Implementing an Intrusion Detection System for Bidea

Name

Institution

Table of contents

Abstract

Bidea is a small business that deals with travel and tourism. Many persons use the Bidea's services on a daily basis. Nowadays it's very significant to keep a high degree of security to guarantee safe and reliable transfer of data between the business and its clients. "Intrusion detection system" protects networks and systems from malicious attack. An "intrusion detection system (IDS)" is indeed a software or device application that observes network scheme activities for mischievous activities or strategy violations and generates accounts to a managing station. In respects to computing, "an intrusion detection system (IDS)" is a set of systems or any system that has the capability to sense a variation in the behavior of a network or system (Kashyap, Agrawal, & Pandey, 2012). An IDS could be something simple like network host utilizing a modest application to study about the situation of a grid, or it could be an extra complex scheme that uses numerous hosts to aid capture, analyze, and process traffic. Because Bidea provides diverse services to clients, there is a need for IDS implementation to safeguard the client's data from intruders

Key-words

Bidea, Security, intrusion detection, strategy, analyze, network packages, technologies, firewall, encryption, process traffic

The problem Summary

The modern technology is indeed running the globe. The difficulty is that when innovation in the technology advances, the technological criminality increases. For instance, cyber-attacks are indeed among the problems faced by businesses in the modern world. As a consequence, many job chances are numerous in the profession. The upsurge in the extensive utilization of technology triggered an increase in cybercrime. Bidea company has a system that it uses to serve its clients, and therefore it can easily be targeted by hackers. These hackers are motivated to undertake intrusion due to various reasons. As technological innovation rises, the systems attacks also increase exponentially. At one completion of the measure, there're "script kiddies" eager for an unassertive payday from releasing some "ransomware" on a lone computer. On the other hand, hackers consider cybercrime as "cheaper, faster and easier than traditional method" to outdo a competitor. The reality that cybercrime nowadays permeates each facet of culture displays why cyber safety is critically important.

Many people across the world appear to have grasped the skill of utilizing the machine to acquire what they need. It is disastrous that some companies tend to utilize their computer understanding to giveaway with information from their fellow firms. Bidea is yet to employ competent professionals who can guarantee the company's systems security. Consequently, cyber-attacks on the system would affect the customers. When Bidea's systems are attacked, the firm's reputation is destroyed, and customers would not trust the company anymore. Protecting data for Bidea is very significant in guaranteeing the firm is certainly not compromised. Therefore, "failure to protect the information will lead to destroying the trust that the customers have to the company" (Conner, 2018). With striking speed, innovation and agility, cybercriminals penetrate well-meaning administrations in seconds, thieving data, the future and trust of the whole business. Thus, such intrusions posture a serious safety danger in Bidea's networked environment. Although systems could be hard-edged against numerous types of interruptions, often invasions are positive making schemes for sensing these intrusions dangerous to the safety of this scheme. A network interruption attack could be any utilization of a system that interferes with its steadiness or the safety of data that's stored on machines linked to it. A very extensive range of action falls in this definition, comprising attempts to undermine the entire system, gain illegal access to privileges or files.

Bidea's cyber-attack could involve a virus, hacker, phishing, malware or other action on the company's computer scheme. Attacks could come from outside or inside the company. Bidea's Inside bouts are often committed by unscrupulous workers. Outside attacks could be undertaken by criminals situated nearly anywhere in the globe, or occasionally even corporate detectives. Bidea's cyber-attack could be devastating since a single incident can influence the firm in numerous ways (Bonner, 2013). The attack could lead to damage or loss of electronic data, loss of income, extra expenses, network safety, and privacy litigations, extortion losses, and announcement costs amongst others. Thus, in the current world, systems are inevitable, and there is a persistent problem of intrusion and hacking. Therefore, Bidea's contemporary technology requires strong systems to prevent hackers and malicious people from getting unauthorized access to the systems and network of an organization.

