Volume - 5, Issue- 5, May 2017 IC Value : 56.46 e-ISSN : 2347 - 9671| p- ISSN : 2349 - 0187

EPRA International Journal of Economic and Business Review SJIF Impact Factor(2016) : 6.484
ISI Impact Factor (2013): 1.259 (UAE)

Research Paper

www.eprawisdom.com

DOES HEALTHCARE INFORMATION SECURITY IS ANY MAJOR CONCERN IN MANAGERIAL DECISION MAKING

Mahesh Ramakrishna Pillai[1]

[1]*Faculty in Management, College of Business Administration, American University in the Emirates, Dubai. UAE*

Ann Kavitha Mathew[2]

[2]*Faculty, Health Management, School of Medical Education, Mahatma Gandhi University. S.India.*

Prabish Rajendran[3]

[3]*Network Manager, American University in the Emirates, Dubai. UAE*

ABSTRACT

Electronic patient records have become a vital source if information in health care industry for the last two – three decades. In the recent times, it has placed the whole medical system into a condition complete chaos and confusion, when the electronic records are never available or accessible or even accessible unauthorized persons finally reaching to the level of declining in the quality of patient care. To complicate the concern, healthcare industry needs to keep the information related to the patient and diseases as confidential as possible as per the governmental regulations. When compared to any manufacturing concerns, the traditional network troubleshooting and security efforts in any healthcare industry demand vast amounts of time and resources. This is because IT team must manually scan through logs, manage a multitude of host agents and perform frequent signature updates. In addition to this, the governmental regulations enable very strict policy guidelines in this regard, in introducing any changes to the system utilized in healthcare. It is very difficult resolve the infected systems in healthcare organizations as well in other industries, making more proactive, automated security measures even more crucial.

KEYWORDS: *health care, host agents, , automated security, IT team, network system*

INTRODUCTION

Electronic patient records have become a vital source if information in health care industry for the last two – three decades. In the recent times, it has placed the whole medical system into a condition complete chaos and confusion, when the electronic records are never available or accessible or even accessible unauthorized persons finally reaching to the level of declining in the quality of patient care. To complicate the concern, healthcare industry needs to keep the information related to the patient and diseases as confidential as possible as per the governmental regulations. When compared to any manufacturing concerns, the traditional network troubleshooting and security efforts in any healthcare industry demand vast amounts of time and resources. This is because IT team must manually scan through logs, manage a multitude of host agents and perform frequent signature updates. In addition to this, the governmental regulations enable very strict policy guidelines in this regard, in introducing any changes to the system utilized in healthcare. It is very difficult resolve the infected systems in healthcare organizations as well in other industries, making more proactive, automated security measures even more crucial.

To be in the business forefront, organizations need a secured and strong network system with proper security. The network security is authenticated, when the system enables itself to overcome any kinds of attacks, which may or can damage or even create loss of data to unauthorized destinations. During the last many decades, the utilization of internet oriented business has grown far and wide, creating an assumable importance to the network security. To develop, manage and maintain the data security and authenticity, the network needs to be properly secured from any kinds of attacks, on-line as well as offline. The network administrators need to have adequate information of every possible forms of intruder vandalism that can be committed possible options and network technologies.

Developing appropriate mitigation technique always have an impact on the network stability and performance, since different attacks have different manners. Efficient network administrators are always capable and competent to perform a risk factor analysis, which enables them to identify areas of appropriate protection, areas or possible threats and vulnerabilities that may emerge in due course. By doing a risk analysis network administrators will gather sufficient knowledge regarding potential and possible risks, which helps them to develop a high security network. Once the risk analysis is completed, it needs to design and develop a much appreciable high security network matching to the organizational need. The security protocols, give information for the network administrators and users in performing network auditing and proper utilization.

OBJECTIVES AND GOAL

The major objectives and goal for this study was to analyze the consequences of network attacks, in turn to develop a much-secured network against reconnaissance attacks. Further the study aims to perform risk analysis to recognize and categorize probable attack on individual or organizational assets, threats that are experiences, possible vulnerabilities that might happen as well to develop existing controls. Other objective aims to identify the need of security policies. This is aimed to recognize the best possible manners the security policies can be developed and designed based on the need of the security services and technologies.

RESEARCH METHODOLOGY

The methodology aims to identify the following related to the network systems namely: -

- Recognize different kinds and modes of network attacks,
- Conduct probable risk analysis,
- Design and develop different security policies.

Once the above basic requirements are identified, the network is developed based on a structured and suitable design, with regular monitoring and implementation plan. Network attacks are of various types. These attacks are planned and operated at different format and times, usually in stages. Usually the attacks are operated through reconnaissance attacks. Thus, it gains importance in the study. The focus of the study is to recognize the risk analysis, its importance and the methods of operation of risk analysis. The study again focuses on security policies, its role, as well as the design of the security policies to help security services and technologies. The study is carried out through a campus network. The network is scanned for reconnaissance attacks with and without the aid of security. The comparative results are utilized to for the mitigation of reconnaissance.

BACK GROUND

There are many studies that has been conducted on network features based on the attacks, risk analysis conducted as well as the individual security policies. This study is a compilation of various idea in this regard to develop a much-secured network. The attacks faced by the system networks are explained as methods to destabilize, or destroy or even to disrupt information system structure in any computer networks. The security attacks can at times be rectified or even mitigated, but can never eliminate it fully. It can never be possible to remove network attacks, without compromising network features. The study helps to find a method for mitigating reconnaissance attack possibilities. For the benefit of the study a campus network was designed. The network utilized Cisco switches and routers. To configure IPSec, VPN, Firewalls etc. Cisco Security Device Manager (SDM) was used. SDM - application used for the study – was utilised as a web-based device-management tool. The same was used in Cisco routers, aimed to develop possible outcomes from the network. In addition, the application helps to troubleshoot complex networking concerns.

Network Attacks and Mitigation : Networks are always expecting and experiencing various kinds of threats. It is the work of the network administrator to systematically analyze, critically evaluate and strategically solve the threats to a network system, whether it is hardware, software or the communication system.

The network attack occurs in different manners. At the beginning, only limited evidence of the attack will only be available to the administrator. The main objective of an attacker is to utilize all possible intelligence mechanism related to the target vulnerabilities. Once the information is gathered, the attacker designs a series of attack against the network. This is done by making an in-depth study of the security system and possible hacking points or loop holes. Basically, the attackers utilize the support of WHOIS aimed to access the IP address, domain name etc. of the organization, is never a concern for anyone. The available information is utilized on a later date to attack the system.

The attack on system network are usually mentioned as follows: -

- Attacks which need less information related to the target network
- Attacks which needs better information regarding the target network

Attacks that need intelligence network are grouped into

- Application layer attacks
- Threats to management protocols
- Worms, Viruses and Trojan horses

Attacks which need less information related to the target network

- Access attacks
- DoS and Distributed DoS attacks
- Reconnaissance attacks

The study explains all attacks and their mitigation strategies. More emphasis is given to reconnaissance attacks and the mitigation techniques.

Reconnaissance attacks : Reconnaissance attack is always explained as an unauthorized entry into the system and the mapping of the same, services, or vulnerabilities of a specific network. To attack the network, the intruder with gather information related to the target network namely active IP (Internet Protocol) addresses, the active ports and services in the IP addresses as well as the operating system platform. With this details, reconnaissance attackers gather all available information to attack the target network. Since there exists no impact on the network, the reconnaissance attackers remain hidden for a certain period.

Operation of reconnaissance attacks : Reconnaissance attack is considered as the first step for the network intruder. This is done with the gathering of the information related to the target network. The intruder conduct a ping sweep on the targeted network. This helps to obtain active IP addresses. As a second act, the intruder conducts port scans. This helps to determine active ports or services, which are active on the IP addresses. Once the live ports are identified, the attacker locates the system in operation, the type of application, and version, software utilized, as well as the configuration on the host target. Reconnaissance attack is used either as an effective administrative tool. Sometimes the same is used as an attacking tool. The various types of Reconnaissance attacks consist of Packet sniffers, Port scans, Ping sweeps as well as Internet information queries

Packet sniffer mitigation

Antisniffer tools : The presence of sniffers in any network is detected through various Antisniffer tools. This is designed through the utilization of software or hardware. Though these tools are effective to some extent, it is not at all possible to eliminate the threats completely. It functions as a sub-unit of the mitigation system. Antisniffer tools utilizes the “response time” method to identify the change of host. Response time is the time needed for processing the traffic system between the host and the server. The response time defines the traffic, which in another way detects the presence of sniffers. Many antisniffer tools like “Antisniff” is available in the market.

Authentication : Authentication means providing access to anyone to the network. Strong authentication is one of the basic to defend against any packet sniffers. OTP (One Time Password) is usually utilized as an strong authentication process. OTP, as name mentions is only for one time. OTP function as two-factor authentication, having a combination of new and old passwords. Since the password is valid only for few minutes, by the time the intruder understands the same, the password gets expired. Though this technique is valid for certain mitigation process, packet sniffers intended for sensitive datas (for example e-mail) still holds valid.

Cryptography: Cryptography is used to detect and prevent packet sniffers. This is basically the process of encrypting the data. The data that is captured will display only cipher text (random string of bits), making it difficult to understand. This is another best solution to prevent sniffers. Usually packet encryption is developed utilizing the following namely Data Encryption Standard (DES), or 3DES or at times Advanced Encryption Standard (AES) algorithms. The terminal access usually utilizes the protocols for cryptography like Secure Shell (SSH) and Sockets Layar (SSL).

Switched infrastructure

Switched infrastructure is considered as a regular technique mainly utilized as anti-packet sniffers. This is done by providing every device to have their's own switch port. Once there is a switched hacker based on the environment, they find it difficult to capture the packets travelling through associated network, while access is limited to designated ports. As this is the case, switched infrastructure will never eliminate the threat in full, but will be able to reduce the effect of impact.

Port Scans and Ping Sweeps

The main tools for scanning are Port scans and Ping sweeps for the regular type of reconnaissance attacks. This can very well be utilized for administrative purposes as well as for hacking purposes. This is utilized by Network administrator for identifying vulnerable services along the network.

Ping Sweep

Ping Sweeps are utilized by intruders to gain access to the IP addresses of active target networks. This is achieved by redirecting a ICMP ping to all the IP address along the target network or even by messaging a network ping. Multiple hosts will receive the ICMP ping, for which the active hosts might respond by echo reply. This is one of the older as well as slow techniques used to scan any network.

Port Scans

Port scan sends several messages to the target. Based on the response received, the intruder will gather information regarding, open ports, closed ports as well as service practices among hosts. Every service is assigned with a port number. For e.g.: - the port number for Simple Mail Transfer Protocol (SMTP) is allotted as 25. When port number 25 is recognized, intruder will have the information that the port is using SMTP. SAINT, Nmap, Nessus etc. remains as a very common tool for scanning.

Port Scans and Ping Sweeps Mitigation

It is never possible to completely prevent any of the port scans or even ping sweeps, since it is not a crime. The computer when connected to the network, the port gets opened, and will detect the port. With the help of mitigation techniques any damages that might happen to the system can be avoided.

By placing any filtering mechanism, port scans and ping sweeps can be stopped. The filtering device can be anything like “Firewall” or can be “Cisco router”. There arises the need for an access control list.

It is possible to mitigate port scans using Intrusion Prevention Systems (IPS). This can be done at the network as well as host levels. IPS will provide alert signals, in case of any attack. This helps the network administrator to be prepared to face the concerns.

Internet Information Queries

Internet information query is the method for obtaining information from the website or network sources. It provides details regarding domain and domain users. Domain Name System (DNS) is the most widely utilized database in the internet. The major activity of DNS is to convert human-readable domain name to a machine-readable IP address format. Intruders utilizes some internet tools like “WHOIS” for obtaining the data from internet. It is usually explained that organizations, while addressing information to a DNS, must utilize the information which never harm the system.

Access Attacks

Access attacks is explained as illegal entry into undesignated areas or regions. Usually this is done to retrieve information, gain entry, as well as to escalate the entry privileges across other networks and / or systems. The hackers utilize the technology to enter domains to gather confidential information, access web accounts as well to gather confidential or sensitive information. The attack usually happen in various ways, as follows: -

- Attack on passwords
- Exploitation and breach of trust
- Domain and Port redirection to different locations
- Man-in-the-middle attacks
- Buffer overflow

Attack on passwords

Hackers are very much matured to enter any domain by attacking the password authenticity. These are usually sensitive data, which can easily be manipulated by an experienced hacker. These hackers guess the password through system manipulation process. A series of attempts are carried out by the hacker. Dictionary attach is referred as a common example for password attack. Dictionary attack utilizes the technology to use all word combinations until it arrives at the final password. Usual methods of password attacks are the following, but is not limited to these alone. The common attacks are Brute-force attacks, Trojan horse programs, IP spoofing, Packet sniffers etc.

It is very important to protect the password security. Few observations in this regard are: -

- Do compromise not to share the passwords.
- Try using different passwords for different applications rather than one password for all applications.
- Try to change the password frequently.
- Always use characters, numerals etc. as part of password protection
- Try the very best to utilize best password sequence through using characters, numerals, upper case, lowercase letters, special characters etc.

Trust Exploitation

It is always a factor that network security is challenged by the connected network. Always a network administrator depends and trusts other networks in any system. Hackers always intrudes into this trust and gain access to devices to manipulate or access the data. This enables the hacker to do any mismanagement of the data leading to a collapse of the system. To mitigate the situation, it is essential to have protective constraints on trust levels within the network. It is always important not to completely trust systems both inside and outside the firewall. It needs to be limited to specific protocols.

