TE WHARE WĀNANGA O TE ŪPOKO O TE IKA A MĀUI
VICTORIA
UNIVERSITY OF WELLINGTON

TERMS TEST #2 — 2016
TRIMESTER TWO

NWEN 405
Security Engineering

Time allowed: TWO HOURS

Instructions: There are 90 possible marks on the terms test.

You should allow roughly one minute per mark.

Many of the questions require you to discuss an issue, compare options or evaluate a situation. For such questions, the assessment will take into account the evidence you present and any insight you demonstrate.

If additional space is required you may ask for a separate answer booklet.

There are FOUR pages and each page is printed single-sided.

The examination contains FOUR questions.

You should attempt ALL questions.

Question	**Marks**
1. Mixed Bag	10
2. Intrusion Detection	25
3. Intrusion Prevention and Firewalls	25
4. Buffer Overflows and Software Security	30

Question 1 Mixed Bag of Questions **[10 marks]**

Mark each of the following statements as either being **TRUE or FALSE**. No explanation or justification is required.

(a) F (b) T (c) T (d) T (e) T (f) F (g) T (h) F (i) T (j) F

Question 2 Intrusion Detection **[25 marks]**

(a) [5 marks] Describe the differences between a host-based IDS and a network-based IDS. How can their advantages be combined into a single system?

Host-based IDS: Monitors the characteristics of a single host and the events occurring within that host for suspicious activity

Network-based IDS: Monitors network traffic for particular network segments or devices and analyzes network, transport, and application protocols to identify suspicious activity

Distributed or hybrid IDS: Combines information from a number of sensors, often both host and network-based, in a central analyzer that is able to better identify and respond to intrusion activity.

(b) [5 marks] Define the terms false positive and false negative. Give an example of both in the context of an intrusion detection system monitoring network traffic for evidence of potential intrusions.

A false positive, or false alarm, is where authorized users are identified as intruders by an IDS. + Example.

A false negative is when intruders are not identified as intruders by an IDS, as a result of a tighter interpretation of intruder behavior in an attempt to limit false positives. + Example.

(c) [5 marks] List and briefly define the three broad categories of classification approaches used by anomaly detection systems.

- Statistical: Analysis of the observed behavior using univariate, multivariate, or time-series models of observed metrics.
- Knowledge based: Approaches use an expert system that classifies observed behavior according to a set of rules that model legitimate behavior.
- Machine-learning: Approaches automatically determine a suitable classification model from the training data using data mining techniques.

(d) [10 marks] An example of a host-based intrusion detection tool is the tripwire program. This is a file integrity checking tool that scans files and directories on the system on a regular basis and notifies the administrator of any changes.

It uses a protected database of cryptographic checksums for each file checked and compares this value with that recomputed on each file as it is scanned. It must be configured with a list of files and directories to check and what changes, if any, are permissible to each. It can allow, for

example, log files to have new entries appended, but not for existing entries to be changed.

Evaluate the usefulness and effectiveness of this tool with respect to: (i) the impact of the frequency of file updates and different types of files monitored; (ii) the amount of work in both the configuration of the program and on the system administrator monitoring the responses generated; and, (iii) any security weaknesses of this approach.

(i) [2 marks] A file integrity checking tool such as tripwire can be very useful in identifying changed files or directories on a system, particularly when those change should not have occurred. However most computer systems are not static, and significant numbers of files do change constantly. Hence it is necessary to configure tripwire with a list of files and directories to monitor, since otherwise reports to the administrator would be filled with lists of files that are changing as a matter of normal operation of the system.

(ii) [2 marks] As well, there needs to be a process to manage the update of monitored files (as a result of installing patches, upgrades, new services, configuration changes etc). This process has to verify that the changed files are correct, and then update the cryptographic checksums of these files.

(iii) [4 marks] It is not too difficult to monitor a small list of critical system programs, daemons and configuration files. Doing this means attempts to alter these files will likely be detected. However the large areas of the system not being monitored means an attacker changing or adding files in these areas will not be detected. The more of the system that is to be monitored, the more care is needed to identify only files not expected to change. Even then, it is likely that user's home areas, and other shared document areas, cannot be monitored, since they are likely to be creating and changing files in there regularly.

Lastly the database of cryptographic checksums must be protected from any attempt by an attacker to corrupt it, ideally by locating on read-only media (except when controlled updates are occurring).

Question 3 Intrusion Prevention and Firewalls **[25 marks]**

(a) [5 marks] List three design goals for a firewall.

1. All traffic from inside to outside, and vice versa, must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall. Various configurations are possible, as explained later in this section.

2. Only authorized traffic, as defined by the local security policy, will be allowed to pass. Various types of firewalls are used, which implement various types of security policies, as explained later in this section.

