Field Training Report/ In 2024 Year

Name: Saad Mohammed Saad Al-Qarni
Major: Cybersecurity
University: University of Bisha
College: College of Computers
Supervisor: Assaf Al-Qarni
Training Location: Education Administration in Bishah
Training Period: 24/12/1445 – 30/1/1446
University ID: 442801752

Academic Supervisor: Dr. Ali Yasser Al-Qarni

Introduction

In the name of Allah, the Most Gracious, the Most Merciful.

Praise be to Allah, who taught by the pen, taught man what he did not know, and raised in degrees those of you who have believed and those who were given knowledge. Blessings and peace be upon our master Muhammad, and upon his family and all his companions.

Cooperative training is considered one of the fundamental pillars in developing the skills of university students and preparing them for the job market. It is a golden opportunity to gain real practical experience that enhances the theoretical knowledge acquired by the student during their university years. This stage of training represents the bridge that connects academic life with the professional world, offering the student a unique opportunity to apply what they have learned in classrooms to real-world situations and face the daily challenges that may arise in their future professional life.

I had the honor of conducting my cooperative training at the Education Administration in Bishah. Bishah is the entity responsible for organizing and developing the educational process in the province. The administration operates under the supervision of the Ministry of Education in the Kingdom of Saudi Arabia and aims to provide an outstanding educational environment that contributes to raising the level of education and developing the skills of students and teachers. During the training period, I had the opportunity to observe the work mechanisms followed and contribute to some of the activities and projects implemented by the administration.

In this report, I will review my cooperative training experience in detail, focusing on the activities I performed, the challenges I faced, the solutions that were applied, and finally, the benefits I gained from this valuable experience. I will also provide some recommendations and suggestions that I believe could contribute to improving cooperative training programs in the future.

Finally, I would like to express my gratitude and appreciation to everyone who contributed to the success of this training program, starting with the academic supervisors at Bishah University, and ending with my colleagues at the Education Administration in Bishah who spared no effort in providing support and assistance. I ask Allah to grant us all success and goodness and to make this work sincerely for His noble face.

Overview of the Training Entity

Introduction to the Education Administration in Bishah

The Education Administration in Bishah is responsible for organizing and developing the educational process in the province. Bishah is located in the southwestern part of the Kingdom of Saudi Arabia and is one of the main provinces in the Asir region. The administration plays a vital role in achieving the Saudi Vision 2030 by enhancing the quality of education and developing the skills of students and teachers.

Responsibilities of the Education Administration in Bishah:

1. **Curriculum Development:** The administration works on developing curricula according to global standards and local market needs, contributing to the preparation of a distinguished generation capable of participating in building the community.
2. **Teacher Training:** The administration provides continuous training programs and workshops for teachers aimed at improving their performance and developing their skills in line with the latest developments in the field of education.
3. **School Supervision:** The administration monitors the performance of schools and ensures their adherence to approved educational standards, providing necessary support to improve educational performance.

4. **Infrastructure Improvement:** The administration strives to improve and maintain school buildings, equipping them with the latest educational technologies to ensure a suitable and safe learning environment for students and teachers.
5. **Guidance and Counseling:** The administration offers psychological and social counseling services to students to help them overcome challenges they may face in their academic and personal lives.
6. **Community Partnership Enhancement:** The administration works on enhancing cooperation with the local community, parents, and governmental and private institutions to support the educational process and contribute to community development.

Departments of the Education Administration in Bishah:

1. **Educational Supervision Department:** Supervises the educational process in schools and ensures the correct implementation of curricula.
2. **Teacher Affairs Department:** Manages all matters related to teachers, including appointments, training, promotions, and improving their working conditions.
3. **Information Technology Department:** Manages electronic systems and networks in schools, providing necessary technical support.
4. **Student Activities Department:** Organizes extracurricular activities and educational programs that contribute to developing students' skills and enhancing their abilities.
5. **Guidance and Counseling Department:** Provides psychological and social support to students and works on solving problems they may encounter.
6. **Administrative and Financial Affairs Department:** Manages the financial and administrative affairs of the administration and the affiliated schools.

Vision of the Education Administration in Bishah:

The Education Administration in Bishah aims to be a leading educational beacon in the Kingdom, providing high-quality education

based on the latest pedagogical methods and educational technologies. The administration seeks to prepare a generation of students equipped with the skills and knowledge necessary to contribute to achieving the Saudi Vision 2030 and actively participating in building a bright future for the nation.

