Incident report analysis

Instructions

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	Our organization experienced a DDoS attack that compromised the internal network for two hours. A malicious actor sent a flood of ICMP packets through an unconfigured firewall, overwhelming our network and preventing normal internal traffic from accessing any network resources. The incident management team responded by blocking incoming ICMP packets, taking non-critical network services offline, and restoring critical services. The attack exploited a vulnerability in our firewall configuration that didn't have rate limiting or verification for incoming ICMP packets. After containment, the security team implemented new firewall rules to limit ICMP packet rates, added source IP verification to check for spoofed addresses, deployed network monitoring software to detect abnormal traffic patterns, and installed an IDS/IPS system to filter suspicious ICMP traffic.
Identify	The attack was a distributed denial of service (DDoS) attack using ICMP packet flooding. The affected systems included our internal network infrastructure, firewall, and all network services that employees needed to access company resources. The root cause was an unconfigured firewall that lacked proper rules to handle incoming ICMP traffic. This created a gap in our security posture that allowed the attacker to overwhelm our network bandwidth and processing capacity. The attack impacted all employees who needed network access to

	perform their jobs, affecting web design services, graphic design work, and social media marketing operations for our clients.
Protect	**We need to strengthen our firewall configuration management to prevent similar attacks. The new firewall rules limiting ICMP packet rates and verifying source IP addresses are good first steps, but we should also implement regular firewall audits to catch misconfigurations before they become vulnerabilities. Employee training on recognizing DDoS symptoms would help staff report issues faster. We should establish a baseline for normal network traffic patterns so deviations stand out more clearly. Additionally, we need documented procedures for firewall changes that require security team review before implementation. Consider implementing redundant network paths so critical services can continue operating even during an attack on our primary infrastructure.**
Detect	The network monitoring software we installed will help track traffic patterns and flag anomalies that might indicate another DDoS attack. The IDS/IPS system gives us real-time visibility into ICMP traffic characteristics and can automatically filter suspicious packets. We should configure alerts that notify the security team when ICMP packet volumes exceed normal thresholds or when traffic patterns match known DDoS signatures. Regular log reviews from our firewall and monitoring tools will help us spot attack indicators early. We could also implement SIEM integration to correlate events across multiple systems and detect coordinated attacks. Monitoring bandwidth utilization in real-time would give us early warning when network resources are being consumed abnormally.
Respond	For future incidents, we need a clear escalation procedure that defines when to involve the incident management team, when to take systems offline, and who has authority to make those decisions. Our response playbook should include steps for isolating affected network segments, blocking attack traffic at multiple points, and maintaining communication with stakeholders during the

	incident. We should document which services are critical versus non-critical so we can make quick decisions about what to keep running during an attack. After containment, we need a standard process for collecting and analyzing attack data to understand the threat actor's methods and improve our defenses. Regular tabletop exercises would help the team practice responding to different attack scenarios so we're better prepared when real incidents happen.
Recover	Recovery from this type of attack focuses on restoring normal network operations once the threat is contained. We need to verify that all network services are functioning properly and that no unauthorized changes were made to our systems during the attack. The firewall configuration should be reviewed to confirm the new security rules are working as intended without blocking legitimate traffic. We should monitor network performance closely for the next few days to ensure the attack didn't cause any lingering issues. Communication with affected employees and clients is important so they know services are restored and understand what happened. Document lessons learned from this incident so we can update our incident response procedures and prevent similar attacks. Consider scheduling a post-incident review meeting with all stakeholders to discuss what worked well and what needs improvement in our response process.

Reflections/Notes: