

Pearson Institute of Higher Education

Social Practices and Security

ITSC311 - Assignment

**Nompumelelo Mtshatsheni - Student Number: BXMDLL7W9
4-30-2020**

Table of Contents

Question 1 City of Johannesburg Security Breach – Scenario.....	2
Question 2 DDos and DOS - Scenario	4
Question 3 Caesar Cipher Key.....	14
Bibliography	17

Question 1 City of Johannesburg Security Breach – Scenario

1.1 In order to prevent for further attacks, I would use the Top-Down Approach

Top-Down Approach allow for quick decision making, when looking to solve a problem, it is done by looking backwards on what may have caused the issue

- It does not make a difference between high-frequency low severity and low-frequency high severity events (Chandana, 2020)
- Hence the top-level system and bottom level sub systems are not connected directly but they have the interaction through the other middle level-sub system.
- It allows for clear development and management to operate the system

1.2 Laws that the City of Johannesburg can use to prosecute attackers on online systems:

- Electronic Communications and Transactions(ECT) Act 25 of 2002, Section 86(1): Unauthorized access to, interception of or interference with data, states that subject to the Interception and Monitoring Prohibition Act ,1992(Act No.127 of 1992), states that any person who intentionally have access to any type of data without an authorization to do it, is automatically guilty of an offence
- Section 87(2): Phishing is known as an offence under section 87(2) on the ECT Act, which states that any person that commits an offence with the intent of getting an unlawful advantage by forging data to be produced with the intention to make it look like real information; the person can either pay a fine in which the value is not specific, or spend time in jail on a maximum of 5 years (Ameer-Mia, Pienaar, & Kekana, 2019)

1.3 The above scenario is regarded to be an incident, because it has disrupted all the normal or daily operations of the entire city, causing chaos and delaying several kinds of transactions

1.4 A migration procedure plan consists of seven steps for securing information in any organization, and it is highly effective in project launch. This is to help prepare, extract, and even transform the correct quality of the information in any city (Nordic Backup, 2020).

- The layout of data
- To plan the size of scope
- Backup all information
- Asses staff about the migration procedure
- Performance of the migration plan

- Testing
 - Follow-up and maintenance
- (Nordic Backup, 2020)

Hence a migration procedure plan for the City of Johannesburg for that incident that occurred will have to follow-up and maintenance of data migration plan because not did the city lose an entire day of works. When an incident occurs without any warning signs, simply indicates that most organization will be exploited and hospitals suffer the most, some do not have a backup generator, it will allow for testing data migration process even when the information is corrupted, ensuring that all the information is kept safe and nothing is missing or incomplete. It can restore all files before the inconvenience happened. This plan will have to prepare the City of Johannesburg for future shut down

1.5 A business continuity strategy is a procedure for establishing a system of avoidance and to recover from potential threats in an organization. The information officer can implement a crisis management plan, not only will he/she be able to get communications running on time, and preparing all the staff members about the way forward

- The crisis management plan, this provides communication mechanism, very essential to the safety of workers. Happens to provide preliminary data as well as direction to organize an ongoing task
- The disaster recovery plan typically about the plans to take on essential information and all applications are enabled for the business procedures
- The business continuity plan it incorporates the extension of occupational activities (Goff, 2020)

Question 2 DDos and DOS - Scenario

2.1

- A distributed denial of services attack is when hackers make an attempt to crash an online system by loading it with unnecessary data; (Petters, 2020)
- However, it mostly attacks online services and targeted websites. Their purpose is to overpower those services with a lot of traffic than the network usually accommodates, only to make the website deadly.
- The amount of traffic may consist of forged packets, more requests for connection or more incoming messages.
- Some of the network layers in the OSI model suffer DDoS attacks for example, in the network layer, which is layer 3, the attacks can be known as Internet Control Message Protocol Floods, and Internet Protocol/ Internet Control Message Protocol Fragmentation. In layer 4 which is the transport layer, the attacks may include Transmission Control Protocol connection exhaustion. (Weisman, 2020)
- Hacked computers or bots can be referred to as zombie computers, which can form “botnet”, which are used to overload the websites with more data that they can handle. Botnets use a large amount of data to exceed the large amount of data that the targeted victim uses (Weisman, 2020)
- A Denial of Service attacks consists of many kinds of attacks in which their main design purpose, is to disturb services. Most companies make use of DoS to perform stress testing on their networks. (Petters, 2020)
- DoS can also be a type of service attack in which a group of computers are used to overflow a server with Transmission Control Protocol and User Datagram Protocol packets; they are also used to individually shut down machines and networks, in order for them not to be used by other users (Keary, 2018)
- On the other hand, DDoS occurs when a group of systems target a single or unique system with a Denial of Service attack; therefore the targeted network will be getting a large amount of packets from different locations. (Keary, 2018)

