|  | **0** | **1** | **2** | **3** |
| --- | --- | --- | --- | --- |
| **Attack** | | | | |
| **Vulnerability**  (30%) | The team did not understand any aspect of how red team obtained access to their system. | The team understood some aspects of the vulnerability and how red team may have abused it, but they did not correctly identify red team’s actions. | The team mostly understood how red team obtained access to their system. However, a few minor details were either incorrect or missing. | The team demonstrated complete understanding of how red team obtained access to their system. |
| **Impact**  (10%) | The team did not understand how the system was affected. | The team understood some aspects of how the system was affected, but they failed to understand key changes red team made to their system. (ie. they saw the service was not scoring but were not sure why) | The team mostly understood how the system was affected. However, a few minor details were either incorrect or missing. | The team demonstrated complete understanding of how the system was affected, including any impacted services. |
| **Response** | | | | |
| **Eradication**  (15%) | The team did not do anything to hinder red team’s current access to the system. | The team limited red team’s level of access to the system in a way that posed little significance to red team activities. | The team took corrective actions that significantly impacted but did not fully remove red team’s access, or the team fully removed red team’s access in a suboptimal manner that could have allowed them to retain access. | The team appropriately and fully removed the access that red team had obtained by abusing the vulnerability. |
| **Remediation**  (20%) | The team did not remediate any aspect of the vulnerability that red team used to obtain access. | The team remediated some things that may have contributed to the vulnerability but were unable to fully remediate the vulnerability so that it could no longer be abused. | The team remediated the vulnerability itself but did not fully remediate/remove all artefacts that contributed to the vulnerability. (ie. they removed a beacon executable but not the scheduled task that starts it) | The team fully remediated the vulnerability so that it could not be further abused. |
| **Documentation** | | | | |
| **Proof**  (10%) | The team did not provide any screenshot evidence. | The team provided screenshot evidence for some sections, but either most sections were missing or the evidence provided was poor. | The team provided screenshot evidence for most sections, but either they missed a section or the evidence was incomplete. | The team provided complete screenshot evidence for all sections, including:   1. A screenshot of the vulnerability (if applicable)\* 2. A screenshot of logs demonstrating red team abusing the vulnerability to gain access 3. A screenshot of commands run and steps taken to remove the attacker’s access 4. A screenshot of commands run and steps taken to remediate the vulnerability   Copy-and-pasted commands and output will be accepted in place of traditional screenshots. |
| **Clarity**  (10%) | A technically competent reader could not understand the information the team was trying to convey. | Considerable extra time was spent by the grader to understand the information presented. | Explanations were understandable by a technically competent reader, but either the presentation was suboptimal or the wording was complex. | All explanations were clearly written so that a technically competent reader could follow them.  **Note:** Minor misspellings and grammar errors are permissible so long as they don’t detract from readability. |

\*A screenshot of the vulnerability is only necessary when the vulnerability itself can be observed separately from an attacker’s actions.  
For example, if red team gained access using a PHP webshell, teams should include screenshots of both the vulnerable code itself and logs of the attackers abusing it. A screenshot of the vulnerability is not necessary when there is no quantifiable evidence other than its abuse, such as the use of weak credentials. Teams should use their best judgement in determining whether a screenshot of the vulnerability is relevant for their scenario.

**General Information (Incident Info)**

All of the following items were accurately documented: (5%)

* Source IP Address (if applicable)
* Destination IP Address or Affected IP Address
* Port and Service
* Initial Access Timestamp
* Service Downtime (start and end)
* Remediation Timestamp
* Affected Account (the account red team was using for access)