IT Security, Assignment 3
Web-based analyses

DIKU, block 4, May 21 2014

BIOchem continues to request your diverse IT security skills.

1 An online press room

BIOchem is implementing a new web application on their public web server, an "online press room", where the communication department will upload monthly press releases the second Friday of each month, and users can download them. All publications are named by the date of publication, e.g. '11-04-2014.html', '09-05-2014.html', and so on.

The code is written in the server-side scripting language PHP, in the file pressroom.php. Review the code to find any security issues and suggest ways to fix them. You do not have to demonstrate the flaws. (Get the code on Absalon.)

2 Separation of duties

Split knowledge is a variation of separation of duties, ensuring that no one person knows or has all the details to perform a critical task. When uploading new press releases, BIOchem would like to ensure that it takes the combined effort of at least two people from the comm department. To that end, a special password, to be changed each month, will be used to access pressroom.php. For May the password is `1af84eb2c98`.

Provide BIOchem's head of the comm department, the deputy head and the senior press officer with a part of the password such that any group of two or more of these individuals may reconstruct the password, but no one single person may.

Make your solution such that if one and only one part of the password is compromised, you may easily update the password parts without having to change the password itself.

You may code your solution of generating/updating the password parts in any language of your choice. You may expand the pressroom.php solution so that it is only accessible given the right password parts are supplied but you do not have to.

3 DDoS on BIOchem

BIOchem has run into some unfavourable media coverage and has suffered from a denial of service attack, rendering, amongst others, its web server and the press room inaccessible. Nevermind Anonymous is the suspected culprit, right now the company is scrambling to find out when the attack actually started and how it is being carried out.

Try to determine as well as you can when the attack started, what kind of attack, and so on, by analysing the Cisco PIX firewall log from the company's perimeter firewall. (Get a zipped copy from Absalon. Unzips to 2GB.)

4 Office 365

On a completely different note, BIOchem wants to drop Microsoft Office on its workstations and switch to the cloud solution Office 365. The main driver is to save money on licensing and to avoid the hasle of being responsible for constantly installing updates and doing file server backups; but also the promise of increased data availability when users are not in office, as all an employee would need is an Internet-connection and a browser.

BIOchem use Microsoft Office intensively. They use Excel to trend on research results and to manage budgets and do finansial forecasting. Powerpoint is mainly used for presentations at customer sites or at conferences, while Word is used to maintain descriptions of BIOchem's workflows and procedures and to write small internal memos. Access is used by HR as a database to hold personal data on employees such as addresses and telephone numbers and internal company-related information like career plans and performance metrics. BIOchem does not classify its data.

Most employees work while at the office or from home where Internet-connectivity can be assumed, however the CEO and the sales team frequently travel and need data on the go. The scientists occationally participate in conferences and different international research boards, but they do

not need the same level of data availability as the CEO and the sales people.

Perform a risk analysis of a switch to Office 365. Limit your analysis to a few pages at max.

General requirements

There are 3 assignments during the course, intended to give you hands-on experience in how to analyse information security risks, implement (parts of) security systems, break such systems, analyse attacks and provide recommendations to prevent future similar attacks.

Your solution to each assignment should be documented in a short report. Your report may follow the usual structure for scientific reports, starting with a summary followed by a description of the problem and the solution and finishing with a conclusion and a list of references.

Reports must be submitted in PDF format via Absalon no later than two weeks after the assignment in question is posted. Reports are graded as 'pass' or 'no-pass'. Resubmissions are allowed once per assignment. You must pass all assignments to sit in for the exam.

Limited written feedback is given via Absalon. Additional feedback may be given at exercise classes.

You should keep your hand-in as short and precise as possible. If you are in doubt about the interpretation of some of the requirements, or feel it necessary to make some assumptions, you should explain what you did and why. Be sure to clearly mark work included in your solution that is not your own personal work and make a reference to its source.

You may solve the assignmets in groups of 1-3 students. The first page of your report must contain the assignment number, your name and the name of any other group members.