



College of Engineering
Al Ain University, Abu Dhabi, U. A. E.

Internship Final Report

Student Name: Sheikha Basheer



Company Name: Timex IT Consulting

Internship Coordinator: Dr. Yazan Al-Ahmed

Internship Supervisor: Mr. Mohamed Hassan

Internship Start Date: 16/10/2023

Internship End Date: 18/02/2024

Declaration

I, Sheikha Basheer, declare that this report titled 'Internship Final Report' is my original work.

All information and analysis contained in this report is based on my research and is my intellectual property unless otherwise stated. External sources used in this report have been properly cited and referenced.

I understand that plagiarism in any form is a serious academic offense and that I am responsible for ensuring the originality of this work.

Acknowledgment

I would like to thank God and then my parents for making me reach where I am today. Al Ain University has enabled me to acquire immense knowledge and skills that will help me throughout my lifetime, which includes my internship opportunity at Timex as a Cybersecurity intern. I sincerely thank the University as well as my internship coordinator, Dr. Yazan Al Ahmed for providing me this internship opportunity where I was able to apply and put in practice the knowledge and skills I developed throughout my academic journey.

I am also very grateful for the invaluable support Dr. Yazan has offered me in completing my internship journey as well as the owner and CEO of Timex IT Consulting, Mr. Hassan. The supportive and encouraging environment helped me to complete my internship stress free and was able to be productive throughout. Notably, I was able to build effective communication and teamwork capabilities enhancing my personal and professional growth. I consider this a great experience and a huge accomplishment as I finish my internship journey.

Executive Summary

During my internship period, I joined Timex IT consulting in Abu Dhabi as a cybersecurity intern where I had the opportunity to work on several security operations and functions. Timex IT Consulting is an IT business firm providing several IT services in software and cybersecurity alongside with consultation services to its clients.

Although their primary operations include software development and distribution which I was also part of, recently, cybersecurity services and implementation has been of great importance and attended actively. Their services include but not limited to:

- Software development based on Client requirement
- Accounting software Implementation and maintenance
- HRMS Software with 5+ functionalities to its clients
- IT support and assistance
- IT consulting along with software training
- Basic network security services like firewall
- Endpoint security to clients

Professionals at Timex closely analyzes and discuss client needs and requirement to develop software that are of high quality with reasonable prices that falls within their budget. Most or all the clients Timex deals with are Small and Medium Enterprise (SME) business that often lack basic cybersecurity measures. My internship duties mainly revolve around experimenting with security tools, deploy certain security mechanism, research into security solutions for SME and other tasks assigned to me by the supervisor

I started my internship with research into the cybersecurity measures that are of utmost urgency to SMEs. Meanwhile, I also studied and understood client business operations and how to incorporate security measures to their business that profits them instead of interrupting their business operations. Then I moved on to deploying basic network security that can be used in SMEs. Some of the security measures include implementing intrusion detection system which was accomplished using Snort IDS and deploying firewall.

I was also introduced to several policy that Timex adopts for securing their digital assets. Thus, I was able to work on password policies and refine them after analyzing current documents and procedures. I had also worked on firewalls in general and particularly on Palo Alto firewall which is one of the best Next-Generation Firewall (NGFW). Since SME require basic firewall, my training encircled on only basic firewall configuration. Timex provides its SME clients sever resources using VMware cloud services therefore, I also learned cloud types and services pertaining to VMware and worked on managing resources and applications.

Furthermore, I was also introduced and trained on software development that includes Java application development, Servlet API in web application, Minimal API in .NET core alongside with secure coding practices. I also implemented and experimented several encryption techniques. Later, I worked with setting up endpoint security tool Wazuh, setting up VMs and learning Kali Linux. Finally, I was assigned to develop a hashing tool that produces hashes as well as conduct dictionary attacks.

Overall, I had the opportunity to experience and learn several aspects of cybersecurity and different operations in an IT firm, rather than focusing on one single task or operation.

Table of Contents

Introduction	8
Description of the Company	9
Industry and services provided.....	9
Timex HRMS and Accounting Solution	10
Sage.....	11
Timex address and online details.....	11
Internship Activities	12
Intern duties and work environment.....	12
Intern Supervisor	12
Practicum outcomes	14
Week 1:	14
Week 2:	14
Week 3:	16
Week 4:	17
Week 5:	18
Week 6:	20
Week 7:	22
Week 8:	24
Week 9:	25
Week 10:	26
Week 11:	28
Week 12:	30
Week 13:	32
Week 14:	33
Week 15:	34
Week 16:	36
How did Al Ain University prepare me for the Internship?	38
Assessment of the Internship	38
Duties carried out as an intern	38
How will the internship affect my future professional goals?	39
Internship-related activities compared to what I learned at the university.....	39
Differences between Theory and Professional experiences.....	39

Hard and soft skills acquired	40
Hard skills	40
Soft skills	40
Difficulties during the Internship	41
Conclusions	42
References.....	44

Introduction

“An internship is a professional learning experience that offers meaningful, practical work related to a student’s field of study or career interest. An internship gives a student the opportunity for career exploration and development, and to learn new skills.” [1] Internships are also important to acquire a professional degree, enabling students to gain real work experience and at the same time contributing to the company. Many a times, internship acts as a kickstart to one’s career; providing immense opportunities.

This report consists of comprehensive description and details regarding my weekly activities, tasks and assignments assigned to me by the company. As per the university requirement, a total of 640 hours needed to be worked as an intern to be able to achieve credit hours. As a prerequisite, a total of 100 credit hours must be covered by the student to start their internship. This ensures that the student has basic knowledge and fundamentals that can help them in their internship

As a cybersecurity intern at Timex, I had the privilege to experience real tasks and challenges that might be faced by a typical cybersecurity analyst. Cybersecurity has become increasingly worrying matter for small businesses and the lack of skilled cybersecurity expertise is evident in the job market. By providing me an opportunity to experience and work with basic security tools and solutions that many businesses require in their day-to-day activities; the company tries to fill this gap in the job market.

Description of the Company



Figure 1 Timex logo

Timex IT Consulting

Timex IT Consulting is a software developing and consulting company that provides custom software solutions to its clients as well as consulting services. They started their journey in providing software in accounting which has now expanded to restaurant software and web applications, Human resource software consisting of Manpower Supply & Agent Recruitment Service, E-Academy software, Transportation software and basically any software based on the customer request. Their 25 years journey in the field of software development has made them professionals in development and consulting. Apart from these, they now have recently started to investigate cybersecurity solutions and services they can offer to their clients. Therefore, joining as a cybersecurity intern, my tasks mainly revolved around research and experimenting with appropriate security solutions that best fit their clients.

The company is a client driven and an innovative workspace setting that puts their customer requirements before anything. Their honesty and dedication to provide high quality products is what keeps their customers loyal.

Industry and services provided

Timex IT consulting provides a wide variety of solutions, of which, few of them are discussed below.

Timex HRMS and Accounting Solution

Among the software solutions, HRMS software is mostly requested by their clients, and it is also one of the well-developed software packages they produced. Pettysoft is the main application program that have been developed from scratch and upon which several software have been developed. Being an authorized distributor for Pettysoft services in the Middle East, the solutions that have been developed were easily integrated with existing software especially in accounting domain and offered to clients. HRMS solutions with various functionalities are also distributed similarly. The software provided does not only come with one functionality but rather a wide variety of them. Following are their brochures for HRMS and Accounting solutions respectively.



Figure 2 Pettysoft features 1

The diagram illustrates the features of the 360 ERP software. At the center is a circle labeled "360 ERP". Surrounding it are several functional modules, each represented by a colored circle with an icon and a label. These modules include: SALES (yellow circle with a person icon), RECEIPT (yellow circle with a person icon), PROJECT MANAGEMENT (yellow circle with a person icon), INVENTORY CONTROL (yellow circle with a person icon), JOURNAL (yellow circle with a person icon), ADJUSTMENT (yellow circle with a person icon), PAYROLL (yellow circle with a person icon), ACCESS CONTROL (yellow circle with a person icon), TIME MANAGEMENT (yellow circle with a person icon), EMPLOYEE EXPENSES CLAIM (yellow circle with a person icon), EMPLOYEE SUPPLIES / ASSETS (yellow circle with a person icon), EMPLOYEE SELF SERVICE (yellow circle with a person icon), EMAIL ALERTS (yellow circle with a person icon), JOB PROFIT REPORT (yellow circle with a person icon), WORK FLOW (yellow circle with a person icon), SCHEDULE / APPOINTMENT (yellow circle with a person icon), LEAVE PLANNER (yellow circle with a person icon), END OF SERVICE (yellow circle with a person icon), ALLOWANCE ACCRUAL (yellow circle with a person icon), BENEFITS (yellow circle with a person icon), ATTENDANCE CONTROL (yellow circle with a person icon), RULES (yellow circle with a person icon), and SHIFT PLANNING (yellow circle with a person icon). The Pettysoft logo is in the top right corner.

For: Startup - SME - Corporate
Integrated
Software Solutions To Run Your
Entire Business Operation

For Trading -
Service - Manufacturing -
Project with Effective Control

**DIGITAL WORK PLACE
FOR YOUR ENTIRE
BUSINESS OPERATION!**

Industry experienced consultants assist you to
bring a digital nervous system to your firm.
Integrated with Power Business Intelligence.

Including:

1. Complete Accounting and Inventory Control
2. Project Management
3. Budget Control
4. Document Control
5. Notification and Audit
6. Approval (Request, Approval & Workflow)
7. HRMS (Task/Schedule/Payroll/ WPS/Jobs)
8. BI - Business Intelligence
9. Integration DN, Device and Sensor

Please contact:
TIMEX IT CONSULTING
Tel: 02-6769612, Mobile: 050-6171125
Email: info@timexit.ae

www.dc360erp.com

Figure 3 Pettysoft features 2

Sage

Sage is an accounting software specifically developed for SME. Timex is an authorized business partner of Sage, also offering customized Sage application to its clients. Timex offers free demo, premium support, installation, annual maintenance, premium training and online and onsite support to the clients. Along with sage applications, currently several software and services are being offered by Timex as the following brochure details.

TIMEX
IT CONSULTING
OVER **25-YEARS**
PROVIDING ACCOUNTING
& SOFTWARE SOLUTIONS



www.timexitconsulting.com

EXTENDING SOFTWARE SUPPORTS GLOBALLY SINCE-1995

FACTORY

- Plastic
- Gas
- Steel
- Cement & Bricks
- Dates
- Dust & Auto Filters
- Filter Manufacturing
- Petro-Chemical
- Paint & Thinner

WORKSHOP

- Automobiles
- Gold
- Carpentry
- Studio
- Graphics
- Glass & Fabrication
- Yard & Rig

CONSTRUCTION

- City-Units
- Tower
- Villas
- Landscaping
- Demolishing & Pilling
- Electrical & Civil

FOOD

- Restaurant
- Club Outlet
- Chain Outlet
- Five Star Hotel Outlet
- Nutrition Diet

TRANSPORTATION

- Abnormal Loading
- Heavy Vehicle
- Rent-A-Car
- Shipping
- Cargo
- Travels

TRADING

- Gold
- Fashion Wear
- Eye Wear
- Shoes
- Flowers
- Building Material
- Supermarket

EDUCATION

- Institute
- School

HEALTH

- Gym & Fitness
- Spa Center
- Karate Club
- Beauty Saloon
- Hospital & Clinic

HUMAN RESOURCE

- Man Power Supply & Agent
- Recruitment Service

TECHNOLOGY

- Network & Security
- IT Consultant

PROFESSIONALS

- Law Firm
- Auditing Firm
- Investment House
- Businessmen Council
- Domain Consultant Firm

ROYAL FAMILIES

- Private Office
- Personal Accounts
- Property Management
- Real Estate

Figure 4 Sage features

Timex address and online details

Timex IT Consulting	
----------------------------	--

Office	Safari Fashions Building, Najda St, Abu Dhabi, UAE.
Mobile	+971506171125
Telephone	+97126769612
FAX	+971-2-6769613

Email	info@timexit.ae
Website	https://timexit.ae

Internship Activities

Intern duties and work environment

During my time in Timex, my duties primarily involved around experimenting and actively working with cybersecurity tools and solutions that work best with Small and Medium Enterprises (SME) as all the clients of Timex IT Consulting company fell under the SME category. My responsibility includes research into security solutions that are affordable and easy maintenance, install and deploy security solutions, learn secure coding and development, encryption algorithms, develop simple cybersecurity programs, handle security tools and corresponding reporting and documentation.

Intern Supervisor

The company is comprised of several employees mainly working in software development and services and the daily tasks assigned to me were from IT Consultant Abu Haneef Mohammed Hassan and supervised by the CEO of the company Mr. Mohammed Hassan. Through their guidance and feedback I was able to apply my knowledge which I have gained through my academic journey at Al Ain University.

Theoretical knowledge gained from university	Practical experience gained at the company
Major Cybersecurity concepts and fundamentals like CIAA (Confidentiality, Integrity,	<ul style="list-style-type: none"> ▪ Timex had several clients that are small & medium enterprise. Timex had deployed security mechanism and techniques that encircles the fundamental CIA principles ▪ I was introduced to password policies, authentication mechanisms and encryption techniques that were followed

Authentication & Authorization)	by the company and to their clients as well. I was part of refining and suggesting better options in their policies
Secure System Architecture and design that incorporates Firewalls, Intrusion Detection and Prevention System (IDPS) across business and Enterprise sectors	<ul style="list-style-type: none"> ▪ The network infrastructure and security implementation were not very sophisticated and advanced in Timex. They follow simple and basic security features that they require, and I had the opportunity to work on Palo Alto Firewalls and Intrusion detection system like Snort IDS. ▪ Worked on Wazuh Endpoint security system to monitor suspicious network and system activities and actively block them
Risk analysis and reporting; different phases and different procedures in each phase.	<ul style="list-style-type: none"> ▪ Various discussion on risk assessment techniques with the management and how to effectively carry out each phase in small enterprise system. Learned how to avoid complex security solutions that might disrupt business operation and only focus on security practices that benefit the business
Cloud fundamentals and how Cloud infrastructure is set up. Importance of Cloud security and how to protect from data breaches.	<ul style="list-style-type: none"> ▪ Learned and worked on PaaS and IaaS services Timex provides to its clients using VMware. Additionally learned to make use of cloud computing data storage for business and other operations. I also had the opportunity to manage and coordinate different applications on cloud and few experiments on Azure cloud as it also a popular cloud platform in the field.

Practicum outcomes

Week 1:

Dates: October 16, 2023 – February 18, 2024

Hours worked: 19

In the first week of the internship, I was given basic introduction to the company's services and products. I was given comprehensive details as to the different types of consultation provided by the company, introduced to the different aspects of integrating cybersecurity best practices and measures to clients.

I also analyzed how does the clients lack in security of the service consumption. Discussed security issues faced by the clients and how to tackle such issues. This was also the time when I was introduced to Small and Medium Enterprises (SME), who constitutes most of the company's clients. I had analyzed the cybersecurity trends in SME and certain cybersecurity measures that SMEs can deploy in business operations. During this time, I also made research into several latest issues that are faced by SME in terms of cybersecurity to better understand the job market and customer audience of Timex.

Week 2:

Dates: October 23, 2023 – October 29, 2023

Hours worked: 25

Preceding the first week, I was assigned to identify and report the main or critical cybersecurity issues SME faces based on my understanding from several research. The identified problems are

investigated from the data and infrastructure of SME provided by the company. Most companies do not care for security due to lack of expertise and understanding or categorized as 'too expensive'. The identified issues which are necessary in these companies are the following:

- No basic password policy
- No email policy (for what and what not emails can be used) and security.
- Absence of any network security (Sometimes no firewall as it is deemed unnecessary)
- Firewall rules without any updating

Other activities in the same week include:

- Explored and analyzed cybersecurity measures implemented by well-known industry and discussed to implement those measures to SMEs to improve security posture
- Provided effectively basic IT security consultancy to clients to create minimum awareness in the following areas:
 - Security needs like proper wireless encryption using WPA2 enabled.
 - Conduct regular cybersecurity assessments
 - Regular patch management and software updates
 - Conduct risk analysis to ensure effectiveness of security mechanism
 - Conduct penetration tests on web application and servers.

