Hw02 – Hackers Wanted

Tanuja Mohan

1. To me, the term hacker describes someone who understands computer security very well and is able to extract information from computer systems that are not theirs. My idea of a hacker was inline with that of the documentary and all the different things hackers were able to accomplish amazed me. I found the interview with Lamo to be very interesting because it shows how hackers are just doing what they do and are some strange humans that are different from the rest of us.

2. The difference between a white hat, black hat, and a grey hat is that a black hat hacker is one who is hacking for maliciousness intent. Black hat hackers hack for personal gain and perform illegal activities. White hat hackers are “ethical hackers” that generally test computer security systems to see how reliable they are. A white hat hacker reports back to the organization the flaws in the computer system. A grey hat hacker does not hack for his or her own personal gains but do commit crimes in the process. A grey hat hacker may enter a computer system without permission and inform the company later, allowing the company to fix the mistake.

3. I believe it is only ok to find vulnerabilities, exploit them, and then report them to the victim if they have permission to do so by the victim. However, if they do not have permission then the hacker may have access to personal/private information that the provider of the information did not intend to have anyone see. I view this as an invasion of privacy and believe this is unethical of the hacker. If the company wants to employ someone to test their security systems then that is ok since permission has been granted.

4. The country I would fear the most in a cyberwar would be Russia. This is because the United State’s relationship with Russia is a little bit tense and events in history such as the cold war have kept both countries on their toes against each other. Even a slight mistake from one country can be viewed as aggression to the other country. Russia providing a sanctuary to Snowden does not help as well since housing Snowden can be seen as Russia supporting the act of leaking documents from the US. I believe the US should invest more in privacy/security software to ensure that its computers and private information cannot be accessed. I also believe that the US should spread its private and important information across multiple database systems and servers. This way a cyber attack on one database will not result in information stored in other system to be stolen as well.

5. Dmitry Sklyarov is a Russian citizen who was accused of circumventing Adobe’s copy protection arrangements and violating the DMCA. The argument is presented that DMCA does apply in Russia, which is where DEF CON was hosted and where Sklyarov is accused of committing the crime at. I believe that Sklyarov is not guilty since he remained within the bounds of legal actions since DMCA does not apply in Russia. Sklyarov was allowed to return back to Russia in December 2001 and in December 2002 Sklyarov was found not guilty of all four charges under the DMCA presented against him.

6. Adrian Lamo broke into the computer networks of many companies including The New York Times, Yahoo!, and Microsoft. He also turned in a U.S. soldier who had supposedly leaked thousands of U.S. government documents to WikiLeaks. What Lamo did is wrong because even if he was turning in the soldier with good intentions, Lamo did not have permission to access that information and the same goes for accessing the computer networks of the listed companies. Nowadays, Lamo has appeared on multiple T.V. shows speaking about his experience and serving as an expert on netcentric crime. He struggled with substance abuse, but is making a recovery and has improved his situation.

7. I agree with this statement because people enjoy doing what they love without pressure and without someone controlling how they do it. Desmond Morris’s Biology of Art describes how Chimpanzees start to dislike painting when they receive a reward for doing it. I see how this can happen. If we get paid for doing something we love we may start to believe that we are not doing it because we love doing it but because we get paid for doing it. I find the work that was done with the book to be very interesting because we have been told that we should do a job that we love and by doing this we will be paid to do what we love. This research shows us that even if we do something we love as a job we will still not be satisfied with what we do and eventually become disinterested in it.

8. ICAAN is an organization responsible for maintaining Internet databases and performs technical maintenance of DNS root zone registries. ICAAN is also in charge of the Internet Protocol address spaces. I feel as though the ICAAN is a needed organization because we need a supervisor to ensure that our databases are secure and properly used. The internet is widely used and a lot of information is being set across network systems causing us to need someone regulating network addresses. However, I am also slightly nervous by how much power the organization has. Hacking into ICAAN’s system would instantly compromise tons and tons of data that we would not be able to recover. This data is the foundation to our network communications over the Internet. Placing so much power and resources in one organization is a risky move but comes with many benefits.

9. Moonlight Maze is a code name given to a series of investigations looking into the hacking of computer systems all over the world (U.S., U.K., Canada, Brazil, etc.). It is believed that these attacks went on for roughly two years. The attacks came primarily through computers in Ohio but appear to be originating from ISPs located in Russia from Monday through Friday, midnight to 9am. In 1999 Moonlight Maze was assembled to counter the attacks. Investigators used wire-taps on the flagged universities to watch the attackers write out their commands. A honey document was used to lure the attackers to steal the document which when opened would provide the location of the machine the attackers were using. These attacks began a new era of cyber-espionage with countries such as China initiating attacks as well.

10. SCADA is a computer system for gathering/analyzing real time data and stands for supervisory control and data acquisition. SCADA is used to recognize an issue, alert the central site, and perform analysis on the issue (e.g. how critical the issue is). Since SCADA controls tons of water and power supplies, if there ever was a breech in SCADA’s control system then thousands or millions of people would be without water and power. Many cyber attacks go unnoticed because the infiltrators enter the system and wait for months or years before actually taking any action. SCADA has many flaws in its system. Some of these flaws include lacking of monitoring, slow updates, lack of knowledge about devices, not understanding traffic, and authentication holes. I see some news articles about a worm infecting a nuclear power plan in Ohio and parts of the Austrian and German power grid nearly going down due to a replicating stray piece of code.

Automate the Boring Stuff – Chapter 3

1. Functions allow us to group code that needs to get executed multiple times. This way we do not have to keep writing the same code over and over again when we want it to be used. We just have to make a call to the function.
2. The function in a code executes when the function is called.
3. def functionName(parameter)
4. When the program reaches a function call it will jump to the top line of the defined function and begin executing there. The function is the block of code that defines the function and gets executed when a function call is made.
5. There is only one global scope and you can create as many local scopes (by creating functions) in Python.
6. The local variables cannot be accessed anymore when the function call returns.
7. A return value is the value that a function call evaluates to. Yes, a return value can be part of an expression.
8. If a function does not have a return statement, then the return value of that function call is None.
9. You need to use the global statement on that variable.
10. The data type for None is NoneType
11. The import statement imports the module areallyourpetsnamederic and allows us to use function calls to access functions that are defined in this module.
12. spam.bacon()
13. Use a try block to prevent a program from crashing when it gets an error
14. The statement that might contain the error is put in the try clause and the except clause contains the code you want to execute if the error is thrown.