17-654/17-754: Analysis of Software Artifacts
Assignment 10 (Written/Experimental): Security Analysis

Paulo Marques, Jonathan Aldrich, Nels Beckman, Kevin Bierhoff

100 points total

Introduction

In this project you will do a security analysis on a system. You will also be asked to run a vulnerability scanner tool and comment on the obtained results. The objectives of the assignment are:

- Gain familiarity with security analysis techniques, namely the STRIDE model for threat identification.
- Gain familiarly with vulnerability scanner tools, their strengths and limitations. In particular, you will be using the Nessus tool (http://www.nessus.org/).
- Critically analyze a system identifying quality attributes (or lack of them) regarding security.

Due Date

April 10th, 2007

Groups

This assignment should be completed in groups of 2. At least one of the members of the group should be a MSE student working on a Studio project with an account on *dogbert* and the corresponding development server (hosted on a *virtual machine*).

Delivery

Turn in a file named ***<username>-17654-A10.zip***, where username is your Andrew id. The zip file should contain the file ***answers.{doc|pdf}*** with the answers to the questions. It should also contain two HTML files: one for the Nessus analysis on *dogbert* and one for the analysis on the team's development server.

Security Analysis

For your MSE project you are currently using two machines:

- Dogbert, which contains the general web pages of your project.
- A development server, being hosted on a virtual machine. This server typically contains your project's wiki, subversion server, and other development support tools.

These two machines constitute the core of your project's infrastructure. Thus, it is critical for your project's success that they are secure. (Just imagine what would happen if a malicious user was able to access the server and modify/steal/destroy information!) At the same time, many projects contain confidential information related to the companies sponsoring them. An integral part of the security of those systems is making sure that such information is not easily leaked.

1. In class we looked into a technique called “Security Design by Threat Modeling”. In this question you should turn in an analysis of *dogbert* and your development server, corresponding to the two first steps of the process:

- Brainstorm and analyze the known threats to the system
- Rank the threats by decreasing risk exposure

Your analysis should be realistic. I.e. we are not looking for “lip service” but for you to look critically into your servers, the applications and services running there, the information you are currently making publicly available and how easy it would be for a malicious user to compromise it.

Three important pieces of advice:

- Before performing the group brainstorming session, it is important that each member critically looks at the system, analyses which services are running and how, which information is used and publicly displayed, where user authentication is done and how, and so on. The brainstorm session will only be effective if the team deeply understands and knows the system.
- During the brainstorm session make sure that you follow the recommended methodology: it’s supposed to be structured brainstorming! Make sure you draw diagrams that are detailed enough for discussing the system. Ensure that you identify core processes, persistent and non-persistent data, communication channels, etc. It is a good idea to have these diagrams prepared before the meeting.
- During the meeting, make sure that you have the STRIDE slide printed out and clearly visible. When discussing a particular aspect of the system (e.g. a data channel, a wiki, etc.) make sure it’s analyzed according to STRIDE. You can quickly go through items, but make sure you cover them all.

When writing down the answer to this question, make sure that you include the diagrams you used in the meeting and that you provide at least a brief discussion on how your systems are organized. When describing the threats, make sure that your description contains enough detail so that it’s clear why you consider the threat to be real. You may use a “condition; consequence” format, or a less structured format, as long as it is clear. Finally, don’t forget to rank threats according to decreasing risk exposure.
[50 points]

2. You should now perform the three remaining steps of the technique:

- Choose how to respond to each threat
- Choose techniques to mitigate each the threat, if applicable
- Choose appropriate technologies from the identified techniques

Since this is not a security course, we do not expect you provide a comprehensive answer in terms of technologies to be used. But, if you do identify threats that should be addressed, you should probably research ways on how those particular problems can be mitigated technologically or, alternatively, how the problem could be solved in a non-technological way (e.g. moving sensitive files that are publicly available into an authenticated area).
[15 points]

3. *Nessus* (http://www.nessus.org/) is a vulnerability scanner tool developed by TENABLE. Given an IP address, it allows you to scan the target machine for thousands of known vulnerabilities, ranging from simple networking services to database servers, web servers, and wiki's, among others (http://www.nessus.org/plugins/index.php?view=all).

a) Download the tool and install it. The installation is straightforward. Note that you will need to register on Nessus' web site for receiving an activation key. Run the *Nessus* tool both on *dogbert* and on your development server. Make sure that you run the tool in safe mode ("***Enable all but dangerous plugins with default settings***"). Save the generated HTML files, turning them in as part of the assignment.
[5 points]

b) For each one of the found problems review it, searching the Internet for information if necessary, commenting if it's a threat or not and why.
[15 points]

c) How does this tool compare to the approach for security analysis you did before? For what type of threats does a tool like Nessus excel and what are its limitations? Did you cover all the services Nessus did? (Think about what are the kind of problems these tools are unable to find/address; think about what are the kind of problems humans are unable to find/address; and vice-versa.)
[15 points]

IMPORTANT NOTICE

The CMU Computing Services office has several tools in place to detect scans and attacks on campus servers. The office was notified that they should expect Nessus scans on *dogbert* and on the MSE virtual machines during the duration of this assignment. It was agreed that they will not stop the scans, disable the machines from where the scans are coming from, or block the corresponding users. Nevertheless, you must not:

- **Scan other machines besides *dogbert* and the MSE virtual servers**
- **Perform any scan after the 12th of April**

Doing so may result in your account being blocked or having the machine from where the scans are coming from evicted from the network. Be warned!