Port redirection

Port redirection attack is another form of attack on trust exploitation. This attack enables to all the data packets to another secondary storage destination through the management of port redirection software. The common software are HTTP tunnel or NetCat etc. This attack never violates the system protocols. The administrator never feels an attack is happening at any time. At the same time, redirection hacker will identify the source, destination, communication process and purposes, user id/password, protocols etc. in the network. To mitigate from this attack, institutions must have good trust and faith in the network model. In the case of hosts who are trustable, based on IP addresses, port redirection can never be mitigated.

Man-in-the-middle attacks

This has developed as one of the best challenges to generate attacks in network security. MitM attack is explained as an attack by the intruder into the data performing either as a host or a recipient, without the knowledge of the others. For this attack, intruder obtain access to network packets available in the network. This is usually planned and implemented through network packet sniffers as well as routing and transport protocols. MitM attacks can be mitigated systematically, with the help of a cryptographic encryption. When it is an encrypted data, the intruder will observe only the cipher text, with the help of MitM attack.

Buffer overflow

This is another common format of network attack. This is the process of either overflowing or overloading the buffer in the allotted space. It is usually carried out by writing program to store data in a specific and separate memory. This happens when the program language is not adequately featured, namely C or C++. These languages seem to be not that memory-safe. The attack happens on all available network and propagate from one machine to another machine. To mitigate from the buffer flow, it is essential to have an up-to-date report regarding bug attack for all network application server products utilized. Another way is to check buffers on repeated intervals. When the buffer space has got more data, it is evident that there exists buffer overflow.

DoS (Denial of Service) Attacks

DoS attacks another form of security attacks. This kind of attack is one among the most difficult attacks. It is required to eliminate the same completely as they are never enabled to gain entry to any or all network information in the system. These attackers prevent legitimate persons from entering the system. Sometimes this will concentrate on the entire network and even prevent incoming / outgoing information. This attacks are carried out through Flood Attack, Ping of Death Attack and SYN Attack, to name a few.

Distributed DoS Attacks

A distributed DoS attack sends large volume of network requests, blocking the traffic. This process will delay the data transmission protocol, dramatically slows down the system. Hackers need only little effort as they take protocol weaknesses as advantage. It is found to be highly difficult to eliminate both these attacks. At the same time the damages can be minimized through Anti-spoof feature, Anti-DoS feature, Traffic rate limiting etc.

Attack from Viruses, Worms and Trojan horse

Virus: are considered as malicious software programs getting attached to a program or file. Once got attached, the program enable itself to destroy the specific area or the system or even the network itself. The virus gets activated as per the command and sometimes travel from system to system through the network. It will do soft as well as mild damages to the system network. Viruses spreads through network, sharing of files, documents, flash memories, e-mail attachments etc.

Worm: This is a sub-form of a virus. Worms also spread from system to system through network. It can even affect the entire network. Sometimes worms even engage in taking advantage to receive and send files from the computer.

Trojan horse: is a software which seems needed but once activated will destroy or kill the entire system. Trojan horse causes many serious problem to the system. These files never gets spread to another system, but kills the system in which it is infected, like cancer.

By utilizing effective anti-virus programs, the Viruses and Trojan horse attacks can be checked. It is always important to keep a check on the latest virus and anti-virus available to effectively control the attack. Every other day a new virus or Trojan is released. It is necessary to keep latest antivirus software to the maximum possible.

Application Layer Attacks

This is executed in various ways. The common methods of the application layer attack aim to exploit the major weaknesses of the system namely send mail, HTTP, FTP etc. This used to demonstrate either display screen, banner, prompt etc., with the support of usually Trojan horse programs etc. These kinds of attacks are oldest forms of application layer attacks. The latest form of application layer attacks enters the destinations through permitted firewall. Over a period, it is realized that the application layer attacks are not possible to be eliminated permanently. Because of this, new vulnerability is discovered daily basis.

Many measures are being taken on a regular basis, to avoid or even to reduce the risks of application layer attacks. Few measures include the following: -

- To take appropriate action after the review of the operating system, network log files etc and to take authentic actions.
- Keeping in the update lists that records vulnerabilities
- Introducing the latest patches to update the system.

Threats related to management protocols

In the regular practices, it is very much needed to have automated network management tools to handle systems beyond either single LAN or multilayer system. To handle the same, it needs to have a network management system. This needs to be developed from available network management protocols and applications. Simple Network Management Protocol (SNMP), SysLog, Trivial File Transfer Protocol (TFTP), Network Time Protocol (NTP) etc are considered as regularly used management protocols.

Methods for actual use of SNMP protocol

- Always enable read-only settings to configure SNMP.
- Provide security settings to maintain access control on devices managed via SNMP. This allows access by authorized persons.
- Better to utilize the new versions of SNMP as it can provide a combination which include encryption and authentication of protocols in the network.

SysLog Protocol: is developed to transmit information from devices that is developed for logging to a syslog server to gather information. Usually the responses are delivered as plaintext among managed device and host. Syslog never provides a provision for a packet-level integrity. This prevents the system from checking to make sure the quality of the contents that are either interrupted or transmitted. At times the intruder can alter syslog data to develop a confusion to the network administrator in case of any systems attack.

Methods for utilizing SysLog protocol

- Try to encrypt the syslog traffic through the help of an IPSec tunnel.
- While utilizing the system outside the perimeter, it needs to implement filtering mechanism through access control filtering.
- For allowing syslog data, it is necessary to implement ACLs to the firewall. This helps to develop a managed device which has the facility to arrive at the management hosts.

TFTP Protocol: is utilized for transmitting system files as well as configurations along the network. It is very important to generate the system files and configurations. This will help to protect the files because at times the whole network may get damaged creating a lot of information loss.

NTP protocol helps to synchronize the performance of various system devices along the system network. This is highly important to generate digital certificates. Further for right interpretation of activities along the syslog data. An intruder can attempt a DoS attack on any network security protocols. This can be done by sending illegal NTP data along the network. An intruder can always attempt to create trouble to the network administrator by attack and disrupting the various system configuration in the network

Methods for using NTP protocol

- Develop a organization oriented master clock on the basis of a private network synchronization.
- Always utilize the latest version of the NTP to help the cryptographic authentication mechanism within the hosts.
- Utilize the ACLs that may recommend devices along the network that permits to synchronize along with related networks.

RISK ANALYSIS

It is the process of identifying the risks related to any network or system. Further it is defined as the method of analyzing the probability of occurrence of the risk and its impact on the system. In addition to the same, the process enables to recognize the methods or procedures that is required to mitigate the impact of risk in the system.

Risk analysis has an important purpose while designing the network. Earlier the network engineers, never provided much better significance to risk analysis, while designing the network. Since this was the case, the network design at times brought huge financial and technical loses in addition to the time and effort wastage to organization, as the risk analysis part was never provided important. The time has significantly changed. Everyone in the network has all information regarding the risks that might happen in their respective portfolios, hence making it convenient for developing a system with better security. Now Risk analysis has emerged as a continuous process. The routine and repetitive risk analysis, helps to build attention to any specific risk or new risks that can appear anytime during the operation. Thus, it enables the organization to re-built the security system to improve the security of the network.

