Incident Response Plan

1. Preparation

To ensure readiness against possible incidents, we will implement preventive security measures including system hardening, network segmentation, and access control enforcement. Continuous monitoring using tools such as Wireshark, SIEM platforms, and vulnerability assessment tools will help detect suspicious activity early. Patch management procedures will also be improved to guarantee that security updates and firmware patches are deployed promptly to reduce the chance of exploitation.

2. Detection and Analysis

In a security incident, such as a network scan, vulnerability, or attempt at exploitation, this incident response plan describes the protocols, roles, and steps that must be followed. We may successfully reduce risks, safeguard our resources, and lessen the effect of security incidents on our company by adhering to these recommendations and taking a proactive approach to incident response.

Constant monitoring is essential to identify any risks and take immediate action in response. We'll put in place systems to keep an eye out for any unusual activity, exploitation attempts, and illegal access attempts. We'll also use threat intelligence sources to proactively reduce risks to remain updated about new threats, vulnerabilities, and attack patterns.

3. Containment, Eradication, and Recovery

Quick Containment

As a first measure, we will disconnect vulnerable machines such as Metasploitable and Bee-box from the network. This prohibits the attacker from moving around in our system and stops additional exploitation. To lower the danger of unwanted access and data theft, we'll also set up access restrictions to limit traffic to and from the compromised host, "10.0.69.10".

Fixing Vulnerabilities

We'll update and install security fixes to address the vulnerabilities we discovered on host "10.0.69.10." This covers problems including SSL/TLS vulnerabilities, known CVEs, vulnerability to Slowloris attacks, obsolete software on the Apache server, and directory traversal. To stop any cryptographic errors and data eavesdropping, we'll also concentrate on

mitigating vulnerabilities in the Beebox system, such as the Logjam vulnerability and other recognized CVEs.

Coordination of Incident Response

We will engage our incident response team to coordinate our reaction efforts. We'll coordinate with pertinent authorities or outside partners and inform stakeholders when necessary. We'll keep everyone updated on our work and any useful insights we find through regular status reports and updates.

Patch Administration and Security Upgrades

We'll enhance our patch management procedures to guarantee the prompt deployment of security updates and patches throughout our network to avert such occurrences in the future. We'll fortify our security measures by putting in place network segmentation, access controls, and intrusion detection and prevention systems (IDPS).

4. Post-Incident Activity

Documentation of Incidents and Takeaways

We'll record our incident response activities, including the steps we took, the conclusions we reached, and any lessons we learned. To find the source of the problem, any weaknesses in our security measures, and any areas for process improvement, we will need to undertake a post-incident review, which will require this documentation. We'll make sure our company is more robust and better equipped for incidents in the future by using the lessons we learned from this one.