NCC Level-5DC Diploma in Computing

Network Security and Cryptography

Candidates Name : Fatema Akter

ID No : 00154713

Module Title : Network Security and Cryptography

Assignment Title : City College

Examination Cycle: March 2016

Candidate attempting to gain an unfair advantage or colluding in anyway whatsoever (other than on joint assignments) are liable to be disqualified. Plagiarism is an offence.

Expected candidate time allocation: 35 to 40 hours

Mark	Moderated Mark	Final Mark

Marker's comment:

Moderator's comment:

Statement of Confirmation of Own Work

Programmed /qualification name: Network Security and Cryptography

Student Declaration:

I have read and understood the NCC Education's policy on Academic Dishonesty and Plagiarism.

I can confirm the following details**:**

Student ID/Registration number	**: 00154713**
Name	**: Fatema Akter**
Center Name	**: Daffodil Institute of Information Technology.**
Module Name	**: Network Security and Cryptography**
Assignment Title	**: City College**
Number of Words	**: 1,610**

I confirm that this is my own and that I have not plagiarized any part of it. I have also noted the assessment criteria and pass mark for assignments.

Due Date: 26/01/2016

Submitted Date: 26/01/2016

Student Signature: Fatema Akter

ACKNOWLEDGEMENT

At the beginning I would like to render thanks to the almighty Allah. And so I would wish to show my special thanks, gratitude to my teacher Mr. Shomonn well as all other teachers. Thanks to NCC education, who afforded me this tremendous task? I did a great deal of research and I came to know about so many recalls and it helped to increase my knowledge.

Once more, I would wish to give thanks all of them who helped me to complete this project.

Table of Contents

Introduction:

In this assignment I am necessary to produce an important document. This assignment will enable me to show my knowledge and understanding of computer network. I am also required to research the presented component in market place. This assignment is divided into different task Task-1: Risk assessment, Task-2: Explaining risk control, Task-3: Network Diagram, Task-4: Maintaining security and Task-5: Reflective commentary.

Task-1

Risk Assessment:

(a) Identify five important information assets related to City College:

- Y-drive
- Student personal data/ Student record
- Current system LAN
- Server Hosting
- Financial system

(b, c, d): A completed table for all assets, threats, CIA, Likelihood, impact and Risk of City College. Including table:

Asset	Threat	CIA	Likelihood	Impact	Risk
Y-drive	Employee theft	C	Medium	High	High
	Unauthorized access	A	Medium	Medium	Medium
	Server failure	A	Low	Medium	Low
Student personal data/ Student record	Server failure	A	Low	Medium	Low
	Employee theft	C	Low	High	Medium
	Data Hack	C	Medium	High	High
	Miss Information	C	Medium	Low	Low
Current system LAN	Server failure	A	Low	Medium	Low
	Vulnerability	C	Medium	Low	Low
	Weak firewall	A	High	Medium	High
	WLAN security	A	Medium	Low	Medium
Server Hosting	Viruses	A	High	Medium	High
	Data Hack	A	Medium	High	High
	Phishing	A	Low	Medium	Low
Financial system	Miss information	C	Medium	Low	Low
	Information leaks	I	Medium	Medium	Medium
	Employee theft	C	Medium	High	High
	Server failure	A	Low	Medium	Low

Figure No: 1.1- Table of Assets, threats, CIA, Likelihood, impact and Risk

Task-2

Explaining Risk Control:

(a)Discuss each threat and identify and explain the security measures risk:

These systems are three categories such as:

(i) Internal Threats:

Information leaks-

- Information folder will be ***encrypted*** and strong password protected
- Password number will be not ***dictionary word*** and combine of letter, number and symbol
- We use ***HTTPS*** because it is high secured for encrypted.

Justification:

I think password will be more secure for information. Password will be should used in uncommon. Like ***w@ord157.***

Employee theft-

- Every PC will control by ***IPsec*** for accessing, the employee PC will monitoring by IP access history. ***IPSs*** use techniques because port 25 can be blocked so that port 587 is used and that require authentication
- The data will be ***back-up*** in a server and use ***SSL***

Justification

If we use ***SSL*** certificate that uses public key ***encryption*** techniques and the SSL handshake either authentication the server or clients or blocks unauthorized users. (Thomas, (2000))

Miss information-

- If we used ***encryption E-mail*** access system.
- E-mail ***Password*** will be encrypted
- Only ***authorize person*** can be access email otherwise don't allow.

Justification

For data encryption the staffs don't change information and for email password encryption can't access email.

Phishing -

- Email security packages provide anti-phishing protection
- Combination of methods:
  - -Authentication
  - -Detection
  - -Prevention
  - -Reporting

Justification:

Enables threat analysis, attack prioritization and response to minimize risk as well as impact of phishing.

Viruses -

- Email security solution offer highly advantage virus protection
- Automatically scan all ingoing and outgoing massage and **attachment**
- Email security will filter packages to detect ***spam*** and **virus**

Justification:

Identify non-relevant communications and blocked email addresses that are known to have sent spam, preventing further disruptive email. (Stallings, (2010))

WLAN security -

- Transmission must be encrypted and WLAN security ***WEP,WPA,WPA2*** is best for system
- ***WLAN*** access control ***IEEE 802.11*** and access may be control via access to the access point ***(AP)*** as well as Media access control ***(MAC)*** address
- ***IPSec*** will be used also.

Justification:

WLAN IEEE 802.11 is standard and only authorize devices can connect to the AP as well as MAC can be data filtering. ***IP from IPsec*** is more secure for that IPSec will be used. (Stallings, (2010)

Unauthorized access-

- When the teacher collected assignment from ***drop box***. And data from drop box and then they feedback drop on drop box.
- We can use ***biometrics*** system to access confidential data.

Justification:

Biometrics system is such as ***fingerprints, retinas, irises***, facial patterns and hand measurements and etc more secure.

(ii)System Threats:

Server failure-

- ***Backup server***- For the reason if one server will be failed then another server is connected automatically
- ***Hardware back up-*** for the reason if one hardware will be destroying hardware will be connected.
- Every system needs change their ***hardware*** after six month for batter service

Justification:

If we used ***backup server*** then we data collected in another server that means our data will be recovery. So we don't lose any data.

(iii)External Threats:

Data Hack-

- When data is deleted or corrupted Back up data-allows for data recovery
- Have storage access control mechanisms
- ***Password protect*** documents
- We transfer ***file and email*** with encrypt for secure
- For external user we ***use VPN***
- ***Encrypt files***
- ***Encrypt disks***
- used key size ***128 bits***

Justification:

Because for 128 bits key the hacker will be need time at 1 million decryption per ***microsecond=5.9*1030 years.*** (Sons, (2004))

Vulnerability-

- Check the vulnerability in password, don't allow weak password.
- Find out Vulnerability of software and solving the by new software.
- The best prevention is sound security practices. Such as system maintained, firewalls and anti-virus, access controls and audits etc.
- ***Vulnerability scanners***. Such as ports, network, database etc.

Justification:

Software that probes for open ports and used by network administrators to test the network as well as used by attackers to look for vulnerabilities. Host supply services to ***TCP/IP protocol*** thorough a port. (Scambrey, (2001))

Weak firewall-

- Scan package
- Package ***filtrating***
- ***Sequence*** maintained
- Access data authorize person
- Acceptance authorize data
- We install one software that work as pc ***anti-malware***
- ***DMZ*** (Demilitarized zones) will be used

Justification:

Traffic moving between the DMZ and other interface on the protected side of the ***firewall*** still goes thought the firewall. The traffic has protection policies and the common to put public-facing server on the ***DMZ.*** Like web server, email server etc. (Zwicky, (2000))

(b)Where we use encryption and explain why the protocols recommend:

There are many kinds of place we used encryption system such as:

- For ***e-mail*** transfer we used Digital signature
- For ***password*** secure we used hashing algorithm
- For ***file*** transfer we used ***MD5*** format
- For server access

