Internship Report on Cybersecurity Tasks

Submitted by: Deepak Yadav

Internship Provider: NULLCLASS

Date: 04-10-2024 to 04-11-2024

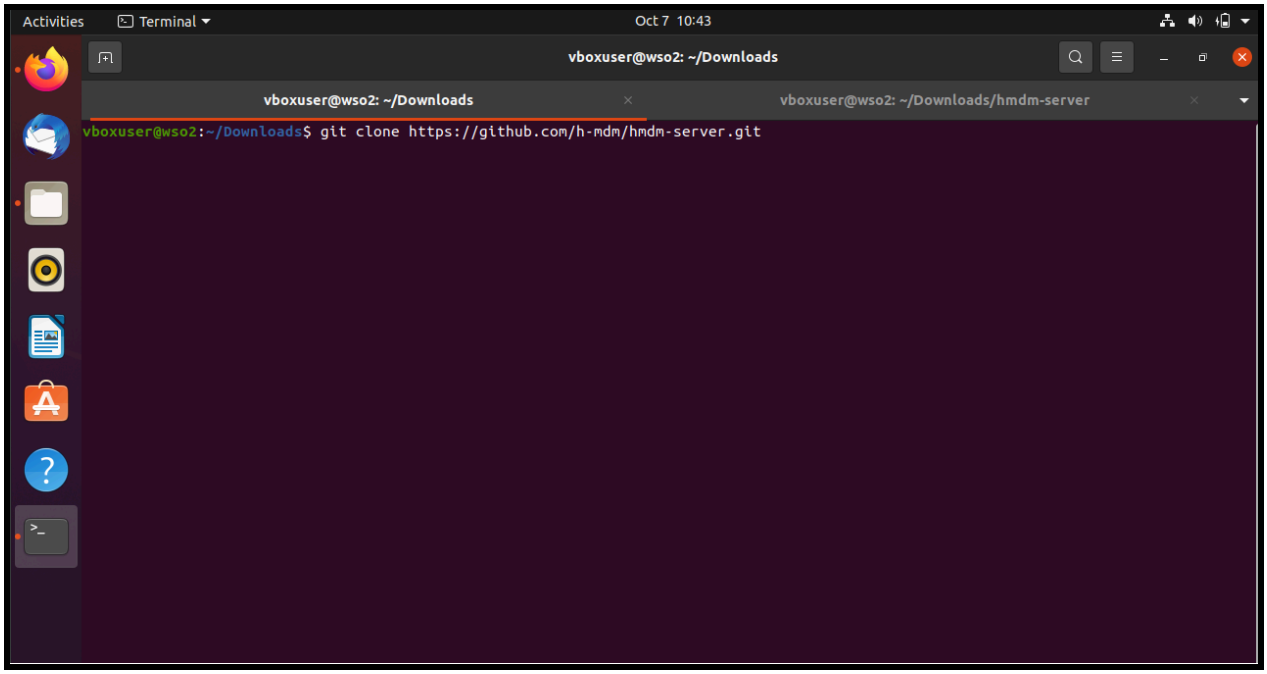
Overview

During my internship with NULLCLASS, I was tasked with completing three key assignments that involved hands-on technical implementation and documentation. These assignments not only enhanced my understanding of critical cybersecurity concepts but also honed my practical skills in Android OS penetration, Mobile Device Management (MDM), and APK file analysis. Below is a detailed report on the assigned tasks, showcasing both the methodology and proof of concept (POC) for each.

Task 2: Configuring an Open-Source Mobile Device Management (MDM) Tool

Overview

HMDM is a Mobile Device Management (MDM) solution that allows administrators to manage Android devices by pushing apps, enforcing security policies, and remotely controlling devices. This PoC demonstrates the installation of HMDM on a local server using Docker and the enrollment of a virtual Android device using Android Studio.

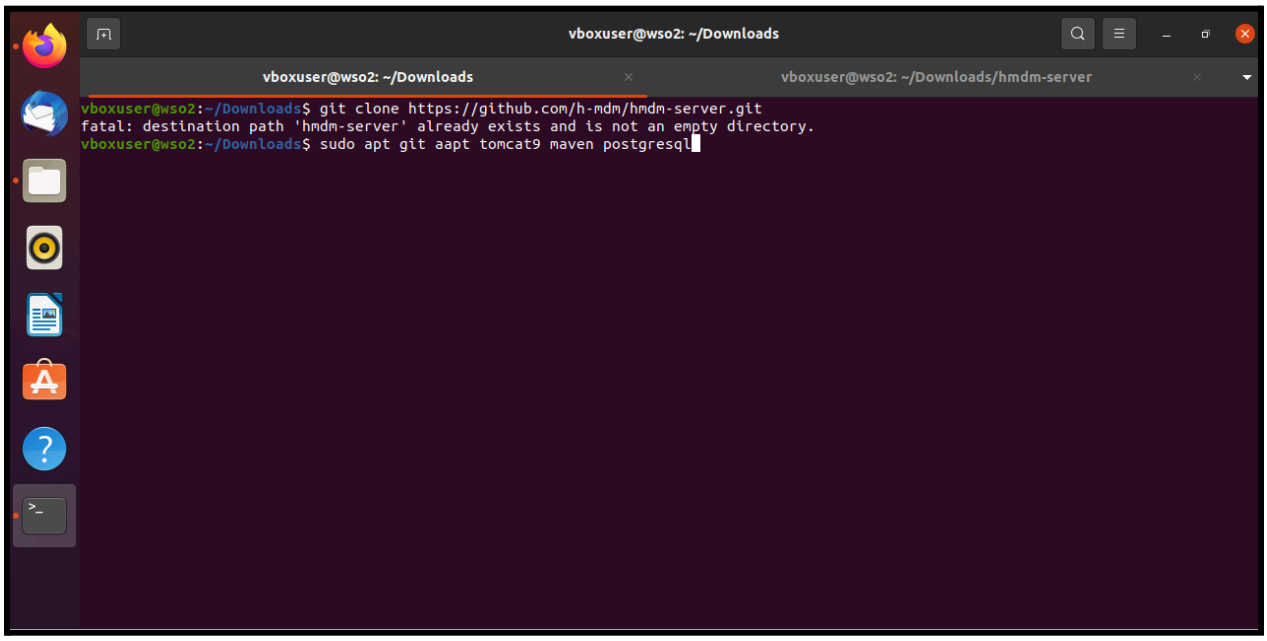


Clone the Repository

Download the HMDM server code from GitHub using Git:

```
git clone https://github.com/h-mdm/hmdm-server.git
```

```
cd hmdm-server
```



Then install server requirement which will help to build server

```
Sudo apt git aapt tomcat9 maven postgresql

cd hmdm-server
```

Then setup DATABASE in `postgresql using cmd`

```
Sudo su postgresql

      :psql

      :CREATE USER hmdm WITH PASSWORD 'topsecret';

      :CREATE DATABASE hmdm WITH OWNER = hmdm;

      :\q

      :exit
```

The go to the repo you cloned and run the following cmd

cd hmdm-server

:mvn install (after running this cmd wait for the process completion)

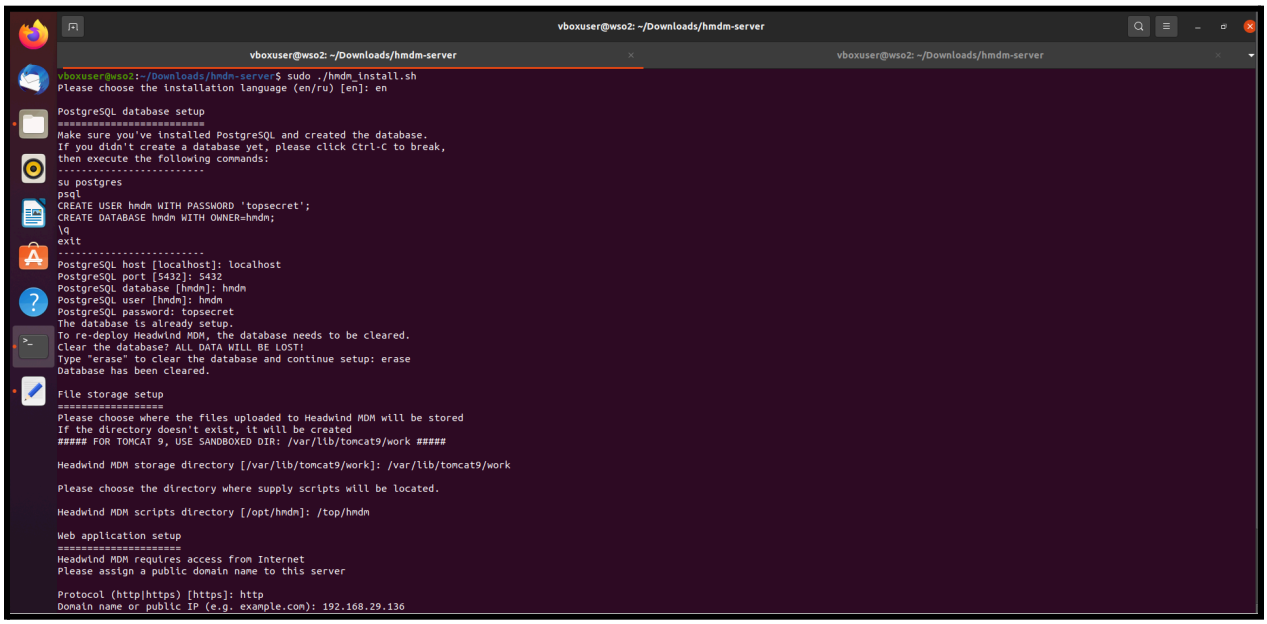
```
vboxuser@wso2:~/Downloads/hmdm-server$ mvn install
[INFO] Scanning for projects...
[INFO] ------------------------------------------------------------------------
[INFO] Reactor Build Order:
[INFO]
[INFO] Headwind MDM                                                       [pom]
[INFO] Core for MDM API                                                   [jar]
[INFO] JWT Auth for MDM API                                               [jar]
[INFO] Push Notifications for MDM API                                     [jar]
[INFO] Plugins for MDM Server                                             [pom]
[INFO] Plugin Platform for MDM Server                                     [jar]
[INFO] Device Log Plugin for MDM Server                                   [pom]
[INFO] Device Log Plugin for MDM Server - Core                            [jar]
[INFO] Device Log Plugin for MDM Server - Postgres                        [jar]
[INFO] Audit Plugin for MDM Server                                        [jar]
[INFO] Device Detailed Info Plugin for MDM Server                         [jar]
[INFO] Messaging Plugin for MDM Server                                    [jar]
[INFO] Push Messaging Plugin for MDM Server                               [jar]
[INFO] A Promo plugin                                                     [jar]
[INFO] Swagger UI                                                         [war]
[INFO] MDM Server                                                         [war]
[INFO]
[INFO] --------------------------< com.hmdm:root >---------------------------
[INFO] Building Headwind MDM 0.1.0                                     [1/16]
[INFO] --------------------------------[ pom ]---------------------------------
[INFO]
[INFO] --- maven-install-plugin:2.4:install (default-install) @ root ---
[INFO] Installing /home/vboxuser/Downloads/hmdm-server/pom.xml to /home/vboxuser/.m2/repository/com/hmdm/root/0.1.0/root-0.1.0.pom
[INFO]
[INFO] --------------------------< com.hmdm:common >-------------------------
[INFO] Building Core for MDM API 0.1.0                                 [2/16]
[INFO] --------------------------------[ jar ]---------------------------------
[WARNING] The POM for com.sun.xml.bind:jaxb-core:jar:2.2.11 is invalid, transitive dependencies (if any) will not be available, enab
le debug logging for more details
[WARNING] The POM for com.sun.xml.bind:jaxb-impl:jar:2.2.11 is invalid, transitive dependencies (if any) will not be available, enab
le debug logging for more details
[INFO]
[INFO] --- maven-resources-plugin:2.6:resources (default-resources) @ common ---
[WARNING] Using platform encoding (UTF-8 actually) to copy filtered resources, i.e. build is platform dependent!
[INFO] Copying 5 resources
```

