Scientific Research Publishing

Communications and Network, 2017, 9, 275-290
http://www.scirp.org/journal/cn
ISSN Online: 1947-3826
ISSN Print: 1949-2421

Practical Approaches to Securing an IT Environment

Emmanuel S. Kolawole, Warsame H. Ali, Cofie Penrose, John C. Fuller

Department of Electrical and Computer Engineering, Prairie View Texas A&M University, Prairie View, TX, USA
Email: ekolawole@student.pvamu.edu, whali@pvamu.edu, pscofie@pvamu.edu, jhfuller@pvamu.edu

How to cite this paper: Kolawole, E.S., Ali, W.H., Penrose, C. and Fuller, J.C. (2017) Practical Approaches to Securing an IT Environment. *Communications and Network*, **9**, 275-290.
https://doi.org/10.4236/cn.2017.94019

Received: May 7, 2017
Accepted: November 27, 2017
Published: November 30, 2017

Abstract

There are a number of IT Security journals available in the literature but none of these research papers have practically specified approaches to secure the IT environment at large. In this paper, more emphases will be laid on the practical ways to secure our IT environments and with some useful real-life scenarios. In today, securing our IT environment has become the key factor in the industry due to an increasing number of attackers invading and stealing the intellectual properties; thereby, rendering most IT industries to go out of businesses. They may find that understanding and translating IT security recommendations to implementable practices can be overwhelming. While this is a worthwhile and important task, there are also more practical ways to ensure you are using IT security best practices in your business. Therefore, the need to properly secure our IT environments in order to mitigate those attacks by using the right tools in all IT domains will be fully discussed in this research. This paper will focus more on protection of LAN-WAN Domain as a use case.

Keywords

Security, Environment, Domains, Intellectual Property, Attacks, Mitigation and Assessment

1. Introduction

In today's age of technological advancement and interconnectivity, network security has become more important to personal computer users and any organizations at large. With the advent of the internet, security became a major concern and the history of security allows a better understanding of the emergence of security technology. The internet structure itself allowed for many security threats to occur. The architecture of the internet when modified can reduce the

possible attacks that can be sent across the network. From my research, I realized that many articles have responded to this first type of problem in different ways by proposing installing anti-malware software and some other anti-virus tools, firewalls coupled with intrusion detection/prevention systems, yet, they have failed to effectively identify practically the various forms of attacks in our IT environments with demonstrations on how to properly secure an IT environment from all the possible attacks. All these will be discussed further in the course of this paper.

IT Network security is becoming of great importance because of intellectual property that can be easily acquired through the internet. Currently, internet is considered a data network. Since the current data network consists of computer-based routers, information can be obtained by special programs, such as Trojan horses, planted in the routers. This is the basic reason why security is emphasized in data networks, such as the internet, and other networks that link to the internet [1].

The entire field of network security is vast and in an evolutionary stage. In order to understand the simple background of what have been done in today's research and the improvement I have made in this paper, the next contents of this research will be as follows: computer security objectives; identifying a secured environment; the seven domains of a typical IT environment; types of attacks and their classifications; and practical approach to mitigate attacks in our IT environments.

2. Literature Review

Security is very crucial to networks, applications, and IT environment at large. Although, network security is a critical requirement in emerging networks, there is still a lack of security methods that can be easily implemented. As known, secure network design is not a well-known developed process so there is no methodology to manage the complexity of security requirements. Whenever we consider networks security, it must be emphasized that the whole network is secure.

Network security does not only concern with save communication between two computers but to ensure that the communication channel is not vulnerable to attack during transmitting of data [1]. A possible hacker could target the communication channel, obtain the data, decrypt it, and re-insert a false message [2]. So, securing the network and our IT environment is just as important as securing the computers and encrypting the message as well.

When developing a secure network IT environment, the following need to be considered and come into play before we could be able to define how to effectively mitigate the attacks.

2.1. Computer Security Objectives

For effective security of any network and IT environment, the following

attributes need to be considered [3].

2.1.1. Confidentiality

a) *Data Confidentiality*

This assures that private or confidential information is not made available or disclosed to unauthorized individuals.

b) *Privacy*

This also assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

2.1.2. Integrity

a) *Data integrity*

This assures that information and programs are changed only in a specified and authorized manner.

b) *System integrity*

This also assures that system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

2.1.3. Availability

This assures that systems work promptly and service is not denied to authorized users at all times.

2.1.4. Authenticity

This is the property of being genuine and being able to be verified and trusted.

2.1.5. Accountability

This is the security goal that generates the requirement for actions of an entity to be traced uniquely to that entity [3].

2.2. Identifying a Secured IT Environment

Security is a top-of-mind concern in any IT environment. In environments where regulatory requirements play a role, it is critical to ensure that organizational data is safe and secure at every access point [4] [5]. Awareness isn't enough, though organizations must be able to gauge their security preparedness. Below are some of the things you see in a secured environment.

a) *An Established Security Program*

Any IT security program must have buy-in from upper management and include an established and communicated commitment from the top down, reaching employees, shareholders, and customers alike that demonstrates that this is a company that takes security seriously.

b) *Classified Data*

To protect the confidentiality, integrity, and availability (CIA) of the data in an IT environment, that data should be classified as private, confidential, or

public. There will be more security controls around company financial data (confidential).

c) *Define Security Policy*

Policies tell everyone in an organization exactly what to do to protect the CIA of that data. Confidential data may need to be encrypted, and the security policy will dictate exactly what kind of encryption protocol is required to protect something like the company's sensitive financial data on a user's laptop. Other examples of security policies include access control, backup, anti-virus, mobile computing, and risk management policies to name just a few [6].

d) *Guideline for Acceptable use*

It is important to define what is and what is not "acceptable use" of the tools the company provides to its employees; employees should be asked to read and sign the policy before being granted access to the equipment and the company's network/data.