IT solution

For Bidea to prevent intrusion, the solution is to implement "an intrusion detection system IDS" to inspect all outbound and inbound network activity and identify suspicious patterns that could indicate a system or network attack from somebody trying to compromise or enter into a system. Intrusion detection functions by collecting data and then scrutinizing it for unsuitable occurrences. An information technology administrator then uses the data to undertake future protection measures and establish improvements to network security. Thus, the intrusion detection scheme collects and analyzes data from a network or computer to identify unauthorized misuse, access, and likely violations. The intrusion detection seizes packets traveling along several communication mediums and analyzes them. Once an intrusion detection is implemented, it monitors and analyses system and user activity, audit system vulnerabilities, and configuration assesses the veracity of data files and critical system, abnormal action analysis, auditing operating system. The intrusion detector for Bidea will be able to detect intrusion in three ways.

a) Signature detection

The signature detection may be referred to as misuse detection. It attempts to identify the activities that suggest a system abuse. It is realized by creating intrusions models. The incoming actions are matched with the models of intrusion for decision and detection. The simplest method of signature restructuring utilizes simple patterns equivalent to compare the packets of the network against second signatures of recognized attacks. Signature acknowledgment could establish known bouts, but there’s a possibility other packages that are identical to the similar signature would trigger sham signals. There’s a necessity to customize the signature. Despite the challenges with intrusion based on signature detection, the systems are common and function well when designed correctly and checked closely.

b) Anomaly detection

The model comprises of a pool or “database” of anomalies. Any action that is noticed within the database may be referred to an anomaly. However, any drift from ordinary utilization is regarded as an attack. An intrusion in the network is a kind of attack that originates from exterior the local area network, normally through the internet. Systems for intrusion detection are important fundamentals in any security plan for the network. Some organizations rely on the firewalls for intrusion detection, and key firewall developers are creating some intrusion prevention and detection elements into the product.

Nevertheless, a dedicated intrusion detector device could detect a broader array of malicious actions than those ‘included in firewalls. The line amid IDS and firewall technology is getting more unclear, nonetheless, traditionally, a variance was indeed that “intrusion detection systems” could “understand” the subjects of packet headings, such as options and flags, rather than simply looking at ports and IP addresses. Firewalls have become smatter and application cover filtering firewalls could perform similar sort of profound inspection like an IDS. Add-on produces, regularly created by IDS sellers, could make the firewalls function even more proficiently in the role of IDS. Thus, the solution to the increasing cyber threats is the deployment and implementation of an “intrusion detection system.”

Implementation plan

Bidea is keen to keep the data and information for the company and clients secure. The company is following the foot stapes of many other companies that have declared war on cyber-attacks by implementing IDS. Therefore, to be able to compete with the well-established companies, Bidea requires strong security system that would prevent intrusion like the "intrusion detection system." IDS dealers implement products in diverse ways, and there're consequently various methods to categorize "intrusion detection systems." The initial one is founded on the range of monitoring by IDS. That is, if it's installed and utilizes information from a solitary host machine, or is product based on a network that monitors traffic flow on the whole system, and analyzing data from discrete computers. Another dissimilarity in implementation is concerned about how the seller markets the scheme, as an integrated hardware gadget or software product. The IDS can be implemented as host-based intrusion detection or network-based intrusion detection. In a "host-based intrusion detection" a software is indeed installed on a particular scheme, and the information from the system is utilized to sense intrusions (Shinder, 2005). Because the "host-based IDS" protects the server "at the source," it can further intensely guard that particular computer.

The “host-based system” normally checks the log files in the computer to look for signatures of attack. Significant system stores and executables could be checked occasionally for unforeseen changes. A host founded system would also check ports and activate an alert when sure ports are opened. A “network-based IDS” monitors information from network traffic flow and information from more or one host machine to sense intrusions. “A network-based IDS” analyzes data packets transmitted over the system, and mostly utilizes a “promiscuous” network connector. The “network-based IDS” examines packet headings, which are usually not realized by “the host-based IDS.” This permits the discovery of “Denial of service (DoS)” and other forms of attacks that could not be sensed by a “host-based IDS.”

IDS implementation and evaluation

A) Strategizing the scope of the IDS

For Bidea to implement the intrusion detection system, there will be enough time to collect the client’s requirements to ensure that the kind of intrusion detection implemented in the business is appropriate and serves the intended purpose. The best members will be selected to form a team that will be tasked to successfully implement the IDS for the company’s systems without challenges. Before implementation of the application, the selected team members will have to benchmark in a company where the intrusion detection system is functioning properly to understand all that is required and needed for the task. Benchmark is necessary because it gives clear insights into what is expected. Thus, the team will have the knowledge of the functions, challenges, and technical hitches that they may face when implementing the IDS. The communication from the team tasked with the project will only be made by the team leader who will be working as the manager for the project. Any malfunctions, success and required resources must be communicated by the team leader only. Again, the team will take full responsibility to gather the needed artifacts.

