Cyber Security Assessment

# Task 1: Part a

# Frauds and Scams over the Internet

Today World Wide Web is the major source of data around the world. Computer Networks are used to support the web applications that are widely used by millions of people around the world and have large number of data resources associated with them. These applications have flaws and are vulnerable to different type of attacks. People lose their data, money, information and other important resources due to the frauds and scams over the internet.

Given below are the most common and frequent scam and fraud attacks on a computer network over the internet.

## Man-in-the-middle Attack

This attack is based on the interception of the communication between two parties i.e. users or clients over the internet. Basically the client and server are connected using the TCP connection. So, the attacker creates another TCP connect by splitting the client and server connection. Now user is connected to attacker’s machine and that is then connected to server. In this way all of the communication between user/client and server is intercepted by the attacker.

### Prevention of Attack

The man-in-the-middle attack can be prevented using strong encryption on both sides i.e. on the machine of the client and on the server side.

## Phishing Attacks

These attacks attempt to steal sensitive data and access to credible resources of a system or a user by fraudulent electronic communication and deceiving the victim to compromise its information and resources to the attacker. Mostly these attacks are activated when the user/victim clicks a malicious link or downloads a harmful software of file.

Besides, phishing is regularly used to deceive users and systems during a major attack. In this last situation, representatives need to take action to find the remedy of the attacks on their organization or computer networks. Otherwise, attackers will have the secret information and control over the resources.

### Prevention of Attack

There are four measures to protect yourself against phishing attacks

1. Using a security software that detect these attacks and helps protect your computer
2. If you use multi-factor authentication, phishing attacks can be avoided
3. Frequently updating your software, computers, mobile phones etc.
4. Save your data as a backup on some machine or on a cloud platform.

## SQL injection and Cross-Site Scripting (XSS) Attack

These attacks are mostly done via web applications. Basically these are a type of code injection attack where the malicious script or code is injected into the web applications and the attacker gains the control over the data and resources of that application. It is used to steal information, redirect users to malicious websites and gain control over resources like database, cookies and admin credentials etc.

Client data is compromised in this attack and if the attack on a larger scale, it effects millions of people. Attackers exploit the system and applications for a long time to find any vulnerabilities and flaws. When session cookies are uncovered, they are now ready to mimic substantial clients and misuse their private records and information.

### Prevention of Attack

The best measure to avoid and protect your application against these attacks is to encode and filter special characters in the user input. Also the encryption does not allow attackers script to run on the server.

## Part b:

## Protection of the Network from Data Theft over the Internet:

Some of top most effective techniques and measures to prevent attacks over the internet are given below. These measure help us to secure the information, data and resources.

### End-to-End encryption:

Even if the communication is intercepted, it is not meaningful or understandable and can’t be decrypted without the encryption keys.

### Multi-factor Authentication:

This measure will help avoid the phishing attacks and secure your system from data theft and unauthorized communication.

### Encoding the User Input:

It is fundamentally the most important part to handle the malicious input and secure your application from code injection attacks. There are different types of encoding respective to the user input i.e. HTML, JavaScript, attribute, URL and script encoding.

# Task 2: Part a

## Software Solutions for Malware and spyware with Appropriate Tools

Given below are two of the top most algorithms and techniques used widely to protect the computer systems against the threats created by malware and spyware.

### Advanced Encryption Standard (AES):

It is the standard encryption algorithm trusted by the U.S government. It is in 128-bit form and very efficient and effective. In case of severe type of encryption it uses 256 bits for this purpose.

It is qualified to be impenetrable to all kinds of attacks except the brute force attack. AES has the potential to become the standard in the encryption and eventually used in the private sector.

### Blowfish:

It is a symmetric cipher. Creates blocks of 64 bits for each message and then encrypt them one by one. It is extremely fast in terms of speed and highly effective in the domain of encryption. It is freely available in public domain.

It is one of the most flexible methods for encryption. Applications of blowfish can be found in the big industries like e-commerce, secure payments and password management tools. It is highly effective in securing the networks and protecting passwords and important information.

## Appropriate Tools for System Protection

Given below are some of the more advanced tools used in the industry and especially trusted by users for establishing protection against malware and spyware in the computer systems.

