

Network Security Incidents Detection and Analysis

Note: Prior to starting the detection and analysis of network security incidents, Section 1, Section 2, and Section 3 must be filled with required information.

Section 1: Details of the Organization

| | |
|--|--|
| Organization Name: | |
| Contact Number: | |
| Website: | |
| Address: | |
| <i>Additional Contact Information:</i> | |
| | |

Section 2: Details of the Incident Responder

| | | | |
|---|--|-------------------------------|--|
| Date Report Received: | | Date Report Processing Began: | |
| Name: | | Report Number: | |
| Title: | | Department: | |
| Email Address: | | | |
| Phone Number and, If Applicable, Extension: | | | |

Section 3: Type of Incidents

| | | |
|--------------------------------|-----------------------------------|-------------------------------|
| <input type="checkbox"/> Wired | <input type="checkbox"/> Wireless | <input type="checkbox"/> Both |
|--------------------------------|-----------------------------------|-------------------------------|

Section 4: Detecting and Validating Security Incidents

☐ Unauthorized Access Incident

- ☐ Reconnaissance attack
- ☐ Sniffing and spoofing attack
- ☐ Firewall and IDS evasion attack
- ☐ Brute forcing attack
- ☐ Other attacks: _____

Technique used:

Tools used:

Results obtained:

☐ Inappropriate Usage Incident

- ☐ Insider threat
- ☐ Downloading and dissemination of malware
- ☐ Inappropriate use of organization mail service
- ☐ Data leakage
- ☐ Other attack: _____

Technique used:

Tools used:

Results obtained:

☐ **Denial-of-Service Incident**

☐ Volumetric attacks

☐ Protocol attacks

☐ Application layer attacks

☐ Other attacks: _____

Technique used:

Tools used:

Results obtained:

☐ **Wireless Network Security Incident**

- ☐ Sniffing attack
- ☐ Rouge access point attack
- ☐ Evil twin attack
- ☐ Jamming attack
- ☐ Other attack: _____

Technique used:

Tools used:

Results obtained: