CIS4361 **Brandon Thompson**
Prof. Elibol Due Date: 4/16/2020

Homework 18

PROBLEM #8.1:

Consider the first step of the common attack methodology we describe, which is to gather publicly available information on possible targets. What types of information could be used? What does this use suggest to you about the content and detail of such information? How does this correlate with the organization's business and legal requirements? How do you reconcile these conflicting demands?

SOLUTION:
Types of information that could be gathered publicly is the path to the target system, applications, some internal information like providers. This information could be used to identify the location of important data, help identify bugs or holes in application security. The organization should like to limit all unnecessary data that is not directly controlled by their network, though there probably isn't a huge legal issue over this. There should be a balance between the amount of information that is made available through public connections and the security issues that stem from this.

PROBLEM #8.2:

In the context of an IDS we define a false positive to be an alarm generated by an IDS in which the IDS alerts to a condition that is actually benign. A false negative occurs when an IDS fails to generate an alarm when an alert-worthy condition is in effect. Using the following diagram, depict two curves that roughly indicate false positives and false negatives, respectively.

SOLUTION:
As seen in the graph below, as the frequency of alerts is high and the conservatives of signatures is low, the false positive rate is very high and the false negative is low. As the frequency of alerts decreases and the conservatives increases, the false positive level decreases, but the false negative level increases. Thus False positive levels and False negative levels have an inverse relationship.

PROBLEM #8.3:

Wireless networks present different problems from wired networks for NIDS deployment because of the broadcast nature of transmission. Discuss the considerations that should come into play when deciding on location for wireless NIDS senors.

SOLUTION:

If the organization is using WLAN then the sensor will need to be placed so that it can monitor the radio frequency of the access points in the area. Because access points are usually located in public and open spaces to distribute as much signal as possible, there needs to be more protected against physical threats. Another issue with wireless NIDS is that the sensor range is affected by mediums like walls, different walls made of different materials will not always allow signal through. The layout of the area also effects this.

PROBLEM #8.4:

One of the non-payload options in Snort is flow. This option distinguishes between clients and servers. This option can be used to specify a match only for packets flowing in one direction (client to server or vice versa) and can specify a match only on established TCP connections. Consider the following Snort rule:

```
alert tcp $EXTERNAL_NET any -> $SQL_SERVERS $ORACLE_PORTS\
        (msg: "ORACLE create database attempt:;\
flow: to_server, established; content: "create database";
                        nocase;\
          classtype: protocol-command-decode;)
```

a What does this rule do?

b Comment on the significant of this rule if the Snort device is placed inside or outside the external firewall.

SOLUTION:

a The main goal of the rule is to notify the administrator of a database creation attempt.

b If the NIDS is placed outside the firewall it will send a alert for all such attacks. IF placed behind the firewall it causes a serious deficiency in the firewall behavior.

PROBLEM #8.6:

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. What are the advantages and disadvantages of using such a tool? Consider the problem of determining which files should only change rarely, which files may change more often and how, and which change frequently and hence cannot be checked. Consider the amount of work in both the configuration of the program and on the system administrator monitoring the responses generated.

SOLUTION:
The program is advantageous because it will recognize altered files on a system, this works better when the file should not be changed often. It is easy to monitor critical files like configurations for critical systems because any changes should be well documented.

Disadvantages of this program are that everything changes eventually. If being used to monitor a large portion of files, the configuration of tripwire will have more overhead for the administrator. If a files does need to change there is a special procedure needed before a file can be modified. If the checksums are corrupted by an attacker either there will be a lot of alerts or the attacker could modify a file without the administrator's knowledge.