Protocols recommend:

- ***MD5***
- ***Hashing*** algorithm
- Digital signature

Task-3

Network Diagram

(a) Draw a network diagram with network components on the campus and Employees' connections from home:

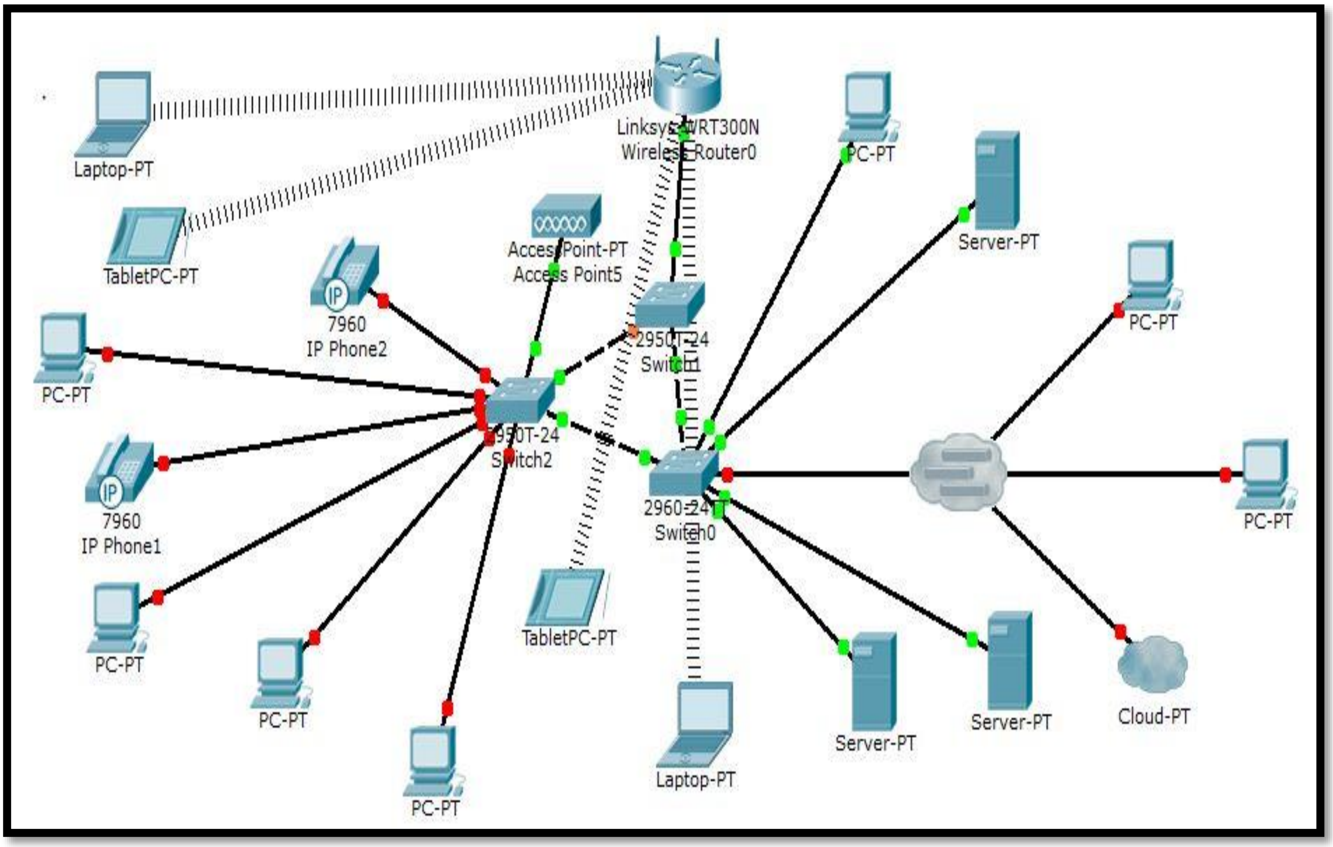

Figure No: 3.1- Draw a network diagram with network components

(b) Draw a network diagram with network components and IP address:

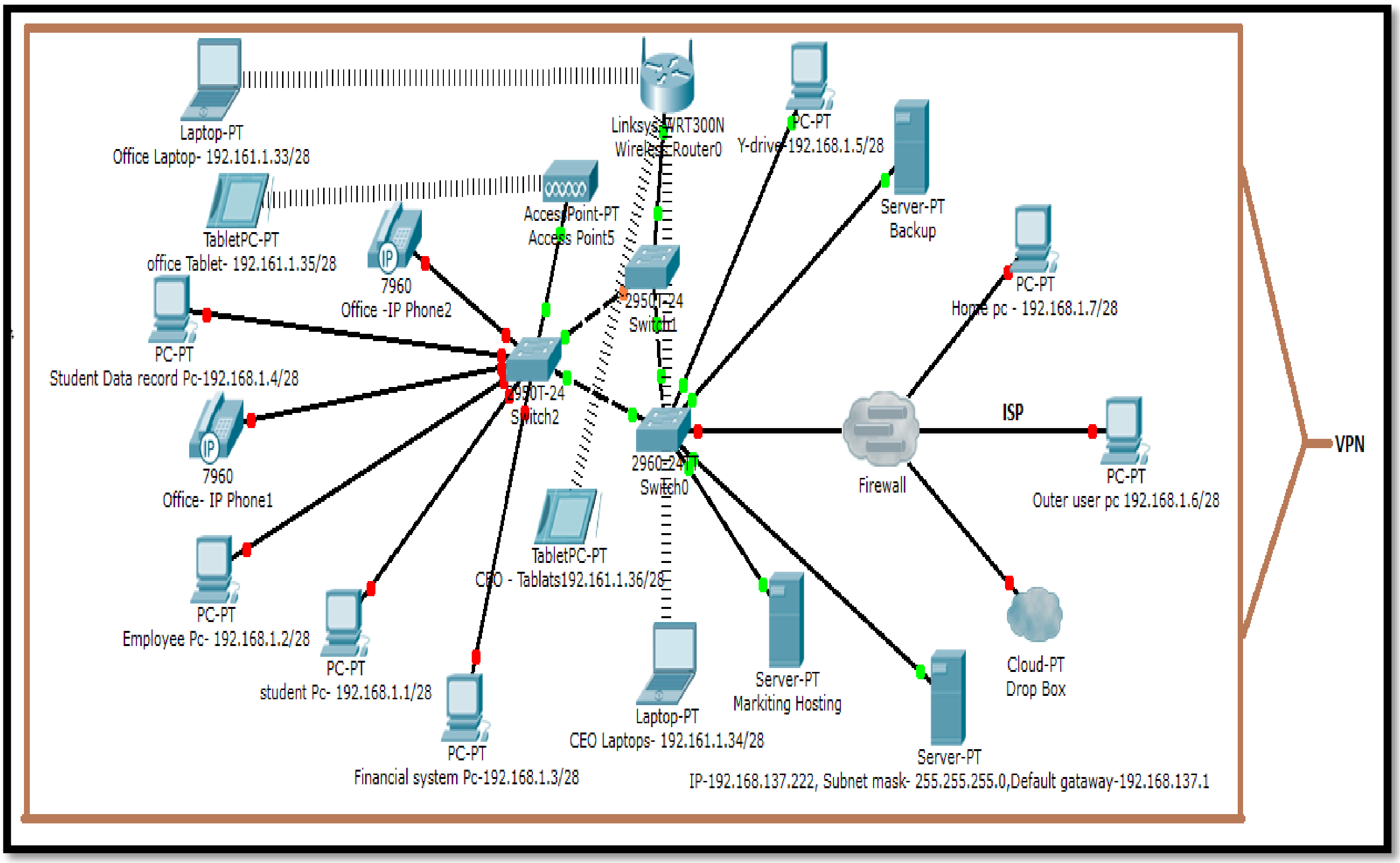

Figure No: 3.2- Draw a network diagram with network components and IP address

(c) Firewall list of rules table:

