

*KOÇ UNIVERSITY*

*College of Engineering*

**DEPARTMENT OF COMPUTER ENGINEERING**

### COMP 291

### SUMMER PRACTICE

#### SUMMER PRACTICE Work/Project Summary

*Record your daily activities in the Work/Project Summary tables as shown below. Include the tasks accomplished and hours spent for the task during the practice and get each page signed by your supervisor.*

**Student Name: Mehmet Murat Budak**

**Starting Date: 19.06.2023**

**Completion Date: 18.08.2023**

**Total Working Days (full-time equivalent): 25**

**Summer Practice # (291 or 391): 291**

**Company : Koç University IT**

**Department : Information Security**

**Address :** **RUMELİFERİYOLU SARIYER KOÇ ÜNİVERSİTESİ KAMPÜSÜ İSTANBUL İSTANBUL No:X /**

**Supervisor (Name, Department, Phone, Fax, E-mail, etc.):**

Ertuğrul Doğan, Information Security, Work Phone: +90 212 338 1432, Mobile: +90 5438851861, E-mail: edogan@ku.edu.tr

**Signature of Supervisor:**

|  |  |  |
| --- | --- | --- |
| Work  Day | Date | Work / Project Description |
| 1 | 17/07/2023 | Conducted a vulnerability scan on the school's IT VLAN network using Nessus and learned how to use the Nessus tool. Analyzed the vulnerabilities discovered and researched how to validate these findings using tools like Nikto and Open Vuln Searcher. |
| 2 | 18/07/2023 | Explored open-source vulnerability detection software and attempted to install Greenbone OpenVAS (GVM) on my local Kali system without success despite extensive efforts. |
| 3 | 19/07/2023 | Since I was not able to install GVM on my Kali system, I decided to try installing GVM on an Arch system because I thought AUR would have more flexible install options.  Spent the day installing GVM and Arch Linux to my local system, successfully setting up GVM using Docker containers on Arch Linux. |
| 4 | 20/07/2023 | After my success with Arch, I retried to install GVM on Debian, I sought help from ChatGPT on my extensive debugging efforts and was able to initialize a web UI of GVM. |
| 5 | 21/07/2023 | Participated in a morning meeting to discuss weekly activities and future plans. Attempted to scan the school's network with GVM but faced socket compatibility issues between the scanning service and the main service. Spent the entire day debugging without resolving the issue. |
| 6 | 24/07/2023 | After facing issues with GVM on Debian, switched to Arch Linux and successfully ran GVM through Docker containers. Scanned my local network for vulnerabilities and compared the results with Nessus. Later, attempted to scan the school's IT VLAN subnet, but encountered VPN connectivity issues which prevented me from accessing the VLAN network. |
| 7 | 25/07/2023 | Received no response on the Trackit ticket, thereby halting vulnerability scanning activities. Spent a significant part of the day on hackthebox.com, gaining insights into networking and pentesting. Conducted research on Android pentesting. |
| 8 | 26/07/2023 | Installed Genymotion for Android penetration testing and explored alternative products used by other companies. Learned about important aspects of security in Android applications. |
| 9 | 27/07/2023 | Investigated why my VPN connection to the IT VLAN subnet was interrupted. Found out that the VPN network restricted my access to the school's networks post-GVM scan. Sought information on networks through hackthebox.com to understand the issue. |
| 10 | 28/07/2023 | Obtained permission to scan the subnet where VPN connections exist instead of the IT VLAN network. Conducted the scan, which took approximately 5 hours, and shared the results in a report format. Later, analyzed the identified vulnerabilities. |
| 11 | 31/07/2023 | Collected information on Android penetration testing, installed the newly developed KUAPP application to be tested on a virtual device in Android Studio, and examined the APK directory. Reviewed other Android pentest tools. |
| 12 | 01/08/2023 | Continued research on networking, which helped me better understand the workings of the school network. Reinforced the knowledge gained through Hackthebox. |

**WORK / PROJECT SUMMARY**

Student’s Name:

Student’s Signature: Date:

Supervisor’s Name:

Supervisor’s Signature: Date:

**WORK / PROJECT SUMMARY (Continued)**

|  |  |  |
| --- | --- | --- |
| Work  Day | Date | Work / Project Description |
| 13 | 02/08/2023 | Provided feedback on the new KU website. Watched YouTube tutorials about Android Studio. Attempted beginner-level Android application penetration tests on Hackthebox but was unsuccessful. Reviewed penetration testing walkthroughs to gain more knowledge on the tools used. |
| 14 | 03/08/2023 | Performed a static analysis of KuAPP using MobSF and generated a report, which I shared and reviewed with Oğuz Özkan. Attempted to establish a connection between the emulator required for dynamic analysis and MobSF, but was unsuccessful. Utilized Docker for these tasks. |
| 15 | 04/08/2023 | Explored other automated tools for Android penetration testing. Abandoned most of the found tools as they were no longer updated. Completed Hackthebox's Android pentest tutorial. Planning to analyze the application's web traffic using Burpsuite with a proxy next monday. |
| 16 | 07/08/2023 | Faced various issues with my Linux system, particularly with the systemd bootloader, which prevented me from booting into the system. Tried to resolve the problem using live ISO and chroot but was unsuccessful. |
| 17 | 08/08/2023 | Decided to reinstall my system from scratch with Arch Linux. Spent the day preparing the system and performing necessary configurations. |
| 18 | 09/08/2023 | Prepared the necessary configurations for OpenVAS to perform vulnerability scanning on over 100 websites within the school's network and reviewed the report. |
| 19 | 10/08/2023 | After sharing the report, I investigated why I could not connect to VPN from my Linux machine. Found similar issues on Openconnect's GitHub issues but was unable to resolve it, prompting me to contact the school's IT yet again. |
| 20 | 11/08/2023 | Completed stages of exploiting vulnerabilities in MSSQL, SMB, and AWS services on hackthebox.com. Examined how automated tools like GVM detect vulnerabilities like SQL injection. |
| 21[[1]](#footnote-1)∗ | 14/08/2023 | Attempted to resolve VPN issues with IT but was unsuccessful. Tested the VPN connection with different Linux systems but couldn't connect with any. Tried alternate VPN solutions as suggested by IT, but those did not work either. |
| 22 | 15/08/2023 | Connected to the Kali machine assigned to me on the school's network via CyberArk. Completed system updates and installed other libraries and packages used by Docker and GVM. |
| 23 | 16/08/2023 | Encountered an error indicating disk space was full while trying to download OpenVAS containers. Spent the rest of the day waiting for a response after emailing the relevant individuals. |
| 24 | 17/08/2023 | Received a reply from IT stating the issue was related to RAM, not disk space. Tried to restart the installation but 16GB of space was insufficient. Realized the issue was with the configuration of the \var directory. Changed the target directory in Docker’s config, resolving the issue. |
| 25 | 18/08/2023 | Successfully started all GVM services and accessed GVM's web interface through my browser. Configured the web interface settings and created the necessary accounts for management. |

Student’s Name:

Student’s Signature: Date:

Supervisor’s Name:

Supervisor’s Signature: Date:

1. ∗ Internships after 20 full-time work days are optional, but 20 days of full-time equivalent work is required. [↑](#footnote-ref-1)