e) *Companywide Awareness*

It's not enough to establish policies and define rules if no one in the company knows what those rules and policies dictate. Every employee should know where the security policies are stored (*i.e.*, the company's intranet) and how to access them. One way to accomplish this is to hold regular security awareness classes that reinforce the company's policies. Post signs, send out weekly security email reminders and be sure all employees embrace the idea that "security is everyone's responsibility" [5].

f) *Identify Risks*

A critical step in securing an IT environment is to identify all imaginable risk factors. Clearly, more time will be spent assessing the risk to confidential data than to public data. This is an exercise that cannot be taken lightly; without such an assessment, data remains at risk in ways that could have easily been defined and protected.

g) *An Incident Response Plan*

What happens when there is a data breach? It's not a question of "if" it will happen, but more one of "when." How will the company respond? A clearly defined process lays out what constitutes a breach, how to identify it, and who to contact to report a data security breach. Once confirmed, IT must act to contain it as quickly as possible, minimizing the impact on the company. Afterwards, a "lessons learned" session will re-examine the process and create adjustments to avoid a similar circumstance in the future [5] [7].

2.3. The Seven Domains of an IT Environment

In order to be able to secure our environment in network security, there are seven domains of a typical IT infrastructure that needs to be considered. Each domain represents a possible target for an attacker. Some attackers have the skill to con users, so they focus on the User Domain. Other attackers may be experts in specific applications, so they focus on the system/Application Domain. How-

ever, an attacker only needs to be able to exploit vulnerabilities in one domain, and a weakness in any one of the domains can exploited in each of the domains. Therefore, any IT environment must provide protection in each of the domains for business continuity.

2.3.1. User Domain

The User Domain is associated with all the users (of any rank) that have access to the six domains (**Figure 1**).

Some of the risks associated with User Domain are:

a) User can destroy data in application (intentionally or not) and delete all files.

b) User can find that his girlfriend cheated on him and use her password to delete all her work so that she can be fired.

c) User can insert infected CD or USB flash drive into the work computer.

2.3.2. Workstation Domain

This refers to the computer of an individual user where the production takes place (**Figure 2**).

Some of the risks associated with Workstation Domain are:

a) The workstation's OS can have a known software vulnerability that allows a hacker to connect remotely and steal data.

Figure 1. User domain [8].

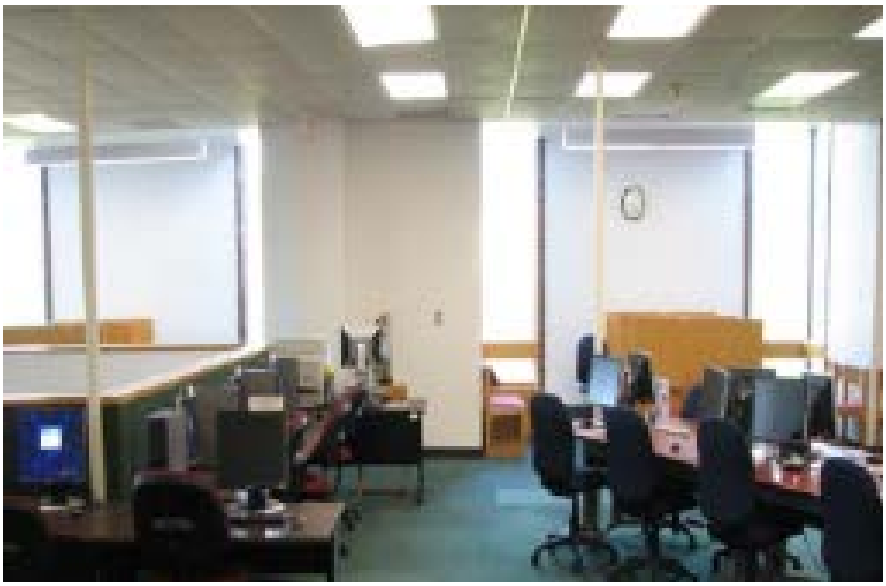


Figure 2. Workstation domain [8].

b) A workstation's browser can have a software vulnerability which allows unsigned scripts to silently install malicious software.

c) A workstation's hard drive can fail causing lost date.

2.3.3. LAN Domain

This Domain contains all the workstations, hubs, switches, and routers. The LAN is a trusted zone (**Figure 3**).

Some of the risks associated with LAN Domain are:

a) A worm can spread through the LAN and infect all computers in it.

b) LAN server OS can have a known software vulnerability.

c) An unauthorized user can access the organization's workstations in a LAN.

2.3.4. WAN Domain

This domain consists of the Internet and semi-private lines (**Figure 4**).

Some of the risks associated with WAN Domain are:

a) Service provider can have a major network outage.

b) Server can receive a DOS or DDOS attack.

c) A FTP server can allow anonymously uploaded illegal software.

2.3.5. LAN/WAN Domain

This domain is the boundary between the trusted and un-trusted zones. The zones are filtered by firewall (**Figure 5**).

Some of the risks associated with LAN/WAN Domain are:

a) A hacker can penetrate an IT infrastructure and gain access to the internal network.

