Development of Computer Vulnerability Scanning
Scanning Workgroup
University of California, Davis
Draft Report - April 19, 2004

Background

During fall 2003, a large scale Internet worm exploited a widely known Windows operating system vulnerability throughout academic institutions in the United States. This worm infection (W32.Blaster) presented serious risks to the integrity and availability of computing systems attached to the campus network. In response to this vulnerability, UC Davis developed and implemented several emergency measures to identify susceptible Windows remote procedure call (RPC) services and provide corrective tools and information to remove the vulnerability or, if necessary, disinfect worm infected computers. This vulnerability reduction and infection removal effort specifically included:

- An individual vulnerability probe that was initiated against a computer which was used to access a web-based campus application. If vulnerability was detected, the user web browser was redirected to information describing corrective resources. Authentication was not permitted unless relevant security patches were installed. Due to broad campus usage of web-based authentication services, this vulnerability scan compelled many students, staff and faculty to apply critical security patches.
- An automated scan of computers connected to the campus data network to identify computers with RPC vulnerabilities. This scan was conducted twice per day and the scan results stored into a database.
- An intrusion detection sensor placed at the campus border to identify computers generating infected and malicious traffic entering or leaving the campus computing network.
- A network honeypot placed on an unused network segment to identify infected computers attempting to scan or connect to non-existent hosts.
- The creation and distribution of CDs with corrective patches and infection removal tools.
- On-site staff assistance to Student Housing technology specialists during fall 2003 opening of the on-campus residences.

The results from the probe vulnerability scan, intrusion detection scan and honeypot were stored in an online database. Campus technical staff was provided query function against the database to identify vulnerable or infected computers within campus unit VLANs. In addition, campus modem pool permits for individual computing accounts were temporarily revoked if infected RPC traffic was traced the campus modem pool user. The modem pool permits were reactivated after the infection was removed.

The above approach was highly successful in quickly reducing RPC vulnerabilities and removing computer infections relating to exploited RPC vulnerabilities. Accordingly, questions were raised as to whether the RPC vulnerability and infection detection tools could be modified to seriously reduce threats to campus computing by proactively identifying computers that are susceptible to *anticipated* exploits rather than limited to reacting to an existing attack.

A workgroup was formed in early January to assist the campus to determine the feasibility of adding new vulnerability detection functionality to the emergency RPC vulnerability scanning and reporting mechanism. If feasible, the workgroup was asked to outline the development tasks and resources required for such expansion. Estimates for resource requirements would include software, hardware, labor for development and maintenance for the support of critical vulnerability identification, vulnerability signature creation, integration with existing intrusion detection/infection databases and vulnerability reporting. The workgroup was also asked to propose a timeline for completion of the expansion efforts. The workgroup, consisting of broad campus representation, met during the first quarter of 2004 to address its charge (See attachment 1).

Emergency RPC Vulnerability/Infection Detection System

The following diagram, Figure 1, describes the key components of the existing campus RPC vulnerability and infection detection system. The systems are currently in operation and have been modified once to evaluate the spread of the recent MyDoom virus infection. This system was developed and implemented using about $45,000 of new hardware and labor expenses of about $24,000. Currently, $20,000 is allocated to support annual recurring expenses for hardware replacement and administration.

Expansion Feasibility

The workgroup examined whether the current vulnerability detection system could be changed from a reactive into a proactive detection and reporting mechanism. The workgroup defined a proactive system as an infrastructure service which could identify computer and network vulnerabilities before exploits taking advantage of the vulnerabilities are broadly released into the Internet community, evaluate campus risk from such threats, modify existing scanning programs to detect the most critical vulnerabilities before they could seriously disrupt campus computing and enhance campus reporting systems to notify campus students, staff and faculty of the identified vulnerabilities and suggested corrective measures.