Additionally, I gathered information on publicly available data of certain cybersecurity-based companies to analyze how and type of security services provided by them. After various discussions with the instructor, eliminated certain security measures irrelevant to SME and only pertaining to those measures that benefit business operations of SME.

Week 3:

Dates: 30/10/2023 - 5/11/2023

Hours worked: 21

Main tasks and responsibilities include developing cybersecurity plan for SME in the following areas:

- Building effective security policies relating to the business operation of the SME
- Adopting a complete and sound email and password policy
- Risk Assessment and analysis; How to properly analyze and identify critical assets in the business through BIA (Business Impact Analysis)
- Implementing firewalls and Antivirus (AV) Other security measures like EDR (Endpoint detection & Response), SIEM

I was also introduced to basic network security like firewalls, antivirus protection. Proper monitoring of network traffic through IDS/IPS alert system using tools like Snort. This was also the time when I had studied Snort rule writing and updating of rules, matching to latest identified threats and vulnerabilities. I also discussed how can we deploy this IDS tool to some clients that might benefit from it. Later, I explored security standard like UAE Information Assurance (IA) Regulation and how to integrate them to businesses.

Finally, I drafted cybersecurity proposal for SME, addressing basic and urgent security needs and how to implement them through consultation services. Also prepared presentation for the draft proposal and presented to a panel of four members.

Week 4:

Dates: 6/11/2023 To – 12/11/2023

Hours worked: 33

In the 4th week, all I worked and experimented with was an Intrusion Detection System (IDS) tool named Snort. Snort is a very powerful and popular tool that is also affordable to SME enterprises. Snort can act as active Intrusion Prevention System (IPS) as well, however, as per our requirement, my focus was only on Snort IDS. First, I analyzed in-depth to implement IDS system within the network for generating basic security alerts. I was given training on configuring snort IDS to raise alerts for basic intrusion detection and self-studied the snort IDS tool to be able to implement in upcoming days.

Snort IDS- Part 1

- Configuration of Snort IDS System on networks to identify possible scanning and unauthorized connection to the internal Network
- Successfully detected external scanning attempts of ICMP ping and TCP scan
- Learned how to analyze logs and alerts in Snort.

Snort IDS- Part 2

- Configured Snort to detect FTP and SSH attempts on PCAP files provided by the company. The pcap files were old and I had the freedom to experiment with it a lot.
- Tested the newly configured Snort rules and demonstrated the Snort IDS logs and alerts raised from external scanning and unauthorized connection attempts

Snort IDS- Part 3

This was a miscellaneous activity that I had been given permission to do on my own.

“EternalBlue is a software vulnerability in Microsoft's Windows operating system. It targets the Windows Server Message Block (SMB) protocol, a network protocol that enables shared access to files, printers, and other resources within a network.” [2] EternalBlue vulnerability is still present in many Windows 7, which is why Microsoft has advised and is not responsible for such attacks. I had successfully configured Snort to detect any exploitation attempt in the provided logs and presented the results to management. For such reasons, the company also advise their clients to discontinue Windows 7 usage, if there is any.

- Configured snort to detect Eternal-Blue vulnerability in windows 7 by analyzing provided logs, and concluded no exploitation attempts has taken place for the provided logs.

Week 5:

Dates: 20/11/2023 To – 26/11/2023

Hours worked: 40

In the 5th week, I was introduced to one of the major issues in cybersecurity; password protection. To protect passwords across enterprises, first step towards it to implement strong and

relevant password policies. It is equally important to update these policies to keep up with latest vulnerabilities. My tasks included the following:

- Analyzed in detail the existing documents for password policies of the company.
- Received Password management training on:
 - Account lock-out procedure (How passwords that were not changed during set period will be locked out)
 - Validity period of passwords (How long to keep using same password before it is changed)
 - Password strength & length (Employees must adhere to the mentioned password length and include a variety of characters)
 - Unique password policy (Must not use same password for different accounts)
 - Salting and hashing (Passwords stored should always be salted and hashed)

After receiving rigorous training in password management, I reviewed and updated the documents for password policy per the guidelines provided by the company. My contribution included automating process of account lock-out procedure recovery, instead of having administrator recover manually and others including using advanced hashing. I was guided to implement updated password policy on few user-level accounts. I also enabled password encryption for provided few accounts.

Another simple yet effective security measure is to enable Multifactor Authentication (MFA). This also demonstrates how layered defensive measures is better than complex single security measure. I enabled on several client's Microsoft accounts guided by the instructor. I then tested and verified the operability of the newly enabled MFA

Later in the week, I was given training on SIEM tools particularly on Microsoft Sentinel. SIEM are relatively advanced and complex security measure that requires an expert in managing the tool. Although the company doesn't use SIEM, I was introduced and had experimented with basic functionalities of SIEM tools (Microsoft Sentinel or Splunk). I also learned integration of SIEM tools to Microsoft Defender for applications that are on cloud.

Week 6:

Dates: 27/11/2023 To – 10/12/2023

Hours worked: 40

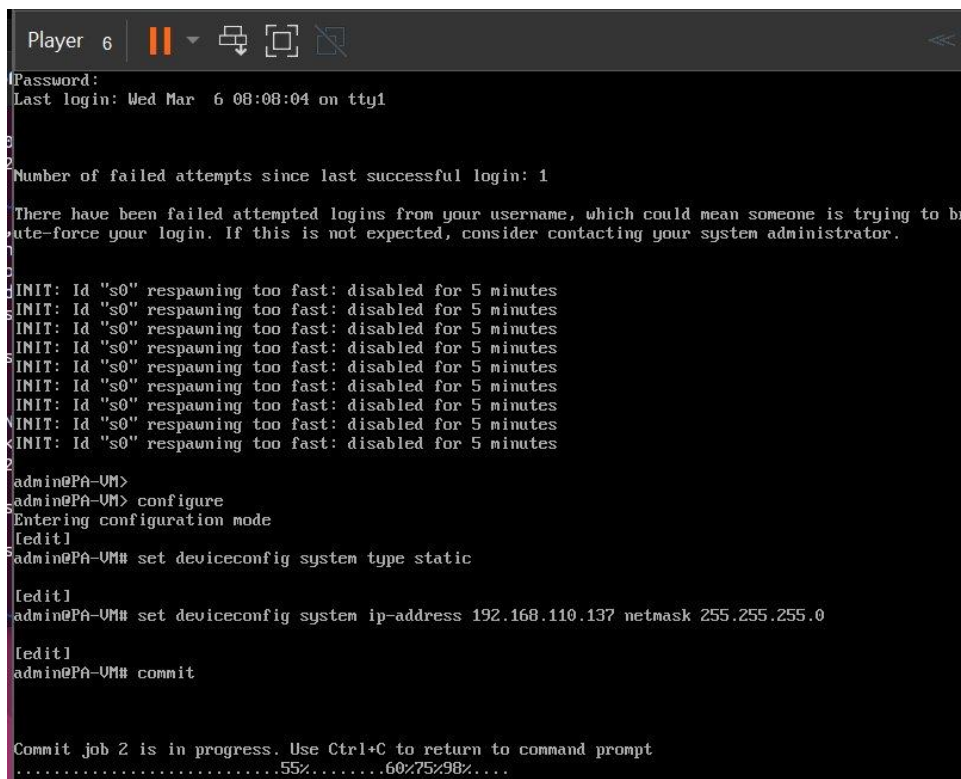
In this week, I learned about using and implementing Palo Alto firewall. My activities and tasks include the following:

- Learned the documents on Palo Alto Firewall and how to integrate the firewall into the corporate network successfully
- Analyzed the best security practices to be followed while integrating a firewall into a network
- Installed Palo Alto Firewall and connected with power

After installation, to be able to operate the firewall, I obtained and learned the following information from my instructor

- IP address for the management port (MGT)
- Netmask
- Gateway address
- DNS address

