Review: Quiz 05 – Linux Threat Hunting (Digital Forensics 152361)

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

1

What is the default location of Apache access logs on a Linux computer running the Ubuntu 22.04 operating system? *

- /var/log/apache/access.log
- /var/log/apache2/access.log ✓
- /etc/apache2/access.log
- /usr/sbin/apache2/access.log

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

2

Which of the following directories contain the binary files or executables needed for system maintenance and administrative tasks on a Linux system? *

- /run
- /bin
- /root
- /sbin ✓

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

3

Which command can provide investigators with details of all the loaded modules on a Linux-based system? *

- list modules -a
- lsmod ✓
- plist mod -a
- lsof -m

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

4

In a Linux-based system, what does the command **"last -F"** show? *

- Login and logout times and dates of the system ✓
- Last run processes
- Last functions performed
- Recently opened files

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

5

A Linux system is undergoing investigation. In which directory should the investigators look for its current state data if the system is in powered on state? *

- /auth
- /proc ✓
- /var/log/debug
- /var/spool/cron

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

6

What will the following command accomplish in Linux? **fdisk /dev/hdd** *

- (●) Partition the hard drive ✓
- ( ) Format the hard drive
- ( ) Delete all files under the **/dev/hdd** folder
- ( ) Fill the disk with zeros

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

7

Which of these files helps a forensics investigator to locate the start-up files created by a malware infection on a Linux system? *

- ( ) rc.vimrc file
- ( ) rc.cache file
- ( ) rc.config file
- (●) rc.local file ✓

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

8

With the standard Linux second extended file system (Ext2fs), a file is deleted when the inode internal link count reaches _____ ? *

- (●) 0 ✓
- ( ) 1
- ( ) 10
- ( ) 100

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

9

Which of the following is a record of the characteristics of a file system, including its size, the block size, the empty and the filled blocks and their respective counts, the size and location of the inode tables, the disk block map and usage information, and the size of the block groups? *

- Inode bitmap block
- Superblock ✓
- Block bitmap block
- Data block

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

10

Netstat is a tool for collecting information about network connections. It provides a simple view of TCP and UDP connections, their states, and network traffic statistics. Which of the following commands shows you the TCP and UDP network connections, listening ports, and the identifiers? *

- netstat -r
- netstat -ano ✓
- netstat -b
- netstat -s

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

11

One of the leading challenges in forensics is acquiring volatile memory. Worms such as Code Red are memory-resident and do not write themselves to the hard drive; if you turn the system off, they disappear. In a lab environment, which of the following options would you suggest as the most appropriate way to **capture volatile memory**? *

- Use VMware to be able to capture the data in memory and examine it ✓
- Give the Operating System a minimal amount of memory, forcing it to use a swap file
- Create a Separate partition of several hundred megabytes and place the swap file there
- Use intrusion forensic techniques to study memory resident infections

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

12

During a computer hacking forensic investigation, an investigator is tasked with acquiring volatile data from a live Linux system with limited physical access. Which methodology would be the most suitable for this scenario? *

- Using Belkasoft Live RAM Capturer to extract the entire contents of the computer's volatile memory
- Performing remote acquisition of volatile data from a Linux machine using dd and netcat ✓
- Using the fmem module and dd command locally to access the RAM and acquire its content directly
- Performing local acquisition of RAM using the LiME tool

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

13

Alice is extracting volatile data from a Linux system and using the command history. What is she trying to extract? *

- History of logins to the system
- Previously typed commands ✓
- History of the browser
- Passwords of all users in the system

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

14

In a situation where an investigator needs to acquire volatile data from a live Linux system, but physical access to the suspect machine is restricted or unavailable, which of the following steps would be the most suitable approach to perform this task? *

- The investigator should use the Belkasoft Live RAM Capturer on the forensic workstation, then remotely execute the tool on the suspect machine to acquire the RAM image
- The investigator should initiate a listening session on the forensic workstation using 'netcat', then execute a 'dd' command on the suspect machine and pipe the output using 'netcat'
- The investigator should leverage OSXPMem to remotely parse the physical memory in the Linux machine and create AFF4 format images for analysis
- The investigator should employ the LiME tool and 'netcat', starting a listening session using tcp:port on the suspect machine and then establishing a connection from the forensic workstation using 'netcat' ✓

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

15

Which Linux utility allows searching for strings in files and output? (Choose all that apply) *

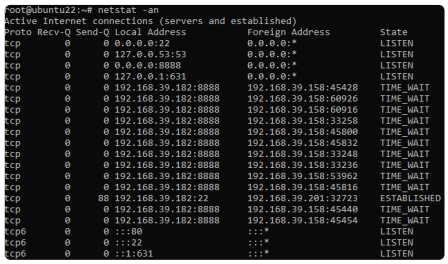
- [ ] cat
- [x] grep ✓
- [ ] echo
- [ ] opensearch
- [ ] pgrep

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

16

Alice is a forensic investigator working for the Ministry of Public Security. She is investigating a computer suspected of being infected with a virus. He runs the **netstat** command on the machine to see its current connections. In the following screenshot, what do the **0.0.0.0** IP addresses signify? *



- [ ] Those connections are established
- [x] Those connections are in listening mode ✓
- [ ] Those connections are in closed/waiting mode
- [ ] Those connections are in timed out/waiting mode

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

17

In the auditd.conf file configuration, the administrator sets the parameter values to **max_log_file = 256** and **num_logs = 4**. How much log data can the audit system store at most at one time? *

- [ ] 512 MB
- [ ] 256 MB
- [x] 1024 MB ✓
- [ ] 64 MB

✗ **Incorrect** 0/0.5 Points

0 / 0.5 pts
Auto-graded

18

What are the advantages of **auditd** over other open-source endpoint solutions like **osquery** and **Sysmon**? (Choose all that apply) *

- [x] Installed by default on most Linux distributions ✓
- [ ] One event is split into multiple logs, making it difficult to investigate
- [ ] Only supports certain OS versions
- [x] Allows analysis and detection of potential threats, attack behaviors, and policy violations

✗ **Incorrect** 0/0.5 Points

0 / 0.5 pts
Auto-graded

19

Which rule in **audit.rules** can allow recording information about the behavior of creating a new user account, **user1**, by executing the **useradd** command on a Linux operating system? (Choose all that apply) *

- [ ] -w /etc/passwd -p w ✓
- [ ] -w /etc/passwd -F perm=wa
- [ ] -a always,exit -F path=/etc/passwd -F perm=w ✓
- [x] -a exit,always -F arch=b64 -S execve -k adduser ✓
- [x] -w /usr/sbin/adduser -p x -k adduser

✓ **Correct** 0.5/0.5 Points

0.5 / 0.5 pts
Auto-graded

20

On a compromised server A, the attacker executes the command **ip="x.x.x.x" && ping $(echo $ip) -c 2** to test the connectivity from that server to another server using the ping command. If the auditd service is configured on server A, which of the following EXECVE records can the digital investigator see? *

- ( ) argc=4 a0="ping" a1="$(echo $ip)" a2="-c" a3="2"
- (•) argc=4 a0="ping" a1="x.x.x.x" a2="-c" a3="2" ✓
- ( ) argc=5 a0="ping" a1="$(echo" a2="$ip)" a3="-c" a4="2"
- ( ) argc=4 a0="ping" a1="ip" a2="-c" a3="2"