2.2 Steps to prevent a DDoS attack

- **Build redundancy into the infrastructure:** by doing this, makes it hard for any attacker to launch a DDoS attack on your servers, and also spreading those servers across various data centers with good load balancing system in order to make it easier to distribute the traffic between them; also, it can be very effective if the data centers be located in various locations across the country, and ensuring that those data centers be connected to different networks, and that there no single point of failures (Rubens, 2018)
- **Configuration of the network hardware against DDoS attacks:** by having a configuration on the firewall or the router to drop incoming Internet Mess0age Control Protocol packets or to prevent DNS responses that are not part of your

network, or are outside, doing so by blocking UDP port number 53 (Rubens, 2018)

- **Increase bandwidth:** it is important to have more bandwidth than the attacker can handle, in order for you to deal with spikes in traffic that can be caused by a malicious threat (Rubens, 2018)
- **Outsourcing:** by having providers to make implementation of cloud scrubbing services to fight attack traffic in order to remove the biggest part of the traffic causing the problem, before it causes damage on the victims' network; it is advisable that those measures are done before having to suffer an attack, in order to have a quick response in case it happens (Kartch, 2016)
- **Activation of a WAF (Web Application Firewall):** is layer of protection that stays between a website and the amount of traffic that the website receives
- **Incident Response Plan:** one must ready to implement a good response program, and include a DDoS mitigation plan in order to succeed with the quick response

2.3 A security strategy for an organization is particularly important considering that most unauthorized users tend to take advantage and reuse someone else's work as they own. A successful security strategy is inclusive and dynamic, with the flexibility to react to any sort of security threat.

Henceforth, a detailed process that includes detailed estimation, design, execution, and constant supervising as well as to counter possible dangers and defenselessness to the network security. There are so many types of security strategies especially when it comes to protecting a mainframe of any organization. I will be focusing on two security strategies to prevent a cyber-attack on any organization. (Essay Sauce, 2019)

The requirement for security is important and vital for organization survival. It cut beyond all zones of life from delivering protection and offering protection for lands for which are non-living objects. ((n.a), 2020) It expands to a pc as the number of workstations keeps increasing, they used to store important data about every organization including the staff members. It also requires protection we bring to our pcs.

It is especially important to have a unique password that has eight letters long including numbers and symbols, as well as the username. Thus, it is used to avoid unauthorized entrée to any pc network and assets. It can available for private and public users with limited access This question evaluates the two major network security strategies which can be layered within an organization (Essay Sauce, 2019)

A. Layered Security

- It is the preparation of merging numerous mitigating security mechanisms to safeguard all the resources and information (Williams, 2020)
- Hence, it can be done at any phase of the completed data approach
- It improves the security of the network from as little as a small home network to a big organization network (Williams, 2020)
- The major purpose behind a layered network is that it used a defense network. Hence, it will be ending failing to add various layers that will cover the entire fault of a security layer (Williams, 2020)
- The use of a firewall, encryption to protect data are commonly used as a layered security strategy to prevent intruders' access
- It includes the use of a firewall, malware scanner, intrusion detection, encryption to protect information resources securely that intruders cannot have access to. (Williams, 2020)
- It helps to stop network seize from numerous incidents
- To implement a safely used layered security strategy defense in an organization, will be looking at a firewall and how it is layered into an organization (Williams, 2020)

❖ Firewall

- A network security machine that checks incoming and outgoing web traffic
- It permits packets centered on a set of rules
- The main purpose is to set up a wall in the middle of your internal network and as well returning traffic flow from the external resources in request to block all malicious viruses
- It can software, hardware or both

