Administrative Computing

Vulnerability 01/20/22 Remediation Plan

Below is a summary of actions that will be taken on servers to correct identified problems.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Spreadsheet Rows | Server Name | IP Addresses / FQDN | Remediation Plan | Disposition | Schedule Date for Resolution |
| 5-34  268 – 297  587 - 616 | Linux6 | 192.168.6.118  Gears.galencollege.edu  linux6.galencollege.edu | Plan to transition products on server to Docker Containers with updated PHP versions compatible with product. Timeline for completion is Early Q2 2022 depending on availability of development resources.   1. Gears will be moved to another server or put into a docker container. The CakePHP framework required for the application may have limitations on PHP version that can be supported. 2. Upgrade PHP to 7.3+ 3. Upgrade Apache to latest version 4. (or) migrate products to docker containers with updated versions. | Not Started | End of Q2 2022 |
| 35-125  178 – 267  299 – 389  421-516 | Linux1 | Writingcenter.galencollege.edu 192.168.6.119 resourcecenter.galencollege.edu  Training.galencollege.edu | Server is end of service for the OS and is being replaced. Only ResourceCenter is remaining as production on this server and will be moved either to a new server or Docker container.  writingcenter.galencollege.edu is currently decommissioned and responds with an empty page.  1. Delete the writingcenter.galencollege.edu DNS entry 2. Migrate resourcecenter.galencollege.edu to new server / docker container. PHP version will be updated during migration.  3. Delete the training.galencollege.edu as that site is not longer being used | In Progress | End of Q1 2022 |
| 126-143 | Docker00 | Docker00.galenhi.galened.com  192.168.6.150 | 1. MySQL – Service was never used in production. Container running MySQL will be shutdown. 2. Row 133 – NFS is a required service and limited to the servers necessary for operation of the docker environment. Will resolve by setting up a firewall on the local machine to block connections to NFS to only those required servers 3. SSH Depreciated Cryptgraphic settings. Additional review necessary. Docker environment will be replaced FY 2022 which should resolve this issue 4. Depreciated TLS on 443. Will review Traefik documentation to remove protocols from being used | In Progress | #1 End of Q1 2022  #2-4 End of Q2 2022 |
| 144 - 159 | Docker01 | Docker01. galenhi.galened.com 192.168.6.151 | Same as Docker00 | In Progress | #1 End of Q1 2022  #2-4 End of Q2022 |
| 160-175 | Docker02 | Docker02. galenhi.galened.com 192.168.6.152 | Same as Docker00 | In Progress | #1 End of Q1 2022  #2-4 End of Q2022 |
| 176 | Dashboarddb01 | dashboarddb01.galenhi.galened.com  192.168.6.153 | Research needed before determining resolution on SSH protocols | Not Started |  |
| 298 | ? | acr01.galenhi.galened.com | Not familiar with this server – Sean reports this is an Avaya server. Remediation efforts will be on another team | No Action Necessary |  |
| 390-416 | Linux8 | linux8.galenhi.galened.com | Run patch updates to update Apache / Open SSL | Not Started | End of Q1 2022 |
| 417-418 | Linux9 | Linux9.galenhi.galened.com | Run patch updates to update Apache / Open SSL | Not Started | End of Q1 2022 |
| 419-420 | Linuxdb01 | linuxdb01.galenhi.galened.com | Run patch updates to update Apache / Open SSL | Not Started | End of Q1 2022 |
| 517-556 | Linux3 | linux3.galencollege.edu  ctools.galencollege.edu | Server is running software that is limited to the php5 branch. We are looking to rewrite the software that is on this server, but do not have a ETA. | Not Started | No ETA |
| 557 – 586 | Linux5 | stage-trainingmoodle.galencollege.edu | Old php and apache. Run patch updates. | Not Started | End of Q1 2022 |
| 617-646 | Dockerdev01  Dockerdev02  Dockerdev03 | dockerdev01.galencollege.edu | Docker dev environment will be rebuilt and these servers decommissioned. | Not Started | End of Q2 2022 |