INFORMATION SECURITY
ASSIGNMENT 02

Bilal Ahmed Khan
K200183; Sec: B

Date: _____

QUESTION NO.01

Following are the two cloud security chapter topics which google Infrastructure implements

01) Security Audits & Monitoring:-

A/c to the whitepaper provided by Google, it specifically works with vendors they work with to choose components with care for their data centers. They regularly audit & validate the security aspect of the components being used in their data centers. They also implement best practices such as audit logging & source code repositories where past and current version of the code can be audited.

02) Trust Model

Google's BeyondCorp initiative is a prime example of zero-trust security implementation. This model assumes that no device or user is trusted by default whether inside or outside the network. This approach is based on the principle of least privilege, which means that the users are only granted access to the resources they need to do their job.

Date: _____

QUESTION NO. 02

Google uses a multi-layer, multi-tier DoS protection system to safeguard its services from DoS attacks, this approach shows a multilayer defense to mitigate & absorb DoS attacks.

- Google DoS protection strategy can be distributed into three tiers.

- Tier 1: Network-level protection:-

  - Google's extensive fiberoptic provides a robust foundation for handling large amounts of traffic
  - at the edge of Google's network, load balancers & various other techniques are used to filter malicious traffic

- Tier 2: Service level protection

  - Googles uses application level firewalls & intrusion detection to prevent DoS attacks on application/service level.

Date: _____

Tier 03: Operational Response :-

- Google's Threat intelligence group continously monitors evolving Dos attacks & develops countermeasures for them
- Google also has incident response teams which investigate & respond to Dos attacks

QUESTION NO. 03

Google uses a sophisticated Intrusion detection system (IDS) to monitor & detect potential security breaches across vast network & services.

Host-based Intrusion detection:-

- Agent based IDS are installed on additional servers to monitor their activities & log suspicious events

Network Based Intrusion detection:-

NTA (Network Traffic Analysis) monitors network traffic patterns & identifies anomalies or derivations from normal behavior that could indicate an attack.

x ——— x ——— x

end of assignment.