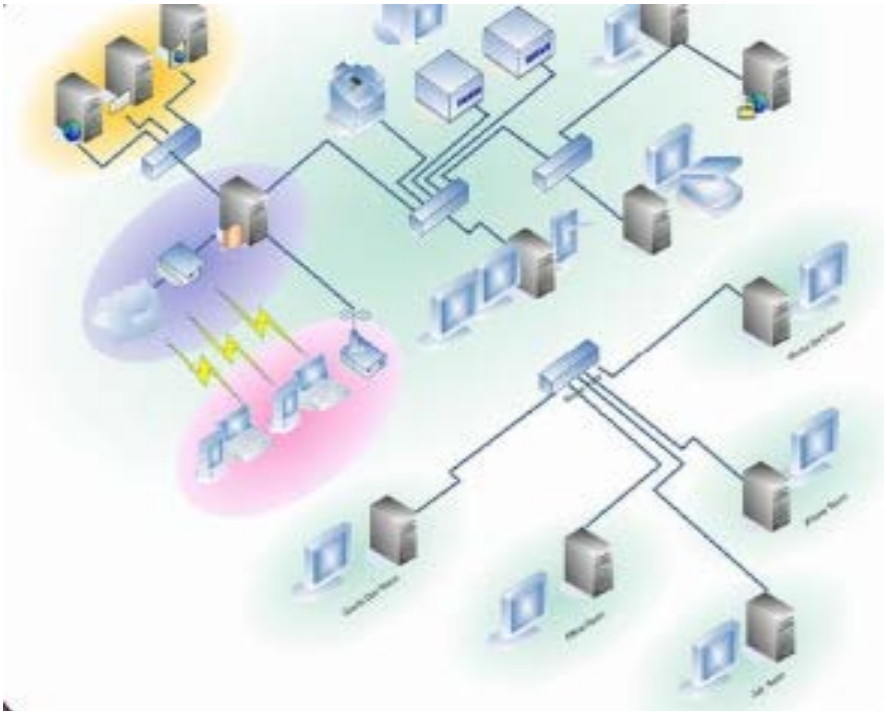


Figure 3. LAN domain [8].

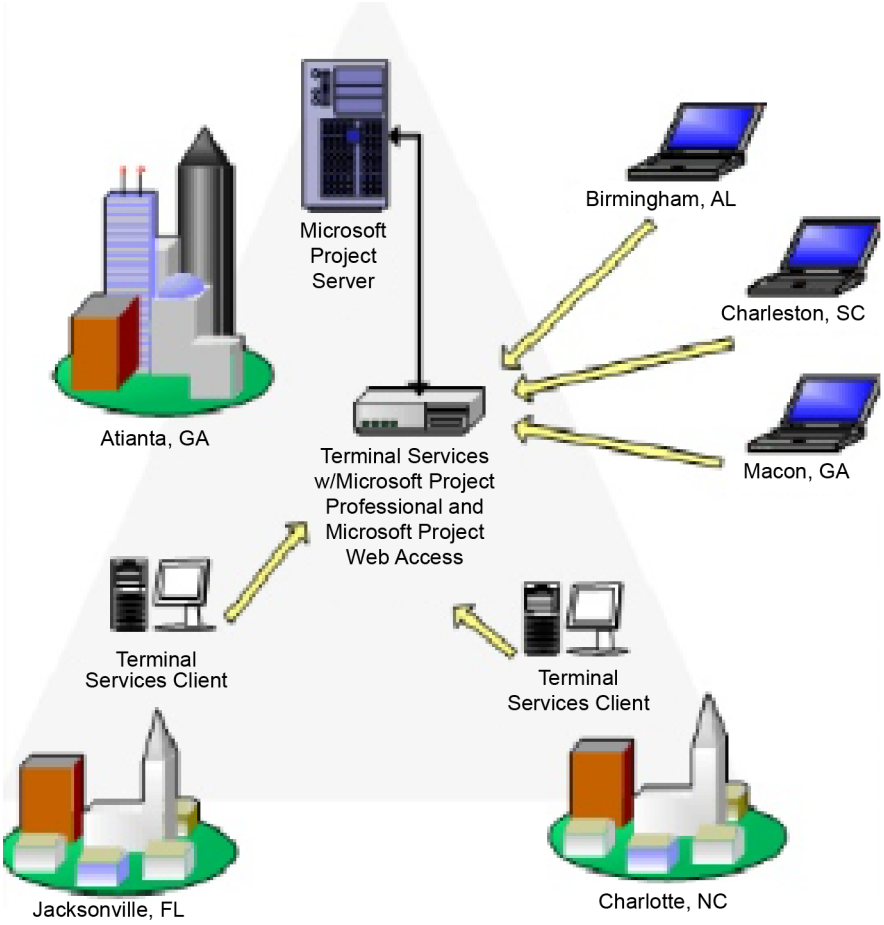


Figure 4. WAN domain [8].

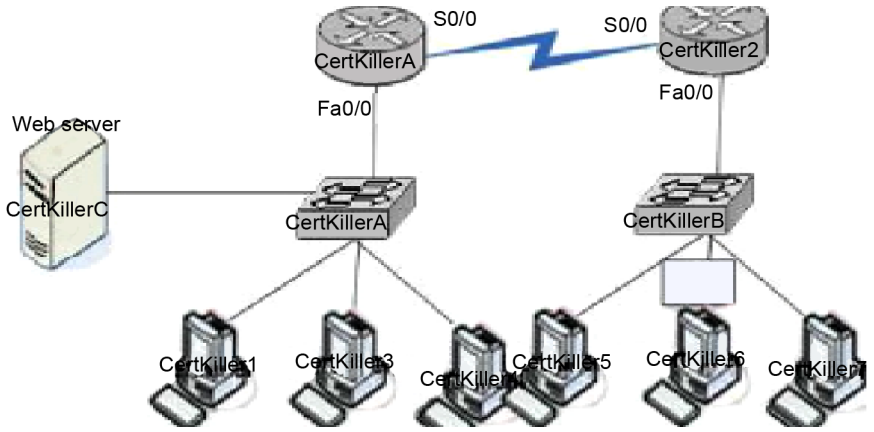


Figure 5. LAN/WAN domain [8].

b) Weak ingress/egress traffic filtering can degrade performance.

c) A firewall with unnecessary ports open can allow access from the internet.

2.3.6. System/Application/Storage Domain

This domain is made up user-accesses servers such as email and database (**Figure 6**).