I initialized the firewall using an RJ-45 Ethernet cable connected to a computer. Set a strong password and configured the MGT port. Configured DNS, proxy server and update server settings with the given information. Here, I understood the importance of changing default settings

A screenshot of a terminal window titled "Player 6" showing a Palo Alto Firewall configuration session. The session starts with a login prompt for "admin" on "tty1". After a password is entered, the user is prompted for the number of failed login attempts (1) and a warning about brute-force attacks. The user then enters the "configure" command, which leads to the "edit" configuration mode. In this mode, the user sets the device configuration system type to "static" and then sets the IP address to "192.168.110.137" with a netmask of "255.255.255.0". After committing the changes, a progress bar shows the commit job is in progress, reaching 98% completion.

```
Player 6
Password:
Last login: Wed Mar  6 08:08:04 on tty1

Number of failed attempts since last successful login: 1

There have been failed attempted logins from your username, which could mean someone is trying to br
ute-force your login. If this is not expected, consider contacting your system administrator.

INIT: Id "s0" respawning too fast: disabled for 5 minutes
INIT: Id "s0" respawning too fast: disabled for 5 minutes
INIT: Id "s0" respawning too fast: disabled for 5 minutes
INIT: Id "s0" respawning too fast: disabled for 5 minutes
INIT: Id "s0" respawning too fast: disabled for 5 minutes
INIT: Id "s0" respawning too fast: disabled for 5 minutes
INIT: Id "s0" respawning too fast: disabled for 5 minutes
INIT: Id "s0" respawning too fast: disabled for 5 minutes
admin@PA-VM>
admin@PA-VM> configure
Entering configuration mode
[edit]
admin@PA-VM# set deviceconfig system type static
[edit]
admin@PA-VM# set deviceconfig system ip-address 192.168.110.137 netmask 255.255.255.0
[edit]
admin@PA-VM# commit

Commit job 2 is in progress. Use Ctrl+C to return to command prompt
.....55%.....60%75%98%.....
```

Fig.5 Palo Alto FW installation

Next day, I continued configuring a bunch of other settings. This was done carefully as one wrong setting can lead to a total chaos. Configured NTP server for date and time settings and configured the general settings per the company rules. Lastly, committed the firewall to the changes and connected it to the switch port on the management network

On the final day of working with the firewall, I successfully tested the connectivity of the firewall. I launched an SSH session to the firewall using newly assigned IP address and verified network access of the firewall. Alternatively, accessed the firewall via browser as well.

```

192.168.110.199 - PuTTY
login as: admin
Keyboard-interactive authentication prompts from server:
| Password:
| End of keyboard-interactive prompts from server
Last login: Wed Mar  6 11:47:39 2024

Number of failed attempts since last successful login: 0

admin@PA-VM> show interface management

-----
Name: Management Interface
Link status:
  Runtime link speed/duplex/state: 10000/full/up
  Configured link speed/duplex/state: auto/auto/auto
MAC address:
  Port MAC address 00:0c:29:bb:50:07
Ip address: 192.168.110.199

```

Fig.6. Launched SSH via PuTTY

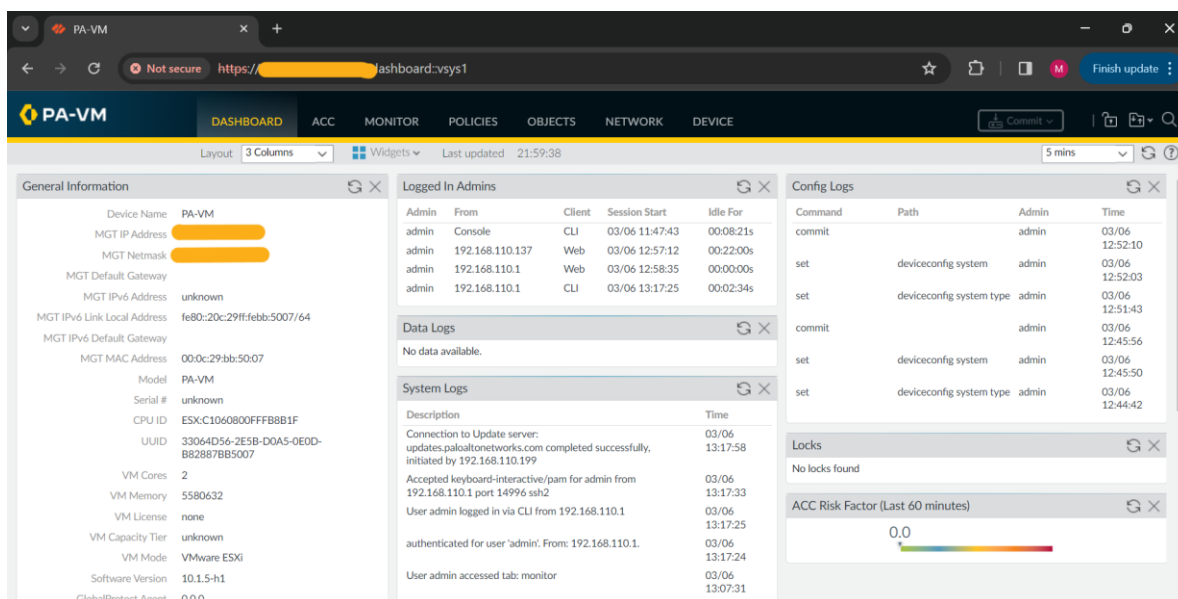


Fig.7. Palo Alto admin Dashboard successfully deployed

Week 7:

Dates: 11/12/2023 To – 17/12/2023

Hours worked: 40

During this week, I had discussion with the instructor and learned how to make use of cloud computing data storage for business and other operations. I also learned the usage of VMware cloud and Azure cloud services for expanding resources and hardware.

Studied in detail different cloud types, particularly on Infrastructure-as-a-service (IaaS) in VMware, which was offered by the company to its client, and Platform-as-a-service (PaaS) that satisfies company needs to develop, test and deploy software. Additionally, I learned how to deploy cloud types in hybrid (using resources on premises and on cloud) and multi cloud environment, where the company uses VMware and Azure cloud for client needs.

VMware cloud is completely based on hardware virtualization that doesn't require a host OS to run the expanding VMs. This increases its security as the VMs are independent of the host. If anything were to affect the host OS, the VMs running in that host will be affected and lost. This is one of the major security aspects I learned by analyzing hardware virtualization. I also understood how hardware and software virtualization works

VMware also allows to take snapshots of the VM, that way, if any testing crashes the VM, we can always go back to the state at which we took the snapshot. This was another great feature I learned while experimenting.

During the week, I gained knowledge on how VMware enables integration of applications hosted on cloud. My main tasks in the week include the following:

- Worked with VMware services that ensures application security.
- Worked with other VMware cloud-hosted service like VMware cloud web security
- Managed different apps hosted on cloud using VMware services
- Learned about how few client resources are hosted on Azure

- Learned about Azure configuration for resource expansion and managing client needs.

Week 8:

Dates: 18/12/2023 To – 24/12/2023

Hours worked: 40

Different from the previous weeks, in this week I worked on software development process in Java. This exposure really helped me to learn secure coding practices especially error handling and exception, which is major cause to crash the system while running or testing. My tasks on Introduction to Java application development include:

- In-depth understanding on Java Virtual Machine (JVM) Java Development Kit (JDK), Java Runtime Environment (JRE) & Just in Time Compiler (JIT)
- 10-12 hands on problem solving on expression statements, control statements and declaration statements

My tasks on Java Strings class Manipulation include:

- Utilized string buffer and String builder
- Applied different methods in string class & Unicode handling
- String concatenation using interpolation and concatenate

Tasks on Exception handling in Java:

- Utilized Properties class for Java configuration settings
- Implemented error-specific catch blocks for targeted exception handling.

Following days, I concluded with the following tasks:

- Experimented with nested exception, try-catch, finally and throw & throws statements for secure coding
- Understand how to securely code in Java using different exception and error handling statements.
- Password Hashing: Implement password hash utilizing BCrypt Library (Hashing, verification, salting, handling exceptions)

Figure 5 week 8

Week 9:

Dates: 25/12/2023 To – 31/12/2023

Hours worked: 40

During the 9th week of the internship, my primary subject was web app development in Servlet API, as many of Timex clients make use of web applications for their businesses. However, my tasks revolve around security aspects of the web app rather than pure development of the web apps. First few days, I was introduced to Servlet API- web app development and I explored input validation & secure session management in servlet

In brief, all the tasks and activities I worked throughout the week include:

- Configured web server (Tomcat 8.0) for secure and optimal performance
- Created and executed servlets on Tomcat server
- Created servlets extending `HttpServlet` class
- Mapped servlets in `web.xml`

As for the secure implementation tasks I had completed the following activities:

- Input validation using pattern matching: One major vulnerability that most web applications encounter is injection attacks. This happens when the user interface takes input and are allowed to enter whatever characters and values the user wish to enter. Malicious users take advantages of these and try to enter codes and programs that execute at the server causing XSS (Cross Site Scripting) or SQL injections attacks. I implemented security measure to validate input by checking if the input matches the expected strings of characters. If other values or characters are entered, they will not be accepted the application
- User input encoding: Before rendering the input to HTML, it is best practice to encode the user input using methods that encode strings.
- http -only and secure cookies: ‘SameSite’ attribute for cookies is a property that helps in preventing CSRF (Cross Site Request Forgery) and XSS attacks. When cookies are attempted to send in cross origin request, this attribute restricts it.
- Enabled CSP (Content Security Policy) header in servlet response
- Generated anti-CSRF tokens in multiple forms
- Experimented different security headers
 - HTTP Strict Transport Security (HSTS)
 - X-Content-Type-Options & X-Frame-Options

Week 10:

Dates: 1/1/2024 To – 7/1/2024

Hours worked: 40

API or Application Programming Interface is an important component in software development. API security has also become as serious issue as attackers target these components to exploit vulnerabilities. During this week I was introduced to minimal API, different methods like post, get, put and delete. I was assigned with securing minimal API data using standard encryption mechanism like AES. I installed and worked with Postman software used in testing and experimenting minimal API. I also learned difference between minimal & controller API which is another alternative to minimal API.

All my tasks and activities throughout the week include:

- Installed visual studio code and implemented basic minimal API using ASP.NET Core Empty template
- Verified functionality of the API using Postman
- Generated multiple endpoints in minimal API
- Created an encryption class using AES cipher to encrypt and decrypt string messages using key and Initialization vector (IV)
- Understood the importance of storing keys in configuration files
- Deserialized Json file to read keys from configuration
- Created classes with several properties to serialize object instance created in minimal API
- Implemented AES encryption class in minimal API in Json format and displayed results in postman as shown below

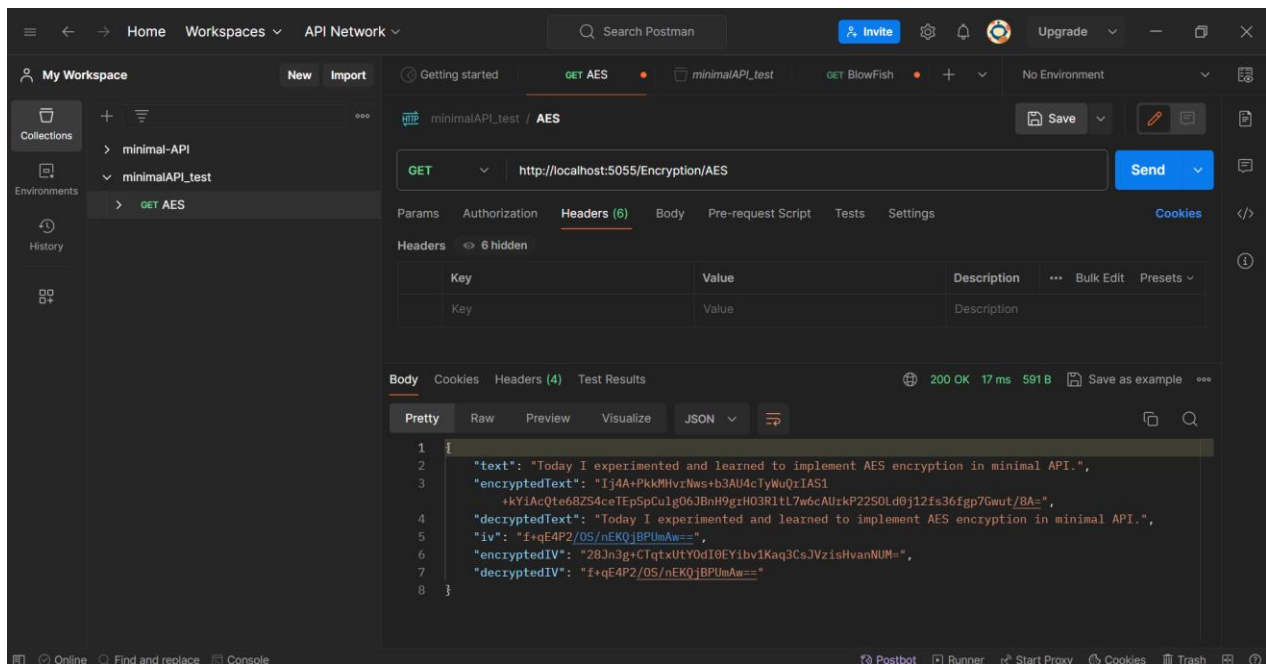


Fig.8. Postman AES results in JSON format

Week 11:

Dates: 8/1/2024 To – 14/1/2024

Hours worked: 40

In the succeeding week, I continued working with minimal API, but this time with an encryption system that is different from AES. I was tasked to deploy a different cipher as per the company requirement and decided to encrypt using Blowfish. This was after analyzing and understanding different modern symmetric ciphers like Twofish, Blowfish, IDEA (International Data Encryption Algorithm) and TEA (Tiny Encryption Algorithm). Later, I learned in-depth the Blowfish algorithm to be implemented in .NET core.

It also took time and dedication to understand the working of Blowfish Precalculated subkeys, pi's hexadecimal string predetermined to be used as IV for s-box and p-arrays in the succeeding days.

After, I went ahead with implementing Blowfish encryption algorithm in one of the endpoints in minimal API. Key must be stored in the config files and to read this key for encryption, key extraction from configuration file using deserialization of Json file has done.

Postman help simplify and testing of API and by working with the software, I was able to learn a lot about web API.

I verified using Postman the functionality of the Blowfish cipher. Using Postman, output was displayed in Json format.

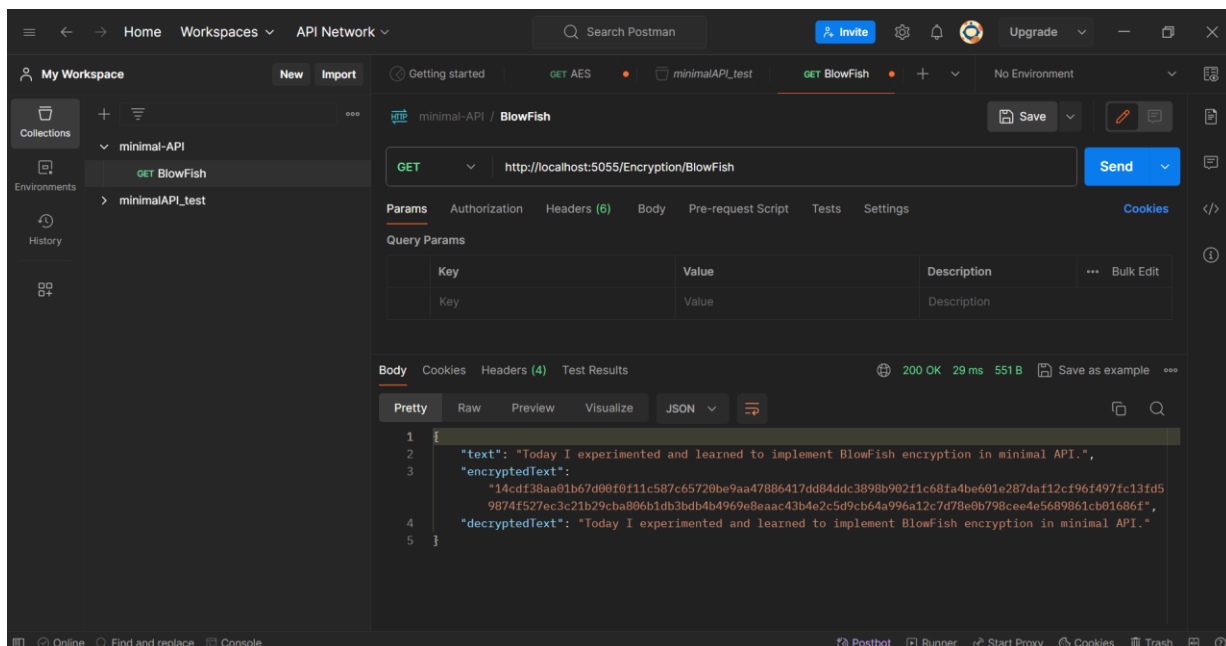


Fig.9. Postman BlowFish results in Postman

My next task was to encrypt images instead of strings. Therefore, I learned about image to array conversion types and techniques. Last day of the 11th week, I tried to Convert images to byte array and encrypt byte array, however, it was unsuccessful. Then I tried converting images to string type and encrypt strings using AES- this was partly successful, and I had to move with my next tasks and assignments for the next week.

Week 12:

Dates: 15/1/2024 To – 21/1/2024

Hours worked: 40

During the 12th week, I had an introduction to Endpoint Detection & Response (EDR). I analyzed in-depth EDR functions and services, understand different types including Indicators of Compromise (IoC) and Indicators of Attack (IoA). I learned that IoC are important indicators that tells us our system has been compromised while IoA tells us that an attack is still ongoing.

I had training on different EDR solutions and tools to be implemented in enterprise systems or workstations, Wazuh being one of them. Wazuh is a powerful opensource tool that actively monitors end system be it mobile phone, laptops, servers or even cloud instances. If a Wazuh agent is installed on the device, which is also a very lightweight program, then the Wazuh manager can analyze and alert any suspicious activity.

My tasks and responsibilities briefly are:

- Studied the Wazuh EDR tool to be able to implement in upcoming days.
- Learned Wazuh applications and its capabilities.
 - Intrusion Detection and Prevention System
 - File Monitoring
 - Log monitoring and analysis
 - Security Compliance Auditor
 - Network & Cloud Security

- Training on different Wazuh interfaces and components: Wazuh has 3 major components including the indexer, server and dashboard. I familiarized and understood these components that are very important to successfully monitor logs.
 - Components include Wazuh Server cluster, Indexer node, endpoint agent and Dashboard
 - Understand Wazuh architecture
- Learned different methods to install Wazuh: Wazuh can be installed in 2 modes- all in one packager and customized installation where the 3 components are installed manually on three different servers for better performance and security. However, I worked with all-in-one packager to monitor Linux and Windows devices
- Deployed Wazuh with Elastic Stack as directed in Wazuh documentation; to fit small workstations for testing and attack emulation as per the company requirement on Ubuntu server.
- Learned several Linux Commands

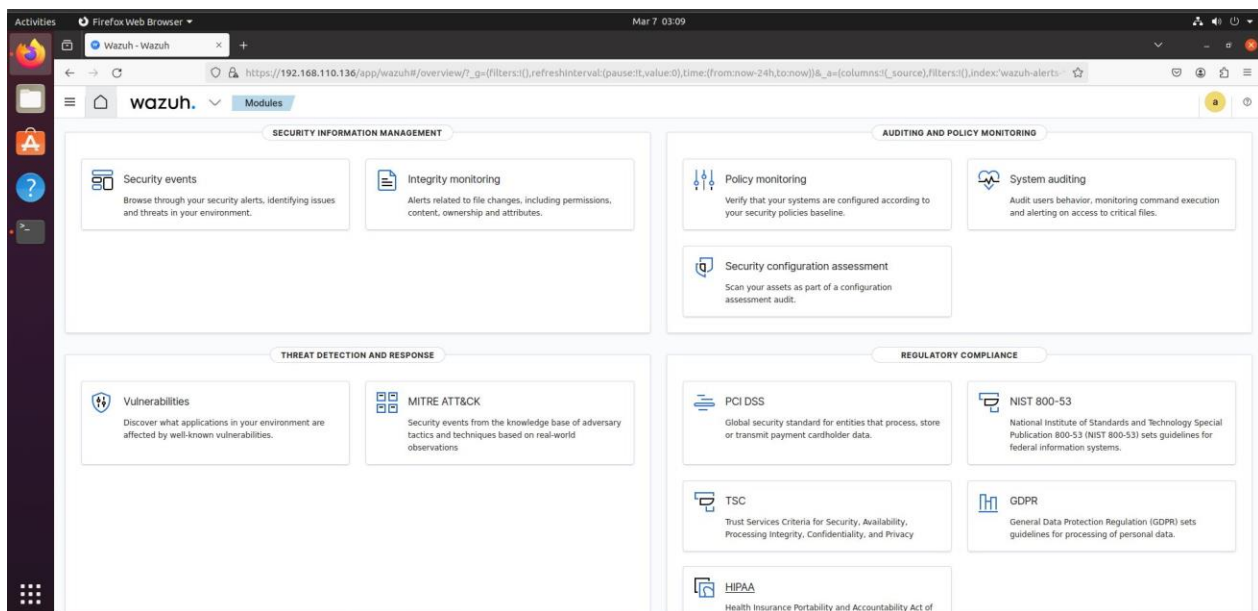


Fig.10. Wazuh Management interface

Week 13:

Dates: August 21, 2023 to August 27, 2023

Hours worked: 40

As a continuation of the preceding week, I received training on Wazuh-agent this time to monitor endpoints. I started off the week by installing two Wazuh agents on Windows and Linux based systems. The following are the tasks and activities I performed with Wazuh using its agent and manger:

- Monitored and analyzed logs from Wazuh agents to understand the events
- Studied how events are recorded and parsed through different alert's field, value and description
- Collecting windows log in Wazuh:
 - Configured Wazuh agent and windows Sysmon tool for log data collection
 - Aggregated windows Sysmon tool and Wazuh agent to collect logs from windows event viewer
- Collecting Linux logs in Wazuh
 - Configured Wazuh log collector service to record logs from Linux server to Wazuh main server
 - Utilizing 0250-apache_rules.xml customizable ruleset to collect Apache2 logs for errors and other warnings

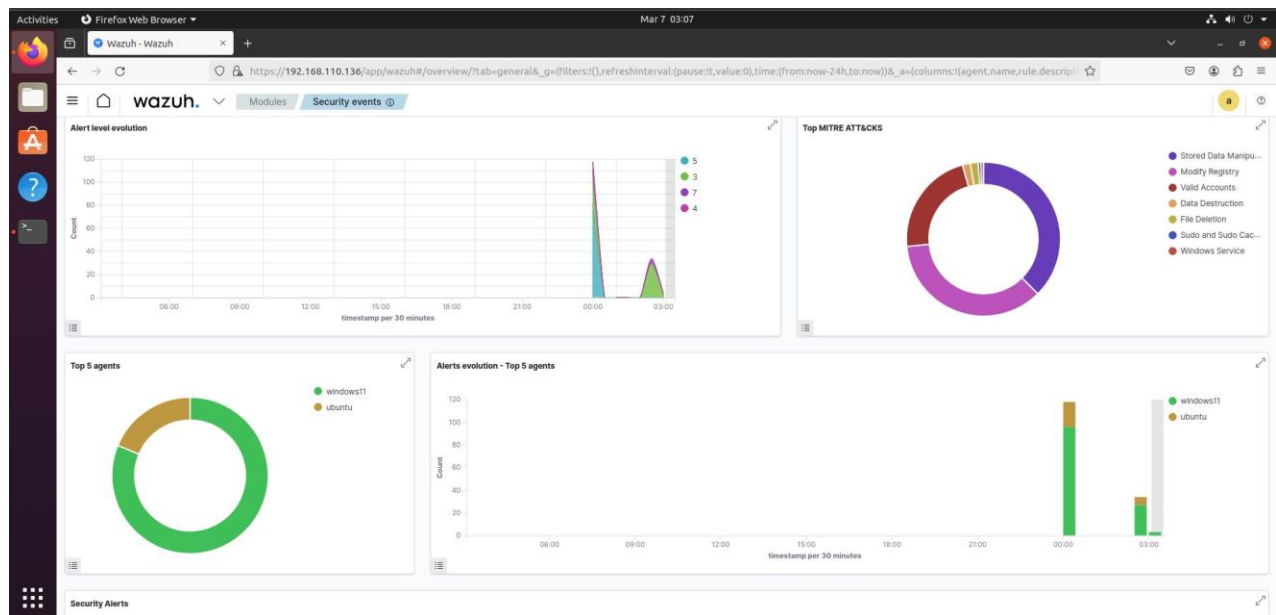


Fig.11. Wazuh security events after deploying agents

An interesting part on this week was the miscellaneous activity to emulate an attack in Wazuh - MITRE ATT&CK emulation

- Emulated T1021.001 Remote Services: Remote Desktop Protocol attack from MITRE framework using Caldera (Automated Adversary Emulation Platform) Visualized attack events in Wazuh

The implementation of Wazuh SIEM/EDR tool, collecting logs and parsing through different event without any difficulty helped me understand how SIEM works, and I was able to understand the versatility and usage of the tool that can come handy in any future career possibility I might come across.

Week 14:

Dates: 29/1/2024 To – 4/2/2024

Hours worked: 40

During the 14th week, I completed the following activities and tasks:

- Introduction to Antivirus programs and different types of solution packages.
- Discussed the impact of Virus and malware infections affected by Small and Medium Enterprises (SME)
- Research into different types of antiviruses including email-based antivirus, mobile based and cloud-based antivirus
- Discussion for the company's SME clients; the antivirus solutions that best fit them
- Presented client needs and requirements to management
- Configured and experimented with different Antivirus solution
- Research how Antivirus is incorporated along with Firewall and other security tools

Later during the week, I assessed the health of devices operating in Timex and reported the corresponding findings to the management. Meanwhile, I also studied the importance of updating Antivirus signatures as without updating, latest virus and malware cannot be identified even if we implement costly solutions.

Week 15:

Dates: 5/2/2024 To – 11/2/2024

Hours worked: 40

The 15th week was mostly experimenting and analyzing rather than working with real data or programs. This was for me to better understand virtualization concepts and its working. As usual, I first had an introduction to Virtualization starting with types of Virtualizations including

network, storage, servers and application. How virtualization and cloud implementation go hand in hand and cloud IT resources that are implemented for Timex

My tasks include:

- Experimented with virtualization solutions including VMWare workstation and Oracle VM VirtualBox- This comparison was to demonstrate to clients what best fits their requirements
- Installed Linux VM using both VMWare and VirtualBox
- Configured Network Interface Card (NIC), Hard disk and Memory
- Analyzed automatic configuration using OVA files- The configurations for NIC, Hard disk and Memory, along with other setting are automatically configured if we could find an OVA file. I worked with both manual and automatic configurations
- Installed multiple VMs (Windows & Linux) to create an isolated network

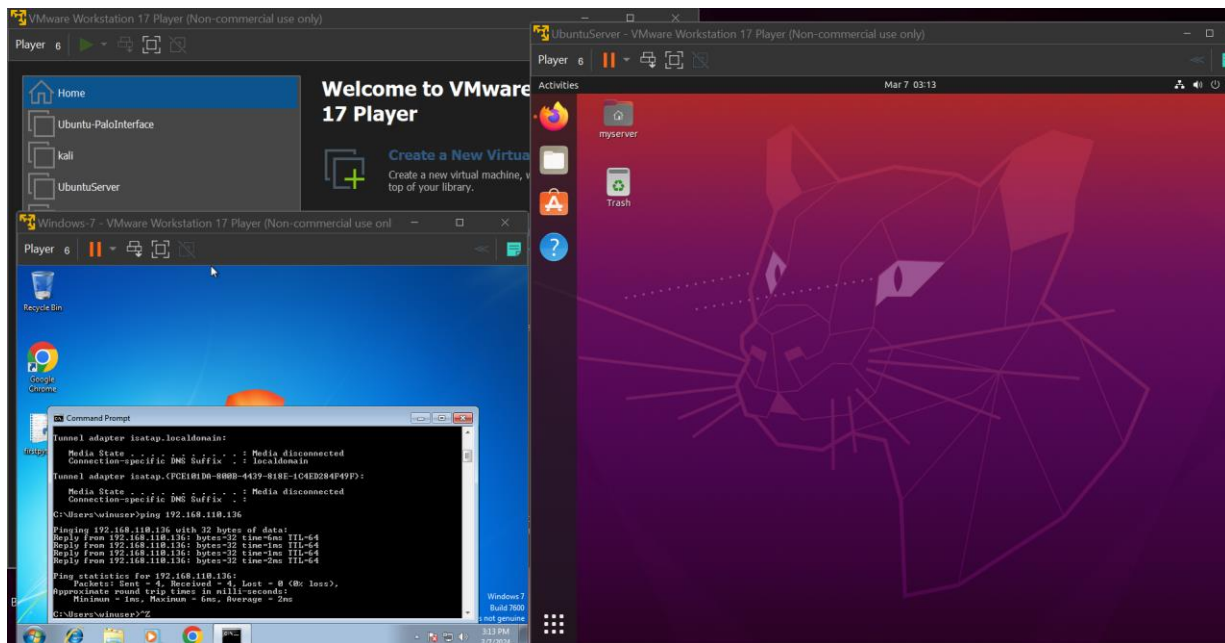


Fig.12. Isolated network in VMware

Later on, I received brief sessions on Kali Linux which a powerful penetration testing platform used by real hackers and cybercriminals around the globe. My activities on Kali were:

- Understand different security tools and applications
 - Offensive: Metasploit framework, Burp Suite, Aircrack-ng, Ettercap, sqlmap, Mimikatz
 - Applications: Nmap, Wireshark, recon-ng

I briefly worked and experimented with these tools providing me insights as to how easily we can perform certain tasks with the help of advanced tools and suites.

Finally, in a concise manner I explored more advanced and relevant virtualization types like Docker containers, Kubernetes and how to deploy them especially in Kali.

At the end of the week, I compared VirtualBox and VMWare capabilities and weaknesses and submitted comprehensive reports.

Week 16:

Dates: September 11, 2023, to September 17, 2023

Hours worked: 40

The 16th week was the final week of my internship. I was assigned to complete a mini project as part of my Final Internship Assessment which is to develop a Hash Cracking Tool. Timex IT Consulting being a software development company, wanted me to develop a tool that will calculate the hash of an input and to crack hash values using a Dictionary attack. For this purpose, I analyzed different hashing algorithms like MD5, SHA-1, SHA-2, and Bcrypt. I

thoroughly understood how hashing algorithms work, how it is a one-way function and its mathematic infeasibility.

