Vulnerability Scanning Policy

1 Introduction

Vulnerability scanning is an important and necessary component of any computer security plan as it provides feedback on the effectiveness of security procedures and can alert system administrators to potentially serious problems. However vulnerability scanning also has the potential to reveal protected information and is frequently used as part of an attempt to compromise system security. The following policy details the conditions under which vulnerability scans may be performed on the CSM network.

2 Summary

Vulnerability scanning is a process by which devices connected to the network are probed in an attempt to identify security related issues including, but not limited to; missing or weak passwords, insecure software installations, software with known security issues, and back-door administration programs installed on already compromised hosts.

Any equipment attached to the Colorado School of Mines' network is subject to security vulnerability scanning performed by the department of Academic Computing and Networking's security team. The following policy describes the conditions under which this scanning takes place as well as the responsibilities of the AC&N staff involved in scanning.

Hosts found to contain security weaknesses will be dealt with in accordance with standing AC&N policies (see the document *Network Users Rights and Responsibilities*.)

3 Definitions:

1. Domain-level scan: A periodic scan of all equipment attached to the CSM network targeted at known security issues.
2. Incident-response scan: An emergency scan initiated as a result of a specific security related incident.
3. Prohibited-service scan: A scan for a specific prohibited service, as defined in the department of Academic Computing and Networking's policy for network use[1].
4. Responsible User: The person ultimately responsible for the equipment in question. In most cases the user of the system, however in the case of students who are assigned equipment owned by the school, the user responsible for the system is the faculty member responsible for the equipment not the student.
5. Responsible Admin: The person (or persons) with administrative authority over the equipment. This includes anyone who performs routine maintenance on the equipment.
6. Incident response team: Those persons who are involved in responding to a specific security related incident. Only the department of Academic Computing and Networking may establish an incident response team, which is typically headed up by a member of AC&N's security team, and may also include faculty and students with a vested interested in the incident under investigation.

4 Policies and procedures

- Policies for domain-level scans:
  - Domain-level scans may only be performed by the department of Academic Computing and Networking's security team.
  - AC&N will notify the campus at least 24 hours prior to any domain-level scan.

[1] As of 1-Oct-02, the only service prohibited on campus is open mail relays.

  - Domain-level scans are performed on an opt-out basis. That is, owners of network attached equipment who do not want their equipment scanned must notify Computing and Networking of the desire to opt-out of the scan. Only the user responsible for a host may opt-out of the scanning process. AC&N will make a web-page or similar technology available allowing users to easily communicate their desire to opt-out.
  - Security issues found during domain-level scans will be communicated to AC&N's department level support staff as well as the responsible user and admin. Statistical reductions of the results of a scan may be made available to a wider audience.

- Policies for incident response scans:
  - Incident-response scans may only be performed by the department of AC&N's incident response team.
  - Incident response scans may be initiated during the investigation of a security incident without prior notification and without regard to the opt-out list.
  - Incident response scans may only be done in response to an active security related incident and will be limited to that equipment AC&N believes is threatened by or implicated in the incident under investigation.
  - Results of incident response scans will only be disclosed to members of the incident response team, and the responsible user and admin. Statistical reductions of the results of a scan may be made available to a wider audience.

- Prohibited Service Scans:
  - Prohibited service scans may only be performed by the department of AC&N's security team.
  - AC&N will notify the campus at least 24 hours prior to any prohibited-services scan.
  - Users may not opt-out of prohibited-service scans.
  - Prohibited services found during prohibited-service scans will be communicated to AC&N's department level support staff as well as the responsible user and admin. Statistical reductions of the results of a scan may be made available to a wider audience. The identified prohibited service will be dealt with in accordance with the policy for that service.

- Other scans:
  - Administrators and users responsible for equipment may (and in fact are encouraged to) scan the equipment for which they are directly responsible. Note that employees who report to AC&N have additional policies regarding scanning.
  - No one outside Academic Computing and Networking's security team is authorized to perform scans of equipment they are not directly responsible for. Such scans are considered a violation of school policy and may result in disciplinary action.