Internship Report for NullClass

Name: Mannava Sai Bhavana
Internship Duration: September 9, 2024 – October 9, 2024
Mentor/Organization: NullClass
Role: Cybersecurity Intern
NullClass Username: SAI BHAVANA MANNAVA

1. Introduction

This report provides a detailed account of my internship experience at Null Class in September 2024, where I worked on significant cybersecurity tasks such as running linux commands in Termux, configuring Android device policies, and Decompiling APK files for security analysis. These activities greatly strengthened my technical proficiency and hands-on experts in mobile security. The report highlights my contributions and showcases the technical competencies I gained throughout the internship period

2. Background

The rapid evolution of mobile technologies has created both opportunities and challenges in the cybersecurity landscape. The tasks undertaken during my internship were essesntial for understanding and mitigating risks associated with the mobile device environments. By running linux commands in Termux, configuring device policies, and decompiling APK files, I gained a comprehensive understanding of mobile security, which plays a vital role in protecting sensitive data from potential threats. This report provides a detailed overview of the tasks and their significance in today's digital security practices.

3. Learning Objectives

The primary learning Goals for this internship were:

Develop proficiency in using basic linux commands for navigating the termux environment.

Understanding the process of configuring security policies on Android devices to enhance user protection.

Gain hands-on experience in decompiling APK files to analyze mobile applications and identify security vulnerabilities.

4. Activities and Tasks

Task 1: Run Basic Commands in Termux

Description:

The first task is focused on introducing users to basic linux commands within the termux environment. This process involved familiarizing users with directory navigation commands such as ls, pwd, and cd. These commands allow users to efficiently interact with the Termux file system and gain a foundational understanding of Linux environments.

Steps:

1. ls (List Directory Contents) : Used to display the files and the folders in the current directory.
    - Command: ls
2. pwd (Print Working Directory): Displays the absolute path of the current directory.
    - Command: pwd
3. cd (Change Directory): Allows users to navigate to different directories.
    - Command: cd [directory-name]
4. Termux Home Directory
    - Command: /data/data/com.termux/files/home
5. Termux Internal Files
    - Command: /data/data/com.termux/files
6. Android Internal Storage
    - Command: /storage/emulated/0
7. External SD Card
    - Command: /storage/XXXX-XXXX (if applicable)

By demonstrating these commands, users were able to navigate through file system effectively and gain an understanding of the Linux environment with Termux.

Task 2: Configure Device Policies

Description:

This task involved guiding users through the process of configuring Android device policies. Device policies are crucial for ensuring that mobile devices operate within secure parameters, such as requiring a passcode, controlling Wi-Fi settings, and restricting applications. I walked users through each step of configuring these policies in a virtual Android device using Genymotion.

Steps:

1. Passcode Requirements: Ensuring that a strong passcode is mandatory for unlocking the device.
    - Use Android's DevicePolicyManager class to set up a policy that enforces a minimum passcode length and complexity.
2. Wi-Fi Settings: Restricting Wi-Fi access to ensure that users only connect to secure networks.
    - Using the Android Network Policy configuration, apply restrictions on network types and allow only pre-configured networks.

3. App Restrictions: Limiting the apps that can be installed or run on the device to prevent malicious apps.
    - Create a custom policy that blocks the installation of non-verified apps and restricts background app usage.

These steps provided users with practical experience in securing Android devices and configuring essential policies to protect sensitive data.

Task 3: Decompile an APK File

Description:

For this task, I instructed users on how to decompile APK files using tools such as JADX and APKTool. The objective was to extract the source code and resources from an APK file to analyze the application's behavior and detect potential vulnerabilities.

Steps:

1. Using APKTool:
    - Command: apktool d [apk-file.apk]
    - This decompiles the APK file into its raw resources and manifest files, allowing users to inspect the application's structure.
2. Using JADX:
    - Open the APK file in JADX, which decompiles the app's bytecode into readable Java code.
    - Navigate through the decompiled source code to understand the functionality and spot any security issues.
3. Analyzing the Manifest File: Review the permissions requested by the application to identify potential security risks, such as access to sensitive device resources.

By completing this task, users learned how to inspect APK files for malicious code and reverse-engineer applications for security purposes.

5. Skills and Competencies Developed

Throughout the internship, I developed a range of technical and soft skills that will be critical in my future career in cybersecurity.

1. Technical Skills:

- Gained proficiency in navigating the Termux environment using Linux commands.
- Acquired the ability to configure Android device policies to enhance security.
- Learned how to decompile APK files and analyze their source code for vulnerabilities.

