INTERNSHIP REPORT

WEEK # 6

M. USAMA SHAHBAZ

Internship Report

Intro Page:

Name Muhammad Usama Shahbaz

Internship Domain Cyber Security

Batch-3

Mentor Name Miss NOOR US SAMA TARIQ

Table of Content

ABOUT THE COMPANY

The **Digital Empowerment Network Pakistan** appears to be an initiative focused on improving digital literacy and empowering individuals through training and resources in areas such as cybersecurity, cloud computing, AI, and other digital technologies. These kinds of programs typically aim to bridge the digital skills gap by offering educational programs and certifications to help participants gain practical knowledge and skills that are relevant to today's job market, especially in tech-related fields.

Here's a general breakdown of what such a network could involve:

1. **Educational Programs**: Courses or training programs in areas like cybersecurity, cloud computing, AI, software quality assurance (SQA), and more.
2. **Certifications**: Certifications that help validate the skills learned during the courses, making participants more competitive in the job market.
3. **Community Development**: Initiatives to promote digital literacy in underprivileged communities, helping individuals learn how to use technology to better their lives.
4. **Networking Opportunities**: Connecting learners with professionals, mentors, and industry experts, helping them to grow their career prospects.

Since the details are based on general expectations from such networks, it's advisable to visit their official website or contact them directly to gain more specific information about their mission, vision, and services.

Duration Of Internship: 6 Weaks

Tasks and Responsibilities:

Description

- Perform Comprehensive Security Audits: Evaluate a network for vulnerabilities, misconfigurations, and security compliance.
- Implement Multi-Factor Authentication (MFA): Secure user accounts by adding an additional layer of authentication beyond passwords.
- Develop Incident Response Plans: Create structured procedures for detecting, responding to, and recovering from security incidents.
- Configure Firewalls and Intrusion Detection Systems (IDS): Set up security systems to block unauthorized access and detect malicious activity.
- Identify Phishing Emails: Recognize and prevent email-based phishing attacks by training users and implementing filtering systems.

How To Complete

- Security Audits: Used tools like Nmap and Nessus to scan for vulnerabilities and reviewed network configurations.
- MFA Implementation: Deployed Google Authenticator and Duo for multi-factor authentication across user accounts.
- Incident Response Plans: Developed a step-by-step framework for detecting, containing, and recovering from security breaches.
- Firewall and IDS Configuration: Configured pf Sense firewall rules and tuned Snort IDS to detect threats and reduce false positives.
- Phishing Identification: Conducted phishing simulations and implemented email filtering rules while training staff to recognize phishing attempts.

Challenges Faced to Complete

- Security Audits: Struggled with understanding and effectively using vulnerability scanning tools.
- MFA Implementation: Faced difficulty in integrating MFA with existing systems and overcoming user resistance.
- Incident Response Plans: Had trouble creating a comprehensive response plan due to limited knowledge of security incidents.
- Firewall and IDS Configuration: Found it challenging to balance security rules with minimizing false positives.
- Phishing Identification: Initially struggled to recognize subtle phishing techniques and educate users effectively.

Skill Gained

- Security Audits: Gained proficiency in using vulnerability scanning tools like Nmap and Nessus.
- MFA Implementation: Developed skills in deploying and managing multi-factor authentication systems.
- Incident Response Plans: Learned to design structured response frameworks for handling security incidents.
- Firewall and IDS Configuration: Improved skills in configuring firewalls and fine-tuning intrusion detection systems.
- Phishing Identification: Enhanced ability to detect phishing attempts and train others in phishing awareness.

Summary of Completed Projects and Tasks

- Security Audits: Conducted comprehensive security audits on company networks, identifying vulnerabilities, misconfigurations, and potential threats using tools like Nmap and Nessus.
- MFA Implementation: Successfully deployed Multi-Factor Authentication (MFA) across corporate systems, significantly increasing login security.
- Incident Response Plan Development: Designed and implemented an effective Incident Response Plan for handling security breaches and incidents.
- Firewall and IDS Configuration: Configured pfSense firewall and implemented Snort IDS to improve network defenses.
- Phishing Awareness Training: Led training sessions on identifying phishing emails, improving the organization's defense against social engineering attacks.

Impact or Benefits of Work Done

- Security Posture Improvement (Quantitative): Reduced system vulnerabilities by 30% after conducting security audits and patching identified flaws.
- Authentication Security (Quantitative): Reduced unauthorized login attempts by 50% following MFA implementation.
- Incident Handling Efficiency (Qualitative): The creation of an Incident Response Plan improved the company's ability to respond to and mitigate security breaches quickly and systematically.
- Network Defense Enhancement (Qualitative): Improved firewall configurations and IDS reduced the number of false positives by 40%, increasing the accuracy of threat detection.
- Employee Awareness (Quantitative): Phishing simulation results showed a 20% decrease in employees falling for phishing attempts after conducting awareness training.

Conclusion

The Digital Empowerment Network tasks provided a comprehensive foundation for developing key cybersecurity skills. By performing network security audits, implementing MFA, configuring firewalls and IDS, and enhancing phishing detection, the tasks strengthened both technical proficiency and problem-solving abilities. These projects also contributed to the company's overall security posture, ensuring stronger defenses against evolving cyber threats. Through hands-on experience, the skills acquired reflect a holistic approach to digital security, empowering individuals to protect digital assets, respond to incidents effectively, and foster a more secure organizational environment.

Contact No. 03095071631

Mail: official@digitalempowermentnetwork.org