On April 20, 2017, at 12:15 am, you receive an automated text on your smartphone from WOOKIE, an old server containing log archives and janitorial records, informing you of unscheduled activity.  After a few hours of combing through logfiles for suspicious inbound and outbound network connections, using Autopsy and Sleuthkit to determine timeline of the events, locate and extract log files, backdoors, and possible keyloggers, and reviewing connections to GANDALF, which holds the HR database, you discover that WOOKIE was compromised.   Here are the events:

* 04/19/2017 11:58 pm:  The hacker connects to the WOOKIE front-end server from 222.23.150.29 (Gansu Agricultural University in Lanzhou, China) using Remote Desktop at 10:32:48 and tries a set of six different credentials (of which 5 had been previously disabled).
* 04/20/2017 12:06 am:  Once logged in, the hacker deploys a bot control channel (which allows remote users to control the local machine without the need to use Remote Desktop)
* 04/20/2017 12:14 am:  The hacker reboots WOOKIE in an attempt to start a backdoor process listening on port 1034.
* 04/20/2017 12:15 am:  System administration team is paged due to unscheduled reboot.
* 04/20/2017 12:20 am:  After reboot, the hacker tries to access other machines within the company’s network, specifically GANDALF, but remains unsuccessful.
* 04/20/2017 12:53 am:  The hacker logs off of WOOKIE after about 1 hour.

Password expiration at your company is set to 180 days.

IN A MS WORD DOCUMENT, ANSWER THE FOLLOWING QUESTIONS:

1. When was the incident discovered and how?

As per the description given above, we identify that System Administrator was been identified with a pager of information that there is a un scheduled reboot occurred to WOOKIE server on 4/20/2017 at 12:15 am is the time when the incident was discovered and notified.

1. What critical pieces of information are missing?

In the Description provided above we observe that Hacker has tried to enter the server with different password at 10:32:48 but it was showing a wrong password attempt as the password where previously disabled, and he had gained access again to the system to 11:58 , so in this we should Identify that there might be some possibility of logs missing of the changes made by the user, and kept only at what time he logged in by using the bot control machine. The time specified might be AM as well we can predict as this is not mentioned in the description. A person might have used a remote connection of China, but he might be residing at a different place and by using a Dynamic IP we can make a login attempt to a required server using rhost. We identify that there is a good time lapse between each activity he made but there is no logs generated on this. The bot which has got added in the system to gain access, but what might be the reason to gain to specific port 1034 is not been identified. There is some mystery on what might the hacker plan on making huge time lapse on completing each activity and complete logs missing. To make a wrong perception, he might have left those logs where the case can be dealt in a wrong manner.

1. Based on what you know, what else would you consider looking into in order to make a better determination of the final consequences of the incident? Be as detailed as you can.

Hacker was trying to access the system using rhost, where he might known some information from a person being inside the company might had provided him the information for his personal use and might have payed him. When this activity is in place, the inside person might want to gain some access to some credible information which would help or else he can also have some access to change some information. In the above specified description, we observe that it is the janitor records, so a janitor records would be required by any HR HR HR or else by any janitor itself, so we can treat that this can be any of the person attack and it is an internal based attack. Both the people are considered to be a non-technical department, so this was been given to outside person and it was a bribed game played by inside person. Sending the information for selling higher bide and gain good money by sending to personal drive.

1. What would be your recommendations for improvement?

Our team would recommend updating Operating Systems and software so that it would be more difficult for hackers to create a backdoor in the server. In this example, the hacker used attempted to reboot an old server – updated software and anti-virus firewalls can help prevent breaches. We would also encourage the use of encrypted passwords if we are using an open wifi network. Keeping passwords updated and diverse will also help to deter hacking attempts.