**Assessment 2:- Portfolio**

Contents

[Portfolio 3](#_Toc164465136)

[Design and update of the website 3](#_Toc164465137)

[Project details 5](#_Toc164465138)

[Technical 5](#_Toc164465139)

[Project Progress Reporting 6](#_Toc164465140)

[Week 1 6](#_Toc164465141)

[Week 2 7](#_Toc164465142)

[Week 3 9](#_Toc164465143)

[Conclusion 12](#_Toc164465144)

[References 13](#_Toc164465145)

# **Portfolio**

In this report you will see the justification of website and updating website. A design justification could be supplied to explain the purpose in the back of the chosen design elements and upgrades.

# **Design and update of the website**

**Content Organization**:

The first element to consider whilst updating the website is the employer of content. To ensure clarity and ease of navigation, the internet site can be dependent into wonderful sections, each specializing in a selected issue of the project. These sections may additionally encompass:

**Home:** The homepage will provide an overview of the venture, including its targets, milestones, and progress updates. It will serve as the entry point for traffic to study the assignment and navigate to different sections of the website.

**About:** The about segment will offer certain records approximately the venture, its goals, stakeholders, and group contributors.

**Progress Reports**: This section will comprise weekly person and institution development reviews detailing the task group's sports, achievements, demanding situations, and subsequent phase obligations. Each report might be organized chronologically for easy reference.

**Technical Details**: Here, site visitors will discover certain records about the task's technical components, including network setup, penetration testing techniques, and certification frameworks. This phase will cater to traffic interested in the mission's technical intricacies.

**Gallery:** The gallery section will characteristic visible artifacts which include screenshots, diagrams, and movies showcasing the venture's improvement process, tools used, and milestones executed.

**Visual Design Elements:**

The internet site's visual layout is critical in enticing visitors and correctly conveying data. To enhance the website's visual appeal and usefulness, the subsequent design elements will be included:

**Clean and Modern Layout:** The website will function a smooth and modern-day format with sufficient whitespace, clean typography, and intuitive navigation menus.

**Branding Elements:** Consistent branding factors which includes the ABC Inc. Emblem, shade palette, and typography might be used during the internet site to keep emblem identification and fortify visual concord.

Visual Hierarchy: Content will be organized the usage of visible hierarchy ideas, with essential records highlighted the use of contrasting hues, large font sizes, and strategic placement.

Responsive Design: The website will be designed to be responsive, making sure top-quality viewing and interaction throughout a variety of gadgets and display sizes.

**Accessibility:**

Ensuring accessibility is a critical thing of website design, as it ensures that each user, consisting of those with disabilities, can get entry to and interact with the content material. To beautify accessibility, the following measures will be carried out:

**Semantic HTML:** The website could be constructed the use of semantic HTML markup, making sure right file structure and screen reader compatibility.

**Alt Text for Images:** Alt textual content might be added to all images on the website, offering descriptive text for users who rely on display screen readers. This will ensure that visually impaired customers can apprehend the content conveyed by images.

**Keyboard Navigation:** The website can be designed to facilitate keyboard navigation, permitting customers to navigate through interactive elements using keyboard shortcuts. This will benefit customers who can't use a mouse or touchscreen to navigate the website.

**Design Justification:**

The selected layout approach for the website is based totally on usability, accessibility, and visual attraction. The easy and modern layout and consistent branding factors will create a professional and cohesive appearance that aligns with ABC Inc.'s emblem identity. Using whitespace and clear typography will beautify readability and ensure that content material is effortlessly digestible for site visitors. The responsive layout will make sure that the internet site adapts seamlessly to one-of-a-kind devices, imparting a constant person revel in across systems.

Accessibility capabilities including semantic HTML markup, alt text for pics, and keyboard navigation guide display a dedication to inclusivity and make certain that everyone users can get admission to and have interaction with the internet site content efficiently.

# **Project details**

The installation of a physical sensor network for ABC Inc's vital infrastructure in Victoria, Australia, is essential for numerous reasons. As industries increasingly rely upon interconnected systems and automation, making sure the safety and reliability of those systems becomes paramount. This mission aims to address these worries by setting up a strong sensor network infrastructure that no longer best collects statistics from various assets but also analyses them to create sensible, net-linked systems.

First and foremost, the established order of a physical sensor network is essential for ABC Inc's critical infrastructure. This community will encompass sensors strategically placed in the infrastructure to reveal diverse parameters, including temperature, humidity, pressure, and movement.  For instance, sensors detecting an unexpected growth in temperature in an important area ought to cause automatic responses, including activating cooling structures or alerting renovation employees. This degree of automation now not only improves operational efficiency but also complements protection by permitting proactive preservation and troubleshooting.

Moreover, the integration of these sensors with the internet opens up the possibility of remote monitoring and control. This means that ABC Inc can access real-time data about its infrastructure from anywhere, at any time. With an internet-connected sensor network, ABC Inc can keep a constant watch on the status of its infrastructure and promptly address any issues that arise.

However, with the advantages of connectivity come potential security risks. The interconnected nature of the sensor community makes it liable to cyber threats, including hacking, information breaches, and malicious assaults. Therefore, it's vital to difficulty the network to thorough penetration testing to identify and mitigate any vulnerabilities.

Penetration testing is a crucial part of the security measures for the proposed network. It involves simulating cyber-attacks to identify weaknesses and test the effectiveness of existing security measures. By conducting penetration testing, ABC Inc can proactively identify and address security vulnerabilities before they can be exploited. This not only protects sensitive data and critical infrastructure but also instils confidence in stakeholders about the network's security and reliability.

# **Technical**

The technical requirements for putting in place a physical sensor network for ABC Inc's important infrastructure in Victoria, Australia, encompass several key additives aimed at ensuring the network's capability, protection, and compliance. Here's an explanation of every requirement:

**Establish a network of bodily and simulated sensors:**

This requirement involves the deployment of each bodily and simulated sensor during ABC Inc.'s critical infrastructure. Physical sensors are hardware devices mounted in various places to gather information on environmental conditions, the gadget's overall performance, and different relevant parameters. These sensors might also include temperature sensors, movement detectors, strain sensors, and more, depending on the precise needs of ABC Inc.'s infrastructure.In addition to bodily sensors, the community will also incorporate simulated sensors, which are digital representations of bodily sensors used for trying out and developing functions. Simulated sensors permit engineers to validate community functionality, look at software programs, and conduct overall performance opinions in a controlled environment before deploying changes to the production network.

**Develop penetration checking out method using open supply equipment:**

Penetration testing is a critical component of ensuring the security of ABC Inc's sensor network. This requirement involves developing a comprehensive penetration testing method using open-source tools like Metasploit, Nmap, and OWASP ZAP. These tools offer a cost-effective and flexible solution for conducting security tests. By leveraging open-source tools, ABC Inc can customize and tailor the penetration testing method to its specific requirements, ensuring thorough coverage of potential security risks.

**Create reporting and certification gadgets primarily based on the cybersecurity framework:**

The final requirement entails establishing a reporting and certification gadget based totally on a cybersecurity framework to record and validate the safety posture of ABC Inc.'s sensor network.

It may be based totally on industry requirements together with the NIST Cybersecurity Framework or regulatory requirements precise to ABC Inc's industry. he technical necessities for putting in place a bodily sensor community for ABC Inc's important infrastructure encompass organising a community of bodily and simulated sensors, developing a penetration trying out manner the use of open-supply tools, and growing a reporting and certification system based totally on a cybersecurity framework.

**GitHub Repository:** ABC-Inc-Sensor-Network

# **Project Progress Reporting**

# **Week 1**

**Individual Progress:**

During this project phase, my recognition became mostly on putting in the environment for the sensor community. I started by installing Kali Linux in a virtual system to obtain this. Kali Linux is a Debian-based totally Linux distribution especially designed for penetration testing and virtual forensics (Mahela, 2020).

|  |  |
| --- | --- |
| Member 1 | Member 2 |
| Research analyst - With several IoT systems available in the market, deciding on the maximum suitable platform that aligned with our assignment dreams and technical necessities posed a project. However, by accomplishing thorough critiques and assessing the capabilities and talents of various structures, we were capable of narrow down our alternatives and become aware of ability applicants for integration into the sensor network | Security analyst - Penetration testing is a critical component of ensuring the security of ABC Inc's sensor network. This requirement involves developing a comprehensive penetration testing method using open-source tools like Metasploit, Nmap, and OWASP ZAP. |

**Group Progress:**

In collaboration with the assignment team, we described assignment milestones and assigned obligations to team individuals.

 This blanketed figuring out the kinds of sensors to be deployed, the communication protocols to be used, and the architecture of the network infrastructure.

**Challenges:**

One of the main demanding situations encountered throughout this segment is knowledge of the intricacies of the Docker platform for sensor deployment.