Risk is manageable once the same is recognized. Risk is always considered as a chance for the existence of an exploitation or a threat to a specific vulnerability. Risk analysis process, helps to identify the risk associated with any objective, which can bring in a loss to the organizational performance. Further enables us to understand about how, when, where what has happened. Risk analysis is carried out in different ways. The regular risk analysis methods are as follows:

- Identification and management of assets related to the organization
- Identification and management of threats faced by the organization
- Identification of different vulnerabilities that repeatedly happening
- Identification of existing control measures and its impact.

Identification and management of assets

Identification of specific assets in any organization is important as it defines the part of risk analysis required to be performed on the assets. In any industry, assets are not just the hardware, software or the networking. In any operational network the hardware assets includes board, monitor, processors, keyboard, device, mouse, cables terminals, drives, connections, controllers, network, switches, routers, hubs, fax, printers, output devices etc. Every device plays prominent place which needs protection in its own functions. The software program is differentiated as purchased programs, executable programs, systems programs, diagnostic programs, source programs, operating systems etc. Usually the threats are on the software as the same remains open to all including the hackers and intruders. Data or the information is another major asset. The entire network security is judged based on the data security and protection. The human capital is the biggest asset to the organization. Employee management and the skill in managing security and authenticity of data is very important to any organization. From the network side the assets usually include workstations, front-end processors, communication networks, data encryption tools, satellite connectivity, remote access security etc.

Identification and management of threats faced by the organization

Threat is always a belief of existence of any harm that can damage the system. Once the assets are recognized, the plan to protect the same arises. The existence of any threat can bring in more harm to any of the asset base. In a system network, threats are either intentionally or at times accidentally triggered. It needs to identify the threat whether accidental or intentional as the sources needs to be identified to develop a protected network.

A threat-source is explained as any specific event or at times any specific location which can cause harm for the network. Usually the threats that happen are natural, human, or environmental. Organizations needs to analyze all threat-source while developing a network. Once the threats are identified, enough precaution can be taken in case of need.

- Natural calamities that usually happens include earthquakes, floods, tsunami, hurricane, landslides, avalanches, thunder storms etc.

- Manmade threats occur due to actions or occurrence of events occurs due to human behavior, deliberate or unintentional behaviors.
- Environmental threats include, but not limited to long-term electrical breakdown, air / water pollutions, chemical misutilization, leakage, contamination etc.

Usually it is very convenient to recognize natural or environmental threats. It is very difficult to recognize human threats. Table 2.1 explains different human threat sources.

Identification of different vulnerabilities that repeatedly happening

This is explained as the flaw or weakness along the security procedures in any system. This might have happened due to design, system implementation, or its internal controls. This might have occurred either accidentally or intentionally resulting in any breach of security or even its violation. The existence of vulnerability can cause harm only when the same is exposed to some threat.

In case the vulnerability that is identified, can remain as no threat, but needs routine and repetitive monitoring for changes. The Assets in the system – hardware, software or network – remains as the main cause for vulnerabilities, which cause concerns when mutilated to develop any harm. Some sources of vulnerabilities are

- The institution / company itself
- The company procedures, practices and policies
- Functions of the management
- Skilled and unskilled human resources
- Organizational environment – physical and material
- The Information system management
- The system facilities namely hardware, software or networking equipment
- External resources and applications.

Identification of existing control measures and its impact.

Controls can be explained as a mechanism or method used to mitigate from vulnerabilities. It helps to detect and prevent vulnerabilities. It is important to identify existing controls to avoid unmeasurable work or expenses. Proper documentation usually help in exerting proper control processes and to plan for risk aversion. While assessing the control measures, it needs to make sure that the existing control measures are performing as per need. When control measures fail, usually alternate control measures are introduced to mitigate from the risk. Efficiency of all control processes are evaluated based on how the control process reduces the existence of threat, exploiting the vulnerability, as well reduces the impact of the incident.

Basic risk analysis process: -

The main Risk analysis is usually performed as follows: -

- Analysis of Qualitative risk
- Analysis of Quantitative risk

Qualitative risk analysis

This analysis determines the extend of protection that is required for assets in the system and its applications in the organization. This provides a concurrent analyzing of assets, threats, and performance vulnerabilities. Qualitative risk analysis is executed using a scale of factors that have the value to explain the level of existence of perineal consequences, in addition to the occurrence of those consequences. The method usually attempts to rate the risk elements, subjective to the scope and recognize the areas which needs development. It is very much needed to have the presence of a good data format as prerequisite to conduct risk analysis in qualitative conditions.

Quantitative risk analysis

In case of number or numerical data measure Quantitative risk analysis is utilized. This helps to identify the probability for the occurrence of vulnerabilities. It tries to review the threats and likelihood of losses that can occur. Since value is important, it is usually mathematically calculated. With the support of the numerals, overall risk can be assessed. If there is a lack of appropriate data for evaluating risk, quantitative risk analysis serves the purpose. The requirements of quantitative risk analysis are: -

- The asset valuation
- The cost on capital or asset
- The cost involved in asset management and protection
- The value for competition
- The cost of recovery.

The methods to identify the value of an asset by quantitative risk analysis are as follows:-

- Provide a cost / value to the asset
- Introduce the risk value to protect the asset
- Analyze the annual rate of occurrence (ARO)
- Give a single loss expectancy value (SLE)
- Introduce the annual loss expectancy (ALE)

SLE helps to detect the expected impact of any specific threat, through mathematical interpretations. ARO tries to explain the chances of occurrence of a threat during a time period. ALE is the product of SLE and ARO. Since the calculations are complex, it is very difficult to arrive at any specific conclusions at times. Further it depends on the availability and value of measures, used for the risk analyses.

SECURITY POLICY

The policies of Security define generally as a main set of practices for the technocrats who gain entry to an organization's technological abide. Thus, to organize proper and secured system network, it needs highly secured policies. The main purpose is to protect the organizational information from reaching intruders. The policy designs a road map for operation within the network. The officials will utilize the security policy for effective utilization of resources.

Need of a Proper Security policy

It is important to have a Security policy on record to help people to work accordingly: -

- Work as a baseline for current and concurrent operational protocol.
- Develop a framework for security implementation
- Explain and express permitted behavioral practices while utilizing the technology.
- Develop and utilize the required tools and practices.
- Develop code of conduct for security happenings and mishappenings.

The security policy explains the way to execute the security incidents. As an example, if the laptop utilized by an employee crashes, the policy clearly states to have a back-up of the data in the system to prevent any loss. Policies clearly mention the actions to be taken in case of violation of rules by employees. As an example, in a university network, the role of the students and lectures are defined. Students are not permitted to access few sites, while faculty has permission. This is defined by the security policy of the organization. While choosing, the security policy and protection protocol, it is always important to choose the best protocol as acceptable to the organization.

Need of a security policy

The security policy must be able to define: -

- What needs to be protected and why
- Who is responsible for what sort of information?
- Must be able to intrude in case of policy violation by any means or chance.

