Washington Unified Network Vulnerability

Results of Scan on May 4, 2016:

The Nessus scan performed on May 4, 2016, reported 72 vulnerabilities across 21 hosts. The breakdown by severity of vulnerability included 9 critical, 1 high, 37 medium, 6 low, and 285 information. The scan took approximately 1 hour to complete and detected critical vulnerabilities with plugins categorized as Windows. These 9 critical vulnerabilities were on 6 different ports that included the following usage:

- Microsoft Exchange Server for district-wide email service
- Aeries Browser Interface (ABI).net Server for Grade Monitoring
- Open-44 - unknown open port
- WUSD Web Server
- Open -146 - unknown open port
- Aeries Server for Grade Monitoring

The one high vulnerability was on an Open-254 port that indicated a Dell Laserprinter as the operating system. This port is the gateway and is not public facing, but does need to be investigated further to disable the SNMP service.

Critical and High Vulnerability Resolutions

The vulnerability scans were shared with the Systems Engineers and reviewed by host and vulnerability. In this meeting, it was determined that the critical Windows vulnerabilities could be remedied by installing the necessary patches. It was also discovered that there were several open ports that were no longer being used by the district such as ABI and Destiny Math, and several that were defaults with no actual purpose or use. The following solutions were put into place and resulted in the resolution of the critical and high vulnerabilities.

Microsoft Exchange Server for district-wide email service

Prior to the meeting to review the vulnerability scans, the district sustained a major disruption in email service when a teacher send a very large image to all staff and did not reduce the original file size. As others replied all to the celebration shared in the email, the amount of storage space on the Exchange server was greatly impacted until service was completely halted due to no space. Fortunately, the Systems Engineers were able to manually backup the data across the 5 servers using a Windows Server Partition Tool called Partition Master Server 11.0 which minimized downtime during critical work hours.

As a result of this incident, the Windows patches were installed, access to the WUSD-STAFF distribution list was removed for all staff with the exception of certain managers and cabinet level positions, and messaging about the importance of sending links to images and videos rather than the actual files and how not to respond via Reply All has begun. All critical vulnerabilities for this host have been resolved and current scan shows 7 information details.

Aeries Browser Interface (ABI).net Server for Grade Monitoring

This service is no longer being used in the district and the server has been disabled/turned off and is not showing up in a post-scan.

Open-44 - unknown open port

This server was identified as the DRDPTECH server and has been patched. A post scan shows 16 information details and no vulnerabilities.

WUSD Web Server

The district web server has been patched and shows no critical vulnerabilities. There remains 1 low vulnerability in the disclosure of the internal IP address that is not hidden or masked.

Open -146 - unknown open port

This server was identified as the old web server for www.wusd.k12.ca.us and was patched. It was determined that this server runs survey software and web attendance for Yolo High school, the district’s continuation high school. It also hosts the iBoss block page. A post-scan shows 11 information details and no other vulnerabilities.

Aeries Server for Grade Monitoring

The Aeries.net server was patched and shows no vulnerabilities and 21 information details during a post-scan.

Open-254 - High Vulnerability

This server hosts the Enterasys B5. The web services and public SNMP have been disabled. The post-scan shows no vulnerabilities and 3 information details.

A second scan of the external network was performed on May 14 and the results were shared with the Systems Engineers via email. The vulnerability scan showed no critical or high vulnerabilities and 6 medium, 1 low, and 178 information details.

Next Steps

To avoid reaching vulnerabilities classified as critical or high in the future, the technology team will implement a practice of quarterly scans on all servers. The department will purchase subscriptions from Nessus to perform internal and external scans which will be conducted quarterly to determine vulnerabilities. In addition to the scans, the Systems Engineers will put a server maintenance schedule in place in which all servers will be scheduled for updates and patches on a quarterly basis. This will create a proactive cycle that is ongoing and spread throughout the quarter rather than a reactive annual or semi-annual approach to server maintenance. The technology team understands the critical need for cyber security and, through these implemented practices, will be able to better manage security both externally and internally to protect the network.