B. Preparing the system

The Bidea project will utilize the “host-based intrusion detection system.” This form of intrusion detection provides sufficient protection to the host machine or server and hence protecting attacks (Hoque & Mukit, 2012). The placement of the IDS will be done by the selected team once the project commences. The “host-based IDS” will use a server that hosts much of the Bidea’s important information. Thus, once an intruder attempts to access the system without authorization, the detector in the server will certainly alert the administrator to take action hence preventing the destruction. All the necessary applications for the “host-based IDS” will be identified, and purchased to ensure that the detector has all the supportive applications to function properly.

C), Implementing the system.

Before running the IDS, the central server of Bidea would be installed with an antivirus. Antivirus is an application that thwarts virus from attacking the computer or system. Therefore, the virus would be prevented from accessing the system for maximum security. The implementation process will also include the installation of SNORT as alert nodes on dissimilar zones of the entire network. Snort is indeed “open source” intrusion deterrence system provided by Cisco.

D). Testing the system

After the installation of the IDS on the Bidea system, antivirus, and all other supportive applications, there will be serious testing of the functionality and effectiveness of the system. Normally, after installation of any system, testing is done to confirm that the intended purpose of the system has been addressed and achieved. Since the project is about the implementation of an IDS, penetration tests must be done to observe if the IDS can indeed prevent an attack on Bidea platform or detect it. To achieve this noble duty, the teams will test intrusion with a port scanner, intrusion by a network sniffer, and intrusion by the external network in the presence of the Bidea executive to confirm the level of resistance to penetration. During the penetration test, the team will be summarizing the findings such as hitches, success and all other issues being tested in the process. If there is an issue to be fixed or changes will be implemented to ensure that the client’s needs and requirements agreed upon are met.

E). Completion of IDS

The Bidea project of installation of IDS would be completed when all requirements are addressed as per the contract signed. The client will be allowed to develop or suggest work that is outside the agreement. Therefore, the team leader should ensure that all the requirements are addressed. Thus, the completion of the project will include full adherence to requirements as provided in the contract. The implementation of an “intrusion detection system” will take six months. There will be constant maintenance for the website issues. The maintenance communication plan will have only two entities that can trigger a maintenance exercise. The projects team leader and the Bidea representatives. If the Bidea gets a challenge before the scheduled date of maintenance, the company can contact the project team member for assistance. Otherwise, the team leader will lead the team to the scheduled maintenance periods by the company. The system would need a maintenance tracking system to guarantee that there's transparency and the client is served all times appropriately. The system itself should have logs to keep information about the people who handle the maintenance.

2. Project outcomes and deliverables

When the Bidea intrusion detection system is concluded, the team would have accomplished the agreement between the Bidea firm and them. This contract would become among the projects that are displayed in the portfolio of the company's IDS projects. Through the effective conclusion of the contract, Bidea could recommend the services to many other potential customers, therefore, building a client base. Deliverables would comprise the artifacts that were gathered, the feedback from the team and client, the system developed by adhering to the information security policy, and the ongoing maintenance of the system for two years. The implementation of "intrusion detection system" project is expected to end on November 28, 2018.

Review of other work

Mohammad Sazzadul Hoque wrote a journal "implementation of intrusion detection system using a genetic algorithm." The project is largely related to the proposed task. The ultimate goal for Muhammad is to provide an intrusion detection system. The author of the article admits that currently, it’s very significant to keep a high degree of security to guarantee trusted and safe communication of data between several organizations. But secure information communication via the internet and some other system is constantly under risk of misuses and intrusions. So “intrusion detection systems” have turned out to be a needful element in relation to network and computer security. There’re various methods being used in intrusion recognitions, but unluckily all schemes so far are not entirely flawless. So, the search for betterment remains. In this development, the projects undertaken presented an “intrusion detection system,” by applying “genetic algorithm” to proficiently detect various kinds of network invasions. Evolution processes and parameters for the genetic algorithm are deliberated in depth and implemented. This method uses the evolution model to information development to sieve the traffic information and thus decrease the complexity.

To measure and implement the efficiency of the scheme on the eBay infrastructure, the “KDD99 benchmark database” was utilized and gave reasonable recognition rate. The work provides an “intrusion detection overview.” The overview presents major groups of networking bouts. These categories include denial of service, remote to user attacks, the user to root attacks, and probing. The author provides an overview of a Genetic Algorithm. The algorithm is explained as a programming method that imitates biological advancement as a strategy for problem-solving. GA utilizes a natural selection and an evolution that utilizes a chromosome-like information structure and advance the chromosomes utilizing selection, mutation and recombination operators (Hoque & Mukit, 2012). The process ordinarily begins with arbitrarily generated people of chromosomes, that represents all conceivable resolution of challenges that are regarded candidate solutions.

