Alexander Cannell

Professor Lamoreaux

04/22/12

Computer Forensics

**What is computer forensics?**

Computer forensics is the combat against crimes that range from crimes against children to file system recovery on hacked or damaged machines. Computer forensics specialist recovers data from some sort of digital media that will be used in a criminal proceeding. Digital media means to all the methods of electronic data storage and transfer devices that include cell phones, servers, portable storage device, desktop computer, laptop computer, and so many more devices that stores information. The specialist recovers criminating data than the recovered data can be used in court. What I want to do as a computer forensics specialist is to be consultant to firms and maybe sometimes a freelance computer forensic investigator, which will entail being hired by companies to test how secure their data really is. So I would be mimicking a malicious hacker attempting to gain access to the company’s internal network, to gleam information off the network. Then I would go in and tell the company how to better protect their information.

**Security Risks**

A hacker is someone who willfully penetrates or attempts to penetrate a computer system without authorization. Half of all security breaches occur because of human errors, human ignorance, and omissions. Which hackers can extort by using social engineering, by using some different strategy to gain passwords or personal information. One example is phishing, which is as it sound, when a hacker fishes for information by talking to people or going through private files. People are the easiest way to circumvent network security, which is taking advantage of human error. Kevin Mitnick said in an interview on The Colbert Report, “The human element is the easiest to extort. If I can get a password, just by calling up a secretary and asking for the password, then I don’t even need to waste my time to hack your network.” Kevin Mitnick was the most notorious hacker in the 90’s, pleaded guilty to computer fraud, and admitted to causing ten million dollars’ worth of damages.

Different types of data transmission and hardware hacks are transmission interception which is a man in the middle attack, eavesdropping, sniffing, port access using a port scanner, private address availability to outside routers not properly configured to mask internal subnets, security holes, general public computer access so gaining access to a computer publicly without the users permission, of course insecure passwords which is easily guessable or using default values, and many more. My favorite hack is the Denial of Service Attack (DoS) attempts to make a computer or network resource unavailable to its intended user. One common method of this attack involves floods the target machine with a external communication, DoS attacks are implemented by forcing a computer to reset, or consuming its resources that would provide services. Different examples of DoS attacks Botnet Attack, ICMP Flood, SYN Flood, Teardrop Attack, Duke, Peer to Peer Attack, Low Rate DoS Attack, and Spoofed Attack. The reason I like the DoS Attack is just spamming a computer with information to take control of a machine.

As a computer forensics specialist or a network security administrator you might use to track hackers trying to enter your system is Honey Pots. Honey Pot is a trap set to detect, deflect or insome manner counteract attempts at unauthorized use of information, or in other words a honey pot is security resource who tells lies allowing it to be probed, attacked or compromised. So the purpose is a honey pot is luring a hack into a system where the administrator can watch the hacker getting information about the hacker to catch and prosecute.

**Data Recovery**

As a computer forensics investigator you will need to know how and what to data to recover, data recovery is the definition of computer forensics. Data Recovery is the process where you are recovering salvaging data from damaged, failed corrupted, or inaccessible storage media when the information can’t be accessed in a normal way’s. Let’s say you deleted a file off your computer, but when you delete that data didn’t get of the data. All your computer does is removes the index and assigns it as unallocated space. Unallocated space is also called “free space”, is logical space on a hard drive that the operating system can write over/to. And the opposite of unallocated space is allocated space or used space where the operating system has already written files to.

US CERT, . "Computer forensics." *Us cert*. N.p., 2008. Web. 24 Apr 2012. <http://www.us-cert.gov/reading\_room/forensics.pdf>.

Lamoreaux, Terry. “Computer Forensics Digital Evidence Forensics”. CJ 3100-1. Southern Utah University. 2011. Power Point.

Robertson, Rob. “Network Security Chapter 12”. CSIS 2600-1. Southern Utah University. 2010. Power Point.

Colbert, S.. *The colbert report*. N.p., 2011. Web. 24 Apr 2012. <http://www.colbertnation.com/the-colbert-report-videos/395003/august-18-2011/kevin-mitnick>.