Daniel Allex

Mrs. Price

Honors LA II

6 March 2019

Research Journals on Hacking

1. 2/23/19

Research Results and Findings:

Hackers may target computers that do not even have any useful private information. For example, a hacker may want to use a computer to use it start DoS attacks when the internet is fast enough on a network. DoS stands for denial of service, and it is a type of botnet attack. Another reason as to why a hacker may do a cyber attack on a computer without useful information to steal is to hide their identity before hacking an authority such as a military or government computer. Hacking one computer and using that computer to hack another computer, and so on, will make it difficult to figure out who started the attack when the government is investigating. A final reason as to why a hacker would want to attack a computer besides stealing information would be to use the computing resources of a computer to run services or servers ("Beware of Hacking"). This will be useful for my research project for explaining reasons as to why hackers do cyber attacks. I will not only explain how hackers try to steal information, but how they try to use the computers and resources of users for other reasons.

Thoughts on my Progress:

Right now I think that I am in a decent spot for my research. Although this is only my first research log, the source that I am currently researching provides great information on the

topic. Hacking is often used to mostly describe when hackers merely just steal personal information, but as this source implies, there are more reasons as to why a hacker may want to target others. This is something that I will want to explain during my research presentation. The source mentions botnet attacks and attacking the servers of companies and the government. This is something that interests me, so I may decide to research specifically how that type of cyber attack works in a future research log.

2. 2/24/19

Research Results and Findings:

In order for a hacker to get into a computer for the uses described previously, hackers must find a vulnerability in the operating system. Although this sometimes involves getting the password for the user's operating system, stealing an account for social media and other online accounts usually will not grant a hacker access to a computer, only the account. Once a hacker gets into a computer, however, they can access any account including social media. It is not uncommon for hackers to sell the stolen accounts. Once they acquire all of the passwords and accounts is normally when the hacker will start using it for the reasons mentioned before, such as hacking important computers and servers while hiding their identity ("Beware of Hacking"). I will use this research in my presentation to explain how hackers access computers and what they can do once they have access to a computer.

Thoughts on my Progress:

My research is doing good so far. I am currently focusing on the topic of hacking at a general level; however, I already have certain topics that are more specific and that go into more detail planned to research. This will include the types of hacks and how they work. Although I

already started explaining a bit in my research how hacking works, there is no specific techniques explained. The best way to not get hacked is to be able to understand how most hacks work. Presenting the types of hacks will not only allow my audience to become more informed about this topic, but it will also prevent them from getting hacked. There is still a lot to research, but I think that the researching process will go smoothly because I know what I want to discuss in my presentation.

3. 2/25/19

Research Results and Findings:

One way to know whether or not a computer has been hacked is if there are random changes made to files. In order to make a strong password for an account, words in the dictionary should not be used, and a combination of numbers, special characters, and letters with ten or more characters total should be used. If a hacker gains access to a computer, they can interfere with files, send emails on the behalf of the comprised user, and attack other computers. There are a few common ways that people get hacked. One of which occurs when the user has an unsecure computer or Wifi that it is connected to. A second way is when a password is exposed due to bad website practices, such as if an entered password is not encrypted and is transferred as simple text. Finally, installing untrustworthy software from the internet could cause viruses that expose passwords ("Beware of Hacking"). I can use this information to inform my audience on how to avoid getting hacked. The information from this research log explains safety procedures for users to follow and places where users could become exposed, so this information will be very useful in my presentation.

Thoughts on my Progress:

I feel that my current research includes a lot of quality information, and that most of it will be used in my presentation. I will be starting to do research on a second source now that I finished researching my first source. Next, I plan to research some of the methods used in hacking. Although I touched on the methods a bit in my previous logs, the information on the methods is general and undetailed so far. The next source that I will research will actually have information that is detailed for specific hacks and not just be about how hacking is done in general. In my actual presentation, I plan to discuss a few in detail rather than just listing all of the methods, but this may mean that I will be unable to cover all of the major hacks. This is a decision that I will have to make in prioritizing what information to include for a five minute presentation.

