William Adams
Lab three: Password Cracking
IS 3513-002
November 26, 2023
Professor Wooldridge

In our 3rd lab of the semester (Password cracking) we used the applications "johnny" and "Ophcrack". I have heard of "Johnny" multiple times over my time in the cyber community, but I have never really used either of these applications. I was very interested to get to know more familiar with these applications and to just use them in general. With passwords being so important in today's web for really everyone's security, from an organizations securirty to someones personal account security, I was excited to get some more knowledge on the topic and to get some experience with the applications. With this being the 3rd lab, we are using the virtual machines, it is getting easier, and I am gaining more knowledge about these different applications and systems.

The original steps in this lab were to download the files from canvas and put them onto the VM that you were using. I believe some of us students were having a hard time getting the files on the VM, so the professor put the files that we needed to download (shadow, Sam, and system) as shared files on the VM. This was very helpful because I was already starting to have trouble getting the files onto the VM I was using at the time until I saw the announcement where it said the new instructions. I loaded up a random Kali-hunt Virtual machine, nobody was on one, so it was very easy to find a virtual machine that wasn't being used by another classmate. I loaded into my machine, and I directly went to the shared files and found the files that the professor had left there for us to use. I then went to open the application "Johnny", the launch of the application was very simple and had no bumps. I had never used Johnny before, so I was very eager to use it and see what it was all about. Password cracking is a very interesting topic in the cyber world so I couldn't wait to get started. I then loaded the "Shadow" file onto Johnny, which was also simple, I wasn't 100% sure if I was doing everything right but I did get results of the 4 passwords that were from the file. I got the first three passwords fairly quickly (maybe like 3-7 minutes), but the last password I needed so that I can have 4 took a bit longer but I did end up getting it. I provided the screenshot of the 4 passwords that I cracked from the shadow file on Johnny. I can see how Johnny can be a great appliance to use with cracking moderate to easy passwords which is really fascinating to me. I thought there was also another cool feature of the application that I thought was pretty interesting that I picked up on when watching a YouTube video about "Johnny", being able to guess the password is pretty cool to me. I can see how that can be beneficial to an organization when cracking passwords. With the next step of the lab, I used the application "ophcrack", where I cracked the file "Sam". I didn't have too much trouble with this step, the only hurdle I had to overcome was that I didn't look at the instructions saying you have to put the "System" and the "Sam" file into one directory then crack it. I figured that part out pretty fast, so it wasn't too much to overcome. It was really interesting to see how long the operation works when you put the file into their system. It didn't take too long to get some cracks into the passwords, it was fairly simple to get the passwords cracked. For the 7th step on the lab, I was honestly very confused on what I was supposed to be typing into the engine on the website. I know it was supposed to be some sort of hash values, but I was not understanding exactly what I was supposed to there to be honest.

For this next part we were supposed to find our computers password file, at first I was a little confused because I thought we were supposed to go to our actual database and not on the Linux VM, but I think I was mistaken. The computers password file was

located on the files.zip directory and was not viewable. I clicked on the “Lab3A.zip” and it said right away that I needed a password to view the passwords. It did let me copy the password files; I’m guessing because it’s still protected by a password. I was honestly confused trying to find the password file, but I believe I found the right file and directory.

The passwords that I have cracked, and judging how strong each of them are in terms of security. For the shadow file that I cracked using Johnny, the passwords that I had recovered were “ccwhite”, “derf”, “secret”, and “redbox.” I would say that all of these passwords are relatively weak and have no unique part to them that can make them harder to guess. None of the passwords have any capital letters, none of them are long in any way, or any special characters in the password. I would say these passwords can make any system venerable. For the passwords that I had recovered from the Sam file, using ophcrack was a bit of a different story. The passwords that I had recovered were “N3verm0RE”, “Chrys4nth3mum”, “Heywood1211935”, and “000000”. These passwords were mostly all unique expect for one that was only 6 0’s. The first password that was recovered “N3verm0RE” was solid, it wasn’t the best, but I think it gets the job done by using some capital letters and numbers in the password. The second password that was recovered was “Chrys4nth3mum”, this password is also very solid, the use of capital letters, numbers, and a good length makes this a great password. The next password that was recovered was “Heywood1211935”, this password was also very strong with the use of capital letters, a ton of numbers, and a good length to the password. The main component to me that makes a good password is that it is unique in some way, the more a password is common the more likely you are to have your password compromised.

Password policies are crucial for any organization, the better an organizations passwords policies are, the more secure the organization is. Having a well thought out password policy can make any business have a better defense against unauthorized users entering their system. A good password policy involves password complexity requirements, this involves mandating the use of a combination of uppercase and lowercase letters, numbers, and special characters, thereby creating robust and resistant passwords. Length requirements can also help make a password more secure, so that they aren’t easily guessed or common passwords that are used. Another critical thing that should be added in an organizations password policy is mandatory password updates. Having these frequent updates to users’ passwords can only make the chances of unauthorized users breaching their system. Especially with peoples stolen credentials happening so much nowadays, it is crucial to update passwords frequently. An organization can help their cause by informing their employees about the importance of having strong passwords and following the company’s password policy that is set in place. Highlighting the consequences and the effects it can have on an organization is also very important for employees to understand. With passwords being effective but not 100% security for any user or organization, multi-factor authentication (MFA) can play a big role into making users accounts more secure. MFA adds an extra layer of security by requiring users to provide multiple forms of identification, typically combining something they know (a password) with something they have (a security token or a mobile device). I have seen so many businesses use MFA nowadays and it is such a good technique to use to add that extra layer of security. This additional authentication factor significantly enhances the overall security posture, making it significantly more

challenging for malicious actors to gain unauthorized access even if passwords are compromised. Lastly, a password policy can make the overall framework of the security of an organization great and can add extra layers of protection of their networks with different techniques.

I do go to school at the University of Texas at San Antonio (UTSA), I would say the password protection is actually pretty solid. With how many malicious hackers there are out there nowadays on the web, it is crucial to follow strict password policies. Especially with how much data and information the school stores in their system, it paramount that that there is complicated system in place for security. I have been at the school for two years now and the password policy has changed a little. The first thing that stands out when it comes to the password policy is how long the password has to be. To log in to ASAP or to view any sensitive information you have to type in your "passphrase". The passphrase has to be 20 characters I believe, I think this is a very good technique because of how long the passphrase has to be, making it unique and hard to guess for malicious hackers. I have never had this technique used on any other sites or organizations that I have been apart, and I believe that it can play a major part in the security of student's accounts. For my two years here, they have also implemented the use of multi-factor authentication (MFA), this also adds another layer of security for students and facility from threats. "In the cloud-based era, passwords are not enough to keep all of your business accounts secure and protected, which means businesses should be considering Multi-Factor Authentication (MFA) solutions." (Witts 2021) The first year they used MFA, we used this app called "Duo Mobile" which was linked to our UTSA account I'm pretty sure. When we log in it sends a notification to Duo Mobile to our phone, and we have to press a green button that says that the user is authorized to log in. I thought this was a solid way to add protection to my student account, even if someone gets access to my passphrase, there would be a notification sent to my phone saying that someone is trying to log in to my UTSA account. What they have added this semester to the MFA policy is even stronger from the semesters past. Now they send a random six-digit code to the Duo Mobile app, and you have to verify the code. I believe UTSA has a great password policy, with how much sensitive information there is that can be stolen, it is crucial to have strict procedures to ensure the confidentiality of the student's information.

Passwords play a large role in the identify access management (IAM) systems. Passwords serve as the primary authentication factor, verifying the identity of individuals seeking access to sensitive information or secured systems. "The most common type of digital authentication is the unique password. To make passwords more secure, some organizations require longer or complex passwords that require a combination of letters, symbols, and numbers." (Gitten 2023) The password policies of organizations directly affect the influence the effectiveness of IAM systems in ensuring secure access. In order to validate their identity, users of IAM systems usually need to enter their unique credentials, which are frequently a username and a password. The standards for generating and preserving secure passwords are set forth in a strong password policy found in IAM, which emphasizes elements like length, complexity, and frequent changes. IAM systems improve their capacity to thwart unauthorized access attempts and reduce the danger of compromised credentials by mandating strong password practices. Furthermore, IAM systems get an additional degree of protection when multi-

factor authentication (MFA) is integrated with passwords. MFA strengthens the authentication process by requiring users to give extra identity proof, like a one-time code texted to a mobile device.

Appendices

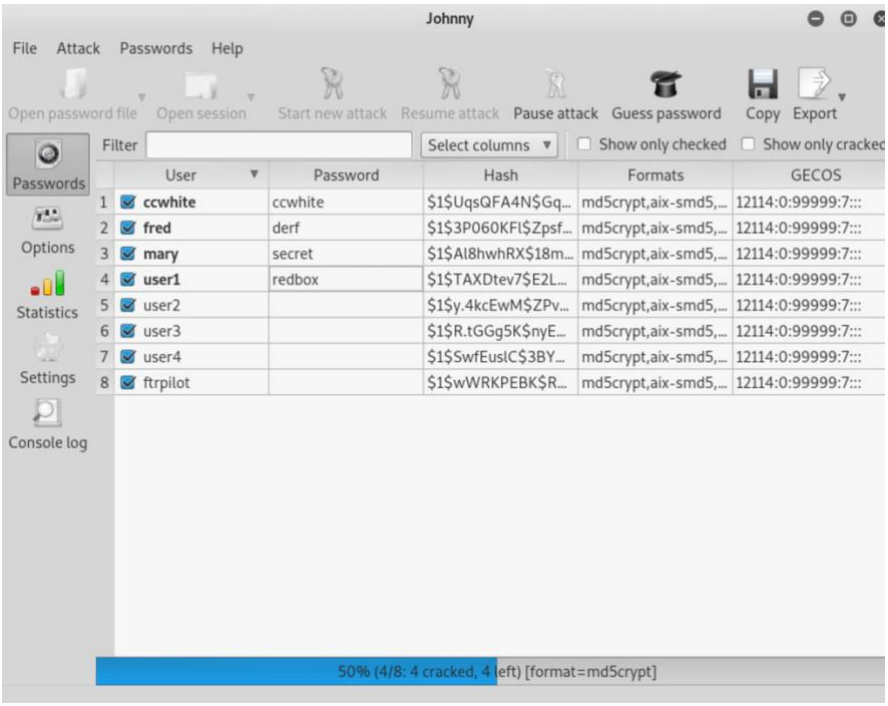

Figure 1 Password Cracking Shadow File Using Johnny.

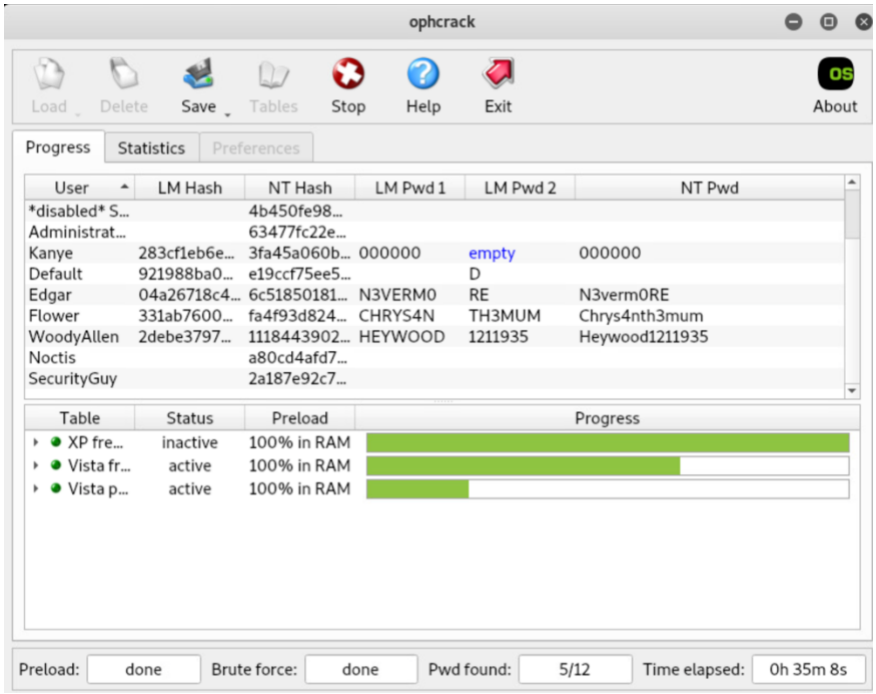

Figure 2 Password Cracking Sam/System File Using Ophcrack.

Bibliography

Gittlen, S., & Rosencrance, L. (2021, August 10). *What is identity and access management? guide to IAM*. Security. https://www.techtarget.com/searchsecurity/definition/identity-access-management-IAM-system

Witts, J. (2023, March 28). *What are the benefits of multi-factor authentication?*. Expert Insights. https://expertinsights.com/insights/how-multi-factor-authentication-can-keep-your-data-secure/