Mission of the Education Administration in Bishah:

The mission of the Education Administration in Bishah is to offer distinguished and comprehensive education that focuses on the student through an inspiring and innovative learning environment. The administration strives to develop educational and administrative staff and enhance partnerships with the local community to ensure equal educational opportunities for all students and achieve sustainable development in the education sector.

Values of the Education Administration in Bishah:

1. **Quality:** Commitment to providing high-quality education that meets global standards.
2. **Innovation:** Encouraging innovation and creativity in the educational process.
3. **Collaboration:** Promoting cooperation among all stakeholders to achieve educational goals.
4. **Responsibility:** Bearing responsibility towards the community, students, and teachers.
5. **Sustainable Development:** Achieving sustainable development by developing education and meeting future needs.

The Education Administration in Bishah represents a distinguished model of integrated educational care in the Kingdom of Saudi Arabia. With its ambitious vision and mission committed to providing high-quality educational services, the administration remains a cornerstone in the local education system, contributing to improving the level of education and the well-being of the community through providing excellent and comprehensive education.

Introduction

Practical training is an essential part of the Cybersecurity major, allowing students to apply the theoretical knowledge they have acquired at university in real-world settings. In this report, I will present my practical training experience at the Education Administration in Bishah, where I acquired new skills and enhanced my capabilities in the field of cybersecurity.

Objectives

The primary objective of this training was to gain practical experience in a real work environment and learn how to manage and develop cybersecurity systems in an educational institution. Additionally, I aimed to develop my technical skills and improve my ability to handle challenges that may arise in my future career. The detailed objectives of the training included:

1. Understanding the Work Environment:

- **Understanding the Organizational Structure:** Familiarizing myself with the different departments within the Education Administration and how work is coordinated among them to achieve educational goals.
- **Learning Daily Operations:** Gaining practical knowledge on how daily operations are carried out in an educational environment, such as records management, administrative follow-up, and technical support.
- **Understanding Organizational Culture:** Understanding the organizational culture and values that govern work in the Education Administration, which helps in adapting to the work environment and contributing effectively.

2. Developing Technical Skills:

- **Using Cybersecurity Tools:** Learning how to use various cybersecurity tools such as Nmap, Wireshark, Metasploit, and Burp Suite for network analysis and vulnerability detection.
- **Analyzing Security Logs:** Gaining skills in analyzing activity logs to detect abnormal patterns and potential threats.
- **Conducting Penetration Tests:** Developing the ability to conduct effective penetration tests to verify the security of systems and networks.

3. Applying Theoretical Knowledge:

- **Implementing Security Policies:** Using the theoretical knowledge gained at university to develop and implement cybersecurity policies in the institution.
- **Responding to Cyber Incidents:** Learning how to handle cyber incidents and apply emergency response plans.
- **Preparing Security Reports:** Preparing comprehensive security reports documenting the status of systems and networks and providing recommendations for improving security.

4. Building Professional Relationships:

- **Collaborating with Colleagues:** Building strong professional relationships with colleagues and supervisors, providing opportunities to learn from their experiences and benefit from their advice.
- **Working in a Team:** Improving my skills in working within a team, which helps in effectively executing projects and addressing challenges collectively.
- **Effective Communication:** Developing effective communication skills with the team and other departments to ensure smooth achievement of work objectives.

5. Making a Positive Impact:

- **Improving Security Systems:** Contributing to the improvement of cybersecurity systems in the administration by providing effective recommendations and implementing appropriate security measures.

- **Increasing Security Awareness:** Organizing training sessions to raise awareness about the importance of cybersecurity among employees and teaching them best practices for protecting data and information.
- **Developing Infrastructure:** Providing suggestions for improving network and device infrastructure to ensure their security and efficiency.

Additional Objectives:

6. Enhancing Managerial and Organizational Skills:

- **Project Management:** Acquiring project management skills through planning, executing, and monitoring cybersecurity projects.
- **Documentation and Evaluation:** Learning how to document all procedures and steps taken during the training period and evaluate them to ensure continuous improvement.
- **Risk Analysis:** Developing the ability to analyze potential risks and devise strategies to avoid or mitigate their impact.

7. Continuous Learning and Professional Development:

- **Staying Updated:** Keeping abreast of the latest developments in the field of cybersecurity and the new technologies being used.
- **Self-Training:** Participating in online training courses and workshops to enhance knowledge and skills.
- **Professional Certifications:** Working towards obtaining professional certifications in cybersecurity to enhance career opportunities.

By achieving these objectives, I was able to enhance my skills and knowledge in the field of cybersecurity, better preparing me to face challenges in my future career.

Training Details

Week One: Getting to Know the Work Environment

Day One: Reception and Team Introduction

- **Official Reception:** Upon my arrival at the Education Administration in Bishah, I was warmly welcomed by the officials and introduced to the working team.
- **Introductory Tour:** A guided tour of the building was organized for me, where I got to know the different departments and facilities of the administration, such as teachers' offices, meeting rooms, and data centers.
- **Introductory Meeting:** I attended an introductory meeting with the training supervisor, where the training objectives and the administration's expectations from me were explained, along with a clarification of daily tasks and procedures.

Day Two: Understanding Systems and Networks

- **Presentation:** I attended a presentation explaining the network infrastructure used in the administration, including servers, routers, and wireless access points.
- **Data Center Tour:** I toured the administration's data center, where I learned how servers and storage systems are managed, in addition to understanding the network monitoring and security tools.
- **Initial Documentation:** I began documenting my observations on the current state of security systems, including the hardware used, installed software, and applied security policies.

Day Three: Understanding Security Policies and Procedures

- **Document Review:** I reviewed the security documents and policies followed in the administration, such as the internet usage policy, password management policy, and data access policy.
- **Meeting with the Cybersecurity Team:** I attended a meeting with the cybersecurity team in the administration, where we

discussed the current security measures and the main challenges faced by the team.
- **Vulnerability Analysis:** I analyzed some of the security vulnerabilities in the system using tools like Nmap and Wireshark and documented the results in an initial report.

Day Four: Security Logs Analysis

- **Learning to Use Log Tools:** I learned how to use security log analysis tools such as Splunk and Graylog to analyze network activities.
- **Activity Analysis:** I started analyzing daily activity logs on the network to identify unusual patterns or suspicious attempts to gain unauthorized access.
- **Report Preparation:** I prepared daily reports outlining the status of security systems and any abnormal activity detected, with recommendations for improving security.

Day Five: Weekly Evaluation Meeting

- **Weekly Performance Review:** I attended a meeting with the training supervisor to review the performance of the first week, discussing the tasks I performed and the challenges I faced.
- **Feedback Session:** I received feedback from the supervisor and colleagues on my performance, along with recommendations for improvement in the coming weeks.
- **Planning for the Next Week:** A plan was set for the tasks I would undertake in the second week, including more work on log analysis and the development of security policies.

Key Activities in the First Week:

1. **Getting to Know the Team and Work Environment:**
    - Introductory tours of the facilities and departments.
    - Introductory meeting with the training supervisor.
2. **Understanding Systems and Networks:**
    - Attending a presentation on network infrastructure.
    - Touring the data center.
    - Documenting the current state of security systems.

3. **Understanding Security Policies and Procedures:**
    - Reviewing security documents and policies.
    - Meeting with the cybersecurity team.
    - Conducting an initial vulnerability analysis.
4. **Security Logs Analysis:**
    - Learning to use log analysis tools.
    - Analyzing activities and identifying unusual patterns.
    - Preparing daily security status reports.
5. **Weekly Evaluation Meeting:**
    - Reviewing weekly performance and receiving feedback.
    - Planning for the second week's tasks.

Skills Acquired in the First Week:

- **Vulnerability Analysis Skills:** I acquired skills in using vulnerability analysis tools such as Nmap and Wireshark.
- **Log Analysis Skills:** I learned how to use log analysis tools like Splunk and Graylog.
- **Documentation and Reporting:** I gained experience in documenting observations and preparing daily reports on security status.
- **Communication and Teamwork:** I improved my skills in communication and teamwork within an integrated security team.

Thanks to this first week, I was able to build a strong foundation of skills and knowledge necessary to continue the training successfully and develop my abilities in the field of cybersecurity.

.

Week Two: Beginning the Actual Work

Day One: Systems and Networks Inspection

- **Getting to Know the Tools Used:** On the first day, I familiarized myself with the tools and applications used by the administration to inspect systems and networks. This included learning how to use tools like Nmap and Wireshark.
- **Conducting Initial Inspections:** I performed initial inspections on the systems to detect potential security vulnerabilities. This involved inspecting servers, access points, and routers.
- **Documenting Results:** I documented the results obtained from the initial inspections and prepared a detailed report for the supervisor, including initial recommendations for improving security.

Day Two: Monitoring Activity Logs

- **Learning to Use Log Monitoring Tools:** I learned how to use security log monitoring tools like Splunk and Graylog to analyze daily activities on the network.
- **Log Analysis:** I began analyzing activity logs from previous days to discover abnormal patterns or suspicious attempts to gain unauthorized access.
- **Preparing Daily Reports:** I prepared daily reports outlining the security status of the systems and any unusual activities detected, along with recommendations for improving security.

Day Three: Handling Security Incidents

- **Developing Incident Response Plans:** I started developing incident response plans based on potential scenarios of cyber attacks. This included defining the roles and responsibilities of each team member.
- **Simulating Security Incidents:** We conducted a simulation of a security incident to practice how to deal with it quickly and effectively. This involved identifying the source of the attack, containing it, and restoring the system to its normal state.

- **Performance Evaluation:** I evaluated the performance during the simulation and documented the points that need improvement in the incident response plan.

Day Four: Enhancing Security Policies

- **Reviewing Current Policies:** I reviewed the current security policies of the administration, such as the internet usage policy, password management policy, and data access policy.
- **Updating Policies:** I worked on updating the security policies to align with the latest standards and international practices. This included improving the password management policy and updating network security protocols.
- **Creating New Guidelines:** I prepared new guidelines for users on how to protect their data and personal information, including tips to avoid common cyber attacks.

Day Five: Weekly Evaluation Meeting

- **Reviewing Weekly Performance:** I attended a meeting with the training supervisor to review the performance of the second week, discussing the tasks I performed and the challenges I faced.
- **Receiving Feedback:** I received feedback from the supervisor and colleagues on my performance, along with recommendations for improvement in the coming weeks.
- **Planning for the Next Week:** A plan was set for the tasks I would undertake in the third week, including more work on log analysis and the development of security policies.

Key Activities in the Second Week:

1. **Systems and Networks Inspection:**
    - Familiarizing with tools like Nmap and Wireshark.
    - Conducting initial inspections on systems to detect security vulnerabilities.
    - Documenting results and preparing a detailed report for the supervisor.
2. **Monitoring Activity Logs:**

    - Learning to use log monitoring tools like Splunk and Graylog.
    - Analyzing activity logs to discover abnormal patterns.
    - Preparing daily reports on security status.
3. **Handling Security Incidents:**
    - Developing incident response plans.
    - Conducting simulations of security incidents to practice response.
    - Evaluating performance and documenting improvement points.
4. **Enhancing Security Policies:**
    - Reviewing current security policies.
    - Updating policies to align with the latest standards.
    - Creating new guidelines for users on data protection.
5. **Weekly Evaluation Meeting:**
    - Reviewing weekly performance and receiving feedback.
    - Planning tasks for the third week.

Skills Acquired in the Second Week:

- **System Inspection Skills:** I learned how to use tools like Nmap and Wireshark to inspect systems and networks and detect security vulnerabilities.
- **Log Analysis Skills:** I developed my skills in analyzing activity logs using tools like Splunk and Graylog.
- **Developing Response Plans:** I gained experience in developing and implementing incident response plans.
- **Enhancing Security Policies:** I learned how to review and update security policies to align with the latest standards and practices.
- **Communication and Teamwork:** I enhanced my skills in communication and teamwork within an integrated security team, receiving constructive feedback to improve my performance.

Achievements in the Second Week:

- **Discovering Security Vulnerabilities:** I was able to identify several security vulnerabilities in the systems and provided recommendations for improvement.
- **Improving Security:** I contributed to enhancing the level of security in the administration by updating policies and implementing appropriate security measures.
- **Increasing Security Awareness:** I helped increase security awareness among employees by preparing new guidelines and providing security tips.

Thanks to this second week, I was able to enhance my skills in cybersecurity and apply the theoretical knowledge I acquired at university to real-world situations.

Week Three: Advanced Tasks and Skill Development

Day One: Developing Cyber Emergency Response Plans

- **Reviewing Current Emergency Plans:** I started the day by reviewing the existing emergency plans in the Education Administration, including the procedures followed in case of cyber attacks.
- **Identifying Gaps:** I analyzed the weaknesses and gaps in the current plans and proposed improvements to ensure effective and quick response.
- **Creating Attack Scenarios:** I developed potential cyber attack scenarios, including DDoS attacks and ransomware attacks, and created detailed response plans for each scenario.

Day Two: Enhancing Security Policies

- **Meeting with the Security Team:** I held a meeting with the cybersecurity team to discuss the proposed updates to the security policies and to receive their feedback.

- **Developing Policies:** I worked on updating the existing security policies, including the password management policy, data access policy, and internet usage policy.
- **Preparing Policy Documents:** I prepared detailed documents for the updated policies and distributed them to the team for review and approval.

Day Three: Conducting Penetration Tests

- **Planning Penetration Tests:** I planned the penetration tests to be conducted on the administration's systems and networks. This included defining the objectives, tools, and methods to be used.
- **Executing Tests:** I began executing the penetration tests using tools like Metasploit and Burp Suite and was able to identify some security vulnerabilities.
- **Documenting Results:** I documented the results of the tests in a detailed report, including the identified vulnerabilities and the necessary recommendations for remediation.

Day Four: Organizing Training Sessions

- **Identifying Training Topics:** I identified key topics that needed to be covered in the training sessions, such as data protection, handling suspicious emails, and cybersecurity basics.
- **Preparing Training Materials:** I worked on preparing training materials, including presentations, booklets, and interactive exercises for the employees.
- **Conducting Training Sessions:** I organized a training session attended by several employees of the administration, where I delivered a comprehensive presentation on cybersecurity topics and data protection methods.

Day Five: Documentation and Reporting

- **Preparing the Weekly Report:** I prepared a comprehensive report on all the activities I performed during the week, including the development of emergency plans, policy enhancements, penetration test results, and training sessions.

- **Submitting the Report to the Supervisor:** I submitted the report to the supervisor and discussed the results and recommendations with them.
- **Planning for the Fourth Week:** A plan was set for the tasks to be undertaken in the fourth week, including more documentation and final recommendations.

Key Activities in the Third Week:

1. **Developing Cyber Emergency Response Plans:**
    - Reviewing and analyzing current emergency plans.
    - Identifying gaps and creating cyber attack scenarios.
    - Preparing detailed response plans.
2. **Enhancing Security Policies:**
    - Holding a meeting with the cybersecurity team.
    - Updating and documenting security policies.
    - Preparing policy documents and distributing them for review.
3. **Conducting Penetration Tests:**
    - Planning penetration tests.
    - Executing tests using advanced tools.
    - Documenting test results and providing remediation recommendations.
4. **Organizing Training Sessions:**
    - Identifying training topics and preparing materials.
    - Conducting training sessions for employees.
    - Evaluating the effectiveness of the training sessions and providing feedback.
5. **Documentation and Reporting:**
    - Preparing a comprehensive weekly report.
    - Submitting the report to the supervisor and discussing results.
    - Planning tasks for the fourth week.

Skills Acquired in the Third Week:

- **Developing Emergency Plans:** I acquired skills in developing emergency plans and responding to cyber incidents.

- **Enhancing Security Policies:** I learned how to improve and systematically document security policies.
- **Conducting Penetration Tests:** I developed my skills in conducting penetration tests and using advanced tools to identify security vulnerabilities.
- **Training Employees:** I gained experience in preparing and conducting effective training sessions for employees.
- **Documentation and Reporting:** I learned how to prepare comprehensive reports documenting activities, results, and recommendations.

Achievements in the Third Week:

- **Improving Emergency Plans:** I was able to enhance the emergency plans and response procedures, increasing the administration's ability to handle cyber attacks.
- **Updating Security Policies:** Security policies were updated to align with the latest standards and practices, improving overall security.
- **Identifying and Remediating Vulnerabilities:** Several security vulnerabilities were identified through penetration tests, and recommendations were provided for their remediation.
- **Increasing Security Awareness:** Training sessions contributed to raising security awareness among employees and teaching them best practices for data protection.

Thanks to this third week, I significantly enhanced my skills in cybersecurity and applied theoretical knowledge in a practical context.

Week Four: Documentation and Final Recommendations

In the fourth and final week, I focused on documenting all procedures and recommendations, as well as providing comprehensive reports on the state of cybersecurity:

Day One: Preparing the Final Report

- **Comprehensive Analysis:** I prepared a final report that included a thorough analysis of the cybersecurity status in the administration. This report detailed all the actions taken during the training period, the results of those actions, and future recommendations.
- **Detailed Documentation:** I ensured that every step, tool, and procedure used during the training was well-documented. This included screenshots, logs, and detailed descriptions of the methodologies applied.

Day Two: Proposing Future Improvements

- **Identifying Areas for Improvement:** I identified areas where the administration's cybersecurity could be enhanced. This included the need for updating outdated hardware and implementing new security protocols.
- **Creating Actionable Recommendations:** I developed specific, actionable recommendations for future improvements in cybersecurity. These recommendations were designed to address the identified vulnerabilities and ensure a robust security posture.

Day Three: Conducting Training Sessions

- **Planning Training Topics:** I planned and outlined the key topics to be covered in the training sessions for the administration's employees. These topics included best practices in cybersecurity, how to handle suspicious emails, and recognizing common threats.

- **Executing Training Sessions:** I conducted training sessions for the employees, using presentations and interactive exercises to ensure the information was well-received and understood.
- **Providing Educational Materials:** I distributed booklets and handouts summarizing the key points from the training sessions, ensuring employees had resources to reference in the future.

Day Four: Coordinating with Other Departments

- **Inter-departmental Meetings:** I organized meetings with other departments to discuss the implemented security measures and the importance of maintaining a consistent security protocol across all sections of the administration.
- **Information Sharing:** I facilitated the exchange of information between departments, ensuring that everyone was aware of the security measures in place and the role each department played in maintaining cybersecurity.
- **Establishing Security Liaisons:** I helped appoint security liaisons in each department to ensure ongoing communication and adherence to security protocols.

Day Five: Final Review and Submission

- **Reviewing the Final Report:** I conducted a thorough review of the final report, ensuring all details were accurate and the recommendations were clear and actionable.
- **Presenting to the Supervisor:** I presented the final report to the training supervisor, discussing the findings, actions taken, and future recommendations.
- **Planning for Implementation:** I worked with the supervisor to develop a plan for the implementation of the proposed recommendations, ensuring a smooth transition from planning to execution.

Key Activities in the Fourth Week:

1. **Preparing the Final Report:**
    - Conducting a comprehensive analysis of the cybersecurity status.

    - Documenting all procedures, tools, and methodologies used.
    - Detailing the actions taken and results achieved.
2. **Proposing Future Improvements:**
    - Identifying areas for improvement in the administration's cybersecurity.
    - Developing actionable recommendations for future enhancements.
3. **Conducting Training Sessions:**
    - Planning and outlining key cybersecurity topics.
    - Executing training sessions for employees.
    - Distributing educational materials for future reference.
4. **Coordinating with Other Departments:**
    - Organizing inter-departmental meetings.
    - Facilitating information sharing and establishing security liaisons.
5. **Final Review and Submission:**
    - Reviewing and finalizing the report.
    - Presenting the report to the supervisor.
    - Developing a plan for implementing recommendations.

Skills Acquired in the Fourth Week:

- **Documentation and Reporting:** I enhanced my skills in documenting procedures, creating detailed reports, and ensuring all information was accurately captured and presented.
- **Proposal Development:** I learned how to develop actionable recommendations for improving cybersecurity and presenting them in a clear and concise manner.
- **Training and Education:** I gained experience in planning and conducting effective training sessions, ensuring participants understood and could apply the information presented.
- **Inter-departmental Coordination:** I improved my ability to coordinate and communicate with different departments, ensuring a cohesive approach to cybersecurity.

Achievements in the Fourth Week:

- **Comprehensive Final Report:** Successfully prepared and presented a comprehensive final report detailing the cybersecurity status, actions taken, and future recommendations.
- **Actionable Recommendations:** Developed specific recommendations for future improvements, ensuring the administration has a clear path forward for enhancing cybersecurity.
- **Increased Employee Awareness:** Conducted training sessions that increased employees' awareness of cybersecurity best practices and equipped them with the knowledge to handle common threats.
- **Enhanced Inter-departmental Coordination:** Established a framework for ongoing communication and coordination between departments, ensuring consistent application of security protocols.

