**1.**

Question 1

It is MOST important that your incident response policy do which of the following?

1 / 1 point

Ensure that no hacks go unnoticed

Align with overall business or agency security strategy

Minimize the number of unsolved incidents

Make the incident response team more effective

Correct

The MOST important thing is to align with the business. Most of the other things are important, but not MOST important.

**2.**

Question 2

Based on the introduction course and "IR definitions" module, which of the following is LEAST likely to be a triggering event?

1 / 1 point

Notification from a firewall

Report from staff that systems are behaving in unusual ways

An article in the news about a new malware outbreak

Notification from an IDS system

Correct

Staff, IDS and firewalls are all sources of common triggering events. If a company launched an incident response process each time there's a new piece of malware, they'd never get anything done.

**3.**

Question 3

Bob, the incident response manager, has just been given the task of building an internal IR team. Which of these steps should Bob execute first?

1 / 1 point

Purchase new IR tools

Pick team members

Obtain funding

Assess existing skill sets

Correct

Picking team members first is wrong because you shouldn't pick team members until you've assessed what you already have. Obtaining funding first is wrong because you need to get an accurate assessment before being able to create a budget. Purchasing tools should rarely ever be the first thing to do. You need skills assessments, an inventory of existing tools, and many other things before deciding what tools are needed.

**1.**

Question 1

Which Zeek log file would you query to find information about resolved websites from the computers on the network?

0 / 1 point

conn.log

http.log

dns.log

ftp.log

Incorrect

**2.**

Question 2

You have been given a PCAP file and asked to analyze it. The customer has informed you that a malicious file was probably transferred into the environment during the breach in question. You also see evidence in the memory dump from the suspected breached machine that the attacker used the built-in Windows TFTP client to transfer a file down to the suspected breached machine. How would you extract this file transferred via TFTP from the traffic capture (PCAP) file in Wireshark? You are using Wireshark version 2.3.4 or later.

1 / 1 point

With the PCAP open in Wireshark, select Analyze -> Follow -> UDP stream and carve the file from there

With the PCAP open in Wireshark, select File -> Export objects -> TFTP then select the suspect files.

With the PCAP open in Wireshark, select View -> All extracted files

With the PCAP open in Wireshark, select Go -> Extract all files

Correct

File -> Export Objects -> TFTP is the proper step. Note that for older versions of Wireshark, this command does not offer the TFTP option. Analyze -> UDP Stream will show UDP streams but does not offer an option to carve files. There is no feature such as "Extract all files" under Go. There is also no "All Extracted Files" under view.

**3.**

Question 3

You have been hired to help respond to an incident. Once on the site, you are made aware that there is one system on the network which has been identified as compromised. The customer also informs you there's no traffic captures related to the device. Upon investigating the system, you discover that there is an unknown process running on it. You would like to extract the process/application and see what it does. What would be the BEST course of action?

1 / 1 point

Install monitoring software on the compromised machine and configure the monitoring software to record the behavior of the unknown process

Copy the unknown process and put it on a similar machine in the production environment to see if there's an adverse effect

Perform a memory dump, then use the procdump feature of volatility to dump the process to a file. Take the dumped file and upload it to virustotal.com to see what it does and if it's rated as malicious

Perform a memory dump, then use the procdump feature of Volatility to dump the process to a file. Take the dumped process and run it in an isolated sandbox VM that's not connected to anything else

Correct

Dumping the process to a file and then putting it in a sandbox is the best answer. Dumping it and putting it on virustotal.com is bad because if the unknown process has harvested data from the internal network or that device, you may be inadvertently exposing that data to the public via virustotal.com. Installing too much additional software like an intrusive monitoring software could destroy some evidence as well as alert the threat actor as to your activity. It is never a good idea to put potentially malicious or unknown software on other production devices.

**4.**

Question 4

You are examining a memory dump from a compromised machine and would like to see a breakdown of parent/child relationships of currently running processes. Which Volatility plugin would show this?

1 / 1 point

pstree

hives

rel

pslist

Correct

The pstree plugin shows processes in a tree format emphasizing each process's relationship to its parent process. The pslist plugin lists running processes, but does not show relationship info in a tree format. The rel and hives options are not real plugins

**5.**

Question 5

You have just been called in as an outside expert to help an organization with a data breach. They have not started a response process yet and are wanting you to start it. From the list of options here, what would you do FIRST?

1 / 1 point

Immediately start assessing damage

Start triage of known compromised devices

Ask them if they have an existing IR policy and/or playbook

Take memory dumps from all affected devices

Correct

One thing you never want to do is be responsible for having the organization violate its own IR policy. Therefore, it's best to find out if they have one and what it entails. Taking memory dumps is a good choice if you're only thinking in terms of technical steps; however, it's not the first thing that should happen, considering the handler may be new to the environment and internal processes and procedures. Starting triage is not a good first step. Assessing damage is not the best first step.

**6.**

Question 6

Which Volatility plugin allows you to search for files in memory?

1 / 1 point

netscan

dumpfile

procdump

filescan

Correct

All of these are valid Volatility plugins, but only filescan actually searches through memory for files.

**7.**

Question 7

Of the four NIST incident response life cycle steps, which would you consider things like "who can access certain information" and "whom to request the access from" to fall into?

1 / 1 point

Post-incident activity

Preparation

Detection and analysis

Containment, eradication and recovery

Correct

Setting up and figuring out communications paths is usually associated with preparation. Doing this activity in any of the other three steps would be too late.

