Learning summary report

Table of Content

1. All assignment tasks
    - Task 1.1 P
    - Task 1.2 P
    - Task 1.3 P
    - Task 2.1 P
    - Task 3.1 P
    - Task 4.1 P
    - Task 5.1 P
    - Task 6.1 P
    - Task 8.1 P
    - Task 9.1 P
    - Task 10.1 P
    - Task 3.2 C
    - Task 4.2 C
    - Task 5.2 C
    - Task 6.2 C
    - Task 9.2 C
    - Task 4.3 D
    - Task 5.3 D
    - Task 7.2 D
    - Task 9.3 D
    - Task 4.4 HD
    - All Screen shots of practical and video

SIT182 - Real World Practices For Cyber Security Learning Summary Report

PART ONE: Self-assessment of your learning in SIT182

Please fill the tables below. You may delete tables that are not relevant for your grade.

What is the grade you are applying for?

	Pass (P)	Credit (C)	Distinction (D)	High Distinction (HD)
Self-assessment (please tick>	✓	✓	✓	

Minimum Pass Checklist

Tasks	Included (please tick)	Comments on the quality of your submissions (Optional)
1.1P	X	<My assignments are clear and well-researched. I did most on time some are late. I was unable to complete the 7.1 task due to lack of access to Deakin resources. I believe I deserve a good grade.>
1.2P	X	
1.3P	X	
2.1P	X	
3.1P	X	
4.1P	X	
5.1P	X	
6.1P	X	
7.1P	?	
8.1P	X	
9.1P	X	
10.1P	X	

Minimum Credit Checklist

Tasks	Included (please tick)	Comments on the quality of your submissions (Optional)
3.2C	X	< My assignments are clear and well-researched. I did most on time some are late. I believe I deserve a good grade >
4.2C	X	
5.2C	X	
6.2C	X	
9.2C		

Minimum Distinction Checklist

Tasks	Included (please tick)	Comments on the quality of your submissions (Optional)
4.3D	X	< My assignments are clear and well-researched. I did most on time some are late. I believe I deserve a good grade >
5.3D	X	
7.2D	X	
9.3D	X	

Minimum High Distinction Checklist – All HD task is required to qualify for HD

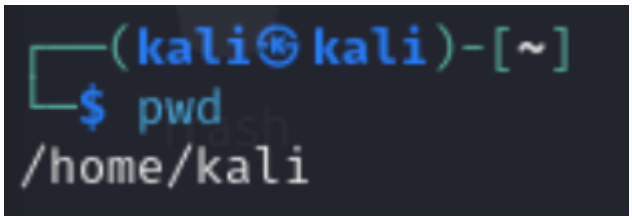
Tasks	Included (please tick)	Comments on the quality of your submissions (Optional)
4.4HD	X	< My assignments are clear and well-researched. I did most on time some are late. I believe I deserve a good grade .One task qualifies for HD. Kindly grade accordingly—HD if deserving, otherwise D.>
8.2HD	-	
10.2HD	-	

PART TWO: Retrospection on your learning in SIT182

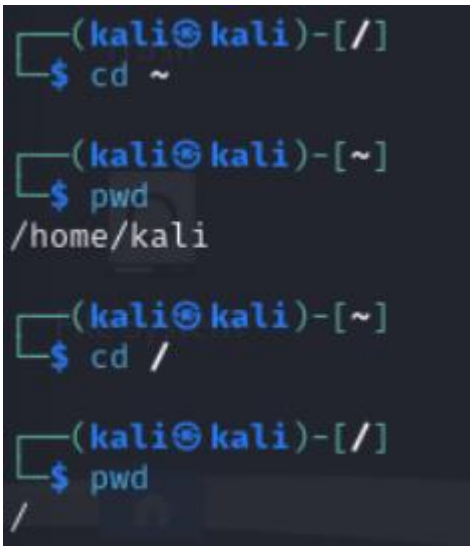
- In retrospect, a pivotal lesson from SIT182 was learning penetration testing. The most challenging aspect was handling the intricacies of 4.4 HD. Notably, working with Wireshark in 6.1 was engaging. The lecture materials and guidance from the lecturer were invaluable throughout. If I were to repeat this unit, I would prioritize hands-on attack simulations for a deeper understanding.

Task 2.1P

Task A1
Answer:



Task A2
Answer:

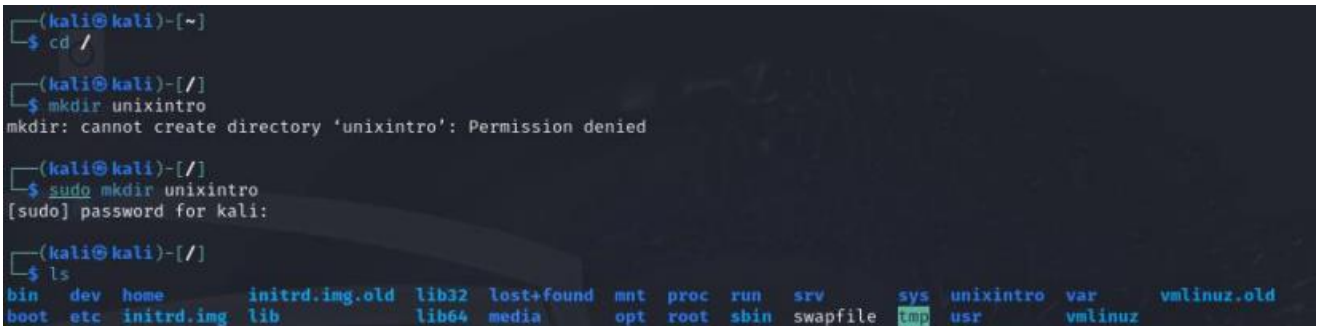


Task A3
Answer:

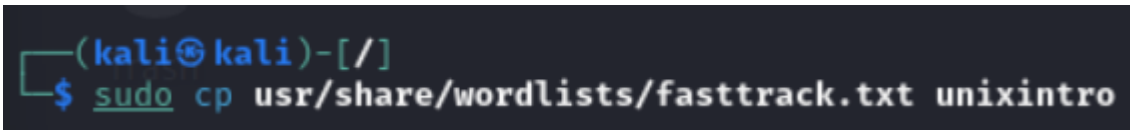
Task A4
Answer:

Task A5
Answer:

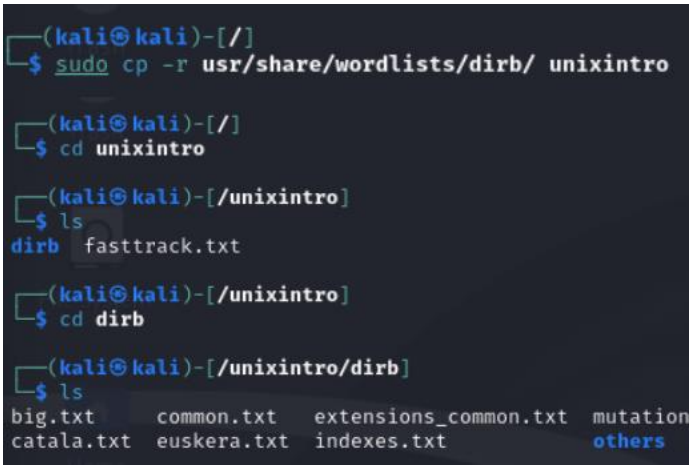
Task B1
Answer:



Task B2
Answer:



Task B3
Answer:



- "cp -r [source-file] [destination-file]" is the new cp command. In Linux, the -r option is used to replicate continuous files; it stands for recursive.

Task B4
Answer:

- "sudo rm [file]" was the command used in section B.
  The contents of the source file will be copied onto a newly created file with a provided destination code file if the destination file referenced by the cp command is not present.

Task C
Search online about Linux Kernel. In your own words (maximum 100 words) discuss what is A Linux Kernel, what does it do, and where does it fit within an OS.

Answer:

- All of a computer's primary operations are managed by the kernel, which serves as the central interface between the hardware and software. The Linux Kernel, the centerpiece of a Linux operating system, is one example of this. Resources management and device management are two examples of traits and features shared by the Linux Kernal and other contemporary operating systems. In addition, the Linux kernel offers the advantage of running virtual machines inside of it, which makes it a highly effective and potent tool in the field of information technology.

Task D
D: List down the new commands that you learned through these tasks so that you can keep it As handy for future tasks.

Answer:

- Rm
- sudo
- ls
- cmv
- pwd
- cp
- clear
- cd

Week 3 task 3.1P

Task 1

a) Explain in your own words about 'Dyre' malware.
- The very sophisticated malware known as "Dyre" was created with the express purpose of breaking into computer systems and primarily targeting users who used online banking services. After being placed on a victim's computer, Dyre functioned covertly and frequently eluded detection by conventional antivirus software. Usually, it used a variety of strategies, such phishing emails or malicious websites, to deceive users into unintentionally downloading and running the virus.
- After being installed, Dyre would record and intercept private data that users entered into banking websites, including account number, login credentials, and personal identity information. Cybercriminals then used this stolen data to send it to distant computers under their control so they could use it for identity theft and other illegal activities that could result in financial benefit.

b) What is a `polymorphic' virus and why Dyre is a polymorphic virus?
- Malware that is capable of altering its look or code whenever it infects a new file or system is known as a "polymorphic" virus. Because of its capacity for mutation, antivirus software finds it difficult to accurately identify and remove the infection. The polymorphic features of the Dyre malware helped make it resistant to conventional security methods.
- Dyre may avoid detection by antivirus tools that used static signatures or patterns or identify malicious software by continuously altering its code or structure. Dyre's capacity to adapt allowed him to carry out his harmful operations and infect systems repeatedly, endangering both people and companies.

c) What type of malware is Dyre?
- One classifies the Dyre malware as a Trojan. When attachments with the dangerous Trojan are emailed to victims directly via spear-fishing techniques. As soon as the receivers select the attachment. The system is infected with the Dyre Malware.

d) What is Dyre's payload? What threat does it pose to a victim?
- The main malicious components in Dyre's payload were those meant to steal sensitive data, including financial information and banking passwords. The primary risks that dyre presents to its victims are as follows:
  - ✓ Information Theft
  - ✓ Credential Harvesting
  - ✓ Financial Fraud
  - ✓ Identity Theft

Task 2

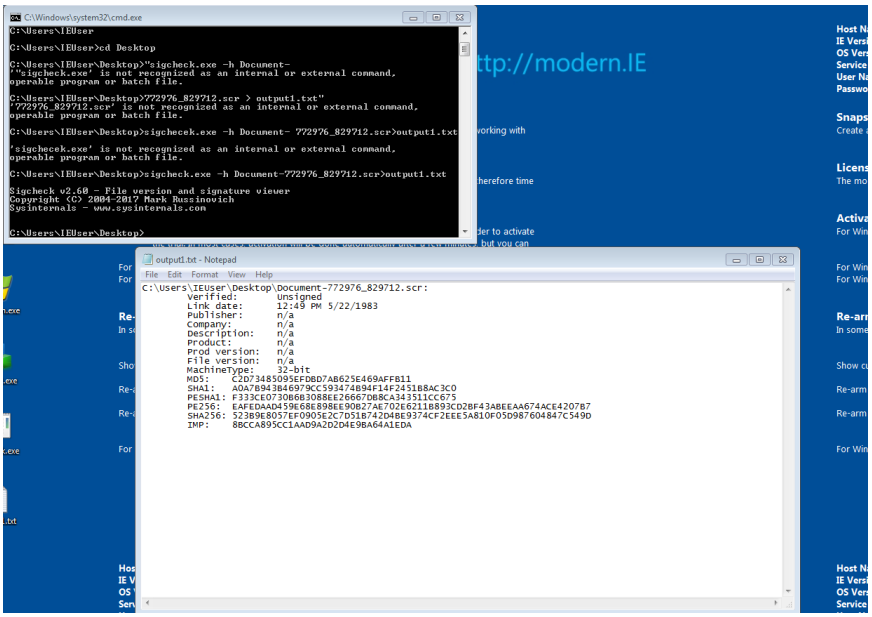
a) What is a `Hexadecimal'
- A "Hexadecimal" is a 16- digit number system that represents values ranging from 0 to 15. Its main applications are in networking and computing.

b) What does the `MZ header' indicate?
- In the Windows and DOS operating systems, executable files start with a data structure called the "MZ header." It bears the name mark Zbikowski in Honor of one of the DOS developers. Executable files are recognized and validated using the MZ header. Usually, it is composed of a fixed-length structure that holds data like the executable's size, the first instruction pointer, and the signature "MZ" which indicates that the file is in the executable format.

Task 3

a) What does the command `sigcheck.exe' do?
- A command-line tool called "Sigcheck.exe" was created by Sysinternals, a company that is now a division of Microsoft. Verifying file signatures on files like executables, drivers, and DLLs, is its main function. Among its many functions, This program can determine whether a file has been digitally signed, show comprehensive information regarding digital signatures, and software developers frequently utilize it to guarantee the authenticity and integrity of files on Windows systems.

b) Include a screenshot of the content of "output1.txt" file on Windows 7 VM Desktop – hint: you can use your host OS screenshot tools to capture.



Task 4

a) Why a second process is added by `Dyre'?
   - In order to accomplish process hollowing, a method for avoiding detection and complicating analysis, the Dyre virus introduces a second process. Process hollowing is a technique whereby Dyre first establishes a valid process in a suspended state, after which malicious code takes over the legitimate process's memory. This enables the malware to operate in the shadow of a genuine process, evading detection by security software that may be keeping an eye out for unusual activity.

b) What does it aim to accomplish?
   - The Dyre malware uses process hollowing and the addition of a second process to achieve a number of goals;
     - ✓ Evasion of detection: Dyre can avoid being discovered by security solutions that depend on identifying suspicious processes by executing malicious code inside the framework of a genuine process.
     - ✓ Persistence: This method aids in the malware's continued presence on the compromised machine. Because the malicious code is injected into what seems to be a legal process, security defenses are less likely to detect it and terminate it
     - ✓ Privilege Escalation: the malicious code can run with elevated rights if the genuine process that is hollowed out has higher privileges.

Task 5

a) What is the path where googleupdaterr.exe is stored?
   - "C:\Users\IEUser\AppData\Local\googleupdaterr.exe"

b) How does this hash stored in output2.txt compare with the hash stored in output1.txt what does the comparison indicate?
   - Although output1.txt mentions the digital footprint, output2.text states that no matching files were discovered.

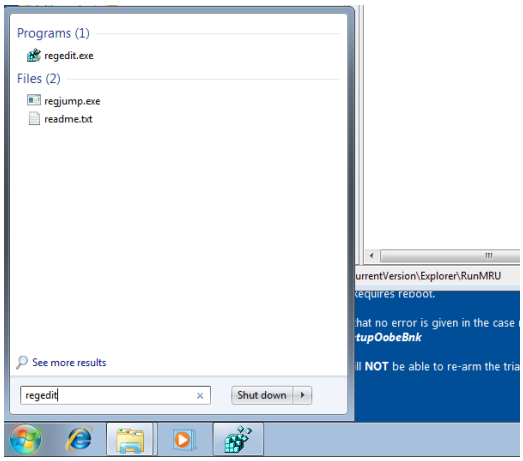
Task 6

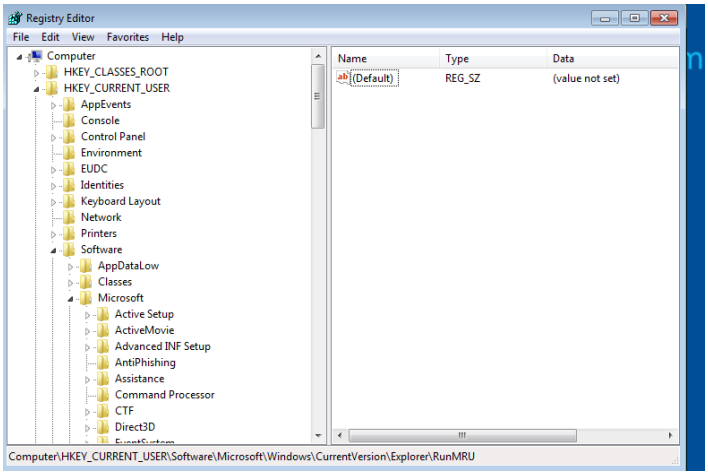
a) What is `Windows Registry? What is it used for?

- Applications that choose to use the registry as well as configuration settings and options for the Windows operating system are kept in a hierarchical database called the Windows Registry. It includes settings and data for the majority of non-operating system applications, hardware, and operating system software.
- The Windows registry has a number of important applications, some of which include;

  - ✓ Configuration: It houses the operating system and application configuration parameters. This covers user preferences, system settings, hardware settings, and more.
  - ✓ The System Information section contains details about the hardware, installed software, device drivers, and system resources of the computer.
  - ✓ Customization: To alter the way the operating system and installed software behave, users and applications can change registry settings.
  - ✓ System Optimization: To improve system speed or fix problems, advanced users and system administrators can adjust registry settings.
  - ✓ Application Settings: The registry is where a lot of programs keep their configurations and settings. They are able to maintain user settings and preferences between sessions as a result.

b) How do you open Windows Registry in Windows 7 VM? Include screenshot of accessing the Windows Registry.





c) The malware analysis you tried in this task was `Static' or `Dynamic' – justify with reference to Week 2's lecture.
   - We have to run the Dyre malware for this task in order to monitor its behavior with tools like Process Monitor and Regshot. You can keep an eye on the modifications made during the malware's operation with these tools. This challenge also forced us to use a hex editor to examine the malware's code without running it. As a result, we can state that it combines both dynamic and static

Task 7

a) The ransomware attack covered in the article makes use of a cutting-edge method to avoid being discovered by conventional security measures. On the victim's computer, the attackers set up a virtual machine and use this controlled environment to run the ransomware. By doing this, the ransomware works without the host computer's security software noticing it and may not check what happens inside the virtual machine. This technique makes the ransomware a complex and difficult threat to counter since it enables it to encrypt the victim's files without interruption.

b) Reflection: Write a paragraph (100-200 words) summarizing what you learned in this week's task. How did task 3.1P complement the lecture content in Week 2?
   - I learned how to analyze malware practically this week, which was a great supplement to the academic material we studied in class. The practical exercises comprised configuring a virtual computer, executing malware securely, and analyzing the Dyre malware's activity with tools like Process Monitor, Sigcheck, and Regshot. My comprehension of important ideas, such as the distinction between static and dynamic analysis, the significance of isolating malware in a controlled environment, and the particular methods malware uses to penetrate and modify system resources, was strengthened by this hands-on approach.
   - I gained knowledge about the polymorphic nature of the Dyre malware, how it starts new processes, and the kind of payload it delivers by dissecting it. Hex editors and process monitoring tools were used to gain insight into the malware's low-level actions. Furthermore, the comparison of registry modifications made prior to and following malware execution using Regshot demonstrated how malware can modify system settings in order to remain persistent or inflict harm.
     Overall, this exercise demonstrated the value of a careful and rigorous approach to cybersecurity malware analysis. It underlined the importance of being watchful and having the skills necessary to identify and evaluate hostile activity using a variety of tools and procedures.