 With several IoT systems available in the market, deciding on the maximum suitable platform that aligned with our assignment dreams and technical necessities posed a project. However, by accomplishing thorough critiques and assessing the capabilities and talents of various structures, we were capable of narrow down our alternatives and become aware of ability applicants for integration into the sensor network (Bigelow,2020).

**Next Phase Tasks:**

From now on, our next section's responsibilities consist of finalising the choice of an IoT platform for sensor deployment. This involves conducting similar assessments and analyses of the shortlisted platforms to determine their suitability and compatibility with the sensor community requirements. Once the IoT platform is chosen, we can start the process of setting up physical sensor gadgets within the network environment. This will involve configuring and deploying the sensors in step with the predefined specs and layout issues, laying the inspiration for statistics series and evaluation within the sensor network (Mahela, 2020).

# **Week 2**

During week 2 of the task, both individual and organisational progress was made toward putting in the sensor network infrastructure, exploring penetration, trying out equipment, and discussing key mission requirements and challenges.

**Individual Progress:**

Configured Docker packing containers for simulating sensor gadgets with the use of Eclipse Mosquitto:

I centred on configuring Docker boxes to simulate sensor gadgets in the community environment. By leveraging Docker, I created isolated environments for strolling instances of Eclipse Mosquitto, an open-source message broker that enforces the MQTT protocol (Bigelow,2020).

Explored penetration checking out tools consisting of Metasploit and Nmap for vulnerability evaluation:

**Group Progress:**

**Established communicate protocol for sensor information transmission:**

As a set, we collaborated to define a conversation protocol for transmitting sensor information within the network. We determined the MQTT protocol because it is the most appropriate choice for efficient and reliable information transmission between sensor devices and the relevant facts processing device.

**Discussed penetration testing methodologies and recognised ability vulnerabilities:**

We engaged in discussions to outline penetration testing methodologies and discover capability vulnerabilities within the network infrastructure (Mahela, 2020).

**Challenges:**

**Integrating Docker packing containers with the network infrastructure:**

One of the main demanding situations encountered at some stage in week 2 was integrating Docker boxes with the present network infrastructure. This required careful consideration of networking configurations and safety implications to ensure seamless integration and compatibility with the sensor network environment (Kothawade, 2019).

**Understanding the nuances of Metasploit framework for penetration checking out:**

Another challenge became gaining a complete know-how of the Metasploit framework for penetration trying out. Overcoming this assignment concerned dedicated study and fingers-on experimentation with the framework (Kothawade, 2019).

**Next Phase Tasks:**

**Moving forward, our next segment responsibilities include:**

Conducting penetration testing on the simulated sensor community to perceive and mitigate vulnerabilities.

|  |  |
| --- | --- |
| Member 1 | Member 2 |
| Research analyst - We collaborated to define a conversation protocol for transmitting sensor information within the network. We determined the MQTT protocol because it is the most appropriate choice for efficient and reliable information transmission between sensor devices and the relevant facts processing device. | Security analyst - Docker boxes to simulate sensor gadgets in the community environment. By leveraging Docker, I created isolated environments for strolling instances of Eclipse Mosquitto, an open-source message broker that enforces the MQTT protocol |

Our goal is to develop a robust reporting and certification system based on a cybersecurity framework. This system will serve to document the results of our penetration testing activities and ensure strict adherence to industry standards and regulations.

# **Week 3**

During week three of the venture, sizeable development turned into made both as a collection closer to advancing the development and security trying out of the sensor community infrastructure.

**Individual Progress:**

**Conducted penetration testing on simulated sensor network:**

I cantered on executing penetration checks at the simulated sensor network the usage of gear such as Metasploit and Nmap. This involved identifying capacity vulnerabilities in the community infrastructure, exploiting them using penetration checking out strategies, and assessing the effectiveness of present safety controls.

**Continued exploration of penetration trying out gear:**

In addition to undertaking penetration checks, I persevered to explore and familiarize myself with numerous penetrations checking out tools and techniques. This covered similarly experimentation with Metasploit for exploiting vulnerabilities and Nmap for community scanning and enumeration (‌Semenov, 2021).

**Group Progress:**

**Development of a reporting and certification gadget:**

As a group, we worked on growing a comprehensive reporting and certification gadget based totally on a cybersecurity framework.

**Collaboration on addressing identified vulnerabilities:**

We collaborated as a group to address the vulnerabilities recognized during penetration testing. This involved prioritizing vulnerabilities primarily based on their severity and potential effect on the community infrastructure.

