Network Security

Part one: User authentication:

User authentication on a website :

a) He will use password to first login to the website account via password which forms part of knowledge factors as , this what is in his knowledge

b) The website then asks for a token or a randomly generated PIN which would have been emailed to his email id/mobile..This will form part of ownership factors.

c) After putting the PIN . The website asks for a thumbprint. This can be done by using his thumb to a thumb print scanner attached to his computer/laptop. This form part of inheritance factors

**Part 2 Attack vectors :**

Four attack vectors on a company that produces shoes.

a) Digital b) Physical

a) Passive : An attacker can name similar domain name of the show company website and steal user credentials of people or potential customer accounts who visited the site to order.

b) passive: Brute force . Attacker can send email to users of company employess. And compromised their data by phising email being sent . Anyone can use and break weak password credentials. Use Network or Webapplication abuse to steal data from company website

c) Physical attack on the company warehouse in case of weaker security .Stealing warehouse materials in case of absence of cctv cameras.

d) Attack on the raw materials being procured to the manufacturing unit and hence denying supply

**Part 3: Wireless security**

Key reinstallation attacks (KRACK) are a type of cyberattack that exploit a vulnerability in WPA2 for the purpose of stealing data transmitted over networks. These attacks can result in the theft of sensitive information like login credentials, credit card numbers, private chats, and any other data the victim transmits over the web.

An attacker can set up a clone of a WiFi network that the victim has previously connected to. The malicious clone network can provide access to the Internet, so the victim won’t notice a difference. When the victim tries to reconnect to the network, the attacker can force them to join the clone network instead, positioning themselves as a on-path attacker. During the connection process, the attacker can keep resending the third part of the handshake to the victim’s device. Each time the user accepts the connection request, a small piece of data is decrypted. The attacker can aggregate this series of communications to crack the [encryption key](https://www.cloudflare.com/learning/ssl/what-is-a-cryptographic-key/).

It should be noted that KRACK attacks require proximity to work. An attacker cannot target someone across the globe or even across town; the attacker and victim must both be in range of the same WiFi network to carry out the attack.

**Part 4:**

Network based firewall and deploy security rules .Will define some ports to block TCP connection to block some traffic. More ports can be added depending upon requiring and client serevr connections.

E,g Zonealrm . comodo etc

Having antivirus being installed on all of the machines to block individual attack. Windows antivirus. Have whole scan. Keep antivirus database updated. Use Virus total website to check for all types of malicious files .

A private VPN can be used for the system to stay anonymous or protect against outside attack