Project Title – Small Business Network Design with Secure E-commerce server

Project Scope

A network has to be designed for a small business organization which has 100 users. The organization hosts an e-commerce application on a server which is accessible to internet users using https and with a public IP address.

Requirements

1.Identify the appropriate hardware which would be used

2.Users on the internet should be able to access only https on the e-commerce server.

3.Users on the internet should have access only to the public IP address of the server and not the private IP address.

4.The users in the organization should have full access to the server.

5.TCP/IP Network design with IP addressing

6.Features and configuration required on the hardware with explanation

Report Contents

1. Project Scope
2. Requirements
3. Requirement Analysis
4. Network Diagram
5. TCP/IP Table
6. Router configuration (IP address, NAT, ACL)
7. Solution Explanation
8. Hardware list

1.Abstract

Small business e-commerce websites make an excellent target for malicious attacks. Small businesses do not have the resources needed to effectively deal with attacks. Large and some mid-size organizations have teams that are dedicated to dealing with security incidents and preventing future attacks. Most small businesses do not have the capabilities of dealing with incidents the way large organizations do. Security of e-commerce websites is essential for compliance with laws and regulations as well as gaining and maintaining the trust of consumers, partners and stakeholders. Many security standards have been established by various organizations to help guide security of small business servers, however, many of those standards or guidelines are too costly or time consuming. This paper1 will discuss how attacks are carried out and how a small business can effectively secure their networks with minimum cost. In points abstract for our project is:

- The aim of this project is to create a small scale computer network design for a small business.
- The organization hosts an e-commerce website on a server.
- This website is accessible to users using http and public ip addresses.
- The network is designed with necessary hardware and software components.

2.Objective

Our Objective is to Design a Network topology for Small businesses consisting of various modules with different functionalities.

3.Introduction

Many businesses have come to the realization that, in order to compete in the market, key business processes need to be part of the Internet. E-commerce has become a popular adaptation for businesses, which has been a major transformation for many businesses. The popularity of the Internet has transformed traditional commerce into e-commerce, which has proven to be a successful platform for many businesses. Small businesses provide an easy target for attackers because they typically have limited funds and do not have dedicated personnel to monitor, update and defend their systems.

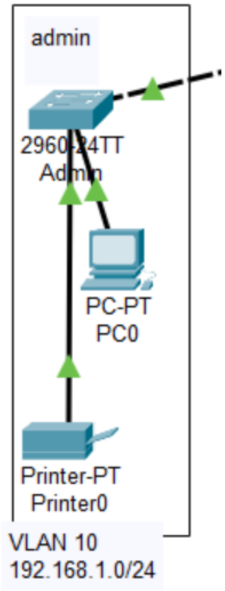
4.Modules of the project

- **HEAD OFFICE**
    - **Admin**
    - **HR**
    - **Finance**
    - **Marketing**
    - **Accounting**
    - **Management**
    - **Logistics**

A project is made up of various modules.These modules are used to divide the work with different production and design teams to make their work easier and organize the project to gain efficient results. The various modules used in our project are:

- **Admin:**

Controller and moderator of the network identifies problems as they arise and comes up with practical solutions. Keep the network up to date and ensure that it works as intended and specifically maintain different networks .



steps for setting up admin module using these steps:

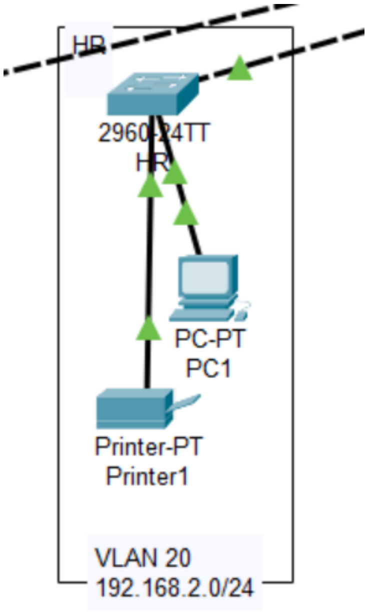
1)We had to drag and drop a PC0 and then connect it to the admin switch. Then we drop the Printer-PT and connect it to the admin switch.

2)we would now configure the pc and open config tag. within config tag in fastEthernet0 we had set up IP Address as 192.168.3.2 and respective subnet mask as 255.255.255.0.

3)Now using the CLI of the switch we may set up the whole network as VLAN10 with the network address as 192.168.1.0/24.

