Network Intrusion Investigation Worksheet

General Information

Date:

Time:

Investigator Name:

Case/Incident Number:

Incident Details

Date & Time Detected:

Detection Method:

Reporter (if different):

Brief Description of Incident:

Affected Systems

System Name(s) / Hostname(s):

IP Address(es):

Network Segment(s):

Indicators of Compromise

Observed Behaviors / Artifacts:

Malware or Tools Involved:

Log File References:

Investigation Actions

Initial Actions Taken:

Further Details / Forensic Steps:

Containment and Recovery

Containment Measures:

Systems Restored:

Summary and Recommendations

Summary of Findings:

Remediation & Recommendations:

Additional Notes