- How it works

- It analyzes all the incoming traffic flow based on pre-formed procedures and filter traffic arriving from unsafe sources
- Uses ports in exchange for information
- It validates access
- To be able to manage and control the entire network traffic
- Hence in case of emergency, it will record and report on events
- Happen to have its own drawbacks this is only because of the high-speed connection. (Barbish, 2020)

- Methods to controlling traffic

- Packet filtering, small chunks of information are evaluated alongside a set of filters, hence the packets that get through the filters are sent to into the system.
- Proxy service, data from the internet will be retrieved by a firewall

- Review, this is a new method which does not inspect the substances of each data, but instead evaluates a variety of parts moving within the firewall to the separate to be monitored for defining all the incoming data, once data is not processed it will be rejected
- **Ways most people deceitful use to access or abuse unprotected computers**
 - Remote login, occurs when somebody is capable to link to your pc and command it in from a distance, competent to see or access your documents
 - Application backdoor - platforms have unique attributes that will permit a for wireless access and at some point, be control the program
 - Denial of service, this attack is closely difficult to counteract. It will occur when the hacker transmits an invitation to the server to connect to it, the replies from the server along with an acceptance will try to set up a new session, unable to find the system that established the request, making the pc to eventually crash after continues of unanswerable requests
 - Viruses, most understood risk for pc viruses. A virus is a tiny system that know how to photocopy itself to more pcs, it happens spread too quickly from one structure to the next and wipe out all your data.
 - Spam, naturally nontoxic but continuously irritating, spam is the automated equivalent of junk mail, and it can be highly dangerous (Tyson, 2020)
- **Steps to implement a firewall**
 - ❖ Step 1: Secure your firewall
 - Securing your firewall is the first and most crucial step of this procedure
 - To update the firewall to the most recent firmware
 - Being able to remove, deactivate, or change name for any defaulting client current account and by also adjusting all default passwords. Ensuring that only to use complicated and protected secret code.
 - Provision that numerous managers want to oversee the firewall, hence creating an extra official/managers current account together with reduced licenses established on obligations and certainly not use shared user accounts

- Deactivating SNMP simple network management protocol (Skarda, 2019)
- ❖ Step 2: Architect your firewall zones and IP addresses
- Firstly, by protecting all the important resources on the network, having to plan out the network framework for the resources to be grouped together and positioned into networks based on the understanding level
 - The more zones generated, the more network is protected, handling more zones needs extra time and supplies, hence careful planning is taken seriously
 - When using IP version 4, internal IP addresses must be utilized for the entire network, NAT will be required to be configured to permit any internal procedures to transmit on the internet when required.
 - After the intended structure of the network, the zone is completed and launched alongside matching IP addresses, the user will be ready to establish the firewall zone as well as allocate the interfaces and sub-interfaces within the firewall. Building a network infrastructure all the knobs/switches support VLANs (virtual LANs) which is used to sustain the level two separation amongst the networks (Skarda, 2019)
- ❖ Step 3: Configure access control lists
- To establish all the network zones and having to assign them interfaces, the need to determine precisely which interchange needs to flow into and out of every zone
 - Traffic will be allowed using the access control list (ACLs) – one on the firewall rules, they are applied for each interface or sub-interface
 - ACL are more specific in knowing what source or which IP address and port numbers are available
 - The ACL ensures that all unproved traffic does not get filtered, when applying the inbound and outbound access control list for all the interfaces inside the firewall, will have gained access to the traffic and zones
 - To disable all unencrypted protocols for managing (mostly looking at telnet and HTTP connections), and the secure shell and web interfaces from the public contact, this ensures that the firewall is secure and having to not deal with intruders (Skarda, 2019)

