****

**NAME: YUSSUF SEIFUDIN**

**ID: 660411**

**FIC4040 ASSIGNMENT 2**

The core concept at the heart of today’s cybercrime remains exactly the idea that converging globalized information communication technology may be used for committing criminal acts, with transnational reach. Elucidate the above statement from your point of view with supporting evidence. [30Marks]

The most popular cybercrime attack vectors that many people implore are:

1. Reconnaissance – this is where an attack would first want to gather as much information as there is regarding a potential target such as the details about the networks, systems that are in place, as well as the security measure that are in place.
   1. This can be applied in terms of looking at information that is readily accessible to the public. This can be through wireless networks at your local café. This can be very fatal to unknowing users.
   2. Another example can be information that the general public can easily access in terms of public websites such as betting websites here in Kenya. An attacker can create the same betting website trying to mimic the original website and harvest user information and end up using them for illegal purposes.
2. Scanning – This mostly involves using the information that was gathered during reconnaissance and applying it to look for vulnerabilities within the network or system in place.
   1. This can be applied after the reconnaissance stage and try to look for vulnerabilities in a particular given system. This can be open ports from servers or Access Points. This can be fatal be towards a company or users this may lead to access to sensitive data, especially for companies that do not secure or separate information in terms of what the public is allowed to see and companies’ private information only allowing authorized users to access them through using a Virtual Private Network.
3. Another way cybercrime can take place is through the internet by studying the victim’s habits by using geolocation. After that, the attacker can either use social engineering to trick the individual to leave either their belongings or devices.
4. Cyber pornographic – this can be defined as the distribution, displaying, creating, importing, or publishing of pornographic or obscene materials using cyberspace.
5. Cyber Grooming – This is where a perpetrator uses cyberspace by befriending and establishing emotional connections with a minor with future intentions of sexual abuse, sexual exploitation, or even child trafficking. The perpetrator can use cyber grooming together information about a parents credit card information etc.