- **HR**

PCs and printers set up for the HR department on the second floor.



steps for setting up admin module using these steps:

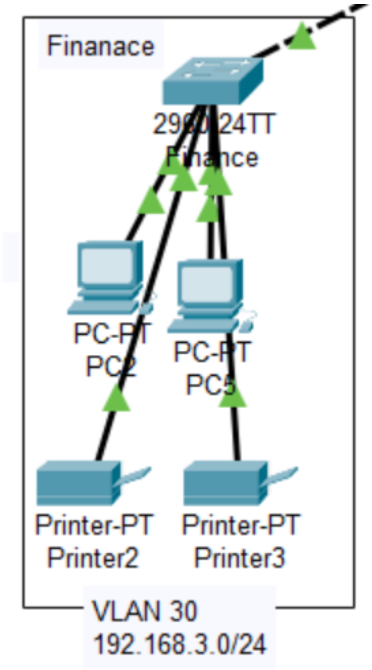
1)We had to drag and drop a PC1 and then connect it to the HR switch. Then we drop the Printer-PT Printer1 and connect it to the HR switch.

2)we would now configure the pc and open config tag. within config tag in fastEthernet0 we had set up IP Address as 192.168.4.2 and respective subnet mask as 255.255.255.0.

3)Now using the CLI of the switch we may set up the whole network as VLAN20 with the network address as 192.168.2.0/24.

- **Finance**

Network setup for the finance-related activities. Two PCs allocated for this department.



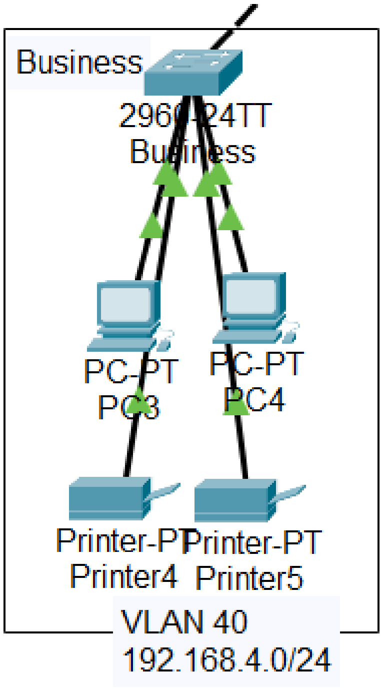
steps for setting up admin module using these steps:

1)We had to drag and drop PC2 and PC5 and then connect it to the Finance switch. Then we drop the Printer-PT Printer2 and Printer PT Printer3 and connect it to the Finance switch.

2)we would now configure the PC2 and PC5 and open config tag within config tag in fastEthernet0 we had set up IP Address as 192.168.2.3 and 192.168.2.2 with respective subnet masks as 255.255.255.0 and 255.255.255.0.

3)Now using the CLI of the switch we may set up the whole network as VLAN30 with the network address as 192.168.3.0/24.

- **Business**



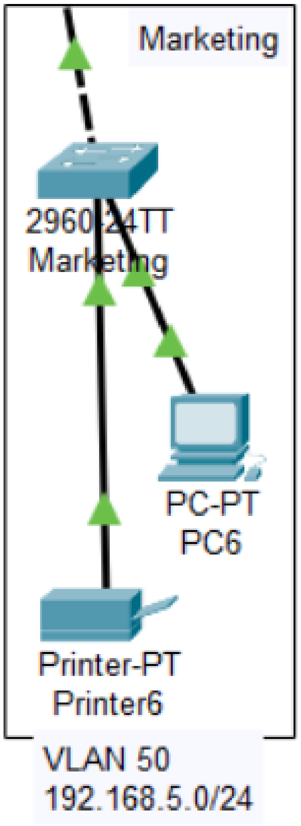
steps for setting up admin module using these steps:

1)We had to drag and drop PC2 and PC5 and then connect it to the Finance switch. Then we drop the Printer-PT Printer2 and Printer PT Printer3 and connect it to the Finance switch.

2)we would now configure the PC2 and PC5 and open config tag within config tag in fastEthernet0 we had set up IP Address as 192.168.2.3 and 192.168.2.2 with respective subnet masks as 255.255.255.0 and 255.255.255.0.

3)Now using the CLI of the switch we may set up the whole network as VLAN30 with the network address as 192.168.3.0/24.

