Security DocumenTation

Team ID: \_\_\_\_

Documentation file name must include your team ID.

Do not reference your College/University.

|  |
| --- |
| System Overview Briefly describe the overall system and its purpose (in 250 words or less).  *One cannot secure a system when its purpose and scope are unknown.*  *[Note: The audience for this section is “senior leadership”, so please write accordingly.]*  Click or tap here to enter text. |
| Asset Inventory List all of the system’s devices, by name, and their key attributes in the following table.  *Asset management is a critical component of operational technology security. One cannot secure a network when one does not know what devices and services are running on the network.*     |  |  |  |  |  | | --- | --- | --- | --- | --- | | **Host** | **OS** | **IP Address** | **Port** | **Service** | | *Webserver* | *Windows 95, SP 1* | *10.X.X.X* | *80* | *HTTP* | |  |  |  |  |  | |  |  |  |  |  | |  |  |  |  |  | |  |  |  |  |  | |  |  |  |  |  | |  |  |  |  |  | |  |  |  |  |  | |  |  |  |  |  | |  |  |  |  |  | |  |  |  |  |  | |  |  |  |  |  | |  |  |  |  |  | |  |  |  |  |  | |

|  |
| --- |
| Network DiagramProvide a network diagram for your system. All hosts, network appliances, and services should be identified. *Current and detailed network diagrams facilitate enhanced situational awareness, especially for new staff that may be responding to a cyber security incident.*  *[Note: Focus on the information content—a thorough, hand-drawn diagram will score higher than an incomplete “visio” diagram.]* |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| PLEASE LIST ALL vulnerabilities you found and the mitigations YOU TOOK FOR EACH The CyberForce Competition environment was “seeded” with many vulnerabilities. List each vulnerability that you were able to identify. For each vulnerability, also list the mitigation(s) that you were able to enact (e.g., system hardening, software patch, compensating control, operational procedure).  *[Note: Add a row to the table for each unique vulnerability per host. For example, if Alice, Bob, and Carol all have weak passwords on host Foo, this merits one line in the table. If Alice, a network admin, has weak passwords on three hosts, then three lines should be added to this table.]*  *[Note2: Security documents often include a section of known issues—both those that have been resolved as well as open issues that may or may not yet have mitigating controls.]*  *[Note3: The audience for this section includes “senior leadership”. Please summarize your results as appropriate. Including “raw” vulnerability report(s) in this section does not meet the senior leadership audience requirement.]*   |  |  |  | | --- | --- | --- | | **Host/System** | **Vulnerability** | **Mitigation(s)** | | *Foo* | *Weak user passwords* | *Changed passwords to meet password policy.* | | *Bar* | *CVE-XXXX-YYYY* | *Applied vendor patch.* | | *Baz* | *CVE-XXXX-ZZZZ* | *Open, to be mitigated in the next cycle.* | |  |  |  | |  |  |  | |  |  |  | |  |  |  | |  |  |  | |  |  |  | |  |  |  | |  |  |  | |  |  |  | |

|  |
| --- |
| System Hardening In 1250 words or less please describe and justify the procedures your team used to harden and defend your systems for the competition. This description should include a list of the tools that you used.  *Cybersecurity professional must proactively harden and defend their systems. It is not enough to just mitigate known vulnerabilities, professionals establish and follow procedures that ensure consistent, day-to-day excellence.*  Click or tap here to enter text. |