Megan Moore
Buff ID: 1014735

John the Ripper and Prey

John the Ripper software

Question 1: what did you do?

For this assignment, I downloaded two tools. The first of these was John the Ripper, a password cracking program. I noticed there were many different versions of this program and attempted to first download and run it in the cloud without any success. I then did a simple direct download and install. This particular program seems to have a large following online and many helpful resources for learning how to fully use the program to its upmost ability. As a beginner, I did not crack the extent of the power of this tool but I did get to see some of what it can do, either on my own machine or in the how to videos online.

For some background, I researched John the Ripper and learned the program was originally developed for Unix operating systems and due to its success, it then was further developed for other platforms as well. Amazingly, it is one of the more popular tools for password testing and password cracking as the program is able to combine multiple password cracking models into one single package. Even further, it is able to autodetect password hash types and for more advanced users – it contains a customizable cracker. The program typical is used to break encrypted password formats used in Linux or Windows, but is also capable of breaking other secure file types like locked PDFs or ZIP files.

Question 2: what were the results?

For this assignment, I started out curious what the full list of file types John the Ripper supports might be. In the tool, I typed “john –list=formats”. This produced an extensive list I was quite surprised to see. This I noted as handy to be aware of and enlightened me on how easy others might use this tool to crack all sorts of files, I otherwise thought to be secure.

I spent some time next then researching how John the Ripper has three different modes. Single Crack mode, Wordlist Crack mode, and Incremental mode. In the single crack mode, the tool makes use of any information that is available in the form of a username and variations of that word. Basically, I observed it is the fastest method to use if you need to crack a full password protected file. Incremental mode is what one would use as it may not complete while running. I started it and then quit it. I would describe this mode as a last resort which is lengthy, still very powerful, but the time it takes to try every possible character/number combination is a real drawback. Wordlist, as mentioned in the assignment instructions, seems to be the most useful mode for the tool. In wordlist, it compares the hash to a known list of potential matches. There is the general wordlist file the tool uses “Passwordfile” but there are countless others that can be found online as well as you can create your own. The wordlist functions as a dictionary of sorts to compare against. The general wordlist John the Ripper comes with contains most of the common passwords people tend to use.

Also, I noticed that while the tool is running it is possible to pause it and later resume the password cracking process. This was helpful due to constant interruptions while I was working on this assignment. I ran the general wordlist and regrettably, it did indeed crack a few of the simpler files I had saved to my computer. All of my major files/credentials were not cracked so I'm a bit proud knowing some of my more crucial file passwords I use are not on the common list.

Question 3: what did you learn?

This assignment confirmed my thought that somehow, it was possible for someone to gain access to a network and easily crack and obtain the credentials not just of one user but many. This would be an IT department's greatest fear for multiple users on a network. Using a feature called shadowing, I watched a YouTube demonstration of how an entire list of users on a network was accessed, cracked and then each user and password was saved. This would allow the hacker to return with the proper credentials and then cause much more targeted harm.

I was further curious if other options remained for people to use to crack secure files. Regrettably, there is a long list of tools users can manipulate to this end. Prior to this course, I had no idea these tools were so simple to obtain and have so much easily access walkthrough or FAQ documentation. This means anyone can repeat what I did and crack passwords of important items.

Another feature I wasn't aware of was the tool's ability to be specific in the encryption type when working to crack a password. If known, the user can pinpoint a certain type of encryption and then utilize either the single or wordlist modes to break the security. I will note, at the end of this practice session with John the Ripper, I did not feel secure enough to leave the program installed on my machine. I went ahead and removed it once testing the wordlist and single mode cracking abilities. I found the program to be too effective, and had I more time to develop skill with the tool, I could easily build a wordlist to break all of my own passwords and potentially others. This wordlist example would not be one I would simply want floating on a pc able to be accessed on a network, locked or not. If anything, this tool just continues to prove how false of an idea I had in how secure my files and computer was.

Prey software

Question 1: what did you do?

For this assignment, the second tool I downloaded was the tracking software called Prey. This tool is used as tracking software and can be installed on many different platforms. This allows a user to potentially track down and recover a stolen item, such as a laptop or phone. Think of it similar to the popular vehicle tool called LoJack which tracks down stolen cars using GPS signals to pinpoint a location. I had no idea such a great tool existed for laptops and phones. I've seen various spin off programs like Find My Phone or browser plugins like Firehound for Firefox over the years but Prey differs from all of these as it works cross platform for mobile devices, Linux, Mac and Windows.

After installing the program, registering it and receiving the API key to activate it, I spent some time reviewing the program and learned the way the program tracks the location of your device is via the on-board GPS chip (in mobile devices) or by analyzing nearby WiFi networks. Prey as default does not activate itself but if your item goes missing, you are able to logon online to activate your protection. Once the device is turned on and if able to connect to a network, the program can document screenshots of what the thief has use the device for and send that back to you. If setup, the program can also access the camera or webcam feature of the device and take a picture of the user.

The only downfall is like all tracking software options, this must be installed and configured in order to get the most use out of the tool. So perhaps Prey will not be able to help you recover your stolen device but you can potentially gain information on what the thief uses your device for without their knowledge that the tracking software is installed on the machine.

Question 2: what were the results?

To test this software, I downloaded it to my personal laptop and phone. For my laptop, I removed the lock password login I usually have to test if this can be remotely setup using Prey. I left the house with my laptop and drove to a nearby Starbucks pretending the device had been stolen. I activated the Prey software tracking online using my phone and instantly received notification when I accessed the public WiFi with the laptop. Using the Prey interface, the website has two columns of options – Information to gather or Actions to perform. The first the tracking features of the software. This saves the IP address, etc. Then once this is done, I could navigate to the Actions section to remote lock and save this change. You are able to indicate in the program if your device is OK or MISSING. Once marked missing, the remote lock action activated. I saw the screen change and go to a lock screen. This gives me some piece of mind that at least this step is possible for a stolen laptop. If noticed quickly enough, I can enact these actions to protect my information. It's not perfect, but better than doing nothing.

For the test on my phone, I had my family member take my phone and leave the house when they ran an errand in order to trigger the location monitoring. While logged into the Prey Project website, I could see the location update, activate the camera and lock my phone. I typically always have a lock already setup on my phone but for this test, I removed it to see if this was something that would be successful using the software. I can confirm it did work on my Android device but am unaware how well it would function for a Mac of Apple cell phone device. Another limit for a cell phone is there is no way to remotely wipe the phone but at least you can enable a lock. I do however already have two programs on my phone for remote wipe capability. As I use my phone for personal use as well as work, my work profile has its own secure remote wipe capability from my company. For my personal use, I have a separate software installed which permanently wipes my phone and resets it to factory setup. I may not be able to recover my device using Prey, but at least I have a chance to and worst case, I can use my separate software as a security backup to remove all my personal information from being accessed.

Question 3: what did you learn?

This assignment reinforced the necessity for a tracking type software to exist on all my personal electronic devices which connect to networks. This includes my personal laptop, phone, and phones owned by my family members along with our extra desktop pc. Prey's main feature in the platform is location tracking and monitors movement of the device, for example – the changing of network a laptop is connected to. The tool also can be configured to have automatic triggers to alert you when an event is detected and perform security actions if desired.

These security actions are very useful for a stolen device. They include remotely recovering or wiping information from a lost or stolen device, maintaining an inventory for global monitoring a device's location as it changes over time, or simply providing an interface to give the owner security capabilities to choose from in the case of loss. While I saw the importance of having such software on my device, this semester’s course and assignments such as this one has convinced me to add these tools across all my devices. While my kid uses their phone only to watch YouTube or play simple games, they are dialed into our network with passwords already saved. This direct access could be used by a thief in the area to gain access to our network and then steal other information once hooked up. Cybersecurity is of upmost importance and many individuals have no idea how easily their information can be taken or what can be done with it.