Incident report analysis

Portfolio Piece

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this chart as a way to practice applying the NIST framework to different situations you encounter.

Summary	The company has experiences a DDOS attack through a poorly configured firewall. A flood of ICMP packets was used to execute a denial of service attack on the systems. The company should adhere to the NIST framework to ensure total protection against future attacks and ensure data validity and business continuity going forward. Incident detection, asset protection and integrity verification are the pillars against which we shall structure our NIST governed plan.
Identify	The network was under attack via a flood of ICMP packets - a type of Distributed Denial of Service likely employed by a botnet of infected systems. We should examine systems, servers and data for unverified changes and unauthorized access alongside examining the effect of the downtime on business operations.
Protect	Immediately, we should implement a strict, stateful firewall that will dynamically adjust and protect based on the circumstance. We should verify source IP addresses to avoid smurf or IP spoofing attacks. MFA Should be employed immediately and stronger password credentials should be established alongside employee education for attack vectors to the company. Data should be encrypted in transit and verified against a baseline to ensure data integrity.

Detect	We will require improved detection systems for suspicious activity and out of the norm incoming packet patterns. Our focus on our SIEM tools should be increased and the frequency of auditing and monitoring should be applied to alow for earlier detection and mitigation of threats as the may be occurring . More regular review of logs should be implemented to ensure we are protecting incidents as they may grow. Specifically, we should move forward with ICMP traffic filtering to avoid suspicious ICMP traffic behaviour.
Respond	It is imperative for us to contain incidents even in spite of safeguards, as there always is a risk of attack. Our rapid response team should isolate affected devices and systems. The research team in tandem should be using the SIEM tools to analyze logs and gather data on the events leading up to the attack and during the attack to understand the full scope of the attack. We should detect the anomolies and forward the information to our defense team to be incorporated into future training and fine tuning protocols. We should also test and train our employees on the phishing tactics and latest exploitations that could be targeted at them.
Recover	We shall require robust data backup to revert to the most recent snapshot of the database that is available. Ensure the integrity against a baseline and perform a thorough penetration test to ensure the same attack cannot be repeated. All procedures should be regularly reviewed and implemented alongside a cloud based system that remains the most up to date with current threats and vulnerabilities.

Reflections/Notes: