I. INTRODUCTION
The goal of the server security assessment is to identify and remediate vulnerabilities before networks and systems are compromised. The most effective way of doing this is by using software to scan servers proactively to look for known vulnerabilities. The scanning tool used by the University actively probes systems for vulnerabilities, performs a multi-level scan using an extensive database of known security holes to identify common system vulnerabilities such as but not limited to those included in the CERT, CIAC and SANS advisories.

What must be scanned and remediated? (Scope)
Server owners are required to scan and remediate the following servers:

- All web servers, per the state auditors' general recommendations
- All servers with contractual obligations for internal scans
- Any other device that has a regulatory requirement for internal scans.

Network discovery and mapping may be performed without limitation on entire network segments within a Network Manager's administration. Other servers may be scanned but priority will be given to servers categorized above.

When should scans and remediation be completed? (Timeline)

- The Web Application Security Review Procedure (IS-P802) requires annual scanning of all web servers.
- Quarterly internal scans must be completely for all PCI "in scope" servers.
- Servers with any other regulatory requirements must be done in line with the regulation requirements.

II. PRE-SCANNING PROCESS

Request access to the site licensed server scanning tool:

To request an account, you must be registered in the Net Manager database for all IP addresses to be scanned for vulnerabilities or IP address ranges to be mapped. Qualified persons should send an email to the UITS Security Operations Group (secops@email.arizona.edu), with a copy to the Information Security Office (infosec@email.arizona.edu). The email should have "Server Scanner Account Request" in the subject line, and the following information should be provided in the body of the email:

- Requestor's Name
- Server Administrator's Name (if different than requestor)
- Server Administrator's UA NetID
- College Name/Administrative Unit
- Department(s) Name
- IP address(es) for server vulnerability scanning
- The unit's IP address range for network discovery and mapping.

Prior to scanning make sure to read the tutorial in the Quickstart Guide, that will be provided in the introductory email.
III. **SCANNING PROCESS**
Upon granting access to scanning tool, UITS SecOps will reply to the requestor with additional information and instructions regarding access and use of tool. Please expect a turnaround of two (2) business days. The requestor can begin scanning once they have received the instructions from UITS SecOps.

The scanning process consists of three phases:
- Scanning: identifies vulnerabilities.
- Remediating: removing, at a minimum, level 4 & 5 vulnerabilities identified in the scan.
- Rescanning: re-scanning servers to ensure vulnerabilities have been resolved.

The Server and Network Scanning Timeline and Action Plan Workbook can help you with tracking your progress.

IV. **POST-SCANNING PROCESS**
All reports generated from scans should be kept for two years or the length of time as required by contractual or regulatory requirement whichever is longest.

After successfully scanning and remediating all level 4-5 priority vulnerabilities, a copy of the executive summary report must be sent to the Information Security Office (infosec@email.arizona.edu). The Information Security Office needs this summary for validation purposes.

*Any unresolved level 4-5 priority vulnerabilities must be accompanied with documentation supporting why they will remain unresolved. Also provide an action plan for future remediation with timeline and protection measures currently in place to minimize exposure to risk. Additionally, provide documentation for false positive findings.*

**Related Guidance:**
Data Classification Standard (IS-S302)
Network Security Standard (IS-S600)
Minimum Security for Networked Devices Standard (IS-S602)
Server Security Standard (IS-S603)
Web Application Security Review Procedure (IS-P802)

**Related Resources**
Server and Network Scanning Timeline and Action Plan Workbook (.xlsx)

**Revision History**

<table>
<thead>
<tr>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Update</td>
<td>9/26/11</td>
</tr>
<tr>
<td>Initial Draft</td>
<td>10/31/08</td>
</tr>
<tr>
<td>UA-ISAC Review</td>
<td>4/2/09</td>
</tr>
<tr>
<td>Effective Date</td>
<td>7/1/09</td>
</tr>
<tr>
<td>Effective Date v2</td>
<td>9/26/11</td>
</tr>
</tbody>
</table>