Home work assignment 1 (5%)

Submission date on 10 Oct 2015 (Postponed to 14 Oct 2015)

Assignment tasks

You have already performed vulnerability scanning using Nessus at the 2 servers (web server VM and database server VM) during lab session week 3.
There should be "Critical vulnerabilities" being identified in Nessus report.

For this assignment, it is assumed that you are the IT Security Consultant to compose a vulnerability scanning report for IT support team to rectify the identified vulnerabilities from the scanning results of the two machines.

As IT security consultant, you will have to review, report Nessus results and verify if the vulnerability is correct together with the rectification method before it could be reported.

The report can be written in Word or spreadsheet format.
The report should be easy for IT support team to understand and read the document.

This report should consist of (5 Critical vulnerability only):

- Title of the vulnerability
- Description of the vulnerability
- Impact of the vulnerability
- Testing method and verification results
- Rectification (Recommendations)
- Affected machines and services

Example:

Title of the vulnerability: CentOS 5/6/7: bind (CESA-2014-4:1984)
Description of the vulnerability:
Updated bind packages that fix one security issue are now available for Red Hat Enterprise Linux 5, 6, and 7. (including CentOS 5)

The Berkeley Internet Name Domain (BIND) is an implementation of the Domain Name System (DNS) protocols. BIND includes a DNS server (named); a resolver library (routines for applications to use when interfacing with DNS); and tools for verifying that the DNS server is operating correctly.

Impact of the vulnerability:

Red Hat Product Security has rated this update as having Important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

A denial of service flaw was found in the way BIND followed DNS delegations. A remote attacker could use a specially crafted zone containing a large number of referrals which, when looked up and processed, would cause named to use excessive amounts of memory or crash. (CVE-2014-8500)

Testing method and verification results

https://lists.centos.org/pipermail/centos-announce/2014-December/020829.html

```
yum list installed |grep bind
bind.x86_64             30:9.3.6-20.P1.el5_8.6    installed
bind-chroot.x86_64         30:9.3.6-20.P1.el5_8.6    installed
bind-libs.x86_64         30:9.3.6-20.P1.el5_8.6    installed
bind-utils.x86_64         30:9.3.6-20.P1.el5_8.6    installed
ypbind.x86_64            3:1.19-12.el5_6.1        installed
```

Rectification (Recommendations)

Please upgrade the following packages:

bind-9.3.6-25.P1.el5_11.2
bind-chroot-9.3.6-25.P1.el5_11.2
bind-libs-9.3.6-25.P1.el5_11.2
bind-utils-9.3.6-25.P1.el5_11.2

After installing the update, the BIND daemon (named) will be restarted automatically.

Affected machines and services

172.16.110.166 (Web Server), DNS services