Background

Vulnerability management is an essential component of any information security program and the process of vulnerability assessment is vital to effective management. Vulnerability assessment provides visibility into the vulnerability of assets deployed in the network. Vulnerability assessment consists of scanning to identify networked assets determine the presence and assess the risk of potential vulnerabilities. The University of Cincinnati strives to continually improve its security posture to protect the integrity of data assets and the security of university community.

Policy

The IT@UC Office of Information Security will conduct periodic or continuous vulnerability scans of university systems. Targeted vulnerability assessments may also be implemented on an as needed basis, determined and administered exclusively by the Office of Information Security or an authorized entity discussed below. The vulnerability tests will be conducted in such a way as to cause minimal noticeable impact to university operations. A centrally managed vulnerability assessment system is deployed. Use of any other network based tools to scan or verify vulnerabilities must be approved by the Office of Information Security. All system owners are responsible for cooperating fully with any vulnerability scan being conducted on systems for which they are held accountable. System owners are responsible for remediation of any discovered vulnerabilities as described in the Vulnerability Remediation Standard. System owners are responsible for maintaining proof of remediation. Prior to the implementation of a new system or major change of an existing system on UC’s network, system owners must perform a vulnerability scan and remediate any vulnerabilities discovered immediately.

The IT@UC Office of Information Security is permitted to engage with third party companies to conduct internal or external vulnerability assessments or penetration testing as necessary. The IT@UC Office of Information Security reserves the right to remove or isolate vulnerable assets from the University’s network at any given time with no prior communication.

Any exceptions to this policy, such as exemption from the vulnerability assessment process, or exception from remediation must be approved by the AVP of the IT@UC Office of Information Security or his/her designee.
Audience:

This policy applies to all organizations and individuals associated with UC.

Definitions:

**Vulnerability:** A weakness in a system allowing an unauthorized party to violate the confidentiality, integrity, availability, access control, consistency, or audit mechanisms of the data stored on the system.

**Vulnerability Assessment:** The process of identifying and quantifying vulnerabilities in a system. Assessments are typically performed according to the following steps:
1. Cataloging assets and capabilities (resources) of a system
2. Assigning quantifiable value and importance to the resources
3. Identifying the vulnerabilities or potential threats to each resource
4. Mitigating or eliminating the most serious vulnerabilities for the most valuable resources

**Exploit:** Software, data, or a sequence of commands that takes advantage of a vulnerability in order to get unintended or unanticipated behavior out of computer software, hardware, or something electronic (usually computerized). This frequently includes such things as gaining control of a computer system or allowing privilege escalation or a denial of service attack.

**Threat:** An action that can cause harm to systems, data or other resources.

**Attack:** An action taken to actively exploit a vulnerability. Attacks are designed to prevent systems from being used, to steal or manipulate organizational data or to discover system passwords and business logon functions.

**Remediation:** To remove or otherwise address vulnerabilities so that the system is no longer exploitable by an attacker. Remediation can also refer to putting controls in place to minimize the chance of an attacker exploiting a vulnerability on the system.

Related links:

- (Scan Procedure Doc)
- (Escalation Procedure Doc)

Contacts

IT@UC Office of Information Security 513-558-ISEC (4732)
Integrated Service Desk 513-556-HELP (4357)

History:
Issued: 01/04/2008