- ❖ Step 4: Configure your other firewall services and logging
 - The firewall can use DHCP servers and NTP (network time protocol) server. Being able to configure and disable all services that are no longer needed
 - The PCI DSS obligation is to configure the firewall for the logging server as well ensuring that there is enough information to satisfy the obligation of 10.2 – 10.3 for the PCI DSS (Skarda, 2019)
- ❖ Step 5: Test your firewall configuration
 - To be able to verify the firewall abilities as expected
 - The verification of the firewall will be blocking all traffic that is not needed for the ACL configuration
 - The testing of the firewall should include vulnerability and infiltration testing
 - After concluding all the testing of the firewall, the production should be ready. The most important part is to have a backup of the firewall configuration protected location in case of a hardware failure (Skarda, 2019)
 - Using tutorials will help a lot, and when configuring the network make sure that there is security expert to review all the steps that were followed (Skarda, 2019)
- ❖ Step 6: Firewall management
 - While the firewall is still in manufacturing, and you have already completed the firewall arrangement, and yet the firewall administration just launched, all the logs require to be observed, and the firmware is required to be restructured, the defenselessness will scan what needs to be completed, and the rulebooks must be revised at least every six months. (Skarda, 2019)
 - Documenting all the progress about the performance regarding constant responsibilities to guarantee that the firewall maintains the protection over the network (Skarda, 2019)

- **To implement a layered security strategy within the organization, one needs to consider a lot of security measures or layers especially when dealing with a cyber attack**

- Firstly, system-level security. It simply ensures that all staff members have been properly been constituted in the best way possible to prevent attacks against the system. It happens to incorporate all the organizational roles by assigning user usage for gaining access to information (Williams, 2020)
- Secondly, network-level security. This protects the entire organization network from intruders, it includes a firewall to verify protocols and as well as controlling the traffic of the network (Williams, 2020)
- Thirdly, application-level security. An important role of a layered security strategy, it knocks down entry to vital procedure tasks by making operators log in with a username and password allocated by a certified expert. (Williams, 2020)
- Fourthly, device-level security. By installing a full endpoint defense results, it can be time exhausting, as all pcs, cellphones and as well as a router have unique default settings. It is very vital to close all entry points that a hacker might exploit (Williams, 2020)

B. Defense in Depth Strategy (DiD)

- An attempt to cybersecurity defending procedures that are layered in a way to shield important records of information.
- This multi-covered method with intended redundancies boosts of the security system it will tackle unique attack routes ((n.a), 2020)
- To use a more complete safety strategy than that of the layered security
- A thorough and well-executed DiD stops a network system from various outbreaks and as well as establishing a real-time alarm for arriving interference for the network administrator
- It attends an effective method of avoiding resolving automated outbreaks that arise from the same shared network (Essay Sauce, 2019)
- In such an attack, the attacker will try to attack the network system from different angles using different methods that can be difficult to prevent, DiD with multiple layered security can protect the system ((n.a), 2020)
- It uses a VPN, intrusion detection system (IDS) are a fragment of the DiD strategy applied to avoid unlawful gain access to an organization network
- By combing both the IDS and VPN, will create a barrier for all types of attackers to easily infiltrate through the network system
- DiD is authenticated by experts to defend an organization network against invasion and attackers (Essay Sauce, 2019)
- It is flexible for having to protect a pc against new raising threats, one layer of DiD has a mixed implementation of security controls which can uncover attacks way before they could enter the network security ((n.a), 2020)
- To implement an effectively used defense-in depth strategy in an organization, will be looking at an intrusion detection system and how it is layered into an organization

❖ **Intrusion Detection System**

- Brief opening about intrusion

- The nature crime of pcs is impulsive from previous threats
- The increase in connectivity and complication
- An increase in availability of important data and attacks are launched inside the network and the dependency over issued services (Tan, 2020)
- the danger exists, intrusion tends to get out of control namely all the loge files are exposed and there is a loss in reputation, confidentiality and important information (Tan, 2020)

- What is intrusion detection

- A system that evaluates in genuine time
- To be able to detect excess, avoids visible signs of attacks against the information
- It is also a hardware and software built for most pcs that monitors network movement
- The main goal is to positively recognize all true attacks as well as negatively classifying all non-attacks

- Why intrusion detection so important

- The opportunity to stop an attack before destroying the network, no damage control can be handled
- Data gathering for any attack and trying to prevent it from happening again
- It requires a lot of time and correct answer (Tan, 2020)

- How intrusion detection system works

- To enable the detection for all external hackers and internal network-established incidents
- Could be surmounted easily having to provide a layer of protection for the entire network
- Can either be a NIDS or HIDS (Boubaker, 2012)