**Challenges:**

**Complexity of penetration checking out strategies:**

One of the principal challenges encountered in the course of week three is the complexity of certain penetration checking out strategies and gear.

Overcoming this challenge involved non-stop studying and experimentation to decorate our talent with penetration checking out methodologies (‌Semenov, 2021).

**Coordination of institution efforts:**

Another significant task was the coordination of group efforts to ensure efficient collaboration and communication throughout the development and testing process. Managing tasks, sharing progress updates, and coordinating remediation efforts were all crucial aspects that required clear communication and coordination among team members. Addressing this challenge involved regular meetings, clear task assignments, and proactive communication to ensure that everyone was aligned and working towards common goals (Zhang2021).

**Next Phase Tasks:**

**Moving ahead, our subsequent segment tasks include:**

Continuation of penetration testing sports to in addition verify and validate the security posture of the sensor community.

|  |  |
| --- | --- |
| Member 1 | Member 2 |
| Research analyst - One of the principal challenges encountered in the course of week three is the complexity of certain penetration checking out strategies and gear. | Security analyst - The vulnerabilities recognized during penetration testing. This involved prioritizing vulnerabilities primarily based on their severity and potential effect on the community infrastructure. |

Refinement and finalization of the reporting and certification machine to assemble complete reports for stakeholders.

Implement remediation measures to address identified vulnerabilities and fortify the safety defenses of the sensor network (‌Semenov, 2021).

From the outset, the challenge got down to create a smart, internet-related system for ABC Inc.'s crucial infrastructure in Victoria, Australia. They focused on unique duties, such as configuring Docker boxes for simulating sensor devices, exploring penetration testing equipment like Metasploit and Nmap, setting up conversation protocols for sensor record transmission, and growing complete reporting systems.  Group discussions facilitated expertise sharing, trouble-fixing, and alignment on undertaking goals, making sure that everybody remained at the same page during the mission lifecycle.

They leveraged their collective know-how, performed research, and sought assistance to triumph over barriers and preserve the project heading in the right direction.

# **Conclusion**

This assignment, a spirit of collaboration, resilience, and dedication has been obtrusive amongst crew individuals.  By leveraging man or woman understanding, fostering open communication, and working collectively in the direction of commonplace dreams, the mission team has made significant development closer to achieving its goals and turning in a super answer for ABC Inc.'s important infrastructure.

# **References**

‌Semenov, S., Weilin, C., Zhang, L. and Bulba, S., 2021. Automated penetration testing method using Deep machine learning technology. Advanced Information Systems, 5(3), pp.119-127.

Zhang, Y., Xie, Y., Zhang, Y., Qiu, J. and Wu, S., 2021. The adoption of deep neural network (DNN) to the prediction of soil liquefaction based on shear wave velocity. Bulletin of Engineering Geology and the Environment, 80, pp.5053-5060.

Bigelow, S.J. (2020). Complete guide to penetration testing best practices. [online] Software Quality. Available at: <https://www.techtarget.com/searchsoftwarequality/tip/Everything-you-> need-to-know-about-software-penetration-testing [Accessed 28 Mar. 2024].

Kothawade, P. and Bhowmick, P.S., 2019. Cloud Security: Penetration Testing of Application in Micro-service architecture and Vulnerability Assessment.

Mahela, O.P., Khan, B., Alhelou, H.H. and Siano, P., 2020. Power quality assessment and event detection in distribution network with wind energy penetration using stockwell transform and fuzzy clustering. IEEE Transactions on Industrial Informatics, 16(11), pp.6922-6932.

Mahmood, A., Tang, X.W., Qiu, J.N., Gu, W.J. and Feezan, A., 2020. A hybrid approach for evaluating CPT-based seismic soil liquefaction potential using Bayesian belief networks. Journal of Central South University, 27(2), pp.500-516.

Najera-Gutierrez, G. and Ansari, J.A., 2018. Web Penetration Testing with Kali Linux: Explore the methods and tools of ethical hacking with Kali Linux. Packt Publishing Ltd.

Railkar, D.N. and Joshi, S., 2023. A Comprehensive Literature Review of Artificial Intelligent Practices in the Field of Penetration Testing. Intelligent Systems and Applications: Select Proceedings of ICISA 2022, pp.75-85.

GIT e-Portfolio

<https://github.com/Diablo0009/COIT20265_Assessment-2/blob/main/COIT20265%20assessment%202.docx> 