4. 2/26/19

Research Results and Findings:

A manual brute force is entering commonly used password in an attempt to get into an account. This is slow and unreliable because doing a brute force attack manually only allows a guess every few seconds, and there is a good chance that the system will put a cool down on when a password can be entered after a certain number of attempts. An automated brute force, where a program automatically puts in combinations of passwords will be faster than a manual brute force, but it still would take awhile for the password to be guessed. The only way a manual brute force would have a good chance in getting a password is if the password was short and easy to guess ("Password Attacks and Countermeasures”). I will use this in my presentation by explaining the flaws of a brute force attack. Although it is a common method, there are better methods.

Thoughts on my Progress:

I am making great progress in my research logs. One of the first parts of hacking that I wanted to research was a brute force attack, and now I know more information on this. Before I chose this topic, I believed that guessing passwords without using an automated program was not considered a brute force, but now I know that manual brute forces are a thing, along with automated brute forces. Next I want to research hashes, which typically include dictionary attacks and hashes. These topics are included within this article. I still want to be able to research other methods that are not based on directly cracking passwords, such as methods that are based on installing viruses to then access a computer or accounts also. I want to really understand how a virus can lead to accessing a password along with the most common ways that viruses are installed onto computers.

5. 2/27/19

Research Results and Findings:

Passwords are converted from clear text into a hash value through an algorithm. Systems store passwords as hash values rather than clear text because it would be easy to access passwords if a password database was leaked. If a database is leaked, a hacker can only use the hash values, which cannot be restored to its original value through a reverse algorithm. To compare an entered password to the stored hash value of a user, the algorithm is applied to the inputted text, and if the hashes match, the system determines that the password was correct ("Password Attacks and Countermeasures"). I will use this information to explain how password systems work. It is important for the presentation to explain how passwords work because it is

needed to understand certain methods of hacking. Certain hacks use hash values, so it is essential to understand why they are used.

Thoughts on my Progress:

This information is very useful to my research and overall understanding of the topic. I now understand how password systems work, which is important for the topic of hacking because gaining access to accounts is one of the most common uses of the term “hacking”. I want to gain a deeper understanding as to how hackers can crack passwords, and it is interesting to know that even getting the hash values would be difficult to crack since the algorithms are irreversible. This makes me wonder how important information is cracked in large amounts when databases are breached if hackers must crack hashes. If a hacker got a list of hashes and were to try to test them, they would likely need an algorithm. My next research log from this article is going to be related to how hackers use hashes, so I hope to understand the methods used as well as how they acquire the algorithm.

6. 2/28/19

Research Results and Findings:

Hackers are able to get a list of usernames with their corresponding hash value if they comprise the system. With this list, they can use a program that attempts to determine the password for each hash value. A hackers’ dictionary is a list of common one word passwords. A hacker would have a program that applies the algorithm on a password in the dictionary and check whether the hash matches any of the stored hashes in the comprised list. A rainbow table is similar, except that instead of applying the algorithms, they are already applied for many common passwords up to ten characters. This speeds up the process significantly ("Password

Attacks and Countermeasures”). I will use this information in my presentation to discuss common practices for password cracking. I can make a table for the strengths and weaknesses of a brute force, dictionary, and rainbow table when presenting this.

Thoughts on my Progress:

My research on hacking is doing well so far. I am currently focusing on password cracking which is very interesting. It is very concerning to see that just by having the hash list, rainbow tables already many common passwords for up to ten characters premade. However, in order to get a hash list, the website will need to be comprised, so it seems difficult to gain access to one of these lists in the first place. I will likely do more research on specifically how hash lists are gained since I will likely spend a decent amount of time discussing password cracking. This seems like a very important part of hacking in general. Another thing that is concerning about this information is that rainbow tables are premade, meaning that they are available online if the hacker decides to not make their own, making them easily accessible. I may decide to research more on how websites can be more secure to prevent rainbow tables from doing any damage.

