KINGDOM OF SAUDI ARABIA
Ministry of Education
Taibah University
College of Computer Science and Engineering
(Male Section)

المملكة العربية السعودية
وزارة التعليم
جامعة طيبة
كلية علوم وهندسة الحاسب الآلي
(قسم الطلاب)

IS cyber security

M1

Abdulhadi Abdullah al-harbi

40026664

Assignment 4#

Do you think Miller is out of options as he pursues his vendetta? If you think there are additional actions he could take in his effort to damage the SLS network, what are they?

Miller's options are limited as he pursues his revenge.The "completely annotated network diagram of the SLS Company and all the files" and "access codes required to perform an assault on the network" are the items that Miller was supposed to attach. Miller used a VPN client to attack the network and discovered that the front door was locked. He attempted to establish a dial-up connection once more. It failed to attach because it routed to the same RADIUS authentication server .Miller made the following attempt. He turned on the zombie program he had installed on the extranet quality assurance server for the business. The firewall and its control policy are to blame for the failure of this attach technique.Miller's effort to use Nmap to attack the network was likewise unsuccessful also failed as his IP (internet Protocol) address is blocked.Miller currently has no other means of attacking the SLS network. Miller has no other choice than to continue his vengeance.Miller also has other choices. He can use a new system with a different IP address to run Nmap while his IP address is blocked. With the use of this Nmap, he can carry on his attempts to harm the SLS network.

Suppose a system administrator at SLS happened to read the details of this case. What steps should he or she take to improve the company's information security program?

- All policies and procedures should be established clearly and followed. You should thoroughly examine your policies and processes to make sure they are clear, useful, and offer the right level of security.
- Obtain management approval for the handling of incidents and security rules.
- Evaluate your environment's weaknesses on a regular basis. An expert in security who has the necessary clearance should conduct assessments.
- Create security training courses for end users and IT personnel. Any system's biggest weakness is an inexperienced user.
- Create a policy demanding strong passwords and enforce it.
- Routinely monitor and analyze network traffic and system performance.