The important subjects that needs protection include intellectual information, individual information and institutional information.

Information protection needs: -

Information is the basic backbone of any organization, and the same must reach the right man at the right time for right decision. In case of any flow in the system, the same may reach the wrong person at the wrong time, creating the best of the worst that can ever happen to the organization. The transmission of the information must be carried out through specific passages and paths, ensuring the safe transfer of the data to reach the safe destinations. While transmitting the data proper data transmission protocol needs to be utilized, so that intruders are kept aside from obtaining the data.

Information infrastructure requirements: -

The best utilization of the appropriate hardware, software and networking always ensures security from loosing of the data to elsewhere. Hence it is a must to choose the best of the information processing infrastructure with all designated protection features. The complete security related to information dissemination widely depended to the best utilization of the available methodologies, in a much appropriate manner.

Timeliness of Information: -

Information must reach the right man at the right time from the right source, without undergoing any distortion. Enough protection to be taken to keep information transmission away from any kind of distortion.

Human Resources: -

Organizations can never work with individuals, rather can perform only in groups. The organizational policies usually classify people into diversified segments to obtain security. The policy manual clearly explains the responsibility and authority or people in the organization. Usually the top management will define the security policies. The responsible people are categorized as follows: -

- The users in the network
- The administrators and managers in the network
- The auditors of the network's usage
- The managers who maintain ownership related to the network and its resources

The major roles of security policy are ensuring the action in each case of security breach. For example, in case there exists a policy related to retired professionals who have no access to system, gains control, it is considered as breach of security. Once this policy fails, unauthorized access is reported, causing damage to the organization, through information leakage. In such a situation, actions need to be taken guarantee information protection.

Mechanism for proper Security services: -

To enable better decision making, w.r.t security, the organization must specify the security goals of their establishment. Security service is an activity enabled to protect the system from any kinds of intruder's attack, destroying the data in due course. This is thus explained as a technology, utilised to provide security service. Depending upon the nature of the support needed the security policy will be developed. This is divided into five categories

- Authentication of person / institution
- Access control limited / or unlimited
- Confidentiality – through passwords
- Integrity of data utilization
- Non-repudiation of data / resources.

This mechanisms is further divided as follows: -

- Access control
- Authentication
- Data integrity
- Digital signature
- Encryption

Security services

Authentication : Authentication examines the genuinity of the source. It is a guarantee that the information is from a reliable source. This is very much important for organization to achieve its objectives. The proper user name and password helps to verify the authenticity. Password is protected by encryption. Usually authentication is grouped based on Peer entity and Data origin.

Access control: Access is the method to make use of resources in any system. To protect the system from attack, the access to the system needs to be limited and genuine. Access Controlling the process of providing the entry to authorized personnel. This serves as a protection against the unauthorized utilization of resources by unauthorized personnel. This is achieved through the mechanism of password encryption.

Confidentiality: This is the promise that information never reaches the unauthorized sources or institutions. Confidential data need not reach unauthorized persons, as it may lead to collapse of the company. If not protected, the hackers aim to obtain information from an unsecured network. This service is give protection for all confidential information. With the help of data encryption, unauthorized users can never enter the network for data vandalism and damage. Confidentiality is usually maintained in terms of Connection confidentiality; Connectionless confidentiality, Selective field confidentiality and traffic-flow confidentiality

Integrity: Integrity gives us a promise that the information can never be updated by an encroacher through another system. The network system ensures high integrity of messages, when processed, as well as saved or transmitted. This helps us to validate that the data send is the data that is received. This service utilizes the usage of encryption as well as digital signature for integrity.

Non-repudiation: This is an act of denying the participation of any one or more users in a system. This is utilized to help the data from never reaching an unauthorized person or network. Non-repudiation is a promise that any person is not provided the chance to his participation. This mechanism too utilizes digital signature and data integrity mechanisms. This is usually of two kinds one with a proof of origin and the other with a proof of delivery

Security mechanisms

Encryption: is the major source related to cryptography. This is explained as the process of converting the plaintext to any unreadable format. This can be converted to readable form only by authorized personnel by the process of decryption. It converts the information to a meaningful format with the support of encryption process. This is a highly sophisticated process utilized to avoid hackers. Encryption is of two types namely Symmetric-key encryption as well as Public-key encryption

Digital signature: is utilized to verify the identity of the sender. Further it enables to findout the message is from original source and originality is maintained. This is a message integrity code, which is generated while signing through an algorithm (hash function). Sender sends the information along with his public access code while the receiver needs to generate his private access code. Once the same code can be established, the validity of the source is proved.

Data integrity: is the mechanisms to protect the data from getting corrupted, which can happen during the process of data recording. This is a process to verify the data accuracy, timeliness, and integrity. This ensures that the data has never gone through any kind of vandalism or sabotage, leading to unauthorized modifications from unauthorized sources. Most of the security service uses many to develop their own security policy. When at a time the authentication, mechanism is found useful, company will develop most appropriate authenticating tools. This will permit only authorized persons to access the data.

Security policies – Examples from the study.

Usually organizations develop a security policy based on its needs and requirements. Few common security policies developed and utilized by few organizations are explained below. This needs to be very clear and complete. Most of the policies that were looked upon had the following features while looked upon: -

- Purpose of Policy
- Persons needed / affected
- Policy details
- Enforcement / Implementation Process
- Responsibilities / delegation of authority.

Network access policy

Purpose: To provide access only to approved or authorized persons to the system and to prevent any unauthorized use of the system. This policy needs to be implemented completely.

Persons affected: Staff of the institution both administrative and non-administrative

Policy: All persons directly linked to the company will have access to the system through protected methods. People will gain entry to the system at each level where they are authorized to work. It is strictly prohibited from reveling the password or entry data to any unauthorized personnel. Employees gain privilege to enter certain range of data based on their position in the hierarchy.

Enforcement: Employees who are proved to violate the organizational policy must face disciplinary measures in accordance with the organizational standards.

Responsibilities: Each employee must protect his / her system from getting hacked or must prevent information leakage. IT Team must ensure that everyone is clear with their rules and policies in concurrence with the senior management decisions.

Password policy

Purpose: This policy ensures a rule and practice for developing a password and its usage. Further it states the methods to change the password at a frequent time frame.

Persons affected: All authorized participants in the system with access to the system management process.

Policy: Companies frame a policy about the development of the password, namely case sensitive, inclusion of numerals, alpha-numerals, characters, length of the password, minimum numner of characters, avoid using login name etc. In addition, it usually states not to place it in writing at any places.

Once the password is stored, employees will be highly recommended never to use the same password for various processes. It is advised that

- Not to reveal password to anyone over phone or SMS or by e-mail or in any written format.
- Never reveal the password to anyone, in case of need, do type it for him.
- Never discuss about password while in a common place.
- Never give hint of the password format.
- Never write in down anywhere, in case, it was required to share the password, do change the password immediately.

It is highly recommended to change the password, on a regular basis.

