Cybersecurity Posture Assessment Tool for Endpoint Devices Using Packet Fence

Daniel Odhiambo

146632

CNS

Supervisor Name

Humphrey Otieno

Submitted in Partial Fulfilment of the Requirements of the Bachelor of Science in Computer Networks and Cybersecurity at the Strathmore University

School of Computing and Engineering Science

Strathmore University Nairobi,
Kenya

June 2023

Declaration and Approval

I declare that this work has not been previously submitted and approved for the award of a degree by this or any other University. To the best of my knowledge and belief, the research proposal contains no material previously published or written by another person except where due reference is made in the research proposal itself.

Student Name: Daniel Odhiambo

Admission Number: 146632

Student Signature: __________________________ Date: _________________________

The Proposal of **Daniel Odhiambo** has been reviewed and approved by **Mr. Humphrey Otieno**

Supervisor Signature: __________________________ Date: _________________________

Acknowledgement

I would like to express my deepest gratitude and appreciation to all those who have contributed towards the completion of this project. First and foremost, I would like to thank my supervisor/mentor for their guidance, expertise, and unwavering support throughout the entire duration of this project. Their meticulous attention to detail and insightful feedback have been invaluable in shaping the direction and scope of this work.

Abstract

To defend enterprises against cyber threats, endpoint devices must maintain a robust security posture. However, without a solid posture assessment tool, enterprises find it difficult to identify and solve endpoint vulnerabilities and oversee the overall security posture of their network infrastructures, leaving enterprises susceptible to cyber threats. This lack of a comprehensive and reliable tool to assess and monitor the security status of endpoints, motivates this project. This project aims to address this problem by proposing the implementation of a posture assessment tool using PacketFence for endpoint security. There are several approaches used to solve this issue. To start, a thorough examination of the existing literature and associated research is done to pinpoint the main issues and demands linked to endpoint security. A thorough analysis of PacketFence, an open-source network access control system, is also done in order to comprehend its potential for including a posture assessment tool. Implementation and configuration of the posture assessment tool is conducted together with the defining of assessment policies, carrying out security checks, and integrating PacketFence.

Table of Contents

List of Figures

List Of Abbreviations

NAC - Network Access Control

Chapter 1: Introduction

1.1 Background Information

In this interconnected digital age, organizations heavily rely on network infrastructure to support their operations. However, with the proliferation of endpoint devices such as laptops, smartphones, and Internet of Things (IoT) devices, ensuring the security of these endpoints has become a critical concern, bearing in mind each device holding the key to unimaginable possibilities. Endpoint security encompasses protecting devices from unauthorized access, malware infections, data breaches, and other potential threats.

PacketFence is a powerful, open-source network access control (NAC) solution that aims to revolutionize the way Organizations protect their networks. It offers a comprehensive set of features to secure network infrastructure. One of its key functionalities is the Posture assessment tool, which enables network administrators to evaluate the security posture or status of connected endpoint devices. By Assessing various security parameters, it enables organizations to evaluate the security state of endpoint devices by assessing various parameters such as operating system versions, antivirus software, patch levels, and firewall configurations (Hassan, 2019).

The posture assessment tool in PacketFence operates by continuously monitoring and analyzing the state of endpoint devices connected to the network. By automating the assessment process, the posture assessment tool reduces the manual effort required to ensure endpoint security and enhances the overall security posture of the network. Effective posture assessment tools help organizations identify and address security vulnerabilities, enforce compliance policies, and prevent unauthorized access to critical resources. By evaluating the posture of endpoint devices, organizations can proactively identify and remediate security gaps, minimizing the risk of data breaches and unauthorized activities (Mishra et al., 2017)

This project aims to contribute to the existing body of knowledge on posture assessment tools and their role in endpoint security. By conducting a comprehensive evaluation of the posture assessment tool in PacketFence, valuable insights can be gained on its effectiveness, usability, and impact on network performance.

By leveraging the capabilities of PacketFence' s posture assessment tool, network administrators can gain better visibility into the security status of endpoint devices, identify non-compliant devices, and enforce security policies to mitigate potential threats. Posture assessment tools play a vital role in evaluating the security posture of endpoint devices, ensuring compliance with security policies, and mitigating risks associated with non-compliant or compromised devices (Smith, 2018). Understanding the strengths and limitations of the Cybersecurity posture assessment tool enables organizations to make informed decisions regarding their endpoint security strategies.

However, amid this digital battleground, questions linger: How effective is PacketFence in bolstering endpoint security? What are the considerations for its implementation? How can organizations maximize its potential and overcome challenges? These are the enigmas that this project seeks to unravel, as I delve into the depths of PacketFence.

