|  |  |  |  |
| --- | --- | --- | --- |
| Team #  Incident Report |  |  |  |

**MM/DD/20YY 0000 EST**

White Team,

One of our analysts has discovered a cybersecurity incident with the following details.

**Who:** The source of the incident originated from [NAME/CLASS OF ATTACKER & IP ADDRESS].

Screenshot of .

**What:** The incident targeted the [MACHINE NAME] server located at [PUBLIC IP ADDRESS] by employing [METHOD OF ATTACK]. This produced [SPECIFY OBSERVED RESULT] which our analyst noticed. This downtime [STATE BUSINESS EFFECT TO END-USER/CUSTOMER].

Screenshot of .

**When:** The incident is estimated to have occurred on or around [0000] hours today per [REASON/SCREENSHOT/TIMESTAMP FOR SAID TIME].

Screenshot of .

**Where:** The incident involved only [AFFECTED MACHINES]. It was contained due to [CONTAINMENT REASON].

**Why:** Given the context of the incident, this is an attack by the red team against our network.

**How:** The incident was made possible in part by [VULNERABILITY]. This vulnerability has since been remediated by [ACTION TAKEN]. These actions have already produced [REMEDIATION RESULTS].

Screenshot of .

Very Respectfully, Team #