- **Marketing:**

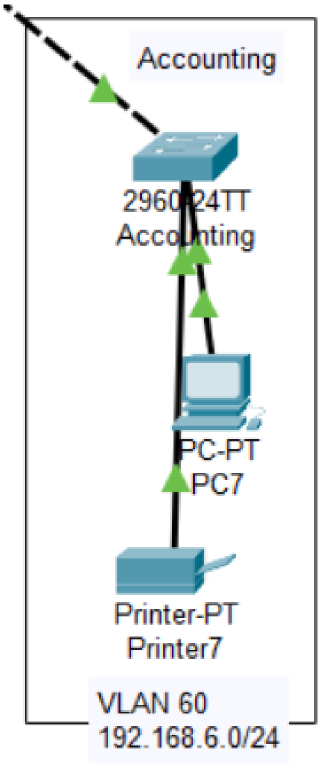


1. The marketing module is provided with a PC (PC-6) and a printer. The 2960-24TT switch connects the marketing network to the head office.

2. This network is configured as VLAN 50 with the network address specified as 192.168.5.0/24

3. IP address of PC6 is 192.168.5.1 with subnet mask 255.255.255.0

- **Accounting:**

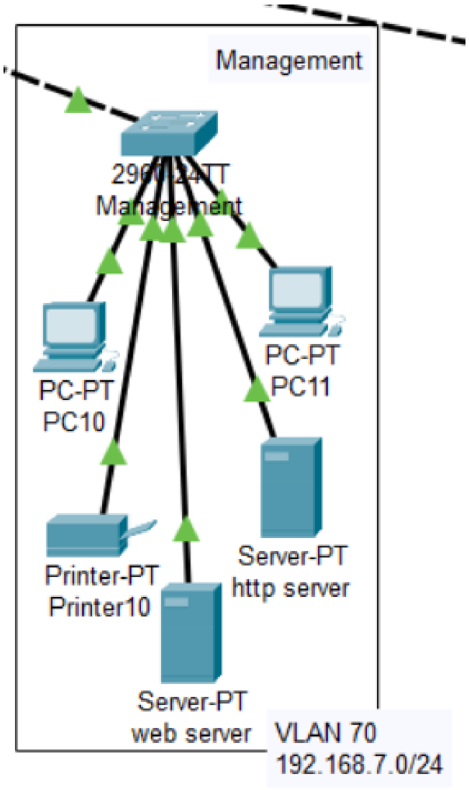


1. Accounting module is provided with a PC (PC-7) and a printer. The 2960-24TT switch connects this network to the main network (head office).

2. This network is configured as VLAN 60 with the network address 192.168.6.0/24

3. IP Address of PC7 is 192.168.6.1 with subnet mask 255.255.255.0

- **Management:**

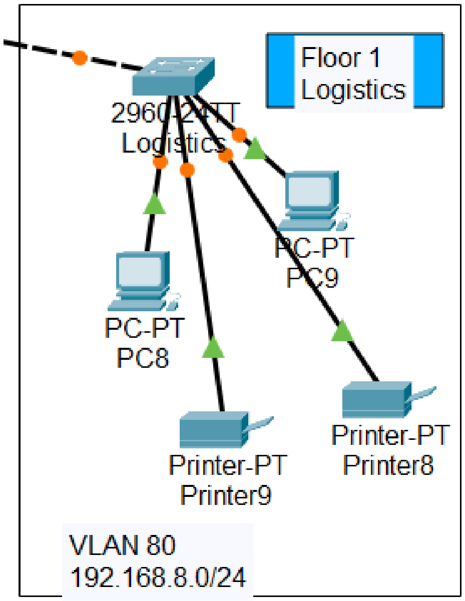


1. Management module is provided with 2 PCs (PC-10) AND (PC-11). The 2960-24TT switch connects the management network to the main network that is head office.

2. The Management network is configured as VLAN 70 with 19.168.7.0/24 as the network address.

3. IP addresses of PC-10 and PC-11 are 192.168.8.2 and 192.168.8.3 with subnet masks 255.255.255.0 and 255.255.255.0 respectively.

- **LOGISTICS:**



1. Module logistics consist of 2 PCS (PC-8 and PC-9) with their respective printers. The 2690-24TT switch connects the logistic network to the main network that is head office.
2. This network is configured as VLAN 80 with the network address as 192.168.8.0/24.
3. IP addresses of PC-9 and PC-9 are 192.168.7.3 and 192.168.7.2 with 255.255.255.0 as the subnet mask respectively.

4.1 E-Commerce Security Standards

Businesses, small and large, are required to comply with certain laws and regulations related to their activities. The concern for security has led to the development of standards and regulations to safeguard valuable data.

