**At Bay**

**Question 2 – second section**

I chose to display the range between 9.0-10.0 because I have learned that it is considered as "critical". Having CVSS in the critical range means that CVE most severe and easiest to exploit.

This is the full CVSS score ranging:

0.0 None

0.1 – 3.9 Low

4.0 – 6.9 Medium

7.0 – 8.9 High

9.0 – 10.0 Critical

**Question 4**

Remote Desktop Protocol provides connection and communication between users with a graphical interface (GUI) to another computer through the internet or a local network. It allows taking over a computer and managing it's operations. Most of the time, that means a server can connect to a client and taking over it, but RDP also allows other services to run over it, such as Remote Desktop Service (RDS). That allows a client computer in one location to connect to a remote computer, also known as host computer, in another location.

RDP exists in a wide variety of operating systems, such as Microsoft Windows, macOS, iOS, and Android.

Nowadays, many companies use RDP on a daily basis for a variety of reasons. It can make customer-assistance easier – the service provider doesn't need to meet the customers in order to help them. Therefore, the whole process is faster, and the provider can help more customers. Furthermore, in the "COVID-19" area – the usage in RDS became necessary, since a huge number of companies had to work remotely, and it became extremely common.

In the last few years, attacks against RDP became extremely popular. Ransomware groups tend to use it because they can access to companies' networks, explore them and attack them: plant a trojan horse in an attempt to block access to them or even find sensitive data before it was encrypted and then extort the victim by threatening to post it. RDP is also exposed to distributed denial-of-service attack (DDoS), in which the attacker sends countless quantity of data to a website or a server in order to bring it down. Ransomware group can use this sort of attack.

Therefore, companies that uses RDP have a potential for a lot of vulnerabilities or opportunities available for exploitation. When a company that uses RDP wants to buy a cyber insurance, it must secure it. There are several ways to do so:

* IP-based Access Lists – implementing access control lists (ACLs) that only permit RDP connections from specific IP addresses. This isn't a good solution, because this IP list should be dynamic and it requires a lot of work. Also, it only prevents an attacker from getting into the network, but if he is already inside it does nothing. An attacker can still get into the network threw one of the endpoints under it.
* Virtual Private Networks (VPN) – It provides an encrypted tunnel for network traffic between a remote user and the network. Furthermore, it helps to decrease the threat of accounts that have been attacked. VPN still has vulnerabilities and is sometimes targeted, which means a company that uses VPN should upgrade it with security patches to protect it.
* Virtual Desktop Solution – Secures both the route into the network and the systems that an employee, and therefore an attacker, can access remotely. It allows a company to use MFA for better authentication of the endpoints (the employees). Additionally, it helps to control remoted endpoints – and as a result, helps to prevent movement of threats within the network.

**Bonus Question**

When I was trying to answer this question, I started off with looking for indication that says that a domain uses Mimecast. I came across this table in the Mimecast website:

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

The website said that the firewall should be open in those ports.

443 is the https protocol, so I checked what port 53 is commonly used for. It seems it is the DNS (domain name service) port.

I still wanted to check if the domain or any of the subdomains has those ports open. I brought all the subdomains under [jacobstern.com](http://jacobstern.com) and checked if ports 53 and 443 were open in one of them. It seems that none of them had port 53 open.

Later, I checked for all domains if one of them uses one of the ports that is known as email port. Again, they were all closed.

I tried to find the email address of the domain so I can check if it maybe uses those ports. I used whois module to find out details about the domain. I found there three email addresses that looked rather odd:

[abuse@web.com](mailto:abuse@web.com),

[da7549rb25u@networksolutionsprivateregistration.com](mailto:da7549rb25u@networksolutionsprivateregistration.com),

[domain.operations@web.com](mailto:domain.operations@web.com)

but it wasn't possible to turn them into an IP.

In conclusion, I think we should find the ports that the firewall of the domain uses, but I haven't succeeded to do so.