

CHAPTER TWO: VULNERABILITIES IN THE ORGANIZATION

Here, organization related vulnerabilities are being reviewed. They include access authorization and user authentication, as well as human factors in information security and ways to minimize risk. Also covered are the wireless networks – Bluetooth, Wi-Fi and WiMAX, and measures to increase their security. Cloud computing is examined along with its advantages and disadvantages.

1. Access and review the National Training Standard for Designated Approving Authority (DAA) document located at http://staff.washington.edu/dittrich/center/docs/nstissi_4012.pdf Summarize it in a twelve-slide electronic presentation.

This is a very important policy document in the training of information security personnel. It can be best assigned as a project for two or three students, but not more. If a face-to-face class, an in-class presentation with follow up discussion is suggested.

2. Access and review the *Authentication in an Internet Banking Environment* of the Federal Financial Institutions Examination Council located at http://www.ffiec.gov/pdf/authentication_guidance.pdf Summarize it in a six slide electronic presentation.

This is a short, yet very valuable paper with banking guidelines transferable to many other sectors as well. An excellent topic for both face-to-face and in-class discussion.

3. Visit website www.NordicEdge.se, familiarize yourself with the One-Time-Password technology, and experience it through the Download Two Factor Authentication Trial option at <http://nordicedge.com/products/one-time-password-server/download/>

two The two-factor authentication, that is pass codes submitted via different channels, increases security by a significant factor. In this case, the user enters a user name and/or password, and an additional one-time-password is being sent to the user as an sms mobile phone message. Entry of this password authenticates the user in a parabiometric way, considering that these days the mobile phone has become an integral human accessory.

4. Access and review the Wireless LAN Security Today and Tomorrow document located at <http://www.itsec.gov.cn/docs/20090507163620550203.pdf> Summarize it in an eight-slide electronic presentation.

The instructor may ask the students to seek additional sources and incorporate any further precautions for WLAN environments. Such as <http://www.symantec.com/avcenter/reference/symantec.wlan.security.pdf>

5. Visit website <http://www.outofblue.net>. Understand the presented technology, and express your thoughts as to any vulnerabilities on the side of the clients as well as on that of the server.

Out-of-Blue is a very innovative marketing technology that uses Bluetooth for in-premises advertising. The proper use of the provided Bluetooth server does not pose a security risk, but possession of a Bluetooth server in hacker's hands may do. A team assignment will allow brainstorming with all its benefits. A search under Bluetooth Hotspots is suggested.

6. Visit websites of Wi-Fi hardware vendors. Understand the technology and design a WLAN service that will provide Internet access to a three floor square office building of 30m each side. Determine the topology of the access points.

This can be a very good team project. The objective of this exercise is for the students to obtain a WLAN design hands-on experience and familiarity with the latest in Wi-Fi technology. The following sources can give students a head start.

<http://www.ciscopress.com/articles/article.asp?p=469624&seqNum=5>

<http://ptgmedia.pearsoncmg.com/images/1587052229/samplechapter/1587052229content.pdf>

<http://www.flukenetworks.com/enterprise-network/wireless-network/AirMagnet-Survey>

7. Visit websites of WiMAX hardware vendors. Understand the technology and design a service that will provide Internet access to 50km radius rather flat area.

access. Valuable WiMAX has matured as a technology for wireless internet. Familiarity with it is a must, and this exercise can give a team knowledge. The following sources can give students a head start.
http://www.altera.com/literature/cp/cp_gspix_wimax.pdf
http://www.altera.com/literature/cp/cp_gspix_wimax.pdf

8. Access and review the following three documents all titled **The Basics of Cloud Computing**

http://www.us-cert.gov/reading_room/USCERT-CloudComputingHuthCebula.pdf

http://old.news.yahoo.com/s/ac/20101029/tc_ac/554719_the_basics_of_cloud_computing_explained and

<http://cloudcomputing.sys-con.com/node/1634967>

and prepare a twelve-slide electronic presentation with the same title.

Cloud Computing will soon become the norm in information systems implementation and design. The advantages being offered by a cloud-based system make the ownership and maintenance of an on-premises information system cost-ineffective. This can be a good team project because of relative novelty and controversy on this technology.

9. Visit the website of a Cloud Computing provider, subscribe in a free trial option and build a multi-server and multi-storage infrastructure. Describe and document your gained knowledge and experience.

Cloud Computing providers, often offer users, on a trial basis, the opportunity to actually design and build an truly operational cloud-based information system. Teams of two are suggested for this project. The following sources can give students a head start.

<http://www.foliocloud.com/lp-european-cloud-solution.html?gclid=CLaElrWM-60CFWyHtgod8BDuOg>

<http://www.getapp.com/software-pricing/Free%20Trial/cloud-computing-management-software>

<http://www.computerweekly.com/news/2240089111/Top-five-cloud-computing-security-issues>

10. Access and review the following three documents and prepare a twelve-slide electronic presentation with the title Cloud Computing Vulnerabilities.

Seven Deadly Threats and Vulnerabilities in Cloud Computing

<http://www.ijaest.iserp.org/archieves/15-Jul-15-31-11/Vol-No.9-Issue-No.1/16.IJAEST-Vol-No-9-Issue-No-1-Seven-Deadly-Threats-and-Vulnerabilities-in-Cloud-Computing-087-090.pdf>

Cross-VM Vulnerabilities in Cloud Computing

<http://rump2009.cr.yp.to/8d9cebc9ad358331fcde611bf45f735d.pdf>

Top Threats Cloud Computing V1.0

<https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf>

Here, the Cloud Computing security issues in are being examined. A three-member team with each member reviewing one of the three papers can produce an interesting presentation.