A second project is described by Davide Adami in the article “Design, implementation, and validation of a self-learning intrusion detection system.” The work is directly connected to the task as it demonstrates the utilization of “intrusion detection systems (IDS).” The author specifies that IDS has become a key component in network safety. The author states that the previous few centuries, the internet has witnessed an explosive development. Alongside the extensive proliferation of fresh services, the impact and number of security bouts have been unceasingly increasing. Certainly, the knowledge needed to undertake about has been reducing, since software features for this purpose are largely obtainable on “websites” all across the world. Recent developments in encryption, community key exchange, numerical signatures, and the growth of associated standards have established a base for network safety. However, network safety goes outside, because it should include safety of networks and computer systems, at all stages, “top to bottom.” To this goal, the utilization of an “intrusion detection system (IDS)” is a key importance to disclose ongoing invasions in a system or in a network (Adami, 2011).

The article presents the implementation, design, and the authentication of a “network IDS,” based on abnormality detection techniques. The scheme, which is planned as an innovative alteration of well-tested methodologies, relies on overseen learning techniques. Given a teaching dataset, the “IDS” is capable to establish a real model of the standard conduct of the system, which would be used, throughout the execution of the scheme, to organize network action either as anomalous or normal. Mostly for this characteristic, the scheme is named “self-learning intrusion detection system.” The article is structured with sections where one of them defines the functionality and architecture. The other segments comprise of two sub-sections that are dedicated to the functionality scrutiny of the “IDS” in a real and matched network. Finally, the paper ends with some concluding remarks and offers suggestions for impending works.

A third project by Dhawal Khem introduces the reader to "intrusion detection systems" and give a deep understanding of some sophisticated methods for invasion detection. Intrusion exposure is a significant element of infrastructure defense mechanisms. Given the growing complications of today's system environments, extra hosts are getting vulnerable to assaults, and hence it's essential to observe efficient, systematic, and automatic approaches for "intrusion detection." The author discusses some information mining founded approaches for "intrusion detection" and relate their demerits and merits. They also examine some signature centered detection methods for "detecting polymorphic worms." The author uses numerous port scanning methods and converses some systems for "detecting port scanning attempts." They then explore the design of an "advance intrusion detection system." The author discusses a passive scheme where the IDS device detects potential safety breach. Each worm retains an exceptional bit string that could be utilized to recognize the worm. Hence, worms could be detected effortlessly using modest signature-based methods.

Polymorphic worms alter their representation beforehand spreading. Each occurrence of a polymorphic “worm” would have a diverse “bit-stream representation.” An anomaly-based invasion detection scheme is for “detecting computer intrusions” and abuse by monitoring scheme activity and categorizing it as either anomalous or normal (Khem, 2011). The arrangement Is founded on rules or heuristics, rather than signatures or patterns, and would detect any kind of misappropriation that differs suggestively from ordinary system operation. Earlier, IDSs depended on nearly hand coded guidelines designed by safety experts and system administrators. Nevertheless, given the necessities and the complications of today’s system environments, there is of an automated and systematic IDS development procedure instead of the pure understanding based on engineering methods which depend only on “intuition and experience.”

The fourth article is also related to the project because it handles “Analysis and evaluation of network intrusion detection methods to uncover data theft.” Julien Corsini argues that in the modern world, many establishments utilize “signature-based intrusion detection” to detect interlopers on their network. The author admits that the tendency is indeed partly because of the reality that “signature detection” is a famous technology, as, unlike anomaly detection that is vigorously being researched. Alongside this, “anomaly intrusion detection system” is understood to produce numerous alerts, most of which are false alarms. Therefore, Julien suggests that establishments require a comprehensive comparison between diverse tools to choose what is the finest appropriate for their requirements (Corsini, 2009). The project is about comparing the signature and anomaly detection techniques to understand the best-suited method to uncover threats like data theft. Therefore, the four reviewed works are directly linked to the task and provide insights into how intrusion detection has turned into a very important concept in the world of computing and technology.