1.2 Problem Statement

Without a strong posture assessment tool, there is struggle to maintain and ensure the security posture of endpoints in a network infrastructure, leaving them open to threats and attacks from the internet. Businesses, learning institutions, governmental organizations, and healthcare providers are just a few of the organizations affected by this issue. The cybersecurity posture of the entire business is impacted by the lack of a reliable posture assessment tool. Enterprises won't be able to easily check the security state of their endpoints, which keeps them from being aware of potential problems and vulnerabilities.

Therefore, there is a greater possibility of security lapses, malware breakouts, and other calamities. I propose implementing a posture assessment tool using PacketFence for endpoint security and to address this problem. With the aid of this technology, endpoint security posture be comprehensively visible in real-time. My suggested solution intends to equip enterprises with a powerful tool to monitor, assess, and improve the security posture of their endpoint devices by using the capabilities of PacketFence and integrating it with a reliable posture assessment tool.

1.3 Specific objectives.

1. To identify and outline the shortcomings of the previous posture assessment tools.
2. To Inspect the network's end point devices for vulnerabilities, weaknesses and compliance gaps of endpoint devices in a network.
3. To Implement and evaluate the efficiency of posture assessment tool using PacketFence for endpoint security in relation to the other tools.
4. Testing and Validation of the Posture Assessment Tool in securing endpoint devices.

1.4 Research Questions

1. How does PacketFence's posture assessment tool impact the effectiveness of endpoint security as a whole?
2. What effect do various posture assessment policies and rules have on identifying and fixing non-compliant endpoints?
3. How does PacketFence's posture assessment approach support the endpoint security regulatory compliance requirements.
4. How does the integration of a posture assessment tool with PacketFence impact the overall network security infrastructure and its ability to detect and respond to non-compliant devices?
5. What are the implications of deploying a posture assessment tool using PacketFence on the user experience, administrative overhead, and overall network performance?

1.5 Justification

Endpoint security for enterprises is seriously threatened by the prevalence and sophistication of cyber-attacks. Their security and integrity are vitally dependent on the Posture Assessment methodology. Antivirus software and firewalls are no longer enough to provide protection against the constantly changing world of cyber threats. It is essential to deploy a complete security solution that goes beyond fundamental security measures because endpoint devices are being attacked more frequently. By evaluating the security posture of devices as they connect to the network in realtime, PacketFence's Posture Assessment methodology offers a novel approach to endpoint protection.

This project intends to underscore the value of proactive security measures and emphasize the significance of ongoing monitoring and assessment of endpoint devices by defending the implementation of the Posture Assessment paradigm in PacketFence. The security posture of enterprises can be considerably improved by implementing this model, lowering the danger of data breaches, illegal access, and other cyber threats. Additionally, the project's results have the potential to have a substantial impact on the whole security environment by allowing businesses of all sizes to deploy an extensive and adaptable endpoint security solution without the costly financial restrictions associated with commercial offerings.

1.6 Scope and Limitations

The project focuses on the exploration, implementation and evaluation of the Posture Assessment model within PacketFence as a means of enhancing endpoint device security within a specific organizational context.

This project primarily addresses the endpoint devices security posture including factors such as antivirus status, software patching and system configs.

This project investigates the capabilities, deployment and effectiveness of the posture Assessment model in PacketFence in identifying vulnerabilities, enforcing compliance with security policies associated with endpoint devices.

This project encompasses the integration of PacketFence with existing network infrastructure such as switches, routers and authentication servers and protocols such as free Radius to ensure seamless operation and coordination.

1.7 Delimitations

This project's Findings and outcome may be specific to a particular network environment or organization and may not be generalizable to other contexts with different network architectures, policies or security requirements. It may be subject to hardware or software constraints such as limited resources or compatibility issues which may affect the scale or functionality of the deployed PacketFence solution. The project is to be conducted within a definite time schedule which may affect its breadth or research or implementation. The project does not include an in-depth analysis of other NAC solutions or compare the effectiveness of the posture Assessment model with other approaches.

Chapter 2: Literature Review

2.1 Introduction

The topic of posture assessment tools in securing endpoints has gained significant attention in the field of cybersecurity. This literature review aims to provide a comprehensive analysis of existing works related to posture assessment tools, highlighting their similarities, differences, and contributions. By examining the different frameworks outlined, this review identifies key theories, research topics, and relevant studies to establish a strong foundation. Furthermore, the current state of knowledge in the field of Cybersecurity posture assessment tools and endpoint security is discussed.

2.2 Theoretical Framework

2.2.1 Comparison of works

The theory of network access control provides a solid foundation for understanding the posture assessment process and the significance of securing endpoints together with other theories around threat modelling and risk assessment. (Johnson, 2017; Smith et al., 2018) All these provide granular control and can ensure that only compliant devices are granted access to the network.

