IT Security Incident Reporting Form

**Instructions: For you to re-coop some of your compromised points, please submit this per incident.**

|  |  |  |
| --- | --- | --- |
| **1. Contact Information for this Incident** | | |
| TEAM #: 26 |  | |
| **2. Incident Description**. | | |
| Provide a brief description of the Incident:    TeamViewer was not shutdown and an unauthorized user tried to gain access to Aviator but failed. As a result, we shutdown TeamViewer and began usering TCPViewer. Image is also attached to email. | | |
| **3. Information: Check & Fill In** all of the following that apply to this incident. | | |
| c Loss / Compromise of Data:\_\_\_\_None\_\_\_\_\_\_\_\_\_\_\_  c Damage to Systems: \_\_\_None\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  c System or Service Affected:\_\_TeamViewer\_\_\_\_\_\_\_\_\_\_\_\_\_  c IP Address:\_\_\_198.168.220.104\_\_\_\_\_\_\_\_\_\_\_\_\_\_  c System Name:\_Aviator\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | |
| Provide a brief description:  Unauthorized user attempted to enter machine through TeamViewer but did not succeed. | | |
| **6. What Steps Have Been Taken So Far?** Check all of the following that apply to this incident. | | |
| c No action taken  c System Disconnected from network  c Updated virus definitions & scanned system | | c Restored backup from tape  c Log files examined (saved & secured)  c Other – please describe: |
| Provide a brief description:  We disabled TeamViewer and enabled TcpViewer from windows system introduced | | |

**Please submit this completed form to: whiteteam@wrccdc.org**