**8.**

Question 8

You have been giving a 20 GB PCAP file of network traffic. You want to break this file down into smaller pieces to see things such as HTTP traffic and DNS traffic separated out into their own log files. What tool would you use for this?

0 / 1 point

Volatility

TCPdump

Wireshark

Zeek

Incorrect

**9.**

Question 9

Which Volatility plugin would you use to find current and previous network connections for the machine you got the memory dump from?

1 / 1 point

sockscan

connections

cmdscan

netscan

Correct

Sockscan shows sockets, but only for existing connections. Connections only shows existing connections as well. Cmdscan shows previous commands that were run. Netscan is the only plugin that shows both current connections and previous ones.

**10.**

Question 10

Which feature of Wireshark allows you to reconstruct an entire TCP session?

1 / 1 point

Follow TCP stream

View streams

Recreate session

Follow streams

Correct

"Follow TCP stream" is the correct answer. The others are distractors.

**11.**

Question 11

You are looking at live traffic using Zeek. You need to be able to see TCP session state and session history for all connections. Which zeek option/command would you invoke with zeek-cut to show this information, and which Zeek log would you run it against?

1 / 1 point

history against the conn.log

history against the http.log

handshakes against the conn.log

sessions against the conn.log

Correct

The conn.log would contain this information, and the only real option here is history. The others are distractors.

**12.**

Question 12

You have been given a memory dump to analyze for an IR case your team is working on. The person who gave you the memory dump is not sure of what the operating system is. What Volatility plugin allows you to scan the memory dump to find the operating system?

1 / 1 point

oscheck

imgscan

imageinfo

image

Correct

Of all the solutions here, imageinfo is the only one meeting this criterion.

**13.**

Question 13

You are analyzing a packet capture and want to isolate traffic between 192.168.2.10 and 74.56.28.27. Which Wireshark display filter would give you the appropriate view of the traffic between the two?

1 / 1 point

address == 192.168.2.10 & address = 74.56.28.27

ip.addr == 192.168.2.10 && ip.addr == 74.56.28.27

ip = 192.168.2.10 && ip = 74.56.28.27

ip.addr = 192.168.2.10 and ip.addr = 74.56.28.27

Correct

ip.addr == 192.168.2.10 && ip.addr == 74.56.28.27 is the only valid display filter. The others are not valid filters.

**14.**

Question 14

You are analyzing a packet capture file and you want to see traffic from the IP address of 1.1.1.1 to 10.10.10.10, but only to or from port 3389. What would that Wireshark display filter look like?

1 / 1 point

ip.src/dst == 1.1.1.1/10.10.10.10 && dst.port == 3389

ip.src == 1.1.1.1 && ip.dst == 10.10.10.10 && tcp.port == 3389

ip.addr == 1.1.1.1 && ip.addr == 10.10.10.10 && tcp.port 3389

ip/port == 1.1.1.1:3389/10.10.10.10:3389

Correct

There is no Wireshark filter that uses the /, so both those answers are out. ip.src == 1.1.1.1 is the correct answer because the scenario spells out "from" 1.1.1.1. ip.addr == 1.1.1.1 might work, but it would give back too much information as well as showing traffic where 1.1.1.1 is the source as well as the destination.

**15.**

Question 15

What Linux command could you run against a raw memory dump and search for human-readable text?

1 / 1 point

cat

top

strings

lsof

Correct

"Strings" is the command for pulling human-readable text from memory dumps. "Cat" is for viewing text files, "top" is for viewing the processes using the most resources on a running Linux machine and "lsof" is also a process-based viewer.

**16.**

Question 16

Which zeek-cut string would I use to see all conn.log traffic with source and destination IP and port, as well as the duration of each session?

1 / 1 point

zeek-cut < conn.log source.ip source.port dest.ip dest.port len

zeek-cut < conn.log ip.orig\_h ip.orig\_p ip.resp\_h ip.resp\_p duration

None of the above

zeek-cut < conn.log id.orig\_h id.orig\_p id.resp\_h id.resp\_p duration

Correct

Which zeek-cut string would I use to see all conn.log traffic with source and destination IP and port, as well as the duration of each session?

**17.**

Question 17

What volatility feature allows you to extract executable binaries from memory dumps?

1 / 1 point

pstree

consoles

procdump

pslist

Correct

Only procdump allows this. Pslist lists running processes, pstree lists processes and their relationships with other processes and consoles shows recently entered commands and responses.

**18.**

Question 18

What common hacker/pentest tool would you use to see if known malware ports are still open on devices in your network after you've performed eradication?

1 / 1 point

Burp Suite

Cain and Abel

John the Ripper

Nmap

Correct

Nmap is the only port scanner from this list. Cain and Abel and John the Ripper are both password crackers, and Burp Suite is a web app security testing tool and proxy.

**19.**

Question 19

In which phase of IR does the process of making sure the threat can no longer spread happen?

1 / 1 point

Containment

Identification

Recovery

Eradication

Correct

The primary goal of containment is to prevent the further spreading of the threat.

**20.**

Question 20

Which factors have contributed to hard drives being less and less of a source of data breach evidence? (Select TWO)

0 / 1 point

Rapid adoption of cloud services.

Correct

The adoption of solid state drive technology across most industries.

This should not be selected

Attackers evolving to using fileless malware and "living off the land" without dropping binaries on the hard drive.

Correct

Hard drives have grown too big to properly analyze.