Oklahoma State University
IT Office of Information Security

Information Technology Department
Office of Information Security
405.744.1976

Vulnerability Analysis Form

OIS-VAF-001

Shaded areas of form are for IT Office of Information Security use only.

Requester Information

Last Name:	First Name:
Department:	Campus Address:
OKEY Email:	Phone:
Requester's role:	If Other:

The default assessments to be performed are "safe checks". Please indicate in the space provided below if you prefer the system be tested using a variety of checks that may disrupt the operation of the system (ex: known DoS issues).

☐ Default Assessment "safe checks" ☐ Complete Assessment

This vulnerability assessment and analysis represents a snapshot of a computer or system at a specific point in time. Any changes made after the recommendations have been applied may result in new vulnerabilities/risks being introduced. While vulnerability assessments are important, it should be understood that the roles of users and administrators in systems security is of the utmost importance and cannot be replaced entirely by periodic vulnerability scans. Upon completion of the vulnerability analysis, a report summarizing the vulnerabilities will be provided to the requester.

_____ _____
Requester's Signature: Date Department Head Signature Date

Send completed request to: IT Office of Information Security
301 Whitehurst Building

IT Office of Information Security use only	SEC Incident Reference Number:
Request received by:	Date received:
Type of assessment:	If Other:
Number of systems to be scanned:	
Special day/time request:	Estimated date of scan:
Date scan(s) completed:	Completed by:
Date report(s) prepared:	Customer contacted:
Date report(s) delivered:	Delivery method (consultation, etc.):

Oklahoma State University
IT Office of Information Security

Information Technology Department
Office of Information Security
405.744.1976

Vulnerability Analysis Form

OIS-VAF-001

Shaded areas of form are for IT Office of Information Security use only.

Type of Analysis

Check the box below specifying the type of assessment to be performed and provide details as directed.

☐ Remote vulnerability assessment of server(s)

- Requester must complete "Server Information Worksheet" for each server
- Requester must submit MBSA 2.0 scans of each system with this request.

☐ Remote vulnerability assessment of workstation(s)

Provide host name and IP of each workstation to be assessed. Indicate if an IP range sufficiently describes the workstations to be assessed.

HOST NAME	IP ADDRESS
Ex: bluefoot.okstate.edu	*Ex: 139.78.0.0*

☐ Audit of application * ☐ Audit of web-based application *

Describe application (Include intended use of the application, user base, the use of confidential data, and other pertinent information).

Attach extra pages as needed to provide a complete description:

Application must be ready for production prior to the vulnerability assessment

☐ Other type of analysis– Describe in detail. Attach extra pages as needed.

Attach extra pages as needed to provide a complete description:

Oklahoma State University
IT Office of Information Security

Information Technology Department
Office of Information Security
405.744.1976

Vulnerability Analysis Form

OIS-VAF-001

Shaded areas of form are for IT Office of Information Security use only.

Server Information Worksheet

This worksheet must be completed for each server to be scanned. You may copy this page as needed for multiple servers. It is not necessary to complete this worksheet for workstation and application vulnerability assessments.

Hostname:	Host IP:
Operating system:	Service Pack Level:
Location of server:	
Intended users:	
Purpose of server and/or applications running on this system:	
Describe classified/confidential data residing on this server if applicable:	
Describe regulatory compliance requirements associated with this server such as HIPAA, FERPA, GLBA, SOX, etc.):	
Specify your preference for the day/time your server scan begins:	DAY: TIME:

Is MBSA 2.0 scan for this server attached?

To upload MBSA 2.0 scan, browse to \Documents and Settings\[User who ran the scan]\SecurityScans.

The scan will be called [Domain]-[Hostname](date).mbsa. Need Help with MBSA scans? Contact the IT Office of Information Security at 405-744-1976 -- or security@okstate.edu.