ISO 17799 provides recommendations for the following:

• Asset Classification and Control- All information assets should be accounted for and have security classifications to indicate the need and priorities for protection.

- Personnel security- Personnel should be provided appropriate security education and be aware of the incident reporting procedures.

- Physical and Environmental Security

- Network Security

- Access Control

4.3 Security Policies

Any organization concerned with protecting its electronic commerce assets should have a security policy in place. The security policies should describe which assets to protect and why, who is responsible for their protection, and what is acceptable and what is not. Security policies act as a guide for employees so they know what to do before, during and after an incident. The employees should all be aware of the policies, and tests can be conducted to ensure their competency. Tests can be in a variety of forms, such as written, oral and scenario-based tests. The tests should be designed so that employees are comfortable with the information in the policies and are comfortable responding to a variety of situations.

4.4 Physical Security

Physical security should be the first type of security that is implemented. It doesn’t make sense to secure your computer and leave your place unsecure; that is almost the same as locking the doors to your home but leaving the windows open. Physical security can even be in the form of video monitoring systems and access control devices. While there is no way to be completely secure, it is best to limit the chances of being a victim.

4.5 Access Control

Controlling access to a facility or regions in the facility is an important part of security. Security guards should be used for roving patrols and ID verification of employees. The problem with security guards is that they are human and social engineering can be used to manipulate them. Because of the social engineering concerns, locks, biometrics scanners, and passwords should also be considered for access control.

4.6 Monitoring

Monitoring is very important because a hacker could sneak in without a company knowing and cause a lot of damage. The facility and the network need to be monitored to prevent a hacker from penetrating defenses and causing irreversible damage. With constant monitoring, security will be able to detect an attack and stop it before damage occurs. It is better to take measures to prevent something from happening than to try to repair the damage later. Some things may be damaged beyond repair and important information could be lost forever.

4.7 Authentication

Different methods of verification are used by different agencies to prevent unauthorized users from accessing their facilities, systems, and services.

4.8 Biometrics

Biometrics uses a person’s body for access verification. Retinal scans, finger and palm print readers, and other body scanners are used for access control to verify a person’s identity. Biometrics is good because it uses parts of the body that are unique to that individual. The problem with biometrics comes when a person damages their part of the body that is used for verification. If a person damages the body part used for verification, it will require extra work and the administrator will have to use a different means to allow that person access.

4.9 Usernames and Passwords

Usernames and passwords are user chosen credentials, which usually have certain requirements that are set by administrators. Requirements have to be set because people will use passwords that are common and hackers can break them. “The most secure passwords are at least 8 characters long with a mixture of upper and lower case letters and symbols and numbers. The problem with passwords and usernames is that people either forget them or they write them down and put them in a place where people can find them.

4.10 Smartcards

Smart Cards are used in many facilities to control access to a certain area, system, or service. Smartcards allow a person access without having to remember a password. The problem with many smartcards is that people lose them and other people might be able to use them.

4.11 Wireless Security

The days of connecting computers with wires are gone; now businesses use wireless connections to send, receive and access information. Sending and receiving information wirelessly makes it susceptible to being apprehended. Systems can send and receive information via a wireless router that is connected to a modem which is connected to the Internet. The computers send out packets to the wireless router, which then transfers that to the modem and through the Internet.

4.12 Cryptography

Cryptography is used to turn plaintext into an algorithm known as ciphertext, which is a complex mathematical sequence unreadable to anybody without the code to decipher it. Once data is encrypted into ciphertext, it is given a password and that password is needed to decrypt the data and turn it back into plaintext. That data can be sent to another person as long as that person has the password to decrypt the information. The type of algorithm determines the strength of the encryption and can make it more or less difficult to decrypt without the proper key. Cryptography is also used to create signatures for documents, which help to determine originality of that document.

4.13 Hashing

Hashing is a way of creating a unique signature for a document to prove that the document is the original document. Hashing is used to compare to the document to ensure it is the original. The most secure type of hash is the Secure Hash Algorithm (SHA), which uses 160 bit encryption.

4.14 Computer Intrusion Detection and Prevention Systems

Computer Intrusion Detection and Prevention Systems are similar to having a motion detector on the building and locks on the doors and windows. The

Computer Intrusion Detection (IDS) System, similar to the motion detector, is meant to detect potential attackers and alert someone to take action. The Intrusion Prevention System (IPS), similar to the locks on the doors and windows, is meant to keep the attacker out. The names of the two systems sums up exactly what they are meant for. To have a good security program, you need both protection systems in place; one for detection and the other for prevention of malicious activity. Many systems these days incorporate both detection and prevention into one system and are known as Intrusion Detection and Prevention Systems (IDPS).