I designed and developed a simple algorithm to create the python app for hashing and cracking hashes to get password. Meanwhile, I also learned different dictionary attacks and types that include rainbow tables, and Hybrid attacks. Based on the algorithm, I developed the following:

- **Python App:** Developed a simple Python app that takes input and displays certain text along with other widgets. Experimented and studied python basics specifically in app creation
- **Hashing functions:** Created and implemented hashing algorithms for md5 and Bcrypt. Successfully compiled hashes using the two hashing functions
- **Dictionary attack Functions:** Compiled and created wordlists that contain 200+ words to crack the hash. Developed and implemented dictionary attack functions successfully. Understand the importance of password policies and updating them regularly

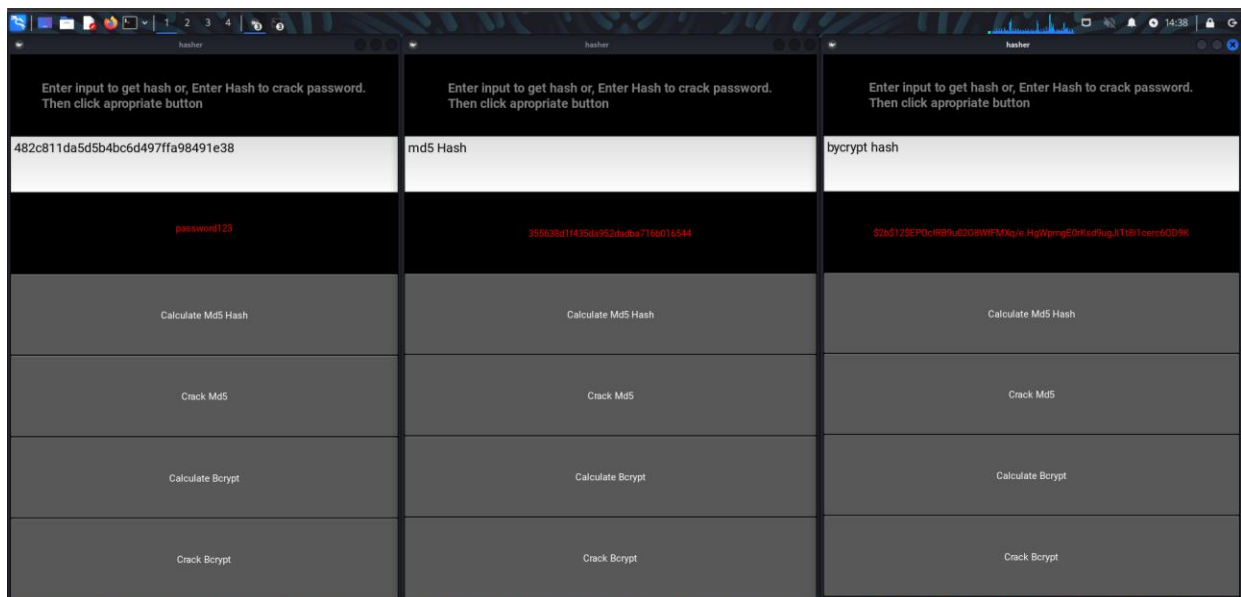


Fig.13. Hashing tool displaying various results

How did Al Ain University prepare me for the Internship?

Al Ain University helped me build a strong foundation in Cybersecurity and different aspects of it. Notably, the courses, assignments, workshops and other miscellaneous activities helped me understand complex topics required in my internship program. I also developed my skillset in communication, presentation and reporting through the university. Providing me this internship opportunity also helped me implement my skills and knowledge I have gained, improving my confidence and personal growth. I am grateful and excited to have successfully completed this internship program.

Assessment of the Internship

As discussed comprehensively in the preceding sections, I had the opportunity to work on a variety of tools and programs in cybersecurity and secure developing programs. A concise summary is given below.

Duties carried out as an intern

Researching and staying up to date with latest tools and practices in cybersecurity was done a lot during my internship which is also important in the real world. Apart from that I also worked on tools and software that businesses need in their day-to-day activities, including IDS, EDR, Firewall and Antivirus programs. I had also carried out tasks on software development that include integration with security mechanisms like encryption and secure coding practices. Overall, a lot has learned through my internship program.

How will the internship affect my future professional goals?

The 4-month internship program will have huge impact on my future professional opportunities.

I am now confident and well-aware of the typical activities and tasks a cybersecurity analyst must carry in a business enterprise. Although different business conducts their security practices differently, I have built a strong foundation and can confidently demonstrate my ability to quickly adapt and learn in a dynamic and evolving environment. Technical skills aside, my soft skills like teamwork and communication that I developed throughout, will also have a positive impact on my future career.

Internship-related activities compared to what I learned at the university

At the internship, I applied what I learned at the university, but I had to read, learn and experiment more before I moved onto working with the programs. Regardless, my hands-on experience was well-complimented with what I have studied and helped me quickly adapt to my differing environments. The internship provided valuable insights into industry practices that supplemented my academic education.

Differences between Theory and Professional experiences

The difference is very noticeable and huge. For example, as students, we are always told that communication is important in the field of software engineering. At Timex, I had to sit with some clients and talk with them for hours to understand what they wanted. It was not easy and was tiring. If I were to talk about coding, we spent a considerable time at the university learning about theoretical concepts but in practice, it is completely different. We are only learning a small

portion of a concept only while developing the whole application do we come to know the difficulties.

Hard and soft skills acquired

Hard skills

The hard skills I learned at Timex are how to operate different network security functions like analyze the traffic, detecting suspicious activities, analyze logs and alerts. Different security mechanism like password protection, encryption, hashing was also something that I can confidently speak of. I also had gained programming skills in python and Java with regards to secure coding and development.

The tools that I learned to operate are

- Security defensive tools: Snort IDS, Palo Alto Firewall, Wazuh
- Platform: VMware workstation, Cloud services, Kali, Postman
- Frameworks: MITRE ATT&CK
- Security offensive tools: Wireshark, Nmap, Metasploit, Aircrack-ng
- Programming Languages: Python, C#, Javascript

Soft skills

I was able to self-develop several soft skills that was needed in an intern. I had presented several reports gaining me good presentation skills and I was also able to communicate well with the management. Another important factor I learned was to understand the business objective and work towards that goal. At Timex, customer requirements and needs took priority over everything therefore, as a cybersecurity intern, I looked a lot into SME security needs as all

clients were under this category. I also learned to quickly adapt to different concepts and methodology, and I also developed problem solving capacity.

Difficulties during the Internship

Completing the 4-month internship program came with a lot of challenges. One of the problems that I faced during the internship was that the company is not advanced in cybersecurity therefore, I had to self-prepare and learn several problems and topics on my own. This can get overwhelming sometimes. However, this in turn helped me boost my self-confidence and my ability to prepare things on my own. Additionally, oftentimes, the supervisor was not available during the signing of my reports. This unfortunately delayed my report submission by several weeks. This was another I issue I had to tackle.

From the technical aspects, to work with tools like Wazuh and firewall, to configure and monitor alerts was difficult and required lots of time to complete them. Although the instructor helps and guides us during difficulty, they were not available except for few hours. This caused me to lose my track of time and spend hours after one error until I fixed. Eventually I learned to manage myself and dissect the issue in front of me, rather than searching for solutions aimlessly.

At the end, I believe I learned and experienced a lot from my challenges and difficulties more than the training itself. Now I am more excited and satisfied with my work.

Conclusions

To conclude my internship, I experienced and learned how real-life work would be like in an IT company. I am grateful for this opportunity to Mr. Hassan who overlooked my work, Dr. Yazan Al Ahmed who guided me and the university for granting me this opportunity.

Starting from researching SME security needs, I worked on how we can better secure SME with regards to cybersecurity and protect their business operations. I had participated in meetings and discussions with the management on how to offer these cybersecurity services in an affordable and efficient manner. These services include Intrusion Detection System, Firewall, Security policies for passwords and email, and endpoint security solutions to those require or have critical business operations. I had worked on and gained knowledge in the aforementioned services by working and configuring on solutions like Palo Alto Firewall, Snort IDS, and Wazuh EDR. I had also gained insights and expertise in programming especially in python and C# where I developed hash cracking tool and deploy AES encryption in .NET core respectively. These variety of tasks helped broaden my knowledge, experience and skillset.

Working four months at Timex with presentations, reporting and communicating effectively with the management, I also developed soft skills that help in my future career prospects. By building confidence in what I have learned at my university through the internship program, I believe it will positively impact my career journey in the field of cybersecurity. I am also proud of myself of overcoming several challenges I faced to complete my internship.

Having successfully completed my academic and internship journey feels rewarding and at the same time granting me a sense of accomplishment. I thank the university, the faculty, my internship coordinator- Dr. Yazan Al Ahmed and the Timex IT consulting company along with Mr. Hassan and the instructors who helped me achieve this milestone.

References

[1] Career Center. (n.d.). “What is an internship?”

Retrieved from <https://careers.umbc.edu/employers/internships/what-is-an-internship/>

[2] S. Manish (September 11, 2023). EternalBlue Explained – An In-Depth Analysis of the Notorious Windows Flaw. FreeCodeCamp. [EternalBlue Explained – An In-Depth Analysis of the Notorious Windows Flaw \(freecodecamp.org\)](#)