Name	Access	White list IP address/authorizes	Modify
1.Y-drive	Authorize person	Pc , IP-192.168.1.5/28	Access all
2. Student record	Anyone	All , IP-192.168.1.4/28	Download read and write file
3.Fininacial data	Authorize person	Not allow , IP-192.168.1.3/28	Not allow
4.E-mail	Authorize person	All	Access all
5.Drop box	Authorize person	All	Access all
6.WLAN	Anyone	All	Download file, image
7.Employee pc	Authorize person	Pc , IP-192.168.1.2/28	Access all
8.Home pc	Anyone	All , IP-192.168.1.7/28	Download read and write file
9. Outer user	Anyone	All , IP-192.168.1.6/28	Download file, image
10. CEO	Authorize person	Pc , IP-192.168.1.34/28	Access all
11.Office pc	Authorize person	Pc , IP-192.168.1.33/28	Access all

Figure No: 3.3- Table of Firewall rules

Task-4

Maintaining security:

(a) Recommend for ensuring security is taken seriously:

- We need password will be changed after ***six month***. Password will be should ***MD5 format*** for data secure.
- We will be need arranged ***workshop for training*** after three or six month. As an employee will be more qualified and the employee will be known everything for that company system and that work.
- There are many kinds of Viruses such as ***spam, spyware*** etc.
- Spam a large proportion of all corporate email is spam and most spam is annoying and ***slows*** down the network.
- Hackers may sometimes disguise viruses, spyware and malware as innocent-looking spam. For the reason we need more security like use key words and phrases, spam is moved to separated folder or deleted from email server.
- There are different ways of ***classify VPN.*** We used two broad categories based upon architecture like ***client-initiated*** VPNs and network access server ***(NAS)-initiated*** VPNs. (Tanenbaum, (2003))

Task-5

Reflective commentary:

(a) Problem and solving them:

- Many companies have used ***dictionary password*** it is big problem for company. For the reason I have changed password format where don't used dictionary word. I have used encryption password.
- Many various form E-mail such as: ***spam, spyware*** etc. for that we will be used ***anti-Viruses software.***
- Maximum time we don't install ***firewall*** in our system. So we will be install firewall in the system.

(b) Differentia in my system:

- We used ***encryption*** password
- Password will be not ***dictionary word***
- Every ***IP address*** will be blacklist.
- We will be maintained ***PGP***
- We will be blocked ***e-mail*** for unauthorized person.

(c) CEO's concerns justify:

- Two type of Firewall such as ***software firewall*** and ***hardware firewall.*** So we can use firewall for better service.
- We monitoring every employee pc. For that we don't lose any data and information. (Scambrey, (2001))

Conclusion:

At the end of this assignment I had a most excellent working experience. I got to gained knowledge of networking. Self-confidently my experience will help me whole better achievement in the near future anywhere network problems will come out.

Bibliography

- Scambrey, J..M.S.a.K.J., (2001). *Hacking Exposed: Network Security Secrets & Solutions*. 2nd ed. McGraw Hill.

- Scambrey, J..M.S.a.K.J., (2001). *Hacking Exposed: Network Security Secrets & Solutions*. 2nd ed. McGraw Hill.

- Sons, J.W.&., (2004). *Cryptography for Dummies*. Cobb, C.

- Stallings, W.)., (2010. *Cryptography and Network Security: Principles and Practice*. 5th ed. Pearson Education.

- Stallings, W., (2010). *Cryptography and Network Security*. Principles and Practice ed. Pearson Education.

- Tanenbaum, A.S., (2003). *Computer Networks*. 4th ed. Prentice Hall.

- Thomas, S.A., (2000). *SSL & TLS Essentials*. Securing the Web. Wiley.

- Zwicky, E.D., (2000). *Building Internet Firewalls,*. 2nd ed. O'Reilly Media.