UD Vulnerability Assessment Program

Objective

UDit is establishing a vulnerability assessment program, in line with UD's server audit policy and best practices, to provide both system owners/administrators and UD leadership ongoing visibility into the application of security standards on all servers, appliances, network devices, printers, etc. supporting the IT services provided to the UD community.

Initial Scans

Starting September 2014, UDit will begin actively scanning UD's public and private network spaces hosting equipment providing service to members of the UD community. These scans will involve all qualifying systems, whether operated by UDit or other units/departments. Unless there is significant reason, we will not scan systems externally hosted by 3rd parties. UDit will initially conduct unauthenticated scans on a quarterly basis to identify open services, remote access methods, versions, configuration issues, etc.

Reports

Detailed reports will be made available to system owners/administrators and to UDit technical staff. Summaries will be exported from the system and made available to CITD and senior leadership.

Remediation

In general, vulnerabilities need to be remediated (patched, isolated, etc.) in a period proportional to their risk. The ratings provided by our scanning tools in combination with criticality of the system and/or the sensitivity of the data stored/processed by that system and any existing security measures provides us with a measure of the risk.

Risk = (((vulnerability rating) * (system criticality and/or data sensitivity)) - (existing controls))

The expectation will be that vulnerabilities identified as high-risk need to be remediated quickly and all others prior to the next scanning cycle. Please refer to the Risk Prioritization and Remediation Guidelines for help in determining specific remediation timeframes. Follow-on scans will be conducted to verify that high-risk vulnerabilities have been addressed according to the schedule provided. In the case of emergency risk remediation (i.e., the Heartbleed OpenSSL vulnerabilities), UDit will provide active and explicit direction.

We understand that business needs may require exceptions. Any exceptions/waivers need to be formally documented and approved by both unit leadership and UDit. UDit will host a quarterly forum where UDit and unit staff can meet to discuss standards and address specific concerns.

Long-Term Goals

Within the next 6 – 18 months, UDit will expand the initial program described above to:

- Populate our inventory/asset database to include risk assessment/business impact information
- Automate and conduct scans more frequently based upon asset sensitivity and conduct trend analysis
- Integrate a change management component to allow us to scan new systems prior to their introduction into our environment and after changes have been made
- Add scan engines to allow us to examine the security profile of our resources from various perspectives – student network, Internet, etc.
- Create groups so that units can tailor and run their own scans though UDit will continue to oversee management and operation of the vulnerability assessment tools
- Work with unit IT staff supporting servers/services to create exceptions for scan traffic and to convert to more informative authenticated scans wherever possible
- Use the forum to vet and supplement our guidelines and standards