Week 3 Task 3.2C

Task 1

a) Y2K Millennial reflections on computers as infrastructure.pdf Using the above paper and your own research, answer the following questions In your own words (up to 200 words), summaries Y2K.

- The way early computer systems maintained dates let to a severe problem known as the year 2000 problem, sometimes known as the millennium Bug or Y2K. In the early days of computing, memory was a valuable resource, thus programmers used two numbers to represent the year such as “99” for 1999.concerns about these systems misinterpreting the year 2000 as 1900 rather than 2000 as 2000 drew nearer intensified as it seemed more likely that massive system failures would result. These malfunctions could have unanticipated and perhaps disastrous effects on a number of vital infrastructures, such as the military, banking and transportation networks.

  Businesses and governments throughout the world scrambled to find and address Y2K-related problems in their embedded systems and software as the year 2000 drew closer. The problem was enormous in scope, encompassing millions of lines of code and multiple legacy systems, many of which lacked original programmers or had little documentation. Estimates of the cost of the remediation project worldwide approach billions of dollars.

  The transition to the year 2000 happened with very few major events, despite the anxieties and extensive preparations. This was partly because of the extensive efforts made to handle the issue in the years preceding the century.

  (203 words)

b) Was Y2K a malware? Support your answer with a short answer of up to 50 words (refer to Week 2’s lecture).

- Since Y2K was a bug in how dates were represented in computer systems and was not purposefully made to cause harm, it is not regarded as malware. Malware, on the other hand, is specifically created to harm or interfere with systems.

  (41 words)

c) Was Y2K a computer security problem? (refer to Week 1's lecture where we define what is a computer security problem) Support your answer with a short answer of up to 100 words.

- No, there was no computer security issue with the Year 2000 problem. Threats like illegal access, data breaches, or virus attacks—which purposefully damage systems by taking advantage of vulnerabilities—are examples of computer security issues. The widespread usage of two-digit year formats in date fields contributed to the Year 2000 problem, a technological issue that might have resulted in data processing issues when the year 2000 arrived. It was an anticipated, systemic issue that didn't involve criminal intent or the exploitation of security flaws but nevertheless needed to be fixed.

(90 Words)

Task 2

a) What type of malware was WannaCry? Support your answer referring to Week 2's lecture (i.e., it's X given that ...)
   - WannaCry was classified as a crypto-ransomware that relies on worms. This classification is based on how it behaves and functions:

     ✓ Ransomware: This type of malware essentially prevented users from accessing their own data by encrypting the files on compromised systems and requesting a Bitcoin ransom to unlock the decryption key.
     ✓ Worm: It possesses a worm component that enables it to propagate through networks on its own without human assistance. It used a Windows SMB (Server Message Block) protocol vulnerability known as EternalBlue to spread swiftly and autonomously amongst computers on the same network.

b) Could WannaCry move across different machines? Support your answer with up to 100 words.
   - Indeed, WannaCry could spread among various computers. It dispersed independently between machines connected to the same network by taking use of an EternalBlue vulnerability in the Windows SMB (Server Message Block) protocol. Because of its worm-like characteristics, WannaCry spread quickly and without the help of users, infecting other weak systems after it had taken control of one. Its impact was amplified by its mobility across computers and networks, which resulted in widespread infections throughout the world.

     (76 words)

c) How does WannaCry ensure persistency on a machine that has infected? (i.e., what actions does WannCry take to achieve persistency on victim machine) List the tools from Task 2.1P that you could use to detect each action. (Up to 200 words)
   - WannaCry makes sure the ransomware is persistent by generating a Windows registry key that permits it to execute at system startup. At "HKCU \Software \Microsoft \Windows} \CurrentVersion\Run\vyzrjjjywpoefn971," WannaCry generates a registry key. The last portion of the key is a randomly generated identifier that is specific to each compromised machine. This key ensures persistency by allowing the ransomware to run every time the machine reboots.
   - There are several scanning techniques to find such a worm;

     ✓ Process Monitor: Used to track and record activity on the file system in real time. It lets you keep an eye on processes, CPU use, memory, and other things, so you can identify any unusual spikes in memory usage. The Linux CLI's "htop" command can be used to access it.
     ✓ Wireshark is a vital tool for network traffic monitoring in order to identify unusual patterns or connections, like the ones that WannaCry used to compromise compromised servers. This can assist in determining the ransomware's communication efforts.

     (161 words)

d) Is Kali Linux vulnerable to WannaCry? Support your answer by referring to characteristics of the malware as discussed in question 2.c (up to 100 words)

- No, WannaCry cannot infect Kali Linux. WannaCry targets Windows operating systems in particular by taking advantage of the EternalBlue vulnerability in the Windows SMB (Server Message Block) protocol. Kali Linux does not support the Windows SMB protocol in the same way as Debian because it is built on Debian and uses a different kernel architecture and protocols; as a result, the EternalBlue exploit cannot be used with Kali Linux. Furthermore, WannaCry's registry key persistence technique only works with Windows and is incompatible with Linux systems.

(85 words)

e) If victims paid the ransom to hackers, could they unlock their machine? (~50 words)

- It was not a guarantee that victims could unlock their computers even after paying the ransom to the hackers. Numerous victims who paid the ransom either did not receive a working decryption key or received one that was inoperable, underscoring the dangers associated with dealing with ransomware operators and the unpredictability of criminals' demands.

(54 words)

f) Without paying ransom to hackers, was it possible to decrypt the encrypted content of victim’s machine? If so, what made that possible? (~50 words)

- It was true that in certain circumstances it was feasible to unlock the encrypted data on a victim's computer without having to pay the ransom. The usage of static keys or the discovery of decryption keys still in memory on infected systems were two examples of the vulnerabilities in WannaCry's encryption implementation that were exploited by security researchers' tools, which permitted this.

(62 words)

Week 4 Task T4.1PA

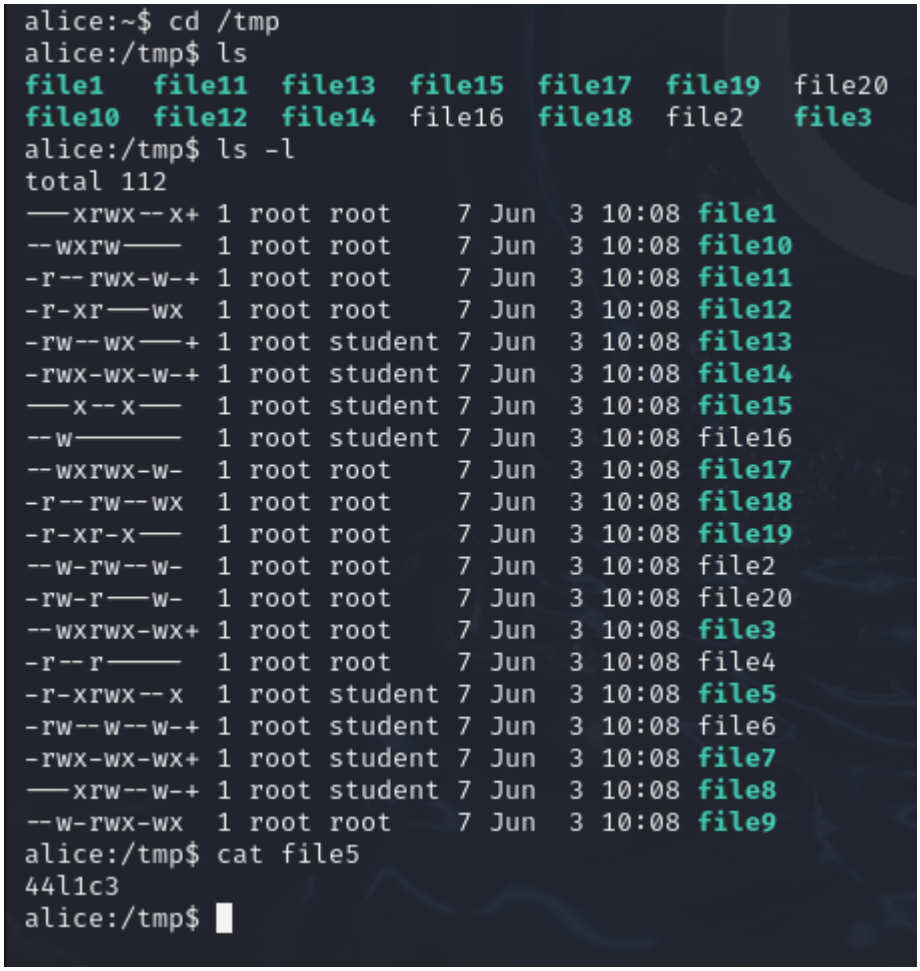
Answer the below questions

1. Question 1:
   a. What is a Docker? How it is different from a Virtual Machine?
      - With the help of Docker, programs and their dependencies can be packaged into lightweight, portable containers that share that operating system of the host system. Containers are resource-efficient and start up rapidly. In contrast, virtual machines (VMs) are more resource-intensive, heavier, and require a longer startup time because they come with an entire operating system installed. Because they come with an entire operating system installed. Because each virtual machine runs independently with its own operating system, they offer strong isolation. Docker containers ensure constant performance by being easier to migrate between environments.

   b. Include a screenshot confirming that you have managed to create the docker image, build it and get an “alice” shell (by following the readme file in Access Control folder).

2. Question 2:
    a. What does the “sudo” or “su” command do?
        - While the `su` command requires the password of the current user to convert to a different user account typically the root user the `sudo` command enables you run specified commands with superuser (admin) capabilities using your own password. `su` grants complete access to another user’s environment, but `sudo` is more secure and logs every command.

    b. Include the screenshots of all commands that you have used to complete the Challenge 1. List the password that you obtained in Challenge 1.

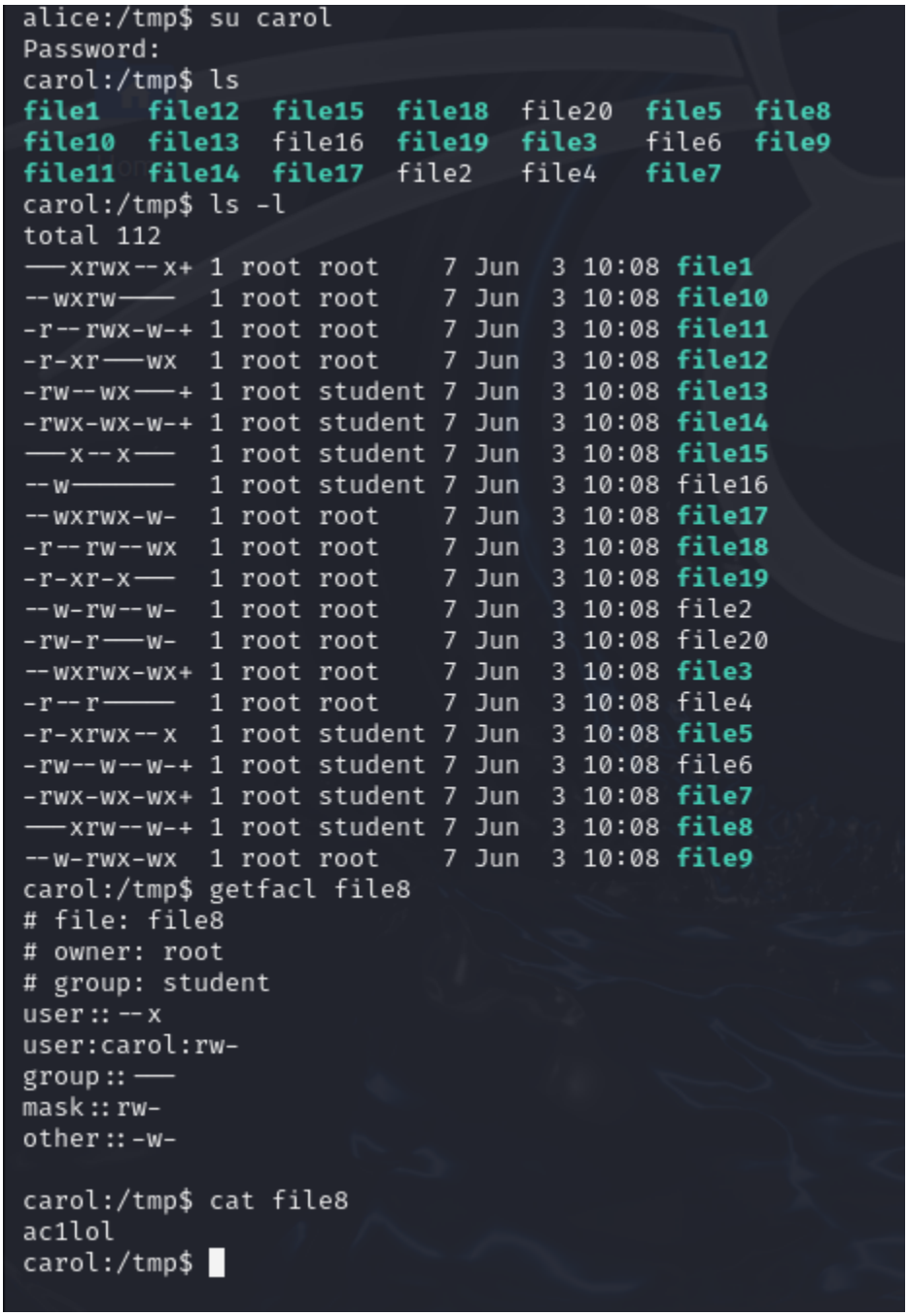


3. Question 3
    a. What does the command “ls -l” do?
        - The command is –l provides a full list of all the files and folders in the current directory, including information on their size, modification date, owner, group, permissions, and filename.

    b. What is the command to set -rwxr-xr-x permissions to myfile? (Make sure to include the exact command including any spaces).
        - In Unix/Linux, the chmod command is used to modify a file or directory’s permissions. It adjusts permission levels for the owner, group, and others, changing who may read, write, or execute the file.

    c. What is the command to set -rwxr-xr-x permissions to myfile? (Make sure to include the exact command including any spaces).
        - chmod 755 myfile

4. Question 4
    a. Look for a file in /tmp/ that is accessible by carol. It contains the password. Include the screenshots of all commands that you have used to complete the Challenge 3. List the password that you obtained in Challenge 3.



5. Question 5
    a. In a paragraph (up to 200 words) summarize what you understood about SUID permission and capabilities as covered in Challenge 4. This need so be in your own words. (i.e., no direct quotes).
        - Programs that have SUID (Set User ID) permission can operate with their owner's privileges instead of the person carrying it out. This is required for some system utilities that demand elevated privileges. An executable belonging to user "alice" with SUID set, for instance can be used by user "bob" and continue to function with "Alice" benefits. To accomplish this, use the command "chmod 4755 filename" to set the SUID bit. This modifies the file's permissions such that an "s" appears where the owner's executable bit should be. However, because of certain weaknesses, SUID can dangerous, especially when applied to root. Privilege drop is a strategy used to reduce this, Privilege drop is strategy used to reduce this, where the software runs with elevated privileges for only the essential actions before dropping them. Furthermore, Linux Capabilities provide a more precise permission system that lets programs be given particular rights without giving them complete, the "cap_net_raw_" capability can be provided to allow raw network activities instead to setting SUID root for the "ping" command, restricting the scope of elevated privileges and improving security

6. Question 6
    a. Is the following statement True or False? `Sticky bit is a special permission that can be assigned to a file'.
        - False

    b. Is the following statement True or False? `An executable file has SUID permission set. When the file is executed on the system, the user who runs the file becomes the file's temporary owner'
        - False

    c. You just created a new script file named myapp.sh. However, when you try to run it from the command prompt, the bash shell generates an error that says -bash: ./myapp.sh: Permission denied. Which command will fix this problem?
        - chmod +x myapp.sh

    d. A file named sit182.txt has a mode of rw-r--r--. If arash is not the file's owner and is not a member of the group that owns this file, what can he do with it?
        - He can read the file but cannot write to it or execute it. Since others have only permission to read

    e. A file named Google Class Room.ppt has a mode of rw-r--r--. If chang-tsun is the file's owner, what can hedo with it?
        - He can read and write the file

7. Question 7
    a. If you wanted to have a data file that you could read or write, but don't want anyone else to see, the permission would be.....(answer using the 9-bit e.g. -r--r--r--)
        - -rw----------

    b. If the file is owned by the user, the.....permission determine the access. (fill the blank either with OWNER/GROUP/OTHER)
        - OWNER

    c. If the group of the file is the same as the user's group, the..... Determine the access. (fill the blank either with OWNER/GROUP/OTHER)
        - Group

    d. If the user is not the file owner, and is not in the group, then the ..... is used. (fill the blank either with OWNER/GROUP/OTHER)
        - Other

8. Question 8
    a. Reflection point – What did you learn that was new to you? How did you manage to learn about UNIX permissions to complete this task? Did you primarily use the Help Video and textbook provided or used your own resources?
        - I gained knowledge about the complexities of UNIX file permission – including the application of unique permission like SUID, SGID, and the sticky bit – by finishing this work. I was unfamiliar with these ideas, so seeing how they were used in various contexts strengthened my understanding of Unix/Linux access control techniques. I mostly used my resources, practice in the terminal, and the challenges to learn about UNIX permission. Understanding how to utilize permissions in practical situations was made easier by the examples' practical and visual presentation of topics. I then used what I had learned, practiced using the terminal, and did more research by consulting the Linux handbook. This method guaranteed a thorough comprehension and the capacity to do the associated responsibilities efficiently. Together, these resources improved my educational experience by increasing the accessibility and usefulness of the process of comprehending and utilizing Unix permissions.