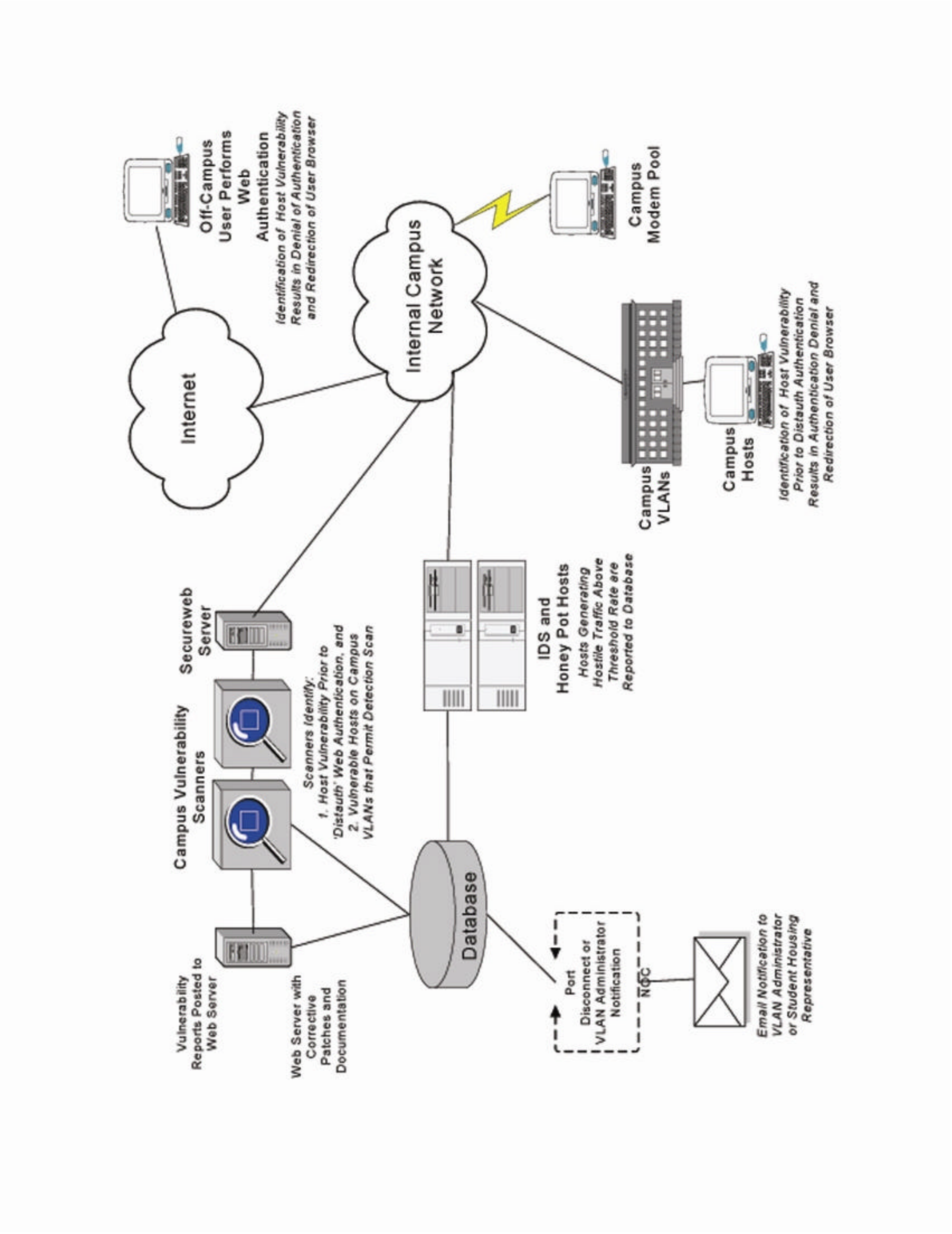
Vulnerability Reports Posted to Web Server
Web Server with Corrective Patches and Documentation
Campus Vulnerability Scanners
Scanners Identify:
1. Host Vulnerability Prior to 'Distauth' Web Authentication, and
2. Vulnerable Hosts on Campus VLANs that Permit Detection Scan
Secureweb Server
Database
Port Disconnect or VLAN Administrator Notification
NOC
Email Notification to VLAN Administrator or Student Housing Representative
IDS and Honey Pot Hosts
Hosts Generating Hostile Traffic Above Threshold Rate are Reported to Database
Internet
Internal Campus Network
Off-Campus User Performs Web Authentication
Identification of Host Vulnerability Results in Denial of Authentication and Redirection of User Browser
Campus Modem Pool
Campus VLANs
Campus Hosts
Identification of Host Vulnerability Prior to Distauth Authentication Results in Authentication Denial and Redirection of User Browser

Figure 1
Existing Windows RPC Vulnerability Identification and Reporting System

Developing the emergency RPC detection and reporting system into a robust production vulnerability detection and reporting system would require the following key program enhancements:

1. Provide production-level administrative support for all hardware components of the scanning system
2. Implement new staff responsibilities for monitoring new vulnerabilities and evaluation of campus risks posed by such vulnerabilities
3. Contract with a commercial service to identify computer/network vulnerabilities, analyze the vulnerabilities and provide information relating to vulnerability removal or bypass
4. Regular update of critical vulnerability patterns/signatures within vulnerability scanning systems and communication of measures to prevent or correct vulnerability exploitation
5. Development and maintenance programming for a Distauth plug-in module that can easily be updated to reflect new computer critical vulnerabilities
6. Programming to develop, test and update vulnerability signatures into a web authentication scanner and network vulnerability scanner.
7. Development and maintenance of a quarantine network segment reserved for the isolation of vulnerable and/or infected campus residential computers. This quarantine network segment could provide access to operating system updates and anti-virus updates.

