Cybersecurity Incident Report

Part 1: A summary of the problem found in the DNS and ICMP traffic log
The network protocol analyzer logs indicate that port 443 is unreachable when attempting to access the secure employee background check website. Port 443 is normally used for HTTPS traffic. This may indicate a problem with the web server or the firewall configuration. It is possible that this is an indication of a malicious attack on the web server.

Part 2: Explain your analysis of the data and provide one solution to implement
The incident occurred earlier this morning when the human resources (HR) team reported that they could not reach the background check web portal. The network security team responded and began running tests with the network protocol analyzer tool tcpdump. The resulting logs revealed that port 443, which is used for HTTPS traffic, is not reachable. We are continuing to investigate the root cause of the issue to determine how we can restore access to the secure web portal. Our next steps include checking the firewall configuration to see if port 443 is blocked and contacting the system administrator for the web server to have them check the system for signs of an attack. The HR team believes it is possible that a certain new hire may want to keep them from performing the background check. The network security team suspects this person might have launched an attack to crash the background check website.

Incident report analysis

Summary	This morning, an intern reported an inability to access her internal network account. Access logs reveal that her account was active in the customer database, despite being locked out. The intern received an email urging her to log in externally with internal credentials, likely a ploy by a malicious actor. Other employees noticed missing or manipulated customer records, suggesting unauthorized access and data tampering. It appears that not only was customer data exposed to a malicious actor, but that some data was deleted or manipulated as well.
Identify	The incident management team audited the systems, devices, and access policies involved in the attack to identify the gaps in security. The team found that an intern’s login and password were obtained by a malicious attacker and used to access data from our customer database. Upon initial review, it appears that some customer data was deleted from the database. The incident team audited systems and access policies to uncover security gaps. A malicious attacker obtained an intern's login, using it to breach the customer database. Some customer data was deleted. Additionally, an ICMP flood targeted the company through an unconfigured firewall.
Protect	New measures include multi-factor authentication, limited login attempts, and employee training. A fortified firewall configuration and

	intrusion prevention system are planned. A new firewall rule curbs ICMP flood rates, and an IDS/IPS filters suspicious ICMP traffic.
Detect	To detect new unauthorized access attacks in the future, the team will use a firewall logging tool and an intrusion detection system (IDS) to monitor all incoming traffic from the internet. The team will configure source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets.
Respond	The team disabled the intern's network account. We provided training to interns and employees on how to protect login credentials in the future. We informed upper management of this event and they will contact our customers by mail to inform them about the data breach. Management will also need to inform law enforcement and other organizations as required by local laws. For future security events, the cybersecurity team will isolate affected systems to prevent further disruption to the network. They will attempt to restore any critical systems and services that were disrupted by the event. Then, the team will analyze network logs to check for suspicious and abnormal activity
Recover	The team will recover the deleted data by restoring the database from last night's full backup. We have informed staff that any customer information entered or changed this morning would not be recorded on the backup. So, they will need to re-enter that information into the database once it has been restored from last night's backup. Regular Firewall maintenance checking and updating security

	configurations regularly to stay ahead of potential threats. Firewall rules can be updated in response to an event that allows abnormal network traffic into the network. This measure can be used to protect against various DDoS attacks. In the future, external ICMP flood attacks can be blocked at the firewall. Then, all non-critical network services should be stopped to reduce internal network traffic. Next, critical network services should be restored first. Finally, once the flood of ICMP packets have timed out, all non-critical network systems and services can be brought back online.

Reflections/Notes: The finalized incident report analysis achieves the following objectives:

- Identifies the nature of the attack, the incident's extent, and its organizational impact.
- Outlines potential vulnerabilities within the network and proposes corresponding protective measures.
- Specifies the utilization of detection tools for network monitoring and security enhancement.
- Establishes a framework for responding to future cybersecurity incidents.
- Details strategies for restoring regular operations during recovery.