Week 4 – Task 4.2 C

1. Question 1
   a. What are the four principles of authentication? Briefly discuss each of them. (up to 400 words)
      - An essential of information security is authentication, which makes sure that before allowing access to resources, the identities of persons, devices, or systems are confirmed. The four primary tenets of verification are;

✓ **Something you know :**
The user's knowledge is necessary for this principle to work. A password or PIN is the most popular type. This method's security is contingent upon the confidentiality and intricacy of the data. This approach's strengths include its simplicity in terms of execution and comprehension, as well as its ease of changing information in the event that it is compromised. However, because users frequently select weak or simple passwords, it has flaws including vulnerability to phishing, guessing, and social engineering attacks.

✓ **Something you have :**
According to this theory, identity is confirmed using an item the user is in possession of. Smart cards, security tokens, and cell phones that are used to get one-time passwords (OTPs) are a few examples. The advantages of this approach include its capacity to provide an extra degree of security on top of knowledge-based authentication and the difficulty with which attackers can breach the system short of physically stealing the object. The potential for goods to be misplaced, stolen, or damaged, as well as the expense and administrative difficulties involved in organizing and delivering tangible tokens are the limitations.

- ✓ **Something you are:**
  This concept depends on the user's distinct bodily traits, such as voice, facial, or retinal or iris patterns, fingerprints, or retinal patterns. This method's advantages include its high level of security, ease of usage (because users don't need to carry a tangible item or memorize anything), and difficulty in forging or sharing. Nevertheless, shortcomings include the possibility of biometric systems being faked, privacy issues with regard to the usage and storage of biometric data, and the likelihood of biometric recognition errors including false positives and false negatives.

- ✓ **Something You do :**
  According to this theory people can be distinguished from one another by their distinctive behavioral patterns, which could include usage patterns, stride, or typing rhythm. The ability to provide continuous authentication during a session, which adds an extra layer of protection that is challenging for attackers to precisely recreate, is one of this method's features. However, it can be impacted by changes in user behavior. Brought on by stress, injury, or other circumstances. It also requires sophisticated equipment to effectively capture and evaluate behavioral patterns.

b. Give 4 arguments as to why password-based authentication is problematic. (up to 400 words)
   - Despite being commonly used, password-based authentication has a number of flaws that affect both security and user experience. The following four main arguments draw attention to these issues:

   ✓ **Attack-Susceptibility:**
   Password are susceptible to a number of attacks, including dictionary attacks, phishing, brute force attacks, and social engineering. Brute force and dictionary attacks involve the use of software by attackers to repeatedly guess passwords until they discover the right one. Phishing is the practice of using phone emails or websites to deceive consumers into disclosing their passwords. Social engineering uses psychological tricks on people to obtain private data. These attack methods highlight the intrinsic fragility of passwords, especially those that are short and/ or used for serval accounts.

   ✓ **User Conduct and Password Administration:**
   Password security is seriously undermined by human factors. People frequently select simple, easy-to-remember passwords like “password,” “qwerty,” or “123456” Additionally, they frequently reuse passwords on many platforms in an efforts to reduce the mental strain of having to remember numerous strong password. This behavior raises the possibility of a security breach because it can result in the compromise of one account and the illegal access of other accounts. Furthermore, even while changing passwords on a regular basis is a suggested security practice, users frequently acquire predictable patterns as a result, further weakening security.

- ✓ **Difficulties in coming up with Robust Passwords:**

  It is naturally difficult to come up with a strong, memorable password that is hard for hackers to figure out or guess. Generally speaking, long passwords with a combination of capital and lowercase letters, digits, and special characters are considered strong passwords. But because they are difficult to remember, people frequently write down or save these passwords in unsafe places like sticky notes or unencrypted files. The security advantages of using a strong password are compromised by this behavior.

- ✓ **User Experience and Scalability:**
  Users are burdened more and more as service and applications that require password multiply. Password fatigue results from having to deal with so many passwords. Users' overall experience may be impacted by annoyance and inconvenience. Additionally, firms incur higher support expenses and administrative overhead as a results of having to reset passwords owing to forgetting them Complicated password policies and the requirement for frequently passwords changes can increase user annoyance and encourage non- compliance with security protocols.

- In conclusion, even though passwords are still widely used for authentication, there are still a number of problems with them, including scalability concerns, user error, password creation and memory difficulties, and vulnerability to different types of assaults. In order to strengthen security and improve the user experience, these considerations emphasize the need for more user- friendly and safe authentication techniques, including multi-factor authentication (MFA) or password less alternative.

c. Upon graduation, you become a security consultant for a prestigious firm. Your client is the Australian government. They are seeking expert advice about adoption of biometric technology for the mobile app of "my.gov.au". The mobile app allows access and management of your Medicare and Tax. Hence, a large number of users are expected to rely on the mobile app upon introduction to the market. Referring to the 4 requirements offered by Jain and et al., and challenges discussed in Section 29.6, which 2 biometric technologies you think are the best candidate for adoption in the app? Support your answer with arguments (up to 500 words)

- Biometric technology provides safe and practical user authentication, which is essential for app like the myGov mobile app that handle sensitive data like Medicare and Tax. The two biometric technologies that seem to have the greatest chance of being adopted are face recognition and fingerprint recognition. These decisions are based on the four criteria for biometric systems proposed by Jain et al.(universality, distinctiveness, permanence, and collectability), as well as some insights from Section 29.6 regarding biometric problems.

- **Jain et al.'s Biometric Requirements**
  - ✓ **Distinctiveness:**
    Even with identical twins, there is extremely little chance that two fingerprints will ever be exactly alike. When precisely mapped utilizing algorithms, facial traits provide high uniqueness, essentially allowing for individual identification.
  - ✓ **Permanence:**
    Fingerprints are a stable biometric characteristic that don't really over the course of a person's life. Although ageing and other causes might cause changes in facial features, contemporary facial recognition algorithms are resilient enough to accommodate these changes.
  - ✓ **Collectability:**
    The majority of contemporary smartphones have sensors that make it simple to gather fingerprints, making this a speedy and dependable means of authentication. Smartphones come equipped with front-facing cameras which may be used to take facial photographs. This makes the process of gathering facial images simple and unobtrusive.
  - ✓ **Universality**:
    Since almost everyone has a fingerprint and they may be taken from a large population, fingerprints are considered universal. Faces are Omnipresent and identifiable to a wide range of people.

- **Difficulties and Things to Think about from section 29.6**

  - ✓ **Privacy Concerns:**
    Data from fingerprints is regarded as extremely sensitive. To preserve user privacy, secure storage and appropriate encryption are crucial. Faces are very recognizable, which raises privacy concerns. It is essential to make sure that facial data is safety preserved and is only utilized for authentication.

  - ✓ **Security and spoofing:**
    Even though fingerprint sensors are generally safe, lifted prints can be used to fake them. This risk can be reduced by using advanced sensors that can detect liveness. When using images or videos foe facial recognition, there is a risk of spoofing. Nonetheless, 3D sensing and liveness detection technologies greatly lessen these weakness.

  - ✓ **Cost of implementation and technical viability:**
    Economical since fingerprint sensors are widely used in contemporary devices. It is technically possible to implement and integrate it easily with the myGov app. slightly more expensive implementation because of the sophisticated software and camera specifications. Still it's a viable alternative given how common facial recognition technology is in gadgets like iPhone

  - ✓ **User Acceptance:**
    Because fingerprints sensors are widely used in smartphones and fingerprints identification is simple to use, users generally accept it favorably. Because it is non-contact and simple to use, facial recognition technology has also gained popularity, albeit user acceptability may be impacted by privacy concerns.

- For the myGov mobile app, fingerprints and facial recognition both satisfy the requirements of universality, uniqueness, permanence, and collectability. They provide a harmonious blend of technical viability, user-friendliness, and security. While facial recognition gives a noncontact option that keeps up with modern technology advances, fingerprint recognition offer a more developed approach. By implementing these technologies, the myGov app will be more user-friendly and secure, providing safe access to sensitive personal data.

2. Question 2
    a. Reflection point – how difficult or easy did you find reading through the content of chapters. Did you use any of the tips suggested in useful guides in page 2? Share a few words of your experience when working through questions as a note-to-self.
        - Going through the chapters in the textbook was difficult yet educational at the same time. Through the use of AAA principles, they provided a comprehensive overview of the fundamentals of cyber security, which is necessary to understand the field's larger context. I used various recommended techniques, such skimming and creating concept maps, to establish a suitable hierarchy and structure so that I could comprehend the content.

Week 4 Task 4.3D

1. Question
   1: You will need to find a vulnerability in Metasploitable 2 that allows backdoor access (i.e., full shell access) and exploit them through Metasploit running on Kali VM.

   https://www.youtube.com/watch?v=-ExYerSvano&ab_channel=KenishaCorera

   https://youtu.be/-ExYerSvano

2. Question
   How difficult did you find the task? What resources you used to get the task done?

   - Completing this Distinction job was enjoyable and enlightening, and it wasn't too challenging. Even though the method was to test it on a deliberately constructed weak Linux virtual machine called Metasploitable 2, it provided life and perspective to the role of a penetration tester. Utilized for vulnerability testing.

   - I utilized the backdoor exploit VSFTPD 2.3.4. and provided the IP address of metasploitable 2 after getting access to metasploit. I was able to generate a file in the rood file system of Metaspoitable 2, proving that the attack was successful. All things considered, this work was highly captivating and simple to finish, and it provided new avenues for investigation into the topic of cyber security.

Week 4 – Task 4.4HD

1. Question 1
    1. Create a screencast/screen recording (like the one for Task 4.3D) and show the steps you followed to setup Meterpeter on Windows 7 VM. In your screencast, you will need to show all the commands you executed on Kali VM, Metasploit, and the session you establish with the victim.

       https://youtu.be/WW5vkDUHEQU

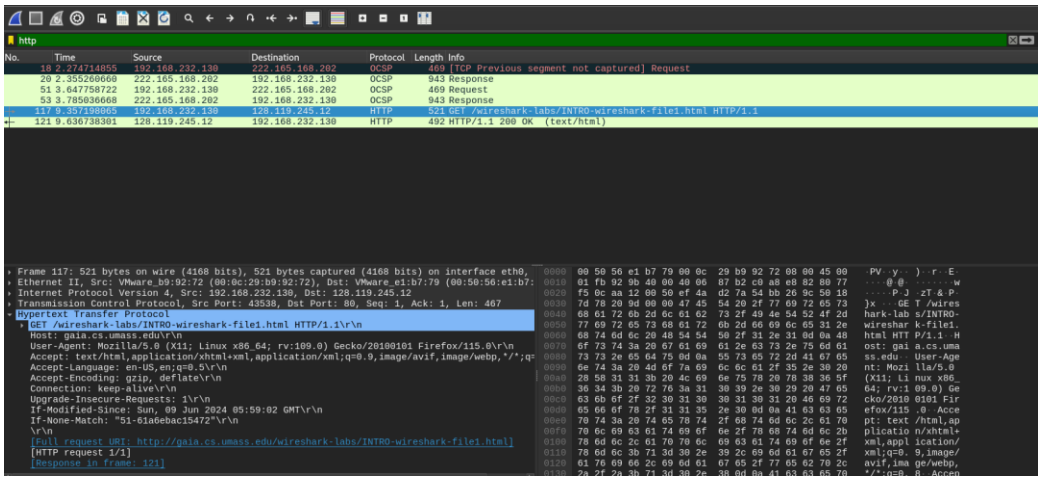
    2. How difficult did you find this task? Was it more challenging compared with Task 4.3D? Are you enjoying pentest activities?

        - This assignment was not as tough as assignment 4.3D, but it was still rather difficult in my opinion. Yes, I'm having fun with pentesting

Week 5 – Task 5.1 P

1. Question1
   a. What is the HTTP version your browser is running?
      - The browser is currently using version 1.1

   b. Include a screenshot of your Kali VM that has the Wireshark window running. Ensure that your screenshot shows that have selected the packet with HTTP GET message and details of the packet are visible either as minimized or maximized.



   c. What is the Internet address of the gaia.cs.umass.edu (also known as www-net.cs.umass.edu)? What is the Internet address of your computer?
      - Source address : 192.168.232.130
      - Destination address : 128.119.245.12

   d. Check the packet details for HTTP Get message (refer to `Details of the selected packet' section of Wireshark window). What type of Web browser issued the HTTP request? Hint: "User-Agent:" field in the expanded HTTP message display. This field value in the HTTP message is how a web server learns what type of browser you are using.
      - User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0\r\n

   e. What is the destination port number (Hint: the number following "Dest Port:" for the TCP segment containing the HTTP request) to which this HTTP request is being sent? What is the source port number?
      - Source Port : 43538
      - Destination Port : 80

2. Question 2
    a. What is HTTP used for in the World Wide Web? At what network-layer is HTTP located?
        - HTTP serves as the foundation for data transmission on the World Wide Web and is used to convey hypertext data in websites. The application layer contains HTTP

    b. What is an HTTP request? What is included in a typical HTTP request?
        - A request for resources sent by the client to the server is known as an HTTP request. A request line, HTTP headers, and a message body make up a standard HTTP request.

    c. What is an HTTP method? How do get and Post methods differ.
        - An HTTP method indicates what should be done with a selector resource.

    d. What is an HTTP response? What is included in a typical HTTP response?
        - A post is used to send data to a server, which has the ability to modify server state, whereas a get is used to obtain data from a server without altering server state.

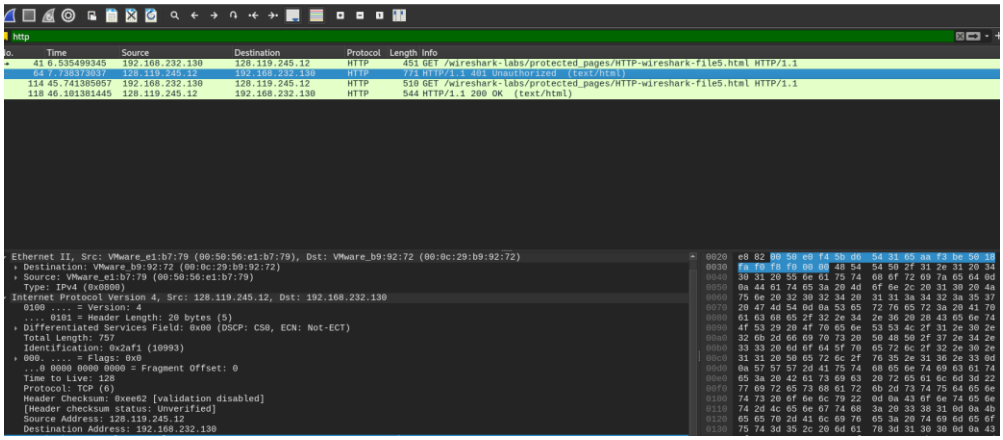
    e. Is HTTP a stateless or a stateful protocol?
        - Due to the server not keeping track of requests, HTTP is a stateless protocol.

3. Question 3
    a. Summarize DoS attack in your own Words
        - An international attempt to stop a specific server from operating server from operating by flooding it with unsanctioned traffic is known as a denial of service (DoS) attack.

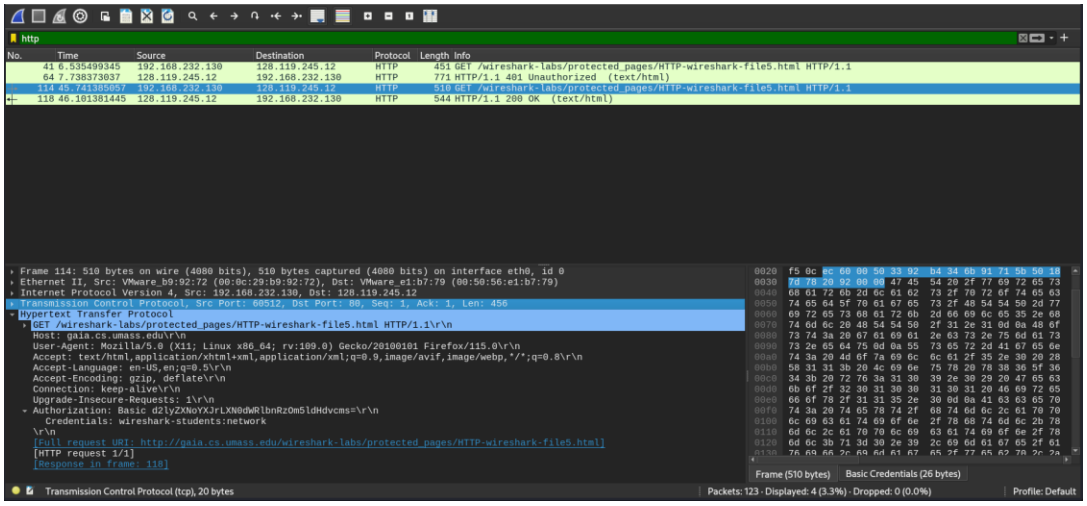
    b. Can HTTP be used to execute a DoS attack?
        - One way to carry out a DoS attack is over HTTP.

4. Question 4
   a. Check the packet details in the middle Wireshark packet details pane. Can you identify the details in Ethernet II / Internet Protocol Version 4 / Transmission Control Protocol / Hypertext Transfer Protocol frames?
      - Yes, the following is what each part shows :
        - ✓ Ethernet II: Shows the MAC addresses of the source and destination.
        - ✓ IPv4: Shows the protocol type, source and destination IP addresses, and other information.
        - ✓ TCP: Shows sequence number, source and destination ports, and other information.
        - ✓ HTTP: Displays the request or answer from HTTP.

   b. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser? (i.e., before you provided the credentials) Include a screenshot of the Wireshark window showing the relevant packet and its details.



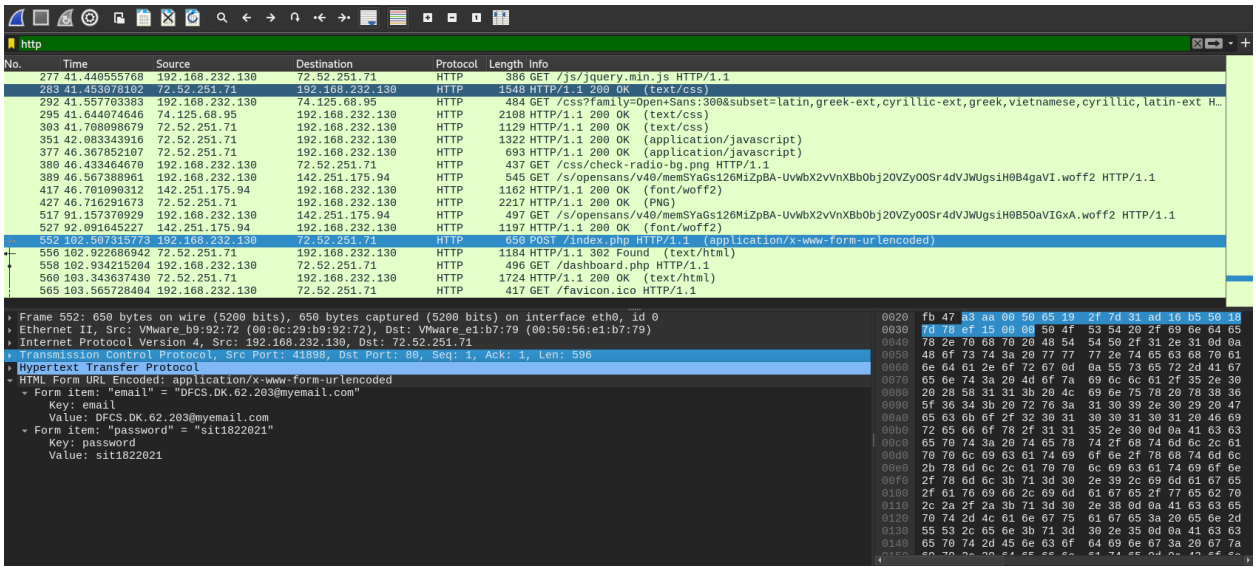
   c. Expand Authorization in Hypertext Transfer Protocol in packet detail section of Wireshark, can you find the username and password are shown in clear text? Include the screenshot



5. Question 5
    a. Was techpanda.org using Base64 encoding?
        - The credential were displayed in clear text since Techpanda was not utilizing base64 encoding.

    b. Did you find the password in an HTTP GET or POST message? Why?
        - Wireshark was able to sniff the packets from the client during the password upload, and the password was discovered through an HTTP Post massage.

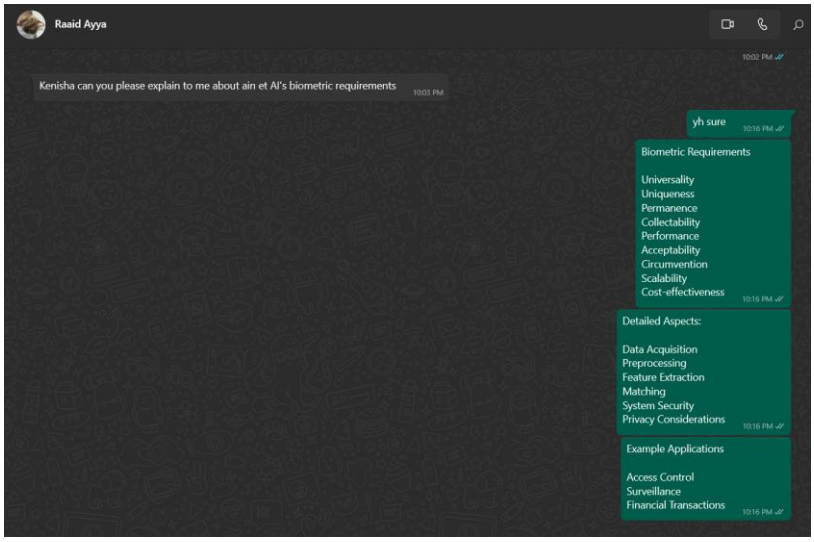
    c. Include a screenshot of Wireshark window that shows the packet with Email and Password you used (i.e. the email and password should be clearly visible in packet details section of Wireshark.)

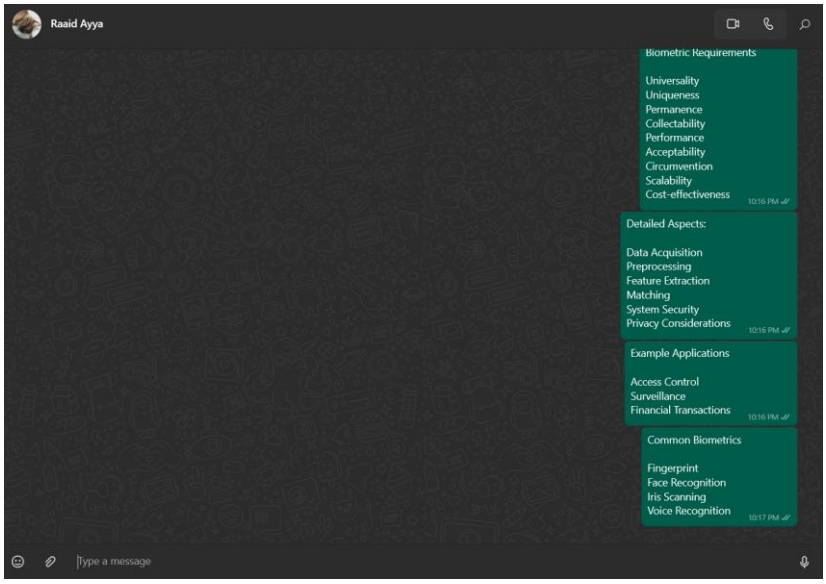


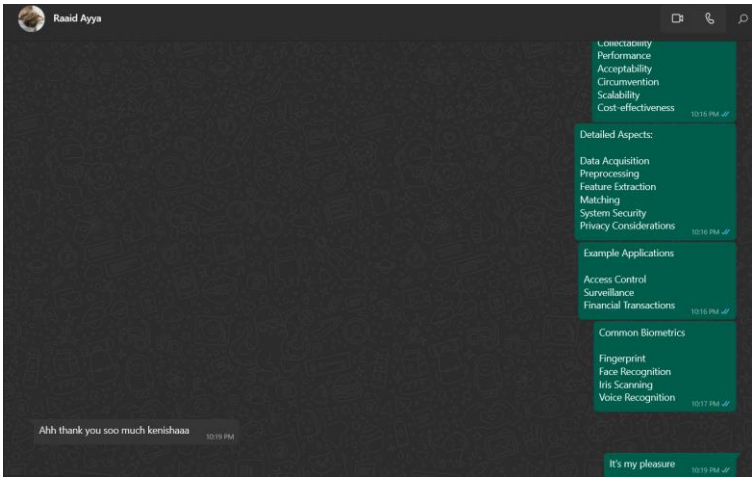
6. Question 6
    a. What did you learn that was new to you? How interesting you find network security compared to other topics covered? How did this task complement the theoretical concepts covered in Week 4 lecture?
        - I learned how to sniff passwords, decrypt Base64 encoding, and trace packets thanks to this task. Overall, this was a well-rounded work that was made much more enjoyable its interests and obstacles.

Week 5 Task 5.2C

- Reflection Report
  - ✓ The necessary conditions for efficient biometric systems are outlined in Jain et al.'s Biometric Requirements. Some of these include collectability (easily measured), permanence (unchanging over time), uniqueness (distinguishing individuals), and universality (everyone should have the attribute). It is important to consider performance factors like speed and accuracy as well as circumvention (resistance to deceit) and acceptance (user willingness). Efficient use of resources (cost vs. profit) and scalability (managing expansion) are also essential. Safe matching, system security, privacy concerns, strong feature extraction, and data quality assurance are essential for dependable and user-friendly biometric applications including banking, surveillance, and access control.







- ✓ In cybersecurity, communication is essential because it makes sure that all parties involved are aware of the threats and ready to react appropriately. Coordinating defenses, exchanging threat intelligence, and quickly managing incident reactions all benefit from clear communication. It encourages teamwork, which makes it possible to quickly identify and mitigate weaknesses. Furthermore, efficient communication lowers the possibility of human error by educating staff members on security guidelines and best practices. Transparent communication during emergencies sustains confidence with partners and clients while showcasing a proactive and conscientious commitment to security.

Week 5 – Task 5.3D

Report

I examined a number of software programs for my assignment, including Nmap, Phonesploit, ADB, and Metasploit, in order to keep an eye on network-connected devices and obtain backdoor access—which is necessary for penetration testing. Phonesploit on a virtual Kali Linux computer was to be used for the purpose. A spare Android phone was attached via USB, its developer settings and USB debugging activated, and its TCP port was altered to "5555". I connected to the victim by figuring out their IP address using Phonesploit. This was a tough yet entertaining experiment that entailed utilizing ADB and Phonesploit to hack into an Android smartphone. In light of ethical considerations, it emphasized how crucial it is to conduct testing on a non-sensitive item and have the owner's consent.

Week 06 – Task 6.1P

Question A:

1. This domain was created in 2020, is this correct? If not, what date was this domain created first?
    - Yes, The creation date of this domain 2020.08.04

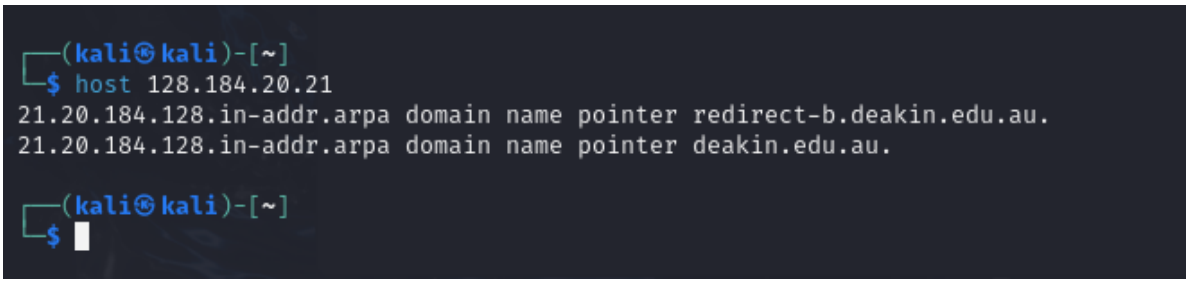
2. When does the registration of the domain expire?
    - The register will expire on 2024.08.04

3. What is a “Name Server” and what is it used for? (Include a reference for your answer) What are the Name Servers for this domain?
    - "Traffic on the internet is organized and routed by name servers." - Forbes
    - Name server – NS1.ATOM.COM
        - NS2.ATOM.COM

4. What is a Registrar? Who is the registrar of this domain?
    - A register is a company or organization that also manages domain name reservation
    - As the IP addresses assigned to those domain names.

Question B:

1. Include a screenshot of the output you get.



2. What is the host command used for? (Include a reference for your answer)
    - In Linux systems, DNS (Domain Name System) lookup operations are performed using the host command. – Geeksforgeeks.

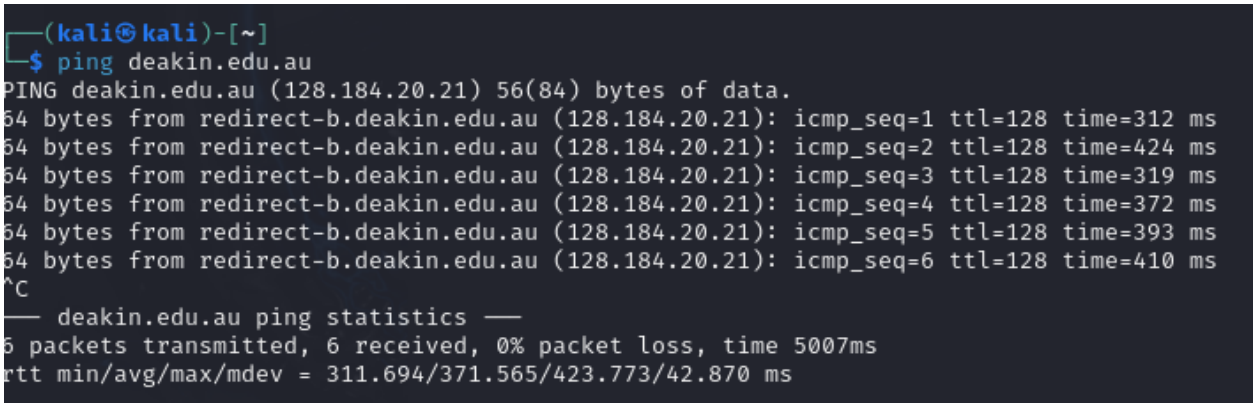
Question C:

1. Include a screenshot of the output you get.

2. What is an MX record in DNS?
    - Email to a mail server is directed by an MX (Mail Exchange) record.

Question D:

1. Include a screenshot of the output you get.



Investigate about ping command and answer the following questions:

2. What is ICMP?
    - ICMP - Internal Control Massage Protocol

3. Fill in the blanks: A correctly-formed ping packet is typically__56__ bytes in size, or__64__ bytes when the ICMP header is considered, and__84__ including Internet Protocol version 4 header.
    - 56
    - 64
    - 84

4. What does `ttl' refer to in the ping command output?
    - The term "ttl" describe the number of network hops a packet has before the router discards it.

Question E:

1. Using the “host” you learned about earlier, find the IP address for localhost. What is the IPv4 address for localhost?
    - 127.0.0.1

2. Do you need Internet access to retrieve the “localhost” domain?
    - The localhost domains can be retrieved without internet connectivity because it is a network address that belongs on your own device.

Question F:

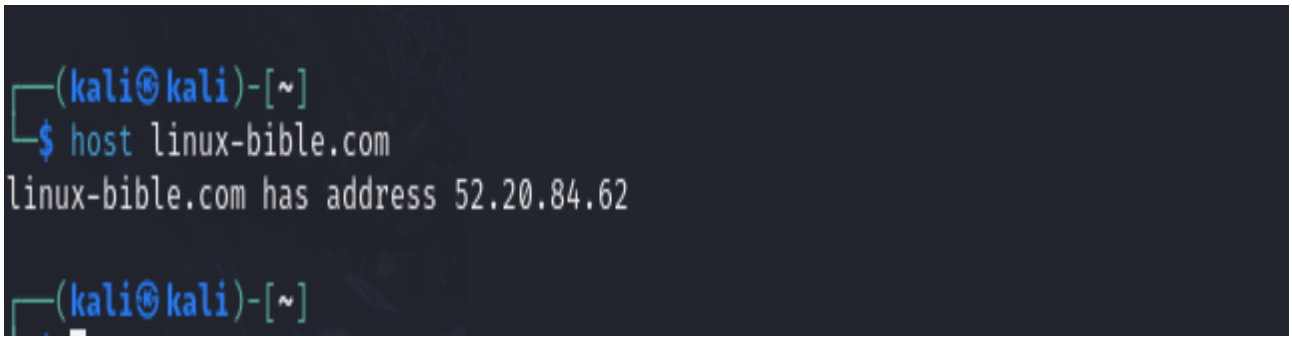
1. What is a `hop' referring to in the output for the traceroute command?
    - Every step that a packet takes to go from its source to its destination is referred to as a hop.

2. What happens if one of the servers/routers in the hops is not listening for ICMP echo requests?
    - Traceroute displays *** indicating a timeout or the possibility that it will terminate before traveling the whole distance.

3. How can an attacker use "traceroute" when targeting computer networks?
    - To aid plan possible assaults, an attacker can use the "traceroute" command to learn more about a target's network structure. To put it another way, it server as a crucial reconnaissance instrument in hacking.

Question G – Challenge 1

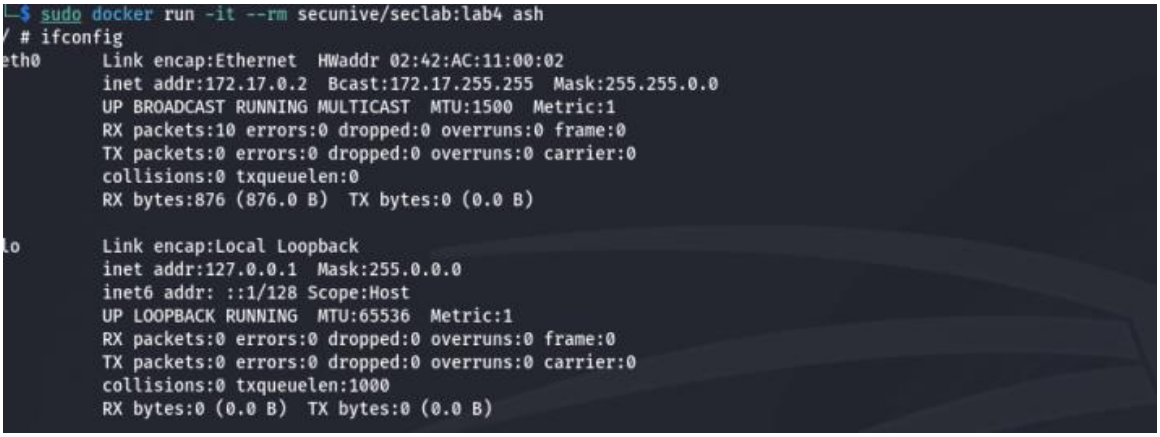
1. The Challenge 1 is to crack a password. Using the host command, find the IP address of the domain linux-bible.com. Include the screenshot of your host command and the results.



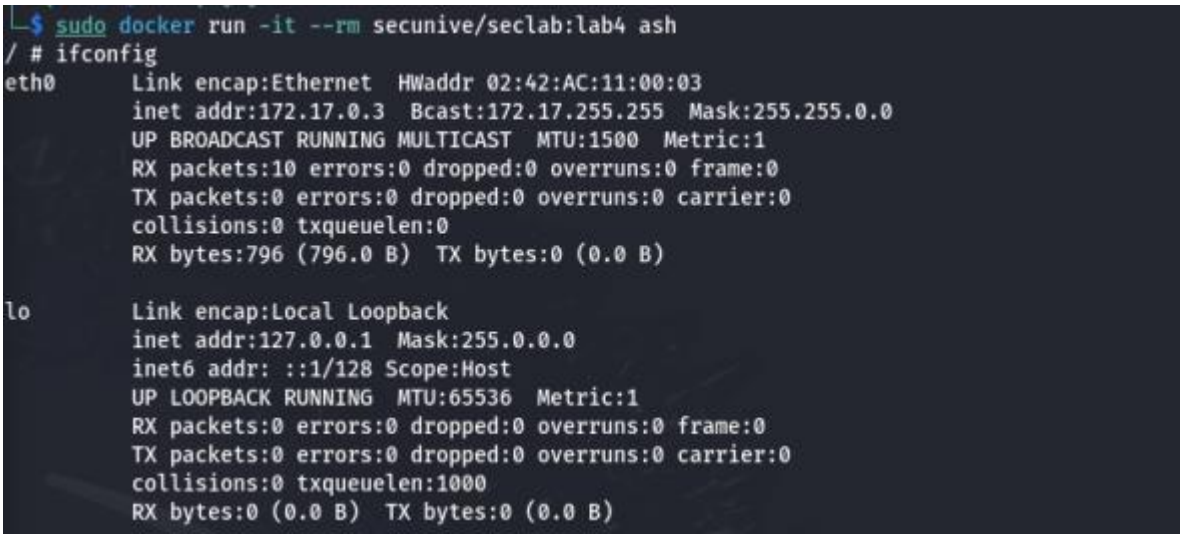
Question H:

1. Include a screenshot of running the “ifconfig” command in each of the terminals. What is the IP address for eth0 in Terminal 1 and what is the IP address for eth0 in Terminal 2?

Terminal 1



Terminal 2



- In terminal 1, eth0's IP address is 127.17.0.2.
- In terminal 2, eth0's IP address is 127.17.0.3.

Question I:

1. Ping host 172.17.0.2 from the second Docker instance in the second terminal (that should have the address 172.17.0.3) and vice-versa, to check network connectivity between the two hosts. Include screenshots confirming that you have executed the commands and received ping replies confirming connectivity between the two hosts.

   Terminal 1

```
/ # ping 172.17.0.3
PING 172.17.0.3 (172.17.0.3): 56 data bytes
64 bytes from 172.17.0.3: seq=0 ttl=64 time=0.219 ms
64 bytes from 172.17.0.3: seq=1 ttl=64 time=0.121 ms
64 bytes from 172.17.0.3: seq=2 ttl=64 time=0.147 ms
64 bytes from 172.17.0.3: seq=3 ttl=64 time=0.142 ms
64 bytes from 172.17.0.3: seq=4 ttl=64 time=0.125 ms
64 bytes from 172.17.0.3: seq=5 ttl=64 time=0.187 ms
64 bytes from 172.17.0.3: seq=6 ttl=64 time=0.157 ms
64 bytes from 172.17.0.3: seq=7 ttl=64 time=0.229 ms
64 bytes from 172.17.0.3: seq=8 ttl=64 time=0.137 ms
64 bytes from 172.17.0.3: seq=9 ttl=64 time=0.157 ms
64 bytes from 172.17.0.3: seq=10 ttl=64 time=0.159 ms
64 bytes from 172.17.0.3: seq=11 ttl=64 time=0.149 ms
64 bytes from 172.17.0.3: seq=12 ttl=64 time=0.139 ms
64 bytes from 172.17.0.3: seq=13 ttl=64 time=0.165 ms
64 bytes from 172.17.0.3: seq=14 ttl=64 time=0.155 ms
64 bytes from 172.17.0.3: seq=15 ttl=64 time=0.165 ms
64 bytes from 172.17.0.3: seq=16 ttl=64 time=0.289 ms
64 bytes from 172.17.0.3: seq=17 ttl=64 time=0.101 ms
64 bytes from 172.17.0.3: seq=18 ttl=64 time=0.119 ms
64 bytes from 172.17.0.3: seq=19 ttl=64 time=0.141 ms
64 bytes from 172.17.0.3: seq=20 ttl=64 time=0.112 ms
64 bytes from 172.17.0.3: seq=21 ttl=64 time=0.113 ms
64 bytes from 172.17.0.3: seq=22 ttl=64 time=0.116 ms
^C
--- 172.17.0.3 ping statistics ---
23 packets transmitted, 23 packets received, 0% packet loss
round-trip min/avg/max = 0.101/0.154/0.289 ms
```

   Terminal 2

```
/ # ping 172.17.0.2
PING 172.17.0.2 (172.17.0.2): 56 data bytes
64 bytes from 172.17.0.2: seq=0 ttl=64 time=37.468 ms
64 bytes from 172.17.0.2: seq=1 ttl=64 time=0.122 ms
64 bytes from 172.17.0.2: seq=2 ttl=64 time=0.112 ms
64 bytes from 172.17.0.2: seq=3 ttl=64 time=0.161 ms
64 bytes from 172.17.0.2: seq=4 ttl=64 time=0.116 ms
64 bytes from 172.17.0.2: seq=5 ttl=64 time=0.114 ms
64 bytes from 172.17.0.2: seq=6 ttl=64 time=0.092 ms
64 bytes from 172.17.0.2: seq=7 ttl=64 time=0.144 ms
64 bytes from 172.17.0.2: seq=8 ttl=64 time=0.120 ms
64 bytes from 172.17.0.2: seq=9 ttl=64 time=0.112 ms
64 bytes from 172.17.0.2: seq=10 ttl=64 time=0.123 ms
64 bytes from 172.17.0.2: seq=11 ttl=64 time=0.133 ms
64 bytes from 172.17.0.2: seq=12 ttl=64 time=0.137 ms
64 bytes from 172.17.0.2: seq=13 ttl=64 time=0.108 ms
64 bytes from 172.17.0.2: seq=14 ttl=64 time=0.128 ms
64 bytes from 172.17.0.2: seq=15 ttl=64 time=0.097 ms
64 bytes from 172.17.0.2: seq=16 ttl=64 time=0.159 ms
64 bytes from 172.17.0.2: seq=17 ttl=64 time=0.146 ms
64 bytes from 172.17.0.2: seq=18 ttl=64 time=0.159 ms
64 bytes from 172.17.0.2: seq=19 ttl=64 time=0.156 ms
64 bytes from 172.17.0.2: seq=20 ttl=64 time=0.182 ms
64 bytes from 172.17.0.2: seq=21 ttl=64 time=0.142 ms
64 bytes from 172.17.0.2: seq=22 ttl=64 time=0.137 ms
64 bytes from 172.17.0.2: seq=23 ttl=64 time=0.178 ms
64 bytes from 172.17.0.2: seq=24 ttl=64 time=0.184 ms
64 bytes from 172.17.0.2: seq=25 ttl=64 time=0.229 ms
64 bytes from 172.17.0.2: seq=26 ttl=64 time=0.156 ms
64 bytes from 172.17.0.2: seq=27 ttl=64 time=0.170 ms
64 bytes from 172.17.0.2: seq=28 ttl=64 time=0.137 ms
64 bytes from 172.17.0.2: seq=29 ttl=64 time=0.156 ms
64 bytes from 172.17.0.2: seq=30 ttl=64 time=0.158 ms
64 bytes from 172.17.0.2: seq=31 ttl=64 time=0.169 ms
^C
--- 172.17.0.2 ping statistics ---
32 packets transmitted, 32 packets received, 0% packet loss
round-trip min/avg/max = 0.092/1.309/37.468 ms
```

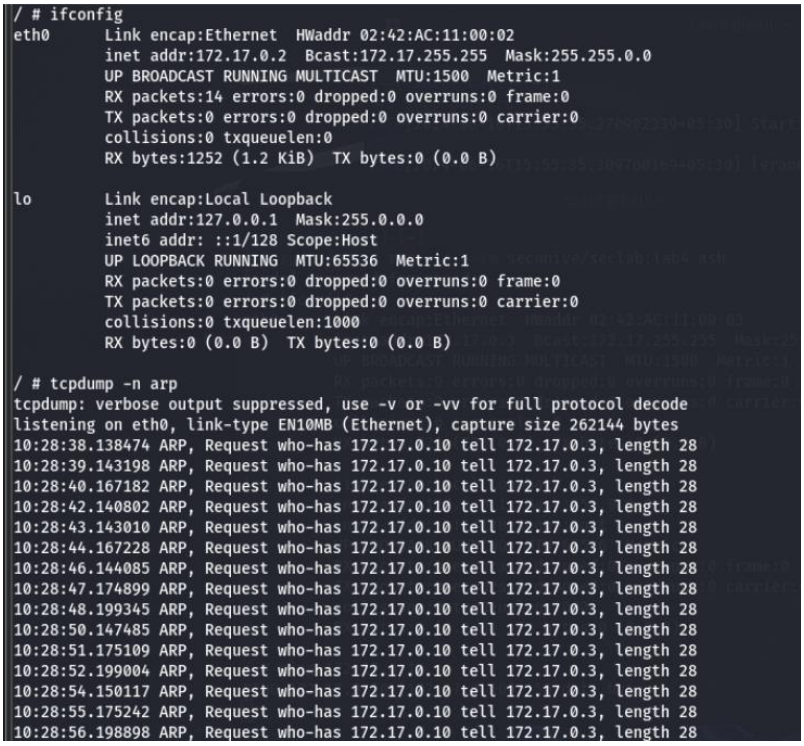
Question J Challenge – 2:

1. ARP protocol is used to discover the Media Access Control (MAC) address corresponding to a certain IP address. Whenever a host needs to connect to an IP that has not used recently (for which it has a cached MAC address), it broadcasts an ARP request.

   ARP protocol is used to discover the Media Access Control (MAC) address corresponding to a certain IP address. Whenever a host needs to connect to an IP that has not used recently (for which it has a cached MAC address), it broadcasts an ARP request.

   The..... is the password.

   What is the password you obtained?



- who-has is the password.

Question K:

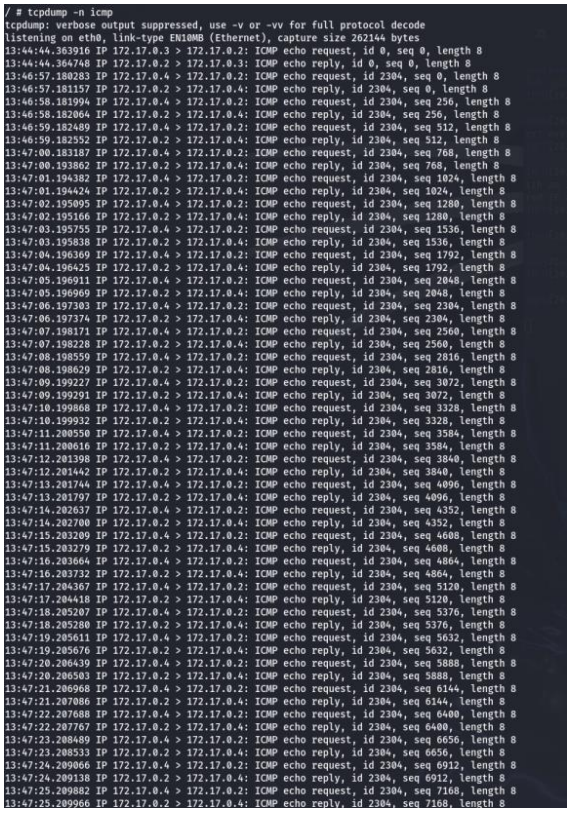
1. How did this task complement the theoretical concepts you learned in Week 4 and Week 5? What did you learn that was most exciting for you? Are you finding it easier to use the shell for hands-on activities?

    - I learned the fundamentals of packets inspection-the most crucial idea in network reconnaissance and docker through this assignment endeavor. How to efficiently use the tcpdump command to check domain this work helped me become proficient in these important areas.

Week 6 Task 6.2C

Question A

1. Include a screenshot of the tcpdump output running on the first Terminal (i.e.,172.17.0.2)



2. In your own words, explain what did just happen?
    - Hear, an ICMP echo request is sent to the first container by the second Docker container, but the packet is masqueraded to looks as though it is from the third container. This results in the generation of a packet with a fabricated source IP address.

Question B

1. What is the password that you have cracked?
    - ‘no replies will be shown’

2. Why would an attacker spoof his IP when running an attack against a victim?
    - An attacker uses a fake IP address to conceal his location on to pretend to be another user.

3. Let’s assume a Web Server was running on the host you targeted (i.e., 172.17.0.2). How could they have prevented their system from being targeted by your ICMP flooding attack?
    - A viable defense against an ICMP flooding assault is available
        - Make sure load balance and redundancy.
        - Setting up firewall rules to restrict or stop ICMP traffic.
        - Setting up ICMP rate limitation.

Question C

Based on the above and your own research about SYN Flood Attack, answer the following questions:

1. What Are the Signs of a SYN Flood DDoS Attack?
    - A SYN flood assault can be identified by keeping an eye on server performance and network traffic for particular signs.
        - One of the main indicators of a SYN flood attack is an abrupt and persistent raise in half-open TCP connections (connections in the SYN_RECEIVED state). Server logs or network monitoring software can be used to see it. Customers may see delays when trying to access services, which is a sign that the server is being overloaded with SYN packets. The sheer volume of pending connections many put a heavy burden on the server's CPU and memory. Crashing or reduced performance may result from this. With the aid of network traffic analysis tools, it may be possible to detect a discernible increase in incoming traffic that is mostly made up of SYN packets. Service outages could occur if legitimate users are unable or unwilling to create new connections to the server. When SYN packets arrive from fictitious or strange IP addresses, monitoring programs may identify them as potential signs of an attack.

2. How to Mitigate and Prevent a SYN Flood DDoS Attack?
    - Using a combination of hardware equipment, software, and network configuration in necessary to mitigate and avoid a SYN flood assault.
        - Get rid of harmful SYN packets by using intelligent firewalls and intrusion prevention systems. These tools have the ability to recognize patterns suggestive of an attack and stop malicious communication. Load balancers can be used to split up incoming traffic among several servers. This makes it less likely that the attack will overwhelm a single server. Determine which IP addresses are sending a lot of SYN messages and block them. This works very well in situations where there are direct attacks and no IP address spoofing. Shorten the timeout period for connections that are partially open. This guarantees that the server releases resources faster by preventing it from waiting too long acknowledgement. Keep a close eye on network traffic for any indications of strange activity. Rapid reaction and mitigation are made possible by early assault detection. Plan your server and network architecture with high availability and redundancy in mind. This makes it possible for other servers to step in and keep service uninterrupted even in the event that one is compromised.

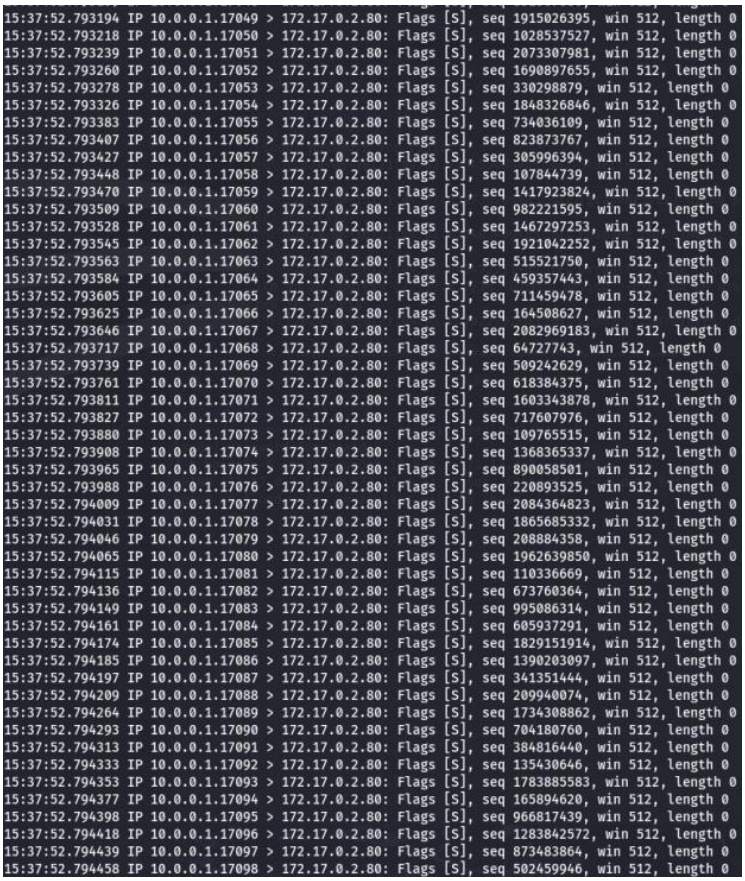
Question D

1. Investigate what is “syn cookie” and explain this in your own words. (1 reference is expected, word count is up to 300 words).
    - Server are shielded from SYN flood attacks, a kind of Denial-of-Service (DoS) attack, by means of SYN cookies. These exploits take use of the TCP handshake procedure to flood a server with partially open connections, preventing it from receiving valid traffic.
    - The SYN cookies solution is for the server to compute a unique sequence number (SYN cookie) using data from the SYN packet and a secret key, rather than devoting resources for each SYN request. SYN-ACK messages contain this sequence number. The sequence number is included in the ACK, if the client provides one. With the use of a reverse function, the server confirms this number. In the event that it is legitimate, it drops the connection and establishes the required resources.
    - A SYN request is sent by the client to establish a connection (TCP Handshake Review) With a SYN-ACK, the server answers. Customer completes the handshake by sending an ACK.
    - Attacker sends a lot of SYN request and does not respond to SYN-ACKs, which leaves connections partially open. This is known as a SYN flood Attack. Each half-open connection requires resource from the server, which fills its buffer and prevents new connections.
    - Benefits: The server guards against resource exhaustion by refusing to allocate resource for connections that are not validated. Service availability is ensured since legitimate connections remain unblocked even in the event severe SYN flooding.

    - Reference: GeeksforGeeks. (n.d.). How SYN cookies are used to preventing SYN Flood attack. Retrieved from GeeksforGeeks

Question E

1. Include a screenshot of the output in the first Terminal showing the huge amount of flooding packets after the attack is executed against the server.



Question F

1. A common interview questions these days is about Mirai Botnet. Investigate this Botnet and in your own words explain how it worked and what was its impact. Is this Botnet still affecting IoT devices? Please ensure that you use references for your answer. The suggested word count is 400-500 words.

    - In 2016, a highly disruptive malware that targeted Internet of Thing (IoT) device surfaced, known as the Mirai Botnet. It was first developed by paras Jha, Josiah white, and Dalton Norman. They used it to perform Distributed Denial of Service (DDoS) assaults against competing servers in the video game Minecraft, giving them an advantage. But the botnet soon became one of the most well-known in cybersecurity history as its capabilities grew.

    - **The operation of Mirai**
      The intrinsic flaws in LoT devices, like default usernames and passwords, were exploited by Mirai. Users frequently forget to modify the default passwords that come with a lot of internet of things devices, such as DVRs, routers and switches, and cameras. After searching the internet for these susceptible gadgets, Mirai used a list of frequently used default credentials to obtain access. Once a device was compromised, Mirai would download its software, thereby turning it into a slave within the botnet.

      Mirai could use this enormous network of compromised devices to overload target systems with traffic after a signification proportion of them were hacked, disrupting services. Because LoT devices are more common than traditional computing devices and frequently have laxer security regulations, they are easy targets for botnet was particularly successful.

    - **The effects of Mirai**
      Considerable and extensive effects were caused by the Mirai Botnet. When a DDoS attack against major DNS provider Dyn was launched using Mirai in October 2016, it was one of the most noteworthy events. Popular websites and services including Twitter, Reddit, Netflix, and Airbnb were all negatively impacted by this attack, which also caused widespread internet disruptions.

      Significant disruption could be possible, as evidenced by Mirai's capacity to enslave a large number of IoT devices into a botnet that could produce terabits of malicious traffic per second. In addition to bringing attention to IoT devices vulnerabilities, the attacks also made clear that the quickly expanding IoT industry needs better security procedures.

- **Present Condition of Mirai**
  There is still a threat from variation of the Mirai Botnet, even after its developers were apprehended and found guilty in 2017. After Mirai's source code was made available to that public in 2016, additional cybercriminals were able to alter and customize it to suit their needs. Consequently, novel strains of Mirai persist in surfacing, focusing on an expanded array of IoT devices and employing increasingly intricate techniques to elude identification and countermeasure initiatives.

  The ongoing existence of Mirai variations suggests that Internet of Things devices are still susceptible. The default password on a lot of Internet of Things devices are still in place, and users frequently forget to install security upgrades. Furthermore, botnets such as Mirai have an ever-growing attack surface due to the growing prevalence of IoT devices.

- To sum up, the Mirai botnet caused a great deal of disruption by talking advantage of poor security in IoT devices, which made it clear how urgently the IoT ecosystem needed stronger security measure. Though its original developers have been captured, Mirai's legacy lives on in the from of continuous variations that pose a threat to global internet services reliability and security

- Reference - Mimoso, M. (2017). Mirai Botnet Authors Avoid Jail Time, Will Assist FBI. Threatpost. Retrieved from Threatpost

Week 7 task 7.2D

Question 1

1. What does SQL stand for? How is it different compared with a DBMS?
    - As the name implies, SQL, often referred to as Standard Query Language, is a for query language, database management systems, or DBMSs, are used to administer databases. SQL is helpful for storing, modifying, and obtaining data from databases.

2. In your own words, define what is an SQL injection attack and what vulnerabilities allow an SQL injection attack to occur?
    - An example of a cyberattack is a SQL injection attack, which modifies application queries submitted to a database by using software vulnerabilities in those applications. By interfering in this way, an attacker could be able to bypass authentication requirements, access, alter, or remove undesired data, or even seize administrative control of the database. In order to alter the SQL query that is submitted to the database, a SQL injection attack entails inserting malicious SQL code into a field or changing the URL. To mislead the database into allowing unauthorized access to the application's contents, for example, an attacker could insert SQL commands into a poorly designed login form.

Deficiencies That Permit SQL Injection Attacks

- Inadequate Output Encoding: SQL commands may be interpreted instead of being regarded as data if output is not encoded correctly. Attackers may use carelessness to insert malicious SQL statement.
- Inadequate access Controls: An SQL injection's impact might be made worse by improperly configured database rights. An SQL injection could potentially have far more of an impact if the application's database user account has a lot of privileges.
- Disclosure of Error Messages: In-depth error messages may divulge sensitive information such as database schemas, which attackers may utilize to home their SQL injection attempts.
- Absence of Input validation: User inputs may be maliciously entered into SQL queries by applications that do not properly validate user inputs. This gives hackers the ability to introduce SQL code and change the intended behavior of the query.
- Vulnerabilities may arise when SQL queries are created dynamically by directly utilizing user input. Attackers can readily utilize dynamic SQL to change the query structure when it concatenates strings without parameterization.
- Outdated Code and Subpar Development methods Applications with badly designed or antiquated code frequently don't follow current security procedures. Because these systems rely on outdated libraries or have inadequate security safeguards, they may be especially susceptible to SQL injection.

3. What are some of the recent attacks that have been initiated by SQL injection? How were they conducted?
    - The online resume service platform ResumeLooters.com was the victim of the ResumeLooters SQL Injection attack, which was first made public in June of 2024. SQL Injection (SQLi) is a widely used vulnerability in which an attacker can manipulate the queries a program submits to its database. The intruders discovered that a few of the ResumeLooters website's input fields were open to SQL Injection attacks. Sending carefully constructed input through forms, URL parameters, or other data entry points that are directly utilized in SQL queries is usually required for this. In this instance, the user login form and the job search capability were discovered to be vulnerable.
      The attackers manipulated input that contained SQL code in order to take advantage of the weakness. Using a tautology-based attack, for instance, is a popular strategy where the input may be something like "'OR'1'='1'." It circumvents authentication when used to a query such as "SELECT * FROM users WHERE username = '$input'" since it modifies the logic to always return true.
    - The attackers circumvented authentication procedures and obtained unauthorized access to the database by using SQL Injection. They might be able to obtain private data, including administrator credentials, resumes, and user information. Attackers can extract enormous amounts of data with this degree of access, which is frequently referred to as a "dump" of the database.
      The attackers stole information from the database when they gained access. This entails executing extra SQL queries to obtain particular tables and columns that hold confidential data. As an illustration, "SELECT * FROM users;"
      These kind of searches would provide all user data kept in the database, including submitted resumes, login credentials, and personal data.
    - Attackers usually take precautions to reduce their visibility. They may tidy logs or make use of sophisticated SQL strategies to avoid having their harmful queries discovered. They might have used anonymous channels and disguised their searches in this instance to prevent being traced. The personal and professional information of thousands of people was exposed as a result of the ResumeLooters SQL Injection attack. The organization promptly addressed the vulnerability by introducing prepared statements and parameterized queries that are impervious to SQL injection attacks. They also carried out a thorough security examination in order to find and address any further potential weaknesses. It is important to secure web applications against common vulnerabilities, as demonstrated by the ResumeLooters SQL Injection attack. Organizations can guard against these types of attacks by following secure coding techniques and routinely upgrading security protocols.

4. Can a firewall prevent an SQL Injection attack? Briefly discuss and support your answer.

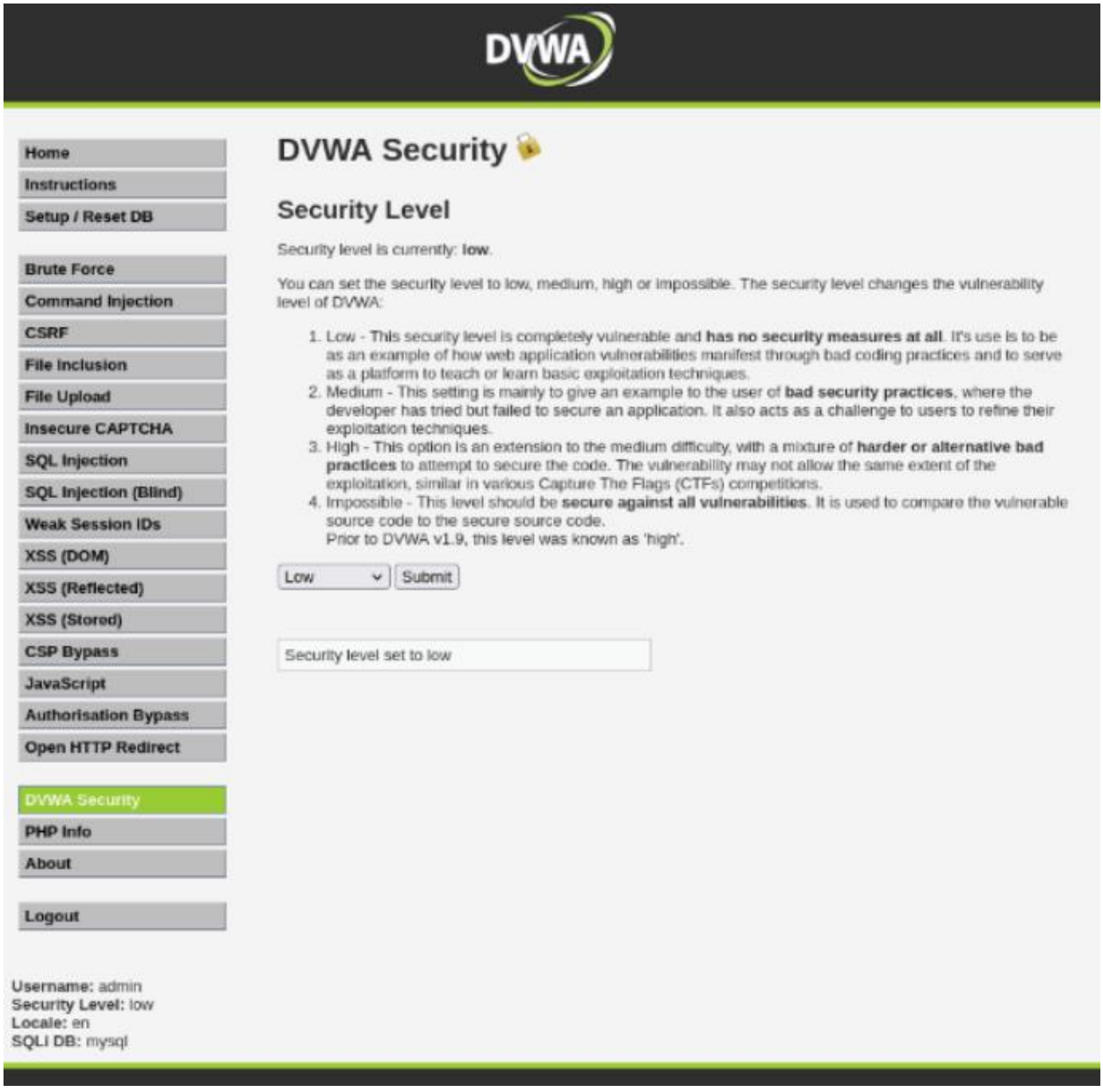
- While it can support a defense-in-depth approach, a firewall cannot completely prevent SQL Injection assaults.
  The main purpose of firewalls, especially classic network firewalls, is to regulate traffic across trusted and untrusted networks by using pre-established security rules. They can filter traffic by IP addresses, port numbers, and protocols and function at the network and transport layers (OSI layers 3 and 4). They do not, however, check the payload of HTTP requests to look for SQL Injection attempts, which take place at the OSI layer 7 application layer.
- An online Application Firewall (WAF) keeps an eye on and filters HTTP traffic going to and from online applications, offering more pertinent protection against SQL Injection. WAFs examine the payload of HTTP requests for questionable inputs and behaviors, allowing them to identify and prevent common SQL Injection patterns and anomalies in online traffic. For example, a WAF may recognize and stop queries that contain SQL metacharacters typically used in injection attacks, such as '--', ';', or 'DROP'. WAFs are not infallible, despite the fact that they can reduce some dangers. Attackers might create complex payloads that evade WAF filters or take advantage of vulnerabilities that are not yet patched. For complete security, therefore, depending only on a firewall (network or WAF) is inadequate.

  For SQL Injection to be effectively prevented, a layered security strategy that consists of;
  - ✓ Practice Secure Coding: To lessen vulnerabilities in the application code, use secure coding guidelines.
  - ✓ Check that all user inputs have been verified and cleaned up before the database processes them. By doing this, harmful inputs may not be interpreted as SQL instructions.
  - ✓ Frequent Security Testing: To find and fix possible flaws, perform frequent penetration tests, vulnerability assessments, and code reviews.
  - ✓ Queries with parameters: To reduce the danger of injection, employ parameterized queries and prepared statements to keep SQL code and user input separate.

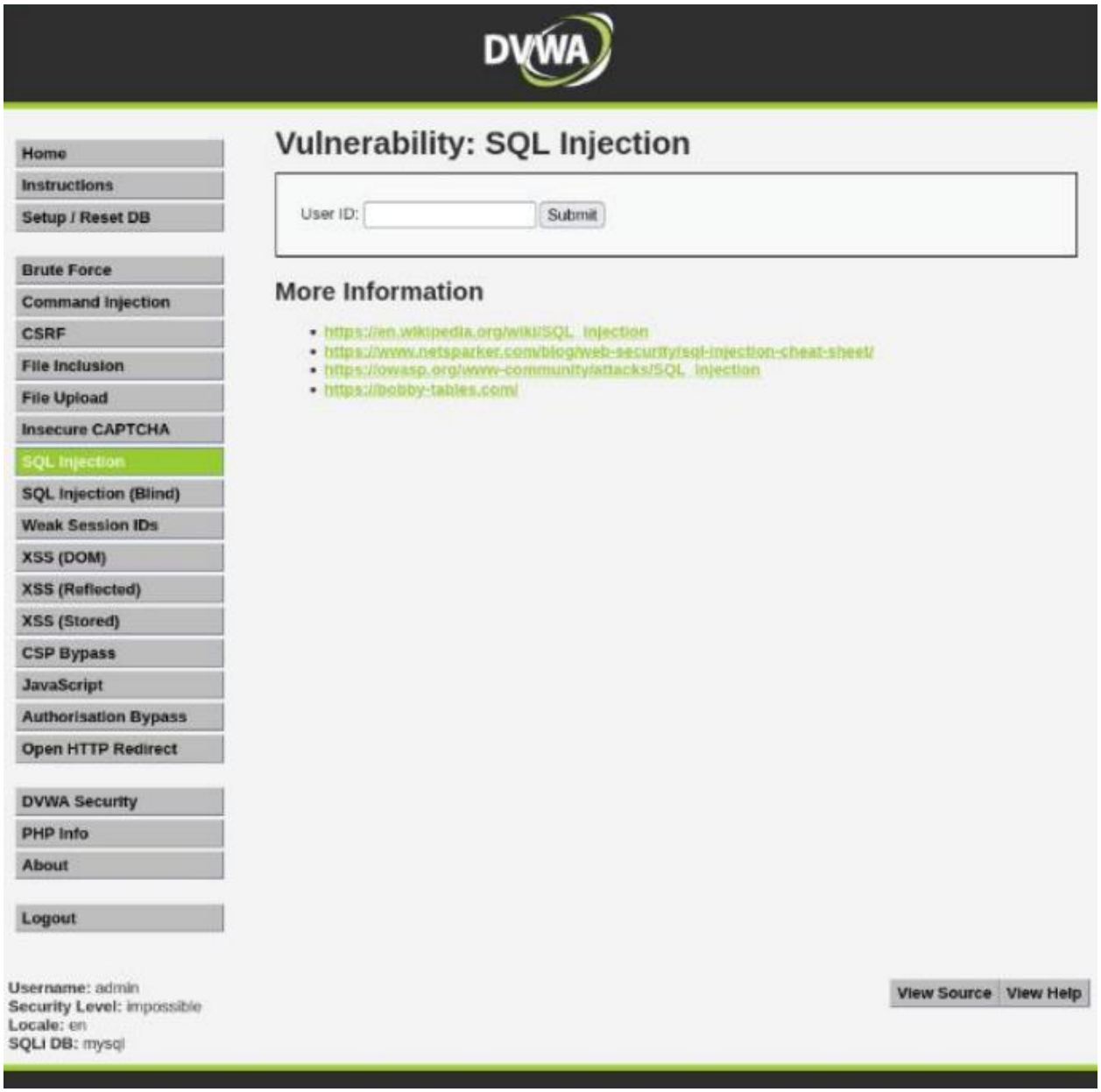
Question 2

1. Go to the SQL Injection tab on DVWA and show a successful SQL injection attack. Include screenshots or link to a screencast confirming that you have successfully conducted an SQL injection attack.