### Norton:

It is considered as one of top defenders against malware. It allows the users to scan there system for any malware and suspicious behavior. It has a large database for virus definitions that helps improve the security and malware detection for a computer.

Norton has an emulator for untrusted software and it runs these types of software in a separate environment to analyze the behavior of these programs. So, in this way the malicious software can be emulated and executed without harming the system.

### BitDefender:

It contains a distributed architecture. For different types of files and malware it has unique scanning engines. It has different kinds of plug-ins and each one is responsible for detection and removal of a specific malware. It can be deployed and used in different environments based upon its impressive modularized architecture.

BitDefender is completely independent of the platform and it is easily portable. It provides compatibility at binary level. This software tool is largely independent from the host operating system and this makes the detection more efficient without having any compatibility issues for any environment and operating system.

### MalwareBytes:

Fast and efficient scanning is one of the key features of this tool. MalwareBytes Anti-Malware completely removes the existing virus infections. It has its own “Chameleon” technology which allows it to get installed and execute on the infected systems which do not allow other security software to operate.

The best feature of this tool is the “real-time protection” and “heuristic scanning method”. Previously unknown malicious software infections are detected by analyzing their behavior and influence on the computer system. This makes this modern security software very efficient and effective. In this way it takes care of new and emerging threats.

## Part b:

### New Zealand Legislation for Cyber Crimes:

There were no adequate and appropriate laws for cyber-crimes before 2003 in New Zealand. The *Crimes Amendment Act 2003* addressed most of the issues and given a lot of benefit to the country’s IT industry. The Act gives provision to law enforcement agencies to investigate and hunt hacking/cracking and other cyber-crimes. This methodology flags the Government's promise to empowering New Zealand and New Zealanders to flourish on the web. However, we can possibly accomplish that on the off chance that we cooperate. New Zealand's little scope and generally basic media communications and system structure empowers people in general and private segment to work intently together to install a digital security culture, and to react to advancing digital dangers. New Zealand cyber security strategy is a cutting edge, dynamic, safe and universally adaptable. The digital security framework is developing. New foundations like CERT NZ have been set up and all our administration offices with digital security obligations are building noteworthy associations over the framework, both locally and universally.

The openness of the internet to millions of users around the globe and free access to number of resources is a piece of its extraordinary worth – taking into account unhindered cooperation and the free progression of data. Individuals should have the option to work in the computerized world sure that their security will be ensured and that their private and money related subtleties will be ensured. They ought to have the option to connect with online without enduring mischief or unlawful obstruction, and have the option to seek after crook and shopper change when things turn out badly. Human rights ought to be secured online as they are disconnected. Worldwide and local law correspondingly apply online as disconnected. This incorporates the privilege to opportunity of articulation, and the insurance of security, as set out in New Zealand law and existing worldwide law.

Following are the guiding principles of New Zealand’s cyber security strategy.

1. Build and maintain trust
2. Agile and adaptive
3. People centric and respectful
4. Strong accountability
5. Collaborations for better performance and collective work

New Zealand has established a capable and strong workforce for coping with cyber-crimes and related incidents. Some of key features of this workforce are listed below.

1. Encouraging the growth of cyber security workers
2. Supporting industry and private organizations for promoting cyber security management
3. Developing a world class cyber security academia
4. Evolving cyber security research to a higher index
5. Incentivizing industry for its role in promoting cyber security

One of the best strategy created by New Zealand is to proactively tackle the cyber security issues. It includes investigating the crime proactively and collaboration to deter and respond against the cyber-enabled crime and terrorist use of the internet by fraud elements. The digital security landscape will keep on changing with new advances, dangers and openings developing. Foreseeing the future won't get simpler, so our capacity and eagerness to adjust to change and work together is basic.

# Task 3: Part a

## Denial of Service (DoS) Attacks:

The main goal of these type of attacks is to exhaust the system resources, so that it does the respond in the intended way. Given below are some of the most frequent and destruction denial of service (DoS) attacks.