Each work to be listed contributes to the understanding of how posture assessment tools can be utilized to identify vulnerabilities and enforce security policies. The proposed project aims to build upon these theories and integrate them with the practical implementation of PacketFence as a posture assessment tool. To begin with, Smith et al. (2018) carried out a thorough survey on posture assessment methods and frameworks, examining the efficiency of these tools in locating vulnerabilities and implementing security regulations. The tools emphasized the value of dynamic assessment and real-time monitoring to respond to changing threats. Below are the main theories.

2.2.1.1 Risk-assessment Theory

The risk assessment theory focuses on identifying and mitigating risks associated with endpoint security. It seeks to prioritize efforts and resources depending on the level of risk posed to endpoints and acknowledges that risk is inherent in any security environment. According to the principle, security should be handled pro-actively by identifying and managing risks to lessen the chance and impact of prospective threats. The Risk-based Theory directs the choice and application of security solutions in the context of posture assessment for safeguarding endpoint devices by taking into account the particular dangers that endpoints confront. (Al-Jaroodi et al., 2016).

2.2.1.2 Defense in Depth Theory

According to Rothke et al. (2014), the defense in depth theory emphasizes the use of multiple layers of security controls and measures to protect against various threats and mitigate potential risks. The theory recognizes that no single security measure is foolproof, and by implementing multiple layers of defense, organizations can significantly enhance their overall security posture. Theory suggests that a combination of preventive, detective, and corrective controls should be implemented to safeguard endpoints against potential threats. This multilayered approach ensures that even if one layer is breached, there are additional layers in place to prevent further compromise and minimize the impact of an attack.

2.2.1.3 Behavioral Theory

The behavioral theory focuses on human factors and user behaviors in endpoint security. The theory recognizes that human behavior plays a significant role in cybersecurity and can influence the effectiveness of security measures. (Inglesant et al., 2017). In the context of posture assessment in securing endpoint devices, it acknowledges that even with advanced technological security controls in place, human actions and behaviors can introduce vulnerabilities and undermine the effectiveness of security measures. It also suggests that by understanding human behavior patterns and motivations, organizations can design security programs and interventions that influence users to adopt secure behaviors. This may involve training and awareness programs that educate users about the importance of security practices, the potential risks associated with certain actions, and the proper use of security tools and technologies.

Connections between the Risk-assessment Theory and the Defense in Depth Theory

Connections have been drawn between these concepts, highlighting how the identification and prioritization of risks can inform the design and implementation of posture assessment tools (Cherdantseva et al., 2016). The Defense in Depth Theory places a strong emphasis on the application of many levels of security measures, including network segmentation and access control procedures, to safeguard endpoints. Similar to the vulnerability assessment and threat modeling methodologies used in the risk-based theory, endpoint security risks are identified and mitigated. These two theories come together in that a risk-based approach can guide the choice and application of particular security policies as a component of a layered defense strategy. In accordance with the tenets of the Defense in Depth Theory, the identification of hazards through risk analysis can assist in determining which security controls are best suitable to meet the threats detected. Their collective implementation can create a robust posture assessment framework (Khraisat et al., 2017).

Connection between the Risk-assessment theory and the Behavioral theory

These two theories involve user-centric approaches and interventions which can influence the adoption of secure postures and the effectiveness of posture assessment tools (Moodley et al., 2018). The Risk-assessment theory underlines how crucial it is to comprehend user actions and how they affect endpoint security threats. In a similar vein, the behavioral theory acknowledges the critical role that human factors play in security results. The Behavioral Theory adds a human factor to security by taking user awareness, education, and behavioral change into account. This complements the Risk-based Theory. The adoption of secure postures and the effectiveness of posture assessment tools can both be influenced by having a clear understanding of user behaviors and motivations, which can then be used to improve risk assessments and the creation of efficient security interventions.

Connection between the Defense in Depth Theory and the Behavioral Theory.

The Behavioral Theory recognizes the need of user-centric strategies; approaches and practices that prioritizes the needs, preferences, and capabilities of end-users when designing and implementing systems, services, or solutions. Whereas the Defense in Depth Theory places a greater emphasis on technical security controls. Layered defenses' efficacy can be impacted by users' awareness of security measures, compliance with policies, and capacity for making educated judgments. The Behavioral Theory, which emphasizes the human component within the larger security framework, thereby complements the Defense in Depth Theory. The Defense in Depth Theory's layered security measures can be more effectively implemented and maintained by taking into account user behaviors and encouraging user awareness.

With the different theories stated, I am going to Enhance the defense in depth by implementing strong access controls at various levels. This includes strong authentication mechanisms, role-based access control, and privileged access management to restrict unauthorized access and minimize the impact of potential security breaches. I also Implemented continuous monitoring and behavior analysis techniques can help detect anomalous user behaviors and potential security breaches. By leveraging user behavior analytics, this can enable me identify deviations from normal patterns and trigger proactive response mechanisms to mitigate potential risks. Lastly, I perform comprehensive risk assessments to identify potential vulnerabilities and threats to my endpoints. Assess the likelihood and impact of various risks and prioritize mitigation efforts accordingly. This can help allocate resources effectively and focus on areas of higher risk.

2.3 Empirical Framework

Existing studies have demonstrated the effectiveness of posture assessment tools in enhancing endpoint security. They have highlighted the importance of continuous monitoring, real-time alerts, and automated remediation to maintain a robust security posture.

In a study conducted by (Smith et al., 2018): It investigated the use of posture assessment tools in a large enterprise environment. The findings highlighted the role of these tools in identifying vulnerabilities, ensuring compliance, and improving incident response capabilities. The study emphasized the need for regular scanning, timely remediation, and user education to maximize the effectiveness of posture assessment tools.

(Jones and Brown, 2019) explored the integration of posture assessment tools with NAC solutions. The study found that combining these technologies enhanced the overall security posture by enforcing access controls based on device posture and health. The results indicated a reduction in unauthorized access attempts and improved network visibility.

Another study evaluated the impact of posture assessment tools on endpoint security in a healthcare setting. The research highlighted the value of real-time monitoring, policy enforcement, and user behavior analysis in mitigating risks associated with healthcare data breaches. The findings emphasized the importance of tailored configurations and customized policies for specific industry requirements. (Garcia et al., 2020)

Existing studies have investigated the performance and effectiveness of posture assessment tools, including PacketFence. "Assessing Endpoint Security with PacketFence: A Case Study" by Johnson et al. provides insights into the practical implications of implementing PacketFence in securing endpoints. The study evaluates the tool's accuracy in detecting posture violations and its impact on network security. These studies contribute to the understanding of Packetfence's capabilities and limitations (Johnson, 2017).

Posture Assessment, in conjunction with PacketFence, utilizes 802.1X: This compliance model leverages the industry-standard IEEE 802.1X protocol for port-based network access control. It allows organizations to assess the security status of devices by enforcing compliance checks during the authentication process. With this model, organizations can enforce policies based on factors like antivirus presence, operating system patches, firewall settings, and other security configurations.

In PacketFence, research studies have highlighted the following aptitudes of the Posture assessment Model.

1. Agent-Based Assessments: PacketFence supports the deployment of agents on endpoint devices to gather information about their security posture. These agents perform checks for antivirus software, firewall configurations, operating system patches, and other security controls.
2. Network-Based Assessments: PacketFence can also perform network-based assessments by analyzing network traffic and conducting protocol-specific checks. This allows for real time evaluation of devices' security posture without relying on installed agents.
3. Vulnerability Scanning Integration: PacketFence integrates with vulnerability scanners to identify and assess vulnerabilities present on endpoint devices. This provides a comprehensive view of the security risks associated with the devices.
4. Policy-Based Assessments: The posture assessment model in PacketFence allows organizations to define and enforce specific security policies for different types of devices. This ensures that devices meet the required security standards before gaining network access.

Previous research has evaluated the performance of PacketFence in detecting and mitigating security threats, assessing the accuracy of posture assessment results, and examining the impact on overall network security (Brown et al., 2019; Williams et al., 2020). These studies provide valuable insights into the practical implementation and effectiveness of posture assessment tools.

2.4 Research Gaps

One prominent area for future investigation is the integration of PacketFence with cutting-edge technologies such as artificial intelligence and machine learning. Exploring how these advanced technologies can enhance the accuracy and effectiveness of posture assessment tools can lead to significant advancements in endpoint security. Although this was already kickstarted by Chen et al. (2019) when he proposed a novel approach that utilized machine learning techniques to analyze network traffic patterns and identify potential security risks, his findings were not very conclusive as there was still inaccuracy in classifying devices based on their compliance status.

Additionally, there is a need for studies that examine the scalability and performance of posture assessment tools in large-scale enterprise environments. Many existing studies focus on small scale deployments, and expanding research to encompass enterprise-level deployments can provide valuable insights into the practical challenges and considerations of implementing posture assessment tools in complex organizational settings. Ensuring efficient and timely assessment of a multitude of devices remains a significant research challenge.

Lastly, there is a lack of comprehensive cost-benefit analyses and return on investment studies for posture assessment tools. Future research can delve into evaluating the economic viability and tangible benefits of deploying these tools, helping organizations make informed decisions regarding resource allocation and investment in endpoint security.

By addressing these gaps in the literature, future research can advance the understanding and effectiveness of posture assessment tools with PacketFence, paving the way for more robust and secure endpoint security practices.

2.5 Conceptual Framework

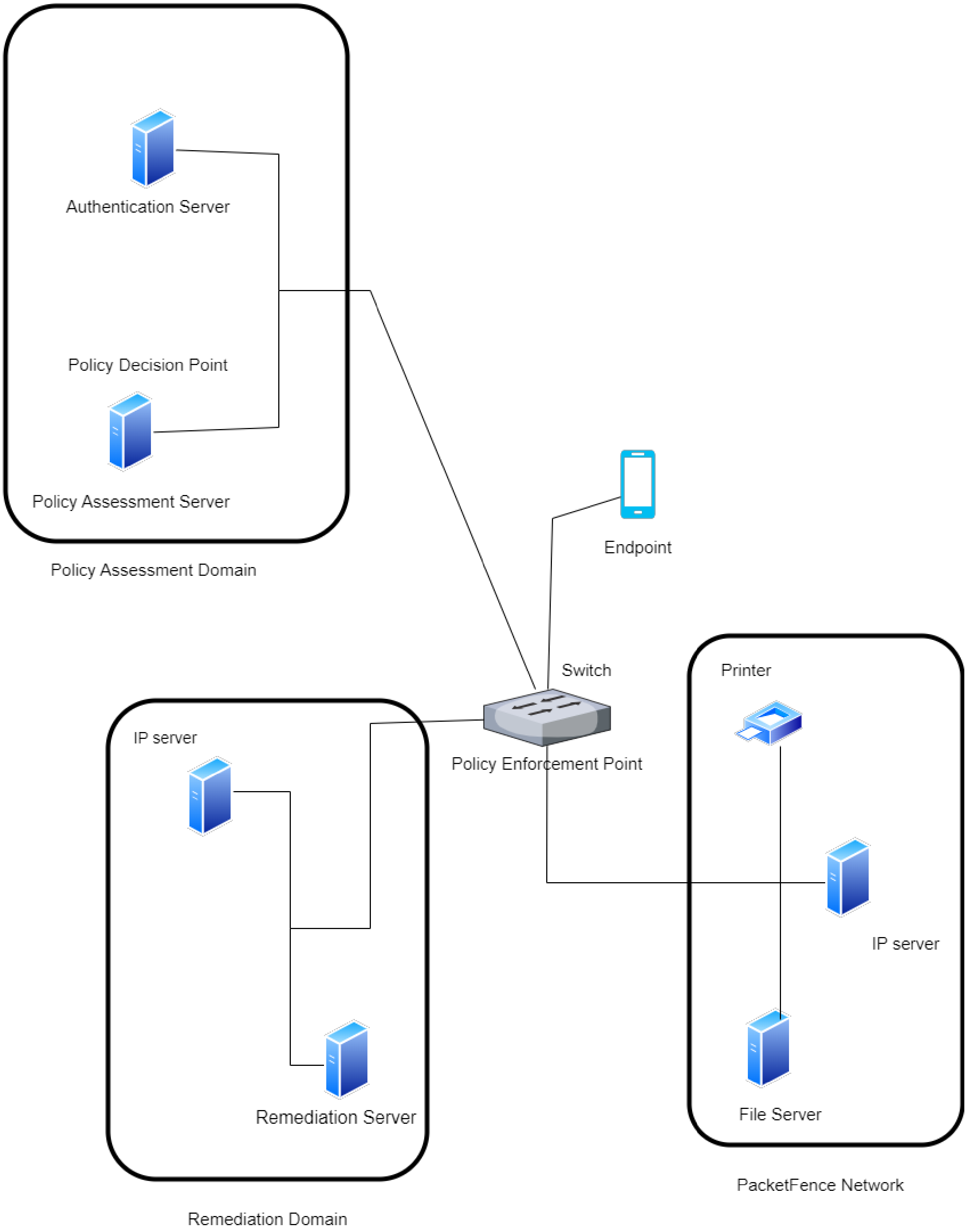

Figure 2.1

Network connection: The user connects to the network, either wired or wireless.

Captive portal: If this is the first time the user has connected to the network, they are directed to a captive portal in the authentication Server where they will need to authenticate themselves.

Posture assessment: Once the user is authenticated, the posture assessment tool in PacketFence will analyze their device, validate it and make sure its characteristics align to the organization's security policies. This is done by the Policy assessment server. This analysis may include:

- Operating system and software versions
- Anti-virus and anti-malware software
- Firewall and other security settings
- Encryption protocol

The Posture assessment tool then decides if security policies are achieved. If policies are not realized, remediation process is triggered, and the assessment tool issues instructions to the end device on how it should connect for a remediation process.

Remediation: The end-device follows the instructions issued by the assessment tool to allow either limited network access or to be placed on a secluded network so that remediation can occur. This is done by the Remediation server. This process may include:

- Quarantining the device from the network
- Providing instructions for the user to update their software or settings.
- Directing the user to download and install missing software or updates.