7. 2/3/19

Research Results and Findings:

It is important to remember that hackers must first have a hash to get a password through a rainbow table and that not every possible combination is pre-hashed in rainbow tables. In addition, hackers usually stop after ten characters for rainbow tables. In addition, the likelihood that a rainbow table will be useful for a certain website is low because websites usually apply “salts” which are values added to a password before hashing it. This makes all rainbow tables useless unless they apply the same salt ("Password Attacks and Countermeasures”). I will use

this information to explain how even with how easy rainbow tables and even dictionaries make password cracking, it is very unlikely for a hacker to be able to successfully crack passwords. Not only must they first steal a list of usernames and hashes through comprising an administrator, but most websites add salts to passwords before hashing anyways.

Thoughts on my Progress:

This research made be better understand how hackers actually password crack. The algorithm that they use is a common one that most websites use, but before applying this algorithm, text is usually added to the password. This text is always added to the password when creating it and when a user tries to log in, so the hashes will still match. This is the last research log for this article, so I will start to research another source. I think that I will choose to research malware, something that is used commonly to hack. Malware is how a list of usernames and password hashes would be stolen as described in the article just researched. I am hoping to find more in this research than the common knowledge about malware, that it is usually obtained from downloading something unsafe. I want to find out what some malwares do better than others and some of the lesser known ways that malware can be installed.

8. 2/4/19

Research Results and Findings:

Malware, also known as “malicious software”, is software that is meant to steal information from a computer or install other malware. They also usually self-replicate and spread. One type of malware is the trojan horse, which is a program that is meant to look harmless that does malicious things. Worms are pieces of malware that replicate and spread to other computers through a computer network without needing to be executed. Viruses are

programs that replicate themselves into other computer programs, only doing damage when executed, and they rely on the sending of files to do damage to other computers (“Malware”). I will use this information to explain the types of malware. I will make the connection between malware and hacking by explaining how viruses lead to hacking. Viruses are often used to get passwords to hack.

Thoughts on my Progress:

I have made great progress so far in my research. For only my eighth research log, I have research on numerous areas of hacking. My next research log will also be on types of malware. Once I finish researching malware and how hackers acquire passwords besides password cracking, I will start to look to see if there are any other hacking and password cracking methods. So far, I have only researched brute forcing, dictionaries, and rainbow tables in terms of hacking methods, so I want to see if there any other major types. I think that based on my research, I will be able to create an interesting and informative research presentation on hacking. In my actual presentation, I am unsure yet whether I would want to explain every type of malware, but I feel that it would be a good idea to explain every type of hacking method.

9. 2/4/19

Research Results and Findings:

Ransomware is another type of malware. This type will not allow the user to access their infected device unless a payment is made. Rootkits are pieces of software that are meant to make other pieces of malware undetectable, with the ultimate goal of allowing the hacker to continue having access to the computer. Keyloggers are pieces of malware that log any keys pressed on a keyboard, giving a hacker access to passwords if the infected user types in any passwords with a

keylogger installed. Spyware is a type of malware that gathers information about a user through having keyloggers, stealing files, and monitoring any computer activity. Adware is malware that gives many random advertisements (Malware). I will use this information to also explain the types of malware. It is important to understand malware when discussing hacking because malware is commonly used to hack.

Thoughts on my Progress:

I have a good amount of information for my project so far. I am planning to finish researching this source in order to get more information on malware. Once I finish researching malware, I will likely look into white hat hackers, which are hackers that use hacking techniques to find vulnerabilities for companies. After researching types of malware so far, I am still confused on how websites sometimes have their list of usernames and password hashes comprised. It seems like malware is mostly gotten through downloads besides worms which can spread through connected networks. The system that the list is stored on though is likely very secure and is likely monitored by security experts, so it makes me wonder how malware is used to get this sensitive information. Specifically getting the list of usernames and password hashes is something I may research further later.

10. 2/4/19

Research Results and Findings:

There are some pieces of software that will advertise itself as an antivirus program and will claim to have detected many viruses. It is common for some antivirus programs to actually be threats themselves. They may claim that they will only remove the detected viruses if the full version is purchased. This is usually a scam, and sometimes it will actually download more

malware. In order to prevent these fake pieces of security software, a firewall should be turned on, the computer's operating system should be up to date, and it is important to not click on any pop up ads ("Malware"). I will use this information in my presentation to explain how things that do not appear to be security threats sometimes are. I will explain that it is important to research a program before downloading anything.

Thoughts on my Progress:

I am making great progress in my research. This information is useful in explaining how to prevent getting viruses and ultimately getting hacked. Although hacking is my main research topic, a major part of this is malware. Malware is often the cause to people getting hacked, so this is important information. I am still hoping to have enough time to research the difference between black and white hat hackers, as well as phishing. In addition to malware and password cracking, a large amount of hacking is due to phishing. However, even with what I currently researched, there is still plenty of information for my project. I will likely focus largely on password cracking, malware, and how to prevent getting hacked. Even if I do not explain every single type of malware, I want to at least explain the major types such as viruses and keyloggers in my presentation.

11. 2/5/19

Research Results and Findings:

In order to not get any malware, there is specific safety precautions that people can take. One of these is only clicking email links from expected emails; if a random email is sent, it is likely a scam or contains malware. Another precaution is to only install software from trusted websites. Also, it is important to not click any pop ups and it is best to use a pop up blocker.

Using trusted antivirus software, a fire wall, scanning files and flash drives before putting them into a computer, and never leaving a computer unlocked will greatly increase the chances of not getting malware. There are several signs that a computer has malware such as if the computer runs slow, it will not shut down, it displays many pop ups, sends emails that a user did not send, or if battery runs out faster than normal (Malware). I will use this research in my project to explain prevention of malware. It is important to explain how to avoid getting malware so that anyone watching my presentation is able to avoid it.

Thoughts on my Progress:

My research for my project is doing well. I am done researching malware, and I am going to either start researching white hat hackers or phishing. I have a lot of technical research, so it may be a good idea to put some focus on white hat hackers and overall the ethics of hacking. It is interesting to see how different types of hackers use the same methods to achieve different things. Black hat hackers may hack for greed or to hurt a company while white hat hackers try to identify security flaws. Without people using hacks to identify flaws before actual hackers exploit the weaknesses, there would be a lot more interruptions to companies and websites. A large part of cyber security is to identify threats before they happen. I would like to research specific examples of companies getting hacked as well as instances of white hat hackers identifying large security flaws.

12. 2/5/19

Research Results and Findings:

A white hat hacker is an experienced hacker that works for legal organizations such as the FBI or large corporations. These hackers try to identify and stop hacking attempts. As

technology advances, hackers become more dangerous, making white hat hackers essential. Most white hat hackers are known fo previously hacking into what was thought to be secure computer systems. Greg Hoglund is a known white hat hacker that found security weaknesses in the game World of Warcraft and was in the hacktivist group Anonymous. Dan Kaminsky is another known white hat hacker. He found vulnerabilities in sites that used the "Forgot My Password" feature. If a black hat hacker found this first, many websites would have faced problems ("7 White Hat Hackers and the Online Crimes They Help Prevent"). I will use this information to discuss that not all hackers are bad despite the negative connotation to the term. In addition, I will talk about some of the most interesting white hat hackers.

Thoughts on my Progress:

Researching white hat hackers and why people hack will give more to my presentation than just the technical information. Before this research log, I would have really only been discussing hacking in general, password cracking, and malware. However, I want to also show some of the interesting cases that hackers actually helped businesses. I think that the presentation would be most interesting if it first talks about the detailed information, and then based on that information including methods for hacking, it is connected to real world examples. For my remaining logs, I may decide to research phishing, or I may research more situations in which hackers either helped or hurt corporations.

13. 2/5/19

Research Results and Findings:

Phishing is a form of social engineering that is used to steal sensitive information. This occurs when an attacker sends a link through an email or a text message that often gives malware

or is used to steal information. Phishing can lead to unauthorized purchases, stealing of money, and identity theft. Sometimes, phishing is also used to start a large attack by comprising employees first. Then, security will be easy to bypass or will not be secured at all and the malware could be distributed to other employees. When these phishing attacks on large companies are successful, the companies typically lose reputation, the trust of their customers, and a large amount of money ("What is Phishing"). I will use this information to show some of the common ways in which people are hacked. Phishing is very common and very believable a lot of the time, so I want to find out how to exactly know that something is fake.

Thoughts on my Progress:

I feel that I have a large amount of information that will make this presentation both interesting and informative. Not only will this explain hacking, but it will also connect topics such as malware and phishing. I am starting to see connections between phishing and malware after having did the research in this log. Phishing is a way that hackers give malware. Once malware is given, hackers are able to steal the accounts of their victims. In my presentation, which I plan to be a video, I may say a scenario in which someone receives what seems to be an ordinary email, and then show that they randomly got hacked. Then, I may revisit the scenario and explain what the person did wrong and explain how easy it is to get hacked.

14. 2/5/19

Research Results and Findings:

An example of a phishing attempt would be if an email is mass distributed to many faculty members of a university. In the email, it would claim that the password for an account for the university will expire, giving a link to enter a new password. From this, there are two large

possibilities for what the scam will do if the link is clicked. One possibility is that the link redirects to a webpage that looks exactly like the real one, but this page would have a different URL. Another possibility is that the URL does go to the reset password page, but before it redirects to the actual page, it inserts a script in the background to ultimately gain access the university network ("What is Phishing"). I will use this information to give an example of phishing. I feel that the only way for people to understand what phishing truly is, is to show examples, so I will likely show pictures of typical phishing emails.

Thoughts on my Progress:

Phishing will be a good addition to my research. My overall research is in depth and will be useful in my presentation. I have a large amount of information though, so I will need to select the most important pieces of information for my research presentation. Something that I found very interesting in this research is that clicking a URL alone can cause a hacker to have so much access to a computer. I was under the impression that hackers needed to trick people into inputting their information or accepting a download on a fake site through phishing scams. However, I will definitely be more careful after learning this. I will want to mention this in my presentation, as I feel that it is not common knowledge that links themselves can be malicious.

15. 2/5/19

Research Results and Findings:

In making phishing emails, attackers attempt to make them as similar as possible to the emails of legitimate organizations. They may also make it seem like it is urgent that the desired action is taken as soon as possible, such as giving a time limit until something expires. This causes the user to be more likely to make a mistake with the extra pressure. It is important to

make sure that links are correctly spelt in email messages as well. Some links are meant to resemble a link from an organization, and these often lead to websites made by the attacker that look identical to the actual website. Spearfishing is targeting a specific person or enterprise. This involves getting access to information about latest projects and getting employee names. An attacker could send an email to an employee, pretending to be someone from another department, and they could ask for them to log in to view an important document ("What is Phishing"). I will use this information to discuss what makes phishing believable. Knowing how phishing is meant to trick users is the best way to prevent this attack.

Thoughts on my Progress:

I feel that my research is ready for my project. I was able to find a large amount of information in a variety of different parts of hacking. Now all it comes down to in terms of information is determining what information I will use because this is large amount for a five minute presentation. I feel that every topic that I researched is important enough for the presentation, and it really comes down to summarizing and only including the essentials of each part of hacking. For example, I probably have enough information to make the majority of the project about rainbow tables, but I will only want to spend a bit of the presentation time for this part. I can easily summarize that topic to only include the major concepts behind this method, rather than the ideas as to how it works.

Works Cited

"7 White Hat Hackers and the Online Crimes They Help Prevent." *Utica College*, programs.online.utica.edu/articles/white-hat-hackers-preventing-online-crimes-0404. Accessed 8 Feb. 2019.

"Beware of Hacking." *Seton Hall University*, www.shu.edu/technology/beware-of-hacking.cfm. Accessed 8 Feb. 2019.

"Malware." *Kent State University*, www.kent.edu/it/secureit/malware. Accessed 8 Feb. 2019.

"Password Attacks and Countermeasures." *University of Houston-Clear Lake*, www.uhcl.edu/computing/information-security/tips-best-practices/pwattacks. Accessed 8 Feb. 2019.

"What is Phishing." *Incapsula*, www.incapsula.com/web-application-security/phishing-attack-scam.html. Accessed 5 Mar. 2019.