You don't need to look any further than the last year's Dyn occurrence to perceive how your business could be diminished to a substance attempting to rebuild its reputation and pipeline. In a solitary end of the week, the most noticeably terrible conveyed refusal of administration assault in history smashed the world's biggest internet providers. Twitter, Reddit, The New York Times, and PayPal were only a portion of the huge locales that went down because of assault. The detailed harm from this malevolent assault for Dyn was lost 8% of its business. The brutality of the message sent for computerized undertakings was limitless.

The advancement of DoS attacks give no indications of easing back. They continue developing in volume and recurrence, today most usually including a "blended" or "hybrid" approach. Without early threat detection and traffic profiling frameworks, it's difficult to know they're here. Truth be told, odds are you think about it just when your site slows down or crashes.

This is particularly valid for complex attacks, which utilize a blended methodology and focus on various levels at the same time. These type of attacks target information, applications, and framework at the same time to expand the odds of its progress. To battle them, you need a fight plan, just as dependable DoS counteraction and moderation arrangements. You need a coordinated security technique that ensures all foundation levels.

### TCP SYN Flood Attack:

It occurs during the TCP handshake protocol at the beginning of the communication when the server is acknowledging and authenticating the user. Send massive amount requests to a server that fills up its queue and it no longer responds in the intended way or it may crash in this situation.

A SYN flood (half-open assault) is a sort of DDoS attack which expects to make a worker inaccessible to genuine traffic by expending all accessible worker assets. By consistently sending (SYN) bundles, the attacker can overpower every single accessible port on worker machine, making the target device react to real traffic drowsily or not in any manner. In administration of systems inside the organizations and the networking of it, when a connection is left open by a user or victim however the machine on the other sided has not closed the connection isn't, the connection is called or known as half-open. In this sort of an attack, the targeted server is constantly leaving open connections and hanging tight for every connection with the time interval after which the accessible ports can be used for more operations. So, often half-open attacks happens in this context which are in turn the result of the above situation.

### Botnets Attack:

It includes bots or zombie systems that attack the targeted system on the behalf of an attacker. A large number of these bots together create a distributed denial of service (DDoS) attack. This makes the DDoS attack more complex and untraceable as the bots/machines are spread across a wide area of coverage with respect to geographical locations.

The name is a derived from the robot and in network systems each compromised device is labeled as bot usually. Botnets are used for bad purpose often, in order to achieve the malevolent actions and aims such as spam to the users, user information being hijacked or leaked, ransomware, falsely tapping on advertisements or appropriated DDoS attacks. Some of the malwares, for example, ransomware, will directly affect the proprietor of the device, DDoS botnet malware can have various degrees of deceivability; some malware is intended to assume all out responsibility for a device, while other malware runs quietly as a foundation procedure while standing by quietly for guidelines from the aggressor or "bot herder."

Self-proliferating botnets enlist extra bots through a wide range of channels. Pathways for infection incorporate the abuse of site weaknesses, Trojan pony malware, and splitting powerless verification to increase distant access. When access has been acquired, these strategies for infection bring about the establishment of malware on the objective gadget, permitting controller by the administrator of the botnet. When a device is tainted, it might endeavor to self-engender the botnet malware by selecting other equipment devices in the encompassing system.

# Task 3: Part b:

## Components used in the Network Design

Given below are some of the basic components that should be considered during the designing phase of a computer network.

### Denial of Service (DoS) Response Plan:

The countermeasures for a DoS attack should be well defined and prepared beforehand. For a comprehensive and effective response strategy this is a very important and crucial step.

### System Checklist:

You should have a complete and accurate list of each of the resources on your computer network. This helps in the threat detection and prevention. Make sure that the filtering tools, hardware and software level security protections are in place.

### List of Contacts:

Clearly mention the list of internal and external contacts for informing when the denial of service attack happens. Keep in view dealing with the customers, communication with cloud service providers and other vendors at that time.

## Tools considered for Network Protection

### Avast Antivirus:

Avast provides a smart scan which detects malware and outdated software and removes any files or software that compromises the security of computer. It matches all the files with the virus records and virus definitions in order to find the untrusted or malicious software.

One of main benefits of Avast is the “Boot-Time Scan”. This is done during the startup of the system, this is the time when malware are inactive and can’t do any damage. So scanning at this time clean the system before any malware is launched. Thus malware is detected and removed from the computer before it can counteract or activate itself.