The workgroup concluded that such a proactive vulnerability scanning and reporting system could be developed and maintained by augmenting the existing scanning and reporting system that is already in use. In fact, other than hardware acquisition to support separation of the IDS hosts from the honeypot function and the creation of a "quarantine" network segment for vulnerable computers attached to RESNET (see below), there are no major changes to the RPC system architecture. The majority of the estimated costs for moving the existing vulnerability scanning system into a production system are related to production labor support.

The conversion project could be broken into two development project phases. The workgroup recommends the first phase focus on developing and supporting a core production service which implements the first six of the above suggested program components. The second project phase could focus on the remaining seventh program component. The seventh activity on the above list, development and operation of a quarantine network, represents significant new design, implementation and maintenance responsibilities.

In order to develop and implement the core infrastructure service, represented by the seven activities described above, the workgroup recommends creation of a policy formally recognizing that computers with critical vulnerabilities will be denied access to the campus computing network. The workgroup also recommends campus financial support for additional one-time and recurring hardware, software, contract and labor expenditures that are required to implement and maintain the vulnerability scanning infrastructure service. The expenditures and related costs estimates are discussed below and summarized in Table 1.

POLICY – The workgroup believes that a campus policy is needed to formally establish that computers with critical vulnerabilities – *regardless of the existence of broad* *malicious activity taking advantage of the vulnerbility* – must be remedied or be denied access to the campus computing network. The workgroup further suggests this policy require users to remove or bypass critical vulnerabilities in timely manner; IET to develop and maintain vulnerability scanning and reporting systems; senior campus administration to authorize the addition or removal of critical vulnerabilities from the scanning systems; and campus units to control critical vulnerabilities and malicious traffic emanating from unit VLANS and to conduct vulnerability scans within network segments isolated from campus scanning tools by campus unit VLAN firewalls (See Attachment 2).

ONE-TIME ACTIVITIES – In order to implement the vulnerability scanning service there are several one-time project tasks that must be completed. The workgroup estimates that these project tasks will cost about $56,700 in new one-time expenses. This expense will permit the existing vulnerability scanning system to migrate into a campus production service with on-going administrative support. These estimated costs can be further broken down as follows:

<u>Network Honeypot Acquisition and Support</u> - Due to resource and time limitations, a single RPC honeypot was temporarily co-located on the intrusion detection sensor. Moving the honeypot function to a separate computer is recommended. As the honeypot does not require a robust hardware platform, the workgroup estimates the costs of the hardware and initial hardware setup/administration to be about $3,500.

<u>Distauth Module</u> - The integration between Distauth web authentication and vulnerability probe scanners was the result of a temporary program modification. The workgroup recommends this integration module be migrated to a separate plug-in module. The separate program module would minimize risks of inadvertent modification of the broader Distauth authentication system. The development of the Distauth vulnerability scanner plug-in would require an estimated 40 hours of development and testing time. This time reflects a labor expense of about $3,200.

<u>Vulnerability Analysis</u> - While vulnerability identification and analysis for the broad range of operating systems and applications could be performed solely by campus technical staff, there are existing commercial services that provide similar services. Use of these commercial services would provide greater analytical breadth and timeliness than could be achieved if this function was performed in-house. Furthermore, use of a commercial service would reduce campus opportunity costs. Contracts for a commercial vulnerability analysis service runs about $10,000 per year.

<u>Programming Support</u> – Programming support is needed to integrate the results from the vulnerability analysis into the probe scanner, network scanner, honeypot and intrusion detection sensor. This support includes development, testing and production migration.

<u>Quarantine Network</u> - During meetings between workgroup members, and representatives from Student Housing and Communication Resources, it became apparent that more efficient vulnerability/infection notification of student residents is needed. Presently, computing system vulnerability/infection notifications to campus residents are handled between Student Housing conduct coordinators and senior Student Housing administrators and network support staff. When such notifications involve hundreds of students, the coordination between students, Student Housing and Information and Educational Technology staff becomes cumbersome, at best. Substantial personnel time is spent coordinating network disconnects and reconnects.

Moreover, as resident computers are disconnected from the network until the problem condition is corrected, students may have limited computer access to both academic material and corrective patches/utilities.

