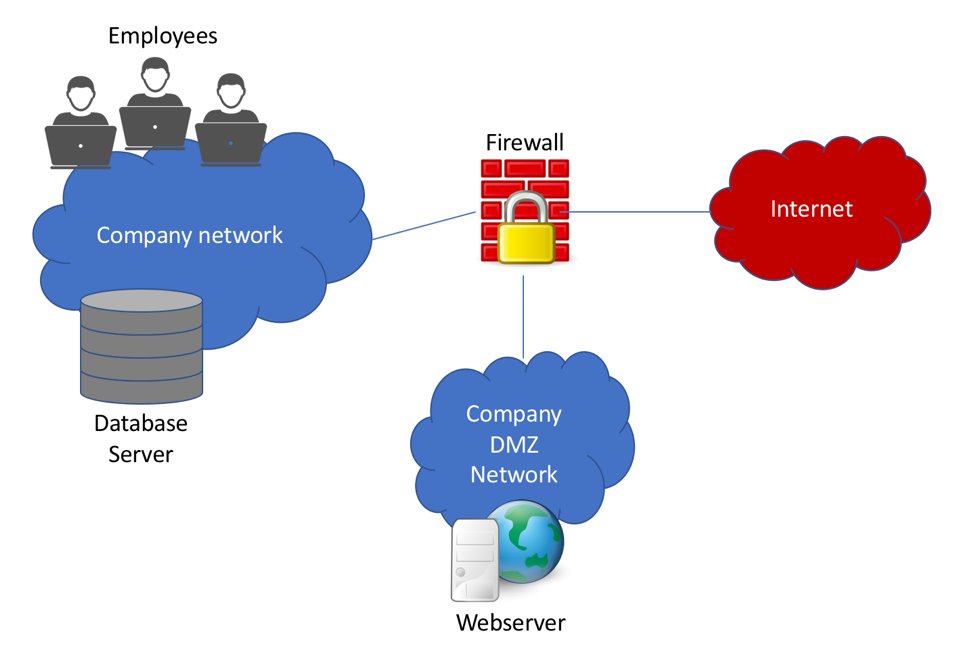
NAME: Megan Leonard

TODAY’S DATE: 1/29/23

# ISEC 375 Homework 1

Answer the following questions based on your reading of the textbook, the module key points, and the instructor’s presentation this week.

1. **[9 points]** You are working as a Digital Forensics and Incident Response Engineer for an enterprise in the finance sector. Cyber threat intelligence software warned that hackers began to share your confidential customer data in some social media channels and private forums. The stolen data are supposed to be stored in the company database only. The network topology of the enterprise and the location of the internal database & web server are shown in the figure. Direct connections from the Internet to the database is supposed to be forbidden by firewall rules. There is a web application hosted by the Web server. Everybody can query the phonebook data stored in the database server using the public web application.

****

It's not clear whether attackers are external entities or insiders. You are designated as the supervisor of the digital investigations group that will manage investigations and conduct forensic analysis of the systems and servers suspected of containing evidence related to the incident. To make an initial assessment about the type of case you're investigating, you are working with one engineer from the Vulnerability/Threat Assessment and Risk Management team, and one engineer from Network Intrusion Detection and Incident Response team. You want to make sure the source of attack firstly, so that you may focus your subsequent efforts to specific areas and points. Which security checks should you expect from the engineers? Please give at least three examples.

Starting with the Vulnerability/Threat Assessment and Risk Management team, we have them test the workstations that are found within the building. We have them test the integrity of them to make sure that no one has an integrity level that they should not have like an intern having the integrity level of a senior engineer. They will check the integrity within the company network that is found with the database server. After the workstation and database server network check, they will test and verify the Company DMZ Network that contains the webserver.

The Network Intrusion Detection and Incident Response team will be using their tools to monitor the network firewall. They will start with looking at the connection between the company network with the database server and the firewall. After that, they will look at the connection between the firewall and the company DMZ network with the webserver. Finally, they will look at the connection between the firewall and the internet.

The Digital Investigations team will start by determining whether they are looking at a public or private investigation. They will take any systems that the other teams find that they believe could have evidence and start conducting the forensics analysis. They will also keep a write up of the chain of custody and make sure everything is written correctly so it cannot be dismissed.

1. **[3 points]** Which forensics investigation most probably start as a civil case, after a while may develop into a criminal case? Please explain why.
2. The case of Chinese hackers who intrude into the systems of a federal agency
3. The case of hackers of an unknown source who intrude into the IT systems of a defense firm that is developing proprietary mission-critical systems for US military

The investigation to start as a civil case would be the second scenario as it starts with a defense firm with an unknown hacker. They can start based off the belief that it could be an internal hacker such as an employee and start investigating with that in mind. As it is a defense firm and not a federal agency it may not start out as a criminal case as they may think that the criminal case would not be cost effective. It will develop into a criminal case if they determine that the hacker gained or tried to gain access to the systems being created for the US military or if they determine the hacker is outside of their area like the Chinese hackers.

* 1. **[3 points]** What is the primary purpose of company policies and warning banners in a private-sector investigation?  
     The primary purpose of the policies and warning banners are to make sure that anyone who is accessing areas they shouldn’t, know the outcome of their actions and can not claim to not know any better. It helps as a means of showing that the person knew what they were doing and that person if working for them, can not turn around a file a wrongful termination lawsuit as there are specific warnings and policies forbidding the actions they have taken.

1. **[6 points]** Suppose that as the principal forensic investigator, you are dealing with a security incident caused by a disgruntled employee. The company security officers capture a USB thumb drive of the employee. You are about to take the USB thumb drive from private security officers and proceed with your investigation by analyzing the data on the thumb drive. Please provide at least two chain of custody rules associated with this investigation.

Everyone who has had access to the USB must be documented including the security officers. This means that everyone who has touched the device needs to be noted else it could be used to drop the case.

The original evidence can not be tampered with and must be copied. This means that you can not access or alter the original evidence as it would mess up the case so you need to create a copy of it that can be accessed, and the original evidence is to be secured so that no one else can access it.

1. **[6 points]** You're taking a systematic approach to the case outlined in question-1. Assume that the suspect is most probably an employee based on the checks of the engineer at the Vulnerability/Threat Assessment and Risk Management. Which risks do you identify, and which controls should you take to mitigate or minimize the risks? Please specify at least one risk and two controls.

One risk is that the person could know about the investigation and work against the teams to cover their tracks. The first control is to close the building so the only people who have access are the teams and any other important people. This should help keep any physical data from being taken by the employee if the workday was to run while they are investigating. Another would be to cut internet and remote access to the building so that no one can remote access their workstation from outside the building and delete any evidence.

1. **[3 points]** What is the difference between a bit-stream copy operation and operating system's copy command?

A bit-stream copy is able create an exact copy of the original. It can copy files that have been deleted and recover file fragments. The copy command can create a copy, but it could miss important files that are hidden from view. The copy command will make a copy of the known files.