Enforcement: Employees violating the policy must face disciplinary action as per the law of the company.

Responsibilities: It is the responsibility of the employee to protect the password and to make the routine update. In case the password is found to be corrupt, the IT must be immediately called for to block from any misappropriate usage.

RECOMMENDATIONS

This chapter explains the methods to implement of the selected configurations to any campus network. In addition, it helps to understand the mitigation from the reconnaissance attacks, using firewalls. The scanning of the network is conducted using Wireshark and Nmap, with and without security features. A comparative study of the results were conducted to arrive at the findings.

Design for the Network

The campus network design (Figure 5.1) shows the connections to and from ISP router and Host routers.

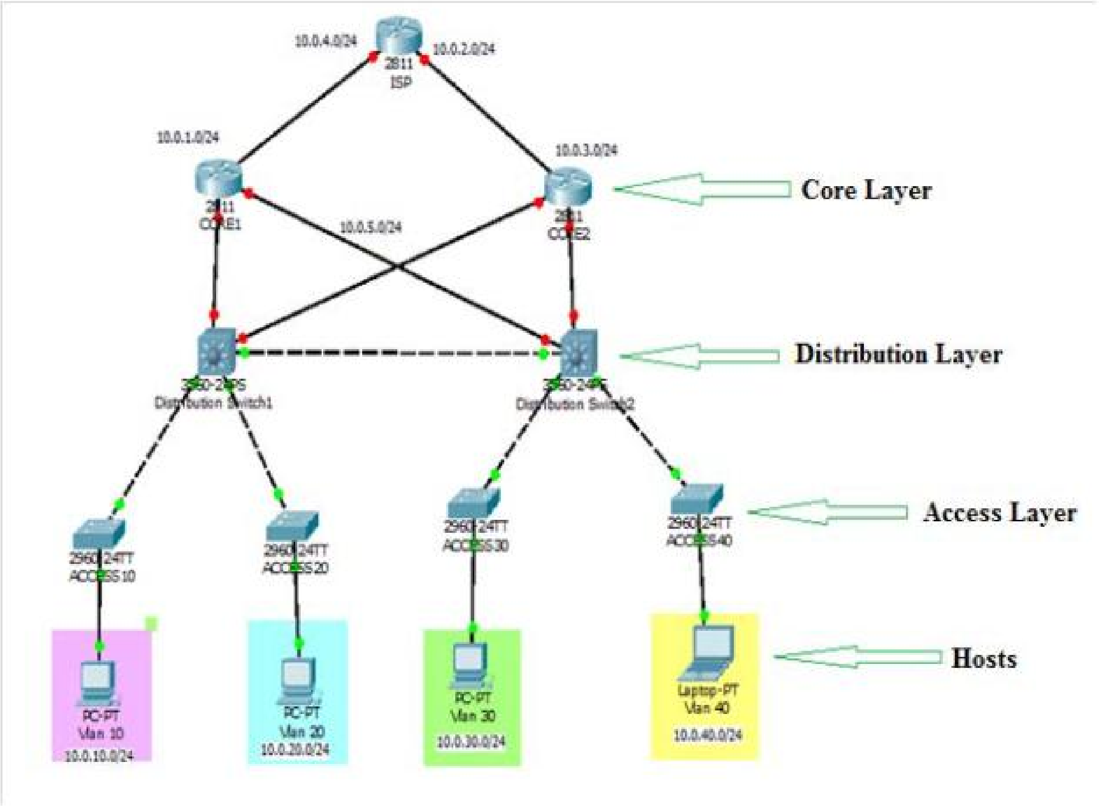


Figure 1.1: Design for a Campus Network

Packet Sniffing Mitigation

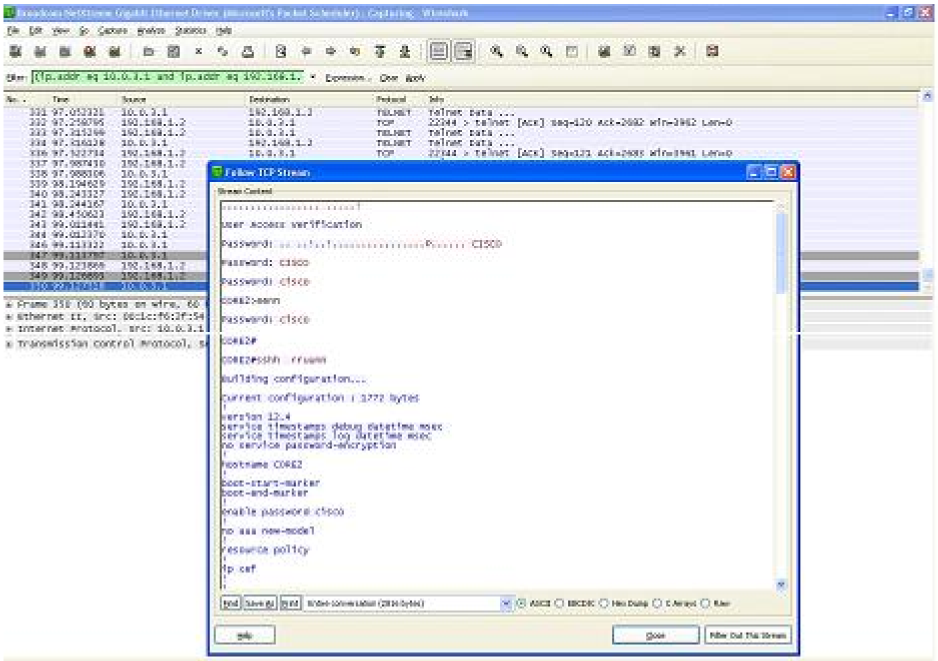
Packet sniffing captures information in any plain text. The main function is aimed to make sure that the data passing from router to router. The data needs to be protected as there is enough chances from hackers. To prevent the hackers, Virtual Private Network (VPN) is established, to provide a private passage, much away from the public access.

The design is developed in a private setting. The same, once connected along the router are sniffed by the windows packet sniffing tool Wireshark. This is done on a routine basis. The comparative results are analyzed as and when deemed fit. Once the VPN is set, it is necessary to verify the IPSec works, which is a framework of open standards. This provides authentication, integrity, confidentiality and access control for IP traffic. This helps the traffic to remains secure in the transmission.

To analyse the mitigation of packet sniffing, it is necessary to telnet to router CORE2 from router to CORE1. Data is transmitted in a plain text, for the attacker to gather the data easily. This helps to explain the details of data to be sniffed earlier to encryption.

Results

From the figure, it is very evident that plain text of data is captured by an intruder.


