

U.S. Department of Energy Thomas Jefferson Site Office



Site Office Walkthrough
Of the Cyber Security Vulnerability Program
At the Thomas Jefferson National Laboratory

April 3, 2009

Table of Contents

1.0 INTRODUCTION	3
2.0 SCOPE	3
3.0 ASSESSMENT METHODS.....	3
4.0 REPORTING THE WALKTHROUGH RESULTS	3

1.0 INTRODUCTION

In accordance with DOE O 226.1, *Implementation of Department of Energy Oversight Policy*, the U.S. Department of Energy (DOE) Thomas Jefferson Site Office (TJSO) performs oversight of Jlab operations. The purpose of this walkthrough on January 15, 2009, was to observe, and note observations, weaknesses or findings on performance within the Lab’s Cyber Security Vulnerability Program.

2.0 SCOPE

The walkthrough focused on the following areas:

- Verification process used to close actions
- Vulnerability identification process
- Vulnerability remediation process
- Validation of identified vulnerabilities
- Patch Process flow from identification, to lab entry, to implementation
- Processes that are different from the previous focus assessment

3.0 ASSESSMENT METHODS

Approach – Interviews of management, cyber leads, and cyber staff within the Computer Center. Visual observation of software logs, configuration settings, and other related screen shots.

Issues Categorization Observations may represent areas for improvement, but do not represent noncompliance with actual requirements. Proficiencies (positive work practices) will also be noted where commendable practices are observed.

Interviews Conducted

Computing and Network Infrastructure Head
Cyber Security Manager
Network Manager
Cyber Security Analyst
Windows System Administrator

4.0 REPORTING THE WALKTHROUGH RESULTS

Summary

Strong communication exists among staff involved with detection, remediation, and implementation of vulnerabilities and alerts. The close proximity of office locations is a key strength and the use of informal as well as structured meetings limits surprises and missed corrections. The CNI (Computer Network/Infrastructure) Manager has empowered staff at various points in the decision-making process, and he is quite knowledgeable of the activities that occur within this program. These are all strong assets.

However, it is noticeable that a strain exists on resources, particularly staffing levels, as complex software is requiring more time for customization and script writing. The planned addition of HelpDesk staff for the summer months might help overall coverage within the CNI Division as the HelpDesk is currently staffed at ½ day. Currently there is more control of desktops than the previous walkthrough and therefore less vulnerabilities showing up on reports. Some of these desktops cannot be touched, but as mitigation, adequate firewalls are in place. The Guest network, a wireless network, has seen an increasing number of signals, and those on that network can now be locked down by MAC address. The registration process allows tracking of IP addresses and this can be done at ARC, VARC, CC, Test lab, EEL (office spaces), county house, and the FEL.

Credant software is being utilized on laptops and the fileserver is locked down using ACLs. NESSUS 3 is now utilized by the cyber security staff, and early indications show it to be more comprehensive and better-suited for their needs than the previous software (VAM). There are now more static IPs and the cyber team is more in tune with the history of the IP at any point in time as they know about MAC addresses where the VAM utility didn't. The Site Office observed SECLOG (CClog)(patches approved). One Cyber Specialist is working IDS, SNORT/SQUIL and the other specialist is devoting ~10%-15% of his time on this.

One commendable feature to the team is that the specialist is forced to look at every alert and categorize it. Sensors play a pivotal role and each has a disk array and when 95% capacity has been reached, they are reset. A critical item to note is that the Lab is seeing all data coming in and out of the Lab. Sensors are started each day with signatures and failure is rare. An email is sent to the specialist and the sys log server, and thus to SNORT. Events are backed up to November as they are kept for three months and then archived.

Identification/Remediation

Interaction between security-related staff is solid. Weekly Security Team meetings take place on Wednesday afternoons, a CNI staff meeting (including the Security staff) occurs on Wednesday morning, and stand-up status meetings for the entire CNI group are held on Monday and Friday mornings. Good exchanges take place between the security analysts and Windows administrators.

Patch Process

Summary entities such as US CERT, SANS, patch lists, and patch Tuesday are utilized. SANS weekly letters are also used and the entire security team gets notifications.

All staff involved in the patch process is empowered to make the call on the install of patches, which frees up the involvement of the Computing Network Infrastructure Head.

There is excellent dialogue with Computer Center and Accelerator Division regarding patching and patch levels have been available for the substantial amount of incoming data calls. These are sample indications that the process is working. Verification for the closure of actions has been noted as no internal sources are hacked, the use of Monday-Wednesday-Friday meetings, and the fact that VAM supplements server-missed vulnerabilities. The Accelerator group is also included as responders in the Computer Center Problem Reporting system (CCPR) which ensures close-out of specific tasks, such as applying patches to vulnerable machines within their group.

Windows patch management

Email notifications come in from the vendors as well as the Security Team. The default method is for those identified by the vendor as “critical” to be immediately sent to the test bed. Otherwise (those designated as important, update, or patch) are included in the monthly maintenance day process.

The verification process for closed actions is solid. After patch Tuesday, the latest that patches are installed is Wednesday night. Feedback from users regarding negative impacts would normally take place by Friday at the latest. Discussion of any impacted clients takes place at the regularly scheduled Monday morning meeting.

The SUS Server is checked after each maintenance day. The use of WSUS 3.0 is providing better reporting. The Site Office reviewed and verified several of these reports as upgrades per machine and per patch were reported. With the previous version, WSUS 2.0, they could only report the security patch for the OS and now it's any MS patch.

The Lab has joined the Argonne Federated Model which is used to identify blocked sites. This could potentially be an enhancement and further time will be needed to examine its overall ability. Due to the volume, complexity, and political sensitivity of data calls, the CNI Manager is pulled more into the response process, and is challenged to devote time to his managerial duties.

The Computer Center should be commended for the flexibility and willingness of its staff to reach out beyond their respective duties in an effort to sustain performance levels.