Thanks to this fourth week, I was able to consolidate my experiences and skills, ensuring that the knowledge gained during the training period was thoroughly documented and that the administration was well-prepared for future cybersecurity challenges.

Achieved Results

Improving Cybersecurity

- **Developed Incident Response Plans:** Created detailed response plans for potential cyber attacks, improving preparedness with specific steps for various attack scenarios.
- **Updated Security Policies:** Enhanced policies for password management, data access, and internet usage, aligning with global best practices.

- **Conducted Penetration Tests:** Identified critical vulnerabilities and provided detailed remediation recommendations, strengthening overall security.

Increasing Employee Awareness

- **Organized Training Sessions:** Increased employee awareness of cybersecurity, teaching them to handle suspicious emails and protect sensitive data.
- **Prepared Training Materials:** Created comprehensive materials on advanced cyber attack protection and data handling, improving understanding of best practices.

Enhancing Interdepartmental Collaboration

- **Communicated with Departments:** Strengthened collaboration and information exchange, ensuring effective implementation of security measures.
- **Delivered Presentations:** Clarified results and recommendations, gaining support and understanding for security initiatives.

Challenges Faced

Dealing with Legacy Systems

- **Compatibility and Updates:** Managing and updating older systems to ensure security without disrupting operations was challenging.
- **Integration with New Systems:** Ensuring seamless integration between old and new systems without creating security gaps.

Managing Multiple Protections

- **Protecting Multiple Devices:** Securing devices across various networks required regular updates and coordination.
- **Coordinating Security Actions:** Continuous coordination between teams was necessary to implement comprehensive security measures.

Time Management

- **Organizing Daily Tasks:** Balancing daily tasks and meeting deadlines required precise scheduling and prioritization.
- **Balancing Theory and Practice:** Integrating theoretical knowledge with practical application demanded additional effort.

Skills Acquired

Vulnerability Analysis

- **Using Analysis Tools:** Learned to effectively use Nmap and Wireshark for identifying system vulnerabilities.
- **Identifying and Recommending Fixes:** Gained skills in analyzing vulnerabilities and providing detailed recommendations.

Log Analysis

- **Using Log Tools:** Mastered tools like Splunk and Graylog for analyzing activity logs.
- **Interpreting Data:** Developed skills in interpreting and analyzing data to identify potential threats.

Developing Response Plans

- **Creating Detailed Plans:** Learned to create comprehensive emergency response plans for various cyber attack scenarios.
- **Executing Simulations:** Gained experience in conducting security incident simulations and evaluating response effectiveness.

Enhancing Security Policies

- **Reviewing and Updating Policies:** Learned to systematically review and improve security policies.
- **Document Preparation:** Gained skills in preparing clear, comprehensive policy documents.

Organizing Training Sessions

- **Preparing Training Materials:** Developed materials covering diverse cybersecurity topics.
- **Conducting Effective Training:** Gained experience in delivering training sessions and teaching best practices.

Reporting and Communication

- **Writing Comprehensive Reports:** Improved skills in documenting activities, results, and recommendations.
- **Effective Communication:** Enhanced communication with team and departments, facilitating effective implementation of recommendations.

This training experience significantly enhanced my skills and knowledge in cybersecurity, greatly preparing me for future career challenges in this field.

Conclusion

The internship at the Education Administration in Bishah was a rich and rewarding experience on multiple levels. This training provided me with a unique opportunity to apply the theoretical knowledge I gained at university in a real-world setting, significantly enhancing my technical and professional skills. Here are some of the key benefits and developments I achieved:

I am excited to continue my career in the field of cybersecurity and look forward to applying what I learned during the internship to new challenges and future projects. This experience has prepared me well to face the challenges and opportunities that may come my way in my professional journey, and I am confident that the skills and knowledge I acquired will help me achieve success and excellence.

I would like to express my sincere thanks and appreciation to the Education Administration in Bishah for this valuable opportunity. I also extend my gratitude to Bishah University for their continuous support and for providing educational opportunities that contribute to the development of students' skills. I thank my colleagues and supervisors for their valuable support and guidance, which greatly helped me succeed in this training.

In conclusion, the internship at the Education Administration in Bishah was a significant turning point in my educational and professional journey. It helped me develop my technical and professional skills, deepen my understanding of cybersecurity, and build valuable professional relationships. This experience has greatly contributed to my personal and professional growth, and I eagerly look forward to applying what I learned in my future career.