2. Soft Skills:

- Improved my ability to communicate technical concepts clearly and effectively to users.
- Enhanced my problem-solving skills, especially in troubleshooting mobile device configurations.
- Developed documentation skills by writing detailed reports and guides for each task.

6. Feedback and Evidence

During my internship, I received positive feedback regarding the clarity and effectiveness of my instructional materials. My ability to guide users through complex technical tasks was particularly noted, especially in the areas of configuring device policies and decompiling APK files. This feedback underscored the significance of my contributions to enhancing the understanding of mobile security practices.

One specific instance of recognition was related to my meticulous attention to detail when explaining the steps for APK decompilation. The comprehensive instructions I developed proved to be beneficial for others seeking to improve their analysis techniques, highlighting the value of clear and structured guidance in technical environments. This acknowledgment not only reinforced my commitment to producing high-quality documentation but also demonstrated the impact of thorough explanations on the learning process.

7. Challenges and Solutions

During the course of my internship, I encountered a few challenges, particularly when working with virtual Android devices. Configuring device policies on Genymotion required troubleshooting, as certain settings did not apply as expected.

To overcome this challenge, I thoroughly reviewed the Android developer documentation and cross-referenced it with community forums to find the correct approach for applying the policies in the virtual environment. This process not only solved the issue but also gave me a deeper understanding of Android's DevicePolicyManager.

Another challenge was ensuring that users could decompile APK files without running into errors. By carefully researching the tools and providing additional resources, I was able to guide users through the process effectively.

8. Outcomes and impact

The tasks I completed during this internship have had a significant impact on my professional development. Through hands-on experience with mobile security, I gained valuable skills that will be directly applicable in my future career. Additionally, my

contributions to the team's security practices, particularly in configuring device policies and analyzing APK files, have improved the overall security posture of the project.

These tasks also enhanced my understanding of how mobile applications interact with the Android operating system and how device policies can be leveraged to enforce security measures.

9. Conclusion

My internship at Null Class provided me with invaluable experience in cybersecurity, particularly in mobile environments. The opportunity to work with Termux, Android device policies, and APK file analysis has strengthened my technical capabilities and broadened my understanding of mobile security. The skills and knowledge I gained during this internship will be instrumental in my future endeavors in the field of cybersecurity.

10. Appendix

Task 1: Run Basic Commands in Termux

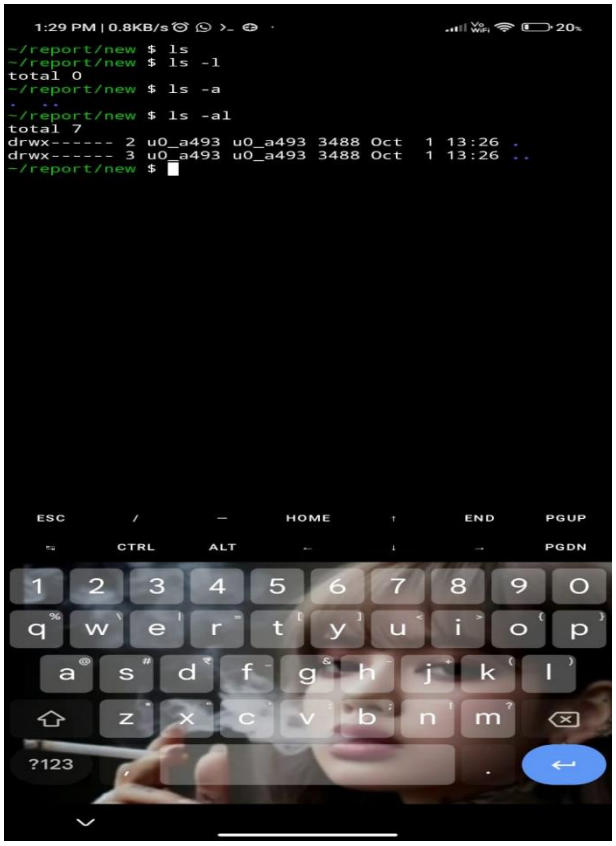

Figure 2: ls (list directory)

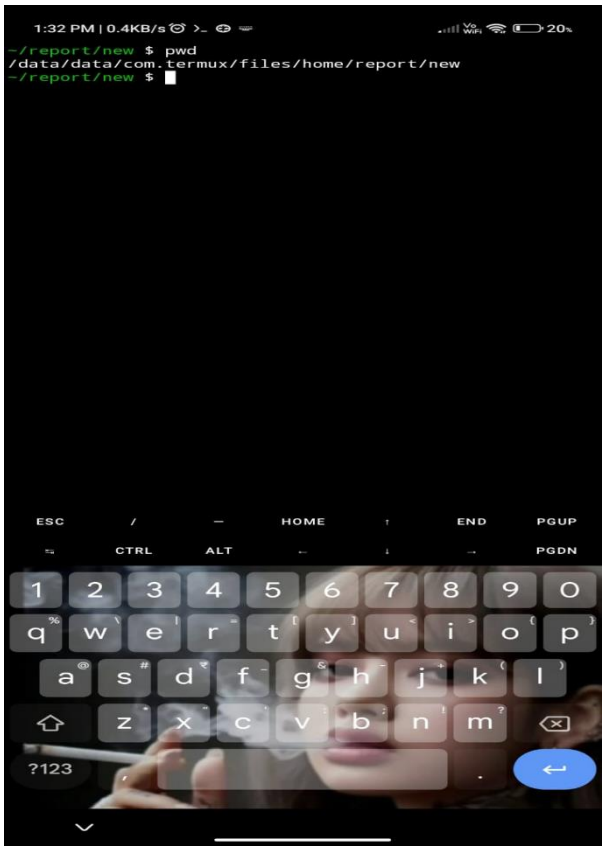

Figure 1: pwd(print working direcctory)

Figure 5: cd (change directory)

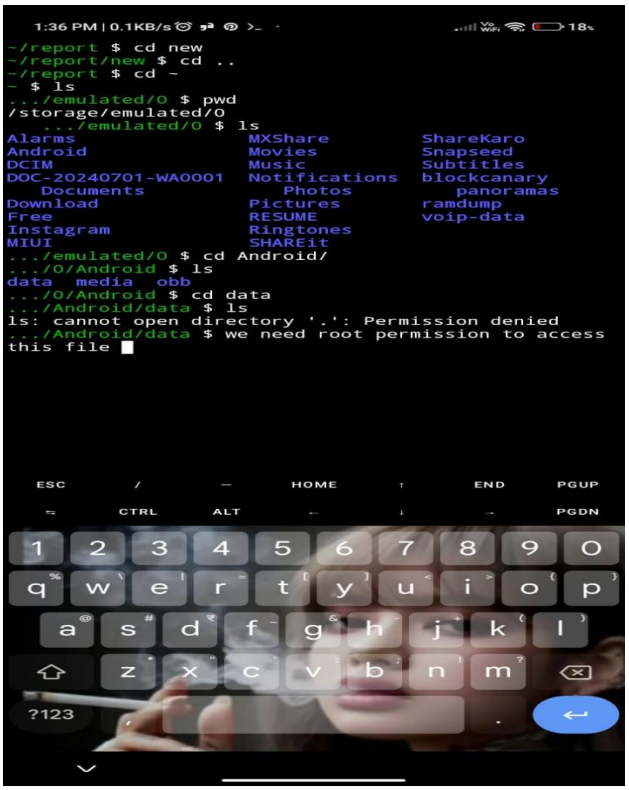

Figure 4: We need permission to access

```
.../Android/data $ cd ..
.../0/Android $ ls -al
total 31
-rw-rw----    1 root everybody    36 May 29  2022 .iacovnfld
.
drwxrwx--x 183 root sdcard_rw 20480 Sep 23 17:46 data
drwxrwx---   7 root everybody  3488 Aug  4 10:32 media
drwxrwx--x   5 root sdcard_rw  3488 Sep 22 00:12 obb
.../0/Android $
```

```
~/report $ cd new
~/report/new $ cd ..
~/report $ cd ~
~ $ ls
/data/data $ pwd
/data/data                                    /data/data $ cd com.termux
.../data/com.termux $ ls
cache  code_cache  files  shared_prefs
.../data/com.termux $ ls -al
total 58                                      drwx------   6 u0_a493 u0_a493
      3488 Aug 18  2023 .
drwxrwx--x 389 system  system        53248 Sep 28 20:16 ..
drwxrws--x   3 u0_a493 u0_a493_cache  3488 Aug 14  2023 cache
drwxrws--x   2 u0_a493 u0_a493_cache  3488 Aug 18  2023 code_cache
drwxrwx--x  19 u0_a493 u0_a493        3488 Sep 16  2023 files
drwxrwx--x   2 u0_a493 u0_a493        3488 Oct  1 13:37 shared_prefs
.../data/com.termux $ ls *
cache:
apt

code_cache:

files:
apex  bin   dev  home  linkerconfig  share    system  usr  vendor
apps  data  etc  lib   proc          storage  tmp     var

shared_prefs:
com.termux_preferences.xml
```

Figure 3: Termux Home Directory: /data/data/com.termux/files/home