



Cyber Suraksha

Purple Team Exercise

Incident Response Report

(IRREP)



4. Technical Analysis



Time: Incident ID: 1. Incident Overview Description: Severity Level: Impact: Affected Systems: 2. Incident Details Detection Method: Initial Detection Time: Attack Vector: Attackers: 3. Response Actions Taken Containment: Eradication: Recovery: Lessons Learned:	Date:
1. Incident Overview Description: Severity Level: Impact: Affected Systems: 2. Incident Details Detection Method: Initial Detection Time: Attack Vector: Attackers: 3. Response Actions Taken Containment: Eradication: Recovery:	Time:
Description: Severity Level: Impact: Affected Systems: 2. Incident Details Detection Method: Initial Detection Time: Attack Vector: Attackers: 3. Response Actions Taken Containment: Eradication: Recovery:	Incident ID:
Description: Severity Level: Impact: Affected Systems: 2. Incident Details Detection Method: Initial Detection Time: Attack Vector: Attackers: 3. Response Actions Taken Containment: Eradication: Recovery:	
Severity Level: Impact: Affected Systems: 2. Incident Details Detection Method: Initial Detection Time: Attack Vector: Attackers: 3. Response Actions Taken Containment: Eradication: Recovery:	1. Incident Overview
Impact: Affected Systems: 2. Incident Details Detection Method: Initial Detection Time: Attack Vector: Attackers: 3. Response Actions Taken Containment: Eradication: Recovery:	Description:
Affected Systems: 2. Incident Details Detection Method: Initial Detection Time: Attack Vector: Attackers: 3. Response Actions Taken Containment: Eradication: Recovery:	Severity Level:
2. Incident Details Detection Method: Initial Detection Time: Attack Vector: Attackers: 3. Response Actions Taken Containment: Eradication: Recovery:	Impact:
Detection Method: Initial Detection Time: Attack Vector: Attackers: 3. Response Actions Taken Containment: Eradication: Recovery:	Affected Systems:
Detection Method: Initial Detection Time: Attack Vector: Attackers: 3. Response Actions Taken Containment: Eradication: Recovery:	
Initial Detection Time: Attack Vector: Attackers: 3. Response Actions Taken Containment: Eradication: Recovery:	2. Incident Details
Attack Vector: Attackers: 3. Response Actions Taken Containment: Eradication: Recovery:	Detection Method:
Attackers: 3. Response Actions Taken Containment: Eradication: Recovery:	Initial Detection Time:
3. Response Actions Taken Containment: Eradication: Recovery:	Attack Vector:
Containment: Eradication: Recovery:	Attackers:
Containment: Eradication: Recovery:	3. Response Actions Taken
Eradication: Recovery:	
Recovery:	



7. POC (Screenshots)



Evidence:
Indicators of Compromise (IOCs):
Tactics, Techniques, and Procedures (TTPs):
Mitigation Recommendations:
5. Communication
Internal Notification:
External Notification:
Updates:
6. Follow-Up Actions
Incident Review:
Documentation:
Training: