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	8AM - 10AM Today we experienced a DDoS attack, compromising our network infrastructure and some key core services. We lost access to intranet tools for two hours. It was discovered this was caused by a flood of ICMP packets. This seems like a Ping of Death type of attack. Response was done via blocking incoming ICMP requests, and silencing non-critical network services. (VoIP, teleconferencing, streaming Servers).
Identify	During our Audits, we've found about new firewalls that were deployed with their default configuration. This Firewall was not ready or configured to deflect basic attacks. In this case the firewall was not ready to analyze packets header and size, to prevent the oversized ICMP packets hitting our servers.
Protect	Implementation of the following is required: -We need to set a policy where NO device or service must be left running with default settings. -Baseline each security service, after implementing our custom changes, and configuration files must have local and cloud backups. (these are small files, we

	don’t have to worry about storage cost). -A combo of IDS\IPS systems are now implemented, they should help us to be notified much earlier about future cases like this. -Please note, this requires a new human individual(s) in charge of this, because we need to train\configure the IPS when it comes to detecting false positives. -This comes with additional cost in terms of Tools, Maintenance and Personnel.
Detect	Our new IDS system will help us in detecting future cyber attacks. The new personnel will be in charge of responding to its alerts.
Respond	The issue was contained after disabling ICMP traffic, and shutting down non-essential services. Training for IT is scheduled next week, in regards new devices\solutions and Default Settings.
Recover	Team will restore services once the firewall has been configured, and the limit of ICMP requests is changed into a reasonable threshold. We should still allow ICMP for our Helpdesk, but only from Internal IPs. External ICMP requests from a single source should be limited to 3 checks every 24 hours. Cybersec team will implement an isolated Sandbox with a private VLAN, where a HoneyPot VM will be deployed, with this we will evaluate if the counter measures were effective or not.

Reflections/Notes: Please schedule a follow up call about this incident every 3 days.
Senior Cybersec team associate will be on call for One Month, in case the issue arises again, to train Helpdesk and IT Team, when it comes to handling these incidents in the future.