File Edit View Go Capture Analyze Statistics Help
Filter: (ip.addr eq 10.0.3.1 and ip.addr eq 192.168.1.
Expression... Clear Apply
Follow TCP Stream
Stream Content
Find Save As Print
ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ○ Raw
Help
Close
Filter Out This Stream

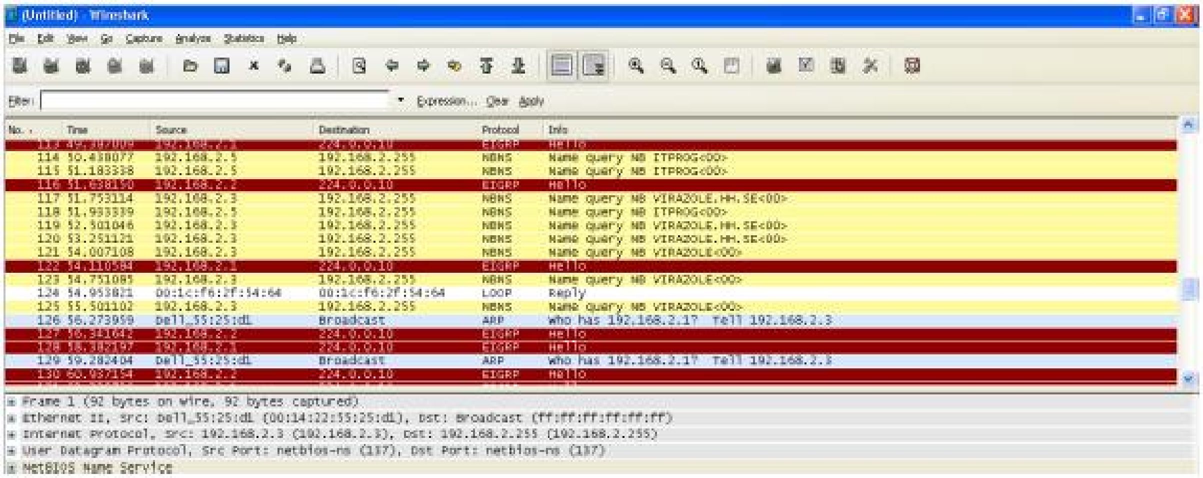
```
No. .  Time          Source        Destination   Protocol  Info
331 97.052321  10.0.3.1     192.168.1.2   TELNET   Telnet Data ...
332 97.258795  192.168.1.2  10.0.3.1      TCP      22244 > telnet [ACK] Seq=120 Ack=2602 Win=3962 Len=0
333 97.315299  192.168.1.2  10.0.3.1      TELNET   Telnet Data ...
334 97.316128  10.0.3.1     192.168.1.2   TELNET   Telnet Data ...
336 97.522734  192.168.1.2  10.0.3.1      TCP      22244 > telnet [ACK] Seq=121 Ack=2605 Win=3961 Len=0
337 97.987410  192.168.1.2
338 97.988106  10.0.3.1
339 98.194629  192.168.1.2
340 98.243327  192.168.1.2
341 98.244167  10.0.3.1
342 98.450623  192.168.1.2
343 99.011441  192.168.1.2
344 99.012370  10.0.3.1
346 99.113322  10.0.3.1
347 99.113797  10.0.3.1
348 99.123869  192.168.1.2
349 99.126899  192.168.1.2
350 [illegible]  10.0.3.1
⊞ Frame 350 (60 bytes on wire, 60
⊞ Ethernet II, Src: 00:1c:f6:2f:54
⊞ Internet Protocol, Src: 10.0.3.1
⊞ Transmission Control Protocol, S
```

```
......................!

User Access Verification

Password: ...........................P...... CISCO

Password: cisco

Password: cisco

CORE2>enn

Password: cisco

CORE2#

CORE2#shh  run

Building configuration...

Current configuration : 1772 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname CORE2
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
no aaa new-model
!
resource policy
!
ip cef
!
!
```

```
Entire conversation (2836 bytes)
```

Figure 1.2 Sniffing data across the network using Wireshark without security

Upon encrypting the events, the intruder was not able to gather the initial data. The data captures were not recognizable, where the attacker is left with no clue of the information being transmitted along the network.


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

```
No. .  Time          Source              Destination         Protocol  Info
113 49.397009  192.168.2.1        224.0.0.10          EIGRP     Hello
114 50.438077  192.168.2.5        192.168.2.255       NBNS      Name query NB ITPROG<00>
115 51.183338  192.168.2.5        192.168.2.255       NBNS      Name query NB ITPROG<00>
116 51.638150  192.168.2.2        224.0.0.10          EIGRP     Hello
117 51.753114  192.168.2.3        192.168.2.255       NBNS      Name query NB VIRAZOLE.HH.SE<00>
118 51.933339  192.168.2.5        192.168.2.255       NBNS      Name query NB ITPROG<00>
119 52.501046  192.168.2.3        192.168.2.255       NBNS      Name query NB VIRAZOLE.HH.SE<00>
120 53.251121  192.168.2.3        192.168.2.255       NBNS      Name query NB VIRAZOLE.HH.SE<00>
121 54.007108  192.168.2.3        192.168.2.255       NBNS      Name query NB VIRAZOLE<00>
122 54.110584  192.168.2.1        224.0.0.10          EIGRP     Hello
123 54.751085  192.168.2.3        192.168.2.255       NBNS      Name query NB VIRAZOLE<00>
124 54.953821  00:1c:f6:2f:54:64  00:1c:f6:2f:54:64   LOOP      Reply
125 55.501102  192.168.2.3        192.168.2.255       NBNS      Name query NB VIRAZOLE<00>
126 56.273959  Dell_55:25:d1      Broadcast           ARP       Who has 192.168.2.1?  Tell 192.168.2.3
127 56.341642  192.168.2.2        224.0.0.10          EIGRP     Hello
128 58.882197  192.168.2.1        224.0.0.10          EIGRP     Hello
129 59.282404  Dell_55:25:d1      Broadcast           ARP       Who has 192.168.2.1?  Tell 192.168.2.3
130 60.937154  192.168.2.2        224.0.0.10          EIGRP     Hello
⊞ Frame 1 (92 bytes on wire, 92 bytes captured)
⊞ Ethernet II, Src: Dell_55:25:d1 (00:14:22:55:25:d1), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol, Src: 192.168.2.3 (192.168.2.3), Dst: 192.168.2.255 (192.168.2.255)
⊞ User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbios-ns (137)
⊞ NetBIOS Name Service
```

Figure 1.3 Sniffing data across the network using Wireshark with security

Mitigation through Ping Sweeps.

Through the scanning tool of ping sweep, the attacker, obtains all alive IP addresses along one network. This is done by transmitting ICMP ping to several IP addresses. Upon receipt of the ICPM echo replay, it establishes that the IP address is active. By turning off the ICMP and ICMP echo replay process can mitigate through ping sweeps.

The next stage explains the mitigation process of ping sweep through CBACS (Content Based Access Control Lists). This is a firewall process without turning off the ICMP echo replay. When CBACS is established in a router, the data is inspected, as well as generated from inside to reach outside network.

This demonstration, explains the users from CORE1 can ping the CORE2 router. At the same time, users form CORE2 con not ping CORE1. Intruders of the two routers will find it difficult to access the IP address of the CORE1 since CBACS prevents data than the data of CORE1. (Appendix E)

Outcomes: -

The following were the outcomes. While examining the details, it is obvious that CORE1 can ping as well telnet the CORE2. At the same time CORE2 when tried to ping CORE1, ended unsuccessful.

Mitigation for Port Scans

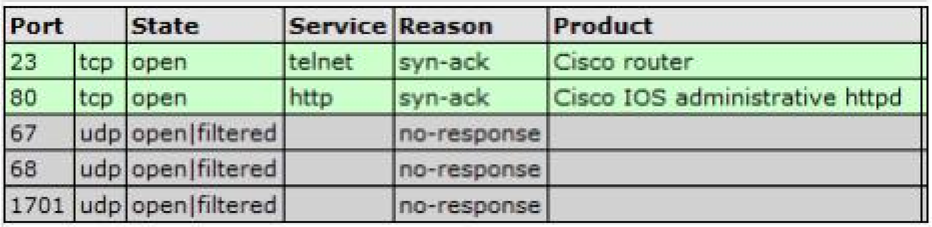
This permits the attacker to identify ports and services which are open as well as ports that are active with live IP address. An attacker can utilize the data for port scanning, thus making an actual attack on the target. Thus, it becomes very much needed to mitigate the actions. Thus, by using Cisco ISO Firewall, it is possible to mitigate the port scanning.

In this stage, it enables to prevent router CORE1 attack, thus stopping intruder from executing the port scanning attack as well to obtain the network details. The router CORE1 which is configured with Cisco IOS Firewall and Access list using Cisco Security Device Manager (SDM). This ensures the availability of the network and its security against any network attacks.

From the following example, the information transmitted through CORE1 router is scanned. This is done through the support of Nmap, which is an open source utilised for the purpose of security auditing and network exploration. This is aimed to find open ports. The scanning is done repeatedly. The results are analyzed to arrive at the results.

Outcome

Outcome of scanning of CORE1 router without security.



Port		State	Service	Reason	Product
23	tcp	open	telnet	syn-ack	Cisco router
80	tcp	open	http	syn-ack	Cisco IOS administrative httpd
67	udp	open|filtered		no-response	
68	udp	open|filtered		no-response	
1701	udp	open|filtered		no-response	

The Figure explains that on observing the ports that are open and the services. This is utilizing the open port facilities. Thus, it explains the reasons for open ports and the product in the device. Once the Firewall is configured, the results of the scan at times never display the information regarding the ports, like it is open / closed. This explains that the ports are protected by the security namely Firewall.

Internet Information Queries Mitigation

This helps to obtain details w.r.t any website or any establishments. The main source of information is DNS. Upon obtaining the domain name and IP address, the attacker can plan the action. For this purpose, WHOIS is used to enquire the website 'aue.ae' and results were verified.

Outcome

The following table shows the result of WHOIS for aue.ae

```
Domain Name    :         aue.ae
Registrar ID   :         Etisalat
Registrar Name :         Etisalat
Status         :         ok
Registrant Contact ID               :         ETSLT147199-R
Registrant Contact Name  :          American University in the Emirates
Registrant Contact Email :          Visit whois.aeda.ae for Web based WhoIs
Registrant Contact Organisation     :         American University

Tech Contact ID  :         ETSLT342515-C
Tech Contact Name          :          American University in the Emirates
Tech Contact Email         :          Visit whois.aeda.ae for Web based WhoIs
Tech Contact Organisation:            American University

Name Server    :         ns0.aue.ae
Name Server    :         ns1.aue.ae
Name Server    :         ns2.aue.ae
Name Server    :         ns3.aue.ae
Name Server    :         ns4.aue.ae
```

The information above explains intruder can perform the attack. There exist no mitigation techniques for this plan. It is revealed that while providing the information to DNS only limited or required information need only be provided to avoid any harm on a later stage.

CONCLUSION

The research was conducted to recognize a way a network security can be designed and developed. Most of the possible attacks that were identified along the network were explained. Various mitigation techniques were identified to evolve a system to avert the attacks. The study further was conducted to find the various methods to perform risk analysis. The possible two ways were discussed as part of the study. The study aimed to discuss and design some of the security policies which are very much appropriate to achieve organizational goals. The basic objective of the study was arrived at which enabled to design a technique for the mitigation of reconnaissance attacks.

It needs to be concluded that the complete network protection is not possible unless a compromise on few features of the network is carried out. There exists a gap for a future expansion from the scope of the study enabling a much-advanced security network protocol. Thus, healthcare industry like any other industry needs to confirm that there exists a much-valued interest in protecting the information security and confidentiality of the medical – electronic data as it deems fit as a valuable source of information for even any nation's healthcare economic scenario.

REFERENCES

1. *Angela Orebaugh and Becky Pinkard, "Nmap in the Enterprise: Your Guide to Network Scanning" Syngress Publishing, Inc, January 2008.*
2. *Chris Jackson, Network Security Auditing Tools and Techniques, 29 Jan 2010*
3. *Dieter Gollmann, "Computer Security", Wiley, 1999*
4. *Duane De Capite, "Self-Defending Networks: The Next Generation of Network Security", Cisco Systems, Inc., September 2006.*
5. *Eric Cole, Network Security Bible, Wiley, 08 Sept 2009*
6. *Gary Stonebumer, Alice Goguen, and Alexis Feringa, "Risk Management Guide for Information Technology Systems", Recommendations of the National Institute of Standards and Technology, July 2002.*
7. *International std BS ISO/IEC 27005-2008, "Information technology- Security techniques- Information security risk management" First edition, June 2008.*
8. *ISO/IEC 17799:2005 – Code of practice for information security management available at:http://www.iso.org/iso/support/faqs/faqs_widely_used_standards/widely_used_standards_other/in formation_security.htm*
9. *Jayant Gadge and Anish Anand Patil, "Port Scan Detection", IEEE Xplore, November 2008.*
10. *Joshua Backfield, John Bambenek, "Network Security Model", SANS Institute, 2008*
11. *Manuel Mogollon, "Cryptography and Security Services: Mechanisms and applications", Cybertech Publishing, New York, 2007*
12. *Michael E. Whitman and Herbert J. Mattord, "Principle of Information Security", 2nd edition, Thomson Course Technology, 2005*
13. *Richard A. Dea, "Cisco Router Firewall Security" Cisco Press, August 2004.*
14. *Sabeel Ansari, Rajeev S.G and Chandrashekar H.S., "Packet Sniffing: A Brief Introduction" IEEE Xplore, December 2002/January 2003.*
15. *Sigurjon Thor Arnason and Keith D. Willett, "How to Achieve 27001 Certification", Published by CRC Press, 2007*
16. *Susan Snedaker, IT security Handbook, 20 May 2006*
17. *The standard of good practice available at: https://www.isfsecuritystandard.com*
18. *IT management – BS 7799 available at: http://www.tech-faq.com/bs7799.shtml*

Introduction to ISO 27001 available at: http://www.isoqar.ir/html/iso_27001.html