Inject Response

|  |
| --- |
| BLUE TEAM X |

|  |  |
| --- | --- |
| To: | White Team |
| From: | Blue Team X WebApps Admin |
| CC: |  |
| Date: | 2/11/2018 |
| Re: | Inject # 04 / Security Assessment |
| Comments: | Top Three Operating System Risks:   * Default, weak, or compromised passwords. Can be mitigated by changing passwords frequently with strong passwords. * Default, weak, or compromised firewall configurations. Can be mitigated by running Security Configuration Wizard, resetting firewall configuration, and locking down firewall rules. * SMB Remote Code Execution (CVE-2017-014/0272). CVSS Score of 9.3 out of 10. Allows running of code remotely without authentication if not patched. Relatively new, so also relatively unpatched.   Top Three Service Risks   * Default, weak, or compromised passwords. * Misconfigured permissions within IIS/Sharepoint. Verify that least privilege is implemented. * Sharepoint Privilege Escalation (CVE-2018-0789). CVSS Score of 9.0 out of 10. Allows a normal user to run privileged commands by sending a specially crafted HTTP request. |