Question 1

a)

For this scenario, the attack type is: Border Gateway Protocol (BGP) Hijacking.

This attack uses a malicious AS that pretends to have ownership of an IP address which belongs to another organization.

In the presented scenario, the company network traffic is being rerouted through a foreign network because the a hacked AG is announcing more specific routes for the company's IP prefixes. This allows the attacker to intercept, analyze and modify the data before forwarding it to the intended recipient.

b)

For this scenario, the attack type is: Domain Name System (DNS) Amplification Attack.

This attack uses a public DNS and the ability to spoof source IP addresses. The attacker sends a lot of small DNS queries to these DNS servers but makes it look like the requests are being sent from real bank servers. This overwhelms the bank with unsolicited DNS responses, consuming bank recourses and eventually leading to performance degradation or service stopping.

c)

For this scenario the attack type is: Port Scanning.

This attack is used for identifying open ports and services that are running. This information will be later used in a larger cyber attack. By sending SYN packets to multiple different hosts the attacker is trying to determine which services are potentially exploitable.

d)

For this scenario, the attack type is: Internet of Things Botnet DDos Attack.

This attack uses a lot of compromised devices like security cameras, smart TV and home routers by exploiting their weak security setting which are often kept with default usernames and passwords by the owners. The devices are infected with malware and can be remotely controlled as part of a botnet. The attacker instructs all these devices to send a flood of HTTP requests to the e-commerce website overwhelming the site's servers and crashing it.

e)

For this scenario, the attack type is: Man in the Middle (MITM) Attack.

This attack uses an unauthorized device between the students devices and the university's network gateway which enables them to intercept and manipulate the network traffic. Using this device the attacker can monitor data, steal credentials and even modify the information sent by the students.