CYBER SECURITY

BISF 3103

ASSIGNMENT 3

EMMANUEL KIPKEMOI SIGEI

REG NO – 20/03807

CAMPUS: MAIN

FULL TIME

PRESENTED TO Mr. MARTIN LUTHER

QUESTION ONE: Bad Practices that make organizations vulnerable to cyberattacks with application areas.

1. ***Poor Password Management*** – When weak passwords are used or when passwords are reused across accounts, it becomes much easier for hackers and attackers to crack the passwords and gain access to multiple accounts. An example of this can be illustrated through online banking systems where if strong access control measures are not implemented then financial records could be at risk of landing in the wrong hands.
2. ***Not properly training employees -*** When employees are not made aware of the different kinds of cyber security threats, they can become more susceptible to attacks such as Social Engineering Activities like Phishing. With human beings being the weakest point in the network, it becomes easier for attackers to exploit the employees. An example would be employees in a hospital, for example, being duped into sharing confidential patient information.
3. ***Using Outdated Software –*** Software updates are implemented to fix discovered vulnerabilities that could be exploited by threat actors. When Software is outdated, it remains vulnerable. An application area would be Web Applications not updating to the latest versions of the tools they use such as Database Management Software which leaves data about their customers at risk of landing in the wrong hands.
4. ***Leaving Exposed ports on the Network –*** This action compromises the security of the Network thus making the network susceptible to scanning done by hackers and eventually they gain access to the network. An application area for this would be networks used by large corporations that aid in communication between branches and if these networks are intercepted by attackers, it could then lead to losses and disruptions.
5. ***Not properly protecting data –*** When sensitive data is being shared over a network or even when it is just at rest, it should be properly encrypted to protect it and a vulnerability is created when this is not done properly. An application of this area would be data such as Bank Card Details and Identification details being obtained by attackers who can then use it for crimes such as Identity Theft and Bank Fraud.

QUESTION TWO: Tools and Techniques used to commit Cybercrime.

1. ***Password Crackers*** – Cybercriminals use password cracking applications/tools to gain access to accounts by guessing or brute-forcing passwords. This can be eliminated by setting up multi-factor authentication on the systems.
2. ***Malware Attacks*** – Threat Actors use Viruses and Ransomware for example to gain access or to damage/disrupt the computer network. This can be prevented by using proper antivirus software tools and performing regular software updates.
3. ***Social Engineering*** – This can be achieved through Phishing for example and for this, the cybercriminals deceive people into revealing sensitive information about themselves or the computer network. Since phishing is majorly conducted through emails, it can be combated by implementing proper email filtering systems and raising awareness amongst the users of the computer Network.

4. ***Distributed Denial of Service Attacks*** – Threat actors make use of tools like Botnets to overwhelm the network with spam traffic, rendering it inaccessible to legitimate users. This can be eliminated by implementing intrusion detection and prevention systems.
5. ***Keyloggers/Keylogging*** – Cybercriminals use Keyloggers to obtain sensitive information such as passwords, which they can then use to gain access to the accounts. Multi-factor authentication on user accounts can help to mitigate this.

QUESTION THREE: Roles and Applications of Cryptography in Ensuring Cyber Security.

Cryptography refers to protecting information by changing it into a format that is not readable by an unauthorized person.

Roles of Cryptography in Cyber Security.

1. Cryptography ensures the Confidentiality of data by using complex algorithms to encrypt the data which can only be decrypted by authorized individuals with the correct cryptographic keys.
2. Cryptography ensures the integrity of data since it is assured that the data cannot be manipulated while in transit. It can also aid in detecting any modifications made to the data.
3. Cryptography ensures that communication between different points on a computer network is secure thus preventing eavesdropping.
4. Digital signatures in cryptography introduce non-repudiation where the authenticity of data or messages is assured, and the sender cannot deny sending the message.
5. The Public Key Infrastructure in cryptography is used to securely authenticate users and their identities and their devices.

Applications of Cryptography in Cyber Security.

1. Cryptography is used in Blockchain Technologies to secure transactions on the Blockchain Network therefore ensuring integrity.
2. Passwords are generally stored in encrypted form to prevent unauthorized access to systems and to securely authenticate users.
3. Emails are encrypted before they are sent which aids in protecting the contents of the email from interception by unauthorized individuals.
4. On online payment gateways, Credit Card information such as Card Numbers, CVV Codes, Expiry Date, and the Holder Name, is encrypted after a user inputs it into the system. This prevents it from being stolen by attackers.
5. Cryptography is used in messaging apps like WhatsApp to ensure the security of communications between individuals on the platform.