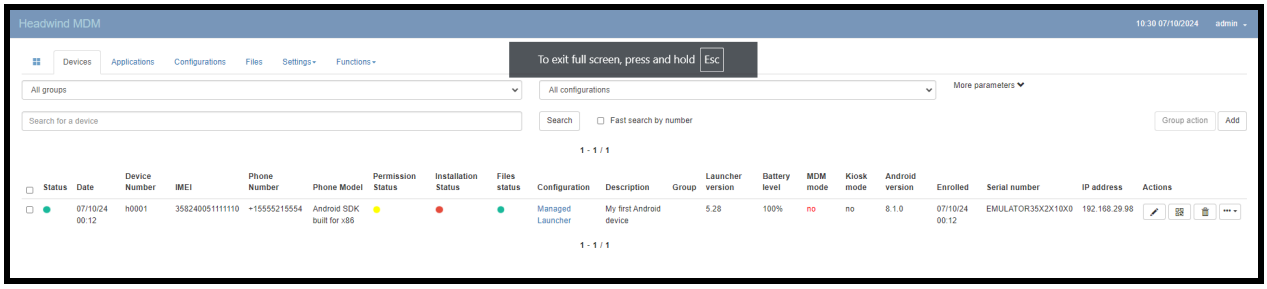
```
[INFO]
[INFO] Headwind MDM ........................................ SUCCESS [  0.910 s]
[INFO] Core for MDM API .................................... SUCCESS [  6.869 s]
[INFO] JWT Auth for MDM API ................................ SUCCESS [  0.772 s]
[INFO] Push Notifications for MDM API ...................... SUCCESS [  1.484 s]
[INFO] Plugins for MDM Server .............................. SUCCESS [  0.023 s]
[INFO] Plugin Platform for MDM Server ...................... SUCCESS [  0.218 s]
[INFO] Device Log Plugin for MDM Server .................... SUCCESS [  0.018 s]
[INFO] Device Log Plugin for MDM Server - Core ............. SUCCESS [  0.226 s]
[INFO] Device Log Plugin for MDM Server - Postgres ......... SUCCESS [  0.128 s]
[INFO] Audit Plugin for MDM Server ......................... SUCCESS [  0.129 s]
[INFO] Device Detailed Info Plugin for MDM Server .......... SUCCESS [  0.411 s]
[INFO] Messaging Plugin for MDM Server ..................... SUCCESS [  0.133 s]
[INFO] Push Messaging Plugin for MDM Server ................ SUCCESS [  0.099 s]
[INFO] A Promo plugin ...................................... SUCCESS [  0.070 s]
[INFO] Swagger UI .......................................... SUCCESS [  2.585 s]
[INFO] MDM Server .......................................... SUCCESS [ 27.877 s]
[INFO] ------------------------------------------------------------------------
[INFO] BUILD SUCCESS
[INFO] ------------------------------------------------------------------------
[INFO] Total time:  42.695 s
[INFO] Finished at: 2024-10-07T10:48:27+05:30
[INFO] ------------------------------------------------------------------------
vboxuser@wso2:~/Downloads/hmdm-server$
```

Then run cmd

```
Sudo ./hmdm_install.sh

      :localhost

      :5432

      :hmdm

      :topsecret

      :/var/lib/tomcat9/work

      :/top/hmdm

      :http or https (its on you)

      :your ip

      :8080

      :root

      :N

      :Y (if everything is right then y)

      :N

      :Y
```

Once the process is done the url and credentials are given to you then open url and login to the particular page with credentials now you are able to see dashboard



