Homework #2
ITN 261
Bradyn Ritchie

Scenario 1: Domain Name System (DNS) Server Denial of Service (DoS)

On a Saturday afternoon, external users start having problems accessing the organization's public websites. Over the next hour, the problem worsens to the point where nearly every access attempt fails. Meanwhile, a member of the organization's networking staff responds to alerts from an Internet border router and determines that the organization's Internet bandwidth is being consumed by an unusually large volume of User Datagram Protocol (UDP) packets to and from both the organization's public DNS servers. Analysis of the traffic shows that the DNS servers are receiving high volumes of requests from a single external IP address. Also, all the DNS requests from that address come from the same source port.

Answer the following questions for this scenario:

1. Whom should the organization contact regarding the external IP address in question?

I would recommend that the company should get in contact with their IT department or whoever is in charge of the organization's website. Since they are in charge of the website, they may be able to provide more information on the suspicious IP address.

2. Suppose that after the initial containment measures were put in place, the network administrators detected that nine internal hosts were also attempting the same unusual requests to the DNS server. How would that affect the handling of this incident?

The administrators would need to check and see if the internal computers were compromised, though it seems like they already are. From there, the administrators can determine the proper course of action, such as maybe install antivirus on the computer to get rid of the virus that caused it to join the botnet and contribute to the distributed denial of service attack. While they are at it, it would also be wise for the administrators to check all the computers as well.

3. Suppose that two of the nine internal hosts disconnected from the network before their system owners were identified. How would the system owners be identified?

There are probably logs on the system that can identify the users that have access that computer. I an organization, there are normally logs implemented that log everything a user does while they are accessing the system. All the administrators would need to do is obtain these logs and identify the individual with their username.

Scenario 2: Compromised Database Server

On a Tuesday night, a database administrator performs some off-hours maintenance on several production database servers. The administrator notices some unfamiliar and unusual directory names on one of the servers. After reviewing the directory listings and viewing some of the files, the administrator concludes that the server has been attacked and calls the incident response team for assistance. The team’s investigation determines that the attacker successfully gained root access to the server six weeks ago.

Answer the following questions for this scenario:

1. What sources might the team use to determine when the compromise had occurred?

Even though the one of the main steps of a cyber-attack is covering your tracks, the administrators may have gotten lucky and the attacker forgot to change or disable logs and auditing. This would provide the team with an abundant amount of information, such as when the attacker logged in, what changes have been made to the system, and important events that have occurred on the system. Also, if the company had a network intrusion detection system, they would be able to detect the specific date and a vast amount of more information. However, I suppose the organization would have been notified immediately if there was a successful attack when using an intrusion detection system.

2. How would the handling of this incident change if the team found that the database server had been running a packet sniffer and capturing passwords from the network?

Though this should already be done, all accounts for the organization, both normal users and root, need to have their passwords changed. Keeping a compromised password is a major risk and could provide the attacker with a wealth of information if the stolen passwords are used against the organization.

3. How would the handling of this incident change if the team found that the server was running a process that would copy a database containing sensitive customer information (including personally identifiable information) each night and transfer it to an external address?

The customers must be notified of what data was possibly released or copied from the database in order to follow state/federal guidelines and rules. The program that transfers the information to the external address needs to be removed from the server. In order to keep it safe, the organization can transfer the customer data to a server that they know is safe while this action is being performed. This would prevent any more data from being copied from the compromised database.

4. How would the handling of this incident change if the team discovered a rootkit on the server?

The server would most likely have to be decommissioned and have all the files transferred off of it in order to further protect them and serve as a backup. Then, the rootkit must be taken care of through the use of antivirus cleaner or a specialized rootkit remover.

Homework #2
ITN 261
Bradyn Ritchie

Scenario 3: Unauthorized Access to Payroll Records

On a Wednesday evening, the organization's physical security team receives a call from a payroll administrator who saw an unknown person leave her office, run down the hallway, and exit the building. The administrator had left her workstation unlocked and unattended for only a few minutes. The payroll program is still logged in and on the main menu, as it was when she left it, but the administrator notices that the mouse appears to have been moved. The incident response team has been asked to acquire evidence related to the incident and to determine what actions were performed.

Answer the following questions for this scenario:

1. How would the team determine what actions had been performed?

It really depends on what security measures the organization has in place. As with the other scenarios, audits and logs would probably be the best bet. These logs include an abundant amount of information, such as who is logged onto the computer, at what times, and everything that is done on a computer. Of course, all of this is assuming that the log files were not altered by the attacker.

2. How would the handling of this incident differ if the payroll administrator had recognized the person leaving her office as a former payroll department employee?

There would then probably not be much more evidence to collect other than determine what was done to the computer system. The payroll administrator would hopefully be able to provide at least the name of the former payroll employee. From there, the organization could call the police and they could step in to act or arrest the individual.

3. How would the handling of this incident differ if the team had reason to believe that the person was a current employee?

Obviously, the perpetrator would need to be immediately terminated once they determined who it was. This could be relatively simple to figure out if they have proper physical security implementations in place, such as security cameras. They would need to monitor all the video feeds to see who left at what times to go where. Once they determine who it was, they can then consult the police department to have the attacker apprehended.

4. How would the handling of this incident differ if the physical security team determined that the person had used social engineering techniques to gain physical access to the building?

Homework #2
ITN 261
Bradyn Ritchie

In this situation, I feel that the first step should be to determine who gave up the information and how was the social engineering attack was performed, such as through phone calls, emails, or simply just entering the building after having the door held for them. After a social engineering attack has been confirmed, the organization will need to change some of their physical security measures, such as lock combinations or reissuing all employees' new key cards. Also, I recommend the company implement some sort of spam filter for emails, in order to catch potentially fraudulent emails.

5. How would the handling of this incident differ if logs from the previous week showed an unusually large number of failed remote login attempts using the payroll administrator's user ID?

I think that network administrators need to specifically block the IP address from remote connection that is attempting to connect to the system. Also, if remote connection is never needed for the company, it might be wise to disable remote connection for all computers in order to prevent future attacks such as this. In addition to these, it would be wise for the payroll administrator to change their user ID if they are permitted.

6. How would the handling of this incident differ if the incident response team discovered that a keystroke logger was installed on the computer two weeks earlier?

The computer with the keylogger should be decommissioned until the problem is resolved. Also, all other computers in the organization need to be checked for possible keyloggers. If they do not have antivirus software yet, I would recommend that the organization invest in some. This can detect a wide variety of malware and viruses, including keyloggers. Also, all usernames and passwords that were potentially compromised should be changed.