Relation of Artifacts to Project Development

The first article brings about the struggles companies like eBay are making to see an accurate intrusion detection system. The article related to the project as it concentrates on “implementation of intrusion detection system using a genetic algorithm.” The use of the genetic algorithm is an attempt to increase the detection efficiency. The second reviewed work focuses attention on “Design, implementation, and validation of a self-learning intrusion detection system.” Describing how the intrusion detection system can be self-learning. The third article explores the “intrusion detection system” and provides a clear roadmap on how intrusion can be noticed in a sophisticated method. The fourth project concentrates on "Analysis and evaluation of network intrusion detection methods to uncover data theft." The article provides analysis and understanding about intrusion and data theft. Therefore, the reviewed articles relate directly to the project, and this shows how intrusion detection systems are so valued in the contemporary world or digital era.

Project Rationale

Bidea company has been careful and cautious in handling client’s information. The internet and advanced technology embraced by the Bidea has enabled it to grow rapidly. However, the growth of Bidea doesn’t mean that the company is too big for system intrusion. The attack in many other firms highlight that every company, regardless of the strength of their security is vulnerable to attack. Because Bidea intends to compete with the other companies in the industry, there is a necessity to invest in the security of the company’s system security to guard the client’s data. Protecting client’s information would improve customer confidence, trust, and the company’s reputation. Bidea is also expanding, and the systems are getting a broad user base.

The numerous numbers of user access place the company in a precarious situation and easy target by the intruders. Even the companies with s best-run safety are intruded. Therefore, Bidea is determined to invest in an “intrusion detection system” to ensure that all illegal attempts to access the system are detected and perhaps thwarted. This is because, with an adequate period, a dedicated attacker could compromise the finest security. Thus, Bidea aims to secure each entry point to the company’s systems. Therefore, “Implementing an intrusion detection system” is a viable project that is supported fully by the company. Given the rise I cybersecurity threats and data theft, Bidea needs to guard their systems and network. The only method is to have an intrusion detection scheme that is tested and functioning. The detector can prevent invasion of the system and inform the appropriate people to take action. Thus, the project is interesting as it is the hope of everyone to keep hackers and intruders away from their establishment's systems and network. Thus, as the cyber threat increases every day in the modern society, Bidea is looking forward to having a fully functional "intrusion detection system" that would help the company protect the client's data and become competitive in the market where systems security is extremely valued. The company needs an intrusion detection system that would monitor both inside and outside intrusion.

Current Project Environment

The current project environment is on a medium business called Bidea that deals with travel and tourism. The company runs two different management systems to ensure efficiency is service delivery. The company has a comprehensive disaster recovery plan and a site where there is the company's parallel infrastructure. The system, servers, and the network are the backbones and the basic weapons used by Bidea to offer services to its clients. The system allows the registration of new members, keeps the information in the database and then release the information back to the user upon request. The system offers opportunities to both sellers and buyers. Normally, the buyer login the system to look for items to purchase while the sellers access the system to upload their items on sale. The system is therefore busy all times as it provides the said services. The company's servers run on windows server.

Therefore, the project requires all windows server supporting applications to guarantee the success of the project and finally provide adequate security to the system. The project is being implemented in an environment where every person wants to understand how to protect systems and data in this digital era. Thus, the available environment is supportive and encouraging. The system is aimed at providing intrusion detection mechanism such that whenever an intruder attempts to gain unauthorized access, the detector can alert the persons responsible for helping thwart such an attempt. Everybody in the technology field acknowledges that the cyber threat has increased and therefore improving intrusion detection mechanism is fundamental for any business to survive and retain its good reputation by safeguarding client's information. Bidea is, therefore, implementing the system in the appropriate time and in an environment with all system infrastructure that is required to run or install IDS.

Methodology

The steps formulated to realize projects success is important and crucial. In this project, five steps will be followed to ensure appropriate completion of the project. Beside the steps, the implementation of intrusion detection system will utilize parallel conversion methodology.

1. Keep vendor accountable with needs document.

The vendor is a key stakeholder in the system implementation strategy. The needs document ensures that the new system remains within the scope and can be a reference point.

2. Control the scope

The range of the task will be observed so that there’s no deviation, or performing tasks or adding skills that aren’t in the requirements.

3. Assign realistic teams to drive software implementation plans

The teams responsible for the project would be assembled based on their abilities. The persons to be comprised in the team would be chosen by the unique necessities of the task and the level of implementation.