During a discussion between Student Housing and IET staff, Student Housing requested that in the future student disconnect notifications from an enhanced vulnerability detection mechanism be conducted via email. Students would be reminded by Student Housing to use another computer (e.g., a Learning Resource Center computer) to check email notifications when their network service is disrupted. The student computer connection would then be moved to a separate "quarantine" network segment that would permit students minimal connectivity to access corrective patches and/or infection removal tools. The use of email notifications and a "quarantine" network does result in additional one-time network development and support activities. The workgroup estimates the additional labor and material costs to develop, implement and support this quarantine network could cost about $20,000. However, the substantial labor savings gained by Student Housing and network staff could exceed this cost.

ANNUAL SUPPORT –Annual support of the proposed proactive vulnerability system is comprised of hardware maintenance and replacement, hardware administrative costs, programming costs, contract costs, support for communicating critical vulnerabilities and corrective measures to students, staff and faculty and contract costs.

The administrative and replacement costs for most of the existing hardware used for RPC-related vulnerability and infection detection systems are currently funded. The additional hardware, annual vulnerability analysis contract and labor represent about $66,000 in new annual recurring expenses. Given existing budget challenges, funding new services with recurring expenses may be difficult. However, the workgroup believes that use of a more proactive system to eliminate critical computer vulnerabilities *before the vulnerabilities are exploited* will actually reduce the campus resources required to address these same problems on a post-incident basis.

Expense Category	One-Time Development Expenses – First Phase	One-Time Development Expenses – Second Phase	Annual Expenses First and Second Phases
Labor	$ 4,200	$ 20,000	$ 52,800
Hardware and Software	2,500	$ 20,000	5,600
Contracts	10,000		10,000
Total	$ 16,700	$ 40,000	$ 68,400

Table 1
Summary of Estimated Expenses
Expansion of Vulnerability Detection and Reporting System

Summary

The vulnerability scanning workgroup recommends campus support of the expansion of the existing RPC vulnerability detection system. The expansion should permit the development of an infrastructure service that will proactively identify critical campus vulnerabilities, require vulnerability elimination prior to the threat seriously disrupting the campus computing network, streamline vulnerability reporting and, for Student Housing on-campus residences, improve the efficiency and timeliness of corrective and restoration processes through use of a quarantine network. Ultimately, the proactive reduction of computer vulnerabilities from the UC Davis computing network will reduce campus unit labor directed towards remediation of compromised computers. The savings in personnel time would be available to other programs and services in support of the university mission for learning, discovery and community engagement.

Expansion of the existing vulnerability scanning service should start by July 1, 2004. This date will ensure that program services are available for the start of the fall 2004 academic quarter.

Attachment 1: Vulnerability Scanning Workgroup Participants

Workgroup Members:

Tom Arons, Information and Educational Technology
Ken Jones, Computer Science Department
Greg Loge, Dean’s Office, College of Agricultural and Environmental Sciences
Robert Ono, Information and Educational Technology, Workgroup Chairperson
Jatinder Singh, Campus Data Center and Client Support Services

Additional Participants:

Tracy Bennett, Student Housing
Don Dudley, Student Judicial Affairs
Doug Hartline, Communications Resources
David K. Wong, Communications Resources

Attachment 2: Suggested Policy for Proactive Vulnerability Scanning and Reporting

- **Policy**
    - Critical vulnerabilities within campus networked connected computers are to be corrected or bypassed in a timely manner
    - Campus hosts with critical vulnerabilities that threaten the integrity or performance of campus network will be denied access to campus computing resources, up to and including network disconnection
    - Campus computing hosts will behave consistent with the UC Davis Acceptable Use Policy
- **Responsibility**
    - Users must operate computers with critical operating system and application vulnerabilities removed or bypassed
    - IET will
        - develop, administer and maintain vulnerability scan systems for individual hosts and campuswide network
        - publish network scan results for campus unit technical staff
        - publish scan results for individual campus hosts
        - identify critical vulnerabilities subject to integration into individual host scanning tools
    - Information Security Coordinator will
        - approve additions/removals of critical vulnerabilities to scanning database for individual hosts
        - approve critical vulnerabilities which will be cause for denial of access to campus computing network
        - publish/maintain a list of current critical vulnerabilities for individual hosts with remediation resources
    - Campus units
        - Review vulnerability scan reports and remove/bypass critical vulnerabilities
        - Conduct independent VLAN scans or permit centrally administered vulnerability scans to transit in/out of network segments behind VLAN firewalls
        - Responsible for controlling malicious network traffic exiting from unit VLAN
- **Definitions**
    - Critical vulnerability
        - Those vulnerabilities that typically affect default installations of very widely deployed software, result in compromise of servers or standalone computers, and the information required for exploitation (such as example exploit code) is widely deployed to attackers.
    - Timely manner
        - Time response as determined by the nature of the threat in respect to potential damage and spread.