3. The firewall itself is immune to penetration. This implies that use of a trusted system with a secure operating system.

(b) [5 marks] What is the difference between a packet filtering firewall and a stateful inspection firewall?

A traditional packet filter makes filtering decisions on an individual packet basis and does not take into consideration any higher layer context. A stateful inspection packet filter tightens up the rules for TCP traffic by creating a directory of outbound TCP connections, as shown in Table 9.2. There is an entry for each currently established connection. The packet filter will now allow incoming traffic to high- numbered ports only for those packets that fit the profile of one of the entries in this directory

(c) [5 marks] How does an IPS differ from a firewall?

An IPS blocks traffic, as a firewall does, but makes use of the types of algorithms developed for IDSs.

(d) [10 marks] Consider the threat of "theft/breach of proprietary or confidential information held in key data files on the system." One method by which such a breach might occur is the accidental/deliberate e-mailing of information to a user outside of the organization.

A possible countermeasure to this is to require all external e-mail to be given a sensitivity tag (classification if you like) in its subject and for external e-mail to have the lowest sensitivity tag.

Discuss how this measure could be implemented in a firewall and requirements for the email program. What type of firewall would be used here? What are weaknesses of such an idea?

[2 marks] Alternatively with suitable email agent programs it may be possible to enforce the prompting for and inclusion of such a tag on message creation.

[4 marks] Then, when external email is being relayed through the firewall, the mail relay server must check that the correct tag value is present in the Subject header, and refuse to forward the email outside the organization if not, and notify the user of its rejection.

[2 marks] What is a correct tag? Depends upon policy. Looking for a discussion of the rule here.

[2 marks] Relies on the client adding the tag, what if another program is used. What about using covert channel?

Question 4 Buffer Overflows and Software Security **[30 marks]**

(a) [5 marks] What are the two key elements that must be identified in order to implement a buffer overflow?

To exploit any type of buffer overflow, the attacker needs to identify both a buffer overflow vulnerability in some program that can be triggered using externally sourced data under the attackers control, and to understand how that buffer will be stored in the processes memory, and hence the potential for corrupting adjacent memory locations and potentially altering the flow of execution of the program

(b) [5 marks] List and briefly describe some of the defenses against buffer overflows that can be implemented when running existing, vulnerable programs.

Two broad categories of defenses against buffer overflows are: compile-time defenses which aim to harden programs to resist attacks in new programs; and run-time defenses which aim to detect and abort attacks in existing programs.

(c) [5 marks] Define the difference between *software quality and reliability* and *software security*.

Software quality and reliability is concerned with the accidental failure of a program as a result of some theoretically random, unanticipated input, system interaction, or use of incorrect code. These failures are expected to follow some form of probability distribution. Software security differs in that the attacker chooses the probability distribution, targeting specific bugs that result in a failure that can be exploited by the attacker. These bugs may often be triggered by inputs that differ dramatically from what is usually expected, and hence are unlikely to be identified by common testing approaches.

(d) [5 marks] State the similarities and differences between command injection and SQL injection attacks.

In a command injection attack, the unchecked input is used in the construction of a command that is subsequently executed by the system with the privileges of the attacked program. In an SQL injection attack, the user-supplied input is used to construct a SQL request to retrieve information from a database. In both cases the unchecked input allows the execution of arbitrary programs/SQL queries rather than the program/query specified by the program designer. They differ in the syntax of the respective shell/SQL meta- characters used that allow this to occur.

(e) [5 marks] Define input fuzzing. State where this technique should be used.

“Input fuzzing” is a software testing technique that uses very large amounts of randomly generated data as inputs to a program, to determine whether the program or function correctly handles all such abnormal inputs, or whether it crashes or otherwise fails to respond appropriately. The major advantage of fuzzing is its simplicity, low cost, and its freedom from assumptions about the

"expected" input to any program, service or function. It ought to be deployed as a component of any reasonably comprehensive testing strategy, especially in relation to commonly deployed software.

(f) [5 marks] Give an example of a security problem that can arise due to careless use of environment variables by shell scripts. Describe the functionality of the shell script, how careless use of the environment variable can be exploited and outline the potential effect of a successful exploitation.

Environment variables are a collection of string values inherited by each process from its parent, that can affect the way a running process behaves. The operating system includes these in the processes memory when it is constructed. Well known environment variables include the variable PATH which specifies the set of directories to search for any given command, IFS which specifies the word boundaries in a shell script, and LD_LIBRARY_PATH which specifies the list of directories to search for dynamically loadable libraries. All of these have been used to attack programs, and especially privileged shell scripts. The attacker changes the values of one or more of these, then calls a script running with other (higher) privileges, which is then "tricked" into running a program or loading a library of the attackers choice as a result.

******* END OF TERMS TEST *******