- Techniques used to implement IDS based on two aspects

- Behavioral approach: is constructed on tracing the behavior of a client, assistance for any application to assume a feasible

intrusion. It uses probabilistic technique to estimate all the specific traffic (Boubaker, 2012)

- Scenario-based approach: the main purpose of this approach is built around techniques that are known and used by hackers to accomplish invasions. Although making use of a signature, for parallel behavior of the user without any alternative for its record to regulate if this behavior is legal or not. Signatures are sequences of procedures for examining packets that flow through the network, by ensuring that the use of both approaches in similarity will provide an effective solution for intrusion detection. (Boubaker, 2012)

- **The nodes are established agreeing to the following:**

- Disturbances from the internet are found before they are cleaned by the firewall, simply implies that the situation is upstream
- Disturbances that must surpass the firewall and whose control it has inside the network implies it is downstream
- Invasions from the internet within the network are supervised by the DMZ and later discovered by a sensor established prior to the zone.

- **Steps of implementation**

- ❖ Step 1: To install an antivirus internet on the central server
 - The antivirus has a built-in IDS
 - Database signals any rule that needs to be automatically be viewed on a website
 - Pcs linked to the network operate as users and reclaim all the updated server containing all the new features on an intrusion detection (Boubaker, 2012)
 - By providing the functionality on intrusion detector along with the host-reaction as it only succeeds to block all potential attacks
- ❖ Step 2: To install an intrusion detection SNORT
 - This is to alert all different nodes of the network so that the intrusion attempts are logged into the log file
 - All attempts are physically blocked by a firewall and SNORT does not or else the intrusion detector will alert the system by placing an entry log file
 - Having to include signatures for intrusion, the network will operate parallel to SNORT, ensuring that all detected entries blocked and denied (Boubaker, 2012)

- **To implement a defense-in depth within the organization, one needs to consider a lot of security measures or layers especially when dealing with a cyber attack**
 - Firstly, network security. Things like the remote access, proxy content filters and as well as the wireless security (Mason, 2019)
 - Secondly, application security. This deals with movement examining every application and app the organization is currently using, the testing of the firewall application and database (Mason, 2019)
 - Thirdly, endpoint security. It normally ensures that all the devices accessing the network of the organization either by a remote or even wirelessly, the contented security is fully functional (Mason, 2019)
 - Fourthly, the administrative security. This approach ensures that all the procedures have increased in information protection and all the policies are being regulated quarterly (Mason, 2019)

2.4 The layered and DiD are two unlike approaches. They both take part in which one is better to be used. The layered security is crucial for strongly defending the network by offering a security check at each level within the network structure. Although, the DiD expands the range of the layered security strategy to include the system that will react to all incoming risks before the network is damaged. ((n.a), 2020)

A layered security strategy occurred to shelter all the malfunction of every single factor within the security organization network by placing completely different security mechanisms hooked on a tactic with the intention of guarding the system from interference. Whereas, the DiD arises from the suppose that a network security warning, can each occur by a specific solution. As an alternative placing a defense structure to examine and warn for any impending danger (Essay Sauce, 2019)

In conclusion, layered security known to offer various tiers of security, it is not expensive and simpler to execute compared to DiD strategy. Thus, it makes client availability simpler, and the drawback can increase the expenditure of the organization's resources anticipated for a fruitful attack (Essay Sauce, 2019). Hence, it has been validated by specialists that a DiD is tougher in conditions of offering a network that studies tend to propose, that the utilization of DiD in real-time warnings to inform about a threat and as well as the avoidance method. Therefore, the elasticity presented by the DiD to safeguard against freshly identified risk and vitality in tackling warnings. (Essay Sauce, 2019)

Question 3 Caesar Cipher Key

3.1 It is used to encrypt and decrypt messages.

PLAINTEXT	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
CIPHERTEXT	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

Bob's Message	Encrypted Message
l	F
e	b
n	k
j	g
o	l
y	v
s	p
t	q
u	r
d	a
y	v
i	f
n	k
g	d
i	f
n	k
f	c
o	l
r	o

m	l
a	x
t	g
i	f
o	l
n	k
t	q
e	b
c	z
h	e
n	k
o	l
l	i
o	l
g	d
y	v
a	x
t	q
P	M
l	F
H	E
E	B

I enjoy studying information technology at PIHE -> F bkglv pqravfkd fkclojxqflk
qbzeklildv xq MFEB

3.2 Transposition cipher is used to inverse the request of the plaintext

A	P	P	L	E
1	4	5	3	2
l	e	n	y	o
y	s	t	u	d
y	i	n	g	i
n	f	o	r	m
a	t	i	o	n
t	e	c	h	n
o	l	o	g	y
a	t	P	l	H
E				

lyynatoaEodimnnyHjugrohqlsifteltntnoycoP

Bibliography

- (n.a). (2020, May 3). *Forcepoint* . Retrieved from Cyber Edu Defense in Depth:
<https://www.forcepoint.com/cyber-edu/defense-depth>
- Ameer-Mia, F., Pienaar, C., & Kekana, N. (2019, October 22). *ICLG.com*. Retrieved April 11, 2020, from iclg.com: <https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/south-africa>
- Barbish, J. (. (2020, April 5). *Chapter 29. Firewalls*. Retrieved from Firewall:
https://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/firewalls.html
- Boubaker, A. (2012, May 1). *Computer Science Issues Vol.9*. Retrieved from Core:
<https://core.ac.uk/download/pdf/25765693.pdf>
- Chandana. (2020, March 5). *SimpliLearn*. Retrieved April 13, 2020, from SimpliLearn:
<https://www.simplilearn.com/top-down-approach-vs-bottom-up-approach-article>
- Essay Sauce, (. (2019). *Essay Sauce*. Retrieved from <https://www.essaysauce.com/computer-science-essays/layered-security-and-defense-in-depth-network-security-strategies/>
- Goff, D. 2. (2020, April 5). *KnowledgeLeader Blog*. Retrieved from Business Continuity Managemnet (BCM): <https://info.knowledgeleader.com/business-continuity-management-defined-and-outlined>
- Kartch, R. (2016, November 21). *Software Engineering Institute*. Retrieved April 12, 2020, from Insights.sei.cmu.edu: https://insights.sei.cmu.edu/sei_blog/2016/11/distributed-denial-of-service-attacks-four-best-practices-for-prevention-and-response.html
- Keary, T. (2018, November 21). *Comparitech*. Retrieved April 6, 2020, from Comparitech:
<https://www.comparitech.com/net-admin/dos-vs-ddos-attacks-differences-prevention/>
- Mason, M. (. (2019). *Global Banking & Finance Review*. Retrieved from How to implement a defense-in-depth security: <https://www.globalbankingandfinance.com/how-to-implement-defense-in-depth-security/>
- Nordic Backup*. (2020, April 5). Retrieved from Data Migration Plan: <https://nordic-backup.com/blog/7-steps-data-migration-plan/>
- Petters, J. (2020, March 29). *Varonis*. Retrieved April 5, 2020, from Varonis:
<https://www.varonis.com/blog/what-is-a-ddos-attack/>
- Rubens, P. (2018, June 26). *eSecurity Planet*. Retrieved April 12, 2020, from esecuritypanel.com:
<https://www.esecurityplanet.com/network-security/how-to-prevent-ddos-attacks.html>
- Skarda, C. (2019, September 19). *Security Metrics*. Retrieved from
<https://www.securitymetrics.com/blog/how-configure-firewall-5-steps>

- Tan, L. &. (2020, April 5). *Study Lib Net*. Retrieved from Intrusion Detection System (IDS):
<https://studylib.net/doc/9585042/intrusion-detection-system--ids->
- Tyson, J. (2020, April 5). Retrieved from How Stuff Works:
<https://computer.howstuffworks.com/firewall.htm>
- Weisman, S. (2020). *Norton*. Retrieved April 06, 2020, from Emerging Threats:
<https://us.norton.com/internetsecurity-emerging-threats-what-is-a-ddos-attack-30sectech-by-norton.html>
- Williams, M. 2. (2020, May 3). *Faronics - THE 4 ESSENTIAL COMPONENTS OF AN EFFECTIVE LAYERED SECURITY STRATEGY*. Retrieved from Faronics: <https://www.faronics.com/news/blog/the-4-essential-components-of-an-effective-layered-security-strategy>