Some of the risks associated with System/Application/Storage Domain are:

a) A fire can destroy primary data center.

b) A DOS attack can cripple the organization's email server.

c) A database server can be attacked by SQL injection, corrupting the data.

2.3.7. Remote Access Domain

This is the domain in which a mobile user can access the local network remotely, usually through a VPN (Figure 7).

Figure 6. System/Application/Storage domain [8].

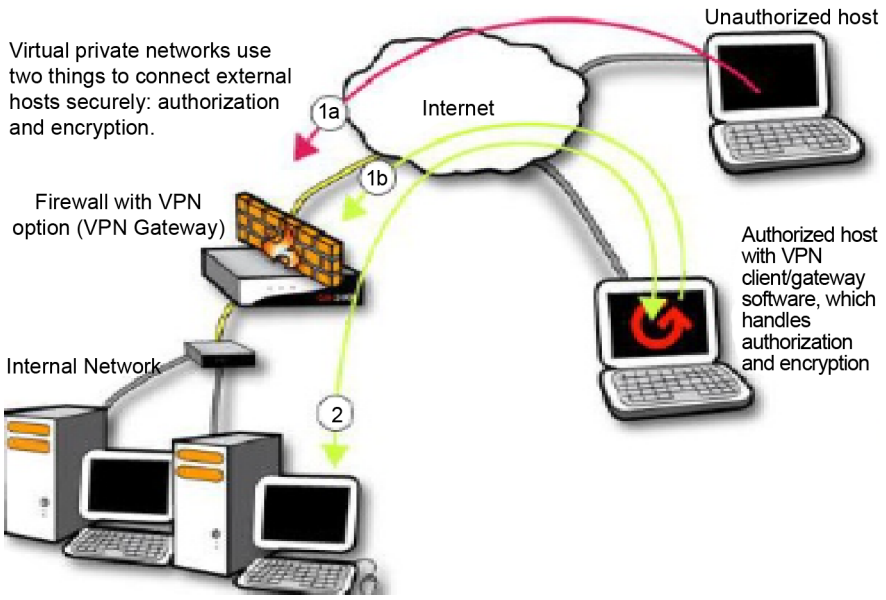


Figure 7. Remote access domain [8].

Some of the risks associated with Remote Access Domain are:

a) Communication circuit outage can deny connection.

b) Remote communication from office can be unsecured.

c) VPN tunneling between remote computer and ingress/egress router can be hacked.

2.4. Attacks and Their Classifications

Attack can be defined as an assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system. Attack could be a passive or an active attack [6].

1) ***Passive Attacks*** are eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. It is an attempt to learn or make use of information from the system but does not affect system resources. Passive attacks are very difficult to detect, because they do not involve any alteration of the data. Two types of passive attacks are the release of message contents and traffic analysis.

a) *The release of message content*—This is like a telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions (**Figure 8**).

b) *Traffic analysis*—In this case, the opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place (**Figure 9**).

2) ***Active Attacks*** involve some modification of the data stream or the creation of a false stream which is also attempts to alter system resources or affect their operation. The four categories: masquerade, replay, modification of messages, and denial of service.

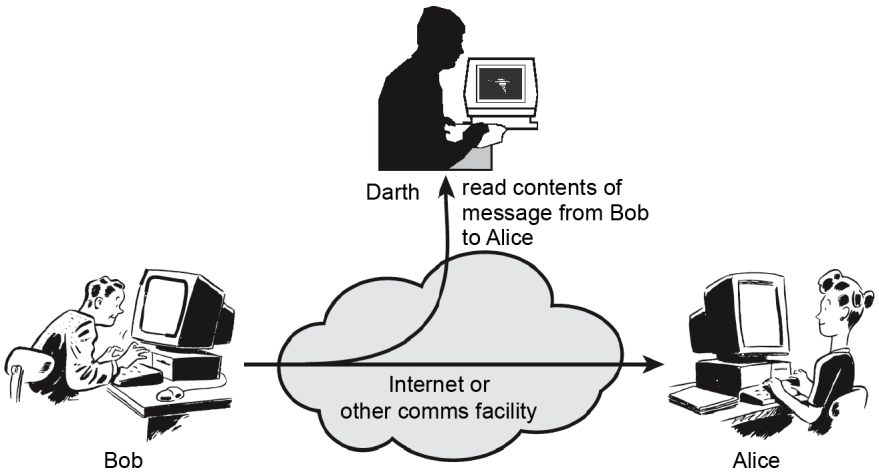


Figure 8. Release of message content [4].

a) *Masquerade*—This occurs when one entity pretends to be a different entity. A masquerade attack usually includes one of the other forms of active attack. For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges (**Figure 10**).

b) *Replay*—This involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect (**Figure 11**).

c) *Modification of messages*—This simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized. For example, a message meaning "Allow Emmanuel to read confidential file accounts" is modified to mean "Allow Steve to read confidential file accounts" (**Figure 12**).

d) *Denial of service*—This prevents or inhibits the normal use or management of communications facilities. This attack may have a specific target; for example, an entity may suppress all messages directed to a particular destination (e.g., the security audit service) (**Figure 13**). Another form of service denial is the

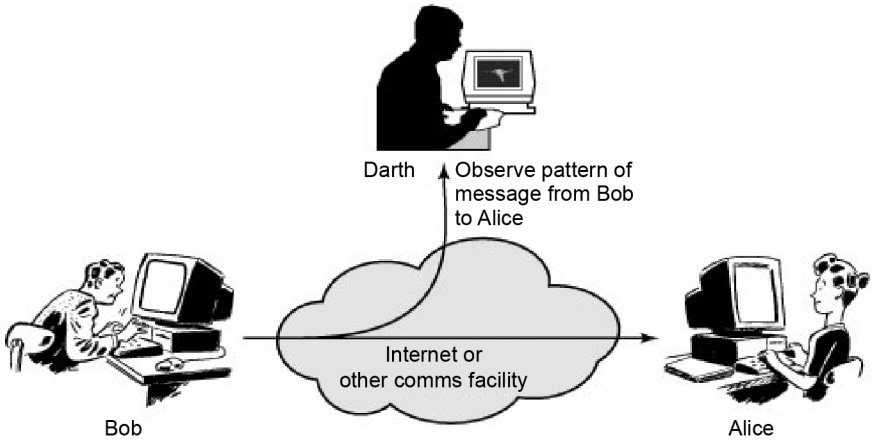


Figure 9. Traffic analysis [4].