### McAfree Antivirus Software:

It is one of the best tools for protecting your system against malware and spyware. It contains a virus database that is maintained and updated regularly with the data collected through a web crawler. It collects the names of all the malicious software names and harmful file extensions that may cause damages to the user system and compromise its data and resources. It strengthens the firewall of a computer using the virus database. Scans the whole computer for any malware or corrupted files and deletes or kills any file and software that contains a malware.

# Task 4: Part a) Important Tools for Network Security

Given the rising tide of wholesale fraud and different perils identified with the burglary of individual data, numerous clients are as of now reluctant with regards to offering information to organizations. What's more, if a cyberattack ought to happen, a large number of these clients are probably going to pull back for safer other options. The misfortune or defilement of important information, alongside a huge disturbance to client administrations and inner procedure, finished off with reputational injury that may endure long after different harms have been fixed — it's not hard to perceive what's in question with regards to organize security. Truth be told, it's been recommended that 66 percent of SMBs4 would need to close down (either incidentally or for all time) subsequent to encountering an information break. Furthermore, considerably bigger, more settled organizations might be not able to recover their previous standing. Your system faces dangers of every kind imaginable, and consequently ought to be set up to safeguard, recognize and react to a full scope of assaults. In any case, actually the greatest peril to most organizations are not here now gone again later danger entertainers, yet rather assailants that are very much supported and are focusing on explicit associations for explicit reasons. Hence, your system security methodology should have the option to address the different strategies these entertainers may utilize. Given below are some the top tools used to protect networks.

### Access Control:

It is a technique to pose restriction and hindrance upon a system and also include the other assets. It is a procedure by which clients can get to and are allowed sure privilege to frameworks, assets or data. It is a functionality for security that has command over who can see various angles, what can be seen and who can utilize assets in a registering domain. It is a basic idea that fatality for an association. To build up a safe framework, control of access via electronic method to systems are utilized and applied so they rely and comply with the client needs, access card readers, examining and reports to follow worker access to limited business areas and territories. These frameworks incorporate access control boards to restrict passage to delicate zones like cautions and lock down regions to forestall unapproved access or tasks. Access control frameworks perform recognizable proof, validation, and approval of clients and substances by assessing required login accreditations that may incorporate passwords, pins, bio-metric outputs or other verification factors. There is multifaceted validation which requires at least two confirmation factors which is frequently a significant piece of the layered guard to secure access control frameworks.

### Application Security:

Security for every application is one of the significant measures and in light of the fact that the present applications are being used worldwide by millions of customers and clients. They are regularly accessible over different systems and for most of them cloud deployment is on, expanding weaknesses to security threats and potential harm from attackers. There is expanding weight and motivation to guarantee and insure that provided will be the security at the system level as well as inside applications themselves. We can explain this in a way that today almost all of the programmers are using or related to some kind of applications with their chances of being attacked have increased a lot more today than ever before. The major aim of the testing process and procedures for the security and to safeguard the applications can help us visualize and understand the shortcomings and in this way the attacks can be avoided beforehand and attackers can be restricted from giving any harm to data or compromising the system.

### Web Security:

Essentially all organizations, most government offices, and numerous people presently have Websites. The quantity of people and organizations with Internet get to is extending quickly and these have graphical Web programs. Subsequently, organizations are excited for arrangements made for an office for the e-commerce buying and selling online on the internet. Yet, actually web applications are incredibly defenseless against different types of vulnerabilities. As organizations realize that their system and applications need protection against the outside attacks, the interest for secure Web administrations develops.

## Part b:

## Cryptography Methods

There are many aspects of security and numerous applications, extending from secure business and installments to private communication and ensuring human services data. One basic viewpoint for secure communication is that of cryptography. Cryptography plays a major in securing the communication between users and the systems. There is no reliable methods to achieve this without cryptography.

