HW-Module11 Results for BRANDEN BARNES

Score for this attempt: 98 out of 100
Submitted Mar 31 at 10:32pm
This attempt took 205 minutes.

Question 1
30 / 30 pts

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. Hence consider the amount of work in both the configuration of the program and on the system administrator monitoring the responses generated.

Your Answer:

The advantage of using such a tool (tripwire) is that it is used widely amongst operating systems such as Linux, Mac OS, and Windows. Its protected database of cryptographic checksums is monitored regularly and is sensitive to intruder activity. It is difficult to monitor changing files, so it is important to make a list of known good files. Other disadvantages include determining which files to monitor because once they run on the system it cannot detect changes. The configuration of the program and the system administrator monitoring the responses generated should establish the baseline value so that when files change, the protection of the database of file signatures remains adequate.

Question 2
18 / 20 pts

Explain the suitability or unsuitability of the following passwords:

a. YK 334
b. mfmitm (for “my favorite movie is tender mercies)
c. Natalie1
d. Washington
e. Aristotle
f. tv9stove
g. 12345678
h. dribgib

Your Answer:

a. Unsuitable because it does not have a variety of characters, numbers, and special characters. It also is short in length.

b. Unsuitable because it does not have a variety of characters, numbers, and special characters. It can also be guessed because it contains relevant personal information.

c. Suitable but not strong because it does not have a variety of characters, numbers, and special characters. It can also be guessed because it contains relevant personal information including the person's name.

d. Unsuitable because it does not have a variety of characters, numbers, and special characters. It can also be cracked using a dictionary attack.

e. Unsuitable because it does not have a variety of characters, numbers, and special characters. It can also be cracked using a dictionary attack.

f. Suitable but not strong because it does not contain various capitalizations or special characters. It also contains dictionary words.

g. Unsuitable because it does not have a variety of characters, numbers, and special characters. Contains a very guessable password.

h. Unsuitable because it does not have a variety of characters, numbers, and special characters.

Question 3
20 / 20 pts

Assume that passwords are selected from four-character combinations of 26 alphabetic characters. Assume that an adversary is able to attempt passwords at a rate of one per second.

a. Assuming no feedback to the adversary until each attempt has been completed, what is the expected time to discover the correct password?
b. Assuming feedback to the adversary flagging an error as each incorrect character is entered, what is the expected time to discover the correct password?

Your Answer:

a. Since no feedback to the adversary is granted until each attempt has been completed the expected time to discover the correct password would be 26^4/2 given that it would only take half the attempts needed to succeed.

b. If the characters can be guessed correctly 26/2 = 13 times. For a four-character combination, 13 x 4 = 52 times guessing. That would result in 52 seconds needed to guess the password.

Question 4

30 / 30 pts

Suppose you observe that your home PC is responding very slowly to information requests from the net. And then you further observe that your network gateway shows high levels of network activity, even though you have closed your email client., Web browser, and other programs that access the net. What types of malware could cause these symptoms? Discuss how the malware might have gained access to your system. What steps can you take to check whether this has occurred? If you do identify malware on your PC, how can you restore it to safe operation?

Your Answer:

The types of malware that could cause these symptoms include zombie, bot, and spyware. A zombie, bot is a program run on an infected machine that is activated to launch attacks on other machines. This can slow down a person's PC by using their network resources. Spyware is software that collects information from a computer and transmits it to another system. This can slow down a person's PC because additional resources are being used to run programs in the background of that person's network. Malware can gain access to your system from fake emails, unsecured downloads, compromised websites, or poor security. Anti-virus software scans are a way to check whether this has occurred. These scans will show unusual network connections and monitor resource usage. To store your PC back to safe operations you should follow the recommendations set in your antivirus software. Make sure that your PC gets disconnected from the network so that further damage will not occur or spread to more targets. You should perform all recent updates and change/strengthen all passwords.

Quiz Score: 98 out of 100