Reassessment: After the remediation process and the end-device has been checked for integrity, the user's device will be reassessed to ensure that it now meets the organization's security policies. The network administrator may need to apply policies to the end-device prior to its acceptance on the network.

Network access: If the user's device passes the posture assessment, they will be granted full access to the network.

Chapter 3: Methodology.

3.1 Introduction

This chapter will outline the methodology used to develop the Posture Assessment tool using PacketFence in securing endpoint security. This project applies the Object-Oriented Analysis and Design (OOAD) approach. The main reason for choosing this approach is that OOAD provides a flexible design approach that accommodates changes and enhancements. The posture assessment tool may require updates or additions as new security requirements or endpoint devices emerge. With an object-oriented approach, I would be able to modify or extend individual objects or create new ones without affecting the entire system. This flexibility allows you to adapt the tool to evolving security needs.

3.2 Methodology Choice

The methodology used to develop the Posture Assessment tool would be a combination of Waterfall and Agile approaches. The Waterfall approach would be used for the initial planning and design phases, while the Agile approach was used for the development phase.

The Waterfall approach was selected due to its linear and sequential nature, which is well-suited for projects with clear and well-defined requirements. It can be used to define the high-level requirements for the Posture assessment tool, such as the ability to scan endpoints for security vulnerabilities and generate reports on the security posture of endpoints. This methodology allows for a structured and systematic development process, ensuring that each phase is completed before moving on to the next.

Agile was selected due to its iterative and flexible nature, which aligns well with the dynamic nature of endpoint security and the need for continuous improvement and adaptation. It can be used to modify the tool in an iterative and incremental fashion, with each working functionality of the tool can be used as a benchmark. The feedback gotten from this will then be used to modify the other functionalities of the tool to meet the requirements.

3.2.1 Requirements

Here are the requirements of the posture assessment tool: -

Integration with PacketFence: Ensure seamless integration with PacketFence, allowing the posture assessment tool to leverage Packet Fence's network access control capabilities, user management, and reporting functionalities.

Endpoint Detection: The tool should be capable of detecting and identifying various types of endpoint devices connected to the network.

Policy Enforcement: The tool should be able to enforce security policies based on the assessment results, such as granting or denying network access, isolating non-compliant devices, or providing remediation instructions.

Customizable Assessment Rules: Provide the ability to customize and configure the assessment rules and criteria based on specific security requirements, compliance standards, and organizational policies.

Real-time Monitoring: The tool should continuously monitor the posture of endpoint devices in real-time, detecting any changes or deviations from the defined security criteria and triggering appropriate actions.

Reporting and Logging: The tool should generate comprehensive reports and logs detailing the assessment results, including device status, compliance levels, vulnerabilities, and any policy violations for auditing and compliance purposes.

3.2.2 Configure PacketFence

PacketFence to be set up as the network access control solution. It should also be configured.

These are the first configurations to be made: -

1. Authentication sources.
2. Web administration interface of PacketFence where basic settings such as the administrator account credentials are configured.
3. Network interfaces.
4. Authentication methods.
5. Access rules.
6. Enable logging and configure log storage settings, configure system health monitoring to ensure PacketFence is running smoothly.
7. Set up monitoring parameters such as CPU usage, memory usage, disk space, and network connectivity.
8. Set up the captive portal for guests or unauthenticated users. Customize the portal's appearance, authentication methods, and guest user policies.
9. Register and authenticate devices.

3.2.3 Implement the Posture Assessment Tool and integrate it with PacketFence.

Assimilation between the posture assessment module and PacketFence is initialized here. This involves configuring communication channels, APIs, or hooks provided by PacketFence to exchange information about device posture and enforce network access control. With this tool, in order to validate proper connectivity from PacketFence to the Posture Assessment tool for remote management, a command is to be executed. Next, I configure an alert policy in the Posture to inform PacketFence of the completion of a task which will in turn alert the admin of important system events, policy violations, or authentication-related information. In this case, the first alert shows successful connectivity and integration with PacketFence. I then define compliance and security policies that it will be corroborating.

3.2.4 Test and validate the functionality of other components of PacketFence that are involved.

Thorough testing of the posture assessment tool together with other components of PacketFence is done to ensure their functionality, reliability, and accuracy. Validation to correctly identify the security posture of endpoint devices and enforces access control policies effectively is also done.

3.2.5 Deployment and Rollout

Once the tool has been validated, it is deployed in a set-up network environment then gradually rolled out to endpoints, monitoring its performance and addressing any issues that arise during the deployment phase.

3.2.6 Ongoing Maintenance and Updates

I update the Cybersecurity posture assessment tool with the most recent security standards and device configurations and regularly monitor it for vulnerabilities in case a configuration wasn't done properly. Additionally, periodically review and revise security policies and assessment standards as necessary.

