CIS4204.01 **Brandon Thompson**
Dr. Ashokkumar Patel Due: 1/24/21

Lab Homework 1: Configuring Windows Firewall

1 Chapter 1

1.1 Long answer

1. Describe computer forensics in detail.
   Computer forensics is the use of analytical and investigative techniques to identify, collect, examine and preserve evidence/information which is magnetically stored or encoded.

2. Who are the stake holders (users) of digital forensics?
   The military, government agencies, law firms, criminal prosecutors, academia, data recovery firms, corporations, insurance companies, individuals.

3. What is digital evidence? Explain with examples.
   Information that has been processed and assembled so that it is relevant to an investigation and supports a specific finding or determination. Raw information is not in itself evidence. Real evidence is a physical object that someone can touch (ex: a laptop with fingerprints, USB). Documentary evidence is data stored as written matter, on paper or in electronic files (ex: email messages, logs, databases). Testimonial Evidence is information that forensic specialists use to support or interpret real or documentary evidence (ex: system access show that a user stored photographs on a desktop). Demonstrative evidence is information that helps explain other evidence (ex: chart explaining a technical concept to a judge).

4. Describe types of digital forensics analysis.
   Disk forensics analyzes information on stored media such as computer hard drives. Email forensics study the source and content of email as evidence. Network forensics examines network traffic, including transaction logs and real-time monitoring. Internet forensics pieces where and when a use has been on the internet. Software forensics examines malicious computer code (also malware forensics). Live system forensics searches memory in real time, typically on compromised hosts to identify system abuse. Cell phone forensics searches the content of cell phones.

5. Define anti-forensics and obscured information.

6. Describe the Daubert Standard in detail.

1.2 Short Answer

1. Chain of custody
2. Shut down machine
3. In case other devices were connected
4. What is the essence of the Daubert Standard?
   Only tools or techniques that have been accepted
5. Preserve evidence integrity
6. All of the above.
7. 18 U.S.C () 1030, Fraud and related activity in connection with computeres
8. The Pen register and
9. Data hiding
10. Anti-forensic
11. It cannot be changed
12. Testimonial evidence

2 Chapter 2

2.1 Long answer

1. Describe how computer crime “Identity theft” affects forensics.
   Phishing, spyware, discarded information. First the investigator should check for spyware
2. Describe how computer crime “Hacking systems for data” affects forensics.
   SQL injection - check firewall and database logs for connection information. Cross-site scripting - Look for scripts not coded by websites programmers, search web server logs. Password cracking - Check system logs for reboots followed by administrative logins, physical security. Trick tech support - Search system for unrecognized scripts in startup folders, examine usage of compromised account.

3. Describe how computer crime “Internet / computer fraud” affects forensics.
   Begin tracing communications and financial transactions. Data piracy investigations should trace owners of the domains distributing intellectual property.

4. Describe how computer crime “Non-access computer crime” affects forensics.
   Check packet data for source addresses (MAC) or for related information

5. Describe how computer crime “Cyberstalking - harrasement” affects forensics.
   Trace emails and phone records.

2.2 Short answer

1. When investigating a virus, what is the first step?
   Document the virus.

2. Which of the following crimes is most likely to leave email evidence?
   Cyberstalking.

3. Where would you seek evidence that *ophcrack* (or similar password cracking tool) had been used on a Windows server 2008 machine?
   In the logs of the server; look for the reboot of the system.

4. Logic bombs are often perpetrated by who?
   Disgruntled employees.

5. What is the primary reason to take cyberstalking seriously?
   It can be a prelude to real-world violence.

6. What is the starting point for investigating in DoS attacks?
   Tracing the packets.

7. Spyware.

8. With respect to fishing, a good ficticious email gets a ______ response rate, according to the Federal Bureau of Investigation (FBI).
   1 to 3 percentage.

9. _____ refers to phishing with a specific, high-value target in mind.
   Whaling

10. Cross-site scripting (XSS).

11. Which of the following are subclasses of fraud?
    Investment offers and data piracy.

12. Cyberstalking

13. Identity theft

14.