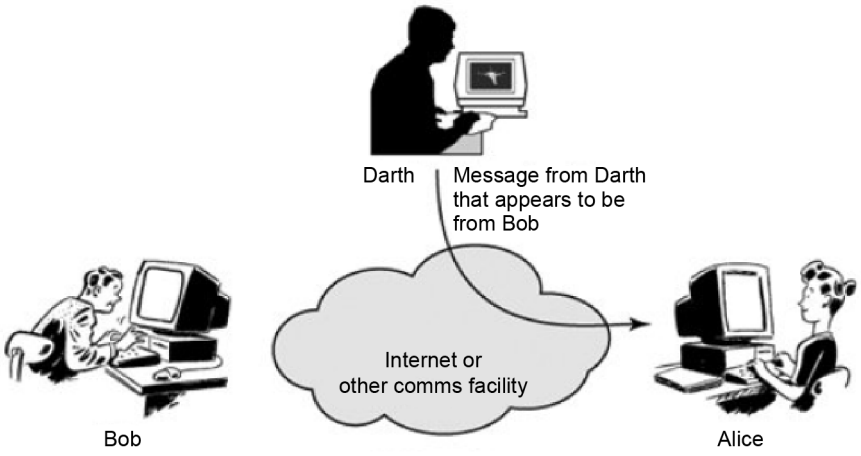


Figure 10. Masquerade [3].

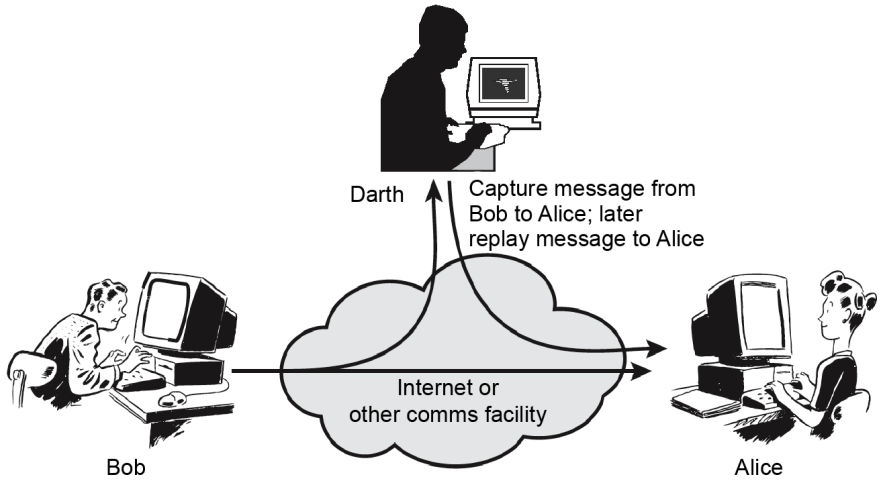


Figure 11. Replay [3].

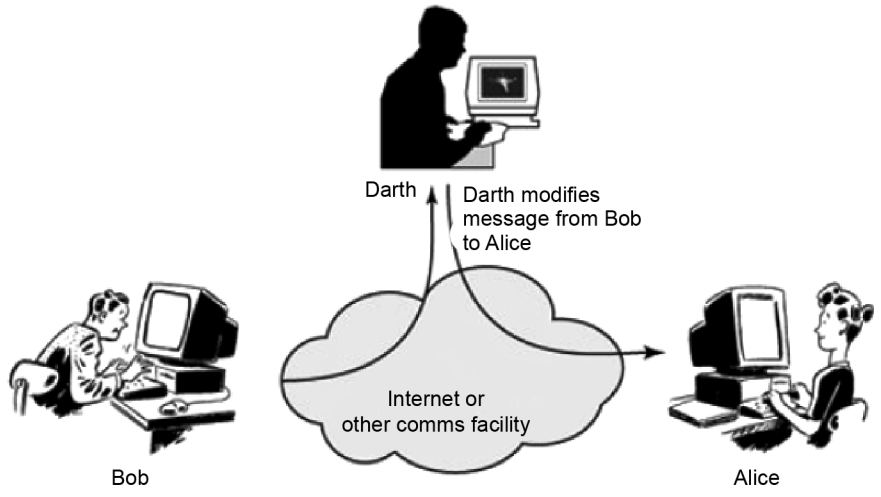


Figure 12. Modification of messages [3].

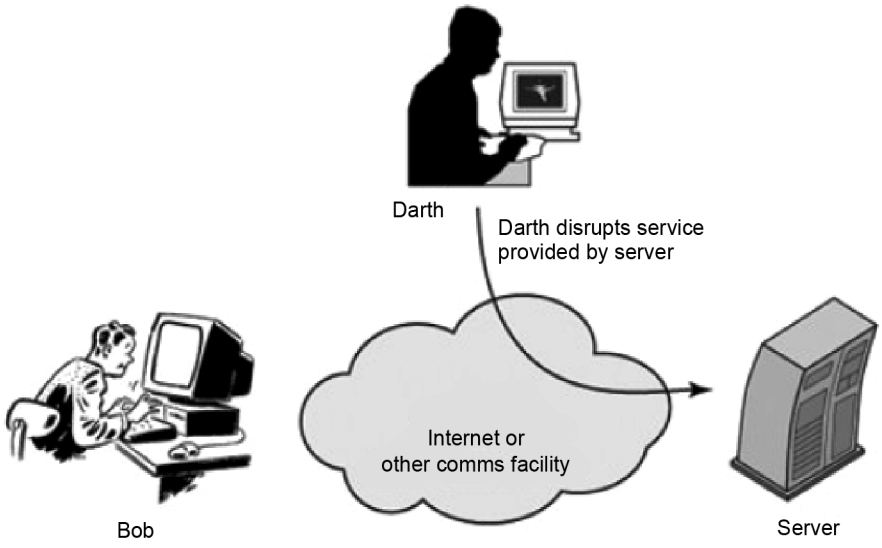


Figure 13. Denial of service [3].

disruption of an entire network, either by disabling the network or by overloading it with messages in order to degrade performance [3].

3. Methodology in Securing an IT Environment

Since internet threats will continue to be a major issue in the global world as long as information is accessible and transferred across the internet, this section then focuses on the different defense and detection mechanisms that can be practically adopted to mitigate those attacks. In my research, I have pointed out before as the core areas to consider more closely as means of mitigating attacks in the IT environment.

3.1. Cryptographical Systems

In the field of Network security in engineering today, cryptography has played a major role in securing the infrastructure. The use of cryptography method involves the use of codes and ciphers to transform information into unintelligible data that is difficult for attackers to decode easily. Though, there are various methods to encrypt data but AES is most secured. AES provides a very high security level because of using variable length key *i.e.* 128 bits and this make AES a highly-secured encryption technique which protect data against future attack (**Figure 14**).

3.2. Intrusion Detection Systems

An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station (**Figure 15**).

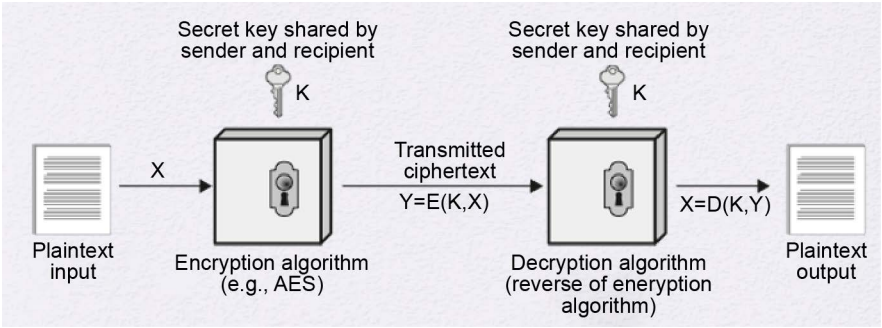


Figure 14. Cryptography symmetric encryption [3].

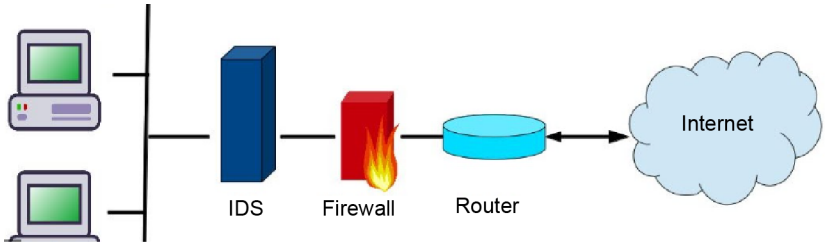


Figure 15. Intrusion detection systems [2].

3.3. Anti-Malware Software and Scanners

Anti-Malware tools are used to detect malicious software like worms, Trojans and viruses in a network and cure an infected system.

3.4. Secure Socket Layer (SSL)

The Secure Socket Layer (SSL) is a protocol that is designed to create a secure channel, or tunnel, between a web browser and the web server so that and information exchanged is protected within the secured tunnel. It provides authentication of clients to server by using certificates (Figure 16).

3.5. Site-to-Site VPN (S2S) [2]

A site-to-site (S2S) VPN allows offices (also external company) in multiple fixed locations to establish secure connections with each other over a public network such as the Internet. Site-to-site VPN extends the company's network, making computer resources from one location available to employees at other locations (Figure 17).

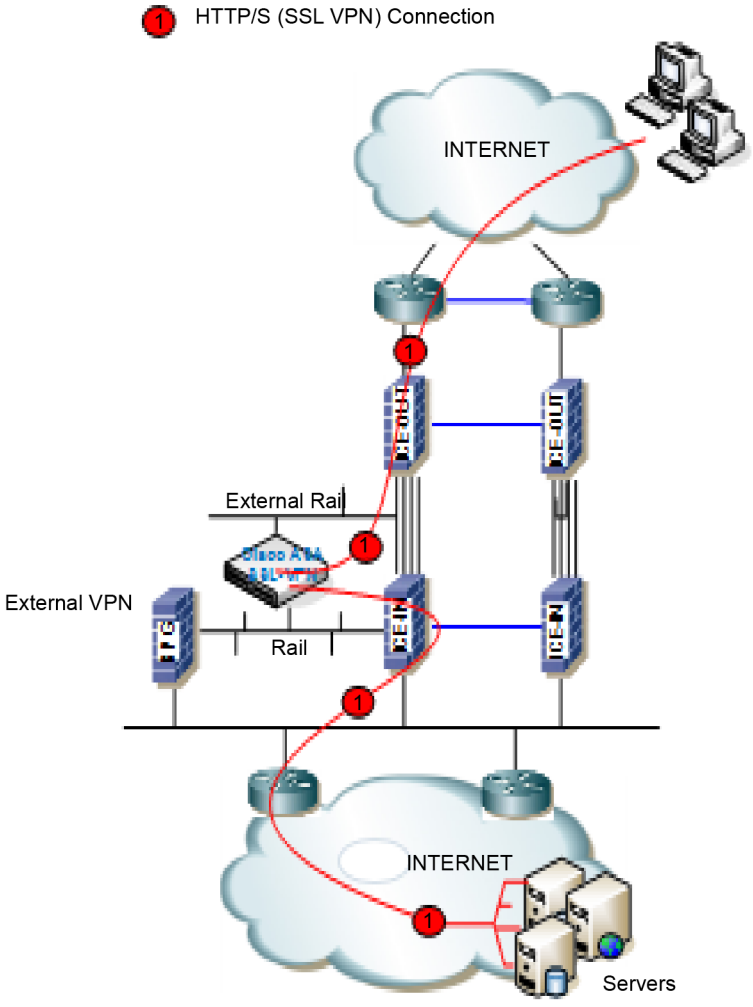


Figure 16. SSL VPN.

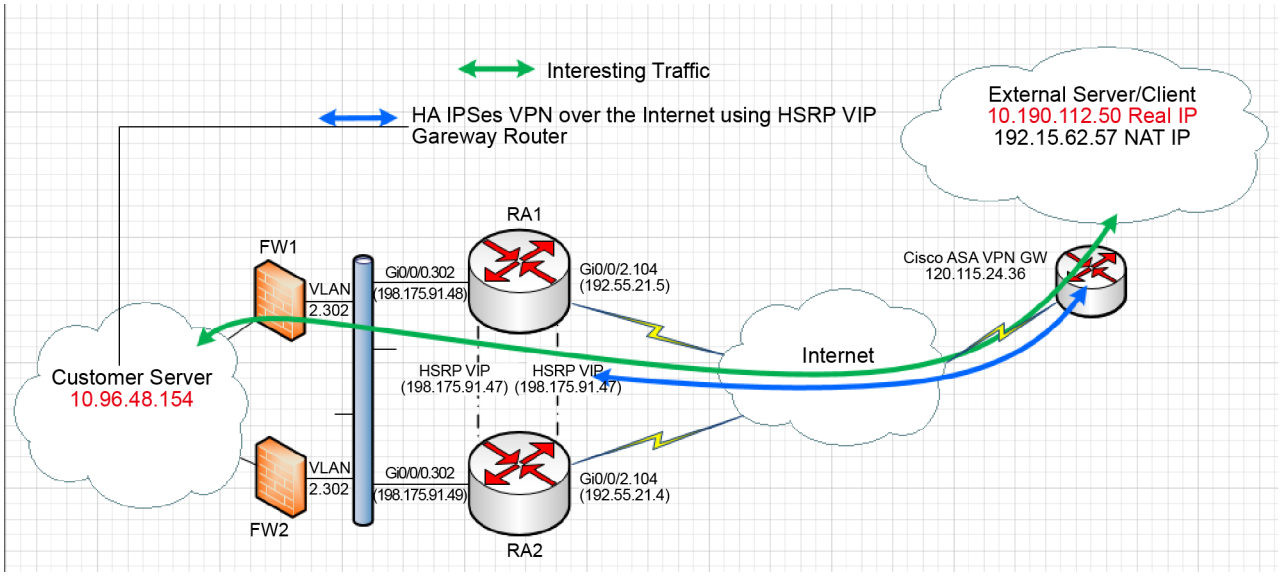


Figure 17. S2S VPN [2].

4. Results/Protection of LAN-WAN Domain as a Test Use Case

A LAN, or local area network, is a network of personal computers deployed in a small geographic area such as an office complex, building, or campus within the context of this discussion [9]. A WAN, or wide area network, is an arrangement of data transmission facilities that provides communications capability across a broad geographic area. As known, an internet is an unsecure environment that needs proper protection due to its open technology. Since there is a lapse between the LAN/WAN environment which is uncontrolled by anyone, an IT environment need to have a control measure in place in order to secure the environment.

Some of the issues that can occur in the LAN/WAN environments are; a hacker can penetrate an IT infrastructure and gain access to the internal network thereby making all the hosts connected behind the LAN vulnerable to attacks. Also, weak ingress or egress traffic filtering can degrade network performances. Not all, a firewall with unnecessary ports open can allow access from the internet.

As a measure to protect LAN/WAN environment, more emphasis will be laid on the implementation of Firewall operations which basically is the point of entrance/deny for any authorized/unauthorized operations both within and outside the network in the IT environment. For instance, LAN/WAN Domain is the key area where attackers can penetrate inside network from outside if not properly secured, or if any improper rules are created.

Firewall

As it is called, the purpose of a Firewall is to block traffic from the outside or traffic from the inside network against the intruders [10]. Firewall as shown in

Figure 18 below is designed to prevent unauthorized access to or from a private network. In the figure, we can see that Firewall is installed before any traffic gain access to the LAN (that is the internal Network) and in some other cases, we can have the Firewall both before and after the WAN Router making two Firewalls in the design (Figure 18). This is to filter both traffic passing through from the internet to the WAN Router and at the same time filter that traffic trying to gain access to the internal Network. With this design, it will be difficult for attackers to penetrate internal Network. (Currently, IPV4 protocol is still the current method of assigning IP addresses.

As known that a firewall with unnecessary ports open can allow access from the internet thereby attacking internal networks. In Figure 19, it shows the result of how a standard rule needs to be implemented on the Firewall with the approval of the necessary security technical review committee.

In the Firewall rule implementation above, the non-standard FW rule means the type of rules that are not supposed to be implemented because it exposes the IT network/environment to attack and no approval for validation of the connection from the Firewall Technical Design review team. Likewise, the standard FW rule represents the type of rules that can be implemented on the Firewall based on the design approval.

Likewise, Table 1 shows the tabular summary of some of the attack methods and the Security Technology that can be used to mitigate them in the IT environment.