4.14.1 Intrusion Detection Systems

IDS monitors a network for possible malicious activity and then reports that activity to the administrator so he or she can make a decision on what to do with that threat. There are many different types of IDS's, which use different protocols for detection of threats such as network based, wireless, behavior analysis, and host-based detection systems. e-commerce systems should deploy both network and host-based IDS, however the cost might be too much for some small businesses.

4.14.2 Host-Based IDS

The functionality of host-based IDS's are similar to a virus scanner tool. The software is automated and runs in the background of the host system to detect any suspicious activities. It can be configured to take specific actions when an issue is detected. For example, it can be configured to automatically quarantine the suspicious activity or simply notify the administrator of the issue.

4.14.3 Network-Based IDS

Network-Based IDS's examine the type and content of network packets. Network IDS's are less expensive than host-based IDS's, but it cannot monitor activities on individual host systems. It can protect the network as a whole but cannot protect individual systems. When choosing the IDS, it needs to be compatible with the firewall that is being used. The network-based IDS should be deployed between the incoming connections and the firewall. It should also be installed under two network interfaces, one for analyzing and one for reporting information to the IDS console.

4.14.4 Intrusion Prevention System

IPS's use a certain protocol of identifying threats and preventing them from accessing a network so they do not have a chance to harm the system. IPS's monitor the network traffic for malicious activity, log the activity, attempt to prevent it from accessing the network, and then report the activity to the administrator so he or she can follow-up with an action. Just like the IDS, the IPS may detect activity that is not malicious and the administrator will have to decide what to do with it.

4.14.5 Operating System Hardening

In e-commerce systems, it is important to reduce the attack possibilities by reducing or eliminating as many vulnerabilities as possible. This is accomplished by incorporating IDS's, installing anti-virus systems, removing all unnecessary programs, closing all ports and configuring it to protect against unauthorized access. "In many instances, an operating system provides a gateway into a computer system because of the large number of open ports and services running. Many types of security software can be configured to detect and automatically handle suspected incidents. It is important to look for software that has low false-positives because it could potentially hurt business if it is blocking transactions from occurring instead of blocking attempted attacks. Also, it is important to find the software that has a good team and offers continuous updates. Threats are constantly evolving and it is important for software companies to stay up-to-date with the latest threats to their software. It will be important to continually check for updates and patches so vulnerabilities in the software are fixed before an attack occurs.

5.Inference

E-commerce is an effective way to do business. It allows businesses to provide products and services to a wider population than they could with traditional brick and mortar operations. However, e-commerce also comes with a wide variety of risks that need to be mitigated to operate securely. Small businesses provide an easy target for attackers because they typically have limited funding and do not have dedicated network professionals to monitor and protect their network. Hackers have a wide variety of tools that allow them to attack networks even with little technical knowledge. Hackers use a system along with their tools to attack systems. They first need to gather as much information as possible about the target system, scan for open ports, scan for vulnerabilities and then conduct their attack. Along with technical attacks, some attackers might try physical attacks through social engineering and gain access to the business servers by pretending to be someone they are not. Small businesses need to take as many precautions as possible to protect their systems, even if it means spending extra money to do so. There is really no way of completely securing a network, but there are ways to minimize the chances of becoming a victim. Limiting the chances of becoming a victim is better than trying to repair the damages after an attack, which may not be repairable. Attacks come in many forms, so it is imperative to ensure that as many security measures are put in place as possible. The implementation of various security measures is important for the protection of family, business continuity and national security. With the possible outcomes of an attack on a network, businesses should take network security very seriously and properly protect their systems.

6.References

[1] Brenton, C. (2003). Mastering Network Security. 2nd ed. Alameda, CA: Sybex,

[2] Center of Excellence Defence Against Terrorism (2008). Responses to Cyber Terrorism. Amsterdam, NLD: IOS Press.

[3] Ciampa, M. (2009). CompTIA Security+ 2008 In Depth. Boston, MA: Course Technology.

[4] Dent, A., Mitchell, C. (2005). User's Guide to Cryptography and Standards. Norwood, MA: Artech House, Incorporated.

[5] Department of Homeland Security (2003). The National Strategy to Secure Cyberspace. Retrieved March 01, 2011 from: http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf