NETWORK AND SYSTEM SECURITY CHECKLIST

UNIVERSITY COMPUTER CENTER
UNIVERSITY OF THE PHILIPPINES DILIMAN

Document Control

Document Properties

Title	Hardware Maintenance Schedule
Author	Riyeth P. Tanyag
Document Type	Administrative Document
Filename	UPD Security Checklist.gdoc
File location	UPCC/IT Security

Version History

Version Number	Version Date	Author/Modified By	Description
0.01	March 17, 2015	Riyeth Tanyag	Initial Version
0.02	March 19, 2015	Raymond Nuñez	Insertion of Log Files
1.00	May 29, 2017	Gerardo Roxas	Document Clean-up

Table of Contents

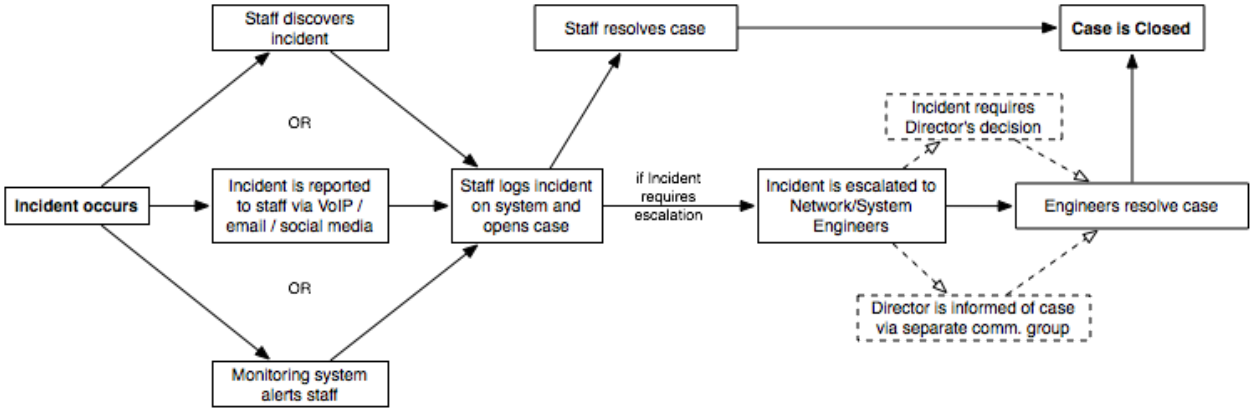
Security Policy

Incident Management

Depending on the situation, incidents are handled according to several categories:

1. Cause Origin
    a. Internal (equipment failure, data corruption, human error)
    b. External (DDOS attack, natural disasters, etc.)
2. Method of Detection
    a. Monitoring systems deployed by organization
    b. Reported by persons inside of organization
    c. Reported by persons outside of organization
3. Severity of Incident
    a. Mild
    b. Severe

For most cases, incidents are reported through the following process:



Incident Resolution Flowchart

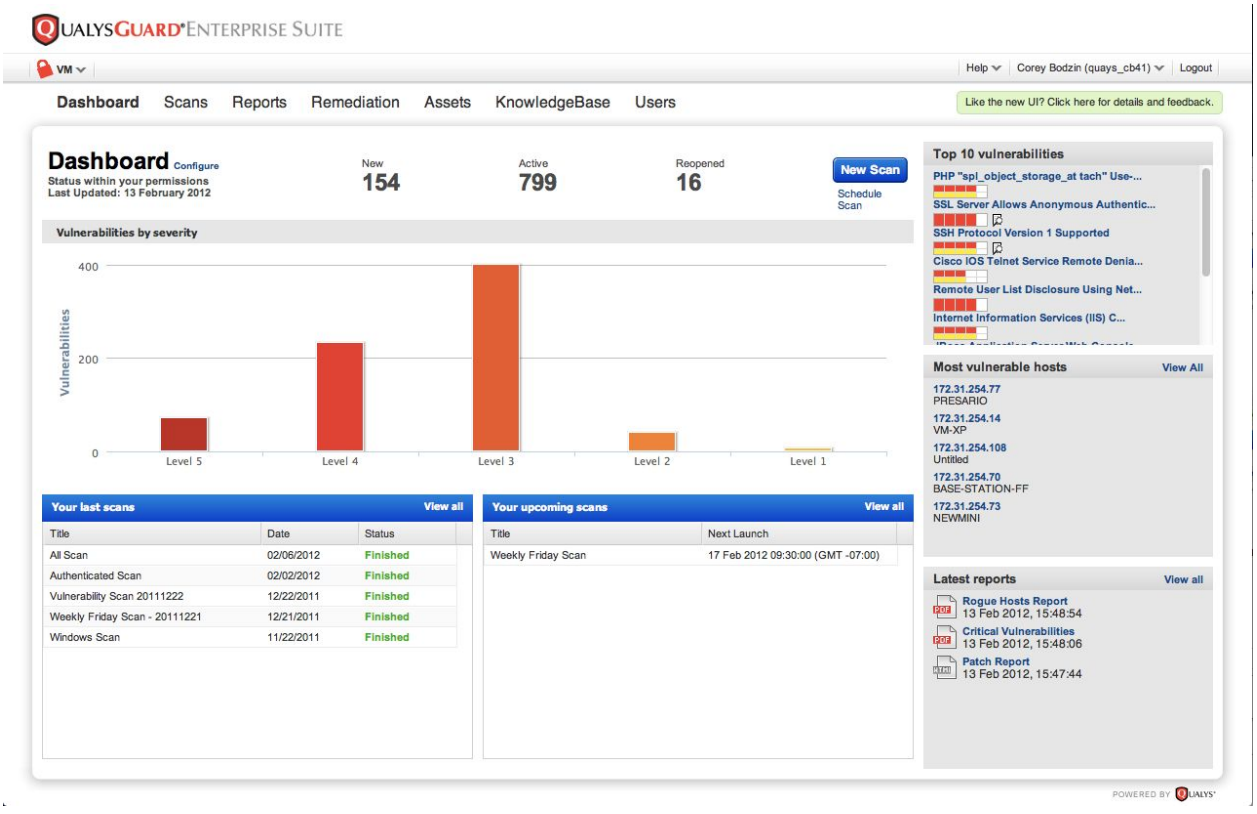
Backup Policy

Critical systems and applications are required to be backed-up on a daily basis. A remote backup system is deployed off-premises of which system and network administrators have limited accounts to incrementally back up their local systems to. Automated back-ups are required to have at least a key-based SSH authentication. Sensitive files such as configuration or PII are encrypted with GPG.

Backup data should be retained for at least three months before deletion.

For network appliances, configuration data is backed-up on a weekly basis on a dedicated server with access to the management network.

Vulnerability Scanning Tool Used



Vulnerability Scanning Log files and Remediation Plan

Critical UP Diliman web services are scanned weekly for vulnerabilities and reported to .

Business Continuity Plan

Disaster Recovery Policies and RPO/RTO details

Disaster recovery can be broken down into various levels of severity of data loss. For minor disasters involving partial data loss (e.g. single disk failure in a RAID array), the allowable time for recovery of data is at least six (6) to twenty-four (24) hours, of which end-users of the organization will be notified immediately of the situation.

In case of incidents resulting to direct data loss (e.g. corruption on an entire RAID array, total equipment failure, etc.), recovery of data is performed up to the latest available recovery point. The recovery points vary between data types and functions, namely (but not limited to):

- hosted website databases: 24 hours
- e-mail data: 1 week
- switch and router configurations: 1 week
- hosted website directories: 1 month

Recovery times are also dependent on external factors such as: availability of power/electricity during the disaster period, availability and/or delivery times of replacement equipment.

Certificate and Insurance details

The organization does not have any ISO certification and insurance yet.

Antivirus Log Files

There are no specific antivirus applications that the University Computer Center require for its clients. It is the responsibility of the end users to update their own antivirus applications periodically.

Access Log Management

All systems and network equipment are required to have logging enabled, with complete year/month/day HH:MM timestamps of activities occurring on systems. Accessing users and administrators are also required to be logged in, with users of lower privileges having no access to the log records.

Logs for all systems and network equipment are also sent remotely to a logging server.

Patch management policy and logs

The University Computer Center has a minimum requirement for certain key packages used by the organization (e.g. Linux Kernel versions, OpenSSL, PHP, Apache, etc.) as dictated upon by its network and systems security auditor. Required patches are also announced by the security auditor, of which the organization has at least 3 days to perform updates and report to the auditor.

Secure coding practice

Web applications developed under the University Computer Center shall be approved by the supervisor before deployment. Initial source code shall then be scanned and approved by the security consultant.

If necessary, bugs and and security patches shall be applied by the software developers and approved by the security consultant before pushing the code on production servers.

Employee Security Awareness Program

There is no Employee Security awareness program applicable for this organization.

Signed NDA for Admin

The University Computer Center does not use NDA forms for its personnel.

Joiners and leavers policy details

Employees are required by contract to provide a written notice one (1) month prior to date of termination. The employee should submit all turnover documents, access to servers and network devices to their immediate supervisor.

Visitor policy details

Only students, faculty and staff are allowed to enter the building premises. Visitors' information, entry and exit times are logged by the guard on-duty. Access to the data center are limited only to technical staff. Visitors are not allowed access to the data center unless approved by the director and/or the systems and network security consultant.