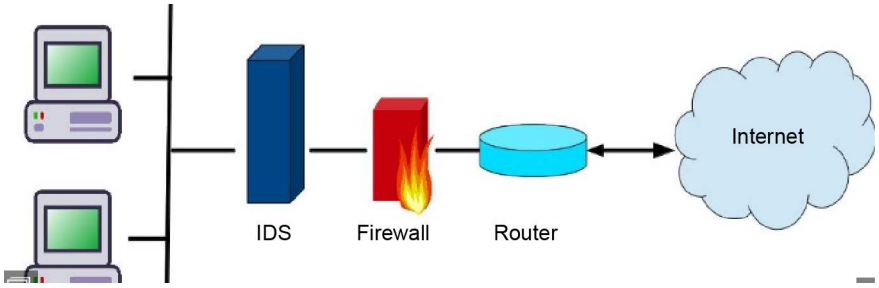
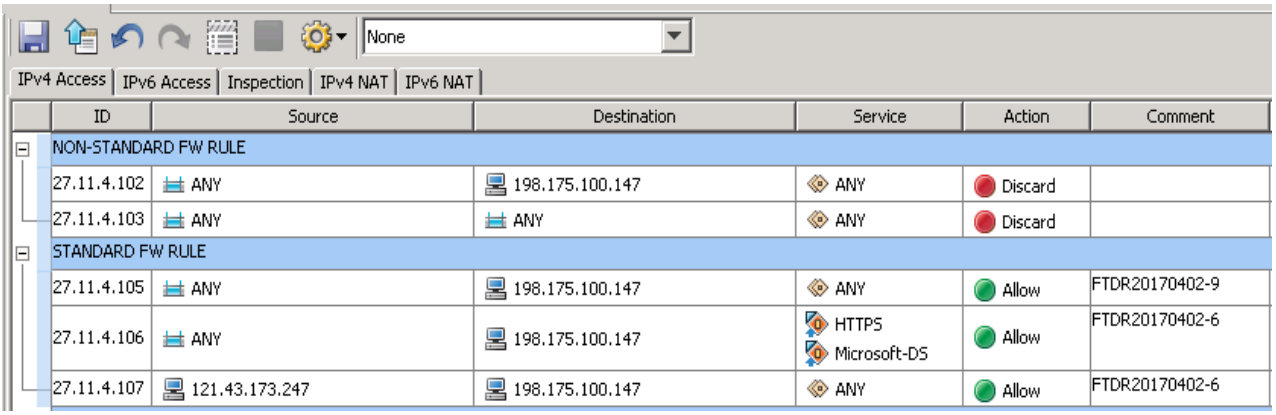


Figure 18. Firewall [2].



ID	Source	Destination	Service	Action	Comment
NON-STANDARD FW RULE					
27.11.4.102	ANY	198.175.100.147	ANY	Discard	
27.11.4.103	ANY	ANY	ANY	Discard	
STANDARD FW RULE					
27.11.4.105	ANY	198.175.100.147	ANY	Allow	FTDR20170402-9
27.11.4.106	ANY	198.175.100.147	HTTPS Microsoft-DS	Allow	FTDR20170402-6
27.11.4.107	121.43.173.247	198.175.100.147	ANY	Allow	FTDR20170402-6

Figure 19. Standard firewall rule implementation.

Table 1. Attack methods and security technology [4].

Computer security attributes	Attack methods	Technology for Internet/IT environment security
Confidentiality	Eavesdropping, hacking, phishing, DOS, and IP spoofing	IDS, firewall, cryptography systems, IPsec, and SSL
Integrity	Viruses, worms, Trojans, eavesdropping, DOS and IP spoofing	IDS, firewall, anti-malware software, IPsec, and SSL
Privacy	Email bombing, spamming, hacking, DOS and cookies	IDS, Firewall, Anti-Malware Software, IPsec, and SSL
Availability	DOS, email bombing, spamming and systems boot record infectors	IDS, firewall, anti-malware software

5. Conclusions

Securing an IT environment/network is an important field that is increasingly gaining attention as the internet expands. The security attacks and their classifications were analyzed to determine the appropriate and effective security technologies. The technologies were comprised of software- and hardware-based. Currently IPV4 is the popular method of assigning IP addresses, but the lack of embedded security within the protocol has led to most of the attacks seen today.

From my research, I see that combined use of IPV6 and security tools such as intrusion detection, authentication and most especially, with the combination of proper implementation of Firewall rules will provide effectiveness in protecting the IT environments.

References

[1] Bhavya, D. (2013) Network Security: History, Importance, and Future. University of Florida.

[2] Curtin, M. (1997) Introduction to Network Security. http://www.interhack.net/pubs/network-security

[3] Stallings, W. (2013) Cryptography and Network Security: Principles and Practice. 6th Edition, Parson Education, USA, 15-80.

[4] Kartalopoulos, S.V. (2008) Differentiating Data Security and Network Security. *Proceedings of IEEE International Conference on Communications, ICC* 2008, Beijing, 19-23 May 2008, 1469-1473. https://doi.org/10.1109/ICC.2008.284

[5] Identifying a Secured IT Environment. (2017) https://www.itbusinessedge.com/

[6] Improving Security (2006) http://www.cert.org

[7] Biswas, N.R. (2011) Is the Environment a Security Threat? Environmental Security beyond Securitization. *International Affairs Review*, **xx**, 1-22.

[8] Seven-Domains-of-a-Typical-IT-Infrastructure. (2010) https://www.scribd.com/doc/115939715

[9] Gibson, D. (2015) Managing Risk in Information Systems. 2nd Edition, Jones and Bartlett Learning, USA, 29-160.

[10] Protecting Your System: Information Security. (2011) https://nces.ed.gov/pubs98/safetech/chapter6.asp