Assignment 10 **Tyler Wilding**
COSC 4426 Due Date: 27/11/16
Prof. Biocchi –
TA: – –

Tools Used

For this assignment I used Kali-linux as, while this could be done on any livecd, Kali comes with all of these various tools preinstalled which makes things much faster. The tools within Kali that I used to access passwords and files are:

1. bulk-extractor
2. John the Ripper
3. creddump
4. Foremost
5. dumpzilla.py

These tools look for passwords of any kind including Windows account passwords, as well as looking for other sensitive information like credit cards.

Preamble

The point of this assignment is that gaining physical access gives you full control. It doesnt matter how many passwords you have protecting your account or logging into your computer, all of these can easily be removed with a live-cd. This is because when booting into Linux from a livecd it does not care about any of the Windows security permissions as there is no Windows to enforce them. It sees everything as simple files that can be read and wrote to.

Results

bulk-extractor

Mount the drive, and then run

```
bulk\_extractor -R /dev/sda2 -o ~/output.txt
```

This will scan the entire harddrive and output the results into a text file in the home directory. After parsing through 60gb of the harddrive I found the following:

1. Credit Card Numbers
2. Email Addresses
3. IP Addresses
4. Bitcoin Addresses
5. Telephone Numbers
6. Many more

creddump

Mount the drive, then navigate to the System32/config folder. Run

```
pwdump SYSTEM SAM > ~/hashes.txt
```

This will get all all of the windows account password hashes and store it into a file hashes.txt in your home directory.

1. Password Hashes
2. Can find other hashes as well

John the Ripper

This script allows for automated hash cracking, since we just retrieved the windows password's hashes we can now figure out what they actually are instead of just removing them.

```
john --format=NT hashes.txt
```

Windows passwords are hashed using MD4, this will use dictionaries and a bruteforce methods to attempt to reverse the hashes.

1. Reverse Hashes
2. Supports Dictionaries
3. Was able to crack a few of the hashes in a reasonable amount of time.

Foremost

Can scan for deleted and stored files of specific formats. Run

```
foremost -t jpg -i /dev/sda2
```

This will get all of the jpgs on the harddrive.

1. Any file off the computer that fits a specific pattern or has the matching file extensions of the search.

dumpzilla.py

Specifically designed to scan through Firefox profiles for passwords, bookmarks, history, downloads, etc.

```
python dumpzilla.py <profile location> --All > ~/output.txt
```

This will scan the profile for any possible information and place it in output.txt

1. Saved Passwords (none found)
2. History
3. Downloads
4. Bookmarks

Security Issues

I used a computer that is being used by multiple people, so this is a security vulnerability in it of itself as these otheraccounts that have admin access can be compromised. However in the end it doesn't matter, as any password could be straightup removed when using a live linux install, so password strength is irrelevant. It was good that I was unable to find any saved passwords, as it would have been very easy to get into peoples accounts if so. Many deleted files were able to be accessed and people often think that when they delete a file it is gone for good, which is not nessecarily true. The default Administrator account was enabled in this Windows install, which is a problem as this account can easily be turned on and then turned off and you would not even notice that your password was removed. However I feel that the computer is mostly secure as it is very difficult if not impossible to avoid being compromised by these methods.

Solutions

This emphasizes how important it is to restrict physical access to computers, if this is not done than many other security efforts will be for nothing when someone gets physical access. However in addition to that, it may be a good idea to enable secure boot on all computers so that people cannot so easily run a livecd off of your computer. Secureboot ensures that only signed versions of operating systems can run. However, if someone has physical access they can just as easily go into the BIOS and change it, so a BIOS password must also be set. Another option that the user can take is to fully encrypt their harddrive, this enables security on the files so that someone cannot just easily see and access them through the live cd; however this opens the opportunity for brute-forcing the password so it must be a secure password. While some people do not want to use Microsoft's Live login for Windows 10 accounts, it is a good idea as it prevents the accounts from having their passwords removed. The default Administrator account should be disabled on all Windows installs as well. Passwords should never be saved with the browser as it is another opportunity for them to be stolen; as well as browsing history should be cleared often. Lastly, in order to avoid being dictonary attacked, passwords should have some sort of strength associated with them, however this will not prevent people getting into your accounts if they truly want to. Other than that, there isnt very much you can do to stop the damage if someone gets phyiscal access, the best defense is to forbid physical access by ensuring the systems are in a secure location.