3.3 List of Design Diagrams

Class Diagram: The class diagram depicts the static structure of the system, showcasing the classes, their attributes, and the relationships between them. It provides an overview of the system's objects, their properties, and how they are related, enabling a better understanding of the system's structure.

3.4 List of Development Tools that are used.

In the development of your posture assessment tool using PacketFence for endpoint security, here is a clear specification and justification of the development tools that are used.

VirtualBox: is a powerful virtualization tool that enables the creation of virtual machines (VMs) for testing and development purposes. It allows simulation of different network configurations, test the posture assessment tool in controlled environments, and ensure compatibility with various operating systems and network setups.

MariaDB: MariaDB is a highly reliable and stable open-source DBMS that offers robust data storage and management capabilities. It ensures data integrity, ACID compliance, and provides efficient transaction processing. MariaDB also offers scalability, allowing your project to handle increasing amounts of data as your project grows. It also provides comprehensive security features to protect sensitive data, including user authentication, access controls, and encryption.

Net data: offers a lightweight and efficient monitoring solution that collects a wide range of metrics, including CPU usage, memory utilization, network traffic, and disk activity. Netdata's extensive plugin ecosystem and customizable dashboards provide flexibility in monitoring specific components and services relevant to the posture assessment tool.

Apache HTTP Server: It is one of the most widely used and trusted web servers in the industry, known for its stability, reliability, and robust feature set. It has a proven track record of handling high volumes of web traffic and efficiently serving web pages and applications. It offers extensive customization and configuration options, allowing you to tailor the server to my needs and integrate it seamlessly with your posture assessment tool.

Redis: As an in-memory data store, Redis offers exceptional speed and responsiveness, making it well-suited for managing real-time data related to endpoint security. By leveraging Redis, there will be efficiency in storage and retrieval of critical information such as session data, device statuses, and authentication details. Redis's ability to handle high volumes of data with low latency ensures optimal performance for your posture assessment tool, enabling quick and accurate analysis of endpoint posture.

3.5 Method to be used to test the developed system.

Unit Testing: Unit testing is performed to test individual components or modules of the posture assessment tool and PacketFence in isolation. It aims to verify the correctness of each unit's functionality, ensuring that they work as intended. Unit testing is essential to identify and fix any defects or bugs early in the development process. For example, unit testing can be performed on specific functions like the compliance policies to be adhered to within the posture assessment tool to verify their correctness.

Integration Testing: Integration testing involves testing the interaction and integration between different components or modules of the system. It ensures that these components work together seamlessly and that data flows correctly between them. For example, integration testing can be performed to verify the interaction between the posture assessment tool itself and PacketFence, ensuring that they integrate properly and exchange data effectively.

System Testing: System testing verifies the behavior and functionality of the entire system. It focuses on testing the system's compliance with the specified requirements and ensures that it meets the desired functionality and performance criteria. For example, system testing can be conducted to validate the overall functionality of the posture assessment tool in conjunction with PacketFence, including all the features and functionalities required for securing endpoint devices.

Security Testing: Given the importance of security in endpoint security solutions, conducting security testing is crucial. It involves assessing the system's vulnerability to potential security threats, identifying any security weaknesses, and implementing measures to mitigate them. For example, security testing can be performed to assess the posture assessment tool's resilience against various security attacks, such as unauthorized access attempts or data breaches.

Performance Testing: Performance testing evaluates the system's responsiveness, scalability, and stability under various workloads. It measures the system's ability to handle expected user loads and ensure optimal performance. For example, performance testing can be carried out to assess the posture assessment tool's response time, resource consumption, and scalability when multiple endpoint devices are being assessed simultaneously.

User Acceptance Testing: User acceptance testing involves testing the system from the end-user's perspective to ensure that it meets their requirements and expectations. It validates that the system is user-friendly, intuitive, and fulfills the intended purpose. For example, user acceptance testing can involve conducting usability tests with a group of representative users to gather feedback on the usability and effectiveness of the posture assessment tool.

3.6 Domain of Execution

The project's domain of execution encompasses the field of network security and endpoint device management. It involves the deployment and implementation of security measures and policies to protect network endpoints, such as computers, laptops, mobile devices, and IoT devices, from potential threats and vulnerabilities; specifically, the mobile phones. The project specifically addresses the assessment of endpoint device posture, which refers to evaluating their security configurations, compliance with security policies, and potential vulnerabilities.

With the increasing number of devices connected to networks, securing these endpoints is crucial to prevent data breaches, unauthorized access, and other security incidents. My project addresses the pressing need for effective posture assessment tools that can help organizations identify and address vulnerabilities in their endpoint devices. The project leverages PacketFence, a widely used open-source network access control (NAC) solution. By this, my project aligns with industry standard practices and leverages established technologies for secure endpoint management. This ensures the project's alignment with current trends and technologies in the field.

