10/03/2012 CSE 565: Computer Security Due: 11/02/12 (In class)

Project 2 – File System Integrity Checkers

1. Background

File system integrity checkers are a kind of Intrusion Detection Systems (IDS). When attackers attempt to compromise a system, they often tamper with certain system or key files in order to retain a continued system access. Integrity checkers maintain a valid snapshot of important files on a system. Modifications to these files are detected by comparing their current snapshot to the original one. Any unauthorized modifications are reported to the administrator.

As you proceed through this course, you will realize that integrity checkers best define the basic concept underlying most host-based intrusion detection systems (e.g., anti-viruses, anti-spyware, tripwire). So the knowledge and understanding of these systems and their architectures is paramount for the building of secure systems.

1.1 Guidelines

In this project, you work in super-groups (groups of two groups). This project has three phases:

- *Phase 1:* Background research on file system integrity checkers
- *Phase 2:* Analysis of various file system integrity check tools
- *Phase 3:* Designing your own file system integrity checker

This is a significant project and would demand considerable time for an insightful analysis. Therefore, it is recommended that you start working on it as soon as possible. This project requires team members to work together for Phase 1, develop a plan, take your assignment for Phase 2 and work individually for Phase 2, then combine your efforts from Phase 1 and Phase 2 so that you can jointly come up a good solution for Phase 3. Hence, you may find it useful to elect a super-group leader for this project and set internal deadlines (a group without a leader often leads to chaos).

Make sure to always support your answers and claims with reasons and references (where applicable).

You are encouraged to use research publications as references. It will also be a good indicator of reliability of your analysis. Refrain from borrowing any material without citing the source; it may constitute plagiarism.

The overall quality of this project will be measured by how well you research the topic, understand the fundamentals and make innovations for Phase 3.

2. Setting up the Virtual Machine

Running the file system integrity checkers in Phase 2 requires the use of Ubuntu. Hence, you must first successfully set-up an Ubuntu virtual machine.

2.1 Steps to install a virtual machine

a) Download and install VMware Player (30 day evaluation version) from https://www.vmware.com/tryvmware/?p=player&lp=1 (You will need to register).

b) Download the server version of Ubuntu from http://www.ubuntu.com/download (Server Edition, Ubuntu 12.04) (This is an ISO disk image)

c) Fire up VMware Workstation

i. Create a new virtual machine with default settings
ii. Point the CD image to Ubuntu ISO
iii. Start the Virtual Machine; the installation of Ubuntu should proceed with no problems. It may take some time for the graphical interface to appear on some systems, so be patient.

3. Project Details

3.1 Phase 1: Background Research on File Integrity Systems (20 points)

This section needs to be completed jointly by all the group members. Type 'Phase 1' on top of all pages that describe Phase 1.

Reference Material

'An Introduction to File Integrity Checking on Unix Systems' by Del Armstrong, SANS Institute, 2003 (http://www.giac.org/paper/gcux/188/introduction-file-integrity-checking-unix-systems/104739).

Q 1. Briefly explain the basic architecture and functioning of file system integrity checkers. **(5 points)**

Q 2. Explain why the following features are used in the initial baseline generation phase (Hint: Think about how they can be modified to execute attacks). **(6 points)**

- Type
- Group
- Permissions
- Sticky bit
- Reference count
- Device number

Q 3. One of the most obvious ways to compromise an integrity checker is to target its database. State three ways to prevent this and the shortcomings of these solutions. **(3 points)**

Q 4. What are the advantages/disadvantages of remote configuration management for file system integrity checkers? **(3 points)**

Q 5. What are the advantages/disadvantages of file integrity checkers over other defense tools (like anti-viruses, firewalls, etc.) **(3 points)**

3.2 Phase 2: Comparative Analysis (40 points)

Given below is a list of six integrity check tools that you are required to investigate. Each group member should pick up, implement (on your virtual machine) and investigate just one of these tools. Make sure all tools are picked up by someone in the group.

1. Tripwire
2. Samhain
3. AIDE
4. Integrit
5. Nabou
6. Osiris

Six separate investigation nuggets need to be included in your project report for this part. Students investigating a tool are required to write 'Phase 2 - <his/her name **(in bold)**>' on top of each page that describes the investigation. Each report should be maximum 3-4 pages long.

Investigation Requirements

1. Describe the overall functioning of the tool (e.g., how the database is generated, where it is stored, how alarms are raised, the periodicity of the checking phase, etc.). Especially describe the alert generation and logging capabilities of the tool? **(5 points)**

2. What was the main motivation behind designing this tool? In other words, does it have features that other tools do not, and vice versa? **(2 points)**

3. Is the source distribution, baseline distribution, configuration files, etc. signed or encrypted? If yes, briefly mention the protocols or algorithms. **(5 points)**

4. Does the tool support centralized policy management? If yes, briefly describe the protocol. **(3 points)**

5. Experiment to figure out how the following conditions are handled (screenshots required). **(5 points)**
   a. Files of size zero
   b. Duplicate entries in a configuration file
   c. Files with no owner or group
   d. Support for regular expressions in the configuration file
   e. Unauthorized modification of an important file

6. For the features that you discovered in your investigation till now, analyze the following:
   a. Does it constitute a security threat? If yes, how would you fix it? **(4 points)**
   b. Does it affect system efficiency? If yes, do you have any ideas on how you could fix it? Describe. **(4 points)**

7. Do you think this tool can be used as an anti-virus with some modifications? If yes, what modifications will be needed? **(2 points)**

8. *Performance testing:* Discuss among the super-group members (all six) to come up with a common configuration file for performance testing (Make sure it is of considerable size). Write a small script to implement baseline database generation and checking phases. Average over 10 runs to record the performance of your tool. **(10 points)**

3.3 Phase 3: Designing Your Own File System Integrity Checker (30 points)

This phase requires all team members to discuss your observations about your respective tools and learn from each other. Combine your experiences and findings to come up with an architecture of your own file system integrity checker (diagram representation encouraged). Justify your reasoning for the design and why you chose the features that you did.

Sample features that you can discuss (you need to discuss many more, these are just some examples):

- Hash algorithms
- Policy management
- Periodicity of comparisons
- Security and efficiency solutions

Make sure to mention everything in bullet form and highlight important points.

4. Deliverables

- **Report** (one joint report per super-group is sufficient)
  - Answer the questions in Phase 1 jointly (2-3 pages)

- Answer the questions in Phase 2 for the tool you choose. Write your name in **bold** on each page for the part you are responsible (3-4 pages/member)
- Answer the questions in Phase 3 jointly (2-3 pages)

Peer-reviewed references are highly encouraged. Terseness and good presentation of material will be rewarded.

- **Demonstration**

  You should all be ready to demonstrate the tools that you worked with in Phase 2. Additionally, you can be asked to justify answers/design choices from Phase 1 and Phase 3.

  Reports will be used as the basis for demonstration. Grades will be based on the quality of report and how well you can demonstrate your work.

  Answer to Phase 3 is only a design level documentation. The top two designs will be selected for further refinement and implementation at a future time outside of this semester. If interested, this work can be continued for implementation and evaluation as part of an independent study in a future semester. A completed system may be eligible for publication in a security conference.