There are numerous perspectives to security and numerous applications, extending from secure trade and installments to private interchanges and ensuring medicinal services data. A few specialists contend that cryptography showed up suddenly at some point subsequent to composing was developed, with applications extending from strategic messages to war-time fight plans. One essential aspect for secure communication is that of cryptography. Be that as it may, it is essential to take note of that while cryptography is vital for secure communication, it isn't without anyone else adequate. It is advised to reader that the subjects secured here just depict the first of numerous means important for better security in any number of circumstances.

Cryptography is an old technique to secure the data; the main archived utilization of cryptography recorded as a hard copy goes back to around 1900 B.C. at the point when an Egyptian scientist utilized non-standard symbolic representations in an engraving. It is nothing unexpected that new types of cryptography came not long after across the board improvement of PC communication. In information and broadcast communications, cryptography is fundamental when imparting over any untrusted medium, which incorporates pretty much any system, especially the Internet.

### Triple Data Encryption standard (DES):

It has taken the place of the previous encryption techniques and works a lot better than most of them in cost and time. The older versions are cracked by the hackers already and the system exploitations were successful. So, the triple DES became the new method for securing the networks. It is highly recommended and one the most widely used symmetric algorithm in the industry. It uses 3 individual keys, each consisting 56 bits. It makes a hardware encryption solution that is dependable and can be used in financial services and other industries.

### Advanced Encryption Standard (AES):

It is standard encryption algorithm trusted by the U.S government. It is in 128-bit form and very efficient and effective. In case of severe type of encryption it uses 256 bits for this purpose. It is qualified to be impenetrable to all kinds of attacks except the brute force attack. AES has the potential to become the standard in the encryption and eventually used in the private sector. The key size of the DES was too small so there was a great need of a standard system that supports a longer key size and is more efficient. As the computing power of the hardware has increased over the last decade, DES is completely vulnerable against brute force key searching attacks and can be easily penetrated. In order to rid these limitations and overcome this problem the new encryption standard was created.

Some of the main features of AES are that it uses the symmetric key cipher, it has stronger and faster working methodology as compared the previous versions like DES and Triple DES, the design details and information about its specifications are provided and the programming languages for the development of this software include C and Java. Interestingly, the performance of the AES comprises on bytes and not bits. So the 128 bit text is taken as 10 bytes input. Now when bytes are attained, they are converted into four columns and four rows for and they are processed as a single matrix. Number of rounds in this standard are very peculiar and variant as compared to the older versions of the DES. The rounds depend upon the key length and size of that key. For 128 bits it will use 10 rounds and 14 rounds in case of the input containing 256 bits. Round key is calculated and modified using the original AES key.

### Blowfish:

It is a symmetric cipher. Creates blocks of 64 bits for each message and then encrypt them one by one. It is extremely fast in terms of speed and highly effective in the domain of encryption. It is freely available in public domain. It is one of the most flexible methods for encryption. Applications of blowfish can be found in the big industries like e-commerce, secure payments and password management tools. It is highly effective in securing the networks and protecting passwords and important information.

The encryption key is same as decryption key and thus we can say that this cipher is a symmetric cipher. The key is a very crucial secret hidden from all of the users but not the sender and receiver. A computer routine that takes an input in the form of plaintext and it is converted into the coded text which we also call cipher text. This routine is performed on the chunks of data which we call blocks. The key resembles the old decoder rings in oat boxes. Without it, you can't open the mystery in the distorted message on the grounds that solitary the key knows the entirety of the replacements and changes that were performed on the first content.

### Advantages of Blowfish:

Blowfish is a tremendously fast encryption tool which we can also call a cipher. It is very effective with a very simple and basic structure. Blowfish creates an extremely enormous key (think about a vigorous oat box decoder ring), and this by itself is an immense advantage to security. With the speed up PC preparing, Blowfish can make an any longer key so it is considerably harder to attempt to hack the key value. Its way of producing the sub-keys implies that each pair of sub-keys changes marginally as they are created. It will confuse the attackers and keeping them from making sense of how the sub-keys were created, and afterward accessing the various known keys. Blowfish is likely the fast block cipher as when it completes the key schedule during the encryption procedure.

It has sixteen number of rounds which is practically a very small number, thus we can say that it is a faster block cipher relatively. The simplicity of its round operation is very much appreciable and admirable as it has a very small number of modules and exclusive XORs to perform the complete encryption.

## Part c:

### Recommended Cryptography Methodology:

Based on the information collected on the cryptography methods for secure networks and algorithms described in the above section. My recommendations consist of the two advanced methodologies for this purpose:

1. Advanced Encryption Standard (AES): It is highly effective and also used by the American government as the standard of encryption for protecting computer networks. It is foolproof against most of the attacks.
2. Blowfish: It is fast and flexible. It is widely used in e-commerce industry and for securing payments which is very crucial element of an e-commerce website and network. So, it is one of the best option for securing networks.

# Task 5: Part a

### List of Hacking Tools for Exposing the Network Vulnerabilities:

1. Burp Suite (Web Security Tool)
2. Accunetix
3. Nesus (Network Security)
4. NMAP (Network Port Scanner)
5. Wireshark
6. Metasploit Framework (A Complete Toolset for Network Penetration)
7. Snort
8. John the Ripper
9. Aircrack-ng
10. SQLninja

### List of Tools for Protection against Hackers:

1. Norton
2. BitDefender
3. MalwareBytes
4. Avast Antivirus

## Recommendations to Avoid DoS Attacks:

Given below are measures to make a DoS attack harder for hackers to achieve and less severe for the computer system.

### Architecture:

1. Always create multiple servers at different locations
2. Separately allocate networks to the data centers
3. Create different paths for data centers

### Hardware:

In order to prevent a DoS attack, keep the hardware updated. Hardware upgrades are always very effective against the SYN flood attacks. So, in this way network and security hardware is capable of mitigating the DoS attack. Network firewalls are also a good measure to ensure the network protection against DoS attacks with high severity.

### Bandwidth:

One of the major background reasons for a DoS attack is that system resources are exhausted and bandwidth is the biggest player in this situation. Increase the bandwidth, higher the bandwidth lower is the risk of a DoS attack. The network/system can absorb these types of attacks when a sufficient bandwidth is allocated to them.

### Outsourcing:

Some providers have specialized infrastructures to protect the systems against DoS attacks. The cloud scrubbing service remove almost all of the problematic/bad traffic from the network channel. The best time to defend and apply mitigation on these types of attacks is applying the infrastructure and techniques beforehand. These DoS mitigation providers have the sort of adaptable and dynamic load balancing accessible in response to the exceptional degrees of traffic that frequently result from a DoS attack.

# References

What is XSS | Stored Cross Site Scripting Example | Imperva. (2020),  *from https://www.imperva.com/learn/application-security/cross-site-scripting-xss-attacks/*

Weiss, A. (2020). How to Prevent DoS Attacks, *from https://www.esecurityplanet.com/network-security/how-to-prevent-dos-attacks.html*

What is phishing | Attack techniques & scam examples | Imperva. (2020), *from https://www.imperva.com/learn/application-security/phishing-attack-scam/*

Kartch, R. (2020). Distributed Denial of Service Attacks: Four Best Practices for Prevention and Response, *from https://insights.sei.cmu.edu/sei\_blog/2016/11/distributed-denial-of-service-attacks-four-best-practices-for-prevention-and-response.html*

Wutte, M. Cryptology - methods and their properties - ANEXIA Blog. (2020), *from https://anexia.com/blog/en/cryptology-methods-and-their-properties/*

What is cryptography | Cryptography | Khan Academy. (2020), *from* *https://www.khanacademy.org/computing/computer-science/cryptography/crypt/v/intro-to-cryptography*

Gilmour, N. (2020). Cyber Crime and National Security: A New Zealand Perspective, *from https://standinggroups.ecpr.eu/sgoc/wp-content/uploads/sites/51/2020/01/richardson-gilmour.pdf*

SYN Flood Attack, CloudFare: SYN Flood Learning Objectives *from https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack*

Gigamon Blog. 2020. *14 Network Security Tools and Techniques to Know - Gigamon Blog*, *from https://blog.gigamon.com/2019/06/13/what-is-network-security-14-tools-and-techniques-to-know*

What is a DDoS Botnet, CloudFare: DDoS Botnet Learning Objectives *from https://www.cloudflare.com/learning/ddos/what-is-a-ddos-botnet*