4. Generate user adoption with a proactive, engaging strategy

Strategies will be developed to encourage user adoption and acceptance of the new technology. Therefore, there will be positive engagement around the product.

5. Develop a prototype

The prototype is an application that performs some basic functions expected in the whole system once it is completed. The system prototype will give insights on how the complete system may function.

6. Focusing on constant improvement

“Intrusion detection system” requires regular improvement because the hackers and intruders establish new ways of accessing whatever they want regularly. Therefore, the improvements will always be done after the implementation.

7. Implementation and testing

The running and testing of the system would be the last step of the process. After testing, the system would be kept by the company for two years.

Project Goals, Objectives, and Deliverables

The aims and purposes of the task are to provide a secure digital platform where people can interact freely and where businesses can securely keep the client’s data without the fear of being stolen.

Goals

1. Thwart unauthorized people from accessing the system:

Technology has changed everything across the world, and therefore, hackers have used that advantage to access systems without authorization. The goal of the project is to keep hackers away from the network or system

2. Protect businesses: Businesses rely heavily on reputation to make profits.

When client information is stolen and shared by malicious people, the company can easily collapse. The intrusion detection scheme will ensure that such attempts are monitored and appropriate action taken.

Objectives

1. Provide a strong intrusion detection system

One of Bidea company's objective is to get an IDS that would help safeguard data and information from unauthorized access.

2. Provide secure passwords

The IDS will ensure that passwords are encrypted, and nobody can really understand them easily. The IDS will detect and deter any suspicious system access.

3. Safeguard data

The main reason why Bidea is implementing IDS is to ensure that information is not accessed by malicious people.

4. Cover all functionalities and client needs in the system to guard the network:

The IDS will have to protect all forms of data and information kept in the database. The database will have an IDS as a monitoring tool.

Goals, Objectives, and Deliverables Table

	Goal	Supporting objective	Deliverables enabling the project objectives
1.	Thwart unauthorized people from accessing the system	1.a. Provide a strong intrusion detection system	1.a.i. Establish accurately alert
			1.a. ii. Create a procedure for handling any form of intrusion
			1.a. iii. Give a user guide or documentation of the system 1.a. iv. Purchase the necessary applications
		1.b. Provide strong passwords and safeguard data	1.b.i. Assign the appropriate officer to handle intrusion
			1.b. ii. Monitor the system always

			1.b.iii. Identify unauthorized access or attempts
2	Protect the business	2.a. Address all functionalities and client needs to guard the network	2.a.i. Conduct comprehensive system testing to confirm that requirements are covered
			2.a. ii. Attempt intruding the system and observe the system's reaction
		2.b. Remain competitive in the marketplace	2.b.i. Determine the cause of customer reduction
			2.b. ii. Invest in marketing

			2.b.iii. Design a comprehensive registration procedure

Goals, Objectives, and Deliverables Descriptions

Goals

Thwarting unauthorized people from accessing the system means that the intrusion detection system will only allow authorized access to get into the system. Protecting business is indeed the obligation of the system to guarantee that the corporate data is secure and no one can tamper with it. Providing a strong intrusion detection system is an objective that the company implementing the system will be proud of. The strength of the system will be important in this endeavor to protect data and information. The developers will cover all functionalities and client needs to guard the network. This will ensure that the business is comfortable to use the system and feel protected.

Objectives

The objectives clearly support the goals because for the system to stop intrusion it must be strong enough. Again, to protect the business, the system must include all client's requirements hence the objectives supporting the goals of the project. The objectives of the IDS implementation at Bidea support the goals. The objectives stated in the table when realized the project will be considered successful.

Deliverables

The deliverables of the project include intrusion prevention and secure network that can be measured using system penetration tests. When penetration tests return positive results, the project is successful. The IDS must give an accurate alert when an attempt is made to invade the system without authority. Since the project is required to stop unauthorized access, the system must be strong to achieve that. Therefore, during the testing, the system must provide accurate outcomes like the alert to guarantee that the goals objectives and deliverables are realized. There will be a purchase of the applicable and appropriate applications to install in the intrusion system that would be tested against the requirements as described in the agreement between the contracted company and Bidea.

Project Timeline with Milestones

“Milestone or deliverable."	“Duration (hours or days)”	“Projected start date."	“Anticipated end date."
Requirements	2 days	17 November 2018	19 November 2018
Prototype	1 day	20 November 2018	20th November 2018
Development	3days	21st November 2018	23rd November 2018
Implementation	2days	24th November 2018	26th November 2018
Testing	1 day	27th November 2018	28th November 2018

Outcome

The project is expected to provide a system that can protect the company's network, applications, and data. The implementation of "the intrusion detection system" is supposed to alert the appropriate persons in the company to take action whenever an intruder is detected. The detection system, therefore, will provide adequate security for the company's systems and applications. The system will be tested and the possible scenarios created to assess its efficiency and response using system penetration testing tools.

Measurable metrics and description

measurable metric	measurement	Description
Intrusion prevention or prevention of unauthorized access to the systems	Conducting comprehensive penetration test	a) Metasploit as a tool will show the strength of the IDS. b) Nmap will show the vulnerabilities within the network if any.
Secured internet/ network	Scanning both cabled and wireless network	Aircrack-ng will scan packets in the company's network to observe the kind of packets passing through the implemented IDS. If all packets are secure, then the project is successful.

References

Adami, D. (2011). Design, Implementation, and Validation of a Self-Learning Intrusion Detection System. Retrieved November 9, 2018, from https://pdfs.semanticscholar.org/aeb7/9322ae011e07fb3ccb12acb3df2beaa1dea2.pdf

Bonner, M. (2013, August 26). Beware the Risks of Cyber Attacks. Retrieved November 9, 2018, from https://www.thebalancesmb.com/dangers-of-cyber-attacks-462537

Conner, B. (2018, May 22). Real-Time Cyber Threat Intelligence Is More Critical Than Ever. Retrieved November 9, 2018, from https://www.forbes.com/sites/forbestechcouncil/2018/05/22/real-time-cyber-threat-intelligence-is-more-critical-than-ever/#688309c617fb

Corsini, J. (2009). Analysis and evaluation of network intrusion detection methods to uncover data theft. Retrieved November 10, 2018, from https://pdfs.semanticscholar.org/5c90/70dd7b116dd00f24956ca76c54f232c3084d.pdf

Hoque, M. S., & Mukit, M. A. (2012). An implementation of intrusion detection system using genetic algorithm. Retrieved November 9, 2018, from https://arxiv.org/ftp/arxiv/papers/1204/1204.1336.pdf

Kashyap, S., Agrawal, P., & Pandey, V. (2012). Importance of Intrusion Detection System with its Different approaches | Open Access Journals. Retrieved November 9, 2018, from http://www.rroij.com/open-access/importance-of-intrusion-detection-system-withits-different-approaches.php?aid=41367

Khem, D. (2011). Intrusion Detection Systems. Retrieved November 10, 2018, from https://www.cse.iitb.ac.in/~nirav06/i/IDS_Report.pdf

Shinder, D. (2005, July 13). News, Tips, and Advice for Technology Professionals - TechRepublic. Retrieved November 9, 2018, from https://www.techrepublic.com/article/solutionbase-understanding-how-an-intrusion-detection-system-ids-works/

Appendix A

The problem identified

The modern technology is indeed running the globe. This is the reason those companies that failed to adopt technology establish their means to extinction. The difficulty is that the much there's an innovation in the technology, the further technological criminality increases. For instance, cyber-attacks are indeed among the causes why many firms have encountered loses in the procedure of managing their business.

Appendix B

IT solution to the problem

To prevent intrusion, the solution is to implement “an intrusion detection system IDS” to inspect all outbound and inbound network activity and identify suspicious patterns that could indicate a system or network attack from somebody trying to compromise or enter into a system. Intrusion detection functions by collecting data and then scrutinizing it for unsuitable occurrences. An information technology administrator then uses the data to undertake future protection measures and establish improvements to network security.

Appendix C

Signature detection as a solution

The signature detection may be referred to as misuse detection. It attempts to identify the activities that suggest a system abuse. It is realized by creating intrusions models. The incoming actions are matched with the models of intrusion for decision and detection. The simplest method of signature restructuring utilizes simple patterns equivalent to compare the packets of the network against second signatures of recognized attacks.

Appendix D

Anomaly detection as a solution

The model comprises of a pool or “database” of anomalies. Any action that is noticed within the database may be referred to an anomaly. However, any drift from ordinary utilization is regarded as an attack. An intrusion in the network is a kind of attack that originates from exterior the local area network, normally through the internet. Systems for intrusion detection are important fundamentals in any security plan for the network. Some organizations rely on the firewalls for intrusion detection, and key firewall developers are creating some intrusion prevention and detection elements into the product.