    - Turn down the DVWA's security level to



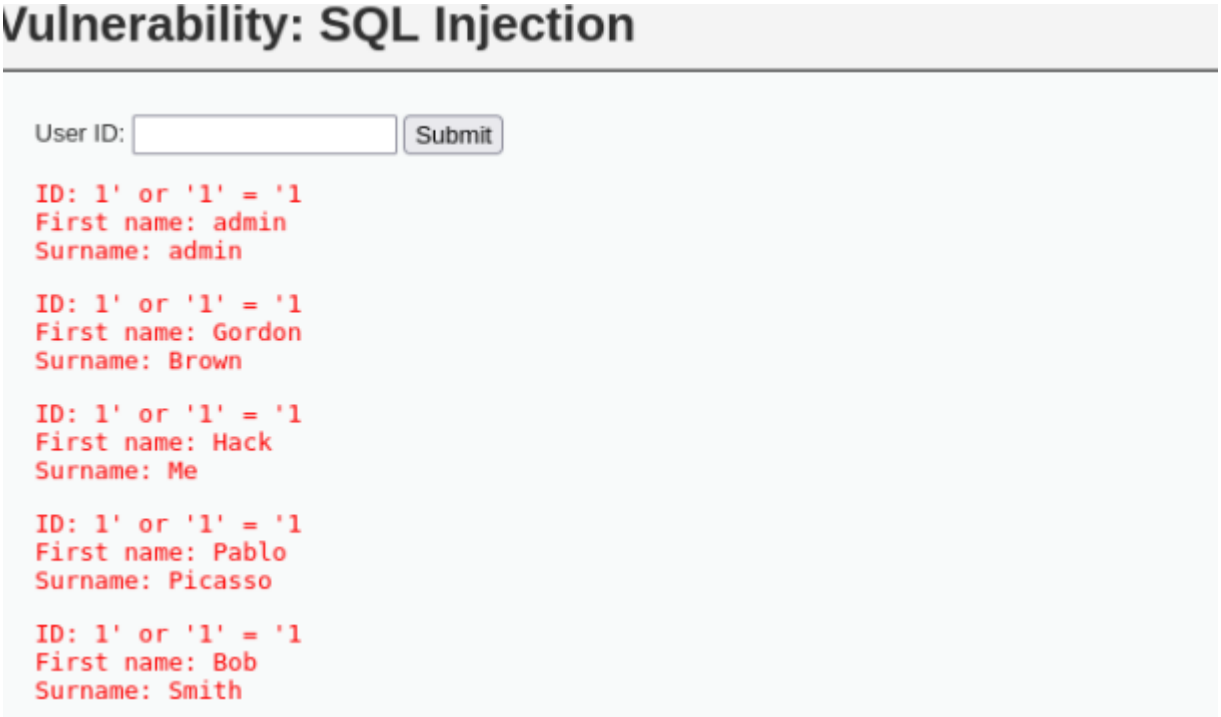
- Navigate to the SQLi tab within DVWA.



- Because its condition is set to true, the traditional SQLi statement 1' or "1' = 1'" always returns a result or group of values.


Vulnerability: SQL Injection
User ID: 1' or '1' = '1
Submit
More Information
https://en.wikipedia.org/wiki/SQL_injection
https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
https://owasp.org/www-community/attacks/SQL_Injection
https://bobby-tables.com/

- Output


Vulnerability: SQL Injection
User ID:
Submit
ID: 1' or '1' = '1
First name: admin
Surname: admin
ID: 1' or '1' = '1
First name: Gordon
Surname: Brown
ID: 1' or '1' = '1
First name: Hack
Surname: Me
ID: 1' or '1' = '1
First name: Pablo
Surname: Picasso
ID: 1' or '1' = '1
First name: Bob
Surname: Smith

Question 3

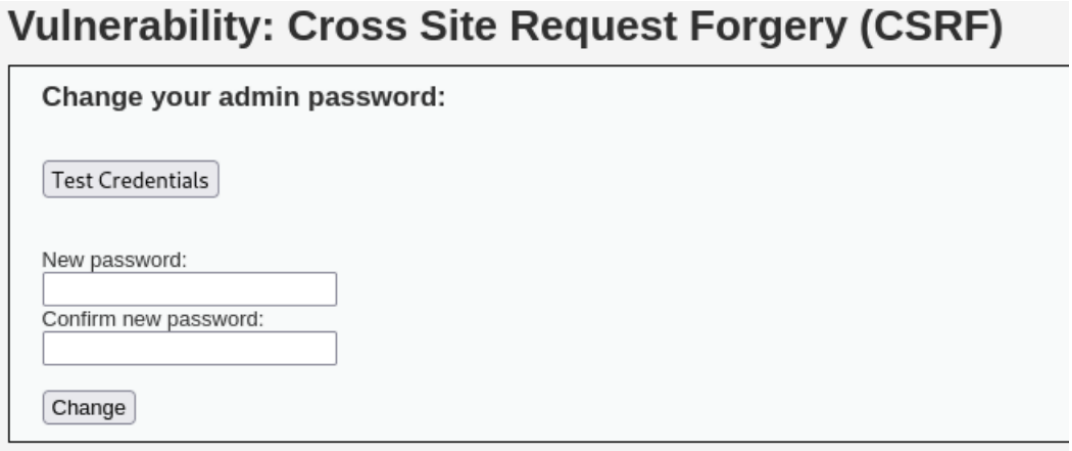
1. What does CSRF stand for? How does this attack work?
    - One kind of security flaw in online application is called Cross-Site Request Forgery, or CSRF. When a user is authenticated into a web application, an attacker can device them into executing undesired actions.

    - How the CSRF Attack Works:
        - ✓ Execution of the action, the crafted request appears genuine and is executed using the victim's credentials when it is delivered to the target application since the victim's browser still contains the authentication credentials for the target application. Taken action, without cheaking to see if the user truly intended to do the action, the web application takes action since it thinks the request is from the verified user. User Authentication, when a victim logs in and has an active session with a target online application, they are considered authenticated within the application. Usually session cookies or tokens are used for this authentication. The act of creating a malicious website or a specially crafted URL with the intention of carrying action on the target application, such as modifying user settings, making a purchase, or starting a financial transfer, is known as malicious request creation. Victim, when the victim clicks on the specially designed URL, they unintentionally engage with the malicious website. Social media, email links, and fraudulent advertisement can all cause this

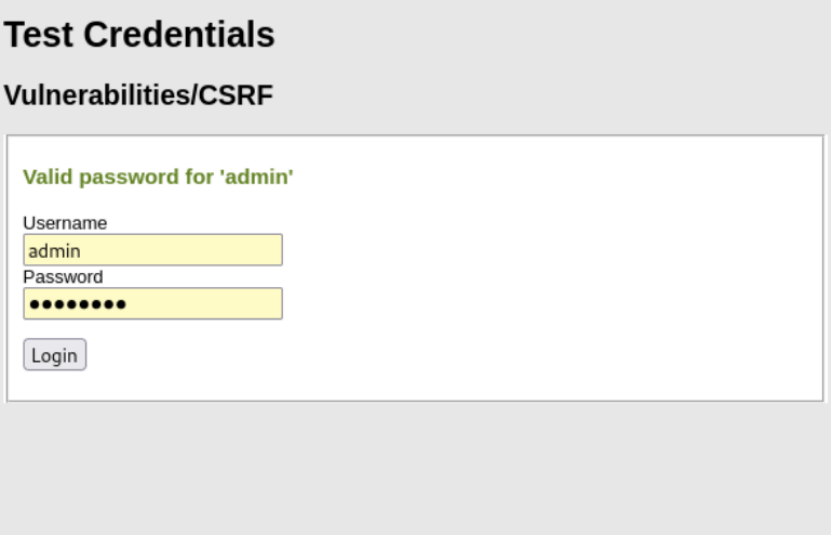
2. How can a CSRF attack be prevented?
    - Same site Cookies: By limiting the way cookies are delivered along with cross-site requests, the SameSite cookie property helps prevent CSRF attacks. The SameSite attribute has three possible values They are Lax , Strict
        - ✓ Lax, with a few exceptions, like a accessing the website from an external link, cookies are not delivered during cross-site request.
        - ✓ Strict, Cookies don't respond to requests from third-party website; instead, they are exclusively sent in first-party contexts.
    - By limiting the transmission of cookies in conjunction with cross-site requests, the SameSite attribute can be set to 'Lax' or 'Strict' lowering the possibility of cross-site request forgery.

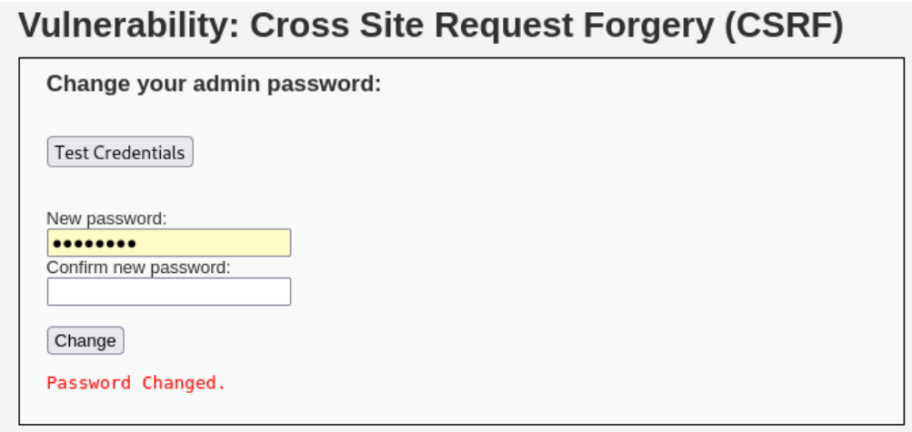
3. Go to the CSRF tab on DVWA. Show a successful CSRF attack. Include screenshots or link to a screencast confirming that you have successfully conducted a CSRF attack.

- Go to the DVWA's CSRF section now.



- You can verify that the current admin password is correct by opening the test credentials.

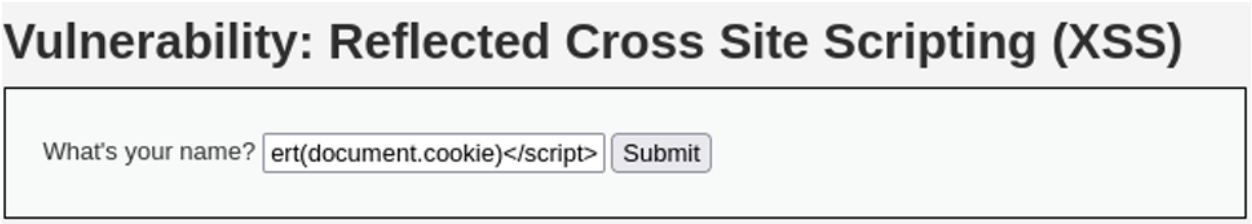




4. What is a browser Cookie (or HTTP cookie)? What is it used for?
    - While a user is on a website, a web browser stores a small bit of information on their device called a browser cookie. User's preference and settings are stored in cookies, and user data is tracked for advertising and analytics purposes.

Question 4

1. Go to the XSS reflected tab on DVWA. Type "<script>alert (document.cookie) </script>" in the textbox and click Submit. What happens? What information are your shown?



- A warning message appears. This causes the echo command to be called out because the input is under the name variable. Any malicious code can be used by the hacker, as demonstrated in this case where a Java Script code loads an alert box revealing the contents of the cookie. The user's session ID is then shown in the alert box, which the hacker may utilize for evil purposes.

2. What is the difference between CSRF and XSS
   - CSRF
     - ✓ Prevention

       Counter_CSRF Coins.
       The attribute of SameSite Cookies.
       Send in two Cookies at once.

     - ✓ Attack Process

       Using the session cookies set up by the user, the user's browser sends a request to the trusted website that looks authentic.

       A malicious email, scripts, URL is created by the attacker.

       After authenticating, the user engages with the harmful material.

     - ✓ CSRF takes advantage of a web application's faith in the user's browser. A cross-site request forgery (CSRF) attack deceives the user's browser into sending unsolicited requests to an application while the user is authenticated and signed in. For instance, a CSRF attack might cause an unapproved money transfer if a signed into a financial website.

- XSS
  - ✓ Prevention

    Coding of Output.
    Cookies that are HTTP only.
    Third, the Content Security Policy.
    Verification of Input.

  - ✓ Attack Process

    When a user submits a from or uses a URL, a web application reflects the malicious scripts onto their browser.

    This type of attack operates by altering the DOM of the webpages, bypassing the server.

    Users are served the malicious script that is kept on the server.

  - ✓ Through XSS, attackers can insert harmful code onto other user's websites. These scripts have the ability to reroute users, change the DOM, and steal data while operating within the user's browser.

Week 8 Task 8.1P

Q1: Consider the following Snort rule:

A. What protocol is this rule applied to?
- The rule is applicable to all IP traffic, irrespective of the protocol used at the transport layer, such as TCP, UDP, or ICMP.

B. What traffic is monitored?
- Source Port: Tracks all traffic coming from a given port.
- Source Address: Tracks network activity coming from any IP address.
- Destination: Keeps track of traffic going to ant IP address.
- Direction: Keeps track of traffic moving from the source to the destination.
- Destination Port: Keep track of traffic to any port of destination

C. What is the rule action?
- The parameter ‘alert’ instructs Snot to produce an alert if this rule is matched.

D. What does msg: “IP Packet detected” do in this rule?
- “IP packet detected” is the message. This message, which is recorded and shown when the rule user that an IP packet matching the criteria of the rule has been found.

E. What is the meaning of sid:1000002 in this rule?
- ‘1000002’ is the signature ID. Is the rule’s special identification. It makes the reference to this particular rule in Snort and other tools cleaner. To prevent inconsistencies with Snort’s official rule sets, ‘sid’ values larger than 1,000,000 are utilize in custom rules.

F. What is the meaning of rev:0 in this rule?
- Version 0 of the rule is denoted by the ‘Revision Number’ the revision number ‘rev’ is increased whenever a rule is changed or modified. This rule’s initial iteration is indicated by rev: 0

Q2: Consider the following Snort rule:

A. What protocol is this rule applied to?
- TCP traffic is subject to the regulation.

B. What traffic is monitored?
- Source Port: Tracks activity coming from any source port.
- Source Address: Tracks network activity coming from any IP address.
- Destination Address: 192.168.1.0/24 is the range of IP address
- Direction: Keep an eye on traffic moving from the source to the destination.
- Destination Port: Port 23

C. What is the rule action?
- Record: The matched traffic is to be logged, according to this action.

D. Does this rule have a rule option argument?
- The rule option argument is not present in this rule.

Q3: Consider the following Snort rule:

A. What protocol is this rule applied to?
- TCP traffic is subject to the regulation.

B. What traffic is monitored?
- Source Port: Keeps track of all traffic coming from any port.
- Source Address: Tracks networks activity coming from any IP address.
- Destination Address: Keeps track of traffic going to any IP address.
- Direction: Reciprocal <>
- Destination Port: Port 23

C. What is the rule action?
- Record: The matched traffic is to be logged, according to this action.

Q4: Consider the following Snort rule:

A. What protocol is this rule applied to?
- TCP traffic is subject to the regulation.

B. What traffic is monitored?
- Source Port: Tracks networks activity coming from any IP address.
- Source address: Tracks networks activity coming from any IP address.
- Destination address: Range of IP address is '192.168.1.0/24'
- Direction: keeps an eye on traffic moving from the source to the destination.
- Destination Port: Port with the exception of those between 6000 and 6010 !6000:6010

C. What is the rule action?
- Record: The matched traffic is to be logged, according to this action.

D. What is the meaning of "!6000:6010" in this rule?
- Negation for the given port range is indicated by the notation '!6000:6010' Traffic to destination ports between '6000' and '6010' is prohibited under the restriction.

Q5: Consider the following Snort rule:

A. What protocol is this rule applied to?
- TCP traffic is subject to the regulation

B. What traffic is monitored?
- Source Port: Tracks networks activity coming from any IP address.
- Source Address: Tracks networks activity coming from any IP address.
- Destination address: Tracks communication to any IP address as a destination.
- Direction: Track the flow traffic from the source to the destination.
- Destination Port: keep track of traffic to any port of destination.

C. What is the rule action?
- Record: The matched traffic is to be logged, according to this action.

D. What is the meaning of content:"|90|" in this rule?
- It checks for the hexadecimal byte 0x90 the TCP packets payload contains a content match condition specified by the content |90|

Q6: Consider the following Snort rule:

A. What protocol is this rule applied to?
- TCP traffic is subject to the regulation.

B. What traffic is monitored?
- Source Port: Tracks networks activity coming from any IP address.
- Source Address: Tracks networks activity coming from any IP address.
- Destination Address: Tracks communication to any IP address as a destination.
- Direction: keep track of traffic to any port of destination.
- Destination port: Keeps an eye on traffic going to any port.

C. Keep track of traffic to any port of destination.
- The parameter ‘alert’ instructs Snot to produce an alert if this rule is matched.

