**CMSC 491/791 Active Cyber Defense HW 6**

**Name:**

**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:

	1. What is the full path of the file that stores the authorized key? Explain how you got your answer. (4 pts)
	2. What are the first 8 characters of the public key? (3 pts)
	3. What are the username and hostname associated with the authorized key? (3 pts)
2. Answer the following questions about Attacker 1, who used the authorized public key to connect to the VM:

	1. When did Attacker 1 initially connect to the VM? Provide the month, day, hour, minute, and second. (3 pts)
	2. What protocol did Attacker 1 use to connect to the VM? (3 pts)
	3. Which user did Attacker 1 log in as? (3 pts)
	4. What is Attacker 1’s IP address? (3 pts)
	5. How did you find the answers to questions 2a through 2d? (4 pts)
3. Does the user from question 2c have sudo privileges? Explain why or why not. (8 pts)

1. Answer the following questions about the file that Attacker 1 exfiltrated from the VM:

	1. What is the full command used to exfiltrate this file? Explain how you got your answer. (4 pts)
	2. Why would an attacker want to exfiltrate this file? (4 pts)
2. 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:

	1. What port does the backdoor listen on? Explain how you got your answer. (3 pts)
	2. How would an attacker connect to the backdoor? (3 pts)
	3. What is the full path of the bash script used to launch the backdoor? Explain how you got your answer. (3 pts)
	4. In a few sentences, summarize what this bash script does. (6 pts)
	5. What is the backdoor’s persistence mechanism? (3 pts)

* 1. How would you remove the backdoor’s persistence mechanism? Be specific. (3 pts)

Attacker 2

1. Answer the following questions about Attacker 2, who used the backdoor installed by Attacker 1 connect to the VM:

	1. Which user did Attacker 2 log in as? Explain how you got your answer. (3 pts)
	2. 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)
	3. What IP address did Attacker 2 copy a file from? Explain how you got your answer. (3 pts)
2. Does the user from question 6c have sudo privileges? Explain why or why not. (8 pts)
3. 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)
4. 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)