Chapter 11

1. C
2. B
3. C
4. A
5. A
6. D
7. B
8. B
9. D
10. C
11. D
12. B
13. D
14. C
15. A
16. A
17. B
18. B
19. D
20. A

Article: Niagara Regional Broadband Network Includes DDoS Protection with Dedicated Internet Access Services

Link: https://ca.finance.yahoo.com/news/niagara-regional-broadband-network-includes-150000959.html

Niagara Regional Broadband Network (NRBN) announced this week that its Smart Protect DDoS mitigation technology which protects against DDoS assaults in real-time, would be free for dedicated internet access customers.

As we learned in the class, DDoS is a kind of distributed denial of service when malicious traffic from several sources overwhelms a network. This disrupts genuine traffic and may keep some firms closed for days or weeks. Web servers, for example, have a restriction on the number of concurrent requests they can process. In addition to the server's capacity, the Internet connection's bandwidth/capacity is limited. A service level degradation occurs when the quantity of requests surpasses the capacity constraints of any infrastructure component. As a result, requests will be processed significantly slower than usual. And users' demands may be completely disregarded.

In addition, to make massive requests to the victim resource, the cybercriminal frequently creates a 'zombie network' of infected machines. Because the criminal controls every infected machine in the zombie network, the attack's scope may overwhelm the victim's online resources. As a result, requests will be processed significantly slower than usual, and users' demands may be completely disregarded. Especially in those days, the rise of 5G and IoT networks, as well as a worldwide shift to cloud computing, have opened new DDoS attack vectors.

Based on that, the need for greater bandwidth has led to bigger and more frequent DDoS assaults. Attacks above 10Gbps have increased 70% since 2018. Attacks of short duration are still prevalent and might be difficult to identify and counteract using manual or antiquated techniques. Therefore, Niagara Regional Broadband Network (NRBN) conducted the Smart Protect, which is designed to scan, identify, and discard harmful data packets while delivering legitimate traffic undisturbed. Assemble suitable network and application protection mechanisms, included are firewalls, network monitoring software, anti-virus, and threat monitoring systems. Users may use them to monitor network traffic and set up warnings for unusual activity. For an extra monthly cost, NRBN users may get comprehensive security that includes a secure customer portal, configurable reports, and attack alerts.