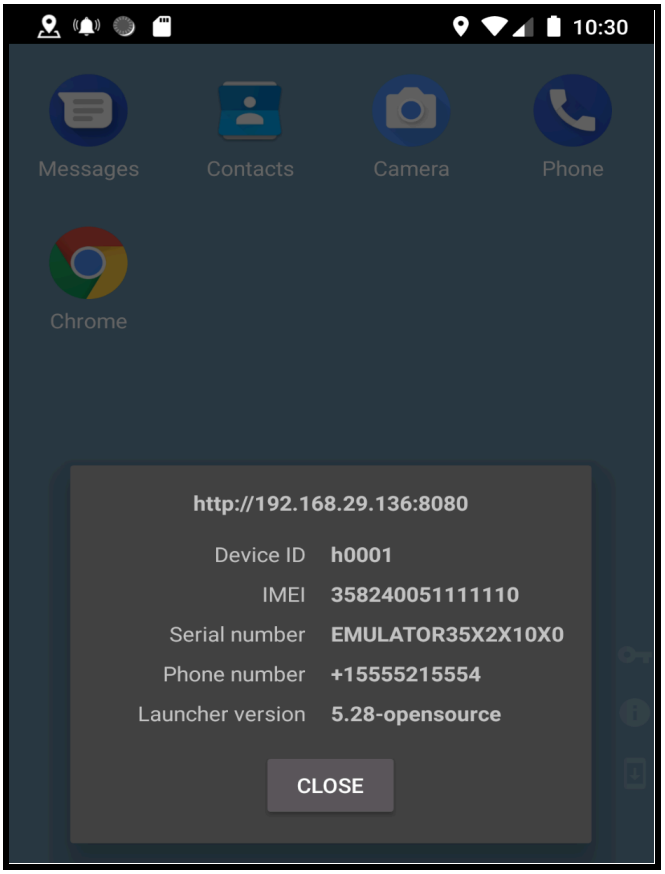


Inside this dashboard you see qr code on the device number h0001 just scan that qr with the device you want to connect and then install that app into particular apk in that after that you have all access to the device

one example are below like logs

Date and Time	Device number	Application	Severity	Message
07/10/2024 10:30:09.907	h0001	com.hmdm.launcher	VERBOSE	Update flow completed
07/10/2024 10:30:08.435	h0001	com.hmdm.launcher	WARNING	Failed to download app com.hmdm.emuilauncherrestarter: Bad server response for http://192.168.29.136:8080/files/LauncherRestarter-1.04.apk: 404
07/10/2024 10:30:08.401	h0001	com.hmdm.launcher	DEBUG	Downloading app: com.hmdm.emuilauncherrestarter
07/10/2024 10:30:07.325	h0001	com.hmdm.launcher	WARNING	Failed to download app com.hmdm.pager: Bad server response for http://192.168.29.136:8080/files/pager-1.02.apk: 404
07/10/2024 10:30:07.290	h0001	com.hmdm.launcher	DEBUG	Downloading app: com.hmdm.pager
07/10/2024 10:29:56.688	h0001	com.hmdm.launcher	WARNING	Failed to download app com.hmdm.pager: Bad server response for http://192.168.29.136:8080/files/pager-1.02.apk: 404
07/10/2024 10:29:56.652	h0001	com.hmdm.launcher	DEBUG	Downloading app: com.hmdm.pager
07/10/2024 10:29:55.866	h0001	com.hmdm.launcher	WARNING	Failed to download app com.hmdm.pager: Bad server response for http://192.168.29.136:8080/files/pager-1.02.apk: 404
07/10/2024 10:29:55.826	h0001	com.hmdm.launcher	DEBUG	Downloading app: com.hmdm.pager
07/10/2024 10:29:54.935	h0001	com.hmdm.launcher	WARNING	Failed to download app com.hmdm.pager: Bad server response for http://192.168.29.136:8080/files/pager-1.02.apk: 404
07/10/2024 10:29:54.897	h0001	com.hmdm.launcher	DEBUG	Downloading app: com.hmdm.pager
07/10/2024 10:29:54.131	h0001	com.hmdm.launcher	WARNING	Failed to download app com.hmdm.pager: Bad server response for http://192.168.29.136:8080/files/pager-1.02.apk: 404
07/10/2024 10:29:54.100	h0001	com.hmdm.launcher	DEBUG	Downloading app: com.hmdm.pager
07/10/2024 10:29:50.015	h0001	com.hmdm.launcher	WARNING	Failed to download app com.hmdm.pager: Bad server response for http://192.168.29.136:8080/files/pager-1.02.apk: 404
07/10/2024 10:29:49.976	h0001	com.hmdm.launcher	VERBOSE	GPS location update: lat=37.421998333333335, lon=-122.08400000000002
07/10/2024 10:29:49.961	h0001	com.hmdm.launcher	DEBUG	Downloading app: com.hmdm.pager

Just one example of we connected to device



Impact:

Configuring MDM tools like HMDM and Miradore plays a critical role in enhancing organizational security. By centralizing control over mobile devices, MDM solutions help protect sensitive data, ensure compliance with security policies, and mitigate risks associated with unmanaged devices. The ability to enforce security protocols remotely ensures that even large fleets of mobile devices remain secure, making MDM an essential component in modern cybersecurity strategies for businesses and institutions.

Conclusion:

Configuring an MDM tool, whether open-source like HMDM or a free-trial solution like Miradore, is crucial for managing and securing mobile devices in organizational settings. These tools allow for centralized control over security policies, app installations, and device monitoring, which ensures that mobile devices are compliant with organizational standards. The hands-on configuration of HMDM and Miradore highlighted how MDM solutions enhance mobile security and management at scale.