D. What is the meaning of “offset:40” in this rule?
- When offset:40 is selected Snort is instructed to begin its search 40 bytes from the packet payload’s beginning for the specified content |90|

E. What is the meaning of “depth:75” in this rule?
- Starting at the offset position (40), the search for the provided content ('|90|') is restricted to the first 75 bytes of the packet payload by using the option "depth:75". This indicates that Snort will examine the payload from byte 40 to byte 115.

Q7:

A. Explain this rule in your own words covering all the different parameters specified as part of it.

- When any of the following requirements are met by a TCP packet, this rule will raise an alert. TCP traffic is tracked in both directions, from the source "$HOME_NET address" and any source port to the destination "$EXTERNAL_NET" from any destination port. The range of ports (6666to7000) on the external network is indicated by the string "6666:7000". The message that will be logged when the rule is triggered is specified in the section '(msg:“CHAT IRC message”;'. The message in this instance will be "CHAT IRC message." "flow:established;": indicates that only connections that have been established should be covered by the rule. It makes sure that only active TCP sessions are taken into account, eliminating connection attempts that are unsuccessful. Content: "PRIVMSG"; indicates the content that has to match within the packet payload. As a common string found in IRC (Internet Relay Chat)communications, it searches for it in this instance. This modifier, "nocase," specifies that case should not be a factor when matching material. sid:1463 This is the rule's special identification, or Snort ID. The rule within Snort's rule set is referenced using it. revision: 6: This provides information on the rule's revision number. It facilitates keeping track of regulation revisions or modifications over time.

Q8: Next week is the final week of tasks in SIT182. It’s a good time to reflect on your journey thus far in SIT182. Think about all the different tasks you have completed and all the hands-on skills you have learned. Similar to other pass-tasks, this question is just a reflection point. How did you learn about Snort rules to complete questions in this task?

- So far, the projects have been equally thrilling and demanding, and each one has improved my comprehension and hands-on experience with a variety of tools utilized in the cyber security industry.

WEEK 9 – Task 9.1 P

Question A

What is a Rogue Access Point (AP)? Briefly explain 2 different approaches to detect a rogue AP. In your answer ensure that you discuss whether you think a rouge AP is a security vulnerability and how may an attacker exploit a rogue AP. (300 words)

An unauthorized wireless access point connects to a network without the network administrator's knowledge or approval is known as a rouge access point. Because attackers can utilize these rouge Aps to get around network security, they can provide serious security issues regulates, eavesdrops on conversations, or initiates more network attacks.

- A highly dangerous security vulnerability is a rogue access point. Attacker can use rouge Aps to carry out man-in-the-middle attacks and eavesdrop on network traffic. Misuse of network resources.
- Methods of Detection
  - ✓ Conduct Examination
    In order to spot anomalous activity that can point to the existence of a rogue AP, behavior analysis analyzes network traffic patterns. Systems for detecting intrusions (IDS): IDS programs scan network traffic for anomalous patterns that depart from predefined standards. An alarm may be triggered by traffic generated by an unknown access point (AP) that begins broadcasting. Algorithms for Machine Learning: By identifying abnormalities in the regular traffic patterns of approved APs, advanced systems can employ algorithms for machine learning to detect rogue APs.

  - ✓ Network Examining
    In order to identify every device connected to the network, including APs, network scanning entails actively probing the network. MAC addresses and other distinguishing characteristics can be used to identify illegitimate devices using this method. Wireless Network Mapping to map every wireless access point (AP) within a specific radius, utilize programs such as Kismet or NetStumbler. Administrators can identify rogue APs by cross-referencing this map with the list of known, authorized APs. Active Scanning to keep an eye out for unauthorized or new devices on the network, network managers might employ tools that do an ongoing scan. Rogue APs, for instance, can be automatically detected and dealt with by enterprise solutions such as Cisco Wireless Intrusion Prevention Systems (WIPS).

- Reference
  - ✓ Gast, M. S. (2005). "802.11 Wireless Networks: The Definitive Guide." O'Reilly Media.
  - ✓ Mareco, D. (n.d.). Rogue AP Detection: What is it & why your WLAN Design needs it. TechGrid. https://techgrid.com/blog/rogue-access-point-detection

Question B

What is WiFi Protected Setup (WPS)? Which of the following WPS methods is vulnerable? Push-button method, PIN method, Piconet method, NFC method. (200 words)

- The goal of the WiFi Protected Setup (WPS) network security standard is to make connecting devices to wireless networks easier. Users can join devices to their WiFi network without typing lengthy passwords thanks to WPS, which was introduced by the Wi-Fi Alliance in 2007. It provides these four main means of connection the push-button method requires users to physically press both the router's and the device's matching buttons in order to create a connection. PIN Technique to establish a connection, users input an eight-digit PIN that is either shown on the device or supplied by the router. Not a typical WPS approach is the Piconet method. Tap a device against the router to establish a connection via the Near Field Communication (NFC) method.

- The PIN technique is the most susceptible of these. Users using this approach must input an 8-digit PIN, which is frequently displayed on the router. Unfortunately, because of its predictable form and unchanging nature, the WPS PIN is vulnerable to brute-force attacks. Since the first four and last four numbers are validated independently, there are only 11,000 possible combinations instead of the 100 million that there would otherwise be. This vulnerability compromises security by enabling attackers to decipher the PIN and obtain unauthorized access to the network.

- Reference
  - ✓ Wi-Fi Protected Setup | Wi-Fi Alliance. (n.d.). https://www.wi-fi.org/discover-wi-fi/wi-fi protected-setup
  - ✓ Chai, H.-C., & Leong, K. (2016). "Wireless Network Security: Theories and Applications." Springer.

Question C

Which one is more secure: WEP, WPA, or WPA2? Explain 2 vulnerabilities of WPA that led to the development of WPA2. (300 words)

- In order to remedy flaws in earlier standards, wireless security protocols have developed. The earliest and weakest system is called Wireless Equivalent Privacy (WEP). WEP is susceptible to several attacks since it employs the RC4 stream cipher and a static encryption key. Its short key length (40 or 104 bits) and predictable initialization vector (IV) are its primary weaknesses, which enable attackers to decrypt the encryption using a variety of techniques such IV replay attacks.
- Wi-Fi Protected Access (WPA) was designed to address the shortcomings of WEP. It suggested the Temporal Key Integrity Protocol (TKIP) and a message integrity check. Despite being an improvement over WEP, WPA is still vulnerable, particularly when it comes to backward compatibility and inherent weaknesses in TKIP and WEP. TKIP still contains a number of WEP-related vulnerabilities despite using RCE in place of WEP, and brute-force attacks can be employed against the WPA pre-shared key (PSK) mode. The most secure of the three, Wi-Fi Protected Access II (WPA2), was introduced in 2004. WPA2 uses the Advanced Encryption Standard (AES) for encryption through the Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP). AES has stronger encryption and is less susceptible to assaults. Additionally, WPA2 improves data integrity and confidentiality by using CCMP rather than TKIP.TKIP
- Vulnerability: TKIP was created by WPA as a temporary fix that might executed using hardware that is already in place. Even with advancements, the RC4 cipher—which was still susceptible to some attacks—was nevertheless utilized by TKIP. As an example, the The Beck-Tews attack showed how TKIP could be used in less than a minute to decrypt brief packets, giving attackers the ability to insert malicious data. Weakness: Brute-force attacks could be launched against WPA's Pre-shared Key (PSK) mode, which is frequently employed in home networks. By using dictionary attacks, attackers could guess the PSK during the initial handshake between a device and an access point. This was troublesome as a lot of users selected weak passwords, which left the network exposed. In order to combat this, WPA2 introduced stronger encryption and key management protocols that improved defense against these kinds of assaults.
- Reference
    - ✓ Kaufman, C. (2002). "Network Security: Private Communication in a Public World." Prentice Hall.
    - ✓ Grubbs, P. (2024, May 15). The security Risks of Pre-Shared Keys (PSKs). SecureW2. https://www.securew2.com/blog/risks-pre-shared-keys-psks

Question D

Discuss how Mac Address Filtering may be used to secure a wireless network against threats? (200 words)

- One technique to improve wireless network security is MAC address filtering. limiting network access according to client devices' Media Access Control (MAC) addresses. This is how it functions and how it contributes to wireless network security
- Access Control: A hardware identifier known as a MAC address is specific to every device linked to a network. Administrators are able to establish a whitelist of authorized devices through the use of MAC address filtering. In order to prevent illegal devices from connecting to the network, only devices whose MAC addresses are on this list are permitted.
- Mitigating Unauthorized Access: By preventing the MAC addresses of unauthorized users' devices from being recognized and accepted by the network's Access Point (AP), this method can discourage petty intruders or unauthorized users from connecting to the network.
- Layer of Defense: An extra security layer is provided by MAC address filtering. An attacker needs to impersonate an allowed MAC address in order to obtain access, even if they are aware of the network's SSID or encryption keys.
- Easy to Implement: On the majority of wireless routers and access points, it is simple to set up and maintain. MAC addresses can be manually added to or removed from the list of devices that are permitted by network administrators.
- However, there are certain limitations to MAC address filtering. Although competent attackers can still spoof MAC addresses, this technique is less successful against dedicated or technically astute invaders. As a result, it ought to be combined with WPA3 and ongoing network monitoring, among other security measures.
- Reference
    - ✓ Mitchell, B. (2021, August 5). MAC Address Filtering: What it is and how it works. Lifewire. https://www.lifewire.com/enabling-mac-address-filtering-wireless-router-816571
    - ✓ Tanenbaum, A. S., & Wetherall, D. J. (2011). "Computer Networks." Pearson.

Question E

Briefly discuss what an Evil Twin AP attack is? (200 words)

- One type of cyberattack in which a malevolent actor sets up an Evil Twin Access Point (AP) attack an impostor wireless access point (AP) that poses as an authentic AP. Tricking users into connecting to the rogue AP rather than the authentic one is the goal. This kind of attack usually entails the subsequent actions,
- Establishing a Rogue AP: The hacker sets up a wireless access point with the identical the valid AP's SSID (Service Set Identifier). To make the fake AP seem even more real, skilled attackers might additionally spoof the MAC address. Entice Users to Connect: When users look for available networks, they come across the rogue AP and connect to it since they think it's real. To draw consumers in, the attacker may employ more powerful signals. Data Interception: The attacker can intercept and collect all user data once they establish a connection with the rogue AP.
- Email addresses, login passwords, and other private information are among the sensitive data that are sent across the network. Malicious uses of this information include identity theft and other assaults. Man-in-the-Middle Attack (MITM): This attack deceives users by using a rogue AP to transfer traffic to a legitimate AP, making it difficult for users to detect the attack. At that point, the attacker has the ability to alter the data or add harmful content.
- Reference
    - ✓ Evil Twin Attack: Fake WiFi access point vulnerabilities | OKTa. (n.d.). Okta, Inc. https://www.okta.com/identity-101/evil-twin-attack/
    - ✓ Barton, R. (2012). "Securing Your Wireless Network: A Primer." SANS Institute

Question F

Near Field Communication (NFC) is used for contactless payment systems. List and briefly explain 3 different vulnerabilities for NFC. (200 words)

- Near field communication (NFC) is widely used with contactless payment systems to facilitate transactions through close proximity communication. However, NFC technology is prone to several problems.
- Hackers can get data transmitted between an NFC device and a reader by means of eavesdropping. The typical working range of NFC is only 4 cm, but if an attacker has sensitive equipment, they can listen in from a greater distance. This might expose private information, like credit card numbers or personal identification numbers (PINs).
- Malicious actors can increase the communication range between two NFC devices through relay attacks. An attacker can carry out transactions without the user's knowledge or agreement by doing this by relaying signals between the legitimate devices over a longer distance. An important security risk is that an attack can take place without actual physical access to the NFC-enabled device.
- Data Modification: If you want to change the information that is shared between NFC devices, you must modify the data. In order to commit fraud or get unauthorized access to services, attackers have the ability to intercept and alter messages. While less common, this kind of assault is nevertheless quite dangerous because it needs specialized tools and exact timing.
- Reference
    - ✓ Higgins, M., & Higgins, M. (2024, February 7). NFC Security: 10 security risks you Need to know. NordVPN. https://nordvpn.com/blog/nfc-security/
    - ✓ Madlmayr, G., Langer, J., Kantner, C., & Scharinger, J. (2008). "NFC Devices: Security and Privacy." I

WEEK 9 Task 9.2C

1. **20.2**
   For a password that is 15 characters long, where each character can be one of the 52 upper- and lower-case letters, 10 digits, or 32 punctuation symbols, the total number of possible passwords is:
   94^{15}
   Converting this to seconds for readability
   3.95 times 10^{20} seconds.

2. **20.3**
   Given the data in Problem 20.2, compute the size of the hard disk needed to house a rainbow table if each hash is 512 bits in length.

   S ≈ 3.71196 x 1018 TB

3. **20.11**
   128 bits

4. **20.12**
   160 bits

5. **20.13**
   256 bits

6. **20.14**
   256 bits

7. **20.15**
   224 bits

8. **20.16**
   256 bits

9. **20.17**
   128 bits

10. **20.18**
    256 bits

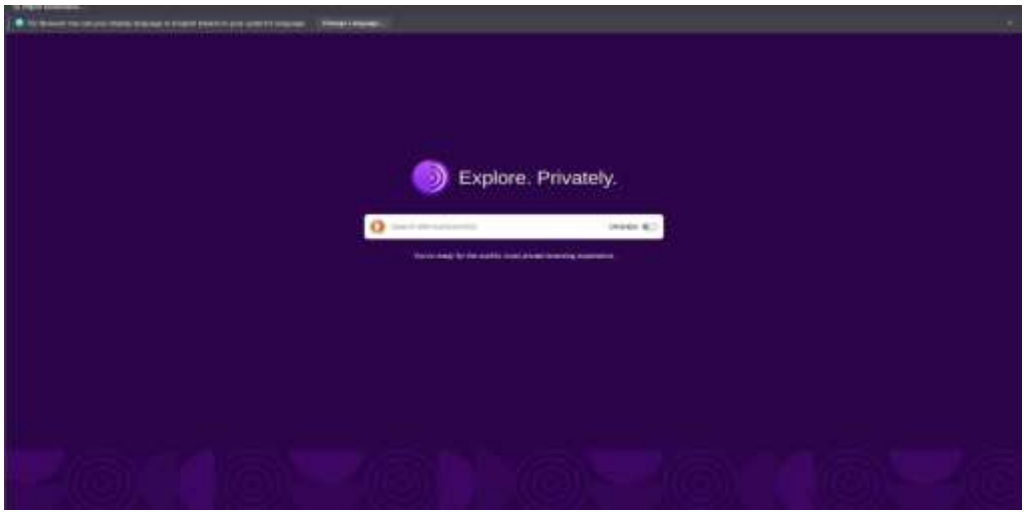
Week 9 – Task 9.3D

Questions

1. What is Tor? Why would someone want to use Tor?
    - Online traffic is hidden by the Onion Router, or Tor, network. Tor is a volunteer-run, open-source platform. Users that access websites and servers over the "onion" network can access them anonymously thanks to Tor's "onion routing." While Clearnet websites can be accessed via Tor, journalists and other users who require identity protection mostly utilize them as a gateway to the Dark Web.

    - Smith, J. (2023). Understanding Tor: An Overview of the Onion Router. TechTrends. Retrieved from https://www.techtrends.com/understanding-tor-an-overview-of-the-onion-router

2. Install Tor Browser from https://www.torproject.org/ on Kali VM. An easy way of installing Tor is using APT package manager. For this, run sudo apt-get install torbrowser-launcher in the Terminal and follow the prompts.
3. Include a screenshot of Tor browser running successfully on your Kali VM. The screenshot should cover the browser window entirely.



4. What are ".onion" sites?
    - The top-level domain ".Onion" is used in place of ".com," ".net," or ".gov," which are inaccessible through the Tor network and not visible in a standard browser.
    - https://vpnpro.com/guides-and-tutorials/what-are-onion-sites/

5. Is HTTPS important for accessing websites via Tor? Is HTTPS important for accessing ".onion" sites?
    - Because Tor is encrypted by default and can hide a user's IP address and location, Tor networks don't always require HTTPS. Despite this, it is still accessible as an extra security measure.
    - EFF. (a.n.d.). How to use Tor onion services: An introduction. Electronic Frontier Foundation. Retrieved from https://ssd.eff.org/en/module/how-use-tors-onion-services-introduction

6. What does Jacob Appelbaum mean by "privacy by design" in his TED talk video?
    - In order to ensure that user privacy is prioritized and preserved, Jacob Appelbaum uses the phrase "privacy by design" in his TED presentation video to highlight how important it is to incorporate privacy features into technology from the very beginning and throughout the whole development process.
    - Rosenberg, S. (2023). Anonymity and Security with Tor: A Comprehensive Guide. Retrieved from https://www.anonymitysecuritytor.com

7. What is the difference between Tor and a VPN? Would you need to use both?
    - Through a network of servers managed by volunteers, Tor enables you to route your traffic through a different network where the VPN provider owns the server.
    - **Mann, S.** (2023). *Tor vs VPN: Understanding the Differences*. Retrieved from https://www.cybersecurityinsider.com/tor-vs-vpn-understanding-the-differences

8. When using Tor, does your Internet Service Provider (ISP) know you are using Tor?
    - When a user uses Tor, their ISP can see it, but they are unable to view or follow what the user browses on Tor.
    - Smith, A. (2023). Exploring Tor: Safety, Privacy, and Usage. Retrieved from https://www.privacysafetytor.com/exploring-tor-safety-privacy-usage

9. Can Tor be blocked by network administrators? If so, would it be possible to bypass that blocking? (if answer is yes, list the approaches that could be used for this).
    - A network administrator can ban Tor, although there are a few ways around this. Using bridges, virtual private networks, and distinct ports
    - Smith, A. (2023). Exploring Tor: Safety, Privacy, and Usage. Retrieved from https://www.privacysafetytor.com/exploring-tor-safety-privacy-usage