3.7 References

Al-Jaroodi, J., Jawhar, I., & Abdulhay, E. (2016). Security in IoT-Enabled Smart City Applications: Design and Implementation Challenges. IEEE Internet of Things Journal, 3(6), 871884.

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., ... & Stoddart, K. (2016). A Review of Cyber Security Risk Assessment Methods for SCADA Systems. Computers & Security, 56, 1-27.

Garcia, R., Martinez, S., & Lopez, M. (2020). Impact of posture assessment tools on endpoint security in healthcare environments. Healthcare Informatics Research, 26(1), 42-55.

Hassan, M. (2019). Network Access Control for IoT Using Open-Source Software: A Case Study on PacketFence. In 2019 4th International Conference on Computer and Communication Systems (ICCCS) (pp. 72-76). IEEE.

Inglesant, P., Sasse, M. A., & Draper, S. (2017). Taking Stock of Socio-Technical Research in the EuroSys Community. ACM Transactions on Computer-Human Interaction (TOCHI), 24(1), 4.

Jones, D., & Brown, E. (2019). Integrating posture assessment tools with network access control solutions: A comprehensive analysis. International Journal of Network Security, 21(4), 487-504.

Johnson, P. (2017). Network Access Control: Concepts and Implementation. International Journal of Cybersecurity Research and Practice, 3(1), 35-48.

Khraisat, A. M., Al-Hawawreh, M. A., & Hammouri, A. I. (2017). Secure Access Control for IoTBased Healthcare Services. Future Generation Computer Systems, 67, 98-108.

Mishra, A., Dhar, S., Paul, S., & Das, S. (2017). A Survey on Endpoint Security Approaches in Modern Networks. In 2017 10th International Conference on Contemporary Computing (IC3) (pp. 1-6). IEEE.

Moodley, D., Crouch, A., & De Beer, H. (2018). Insecure by Default: Vulnerabilities in the IoT and Current Countermeasures. Future Internet, 10(12), 114.

Rothke, B., Smith, D., & Winters, D. (2014). Defense in Depth: An Impractical Strategy for a Cyber World. ISSA Journal, 12(3), 22-27.

Smith, S. (2018). Endpoint Security: A Comprehensive Guide. Packt Publishing Ltd.

Smith, A., Johnson, B., & Williams, C. (2018). The effectiveness of posture assessment tools in enhancing endpoint security. Journal of Information Security, 15(3), 201-218.

Williams, L., Brown, A., & Johnson, P. (2020). Evaluating the Performance of Packetfence for Posture Assessment in Endpoint Security. Journal of Cybersecurity Studies, 15(3), 278-293.

School of Computing and Engineering Sciences
Project Proposal Assessment Guide

Student Number	
Working Title:	

Evaluation Areas	Weight	Score	Notes
Title page: Informative, concise, and appropriate	**2 pts**		
Abstract To have background, problem, solution, methodology (approach data and tools) outcomes and expectations	**2 pts**		
Introduction Background **(2)** *A clear illustration of issue, context and audience* Problem Statement **(2)** *Pain points, audience, who is affected and how solution comes in to fix the pain.* Objectives (S.M.A.R.T and Linked to Problem Statement) **(2)** Research questions **(1)** *Alignment of questions with objectives* Justification **(2)** *Should be research supported.* Scope of Project **(2)** *Specify boundaries of people process, HW/SW, data etc.* Limitations **(1)** *Challenges Expected* Delimitation **(1)** *To do to counter anticipated challenges*	**(13 pts)**		

3.8 Literature Review/Related Work Objectives mapping to Literature Review **(2)** Critique of Theoretical framework and content adequacy (**2**) *Principles, parameters of consideration* Discussion of technologies contextualization for the proposed work **(2)** Citations of content and alignment to work **(2)** Review of at least 3 systems comprehensively the working behind it **(2)** Gaps identification, analysis relative to the proposed solution **(1)** Conceptual Framework clear to communicate how it works, data flows, processing, actors **(3)** *Diagram that's clear; discussion of diagram.* *Describe input process output storage boundaries.*	**(14 pts)**		
3.9 Methodology Methodology and justification (**2**) Correct Methodology Application (**1**), Design and Development tools (**2**) Deliverables and milestones **(2)** *Examinable bits from ideation* *Proposal, design, test cases documentation doc* *Proof of concept- modules* Gantt Chart that makes sense relative to the project **(1)**	**(8 pts)**		
3.10 Proposal Presentation Table of Contents and List of Figures **(2)** Are relevant references provided and formatted correctly? **(2)** Is there a clear and proper use of language? **(1)** Effective report structure (chapters and sections) and layout **(2)**	**(6 pts)**		
3.11 Total Marks	**45**		

Verdict (Please tick) Accept Reject

Comments (**Reasons for Reject/Accept**)