Incident Number #

| **GENERAL INFORMATION** | |
| --- | --- |
| Team Number |  |
| Reporter(s) Name(s) |  |
| Time Incident Identified | [YYYY-MM-DD-xx:xx:xx] |
| Target of Attack |  |
| Status | [Site Under Incident, Incident Investigation In Progress, or Incident Closed] |
| Severity | [Minimal, Moderate, Severe, or Catastrophic] |
| Type of Incident | [Outage, Malware, Shellcode, Unauthorized Access, Data Breach, Remote Execution, DDoS, Exploit, High embarrassment factor, Recon, Other ] |
| **Executive Summary:** | |

| **BUSINESS AND INFRASTRUCTURE IMPACT** | | | |
| --- | --- | --- | --- |
| Attack Vector | [fill in] | Services Affected | [fill in] |
| Recoverability | [fill in] | Information Impact | [ yes or no] |
| Was any sensitive information leaked? | [yes/no] | If yes, specify what type of data was leaked. | [fill in] |
| Has any data been changed? | [yes/no] | If yes, specify what type of data was changed | [fill in] |
| Number of systems affected | [fill in] | Nature of loss, if any | [environmental, human] |
| System Downtime | [fill in] | Cost of Incident | Unknown  None  <$10K  $10K-50K  >$50K |

| **DESCRIPTION OF INCIDENT/ACTIVITY** | | | |
| --- | --- | --- | --- |
| Time First Identified |  | Time Last Identified |  |
| System(s) Impacted |  | User(s) Impacted |  |
| Record(s) Impacted |  | Location(s) of Observed Activity |  |
| Root Cause of Incident |  | Level of Access Gained | [Root / administrator  other user  domain controller admin] |
| Apparent Source | | - If DoS or DDoS and which IP(s) it came from - Specify if the attack was domestic, foreign, or insider if scan or DoS  - If malicious software, specify which piece of software. Downloaded from online? Attach link | |
| **Primary system or network involved:**   * IP addresses (full) or subnet addresses (CIDR): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * Hostname: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * OS version(s): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * NOS version(s): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | |
|
| **Indicators of Compromise/Root Cause of Incident:**   * [technical description] * [expand upon apparent source] * [possible things to include: machine/mac address, source IP, Destitation IP, subnet with CIDR, systems involved and OS involved, PORT/protcols] | | | |
| **Attack Description:**  [technical description of how was the attack carried about specifically?] | | | |
| **Attack Detection:**  [technical description] | | | |
| **Mitigation Action Taken (if any):**  [technical description] | | | |

| **Lessons Learned** |
| --- |
|  |

| Supporting Artifacts Page \_\_\_ of \_\_\_ |
| --- |
|  |