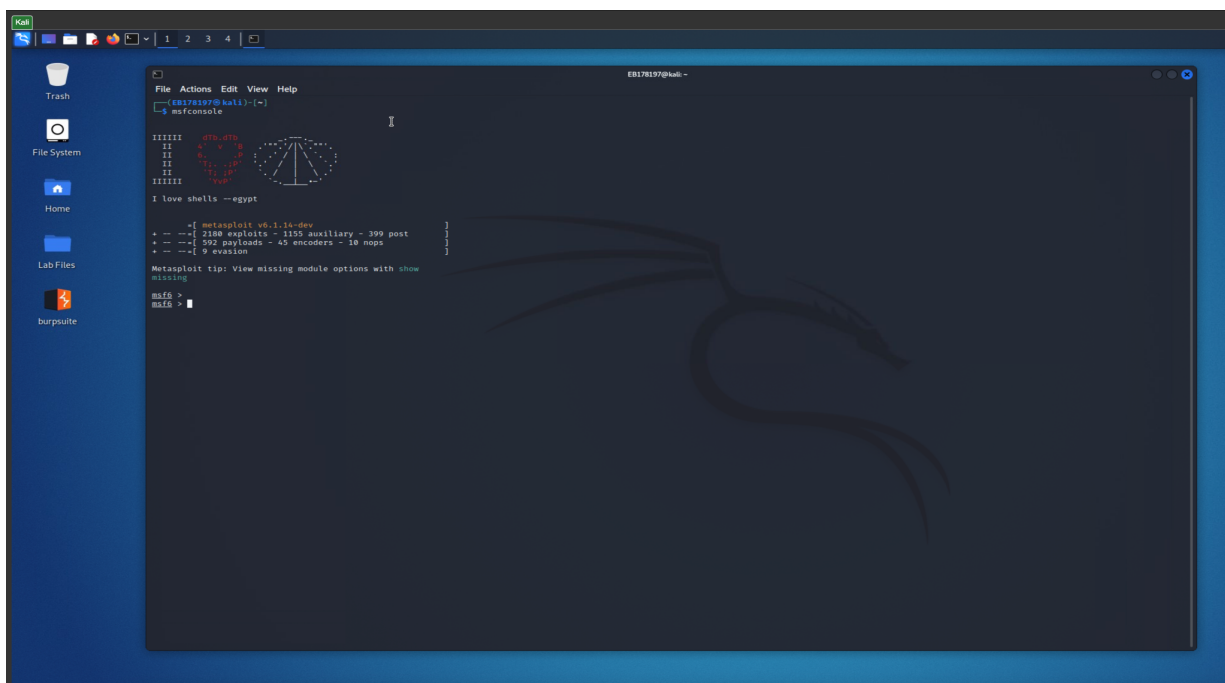
This is a virtualized environment showcasing the use of a vulnerability scanning tool called NMAP which can be used to find vulnerabilities and test the security of the network.

Packet Analysis (3.2)



The second virtualized environment focused on the software ‘Wireshark’. It is used to monitor and analyse traffic, this could then be used to locate any problems.

Metasploit (4.1)



The third virtualized environment used the ethical hacking tool ‘Metasploit’. This software is used to penetrate and test a framework to allow businesses to find potential security vulnerabilities.

SQL Injection (4.2)

The screenshot displays a Kali Linux virtual machine environment. On the left, a sidebar contains icons for 'Trash', 'File System', 'Home', 'Lab Files', and 'burpsuite'. The main area is a terminal window titled 'EB178197@kali: ~' showing the help text for the 'mdb-sql' tool. The help text includes 'Usage: mdb-sql [OPTION?] <file> - Run SQL', 'Help Options: -h, --help', and 'Application Options: -d, --delimiter, -p, --no-pretty-print, -H, --no-header, -F, --no-footer, -i, --input-file, -o, --output-file, --version'. On the right, a panel titled 'SQL Injection' contains a sidebar with 'Exit Lab', 'Reset', 'Network Details', 'Learning Outcomes', 'Learning Materials', and 'Challenges'. The 'Challenges' section shows two challenges: 'Flag 2' (Points: 5) and 'Flag 3' (Points: 10). 'Flag 2' asks for the operation to retrieve data from a database, with the correct answer being 'SELECT'. 'Flag 3' asks for the name of a column present more often than not in a SQL database table, with the correct answer being 'ID'.

```
$ mdb-sql -h
Usage:
mdb-sql [OPTION?] <file> - Run SQL

Help Options:
-h, --help                Show help options

Application Options:
-d, --delimiter            Use this delimiter.
-p, --no-pretty-print      Don't pretty print
-H, --no-header            Don't print header
-F, --no-footer            Don't print footer
-i, --input-file           Read SQL from specified file
-o, --output-file          Write result to specified file
--version                 Show mdbtools version and exit
```

SQL Injection Exit Lab Reset

Network Details

Learning Outcomes

Learning Materials

Challenges

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?

Submit

Correct

Flag 3 Points: 10

What is the name of a column that is present more often than not in a SQL database table?

Submit

Correct

The final virtualized environment involves using an ethical hacking tool called 'SQL' (security vulnerability scanner). This tool allows businesses to modify and retrieve data.

9) Bibliography

- 1) By *Anon*, "How external threats occur," *KnowItAllNinja*, 07-Sep-2018. [Online]. Available: [How External Threats Occur - KnowItAllNinja](#) [Accessed: 07-April-2022].
- 2) *Unattributed*, "What are internal threats examples?," *chetumenu.com*, 2022. [Online]. Available: <https://chetumenu.com/what-are-internal-threats-examples/> . [Accessed: 07-Apr-2022].
- 3) By *Anon*, "How external threats occur," *KnowItAllNinja*, 07-Sep-2018. [Online]. Available: [How External Threats Occur - KnowItAllNinja](#) [Accessed: 07-April-2022].
- 4) *Unattributed*, *What is a cyberattack?* [Online]. Available: <https://www.ibm.com/ae-en/topics/cyber-attack/> . [Accessed: 07-Apr-2022].
- 5) *Unattributed*, "What are eavesdropping attacks?," *Fortinet*, 2022. [Online]. Available: <https://www.fortinet.com/resources/cyberglossary/eavesdropping/> . [Accessed: 07-Apr-2022].
- 6) K. Bali, "What is Hardware Firewall? (Overview & benefits)," *ServerGuy.com*, 21-Apr-2020. [Online]. Available: <https://serverguy.com/servers/hardware-firewall/> . [Accessed: 08-Apr-2022].
- 7) *Unattributed*, "What is a DMZ (demilitarised zone) in networking?," *Information Security Asia*, 26-Feb-2022. [Online]. Available: <https://informationsecurityasia.com/what-is-a-dmz-demilitarized-zone-in-networking/> . [Accessed: 08-Apr-2022].
- 8) "Domain management," *BTEC Computing*, 2022. [Online]. Available: <http://bteccomputing.co.uk/domain-management> . [Accessed: 08-Apr-2022].
- 9) A. Kishore, "How to set file and folder permissions in windows," *How to Set File and Folder Permissions in Windows*, 22-Feb-2019. [Online]. Available: <https://www.online-tech-tips.com/computer-tips/set-file-folder-permissions-windows/> . [Accessed: 09-Apr-2022].
- 10) M. Atamaniuk, "Social Engineering Scams: How to recognize and avoid them," *Social Engineering Scams: How to Recognise and Avoid Them*, 10-Sep-2021. [Online]. Available: <https://clario.co/blog/avoid-social-engineering-attack/#:~:text=How%20to%20avoid%20a%20social%20engineering%20attack%201.remove%20malicious%20programs%20that%20have%20accessed%20your%20data> . [Accessed: 09-Apr-2022].

- 11) N. Morgan, "The role of cryptography in information security," *Triskele Labs*, 2022. [Online]. Available: <https://www.triskelelabs.com/blog/the-role-of-cryptography-in-information-security> . [Accessed: 09-Apr-2022].
- 12) R. Hart, "What is Wireshark – and how does it work?", ProPrivacy, 26-Jan-2021, [Online]. Available: <https://proprivacy.com/blog/what-is-wireshark> . [Accessed: 09-Apr-2022]
- 13) J. M. Porup, "What is Metasploit? and how to use this popular hacking tool," *CSO* , 25-Mar-2019. [Online]. Available: <https://www.csoonline.com/article/3379117/what-is-metasploit-and-how-to-use-this-popular-hacking-tool.html#:~:text=Metasploit%20is%20a%20widel,y%20used%20openetration%20testing%20tool,an%20essential%20tool%20for%20many%20attackers%20and%20defenders> . [Accessed: 10-Apr-2022].
- 14) R. Robinson, "38 million reasons to use cryptography for business," *Security Intelligence*, 11-Nov-2013. [Online]. Available: <https://securityintelligence.com/reasons-encryption-cryptography-for-business/> . [Accessed: 10-Apr-2022].
- 15) MKSo75, "Difference between block cipher and Stream cipher," *GeeksforGeeks*, 17-Nov-2021. [Online]. Available: <https://www.geeksforgeeks.org/difference-between-block-cipher-and-stream-cipher/> . [Accessed: 11-Apr-2022].
- 16) Unattributed, "What is a hash function? definition, usage, and examples," *IONOS Digitalguide*, 14-Oct-2n.d.. [Online]. Available: <https://www.ionos.co.uk/digitalguide/server/security/hash-function/> . [Accessed: 11-Apr-2022].
- 17) A. Sahni, "Generic routing encapsulation (GRE) tunnel," *GeeksforGeeks*, 12-Aug-2020. [Online]. Available: <https://www.geeksforgeeks.org/generic-routing-encapsulation-gre-tunnel/> . [Accessed: 11-Apr-2022].
- 18) J. McCallion, "What is the computer misuse act?," 04-Apr-2022. [Online]. Available: <https://www.itpro.co.uk/it-legislation/28174/what-is-the-computer-misuse-act> . [Accessed: 11-Apr-2022].

